Systémy IBM - iSeries

Zabezpečení
Digital Certificate Manager

Verze 5, vydání 4

Systémy IBM - iSeries

Zabezpečení
Digital Certificate Manager

Verze 5, vydání 4

Poznámka

Před použitím těchto informací a před použitím produktu, který podporují, se ujistěte, že jste přečetli informace v části “Poznámky”, na stránce 81.

Deváté vydání (únor 2006)

Toto vydání se týká verze 5, vydání 4, modifikace 0 produktu IBM i5/OS (číslo produktu 5722-SS1) a všech následujících vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tato verze nefunguje na všech modelech počítačů RISC (reduced instruction set computer) ani na modelech CISC.

Obsah

Digital Certificate Manager

Digitální certifikát je elektronický prostředek pro ověřování, který lze použít, pokud je nutno v elektronické transakci provádět prokazování totožnosti. Počet možných použití digitálních certifikátů se stále zvyšuje, což umožňuje zdokonalovat opatření pro zabezpečení sítí. Digitální certifikáty jsou např. zásadní pro konfiguraci a použití SSL (Secure Sockets Layer). Použití SSL vám umožní vytvořit zabezpečená spojení mezi uživateli a aplikacemi na serveru v rámci nedůvěryhodných sítí, jakou je např. Internet. SSL poskytuje jedno z nejlepších řešení ochrany soukromých citlivých dat, jako jsou jména uživatelů a hesla, při použití Internetu. Mnoho služeb a aplikací serveru iSeries, jako například FTP, Telnet nebo HTTP server, poskytují za účelem zajištění utajení dat podporu SSL.

Server iSeries poskytuje rozsáhlou podporu digitálních certifikátů, což vám umožní použít digitální certifikáty jako doklady v řadě aplikací pro zabezpečení. Kromě použití certifikátů při konfiguraci SSL je můžete použít jako doklady při autentizaci klientů jak v transakcích SSL, tak v transakcích v rámci sítí VPN (Virtual Private Network). Digitální certifikáty a přiřazené bezpečnostní klíče můžete používat také k podepisování objektů. Podepisování objektů vám umožňuje zaznamenat změny obsahu objektů nebo pokusy o jeho nedovolené užívání, a to pomocí ověřování podpisů na objektech, které zajišťují integritu objektů.

Využití podpory certifikátů na serveru iSeries je snadné, jestliže k centrální správě certifikátů pro vaše aplikace použijete bezplatně dodávanou funkci DCM. Produkt DCM vám umožní spravovat certifikáty, které obdržíte od kteréhokoliv vydavatele certifikátů (CA). Produkt DCM můžete také použít k tomu, abyste vytvořili a provozovali vlastního, lokálního vydavatele certifikátů a mohli vydávat soukromé certifikáty pro aplikace a uživatele ve vaší organizaci.

Klíčem k efektivnímu použití certifikátů a dosažení přínosů v oblasti bezpečnosti je správné plánování a ohodnocení. Další informace o tom, jak certifikáty fungují a jak lze pomocí produktu DCM spravovat certifikáty a aplikace, které je využívají, uvádějí tato témata:

Novinky ve verzi V5R4

Tato část popisuje, které informace jsou nové nebo se významně změnily v tomto vydání.

Nové informace pro obnovu certifikátů

Tato nová část popisuje krok za krokem proces obnovy existujících certifikátů lokálních nebo internetových CA.

- “Obnovení existujícího certifikátu” na stránce 51

Nové informace pro import certifikátů

Tato nová část popisuje krok za krokem proces importu certifikátů, které jsou umístěny v souborech na vašem nebo jiném serveru.

- “Import certifikátu” na stránce 52

Informace o vylepšení CRL (seznamu odvolaných certifikátů) a protokolu LDAP (Lightweight Directory Access Protocol)

Tato část byla aktualizována a obsahuje nyní informace o anonymního přiřazení serveru LDAP pro zpracování CRL.

- “Správa umístění CRL” na stránce 65
- “Správa umístění LDAP pro uživatelské certifikáty” na stránce 68
- “Umístění seznamu odvolaných certifikátů (CRL)” na stránce 6

Jak zjistit, co je nového nebo co se změnilo

Abyste snadno zjistili, kde byly provedeny technické změny, jsou v těchto informacích použity tyto grafické symboly:

- Obrázek označuje místo, kde začíná nová nebo změněná informace.
- Obrázek označuje místo, kde končí nová nebo změněná informace.

Více informací o tom, co je nového a co se změnilo najdete v tématu Sdělení pro uživatele.

Tisk PDF

Na této straně je uveden postup vytištění celého tohoto tématu ve formě souboru PDF.

Chcete-li si toto téma prohlédnout nebo stáhnout ve formátu PDF, vyberte téma Digital Certificate Manager (velikost souboru je přibližně 600 KB, asi 116 stran).

Jak ukládat soubory ve formátu PDF

Pokud chcete soubor typu PDF uložit na svou pracovní stanici za účelem prohlížení nebo tisku:

1. Klepněte pravým tlačítkem myši na soubor typu PDF ve svém prohlížeči (klepněte pravým tlačítkem myši na výše uvedený odkaz).
2. Pokud používáte program Internet Explorer, klepněte na **Uložit cíl jako...**. Pokud používáte program Netscape Communicator, klepněte na **Save Link As**.
3. Vyhledejte adresář, do něhož chcete soubor typu PDF uložit.
4. Klepněte na **Uložit**.

Jak stáhnout produkt Adobe Reader

K prohlížení a tisku těchto souborů ve formátu PDF potřebujete produkt Adobe Acrobat Reader. Jeho kopii si můžete stáhnout z webových stránek společnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

Koncepty produktu DCM

V této části najdete informace o tom, co to jsou digitální certifikáty a jak fungují. Dovíte se o různých typech certifikátů a o tom, jak je lze použít v rámci vaší strategie zabezpečení.

Předtím, než začnete používat digitální certifikáty v rámci rozšíření strategie zabezpečení vašeho systému a sítě, musíte dobře chápat význam certifikátů a jaké přínosy v oblasti zabezpečení ochrany dat poskytují.

Digitální certifikát je digitální doklad, který potvrzuje platnost totožnosti vlastníka certifikátu, podobně jako např. cestovní pas. Identifikační informace poskytované digitálním certifikátem jsou známy pod názvem rozlišovací jméno subjektu. Důvěryhodná strana, zvaná vydavatel certifikátů (CA), vydává digitální certifikáty uživatelům nebo organizacím. Důvěra ve vydavatele certifikátů je základem důvěry v certifikát jako platný doklad.

Digitální certifikát také obsahuje veřejný klíč, který je součástí dvojice klíčů veřejný-soukromý. Různé zabezpečovací funkce spoléhají na použití digitálních certifikátů a dvojic klíčů k nim přidružených. Pomocí digitálních certifikátů můžete konfigurovat relace SSL (Secure Sockets Layer), čímž zajistíte zabezpečené komunikační relace mezi uživateli a aplikacemi vašeho serveru. Tuto ochranu můžete rozšířit konfigurací mnoha aplikací, které podporují SSL, a požadovat certifikáty místo uživatelských jmen a hesel kvůli lepšímu zajištění uživatelské autentizace.

Další informace o principu fungování digitálních certifikátů naleznete v těchto tématech:

Rozšíření certifikátu

Rozšíření certifikátu jsou informační pole, která poskytují dodatečné informace o certifikátu.

Rozšíření certifikátu poskytují nástroje k rozšíření původních standardů x.509. Zatímco informace pro některá rozšíření jsou poskytovány za účelem rozšíření identifikačních informací certifikátu, jiná rozšíření poskytují informace o šifrovacích funkcích certifikátu.

Ne všechny certifikáty používají pole pro rozšíření, aby rozšířily rozlišovací jméno a další informace. Počet a typ rozšířených polí, která certifikáty používají, se liší mezi vydavateli certifikátů, kteří certifikáty vydávají.

Například lokální CA, který poskytuje produkt DCM (Digital Certificate Manager), vám umožní použít pouze rozšíření certifikátu Alternativní jméno subjektu. Toto rozšíření umožňuje přiřadit certifikát ke specifické IP adrese, plně kvalifikovanému jménu domény nebo adrese elektronické pošty. Pokud zamýšlíte používat certifikát k identifikaci koncového bodu připojení iSeries VPN (Virtual Private Network), musíte poskytnout informace pro tato rozšíření.

Související pojmy

"Rozlišovací jméno"
V této části najdete informace o identifikačních charakteristikách digitálních certifikátů.

Obnovení certifikátu

Proces obnovení certifikátu, který používá produkt DCM, se liší dle typu vydavatele certifikátů (CA), který příslušný certifikát vydal.

Pokud použijete lokálního CA k podepsání obnoveného certifikátu, použije produkt DCM poskytnuté informace k vytvoření nového certifikátu v aktuální paměti certifikátů a dřívější certifikát zachová.

Pokud k vydání certifikátu používáte známého internetového CA, můžete obnovu certifikátu obsluhovat jedním ze dvou způsobů: importovat obnovený certifikát ze souboru, který obdržíte od vydavatele certifikátů pro podepisování, nebo nechat DCM pro certifikát vytvořit dvojici klíčů. Produkt DCM poskytuje první volbu v případě, že dáváte přednost obnovení certifikátu přímo s CA, který jej vydal.

Pokud zvolíte vytvoření nové dvojice klíčů, ovládá produkt DCM obnovu stejným způsobem, jakým ovládal vytváření certifikátu. Produkt DCM vytvoří novou dvojici klíčů (veřejný-soukromý) pro obnovený certifikát a vygeneruje požadavek CRS (požadavek na podepsání certifikátu) zahrnující veřejný klíč a další informace, které jste uvedli pro nový certifikát. CSR můžete použít pro požadavek na nový certifikát od VeriSign nebo jiného veřejného CA. Jakmile od CA obdržíte podepsaný certifikát, můžete produkt DCM používat k importu certifikátů do odpovídající paměti certifikátů. Paměť certifikátů potom obsahuje obě kopie certifikátu, původní a nově vydaný, obnovený certifikát.

Pokud nenecháte DCM vygenerovat novou dvojici klíčů, DCM vás povede procesem importu obnoveného, podepsaného certifikátu ze stávajícího souboru, který jste obdrželi od CA, do paměti certifikátů. Předchozí certifikát je pak nahrazen importovaným, obnoveným certifikátem.

Rozlišovací jméno

V této části najdete informace o identifikačních charakteristikách digitálních certifikátů.

Každý CA má určitou strategii, která určuje, jaké identifikační informace tento CA vyžaduje pro vydání certifikátu. Někteří veřejní internetoví CA vyžadují jen málo informací, jako např. jméno a adresu elektronické pošty. Jiní veřejní CA mohou před vydáním certifikátu vyžadovat přísnější prokázání těchto identifikačních informací. Například CA, kteří podporují standardy PKIX (Public Key Infrastructure Exchange), mohou před vydáním certifikátu požadovat, aby žadatel verifikoval identifikační informace prostřednictvím tzv. vydavatele registrace (Registration Authority, RA). Jestliže tedy plánujete používat certifikáty jako prostředek pro ověřování, měli byste se seznámit s požadavky na způsob identifikace u různých CA, abyste zjistili, zda jejich požadavky odpovídají vašim potřebám v oblasti zabezpečení.

Rozlišovací jméno (Distinguished name, DN) je termín, který popisuje identifikační informace certifikátu a je součástí certifikátu samotného. Certifikát obsahuje informaci o rozlišovacím jméně jak pro vlastníka, tak pro žadatele certifikátu (takzvané rozlišovací jméno subjektu) a o CA, který vydává certifikát (nazývá se rozlišovací jméno vydavatele). V závislosti na identifikační metodě CA, který certifikát vydává, může DN obsahovat řadu různých informací. Pomocí produktu Digital Certificate Manager (DCM) můžete provozovat soukromého vydavatele certifikátů a vydávat soukromé certifikáty. Pomocí produkt DCM také můžete generovat informace v DN a dvojice klíčů pro certifikáty, které vaší organizaci vydává veřejný internetový CA. Informace v DN, které můžete vygenerovat pro oba typy certifikátu, obsahují tyto údaje:

- běžné jméno vlastníka certifikátu
- organizace
- organizační jednotka
- lokalita nebo město
- stát nebo oblast
- země nebo region

Pokud pomocí produktu DCM vydáváte soukromé certifikáty, můžete prostřednictvím rozšíření certifikátu uvádět pro certifikát další DN informace, včetně:

- duplicitní IP adresa
- plně kvalifikované jméno domény
- adresa elektronické pošty

Související pojmy

“Rozšíření certifikátu” na stránce 3
Rozšíření certifikátu jsou informační pole, která poskytují dodatečné informace o certifikátu.

Digitální podpisy

Digitální podpis na elektronickém dokumentu nebo jiném objektu je vytvořen za použití určité formy šifrování a je ekvivalentem osobního podpisu na psaném dokumentu.

Digitální podpis poskytuje důkaz o původu objektu a prostředek ověření integrity objektu. Vlastník digitálního certifikátu ″podepisuje″ objekt pomocí soukromého klíče certifikátu. Příjemce objektu použije odpovídající veřejný klíč certifikátu k dešifrování podpisu, který ověřuje integritu podepsaného objektu a ověřuje odesílatele jako zdroj objektu.

Vydavatel certifikátů (CA) podepisuje certifikáty, které vydává. Tento podpis sestává z datového řetězce, který je zašifrován soukromým klíčem vydavatele certifikátů. Libovolný uživatel pak může ověřit podpis na certifikátu, použije-li veřejný klíč vydavatele certifikátů k dešifrování podpisu.

Digitální podpis je elektronický podpis, který vy nebo určitá aplikace vytvoří na objektu pomocí soukromého klíče digitálního certifikátu. Digitální podpis na objektu poskytuje jedinečnou elektronickou vazbu mezi totožností podepisovatele (vlastníka podepisovacího klíče) a původem objektu. Když přistupujete k objektu, který obsahuje digitální podpis, můžete ověřit podpis na objektu a zjistit tak, zda je zdroj objektu platný (například že aplikace, kterou právě stahujete, pochází z autorizovaného zdroje, jako je např. IBM). Proces verifikace vám rovněž umožní zjistit, zda u objektu nedošlo od okamžiku jeho podepsání k nějakým neautorizovaným změnám.

Příklad použití digitálního podpisu

Vývojář softwaru vytvořil aplikaci pro operační systém i5/OS a chce ji distribuovat prostřednictvím Internetu, což je pro jeho zákazníky pohodlný a efektivní způsob. Uvědomuje si však, že zákazníci mají oprávněné obavy ze stahování programů z Internetu vzhledem k rostoucímu počtu objektů, které se tváří jako normální programy, avšak ve skutečnosti obsahují škodlivé programy, např. viry.

Proto se rozhodne, že bude aplikaci digitálně podepisovat, aby si zákazníci mohli ověřit, že zdrojem aplikace je skutečně jeho společnost. K podpisu aplikace použije soukromý klíč digitálního certifikátu, který získal od známého veřejného vydavatele certifikátů. Pak dá aplikaci k dispozici zákazníkům ke stažení. Součástí stahovaného balíku je i

kopie digitálního certifikátu, který použil k podepsání objektu. Když zákazník stahuje aplikační balík, může pomocí veřejného klíče certifikátu ověřit podpis na aplikaci. Zákazník takto může identifikovat a ověřit zdroj aplikace, a zároveň si ověří, že obsah objektu s aplikací nebyl od okamžiku podpisu objektu změněn.

Související pojmy

"Vydavatel certifikátu (CA)"
Vydavatel certifikátů (CA) je důvěryhodná centrální administrační entita, která může vydávat digitální certifikáty uživatelům a serverům.

"Šifrování" na stránce 8
Tato část popisuje, co je to šifrování a jak digitální certifikáty používají funkce šifrování při zajišťování zabezpečení.

"Dvojice veřejného a soukromého klíče"
Každý digitální certifikát má dvojici přiřazených šifrovacích klíčů, která se skládá ze soukromého a veřejného klíče.

Dvojice veřejného a soukromého klíče

Každý digitální certifikát má dvojici přiřazených šifrovacích klíčů, která se skládá ze soukromého a veřejného klíče.

Poznámka: Výjimkou z tohoto pravidla jsou certifikáty pro ověřování podpisů, které mají přiřazený pouze veřejný klíč.

Veřejný klíč je součástí digitálního certifikátu vlastníka a může ho použít kdokoliv. Soukromý klíč je však vlastníkem chráněn a je k dispozici pouze jemu. Tento omezený přístup zaručuje, že komunikace, používající daný klíč, jsou zabezpečené.

Vlastník certifikátu používá tyto klíče k tomu, aby využil výhod šifrovacích bezpečnostních funkcí, které klíče nabízejí. Vlastník certifikátu může např. použít soukromý klíč certifikátu k tomu, aby ″podepsal″ a zašifroval data, jako je např. zpráva, dokument nebo kód, posílaná mezi uživateli a servery. Příjemce podepsaného objektu pak může použít veřejný klíč obsažený v certifikátu podepisovatele, aby podpis dešifroval. Tyto digitální podpisy zajišťují spolehlivost původu objektu a poskytují prostředek pro ověření integrity objektu.

Související pojmy

"Digitální podpisy" na stránce 4
Digitální podpis na elektronickém dokumentu nebo jiném objektu je vytvořen za použití určité formy šifrování a je ekvivalentem osobního podpisu na psaném dokumentu.

"Vydavatel certifikátu (CA)"
Vydavatel certifikátů (CA) je důvěryhodná centrální administrační entita, která může vydávat digitální certifikáty uživatelům a serverům.

Vydavatel certifikátu (CA)

Vydavatel certifikátů (CA) je důvěryhodná centrální administrační entita, která může vydávat digitální certifikáty uživatelům a serverům.

Důvěra ve vydavatele certifikátů je základem důvěry v certifikát jako platný doklad. CA pomocí svého soukromého klíče vytváří na certifikátu, který vydává, digitální podpis, aby potvrdil platnost původu certifikátu. Ostatní mohou ověřit autenticitu certifikátů, které CA vydává a podepisuje, pomocí veřejného klíče vydavatele certifikátů.

CA může být buď veřejná komerční entita, jako je např. VeriSign, nebo to může být soukromá entita, kterou organizace provozuje pro své interní účely. Některé společnosti poskytují komerční služby vydavatele certifikátů pro uživatele Internetu. Produkt Digital Certificate Manager (DCM) vám umožňuje používat certifikáty od veřejných CA i soukromých CA.

Produkt DCM můžete také použít k tomu, abyste provozovali vlastního, soukromého vydavatele certifikátů a mohli pro aplikace a uživatele vydávat soukromé certifikáty. Když lokální CA vydá uživatelský certifikát, produkt DCM automaticky přiřadí tento certifikát k uživatelskému profilu na serveru iSeries nebo jiné totožnosti uživatele. To, zda produkt DCM přiřadí certifikát k uživatelskému profilu nebo k jiné totožnosti uživatele závisí na tom, zda jste produkt

DCM nakonfigurovali tak, aby používal produkt EIM (Enterprise Identity Mapping). Tím je zajištěno, že se přístupová a autorizační oprávnění certifikátu shodují s oprávněními vlastníka daného uživatelského profilu.

Status důvěryhodný zdroj

Slovní spojení důvěryhodný zdroj se týká zvláštního pojmenování, jímž je označen certifikát vydavatele certifikátů. Toto určení - důvěryhodný zdroj - umožňuje, aby prohlížeč nebo jiná aplikace autentizovaly a přijímaly certifikáty, které tento vydavatel certifikátů vydá.

Když stahujete nějaký certifikát CA do svého prohlížeče, prohlížeč vám umožní, abyste jej označili jako důvěryhodný zdroj. Ostatní aplikace, které podporují použití certifikátů, musí být také nakonfigurovány tak, že nejprve musí důvěřovat danému CA a pak teprve mohou provést autentizaci certifikátů od tohoto CA a důvěřovat jim.

Pomocí produktu DCM lze aktivovat nebo deaktivovat status důvěryhodného zdroje u certifikátů CA. Pokud zaktivujete určitý certifikát CA, můžete uvést, že aplikace mohou certifikát použít k autentizaci a schvalování certifikátů, které daný CA vydá. Jestliže určitý certifikát CA deaktivujete, nemůžete uvést, že aplikace mohou certifikát použít k autentizaci a schvalování certifikátů, které daný CA vydá.

Strategická data vydavatele certifikátů

Když vytváříte lokálního CA pomocí programu DCM, můžete pro lokálního CA zadat data týkající se zásad. Data týkající se zásad lokálního CA popisují oprávnění k podpisu, jež CA vlastní. Data týkající se zásad určují:

- Zda může lokální CA vydávat a podepisovat uživatelské certifikáty.
- Jak dlouho jsou certifikáty vydané lokálním CA platné.

Související pojmy

“Digitální podpisy” na stránce 4
Digitální podpis na elektronickém dokumentu nebo jiném objektu je vytvořen za použití určité formy šifrování a je ekvivalentem osobního podpisu na psaném dokumentu.

“Dvojice veřejného a soukromého klíče” na stránce 5
Každý digitální certifikát má dvojici přiřazených šifrovacích klíčů, která se skládá ze soukromého a veřejného klíče.

Umístění seznamu odvolaných certifikátů (CRL)

Seznam odvolaných certifikátů (CRL) je soubor, který obsahuje všechny neplatné a odvolané certifikáty pro určitého vydavatele certifikátů (CA).

Vydavatelé certifikátů periodicky aktualizují své CRL a dávají je k dispozici ostatním, aby je mohli publikovat v adresářích LDAP. Někteří CA, např. SSH ve Finsku, publikují CRL sami v adresářích LDAP, ke kterým lze přistupovat přímo. Jestliže CA publikuje svůj vlastní CRL, certifikát tuto skutečnost indikuje tím, že obsahuje distribuční místo CRL ve formě URI (Uniform Resource Identifier).

Pomocí produktu DCM (Digital Certificate Manager) můžete definovat a spravovat umístění CRL, čímž zajistíte ještě přísnější autentizaci certifikátů, které používáte nebo které přijímáte od ostatních. Definice umístění CRL popisuje umístění serveru LDAP (Lightweight Directory Access Protocol), na němž je uložen CRL, a informace o přístupu k němu.

| Při připojení k serveru LDAP musíte poskytnout DN a heslo, abyste se vyvarovali anonymnní vazby na server LDAP.
| Anonymní vazba na server nezajišťuje úroveň zabezpečení potřebnou pro přístup ke ”kritickým” atributům jako je
| například CRL. V takovém případě může produkt DCM potvrdit odvolaný certifikát, protože není schopen získat
| správný stav z CRL. Pokud potřebujete anonymní přístup k serveru LDAP, pak musíte použít nástroj Directory Server
| Web Administration Tool a vybrat úlohu ″Správa schématu″ za účelem změny třídy zabezpečení (která je nazývána
| rovněž jako ″přístupová třída″) u atributů **certificateRevocationList** a **authorityRevocationList** z hodnoty ″kritický″
| na hodnotu ″normální″.

Aplikace provádějící autentizaci certifikátů přistupují do místa uložení CRL daného CA, pokud je toto definováno, a ověřují, zda CA určitý certifikát neodvolal. Produkt DCM vám umožňuje definovat a spravovat informace o umístění CRL, které aplikace potřebují při práci s CRL v průběhu autentizace certifikátů. Příklady aplikací a procesů, které mohou provádět zpracování CRL při autentizaci certifikátů jsou: server IKE (Internet Key Exchange) v rámci VPN, aplikace, které umožňují SSL (Secure Sockets Layer), nebo proces podepisování objektů. Pokud nadefinujete umístění CRL a přidružíte ho k certifikátu CA, bude produkt DCM provádět zpracování CRL jako součást procesu ověřování certifikátů, které tento CA vydává .

Související pojmy

"Potvrzování certifikátů a aplikací" na stránce 64
Pomocí produktu DCM (Digital Certificate Manager) můžete potvrzovat jednotlivé certifikáty nebo aplikace, které je používají. Seznam věcí, které produkt DCM kontroluje, se mírně liší podle toho, zda se potvrzuje certifikát nebo aplikace.

Související úlohy

"Správa umístění CRL" na stránce 65
Pomocí produktu DCM (Digital Certificate Manager) můžete definovat a spravovat informace o umístění seznamu odvolaných certifikátů (CRL) pro určitého vydavatele certifikátů (CA), který se pak používá v rámci procesu potvrzování certifikátu.

Paměti certifikátů

Paměť certifikátů je speciální soubor databáze klíčů, který produkt DCM (Digital Certificate Manager) používá pro uložení digitálních certifikátů.

Paměť certifikátů také obsahuje soukromý klíč certifikátu, pokud se nerozhodnete klíč uložit do produktu IBM Cryptographic Coprocessor. Produkt DCM vám umožňuje vytvořit a spravovat několik typů pamětí certifikátů. Přístup do pamětí certifikátů řídí produkt DCM pomocí hesel a také prostřednictvím řízení přístupu k adresáři integrovaného systému souborů a k souborům, které vytvářejí paměti certifikátů.

Paměti certifikátů se dělí na základě toho, jaké typy certifikátů obsahují. Podle typu certifikátu, jenž paměť certifikátů obsahuje, se liší administrátorské úlohy, které lze pro danou paměť certifikátů provádět. Produkt DCM nabízí tyto předdefinované paměti certifikátů, které lze definovat a spravovat:

Lokální vydavatel certifikátů (CA)
Tuto paměť certifikátů produkt DCM používá k uložení certifikátu lokálního CA a jeho soukromého klíče v případě, že vytvoříte lokálního CA. Certifikát v této paměti certifikátů se používá k podepisování certifikátů, které vydává lokální CA. Když lokální CA vydá certifikát, produkt DCM uloží kopii certifikátu CA (bez soukromého klíče) do příslušné paměti certifikátů (např. *SYSTEM) pro účely autentizace. Aplikace používají certifikáty CA k tomu, aby ověřily původ certifikátu, jehož platnost musí potvrdit v rámci procesu SSL při poskytování oprávnění k prostředkům.

***SYSTEM**
Produkt DCM používá tuto paměť certifikátů při správě serverových a klientských certifikátů, které aplikace používají při navazování komunikačních relací SSL (Secure Sockets Layer). Aplikace společnosti IBM iSeries (a aplikace mnohých dalších vývojářů softwaru) jsou naprogramovány tak, že používají pouze certifikáty uložené v paměti certifikátů *SYSTEM. Když pomocí produktu DCM vytváříte lokálního CA, DCM tuto paměť certifikátů vytvoří v rámci tohoto procesu. Pokud se rozhodnete získávat certifikáty pro své serverové nebo klientské aplikace od veřejného CA, jako je např. VeriSign, musíte tuto paměť certifikátů vytvořit.

***OBJECTSIGNING**
Produkt DCM používá tuto paměť certifikátů při správě certifikátů, které se používají k digitálnímu podepisování objektů. Úlohy v této paměti certifikátů vám umožní vytvářet digitální podpisy na objektech a rovněž podpisy zobrazovat a ověřovat. Když pomocí produktu DCM vytváříte lokálního CA, DCM tuto paměť certifikátů vytvoří v rámci tohoto procesu. Pokud se rozhodnete získávat certifikáty pro podepisování objektů od veřejného CA, jako je např. VeriSign, musíte tuto paměť certifikátů vytvořit.

***SIGNATUREVERIFICATION**
Produkt DCM používá tuto paměť certifikátů při správě certifikátů, které se používají k ověření digitálního

podpisu na objektech. Chcete-li ověřit digitální podpis, musí tato paměť certifikátů obsahovat kopii certifikátu, kterým je objekt podepsaný. Paměť certifikátů musí také obsahovat kopii certifikátu CA pro toho CA, který vydal certifikát pro podepisování objektů. Tyto certifikáty získáte buď pomocí exportu certifikátů pro podepisování objektů v aktuálním systému do této paměti, nebo pomocí importu certifikátů, které získáte od podepisovatele objektu.

Jiná systémová paměť certifikátů
Tato paměť certifikátů představuje alternativní místo uložení serverových a klientských certifikátů, které používáte pro relace SSL. Jiné systémové paměti certifikátů jsou uživatelsky definované sekundární paměti certifikátů pro certifikáty SSL. Volba Jiná systémová paměť certifikátů vám umožní správu certifikátů pro aplikace, které naprogramujete vy nebo někdo jiný a které používají rozhraní SSL_Init API k programovanému přístupu a použití certifikátů při vytváření relace SSL. Díky tomuto rozhraní API může aplikace používat předvolený certifikát pro určitou paměť certifikátů namísto certifikátu, který konkrétně určíte. Nejčastěji se tato paměť certifikátů používá při migraci certifikátů z dřívějšího vydání produktu DCM nebo tehdy, když je potřeba vytvořit zvláštní podmnožinu certifikátů určených pro použití v SSL.

Poznámka: Jestliže máte ve vašem systému nainstalován produkt IBM Cryptographic Coprocessor, můžete si vybrat jiné volby pro ukládání soukromého klíče vašich certifikátů (s výjimkou certifikátů pro podepisování objektů). Můžete se rozhodnout, že soukromý klíč uložíte v koprocesoru samotném, nebo můžete pomocí něj zašifrovat soukromý klíč a ten uložit ve zvláštním souboru klíčů namísto v paměti certifikátů.

Produkt DCM řídí přístup k pamětem certifikátů prostřednictvím hesel. Produkt DCM rovněž zajišťuje řízení přístupu k adresáři integrovaného systému souborů a k souborům, které vytvářejí paměti certifikátů. Paměti certifikátů typu Lokální vydavatel certifikátů (CA), *SYSTEM, *OBJECTSIGNING a *SIGNATUREVERIFICATION musí být umístěny ve specifických cestách v rámci integrovaného systému souborů. Jiné systémové paměti certifikátů mohou být umístěny kdekoliv v integrovaném systému souborů.

Související pojmy

“Typy digitálních certifikátů” na stránce 27
V této části najdete informace o různých typech certifikátů, které můžete použít a jak jsou použity v produktu DCM.

Šifrování

Tato část popisuje, co je to šifrování a jak digitální certifikáty používají funkce šifrování při zajišťování zabezpečení.

Kryptografie (šifrování) je věda o zabezpečení dat. Šifrování vám umožňuje ukládat informace nebo komunikovat s jinými stranami tak, že přitom zabraňuje nezúčastněným stranám, aby uloženým informacím nebo komunikaci porozuměly. Šifrování převádí srozumitelný text do nesrozumitelné části dat (šifrovaný text). Dešifrování vytváří z nečitelných dat opět srozumitelný text. Oba procesy zahrnují matematickou formuli či algoritmus a tajnou sekvenci dat (klíč).

Existují dva typy šifrování:

- V šifrování se **sdíleným nebo tajným klíčem (symetrické)** je jeden klíč sdíleným tajemstvím mezi dvěma komunikujícími stranami. Šifrování a dešifrování používá stejný klíč.
- V šifrování s **veřejným klíčem (asymetrické)** používá zašifrování i dešifrování různé klíče. Jedna strana má dvojici klíčů, která se skládá z veřejného klíče a soukromého klíče. Veřejný klíč se distribuuje volně, obvykle jako součást digitálního certifikátu, zatímco soukromý klíč si jeho vlastník udržuje v tajnosti. Tyto dva klíče jsou matematicky příbuzné, ale je prakticky nemožné odvodit soukromý klíč od veřejného klíče. Objekt, např. zpráva, který je zašifrován pomocí něčího veřejného klíče, lze dešifrovat pouze pomocí přiřazeného soukromého klíče. Alternativně může server nebo uživatel pomocí soukromého klíče ″podepsat″ objekt a příjemce pak použije odpovídající veřejný klíč k dešifrování digitálního podpisu a ověří tak zdroj a integritu objektu.

Související pojmy

“Digitální podpisy” na stránce 4
Digitální podpis na elektronickém dokumentu nebo jiném objektu je vytvořen za použití určité formy šifrování a je ekvivalentem osobního podpisu na psaném dokumentu.

"SSL (Secure Sockets Layer)"
Produkt SSL (Secure Sockets Layer), který původně vyvinula společnost Netscape, je odvětvovým standardem pro šifrování relací mezi klienty a servery.

IBM Cryptographic Coprocessors for iSeries

Produkt Cryptographic Coprocessor poskytuje ověřené šifrovací služby, které zajišťují soukromí a integritu pro vznikající aplikace e-businessu.

Použití produktu IBM Cryptographic Coprocessor for iSeries umožní vašemu systému používat vysoce zabezpečené šifrování. Jestliže máte ve svém systému nainstalovaný a logicky zapnutý šifrovací koprocesor, můžete jej používat pro bezpečnější ukládání soukromých klíčů vašich certifikátů.

Produkt Cryptographic Coprocessor můžete využít k uložení soukromého klíče certifikátu pro server, certifikátu pro klienta nebo certifikátu lokálního vydavatele certifikátu. Šifrovací koprocesor však nelze použít pro uložení soukromého klíče uživatelského certifikátu, neboť tento klíč musí být uložen v systému uživatele. V současné době také nelze pomocí koprocesoru uložit soukromý klíč certifikátu pro podepisování objektů.

Soukromý klíč certifikátu můžete buď přímo uložit do šifrovacího koprocesoru, nebo můžete využít hlavní klíč šifrovacího koprocesoru k zašifrování klíče, a ten pak uložit ve speciálním souboru klíčů. Tyto volby uložení klíče pomocí koprocesoru lze vybrat v rámci procesu vytváření nebo obnovy certifikátu. Jestliže pomocí koprocesoru ukládáte soukromý klíč certifikátu, můžete také změnit přiřazení koprocesorového zařízení pro tento klíč.

Chcete-li používat šifrovací koprocesor k uložení soukromých klíčů, musíte zajistit, aby byl koprocesor předtím, než začnete pracovat s produktem Digital Certificate Manager (DCM), logicky zapnutý. Jinak by totiž produkt DCM v rámci procesu vytváření nebo obnovy certifikátu vůbec možnost volby místa uložení klíčů neposkytl.

Související pojmy

"Uložení klíčů certifikátů do produktu IBM Cryptographic Coprocessor" na stránce 66
V této části je vysvětleno, jak lze pomocí nainstalovaného koprocesoru zajistit bezpečnější uložení soukromých klíčů certifikátů.

SSL (Secure Sockets Layer)

Produkt SSL (Secure Sockets Layer), který původně vyvinula společnost Netscape, je odvětvovým standardem pro šifrování relací mezi klienty a servery.

SSL používá pro zašifrování relace mezi serverem a klientem asymetrické šifrování, neboli šifrování veřejnými klíči. Klientské a serverové aplikace si sjednají klíč pro danou relaci během výměny digitálních certifikátů. Platnost klíče vyprší automaticky po 24 hodinách a proces SSL vytvoří pro každé připojení na server a pro každého klienta odlišný klíč. Pokud by tedy neautorizovaní uživatelé zachytili a dešifrovali klíč relace (což není pravděpodobné), nemohou jej použít na pozdější relace.

Související pojmy

"Šifrování" na stránce 8
Tato část popisuje, co je to šifrování a jak digitální certifikáty používají funkce šifrování při zajišťování zabezpečení.

"Typy digitálních certifikátů" na stránce 27
V této části najdete informace o různých typech certifikátů, které můžete použít a jak jsou použity v produktu DCM.

Definice aplikace

Tato část obsahuje informace o tom, co jsou to definice aplikací v rámci produktu DCM a jak s nimi lze pracovat při konfiguraci SSL a podepisování objektů.

Existují dva typy definice aplikace, které můžete použít ke správě v prostředí produktu DCM:

- Definice aplikací typu klient nebo server, které používají komunikační relace SSL (Secure Socket Layer).

- Definice aplikací pro podepisování objektů, které podepisují objekty k zajištění jejich integrity.

Chcete-li v produktu DCM pracovat s definicemi aplikací pro SSL a jejich certifikáty, musí být aplikace nejdříve v produktu DCM zaregistrována jako definice aplikace tak, aby měla jedinečné ID aplikace. Vývojáři aplikací provádějí registraci aplikací využívajících SSL pomocí rozhraní API (QSYRGAP, QsyRegisterAppForCertUse), takže ID aplikace se v produktu DCM vytvoří automaticky. Všechny aplikace IBM iSeries využívající SSL jsou takto registrovány produktem DCM, takže k nim můžete pomocí produktu DCM snadno přiřadit certifikát a aplikace pak mohou vytvářet relace SSL. Také pro aplikace, které naprogramujete nebo zakoupíte, můžete definovat definici aplikace a vytvořit pro ni ID aplikace v rámci samotného produktu DCM. Chcete-li definici aplikace pro SSL vytvořit pro klientskou nebo serverovou aplikaci, musíte pracovat v paměti certifikátů *SYSTEM.

Chcete-li pomocí nějakého certifikátu podepisovat objekty, musíte nejprve nadefinovat aplikaci, kterou bude certifikát používat. Na rozdíl od definice aplikace v rámci SSL nepopisuje aplikace pro podepisování objektů žádnou skutečnou aplikaci. Definice aplikace, kterou vytvoříte, může namísto toho popisovat typ nebo skupinu objektů, které hodláte podepisovat. Při vytváření definice aplikace pro podepisování objektů musíte pracovat v paměti certifikátů *OBJECTSIGNING.

Související pojmy

“Správa aplikací v produktu DCM” na stránce 61
Jsou zde uvedeny informace o tvorbě definic aplikací a o tom, jak spravovat přiřazování certifikátů k aplikaci. Dále je zde vysvětleno definování seznamů důvěryhodných CA, které aplikace používají jako základ pro schválení certifikátu při autentizaci klienta.

Související úlohy

“Vytvoření definice aplikace” na stránce 61
V tomto tématu se můžete dozvědět o dvou odlišných typech aplikací, které můžete definovat a se kterými můžete pracovat.

Ověření platnosti

Produkt DCM poskytuje úlohy, prostřednictvím kterých lze potvrdit platnost certifikátu nebo aplikace a ověřit tak různé vlastnosti, které musí mít.

Ověření platnosti certifikátu

Když potvrzujete certifikát, produkt DCM (Digital Certificate Manager) ověřuje řadu položek týkajících se certifikátu, aby zajistil autenticitu a platnost certifikátu. Potvrzováním certifikátu se zajistí, že aplikace, které používají certifikát k zabezpečené komunikaci nebo k podepisování objektů, pravděpodobně nenarazí při použití certifikátů na nějaké problémy.

Jako součást procesu potvrzení produkt DCM kontroluje, zda vybranému certifikátu nevypršela platnost. Produkt DCM také kontroluje, zda certifikát není uveden v seznamu odvolaných certifikátů (CRL) jako odvolaný, pokud pro CA, který certifikát vydal, existuje umístění CRL.

| Pokud nakonfigurujete mapování protokolu LDAP pro použití CRL, produkt DCM kontroluje CRL při ověřování
| platnosti certifikátu, aby se ujistil, že certifikát není evidovaný v CRL. Aby však proces ověření platnosti důkladně
| prověřil CRL, server adresářů (LDAP), nakonfigurovaný pro mapování LDAP, musí obsahovat odpovídající CRL. V
| opačném případě nebude certifikát správně ověřen. Musíte poskytnout DN a heslo, abyste se vyvarovali ověření
| certifikátu s odvolaným stavem. Také v případě, že při konfiguraci mapování LDAP neuvedete DN a heslo, budete
| anonymně spojeni se serverem LDAP. Anonymní připojení k serveru LDAP neposkytuje úroveň oprávnění potřebnou
| pro přístup ke “kritickým” atributům a CRL je “kritickým” atributem. V takovém případě může produkt DCM potvrdit
| odvolaný certifikát, protože není schopen získat správný stav z CRL. Pokud potřebujete anonymní přístup k serveru
| LDAP, pak musíte použít nástroj Directory Server Web Administration Tool a vybrat úlohu ″Správa schématu″ za
| účelem změny třídy zabezpečení (která je nazývána rovněž jako ″přístupová třída″) u atributů
| **certificateRevocationList** a **authorityRevocationList** z hodnoty ″kritický″ na hodnotu ″normální″.

Produkt DCM také kontroluje, zda certifikát CA pro vydávajícího CA je v aktuální paměti certifikátů a zda je certifikát CA označen jako důvěryhodný. Jestliže má certifikát soukromý klíč (např. serverový certifikát, klientský certifikát nebo certifikát pro podepisování objektů), pak produkt DCM také prověřuje dvojici veřejného a soukromého klíče, aby zajistil, že si dvojice veřejného a soukromého klíče odpovídá. Jinými slovy, produkt DCM zašifruje data pomocí veřejného klíče a pak zjistí, zda se data mohou dešifrovat pomocí soukromého klíče.

Ověření platnosti aplikace

Když potvrzujete určitou aplikaci, produkt DCM ověřuje, že pro tuto aplikaci existuje přiřazení certifikátu, a zjišťuje, zda je přiřazený certifikát platný. Produkt DCM dále zjišťuje, zda v případě, že je aplikace konfigurována pro použití seznamu důvěryhodných CA, obsahuje tento seznam alespoň jeden certifikát CA. Produkt DCM pak ověřuje, zda certifikáty CA v seznamu důvěryhodných CA pro danou aplikaci jsou platné. Pokud definice aplikace uvádí, že se má provádět zpracování seznamu odvolaných certifikátů (CRL), a je definováno umístění CRL pro daného CA, pak produkt DCM v rámci ověřovacího procesu kontroluje i CRL.

Ověření platnosti aplikace vás pomůže upozornit na některé možné problémy, které aplikace může mít při provádění funkcí vyžadujících certifikát. Tyto problémy mohou u aplikace způsobit, že se nebude moci úspěšně účastnit relace SSL (Secure Sockets Layer) nebo nebude moci úspěšně podepisovat objekty.

Související pojmy

"Potvrzování certifikátů a aplikací" na stránce 64
Pomocí produktu DCM (Digital Certificate Manager) můžete potvrzovat jednotlivé certifikáty nebo aplikace, které je používají. Seznam věcí, které produkt DCM kontroluje, se mírně liší podle toho, zda se potvrzuje certifikát nebo aplikace.

Scénáře použití produktu DCM

V této části naleznete dva scénáře, které popisují typická schémata implementace certifikátů a které vám mohou pomoci při plánování vaší vlastní implementace certifikátů jako součásti celkové zásady zabezpečení iSeries. U každého scénáře jsou uvedeny rovněž všechny potřebné konfigurační úlohy, které musíte provést, aby bylo možno scénář použít tak, jak bylo popsáno.

Produkt DCM a podpora digitálních certifikátů na serveru iSeries vám umožňují použít certifikáty za účelem zdokonalení vaší strategie zabezpečení řadou různých způsobů. To, jakou variantu použití certifikátů zvolíte, bude záviset jak na vašich obchodních cílech, tak na potřebách v oblasti zabezpečení.

Použití digitálních certifikátů vám napomůže posílit zabezpečení vašeho systému v mnoha směrech. Digitální certifikáty vám umožní použít SSL (Secure Sockets Layer) pro zabezpečený přístup na webové stránky a k dalším internetovým službám. Digitální certifikáty můžete použít pro konfiguraci připojení VPN (Virtual Private Network). Klíč k certifikátu můžete také použít k digitálnímu podepisování objektů nebo k ověření digitálních podpisů a zajištění autenticity objektů. Tyto digitální podpisy zajišťují spolehlivost původu daného objektu a chrání integritu objektu.

Zvýšit zabezpečení systému můžete také tím, že digitální certifikáty použijete při autentizaci a autorizaci relací mezi serverem a uživateli (namísto uživatelských jmen a hesel). Produkt DCM můžete podle toho, jak jej nakonfigurujete, použít dále pro přiřazení uživatelského certifikátu k jeho uživatelskému profilu na serveru iSeries nebo k identifikátoru EIM. Certifikát má pak stejná oprávnění a povolení jako přiřazený uživatelský profil.

Z uvedeného je zřejmé, že systém, jakým budete certifikáty používat, může být složitý a bude záviset na řadě faktorů. Scénáře použití certifikátů popsané v této části, vycházejí z několika nejběžnějších bezpečnostních důvodů použití digitálních certifikátů pro zabezpečenou komunikaci v rámci typického podnikového prostředí. V každém scénáři jsou rovněž popsány všechny nezbytné systémové a softwarové předpoklady a všechny konfigurační úlohy, které musíte provést při implementaci daného scénáře.

Související informace

Scénáře podepisování objektů

Scénář: Použití certifikátů pro externí autentizaci

V tomto scénáři je popsáno, kdy a jak použít certifikáty jako prostředek autentizace, chcete-li chránit a omezovat přístup veřejných uživatelů k veřejným nebo extranetovým prostředkům a aplikacím.

Situace:

Představte si, že pracujete v pojišťovací společnosti MyCo., Inc a máte na starosti údržbu různých aplikací v rámci intranetu a extranetu vaší společnosti. Jednou z aplikací, za které jste zodpovědní, je aplikace pro výpočet pojistných sazeb, kterou používají nezávislí pojišťovací agenti vaší společnosti při vytváření cenových nabídek pro klienty. Protože informace, které tato aplikace poskytuje, jsou poněkud citlivé, chcete zajistit, aby aplikaci mohli používat pouze registrovaní agenti. Chcete také uživatelům časem poskytnout bezpečnější metodu uživatelské autentizace k aplikaci, než je vaše současná metoda využívající uživatelská jména a hesla. Obáváte se, že by neautorizovaní uživatelé mohli tuto informaci zachytit při jejím přenosu přes nedůvěryhodnou síť. Také se obáváte, že někteří pojišťovací agenti by tuto informaci mohli sdělit jiným osobám, které autorizaci nemají.

Když si zjistíte, jaké jsou v této oblasti možnosti, rozhodnete se, že vašim potřebám bude nejlépe vyhovovat použití digitálních certifikátů, které ochrání citlivé informace zadané do aplikace a načtené z aplikace. Použití certifikátů vám umožní používat SSL (Secure Sockets Layer) pro ochranu dat při jejich přenosu. Plánujete, že v konečné fázi budou všichni agenti používat pro přístup k aplikaci certifikát, ale víte, že než tohoto cíle dosáhnete, bude váš podnik i externí agenti potřebovat jistý čas. Kromě použití certifikátů pro autentizaci klientů máte v úmyslu stále používat současná uživatelská jména a hesla, protože SSL poskytuje citlivým datům při přenosu dostatečnou ochranu.

Na základě typu aplikace a jejích uživatelů a na základě vašeho budoucího cíle autentizace všech uživatelů pomocí certifikátů se rozhodnete při konfiguraci SSL u vaší aplikace použít veřejný certifikát od některého dobře známého vydavatele certifikátů.

Výhody scénáře

Tento scénář má následující výhody:

- Použitím digitálních certifikátů pro konfiguraci SSL přístupu k aplikaci sloužící k výpočtu pojistných sazeb zajistíte, že informace přenášené mezi serverem a klientem budou chráněné a soukromé.
- Použitím digitálních certifikátů pro autentizaci klientů, v co největší míře to bude možné, poskytnete autorizovaným uživatelům bezpečnější metodu identifikace. Dokonce i tehdy, kdy použití digitálních certifikátů nebude možné, autentizace na základě uživatelského jména a hesla bude díky relaci SSL chráněna a zachována soukromá, takže výměna těchto citlivých dat bude bezpečnější.
- Použití *veřejných* digitálních certifikátů k autentizaci uživatelů pro přístup k vašim aplikacím a datům způsobem, který popisuje tento scénář, bude praktickou volbou za těchto nebo podobných podmínek:
  - Vaše data a aplikace vyžadují různou míru zabezpečení.
  - Vaši důvěryhodní uživatelé se často střídají.
  - Poskytujete veřejný přístup k aplikacím a datům, jako jsou např. webové stránky na Internetu nebo extranetové aplikace.
  - Nechcete provozovat vlastního vydavatele certifikátů z administračních důvodů, jako je například velký počet externích uživatelů, kteří přistupují k vašim aplikacím a prostředkům.
- Použijete-li ke konfiguraci SSL u aplikace pro výpočet pojistných sazeb veřejný certifikát, snížíte rozsah konfigurace, kterou budou muset uživatelé provádět při přístupu k dané aplikaci zabezpečeným způsobem. Klientský software většinou obsahuje certifikáty CA pro většinu známých vydavatelů certifikátu.

Úkoly

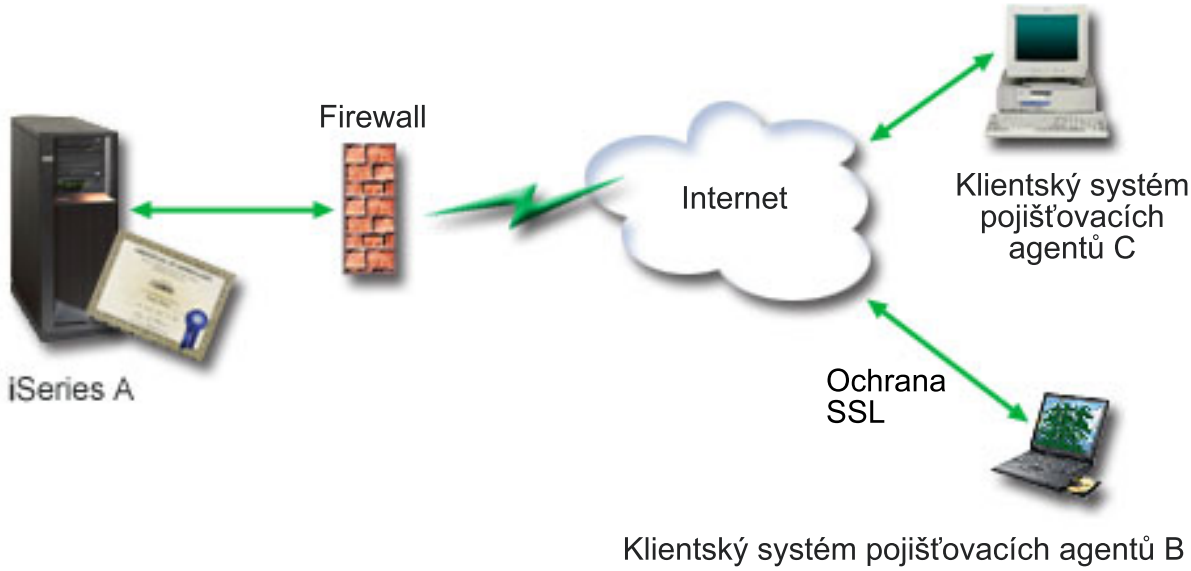
V tomto scénáři chce společnost MyCo, Inc. pomocí digitálních certifikátů zajistit ochranu informací, které jejich aplikace pro výpočet pojistných sazeb poskytuje autorizovaným veřejným uživatelům. Společnost chce také bezpečnější metodu autentizace těch uživatelů, kteří mají k aplikaci oprávněný přístup.

Cíle tohoto scénáře jsou následující:

- Veřejná aplikace pro výpočet pojistných sazeb musí používat SSL, aby byla zajištěna ochrana a soukromost dat, které aplikace uživatelům poskytuje a které od nich získává.
- Konfigurace SSL musí být provedena pomocí veřejného certifikátu od známého veřejného internetového vydavatele certifikátů.
- Autorizovaní uživatelé musí zadat platné uživatelské jméno a heslo, aby mohli přistupovat k aplikaci v režimu SSL. V konečné fázi musí být autorizovaní uživatelé schopni používat jednu ze dvou metod zabezpečené autentizace, aby jim byl poskytnut přístup k aplikaci. Externí agenti musí předložit buď veřejný digitální certifikát od známého vydavatele certifikátů, nebo platné uživatelské jméno a heslo, pokud není k dispozici certifikát.

Podrobnosti

Na obrázku je znázorněno schéma konfigurace sítě podle uvedeného scénáře:



Z obrázku vyplývají tyto informace o situaci popisované ve scénáři:

Podnikový veřejný server – iSeries A

- Server iSeries A je hostitelský systém podnikové aplikace pro výpočet pojistných sazeb.
- Server iSeries A provozuje operační systém i5/OS verzi 5, vydání 4 (V5R4).
- Server iSeries A má nainstalován a nakonfigurován produkt Digital Certificate Manager (i5/OS volba 34) a produkt IBM HTTP Server for i5/OS (5722–DG1).
- Na serveru iSeries A běží aplikace pro výpočet pojistných sazeb, která je nakonfigurovaná následovně:
  - Vyžaduje režim SSL.
  - Pro svou autentizaci za účelem inicializace relace SSL používá veřejný certifikát od známého vydavatele certifikátů.
  - Vyžaduje autentizaci uživatelů pomocí uživatelského jména a hesla.
- Když se klienti B a C přihlašují k aplikaci pro výpočet pojistných sazeb, server iSeries A předkládá svůj certifikát, aby zahájil relaci SSL.
- Když se spustí relace SSL, server iSeries A předtím, než povolí přístup k aplikaci pro výpočet pojistných sazeb, požaduje, aby klienti B a C předložili platné uživatelské jméno a heslo.

Klientské systémy pojišťovacích agentů – klient B a klient C

- Klienti B a C jsou nezávislí pojišťovací agenti, kteří mají přístup k aplikaci pro výpočet pojistných sazeb.

- Klienti B a C mají ve svém klientském softwaru nainstalovanou kopii certifikátu známého CA, který vydal certifikát aplikace.
- Klienti B a C přistupují k aplikaci pro výpočet pojistných sazeb na serveru iSeries A,který následně předkládá svůj certifikát jejich klientskému softwaru, aby autentizoval svoji identitu a inicializoval relaci SSL.
- Klientský software na klientech B a C je nakonfigurován tak, aby byl schopen akceptovat certifikát ze serveru iSeries za účelem inicializace relace SSL.
- Když se spustí relace SSL, musí klienti B a C zadat platné uživatelské jméno a heslo, a pak teprve server iSeries A povolí přístup k aplikaci.

Nezbytné podmínky a předpoklady

Nezbytné podmínky a předpoklady pro realizaci uvedeného scénáře jsou tyto:

- Aplikace pro výpočet pojistných sazeb na serveru iSeries A je generická aplikace, která může být nakonfigurovaná pro použití SSL. Většina aplikací, včetně mnohých aplikací serveru iSeries, podporuje SSL. Postup při konfiguraci SSL se však u různých aplikací velmi liší. V tomto scénáři proto neuvádíme konkrétní pokyny, jak aplikaci pro výpočet pojistných sazeb nakonfigurovat pro použití SSL. Scénář poskytuje pokyny pro konfiguraci a správu certifikátů, které jsou nezbytné k tomu, aby aplikace mohla SSL používat.
- Aplikace pro výpočet pojistných sazeb může zajišťovat vyžadování certifikátů pro autentizaci klienta. Tento scénář poskytuje instrukce k tomu, jak pomocí produktu DCM nakonfigurovat ověřování certifikátů pro aplikace, které tuto podporu poskytují. Protože postupy při konfiguraci autentizace klientů se u různých aplikací velmi liší, neposkytuje tento scénář konkrétní návod, jak konfigurovat autentizaci klientů formou certifikátů u této konkrétní aplikaci pro výpočet pojistných sazeb.
- Server iSeries A splňuje požadavky pro nainstalování a použití produktu DCM.
- Na serveru iSeries A doposud nikdo nekonfiguroval a nepoužíval produkt DCM.
- Ten, kdo bude pracovat s produktem DCM při provedení úloh popsaných v tomto scénáři, musí mít ve svém uživatelském profilu zvláštní oprávnění *SECADM a *ALLOBJ.
- Na serveru iSeries A není nainstalován produkt IBM Cryptographic Coprocessor.

Úlohy nastavení

Související úlohy

“Spuštění produktu Digital Certificate Manager” na stránce 37
V této části je vysvětleno, jak ve vašem systému zpřístupníte produkt DCM.

Vyplňte plánovací formuláře

Následující plánovací formulář zobrazuje informace, které je třeba shromáždit, a rozhodnutí, která je třeba učinit, abyste připravili implementaci digitálního certifikátu tak, jak to popisuje tento scénář. Chcete-li zajistit úspěšnou implementaci, je třeba, abyste před provedením všech konfiguračních úloh, byli schopni odpovědět na všechny položky otázek týkajících se nezbytných podmínek Ano.

Tabulka 1. Plánovací formulář nezbytných podmínek při implementaci certifikátu

Formulář nezbytných podmínek	Odpovědi
Je verze vašeho systému i5/OS V5R42 (5722-SS1)?	Ano
Je ve vašem systému nainstalována volba 34 operačního systému i5/OS?	Ano
Je ve vašem systému nainstalován produkt IBM HTTP Server for i5/OS (5722–DG1) a je spuštěna instance administračního serveru?	Ano
Je v systému nakonfigurován protokol TCP, abyste mohli pro přístup k produktu DCM používat webový prohlížeč a instanci administračního rozhraní HTTP serveru?	Ano
Máte zvláštní oprávnění *SECADM a *ALLOBJ?	Ano

Abyste mohli dokončit implementaci, potřebujete shromáždit následující informace o implementaci digitálních certifikátů a následně provést potřebné úlohy konfigurace.

Tabulka 2. Plánovací formulář konfigurace pro implementaci certifikátu

Plánovací formulář pro server iSeries A	**Odpovědi**
Budete provozovat váš vlastní lokální CA nebo budete získávat certifikáty pro vaše aplikace od veřejného CA?	Získávat certifikáty od veřejného CA
Je server iSeries A hostitelským systémem aplikací, pro které chcete aktivovat SSL?	Ano
Které informace o rozlišovacím jméně budete používat pro požadavky na podpis certifikátů (CSR), k jejichž vytváření používáte produkt DCM? • **Velikost klíče**: určuje sílu šifrovacích klíčů pro certifikát. • **Označení certifikátu**: identifikuje certifikát prostřednictvím jedinečného řetězce znaků. • **Obecné jméno**: identifikuje vlastníka certifikátu, jako například osobu, entitu nebo aplikaci; součást DN (rozlišovacího jména) subjektu certifikátu. • **Organizační jednotka**: identifikuje organizační sekci nebo oblast pro aplikaci, která bude certifikát používat. • **Jméno organizace**: identifikuje vaši společnost nebo divizní sekci pro aplikaci, která bude tento certifikát využívat. • **Lokalita nebo město**: identifikuje vaše město nebo označení lokality vaší organizace. • **Stát nebo oblast**: identifikuje stát nebo oblast, ve které budete tento certifikát používat. • **Země nebo region**: identifikuje dvěma písmeny zemi nebo region, ve kterém budete certifikát používat.	**Velikost klíče**: 1024 **Označení certifikátu**: Myco_public_cert **Obecné jméno**: myco_rate_server@myco.com **Organizační jednotka**: Rate dept **Jméno organizace**: myco **Lokalita nebo město**: Any_city **Stát nebo oblast**: Any **Země nebo region**: ZZ
Jaký je ID aplikace DCM pro aplikaci, kterou chcete konfigurovat pro použití SSL?	mcyo_agent_rate_app
Budete konfigurovat aplikaci podporující SSL, aby používala pro autentizaci klientů certifikáty? Pokud ano, které CA chcete přidat do seznamu důvěryhodných CA aplikace?	Ne

Požadavek na vytvoření serverového nebo klientského certifikátu

1. Spusťte produkt DCM.
2. V navigační liště produktu DCM vyberte volbu **Vytvoření nové paměti certifikátů**, čímž spustíte úlohu s průvodcem a zobrazí se série formulářů. Pomocí těchto formulářů budete provedeni procesem vytvoření paměti certifikátů a certifikátu, které vaše aplikace budou používat pro relace SSL.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
3. Vyberte ***SYSTEM** jako paměť certifikátů, kterou chcete vytvořit, a klepněte na **Pokračovat**.
4. Vyberte **Ano**, abyste v rámci vytvoření paměti certifikátů *SYSTEM vytvořili i certifikát, a klepněte na **Pokračovat**.
5. Vyberte **VeriSign nebo jiného internetového vydavatele certifikátů (CA)** jako toho, kdo bude podepisovat nové certifikáty, a klepněte na **Pokračovat**, čímž se vám zobrazí formulář na vložení identifikačních informací pro nový certifikát.
6. Vyplňte formulář a klepněte na **Pokračovat**. Zobrazí se potvrzující stránka. Tato potvrzující stránka zobrazuje údaje žádosti o certifikát, které musíte poskytnout veřejnému vydavateli certifikátů (CA), jenž bude certifikát

vydávat. Data tohoto tzv. požadavku na podepisovací certifikát (Certificate Signing Request, CSR) zahrnují veřejný klíč, rozlišovací jméno a další informace, které jste uvedli pro nový certifikát.

7. Pečlivě zkopírujte a vložte data CSR do formuláře žádosti o certifikát nebo do zvláštního souboru, který veřejný CA požaduje při žádostech o certifikát. Musíte použít veškerá data CSR, včetně řádek Begin a End New Certificate Request.

   Poznámka: Jakmile tuto stránku opustíte, budou data ztracena a nebude možné je obnovit.
8. Jakmile tuto stránku opustíte, budou data ztracena a nebude možné je obnovit.
9. Než budete moci pokračovat, musíte počkat, až vám CA vrátí podepsaný dokončený certifikát.

Když vám vydavatel certifikátů vrátí podepsaný dokončený certifikát, budete moci nakonfigurovat danou aplikaci pro SSL, provést import certifikátu do paměti certifikátů *SYSTEM a přiřadit jej k vaší aplikaci, aby jej používala při SSL.

Konfigurace aplikace pro použití SSL

Když obdržíte podepsaný certifikát od veřejného vydavatele certifikátů (CA), můžete pokračovat v procesu nastavení SSL komunikace u vaší veřejné aplikace. Aplikaci musíte nakonfigurovat pro použití SSL předtím, že začnete pracovat s podepsaným certifikátem. Některé aplikace, např. HTTP Server for iSeries , v rámci procesu konfigurace aplikace pro použití SSL vygenerují jedinečné ID aplikace a zaregistrují ho v produktu DCM. ID aplikace musíte znát předtím, než můžete pomocí produktu DCM přiřadit podepsaný certifikát k aplikaci a dokončit tak proces konfigurace SSL.

Způsob konfigurace aplikace pro použití SSL se může měnit v závislosti na typu aplikace. V tomto scénáři nepředpokládáme nějakou konkrétní aplikaci pro výpočet pojistných sazeb, protože společnost MyCo., Inc. by mohla zvolit při poskytování těchto informací svým pojišťovacím agentům řadu způsobů.

Při konfigurování SSL u aplikace postupujte podle pokynů uvedených v dokumentaci k dané aplikaci. Další informace o konfigurování SSL u řady běžných aplikací IBM uvádí téma Secure Sockets Layer (SSL) v rámci aplikace iSeries Information Center.

Po dokončení konfigurace SSL vaší aplikace, můžete pro aplikaci konfigurovat podepsaný veřejný certifikát, aby mohl inicioval relace SSL.

Import a přiřazení podepsaného veřejného certifikátu

Jestliže jste nakonfigurovali aplikaci pro použití SSL, můžete nyní pomocí produktu DCM provést import certifikátu a přiřadit jej k dané aplikaci.

Dále je uveden postup importu certifikátu a jeho přiřazení k aplikaci, jimiž dokončíte proces konfigurace SSL:

1. Spusťte produkt DCM.
2. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***SYSTEM**.
3. Když se zobrazí stránka **Paměť certifikátů a heslo**, zadejte heslo, které jste pro danou paměť certifikátů uvedli, když jste ji vytvářeli, a klepněte na **Pokračovat**.
4. Když se obnoví navigační lišta, vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
5. Ze seznamu úloh vyberte volbu **Import certifikátů**, čímž zahájíte proces importu podepsaného certifikátu do paměti certifikátů *SYSTEM.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
6. Dále vyberte volbu **Přiřazení certifikátu** ze seznamu úloh **Správa certifikátů**. Zobrazí se seznam certifikátů pro aktuální paměť certifikátů.
7. Vyberte ze seznamu váš certifikát a klepněte na volbu **Přiřazení k aplikacím**. Zobrazí se seznam definic aplikací pro aktuální paměť certifikátů.

8. Vyberte ze seznamu vaši aplikaci a klepněte na **Pokračovat**. Zobrazí se stránka buď se zprávou potvrzující zvolené přiřazení, nebo s chybovou zprávou v případě nějakého problému.

Pokud jste provedli výše uvedené úlohy, můžete spustit aplikaci v režimu SSL a zajistit tak ochranu soukromosti dat, které aplikace poskytuje.

Spuštění aplikace v režimu SSL

Jestliže jste provedli import a přiřazení certifikátu k dané aplikaci, bude možná nutno aplikaci ukončit a restartovat ji v režimu SSL. V některých případech je to nezbytné, protože aplikace nemusí být schopna za provozu identifikovat, že existuje přiřazení certifikátu. V dokumentaci k aplikaci zjistíte, zda je nutno aplikaci restartovat, případně další konkrétní informace o spuštění aplikace v režimu SSL.

Pokud chcete používat certifikáty pro autentizaci klientů, můžete nyní pro aplikaci definovat seznam důvěryhodných CA.

(Volitelné): Definování seznamu důvěryhodných CA pro aplikaci

Aplikace, které podporují použití certifikátů při autentizaci klientů během relace SSL (Secure Sockets Layer), musí určovat, zda přijmout určitý certifikát jako platný průkaz totožnosti. Jedním z kritérií, které aplikace používá k autentizaci certifikátu, je to, zda aplikace důvěřuje vydavateli certifikátů (CA), který certifikát vydal.

Situace, kterou popisuje tento scénář, nevyžaduje, aby aplikace pro výpočet pojistných sazeb používala při autentizaci klientů certifikáty, ale aby byla tato aplikace schopna přijímat certifikáty za účelem autentizace, pokud jsou tyto dostupné. Mnoho aplikací poskytuje podporu pro autentizaci klientů na základě certifikátů. Způsob konfigurace této podpory se však u jednotlivých aplikací velmi liší. Tuto volitelnou úlohu zde uvádíme pro lepší pochopení způsobu, jak lze pomocí produktu DCM vytvořit seznam důvěryhodných CA, který pak bude základem pro konfiguraci autentizace klientů na základě certifikátů u vašich aplikací.

Předtím, než můžete definovat seznam důvěryhodných CA pro určitou aplikaci, musí být splněno několik podmínek:

- Aplikace musí podporovat použití certifikátů při autentizaci klientů.
- V definici této aplikace v produktu DCM musí být specifikováno, že aplikace používá seznam důvěryhodných CA.

Jestliže v definici aplikace je specifikováno, že aplikace používá seznam důvěryhodných CA, musíte tento seznam definovat předtím, než bude aplikace moci úspěšně provádět autentizaci klientů na základě certifikátů. Tím zajistíte, že aplikace bude potvrzovat pouze certifikáty těch CA, které v seznamu uvedete jako důvěryhodné. Pokud uživatelé nebo klientská aplikace předloží certifikát od CA, který není uveden jako důvěryhodný v seznamu důvěryhodných CA, aplikace certifikát nepřijme za základ platné autentizace.

Chcete-li pomocí produktu DCM definovat pro aplikaci seznam důvěryhodných CA, postupujte následovně:

1. Spusťte produkt DCM.
2. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***SYSTEM**.
3. Když se zobrazí stránka **Paměť certifikátů a heslo**, zadejte heslo, které jste pro danou paměť certifikátů uvedli, když jste ji vytvářeli, a klepněte na **Pokračovat**.
4. Když se obnoví navigační lišta, vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
5. Ze seznamu úloh vyberte **Nastavit stav CA**. Zobrazí se seznam certifikátů CA.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
6. Vyberte ze seznamu jeden nebo více certifikátů CA, kterým aplikace bude důvěřovat, a klepněte na **Povolit**. Zobrazí se seznam aplikací, které používají seznam důvěryhodných CA.

7. Vyberte ze seznamu aplikaci, pro kterou chcete do seznamu důvěryhodných CA doplnit vybraného CA, a klepněte na **OK**. V horní části stránky se zobrazí zpráva, která informuje, že aplikace, kterou jste vybrali, bude důvěřovat danému CA a certifikátům, které CA vydá.

Nyní můžete nakonfigurovat aplikaci tak, aby při autentizaci klientů požadovala certifikáty. Postupujte přitom podle pokynů, které uvádí dokumentace k dané aplikaci.

Scénář: Použití certifikátů pro interní autentizaci

V tomto scénáři se můžete naučit, jak použít certifikáty jako prostředek autentizace, chcete-li chránit prostředky a aplikace na interních serverech a omezit v tomto smyslu přístupy interních uživatelů.

Situace

Jste správcem sítě ve společnosti (MyCo, Inc.), jejíž personální oddělení řeší problémy právních otázek a soukromosti osobních záznamů. Zaměstnanci podniku požadovali, aby měli online přístup k informacím o svých platech, dávkách na zdravotní pojištění apod. Společnost reagovala na tento požadavek tak, že vytvořila webové stránky, kde jsou tyto informace zaměstnancům k dispozici. Jste zodpovědný za správu těchto interních webových stránek, které jsou provozovány na serveru IBM HTTP Server for i5/OS (provozovaném na základě technologie Apache).

Protože se zaměstnanci nacházejí na dvou různých pracovištích a někteří zaměstnanci často cestují, musíte zajistit, aby se zachovala soukromost informací při jejich přenosu po Internetu. Také tradičně používáte proces autentizace uživatelů prostřednictvím uživatelského jména a hesla, abyste omezili přístup k datům společnosti. Vzhledem k citlivosti a soukromosti těchto informací si však uvědomujete, že omezení přístupu k informacím na základě hesla nemusí být dostačující. Přece jen hesla mohou lidé někomu říci, mohou je zapomenout, heslo někdo dokonce může ukrást.

Když si zjistíte, jaké jsou v této oblasti možnosti, rozhodnete se, že vašim potřebám bude nejlépe vyhovovat použití digitálních certifikátů. Certifikáty vám umožní používat SSL (Secure Sockets Layer) pro ochranu dat při jejich přenosu. Navíc můžete používat certifikáty namísto hesel, čímž docílíte vyšší bezpečnosti autentizace uživatelů a budete moci omezit personální informace, ke kterým bude mít daný uživatel přístup.

Proto se rozhodnete vytvořit soukromého lokálního CA, vydávat certifikáty všem zaměstnancům a přiřadit certifikáty zaměstnanců k jejich uživatelským profilům na serveru iSeries. Tento typ implementace soukromých certifikátů vám umožní účinněji řídit přístup k citlivým datům a také zajistit soukromost dat pomocí SSL. Tím, že budete certifikáty vydávat sami, konečně také zvyšujete pravděpodobnost, že vaše data zůstanou bezpečná a že budou přístupná pouze určitým jedincům.

Výhody scénáře

Tento scénář má následující výhody:

- Použitím digitálních certifikátů pro konfiguraci SSL přístupu na váš webový server s personálními informacemi zajistíte, že informace přenášené mezi serverem a klientem budou chráněné a soukromé.
- Použitím digitálních certifikátů při autentizaci klientů poskytnete autorizovaným uživatelům bezpečnější metodu identifikace.
- Použití *soukromých* digitálních certifikátů za účelem autentizace uživatelů pro přístup k vašim aplikacím a datům bude praktickou volbou za těchto nebo podobných podmínek:
  - Požadujete vysokou míru zabezpečení, zejména co se týče autentizace uživatelů.
  - Důvěřujete osobám, kterým budete certifikáty vydávat.
  - Vaši uživatelé již mají uživatelské profily na serveru iSeries za účelem řízení jejich přístupu k aplikacím a datům.
  - Chcete provozovat vlastního vydavatele certifikátů (CA).
- Použijete-li k autentizaci klientů soukromé certifikáty, budete moci snadněji přiřazovat certifikát k autorizovanému uživatelskému profilu na serveru iSeries. Přiřazení certifikátu k uživatelskému profilu umožňuje, aby HTTP server

během autentizace určil uživatelský profil vlastníka certifikátu. HTTP server pak může na tento profil přejít a pracovat pod tímto uživatelským profilem nebo pro daného uživatele provádět operace na základě informací v uživatelském profilu.

Úkoly

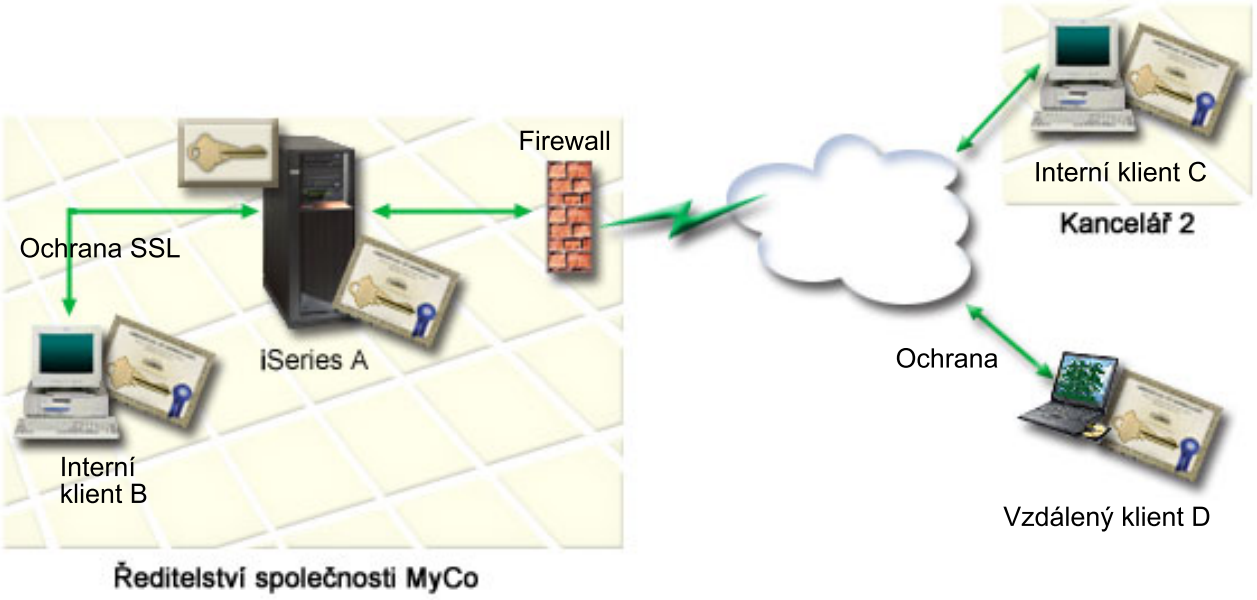
V tomto scénáři chce společnost MyCo, Inc. pomocí digitálních certifikátů zajistit ochranu personálních informací, které jejich interní webové stránky poskytují podnikovým zaměstnancům. Společnost chce také bezpečnější metodu autentizace těch uživatelů, kteří mají k těmto webovým stránkám oprávněný přístup.

Cíle tohoto scénáře jsou následující:

- Interní podnikové webové stránky s personálními informacemi musí používat SSL, aby se zajistila ochrana a soukromost dat poskytovaných uživatelům.
- Konfigurace SSL musí být provedena pomocí soukromých certifikátů od interního lokálního vydavatele certifikátů (CA).
- Autorizovaní uživatelé, kteří chtějí přistupovat na webové stránky v režimu SSL, musí zadat platný certifikát.

Podrobnosti

Na obrázku je znázorněno schéma konfigurace sítě podle uvedeného scénáře:



Z obrázku vyplývají tyto informace o situaci popisované ve scénáři:

Podnikový veřejný server – iSeries A

- iSeries Server A je hostitelský systém podnikové aplikace pro výpočet pojistných sazeb.
- iSeries Server A provozuje i5/OS verzi 5, vydání 4 (V5R4) operačního systému.
- iSeries Server A má nainstalován a nakonfigurován produkt Digital Certificate Manager (i5/OS volba 34) a produkt IBM HTTP Server for i5/OS (5722–DG1).
- iSeries Na Serveru A běží aplikace pro výpočet pojistných sazeb, která je nakonfigurovaná následovně:
  - Vyžaduje režim SSL.
  - Pro svou autentizaci za účelem inicializace relace SSL používá veřejný certifikát od známého vydavatele certifikátů.
  - Vyžaduje autentizaci uživatelů pomocí uživatelského jména a hesla.

- Když se klienti B a C přihlašují k aplikaci pro výpočet pojistných sazeb, server iSeries A předkládá svůj certifikát, aby zahájil relaci SSL.
- Když se spustí relace SSL, server iSeries A předtím, než povolí přístup k aplikaci pro výpočet pojistných sazeb, požaduje, aby klienti B a C předložili platné uživatelské jméno a heslo.

Klientské systémy pojišťovacích agentů – klient B a klient C

- Klienti B a C jsou nezávislí pojišťovací agenti, kteří mají přístup k aplikaci pro výpočet pojistných sazeb.
- Klienti B a C mají ve svém klientském softwaru nainstalovanou kopii certifikátu známého CA, který vydal certifikát aplikace.
- Klienti B a C přistupují k aplikaci pro výpočet pojistných sazeb na serveru iSeries A,který následně předkládá svůj certifikát jejich klientskému softwaru, aby autentizoval svoji identitu a inicializoval relaci SSL.
- Klientský software na klientech B a C je nakonfigurován tak, aby byl schopen akceptovat certifikát ze serveru iSeries za účelem inicializace relace SSL.
- Když se spustí relace SSL, musí klienti B a C zadat platné uživatelské jméno a heslo, a pak teprve server iSeries A povolí přístup k aplikaci.

Nezbytné podmínky a předpoklady

Nezbytné podmínky a předpoklady pro realizaci uvedeného scénáře jsou tyto:

- Server IBM HTTP Server for i5/OS (provozovaný na základě technologie Apache) provozuje aplikaci s personálními informacemi na serveru iSeries A. V tomto scénáři neuvádíme konkrétní pokyny, jak konfigurovat HTTP server pro použití SSL. Scénář poskytuje pokyny pro konfiguraci a správu certifikátů, které jsou nezbytné k tomu, aby aplikace mohla SSL používat.
- HTTP server musí mít schopnost požadovat při autentizaci klientů certifikáty. Tento scénář poskytuje pokyny k tomu, jak pomocí produktu DCM nakonfigurovat požadavky správy certifikátů tak, aby scénář fungoval. Ve scénáři však není uveden konkrétní postup při konfiguraci autentizace klientů na bázi certifikátů na HTTP serveru.
- HTTP server personálních informací na serveru iSeries A již používá autentizaci pomocí hesel.
- Server iSeries A splňuje požadavky pro nainstalování a použití produktu DCM.
- Na serveru iSeries A doposud nikdo nekonfiguroval a nepoužíval produkt DCM.
- Ten, kdo bude pracovat s produktem DCM při provedení úloh popsaných v tomto scénáři, musí mít ve svém uživatelském profilu zvláštní oprávnění *SECADM a *ALLOBJ.
- Na serveru iSeries A není nainstalován produkt IBM Cryptographic Coprocessor.

Úlohy nastavení

Vyplňte plánovací formuláře

Následující plánovací formulář zobrazuje informace, které je třeba shromáždit, a rozhodnutí, která je třeba učinit, abyste připravili implementaci digitálního certifikátu tak, jak to popisuje tento scénář. Chcete-li zajistit úspěšnou implementaci, je třeba, abyste před provedením všech konfiguračních úloh, byli schopni odpovědět na všechny položky otázek týkajících se nezbytných podmínek Ano.

Tabulka 3. Plánovací formulář nezbytných podmínek při implementaci certifikátu

Formulář nezbytných podmínek	Odpovědi
Je verze vašeho systému i5/OS V5R4 (5722-SS1)?	Ano
Je ve vašem systému nainstalována volba 34 operačního systému i5/OS?	Ano
Je ve vašem systému nainstalován produkt IBM HTTP Server for i5/OS (5722–DG1) a je spuštěna instance administračního serveru?	Ano

Tabulka 3. Plánovací formulář nezbytných podmínek při implementaci certifikátu (pokračování)

Formulář nezbytných podmínek	**Odpovědi**
Je v systému nakonfigurován protokol TCP, abyste mohli pro přístup k produktu DCM používat webový prohlížeč a instanci administračního rozhraní HTTP serveru?	Ano
Máte zvláštní oprávnění *SECADM a *ALLOBJ?	Ano

Abyste mohli dokončit implementaci, potřebujete shromáždit následující informace o implementaci digitálních certifikátů a následně provést potřebné úlohy konfigurace.

Tabulka 4. Plánovací formulář konfigurace pro implementaci certifikátu

Plánovací formulář pro server iSeries A	**Odpovědi**
Budete provozovat váš vlastní lokální CA nebo budete získávat certifikáty pro vaše aplikace od veřejného CA?	Vytvořit lokální CA, který bude vydávat certifikáty
Je server iSeries A hostitelským systémem aplikací, pro které chcete aktivovat SSL?	Ano
Jakou informaci o rozlišovacím jménu budete používat pro lokálního CA? • **Velikost klíče**: určuje sílu šifrovacích klíčů pro certifikát. • **Jméno vydavatele certifikátů (CA)**: identifikuje CA a stává se běžným jménem pro certifikát CA a rozlišovacím jménem (DN) vydavatele pro certifikáty vydané tímto CA. • **Organizační jednotka**: identifikuje organizační sekci nebo oblast pro aplikaci, která bude certifikát používat. • **Jméno organizace**: identifikuje vaši společnost nebo divizní sekci pro aplikaci, která bude tento certifikát využívat. • **Lokalita nebo město**: identifikuje vaše město nebo označení lokality vaší organizace. • **Stát nebo oblast**: identifikuje stát nebo oblast, ve které budete tento certifikát používat. • **Země nebo region**: identifikuje dvěma písmeny zemi nebo region, ve kterém budete certifikát používat. • **Období platnosti vydavatele certifikátů**: specifikuje počet dní, po který je certifikát od vydavatele certifikátů platný.	**Velikost klíče**: 1024 **Jméno vydavatele certifikátů (CA)**: Myco_CA@myco.com **Organizační jednotka**: Rate dept **Jméno organizace**: myco **Lokalita nebo město**: Any_city **Stát nebo oblast**: Any **Země nebo region**: ZZ **Období platnosti vydavatele certifikátů**: 1095
Chcete nastavit strategická data pro lokálního CA tak, aby mohl vydávat uživatelské certifikáty pro autentizaci klientů?	Ano

Tabulka 4. Plánovací formulář konfigurace pro implementaci certifikátu (pokračování)

Plánovací formulář pro server iSeries A	Odpovědi
Jakou informaci o rozlišovacím jménu budete používat pro serverový certifikát vydaný lokálním CA? • **Velikost klíče**: určuje sílu šifrovacích klíčů pro certifikát. • **Označení certifikátu**: identifikuje certifikát prostřednictvím jedinečného řetězce znaků. • **Obecné jméno**: identifikuje vlastníka certifikátu, jako například osobu, entitu nebo aplikaci; součást DN (rozlišovacího jména) subjektu certifikátu. • **Organizační jednotka**: identifikuje organizační sekci nebo oblast pro aplikaci, která bude certifikát používat. • **Jméno organizace**: identifikuje vaši společnost nebo divizní sekci pro aplikaci, která bude tento certifikát využívat. • **Lokalita nebo město**: identifikuje vaše město nebo označení lokality vaší organizace. • **Stát nebo oblast**: identifikuje stát nebo oblast, ve které budete tento certifikát používat. • **Země nebo region**: identifikuje dvěma písmeny zemi nebo region, ve kterém budete certifikát používat.	**Velikost klíče**: 1024 **Označení certifikátu**: Myco_public_cert **Obecné jméno**: myco_rate_server@myco.com **Organizační jednotka**: Rate dept **Jméno organizace**: myco **Lokalita nebo město**: Any_city **Stát nebo oblast**: Any **Země nebo region**: ZZ
Jaký je ID aplikace DCM pro aplikaci, kterou chcete konfigurovat pro použití SSL?	mcyo_agent_rate_app
Budete konfigurovat aplikaci podporující SSL, aby používala pro autentizaci klientů certifikáty? Pokud ano, které CA chcete přidat do seznamu důvěryhodných CA aplikace?	AnoMyco_CA@myco.com

Konfigurace HTTP serveru osobního oddělení pro použití SSL

Konfigurace SSL (Secure Sockets Layer) u HTTP serveru (provozovaném na základě technologie Apache) osobního oddělení na serveru iSeries A vyžaduje množství úloh, které se liší dle toho, jak je váš server v současné době nakonfigurován.

Chcete-li konfigurovat server tak, aby používal SSL, postupujte takto:

1. Spusťte rozhraní HTTP Server Administration.
2. Chcete-li pracovat se specifickým HTTP serverem, vyberte postupně karty **Manage —> All Servers —> All HTTP Servers** a zobrazí se seznam všech konfigurovaných HTTP serverů.
3. Vyberte příslušný server ze seznamu a klepněte na volbu **Manage Details**.
4. V navigační liště vyberte volbu **Security**.
5. Ve formuláři vyberte kartu **SSL with Certificate Authentication**.
6. V poli **SSL** vyberte volbu Enabled.
7. Do pole **Server certificate application name** zadejte ID aplikace, pod kterým je známa instance tohoto serveru. Nebo je můžete zvolit ze seznamu. Tento ID aplikace je uveden ve formuláři QIBM_HTTP_SERVER_[jméno_serveru] , například QIBM_HTTP_SERVER_MYCOTEST. **Poznámka:** Zapamatujte si toto ID aplikace. Budete je zadávat ještě jednou v rámci produktu DCM.

Podrobné informace o obecné konfiguraci HTTP serveru pro použití SSL najdete v tématu HTTP Server for iSeries, zejména v příkladu nazvaném Scénář: JKL umožňuje ochranu pomocí (Secure Sockets Layer) na svém HTTP serveru (provozovaném na základě technologie Apache). V tomto scénáři je uveden kompletní postup vytvoření virtuálního hostitelského systému a jeho konfigurace pro použití SSL, včetně těchto úloh:

1. Nastavení virtuálního hostitele založeného na jméně.
2. Nastavení direktivy Listen pro virtuálního hostitele.

3. Nastavení adresářů virtuálního hostitele.
4. Nastavení ochrany heslem prostřednictvím základní autentizace.
5. Aktivování SSL pro virtuálního hostitele.

Další informace o konfigurování jak současných, tak budoucích verzí produktu HTTP Server for iSeries, naleznete v tématu HTTP Server for iSeries.

Poté, co dokončíte konfiguraci HTTP serveru, aby používal SSL, můžete použít produkt DCM ke konfiguraci podpory certifikátů, kterou potřebujete pro SSL a autentizaci klienta.

Vytvoření a provozování lokálního CA

Když jste nakonfigurovali HTTP server personálních informací tak, aby používal SSL, musíte nyní nakonfigurovat certifikát, který bude server používat při inicializaci SSL. Na základě cílů tohoto scénáře jste se rozhodli vytvořit a provozovat lokálního vydavatele certifikátů (CA), pomocí něhož vydáte certifikát pro server.

Když pomocí produktu DCM vytváříte lokálního CA, proveďte v rámci tohoto procesu také veškeré nezbytné konfigurace, aby mohla aplikace používat SSL. To zahrnuje např. přiřazení certifikátu, který vydá lokální CA, k aplikaci webového serveru. Také přidáváte lokálního CA do seznamu důvěryhodných CA aplikace webového serveru. Pokud je lokální CA uveden v seznamu důvěryhodných vydavatelů certifikátu aplikace, aplikace je schopna rozpoznat a autentizovat uživatele, kteří předkládají certifikáty vydané tímto CA.

Chcete-li pomocí produktu DCM vytvořit a provozovat lokálního CA a vydat certifikát pro serverovou aplikaci personálních informací, postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště produktu DCM vyberte volbu **Vytvoření vydavatele certifikátů (CA)** a zobrazí se vám série formulářů. Tyto formuláře vás provedou procesem vytvoření lokálního CA a dalšími úlohami potřebnými k zahájení používání digitálních certifikátů pro SSL, podepisování objektů a ověřování podpisů.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
3. Vyplňte všechny formuláře pro tuto vedenou úlohu. V rámci vyplňování těchto formulářů provádíte všechny úlohy nutné pro nastavení funkčního vydavatele certifikátů (CA) následujícím způsobem:
   a. Zadáte identifikační informace pro lokálního CA.
   b. Instalujete certifikát lokálního CA na váš PC nebo do vašeho prohlížeče, aby váš software mohl rozpoznat lokálního CA a potvrdit certifikáty, které lokální CA vydá.
   c. Zvolíte strategická data pro lokálního CA.

      Poznámka: Nezapomeňte vybrat volbu povolující lokálnímu CA vydávat uživatelské certifikáty.
   d. Pomocí nového lokálního CA vydáte serverový nebo klientský certifikát, který vaše aplikace budou moci používat pro připojení přes SSL.
   e. Vyberete aplikace, které mohou používat serverový nebo klientský certifikát pro připojení přes SSL.

      Poznámka: Ujistěte se, že jste vybrali ID aplikace pro HTTP server personálních informací.
   f. Pomocí nového lokálního CA vydáte certifikát pro podepisování objektů, který aplikace budou moci používat k digitálnímu podepisování objektů. Tato dílčí úloha vytvoří paměť certifikátů *OBJECTSIGNING. Tuto paměť certifikátů budete používat při správě certifikátů pro podepisování objektů.

      Poznámka: I když se v tomto scénáři certifikáty pro podepisování objektů nepoužívají, určitě tuto úlohu proveďte. Kdybyste v tomto místě úlohu zrušili, úloha se ukončí a museli byste provést další samostatné úlohy, abyste konfiguraci SSL a certifikátů dokončili.
   g. Vyberete aplikace, které budou důvěřovat vašemu lokálnímu CA.

Poznámka: Ujistěte se, že jste jako jednu z aplikací, které budou důvěřovat vašemu lokálnímu CA, vybrali ID aplikace pro HTTP server personálních informací, například QIBM_HTTP_SERVER_MYCOTEST.

Když jste provedli konfiguraci certifikátu, který vaše aplikace webového serveru potřebuje pro SSL, můžete nakonfigurovat webový server tak, aby požadoval při autentizaci uživatelů certifikáty.

Konfigurace autentizace klientů pro webový server osobního oddělení

Pokud zadáte, že HTTP server vyžaduje pro autentizaci certifikáty, musíte konfigurovat obecná nastavení autentizace pro HTTP server. Tato nastavení konfigurujete ve stejném formuláři zabezpečení, který jste použili během konfigurace serveru pro použití SSL (Secure Sockets Layer).

Chcete-li konfigurovat server, aby při autentizaci klientů vyžadoval certifikáty, postupujte takto:

1. Spusťte rozhraní HTTP Server Administration.
2. Pomocí prohlížeče přejděte na stránku úloh ve vašem systému i5/OS na adrese http://your_system_name:2001.
3. Vyberte volbu **IBM Web Administration for i5/OS**.
4. Chcete-li pracovat se specifickým HTTP serverem, vyberte postupně karty **Manage → All Servers → All HTTP Servers** a zobrazí se seznam všech konfigurovaných HTTP serverů.
5. Vyberte příslušný server ze seznamu a klepněte na volbu **Manage Details**.
6. V navigační liště vyberte volbu **Security**.
7. Ve formuláři vyberte kartu **Authentication**.
8. Vyberte volbu **Use i5/OS profile of client**.
9. V poli **Authentication name or realm** zadejte jméno sféry autentizace.
10. Vyberte volbu Enabled pro pole **Process requests using client's authority** a klepněte na **Apply**.
11. Ve formuláři vyberte kartu **Control Access**.
12. Vyberte volbu **All authenticated users (valid user name and password)** a klepněte na **Apply**.
13. Ve formuláři vyberte kartu **SSL with Certificate Authentication**.
14. Zajistěte, že je vybrána volba Enabled v poli **SSL**.
15. Ujistěte se, že v poli **Server certificate application name** je zadána správná hodnota, například QIBM_HTTP_SERVER_MYCOTEST .
16. Vyberte volbu **Accept client certificate if available before making connection**. Klepněte na **OK**.

Podrobné informace o obecné konfiguraci HTTP serveru pro použití SSL najdete v tématu HTTP Server for iSeries Information, zejména v příkladu nazvaném Scenario: JKL enables Secure Sockets Layer (SSL) protection on their HTTP Server (powered by Apache). V tomto scénáři je uveden kompletní postup vytvoření virtuálního hostitelského systému a jeho konfigurace pro použití SSL.

Po dokončení konfigurace autentizace klienta, můžete HTTP server restartovat v režimu SSL a začít s ochranou soukromých dat aplikace pro zpracování personálních informací.

Spuštění webového serveru osobního oddělení v režimu SSL

Chcete-li mít jistotu, že HTTP server bude schopen identifikovat přiřazení certifikátu a používat jej při inicializaci relace SSL, bude vhodné HTTP server zastavit a restartovat.

Chcete-li zastavit a spustit HTTP server (provozovaný na bázi Apache) postupujte takto:

1. V produktu iSeries Navigator rozbalte váš systém.
2. Rozbalte **Síť → Servery → TCP/IP → Správa HTTP** .
3. Klepněte na **Start** a spustí se rozhraní HTTP Server Administration.
4. Klepněte na kartu **Manage** a zobrazí se seznam všech konfigurovaných serverů HTTP.

5. Vyberte příslušný server ze seznamu a pokud je tento server spuštěný, klepněte na volbu **Stop**.
6. Klepněte na **Start**, čímž server restartujete. V online nápovědě získáte další informace o parametrech spuštění.

Předtím, než budou uživatelé schopni přistupovat k webové aplikaci personálních informací, musí nejprve nainstalovat kopii certifikátu lokálního CA do svého prohlížeče.

Související informace

Přehled tématu HTTP Server v rámci aplikace Information Center

Mají uživatelé nainstalovánu kopii certifikátu lokálního CA v prohlížeči

Když uživatelé přistupují na server, který používá připojení přes SSL (Secure Sockets Layer), předloží server klientskému softwaru uživatele certifikát jako důkaz své totožnosti. Klientský software musí serverový certifikát ověřit, a pak teprve server zahájí relaci. Při potvrzení serverového certifikátu musí mít klientský software přístup k lokálně uložené kopii certifikátu toho vydavatele certifikátů (CA), který serverový certifikát vydal. Pokud server předloží certifikát od veřejného internetového CA, musí mít prohlížeč nebo jiný klientský software uživatele již kopii certifikátu CA. Pokud ale, jak je tomu v tomto scénáři, server předloží certifikát od soukromého lokálního CA, musí si každý uživatel pomocí produktu DCM nainstalovat kopii certifikátu lokálního CA.

Uživatelé (klienti B, C a D) musí při získání kopie certifikátu lokálního CA postupovat takto:

1. Spusťte produkt DCM.
2. V navigační liště vyberte volbu **Instalace certifikátu lokálního CA na počítač** a zobrazí se stránka, pomocí níž můžete stáhnout certifikát lokálního CA do prohlížeče nebo jej uložit do souboru ve vašem systému.
3. Vyberte způsob instalace certifikátu. Pomocí této volby stáhnete certifikát lokálního CA jako důvěryhodný zdroj do svého prohlížeče. Tím zajistíte, že prohlížeč bude umět vytvářet zabezpečené komunikační relace s webovými servery, které používají certifikát od tohoto CA. Prohlížeč zobrazí sérii oken, která vám napomohou dokončit instalaci.
4. Klepněte na **OK** a vrátíte se na domovskou stránku produktu DCM.

Nyní, když uživatelé mají přístup k webovému serveru personálních informací v režimu SSL, musí být tito uživatelé schopni předložit příslušný certifikát pro autentizaci k serveru. Musí tedy obdržet uživatelský certifikát od lokálního CA.

Vyžádal si každý uživatel certifikát od lokálního CA

V předchozích úlohách jste nakonfigurovali webový server personálních informací tak, aby požadoval při autentizaci uživatelů certifikáty. Nyní tedy uživatelé předtím, než jim je povolen přístup na webový server, musí předložit platný certifikát od lokálního CA. Každý uživatel, který chce získat certifikát, musí použít DCM a v jeho rámci úlohu **Vytvoření certifikátu**. Aby mohl uživatel získat certifikát od lokálního CA, musí strategie CA povolovat danému CA vydávání uživatelských certifikátů.

Uživatelé (klienti B, C a D) musí při získání certifikátu postupovat takto:

1. Spusťte produkt DCM.
2. V navigační liště vyberte volbu **Vytvoření certifikátu**.
3. Vyberte **Uživatelský certifikát** jako typ certifikátu, který budete vytvářet. Zobrazí se formulář, do kterého zadáte identifikační informace pro certifikát.
4. Vyplňte formulář a klepněte na **Pokračovat**.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
5. V tomto bodě produkt DCM ve spolupráci s vaším prohlížečem vytvoří soukromý a veřejný klíč certifikátu. Prohlížeč pravděpodobně zobrazí okna, aby vás tímto procesem provedl. Postupujte podle instrukcí, které vám pro tyto úlohy poskytne prohlížeč. Když prohlížeč vygeneruje klíče, zobrazí se potvrzující stránka, která oznamuje, že produkt DCM vytvořil certifikát.

6. Nainstalujte nový certifikát do prohlížeče. Prohlížeč pravděpodobně zobrazí okna, aby vás tímto procesem provedl. Při provádění této úlohy postupujte podle instrukcí, které vám poskytne prohlížeč.
7. Klepnutím na **OK** úlohu dokončíte.

Během zpracování produkt DCM automaticky přiřadí certifikát k vašemu uživatelskému profilu na serveru iSeries.

Po dokončení těchto úloh budou moci přistupovat k datům webového serveru s personálními informacemi pouze autorizovaní uživatelé s platným certifikátem a tato data budou během přenosu chráněna prostřednictvím protokolu SSL.

Plánování použití produktu DCM

Tato část obsahuje informace, které vám pomohou při rozhodování, jak a kdy můžete digitální certifikáty použít, abyste splnili své cíle v oblasti zabezpečení dat. Dovíte se zde, jaké jsou nezbytné předpoklady pro instalaci a také další požadavky, které musíte uvážit předtím, než začnete produkt DCM používat.

Chcete-li pomocí produktu DCM (Digital Certificate Manager) efektivně spravovat digitální certifikáty ve vaší společnosti, musíte si vytvořit obecný plán, jak budete digitální certifikáty v rámci vaší strategie zabezpečení používat.

Další informace o plánování použití produktu DCM a o tom, jak mohou digitální certifikáty doplnit vaši strategii zabezpečení, naleznete v těchto tématech:

Požadavky pro nastavení produktu DCM

V této části můžete zjistit, zda máte nainstalovány všechny volby, které jsou potřeba ke spuštění produktu DCM.

Produkt DCM (Digital Certificate Manager) je bezplatnou funkcí serveru iSeries, s jejíž pomocí můžete centrálně spravovat digitální certifikáty pro vaše aplikace. Chcete-li produkt DCM úspěšně používat, musíte zajistit splnění těchto požadavků:

- V operačním systému i5/OS. Tato volba obsahuje produkt DCM založený na prohlížeči.
- Nainstalujte produkt IBM HTTP Server for i5/OS (5722–DG1) a spusťte instanci administračního rozhraní serveru.
- Ujistěte se, že je v systému nakonfigurován protokol TCP, abyste mohli pro přístup k funkci DCM používat webový prohlížeč a instanci administračního rozhraní HTTP serveru.

Poznámka: Dokud nebudete mít nainstalovány všechny požadované produkty, nebudete moci vytvářet certifikáty. Jestliže požadovaný produkt není nainstalován, produkt DCM zobrazí chybovou zprávu, ve které vám dá pokyn k instalaci chybějící součásti.

Pokyny pro zálohování a obnovu dat produktu DCM

Toto téma obsahuje informace o tom, jak lze zajistit, aby byla důležitá data produktu DCM přidána do plánu zálohování a obnovy vašeho systému.

Zašifrovaná hesla databáze klíčů, která používáte pro přístup k paměti certifikátů v produktu DCM, jsou uložena nebo *založena* ve speciálním souboru zabezpečení ve vašem systému. Když použijete produkt DCM pro vytvoření paměti certifikátů ve vašem systému, produkt DCM za vás automaticky založí heslo. Avšak za jistých okolností je třeba, abyste se ručně přesvědčili, že produkt DCM hesla paměti certifikátů založí.

Příkladem takové okolnosti je, když použijete produkt DCM k vytvoření certifikátu pro jiný server **iSeries** a rozhodnete se, že pro vytvoření nové paměti certifikátů mají být použity soubory certifikátů v tomto cílovém systému. V takové situaci je třeba, abyste otevřeli nově vytvořenou paměť certifikátů a prostřednictvím úlohy **Změna hesla** změnili heslo pro paměť certifikátů v cílovém systému, čímž zajistíte, že produkt DCM toto nové heslo založí. Pokud je paměť certifikátů jinou (sekundární) systémovou pamětí certifikátů, měli byste také zadat, že chcete použít volbu **automatického přihlášení**, když změníte heslo. Další informace o použití produktu DCM k vytváření certifikátů pro ostatní systémy iSeries najdete v části Použití lokálního CA k vydávání certifikátů pro jiné servery iSeries.

Volbu **automatického přihlášení** musíte zadat také vždy, když změníte nebo resetujete heslo pro jinou systémovou paměť certifikátů.

Chcete-li zajistit úplné zálohování vašich kritických dat produktu DCM, postupujte takto:

- Použijte příkaz SAV pro uložení všech souborů .KDB a .RDB. Každý certifikát produktu DCM se sestává ze dvou souborů, jednoho s příponou .KDB a druhého s příponou .RDB.
- Použijte příkaz SAVSYS (Uložení systému) a příkaz SAVSECDTA (Uložení informací o zabezpečení) k uložení speciálního souboru zabezpečení, který obsahuje hesla databáze klíčů pro přístup k paměti certifikátů. Chcete-li obnovit soubor zabezpečení s hesly produktu DCM, použijte příkaz pro obnovu uživatelských profilů RSTUSRPRF (Obnova uživatelských profilů) a pro volbu uživatelského profilu zadejte *ALL.

Další strategie obnovy bere v úvahu použití operace SAVSECDTA a potenciální možnost zrušení synchronizace mezi aktuálními hesly paměti certifikátů a hesly v uloženém souboru zabezpečení s hesly DCM. Pokud změníte heslo pro paměť certifikátů poté, co provedete operaci SAVSECDTA, avšak předtím, než obnovíte data z této operace, nebude aktuální heslo paměti certifikátů synchronizované s heslem v obnoveném souboru.

Pokud se této situaci chcete vyhnout, musíte použít úlohu **Změna hesla** (v navigačním rámci pod volbou **Správa paměti certifikátů**) v prostředí produktu DCM a poté, co obnovíte data z operace SAVSECDTA, změnit hesla paměti certifikátů, čímž zajistíte, že budou příslušná hesla opět synchronizována. V této situaci však nepoužívejte tlačítko **Resetovat heslo**, které se zobrazí, když vyberete paměť certifikátů, jež se má otevřít. Když se pokoušíte resetovat heslo, produkt DCM se pokusí načíst založené heslo. Pokud není založené heslo synchronizované se současným heslem, operace resetování se nezdaří. Pokud neměníte hesla paměti certifikátů často, můžete zvážit možnost použití příkazu SAVSECDTA pokaždé, když tato hesla měníte. Tak zajistíte, že budete mít vždy uloženou nejaktuálnější verzi založených hesel pro případ, že budete někdy potřebovat tato data obnovit.

Související úlohy

“Použití lokálního CA k vydávání certifikátů pro jiné servery iSeries” na stránce 53
V této části najdete informace o tom, jak pomocí soukromého lokálního CA vydávat certifikáty, které se budou používat na jiných serverech iSeries.

Typy digitálních certifikátů

V této části najdete informace o různých typech certifikátů, které můžete použít a jak jsou použity v produktu DCM.

Pomocí produktu DCM můžete spravovat tyto typy certifikátů:

Certifikáty vydavatele certifikátů (CA)
Certifikát vydavatele certifikátů je digitální doklad totožnosti vydavatele certifikátů (CA), který vlastní certifikát. Certifikát CA obsahuje identifikační informace o daném CA a také jeho veřejný klíč. Ostatní mohou ověřit autenticitu certifikátů, které CA vydává a podepisuje, pomocí veřejného klíče vydavatele certifikátů. Certifikát vydavatele certifikátů může být podepsán jiným CA, jako je např. VeriSign, nebo může být podepsán sám sebou, jedná-li se o nezávislou entitu. Lokální CA vytvořený a provozovaný pomocí produktu DCM je nezávislý subjekt. Ostatní mohou ověřit autenticitu certifikátů, které CA vydává a podepisuje, pomocí veřejného klíče vydavatele certifikátů. Chcete-li určitý certifikát použít pro SSL, podepisování objektů nebo ověřování podpisů na objektech, musíte mít také kopii certifikátu CA, který certifikát vydal.

Serverové nebo klientské certifikáty
Serverový nebo klientský certifikát je digitální doklad, který identifikuje serverovou nebo klientskou aplikaci, která certifikát používá pro zabezpečenou komunikaci. Serverové nebo klientské certifikáty obsahují identifikační informace o organizaci, která aplikaci vlastní, jako je např. rozlišovací jméno systému. Certifikát také obsahuje veřejný klíč systému. Server musí mít digitální certifikát, má-li používat SSL (Secure Sockets Layer) pro zabezpečenou komunikaci. Aplikace, které podporují digitální certifikáty, mohou přezkoumat serverový certifikát a ověřit tak identitu serveru, když klient přistupuje na server. Aplikace pak může autentizaci certifikátu použít jako základ pro inicializaci relace mezi klientem a serverem šifrované pomocí SSL. Správu těchto certifikátů lze provádět pouze z paměti certifikátů *SYSTEM.

Certifikáty pro podepisování objektů
Certifikát pro podepisování objektů je certifikát, pomocí kterého digitálně ″podepisujete″ objekty. Podepsáním

objektu poskytnete prostředek, pomocí kterého lze ověřit jak integritu objektu, tak původ nebo vlastníka objektu. Pomocí certifikátu lze podepisovat řadu objektů, včetně většiny objektů v integrovaném systému souborů (IFS) a objektů *CMD. Úplný seznam objektů, které lze podepisovat, je uveden v tématu Podepisování objektů a ověřování podpisů. Použijete-li soukromý klíč certifikátu pro podepisování objektů k podpisu určitého objektu, musí mít příjemce objektu přístup ke kopii odpovídajícího certifikátu pro ověřování podpisů, aby mohl podpis objektu správně autentizovat. Správu těchto certifikátů lze provádět pouze z paměti certifikátů *OBJECTSIGNING.

Certifikáty pro ověřování podpisů
Certifikát pro ověřování podpisů je kopie certifikátu pro podepisování objektů bez soukromého klíče tohoto certifikátu. Veřejný klíč certifikátu pro ověřování podpisů se používá k autentizaci digitálního podpisu, který vytvořil certifikát pro podepisování objektů. Při ověřování podpisu zjistíte původ objektu a také to, zda objekt nebyl od okamžiku podpisu změněn. Správu těchto certifikátů lze provádět pouze z paměti certifikátů *SIGNATUREVERIFICATION.

Uživatelské certifikáty
Uživatelský certifikát je digitální doklad totožnosti klienta nebo uživatele, jenž certifikát vlastní. Mnoho aplikací nyní poskytuje podporu, která umožňuje při autentizaci uživatelů používat certifikáty namísto uživatelských jmen a hesel. Produkt DCM automaticky přiřazuje uživatelské certifikáty, které vydá váš soukromý CA, k uživatelským profilům na serveru iSeries. Pomocí produktu DCM můžete rovněž k uživatelskému profilu na serveru iSeries přiřadit certifikát vydaný jiným vydavatelem certifikátů.

Pokud ke správě certifikátů používáte produkt DCM, pak produkt DCM organizuje a ukládá certifikáty a jejich přiřazené soukromé klíče do paměti certifikátů podle těchto kategorií.

Poznámka: Jestliže máte ve vašem systému nainstalován produkt IBM Cryptographic Coprocessor, můžete si vybrat jiné volby pro uložení soukromého klíče vašich certifikátů (s výjimkou certifikátů pro podepisování objektů). Můžete si zvolit uložení soukromých klíčů do šifrovacího koprocesoru samotného. Nebo můžete pomocí šifrovacího koprocesoru soukromé klíče zašifrovat a uložit je ve zvláštním souboru klíčů namísto v paměti certifikátů. Uživatelské certifikáty a jejich soukromé klíče jsou však uloženy v systému uživatele, buď v softwaru prohlížeče, nebo v souboru, který používá jiný klientský programový balík.

Související pojmy

“SSL (Secure Sockets Layer)” na stránce 9
Produkt SSL (Secure Sockets Layer), který původně vyvinula společnost Netscape, je odvětvovým standardem pro šifrování relací mezi klienty a servery.

“Paměti certifikátů” na stránce 7
Paměť certifikátů je speciální soubor databáze klíčů, který produkt DCM (Digital Certificate Manager) používá pro uložení digitálních certifikátů.

Používání veřejných certifikátů versus vydávání soukromých certifikátů

V této části je vysvětleno, jak určit, který typ certifikátu (veřejný nebo soukromý) bude optimální vzhledem k vašim obchodním potřebám.

Můžete použít certifikáty od veřejného vydavatele certifikátů nebo můžete vytvořit a provozovat soukromého vydavatele certifikátů a vydávat vlastní certifikáty. To, který způsob získávání certifikátů zvolíte, závisí na tom, jak certifikáty plánujete používat. Jakmile se rozhodnete jaký typ CA budete využívat k vydání certifikátů, musíte si zvolit typ implementace certifikátů, který bude nejlépe vyhovovat vašim potřebám v oblasti zabezpečení. K dispozici máte následující možnosti:

- Kupovat si certifikáty od veřejného internetového vydavatele certifikátů (CA).
- Provozovat vlastního lokálního CA a vydávat soukromé certifikáty pro své uživatele a aplikace.
- Používat kombinaci certifikátů od veřejných internetových CA a vašeho vlastního lokálního CA.

To, který typ implementace zvolíte, závisí na řadě faktorů. Jedním z nejdůležitějších je prostředí, ve kterém se budou certifikáty používat. Následuje několik informací, které vám napomohou lépe určit, která varianta implementace je z hlediska potřeb vašeho podnikání a zabezpečení vhodná.

Použití veřejných certifikátů

Veřejní internetoví CA vydávají certifikáty komukoliv, kdo zaplatí požadovaný poplatek. Předtím, než certifikát vydají, však vyžadují určité prokázání totožnosti. Úroveň tohoto prokázání se liší v závislosti na identifikační metodě daného CA. Předtím, než se rozhodnete používat certifikáty od určitého CA nebo důvěřovat certifikátům, které vydává, byste měli zvážit, zda náročnost identifikační metody tohoto CA vyhovuje vašim potřebám zabezpečení. S vývojem standardů PKIX (Public Key Infrastructure for X.509) nyní někteří veřejní CA poskytují mnohem přísnější identifikační standardy pro vydávání certifikátů. Přestože proces získání certifikátů od CA používajících standardy PKIX je složitější, certifikáty, které CA vydává, poskytují lepší zabezpečení přístupu k aplikacím na úrovni konkrétních uživatelů. Produkt DCM (Digital Certificate Manager) vám umožňuje používat a spravovat certifikáty od PKIX CA, kteří používají tyto nové certifikační standardy.

Musíte také zvážit náklady spojené s používáním veřejných CA k vydávání certifikátů. Pokud potřebujete certifikáty pouze pro omezený počet serverových nebo klientských aplikací a uživatelů, náklady pro vás zřejmě nebudou představovat významný faktor. Náklady však mohou značně nabýt na důležitosti, pokud máte velký počet *soukromých* uživatelů, kteří potřebují veřejné certifikáty k autentizaci klientů. V tom případě je rovněž třeba, abyste brali v úvahu administrační a programovací úsilí nutné pro nakonfigurování serverových aplikací tak, aby akceptovaly pouze specifickou sadu certifikátů, které vydává určitý veřejný CA.

Použití certifikátů od veřejného CA vám může ušetřit čas a prostředky, neboť mnoho serverových, klientských a uživatelských aplikací je nakonfigurováno tak, aby rozpoznaly většinu známých veřejných CA. Také další podniky a uživatelé budou pravděpodobně uznávat certifikáty a důvěřovat certifikátům, které vydává známý veřejný CA, více než těm, které vydá váš soukromý lokální CA.

Použití soukromých certifikátů

Jestliže si vytvoříte vlastního lokálního CA, budete moci vydávat certifikáty pro systémy a uživatele v jemněji škálovatelném rozsahu, například uvnitř vaší společnosti nebo organizace. Vytvoření a údržba vlastního lokálního CA vám umožňuje vydávat certifikáty pouze těm uživatelům, kteří jsou důvěryhodnými členy vaší pracovní skupiny. To poskytuje lepší zabezpečení, protože můžete důsledněji řídit, kdo má certifikáty, a tím i to, kdo má přístup k vašim prostředkům. Potenciální nevýhodou udržování lokálního CA je množství času a prostředků, které musíte investovat. Produkt DCM (Digital Certificate Manager) vám však tento proces značně ulehčuje.

Jestliže budete pomocí lokálního CA vydávat certifikáty uživatelům pro účely autentizace klientů, měli byste se rozhodnout, kam budete chtít uživatelské certifikáty ukládat. Když uživatelé obdrží prostřednictvím produktu DCM od lokálního CA své certifikáty, jsou tyto certifikáty standardně uloženy s jejich uživatelským profilem. Produkt DCM však můžete konfigurovat, aby spolupracoval s EIM (Enterprise Identity Mapping), takže jsou příslušné certifikáty uloženy do umístění LDAP (Lightweight Directory Access Protocol). Pokud dáváte přednost tomu, aby uživatelské certifikáty nebyly přiřazeny nebo ukládány k uživatelskému profilu, můžete vydávat certifikáty jiným uživatelům než uživatelům serveru iSeries pomocí rozhraní API.

Poznámka: Bez ohledu na to, kterého CA zvolíte pro vydávání certifikátů, řídí systémový administrátor, kterým CA budou aplikace v systému důvěřovat. Jestliže se ve vašem prohlížeči nachází kopie certifikátu CA nějakého známého CA, může být prohlížeč nastaven tak, aby důvěřoval serverovým certifikátům, které byly tímto CA vydány. Administrátoři nastavují důvěru pro certifikáty CA v příslušné paměti certifikátů produktu DCM. Tato paměť certifikátů obsahuje kopie nejznámějších certifikátů CA. Jestliže však certifikát tohoto CA není uložen v paměti certifikátů, nemůže váš server důvěřovat uživatelskému nebo klientskému certifikátu, který byl tímto CA vydán do té doby, než obdržíte a importujete kopii certifikátu tohoto CA. Tento certifikát musí být ve správném formátu souboru a musíte jej přidat do paměti certifikátů v produktu DCM.

Při rozhodování, zda vašim podnikatelským a bezpečnostním potřebám budou lépe vyhovovat veřejné nebo soukromé certifikáty, bude pro vás možná užitečné prostudovat si některé typické scénáře použití certifikátů.

Související úlohy

Když se rozhodnete, jak chcete certifikáty používat a který budete používat typ, prostudujte si následující procedury, které vám osvětlí, jak použít produkt DCM při realizaci vašeho plánu:

- Vytvoření a provozování soukromého vydavatele certifikátů popisuje úlohy, které musíte provést, pokud se rozhodnete provozovat vlastního CA a vydávat soukromé certifikáty.
- Správa certifikátů od veřejného internetového CA popisuje úlohy, které musíte provést, pokud budete používat certifikáty od některého známého veřejného CA, včetně CA využívajících standardy PKIX.
- Téma Použití lokálního CA na jiných serverech iSeries popisuje úlohy, které musíte provést, pokud budete používat certifikáty od soukromého lokálního CA ve více systémech (než v jednom).

Související pojmy

"Správa certifikátů od veřejného internetového CA" na stránce 45
V této části naleznete informace o správě certifikátů od internetových CA pomocí vytvoření paměti certifikátů.

"Používání veřejných certifikátů versus vydávání soukromých certifikátů" na stránce 28
V této části je vysvětleno, jak určit, který typ certifikátu (veřejný nebo soukromý) bude optimální vzhledem k vašim obchodním potřebám.

"Prvotní nastavení certifikátů" na stránce 37
V této části se dozvíte se, jak začít spravovat certifikáty od veřejného internetového vydavatele certifikátů (CA) a jak vytvořit a provozovat soukromého lokálního vydavatele certifikátu (CA) pro vydávání certifikátů.

"Digitální certifikáty pro podepisování objektů" na stránce 34
Tato část vysvětluje, jak lze certifikáty používat k zajištění integrity objektů nebo k ověření digitálního podpisu na objektu za účelem ověření jeho pravosti.

Související úlohy

"Digitální certifikáty a produkt EIM (Enterprise Identity Mapping)" na stránce 32
Produkt EIM společně s produktem DCM vám umožní použít certifikát jako zdroj pro operaci vyhledávání během mapování EIM za účelem mapování z certifikátu na cílovou totožnost uživatele, která je přidružena ke stejnému identifikátoru EIM.

"Vytvoření uživatelského certifikátu" na stránce 40
Tato část popisuje, jak mohou uživatelé pomocí lokálního CA vydat certifikát pro účely autentizace klienta.

"Vytvoření a provozování lokálního CA" na stránce 38
Toto téma popisuje, jak vytvořit a provozovat lokálního CA k vydávání souktomých certifikátů pro vaše aplikace.

"Použití lokálního CA k vydávání certifikátů pro jiné servery iSeries" na stránce 53
V této části najdete informace o tom, jak pomocí soukromého lokálního CA vydávat certifikáty, které se budou používat na jiných serverech iSeries.

Související odkazy

"Vydávání certifikátů jiným uživatelům než uživatelům systému iSeries pomocí rozhraní API" na stránce 43
V této části je vysvětleno, jak lze pomocí lokálního CA vydávat uživatelům soukromé certifikáty, aniž by se certifikáty přiřazovaly k uživatelskému profilu na serveru iSeries.

Digitální certifikáty pro bezpečnou komunikaci SSL

Tato část vysvětluje, jak certifikáty používat k tomu, aby vaše aplikace mohly vytvářet zabezpečené komunikační relace.

Pomocí digitálních certifikátů můžete konfigurovat aplikace tak, aby používaly SSL (Secure Sockets Layer) pro zabezpečené komunikační relace. Při navázání relace SSL server vždy poskytne kopii svého certifikátu, aby si klient, který vyžaduje spojení, mohl ověřit autenticitu serveru. Použití připojení přes SSL:

- Poskytuje klientovi nebo koncovému uživateli důkaz, že váš počítač je autentický.
- Umožňuje zašifrovat komunikační relaci, což zajistí zachování soukromosti dat, která procházejí přes dané spojení.

Serverová aplikace a aplikace na straně klienta spolupracují při zajištění zabezpečení ochrany dat takto:

1. Serverová aplikace předloží certifikát klientské (uživatelské) aplikaci jakožto doklad o identitě serveru.
2. Klientská aplikace ověřuje identitu serveru srovnáním s kopií certifikátu CA (vydavatele certifikátů), který certifikát vydal. (Klientská aplikace musí mít přístup k lokálně uložené kopii příslušného certifikátu CA.)

3. Serverová a klientská aplikace se dohodnou na symetrickém klíči pro šifrování a použijí jej k zašifrování komunikační relace.
4. Nyní může server (volitelně) požadovat po klientovi, aby předtím, než mu povolí přístup k požadovaným prostředkům, prokázal svoji identitu. Aby bylo možno k prokázání totožnosti použít certifikáty, musí komunikační aplikace podporovat použití certifikátů při autentizaci uživatelů.

V době, kdy SSL navazuje komunikaci a sjednává symetrický klíč, který je následně použit k zašifrování a dešifrování dat aplikace pro tuto konkrétní relaci, používá SSL algoritmus asymetrického klíče (veřejný klíč). To znamená, že váš server a klient používají různé relační klíče, jejichž platnost po určité době automaticky vyprší, a to u každé relace. I v tak nepravděpodobné situaci, že by někdo zachytil a dešifroval určitý relační klíč, nebude tento relační klíč moci být použit pro odvození budoucích klíčů.

Související pojmy

"Digitální certifikáty pro autentizaci uživatelů"
V této části naleznete informace o možném použití certifikátů jako prostředku pro přísnější autentizaci uživatelů, kteří přistupují k prostředkům serveru iSeries.

Digitální certifikáty pro autentizaci uživatelů

V této části naleznete informace o možném použití certifikátů jako prostředku pro přísnější autentizaci uživatelů, kteří přistupují k prostředkům serveru iSeries.

Tradičně uživatelé získávají přístup k prostředkům od aplikace nebo systému na základě svého jména uživatele a hesla. Zvýšit zabezpečení systému můžete dále tím, že namísto uživatelských jmen a hesel použijete k autentizaci a autorizaci relací mezi serverem a uživateli digitální certifikáty. Pomocí produktu DCM (Digital Certificate Manager) také můžete přiřadit uživatelský certifikát k uživatelskému profilu na serveru iSeries nebo jiné totožnosti uživatele. Certifikát má pak stejná oprávnění a povolení jako přiřazená totožnost uživatele nebo uživatelský profil. Alternativně můžete používat rozhraní API a pomocí soukromého lokálního vydavatele certifikátů vydávat certifikáty i uživatelům jiných serverů než serveru iSeries. Tato rozhraní API vám umožní vydávat soukromé certifikáty uživatelům v případech, kdy nebudete chtít, aby tito uživatelé měli uživatelský profil systému iSeries nebo jinou interní totožnost uživatele.

Digitální certifikát funguje jako elektronický doklad a ověřuje, zda osoba předkládající tento certifikát je skutečně tou osobou, za kterou se prohlašuje. V tomto ohledu je certifikát něco podobného jako cestovní pas. Oba tyto ″doklady″ zakládají totožnost jedince, obsahují jedinečné číslo pro účely identifikace a mají rozeznatelnou vydávající instituci, která ověřuje daný doklad jako autentický. V případě certifikátů působí jako důvěryhodná třetí strana, která certifikáty vydává a verifikuje je jako autentický doklad, tzv. vydavatel certifikátů (Certificate Authority, CA).

Pro účely autentizace využívají certifikáty veřejného klíče a souvisejícího soukromého klíče. Vydávající CA tyto klíče spolu s dalšími informacemi o vlastníkovi certifikátu vkládá za účelem identifikace do samotného certifikátu.

Rostoucí počet aplikací nyní zajišťuje podporu pro použití certifikátů při autentizaci klientů během relace SSL. V současné době podporují autentizaci klientů prostřednictvím certifikátů tyto aplikace serveru iSeries:

- Telnet server
- IBM HTTP Server for i5/OS (provozovaný na základě technologie Apache)
- IBM Directory Server
- iSeries Access for Windows (včetně produktu iSeries Navigator Navigator)
- FTP server

V průběhu doby budou podporu pro certifikáty při autentizaci klientů poskytovat zřejmě i další aplikace. Chcete-li zjistit, zda konkrétní aplikace podporu poskytuje, prostudujte si dokumentaci k této aplikaci.

Certifikáty poskytují silnější prostředek autentizace uživatelů z několika důvodů:

- V případě použití hesel existuje vždy možnost, že uživatel své heslo zapomene. Uživatelé se proto musí své uživatelské jméno a heslo učit nazpaměť nebo si je někam zaznamenat, aby si na ně vždy vzpomněli. V důsledku toho mohou neoprávnění uživatelé snadněji získat uživatelská jména a hesla od oprávněných uživatelů. Vzhledem k

tomu, že certifikáty jsou uloženy v souboru nebo na jiném elektronickém místě, zajišťuje přístup k certifikátu a jeho předložení při autentizaci klientská aplikace (nikoliv uživatel samotný). Tím se snižuje pravděpodobnost, že by uživatelé sdíleli certifikáty s neoprávněnými uživateli, pokud neautorizovaní uživatelé nemají přístup do systému daného uživatele. Jako další prostředek ochrany proti neoprávněnému použití lze také certifikáty nainstalovat na čipové karty.

- Certifikát obsahuje soukromý klíč, který se nikdy s certifikátem při identifikaci neposílá. Systém namísto toho používá tento klíč během zpracování zašifrování a dešifrování. Ostatní mohou k identifikaci odesílatele objektu, který je podepsán soukromým klíčem, použít odpovídající veřejný klíč certifikátu.
- Mnoho systémů požaduje hesla, která mají délku 8 znaků nebo i méně, takže tato hesla jsou ve větší míře zranitelná při neoprávněných pokusech o uhádnutí jejich obsahu. Šifrovací klíče certifikátů mají stovky znaků. Díky délce a náhodné povaze obsahu klíčů je uhádnutí klíče mnohem těžší, než je tomu v případě hesla.
- Klíče digitálních certifikátů poskytují několik potenciálních možností použití, které hesla poskytnout nemohou, jako např. zajištění integrity a soukromosti dat. Certifikáty a jejich přiřazené klíče můžete použít např. pro:
  - Zajištění integrity dat prostřednictvím zaznamenávání změn provedených v datech.
  - Prověření, že určitá operace byla skutečně provedena. To se nazývá ″neodmítání″.
  - Zajištění soukromosti přenosu dat použitím SSL (Secure Sockets Layer) při zašifrování komunikačních relací.

Další informace o tom, jak nakonfigurovat aplikace na serveru iSeries, aby během relací SSL používaly při autentizaci klientů certifikáty, uvádí téma Secure Sockets Layer (SSL) v rámci aplikace iSeries Information Center.

Související pojmy

“Digitální certifikáty pro bezpečnou komunikaci SSL” na stránce 30
Tato část vysvětluje, jak certifikáty používat k tomu, aby vaše aplikace mohly vytvářet zabezpečené komunikační relace.

Související odkazy

“Vydávání certifikátů jiným uživatelům než uživatelům systému iSeries pomocí rozhraní API” na stránce 43
V této části je vysvětleno, jak lze pomocí lokálního CA vydávat uživatelům soukromé certifikáty, aniž by se certifikáty přiřazovaly k uživatelskému profilu na serveru iSeries.

Digitální certifikáty a produkt EIM (Enterprise Identity Mapping)

Produkt EIM společně s produktem DCM vám umožní použít certifikát jako zdroj pro operaci vyhledávání během mapování EIM za účelem mapování z certifikátu na cílovou totožnost uživatele, která je přidružena ke stejnému identifikátoru EIM.

Produkt EIM představuje technologii e server , která vám ve vašem podniku umožňuje spravovat totožnosti uživatelů včetně uživatelských profilů a uživatelských certifikátů. Nejčastější formou totožnosti uživatele je uživatelské jméno a heslo. Certifikáty jsou jinou formou totožnosti uživatele. Některé aplikace jsou konfigurovány tak, aby umožnily ověřovat totožnost uživatelů pomocí uživatelského certifikátu spíše než prostřednictvím uživatelského jména a hesla.

EIM můžete použít pro vytvoření mapování mezi totožnostmi uživatelů, což umožňuje uživateli jeho autentizaci pomocí jedné totožnosti uživatele a přístupu k prostředkům jiné totožnosti uživatele, aniž by bylo nutné, aby uživatel zadával požadovanou totožnost uživatele. V EIM toho dosáhnete tak, že definujete přidružení mezi jednou totožností uživatele a jinou totožností uživatele. Identity uživatelů mohou mít různé formy včetně uživatelského certifikátu. Můžete vytvořit individuální přidružení mezi identifikátorem EIM a různými totožnostmi, které patří uživateli s daným identifikátorem EIM. Nebo můžete vytvořit přidružení metod mapující skupinu totožností uživatelů na jednu cílovou totožnost uživatele. Identity uživatelů mohou mít různé formy včetně uživatelského certifikátu. Pokud vytvoříte tato přidružení, mohou být uživatelské certifikáty mapovány na vhodné identifikátory EIM, čímž se zjednoduší použití certifikátů pro autentizaci.

Chcete-li využít této funkce EIM pro správu uživatelských certifikátů, je třeba předtím, než provedete jakékoliv úlohy pro konfiguraci produktu DCM, provést tyto úlohy pro konfiguraci EIM:

1. Chcete-li konfigurovat EIM, použijte průvodce **konfigurací EIM** v produktu **iSeries Navigator**.

2. Pro každého uživatele, který se má podílet na EIM, vytvořte identifikátor EIM.
3. Vytvořte cílové přidružení mezi každým identifikátorem EIM a uživatelským profilem příslušného uživatele v lokálním registru uživatelů operačního systému i5/OS , takže jakýkoliv uživatelský certifikát, který uživatel přiřadí prostřednictvím produktu DCM nebo vytvoří v produktu DCM, může být mapován na uživatelský profil. Použijte definiční jméno registru EIM pro lokální registr uživatelů operačního systému **i5/OS**, které jste zadali v průvodci **konfigurací EIM**.

Po dokončení potřebných úloh konfigurace EIM, musíte použít úlohu **Správa umístění LDAP** a konfigurovat produkt DCM, aby ukládal uživatelské certifikáty do umístění LDAP (Lightweight Directory Access Protocol) namísto uložení s uživatelským profilem. Pokud nakonfigurujete produkty EIM a DCM tak, aby spolu spolupracovaly, budou certifikáty pro použití EIM zpracovávány spíše pomocí úlohy **Vytvořit certifikát** pro uživatelské certifikáty a úlohy **Přiřazení uživatelského certifikátu**, namísto přiřazení certifikátu k uživatelskému profilu. Produkt DCM uloží certifikát do konfigurovaného adresáře LDAP a používá informace rozlišovacího jména (DN) certifikátu pro vytvoření zdrojového přidružení odpovídajícího identifikátoru EIM. To umožňuje operačním systémům a aplikacím používat certifikáty jako zdroje pro operaci vyhledávání během mapování EIM za účelem mapování z certifikátu na cílovou totožnost uživatele, která je přidružena ke stejnému identifikátoru EIM.

Dále, pokud nakonfigurujete produkty EIM a DCM tak, aby spolu spolupracovaly, můžete použít produkt DCM a zkontrolovat data ukončení platnosti uživatelských certifikátů na podnikové úrovni spíše než na systémové úrovni.

Související pojmy

“Používání veřejných certifikátů versus vydávání soukromých certifikátů” na stránce 28
V této části je vysvětleno, jak určit, který typ certifikátu (veřejný nebo soukromý) bude optimální vzhledem k vašim obchodním potřebám.

Související úlohy

“Správa uživatelských certifikátů prostřednictvím data ukončení platnosti” na stránce 42
Produkt DCM poskytuje podporu správy certifikátů prostřednictvím ukončení jejich platnosti, což administrátorům umožňuje ověřovat data ukončení platnosti uživatelských certifikátů na lokálním serveru iSeries. Uživatelská služba produktu DCM pro správu ukončení platnosti certifikátů může být používána společně s produktem EIM (Enterprise Identity Mapping), proto aby administrátoři mohli produkt DCM používat ke kontrole ukončení platnosti uživatelských certifikátů na podnikové úrovni.

“Správa umístění LDAP pro uživatelské certifikáty” na stránce 68
Zde se dozvíte, jak konfigurovat produkt DCM tak, aby ukládal uživatelské certifikáty do umístění serveru adresářů LDAP (Lightweight Directory Access Protocol) a rozšířil tak použití EIM (Enterprise Identity Mapping) pro práci s uživatelskými certifikáty.

Související informace

Téma EIM (Enterprise Identity Mapping) v rámci aplikace Information Center

Digitální certifikáty pro připojení v rámci VPN

V této části je vysvětleno, jak lze certifikáty používat jako součást konfigurace připojení VPN.

Digitální certifikáty můžete použít jako prostředek pro vytvoření připojení VPN na serveru iSeries. Oba koncové systémy dynamického spojení přes VPN se musí být schopny před aktivací spojení navzájem autentizovat. Autentizace koncového systému je na každém konci provedena serverem IKE (Internet Key Exchange). Po úspěšné autentizaci pak servery IKE dohodnou metodologii a algoritmus šifrování, které použijí k zabezpečení daného spojení přes VPN.

Jednou z metod, kterou mohou používat servery IKE ke vzájemné autentizaci, je předem sdílený klíč. Použití předem sdílených klíčů je však méně bezpečné, protože je nutné klíč sdělit administrátorovi druhého koncového systému v rámci VPN manuálně. Existuje tudíž možnost, že by klíč mohl být během procesu sdělování klíče odhalen někomu jinému.

Tomuto riziku se lze vyhnout tak, že namísto předem sdílených klíčů použijete k autentizaci koncových systémů digitální certifikáty. Server IKE je schopen autentizovat certifikát druhého serveru a navázat s ním spojení, aby se mohly dohodnout na metodologii a algoritmu šifrování, které pak použijí k zabezpečení spojení.

Pomocí produktu DCM můžete spravovat certifikáty, které váš server IKE používá k vytvoření dynamického připojení VPN. Nejprve se musíte rozhodnout, zda budete pro server IKE používat veřejné certifikáty nebo zda budete vydávat soukromé certifikáty.

Některé implementace VPN vyžadují, aby certifikáty obsahovaly kromě informace o standardním rozlišovacím jménu i informaci o alternativním jménu subjektu, jako je např. jméno domény nebo adresa elektronické pošty. Pokud použijete k vydání certifikátu funkci lokálního CA, obsaženou v produktu DCM, můžete u certifikátu specifikovat informaci o alternativním jménu subjektu. Specifikací této informace zajistíte kompatibilitu připojení VPN s jinými implementacemi VPN, které by mohly tuto informaci při autentizaci vyžadovat.

Další informace o správě certifikátů pro připojení VPN uvádí tato témata:

- Pokud jste doposud nikdy nepoužívali produkt DCM ke správě certifikátů, tato témata vám pomohou začít:
  - Vytvoření a provozování soukromého lokálního CA popisuje, jak pomocí produktu DCM vydávat soukromé certifikáty pro vaše aplikace.
  - Správa certifikátů od veřejného internetového CA obsahuje informace o tom, jak použít produkt DCM při práci s certifikáty od veřejného CA.
- Pokud již v současné době používáte produkt DCM ke správě certifikátů pro jiné aplikace, dovíte se v následujících tématech, jak specifikovat, aby určitá aplikace používala existující certifikát a které certifikáty může aplikace schválit a autentizovat:
  - Správa přiřazení certifikátu k aplikaci popisuje, jak pomocí produktu DCM přiřadit existující certifikát k nějaké aplikaci, např. serveru IKE.
  - Definování seznamu důvěryhodných CA pro aplikaci obsahuje informace o tom, jak specifikovat, kterým CA může daná aplikace důvěřovat, když aplikace schvaluje certifikát při autentizaci klienta (nebo VPN).

Související informace

Konfigurace spojení VPN

Digitální certifikáty pro podepisování objektů

Tato část vysvětluje, jak lze certifikáty používat k zajištění integrity objektů nebo k ověření digitálního podpisu na objektu za účelem ověření jeho pravosti.

Operační systém IBM i5/OS poskytuje podporu pro používání certifikátů k digitálnímu ″podepisování″ objektů. Digitální podepisování objektů představuje způsob, jak ověřit jak integritu obsahu daného objektu, tak zdroj původu objektu. Podpora pro podepisování objektů posiluje tradiční systémové nástroje systému iSeriespro řízení toho, kdo může měnit objekty. Tradiční řídicí nástroje nemohou objekt chránit před neoprávněným narušením v době, kdy se objekt přenáší v rámci Internetu nebo jiné nedůvěryhodné sítě nebo když se objekt ukládá v jiném systému než iSeries. Tradiční ovládací prvky také nemohou určit, zda došlo k neautorizovaným změnám objektů nebo k pokusům o neoprávněné zásahy do jejich obsahu. Digitální certifikáty poskytují spolehlivý prostředek pro detekci změn podepsaných objektů.

Digitální podepsání určitého objektu spočívá v tom, že se do objektu za použití soukromého klíče certifikátu přidá zašifrované matematické shrnutí dat. Podpis chrání data před neoprávněnými změnami. Digitálním podpisem nedojde k zašifrování objektu a jeho obsahu a k zajištění jeho soukromosti, avšak shrnutí samotné je zašifrováno, a zabraňuje tak neoprávněným změnám do shrnutí. Každý, kdo se chce ujistit, že objekt nebyl v průběhu přenosu změněn a že pochází ze schváleného, legálního zdroje, může pomocí veřejného klíče podpisového certifikátu ověřit originální digitální podpis. Pokud již podpis neodpovídá, mohla být data změněna. V takovém případě může příjemce odmítnout objekt přijmout a požádat podepisovatele objektu o zaslání další kopie objektu.

Jestliže dojdete k závěru, že použití digitálních podpisů vyhovuje vašim potřebám a strategiím v oblasti zabezpečení, měli byste dále vyhodnotit, zda používat veřejné certifikáty nebo vydávat soukromé certifikáty. Hodláte-li distribuovat objekty uživatelům z řad široké veřejnosti, můžete uvažovat o použití certifikátů pro podepisování objektů od některého známého veřejného vydavatele certifikátů (CA). Použití veřejných certifikátů zajišťuje, že ostatní mohou snadno a levně ověřovat podpisy, které na objekty, jež jim distribuujete, umístíte. Jestliže však hodláte distribuovat

objekty výhradně uvnitř vaší organizace, může být vhodnější vydávat certifikáty pro podepisování objektů pomocí produktu DCM a lokálního CA. Použití soukromých certifikátů od lokálního CA je levnější varianta, než nakupování certifikátů od známého veřejného CA.

Podpis na určitém objektu reprezentuje systém, který objekt podepsal, nikoliv konkrétního uživatele v rámci tohoto systému (i když uživatel musí mít příslušné oprávnění, aby mohl používat certifikáty pro podepisování objektů). Pomocí produktu DCM můžete spravovat certifikáty, které používáte při podepisování objektů a při ověřování podpisů na objektech. Produkt DCM můžete rovněž využít k podepisování objektů a ověřování podpisů na objektech.

Související pojmy

"Používání veřejných certifikátů versus vydávání soukromých certifikátů" na stránce 28
V této části je vysvětleno, jak určit, který typ certifikátu (veřejný nebo soukromý) bude optimální vzhledem k vašim obchodním potřebám.

"Digitální certifikáty pro ověřování podpisů na objektech"
V této části je vysvětleno, jak lze certifikáty použít k ověření digitálního podpisu na objektu za účelem ověření jeho pravosti.

Související úlohy

"Ověřování podpisu objektů" na stránce 71
Pomocí produktu DCM (Digital Certificate Manager) lze ověřovat autenticitu digitálních podpisů na objektech. Když ověříte podpis, budete mít jistotu, že data v objektu nebyla změněna poté, co vlastník objektu objekt podepsal.

"Správa veřejných internetových certifikátů k podepisování objektů" na stránce 47
Pomocí produktu DCM (Digital Certificate Manager) můžete spravovat veřejné internetové certifikáty pro digitální podepisování objektů.

"Správa certifikátů pro ověřování podpisů na objektech" na stránce 49
Pomocí produktu DCM (Digital Certificate Manager) můžete spravovat certifikáty pro ověřování podpisů, které používáte při ověření platnosti digitálního podpisu na objektech.

Digitální certifikáty pro ověřování podpisů na objektech

V této části je vysvětleno, jak lze certifikáty použít k ověření digitálního podpisu na objektu za účelem ověření jeho pravosti.

IBM i5/OS poskytuje podporu pro používání certifikátů k ověřování digitálních podpisů na objektech. Každý, kdo se chce ujistit, že objekt nebyl v průběhu přenosu změněn a že pochází ze schváleného zdroje, může pomocí veřejného klíče podpisového certifikátu ověřit originální digitální podpis. Pokud již podpis neodpovídá, mohla být data změněna. V takovém případě může příjemce odmítnout objekt přijmout a požádat podepisovatele objektu o zaslání další kopie objektu.

Podpis na určitém objektu reprezentuje systém, který objekt podepsal, nikoliv konkrétního uživatele v rámci tohoto systému. Jako součást procesu ověřování digitálních podpisů musíte rozhodnout, kterým CA budete důvěřovat a kterým certifikátům budete důvěřovat při podepisování objektů. Pokud se rozhodnete důvěřovat určitému CA (vydavateli certifikátů), můžete si dále zvolit, zda budete důvěřovat podpisům, které někdo jiný vytvoří za použití certifikátu, který tento důvěryhodný CA vydal. Pokud se rozhodnete nedůvěřovat určitému CA, pak také zároveň volíte, že nebudete důvěřovat certifikátům, které tento CA vydává, nebo podpisům, které někdo vytvoří za použití těchto certifikátů.

Systémová hodnota QVFYOBJRST (Ověření obnovy objektu)

Jestliže se rozhodnete provádět ověřování podpisů, jedním z prvních důležitých rozhodnutí, které musíte učinit, je stanovit, jak důležité jsou podpisy pro objekty obnovované ve vašem systému. Tento aspekt řídíte pomocí systémové hodnoty nazvané QVFYOBJRST (Ověření podpisů objektu během obnovy). Předvolené nastavení pro tuto systémovou hodnotu umožňuje, aby nepodepsané objekty byly obnoveny, ale zajišťuje, že podepsané objekty lze obnovit pouze tehdy, když mají platný podpis. Systém definuje objekt jako podepsaný pouze v tom případě, že objekt má podpis, kterému váš systém důvěřuje. Jiné, ″nedůvěryhodné″ podpisy na objektu systém ignoruje a pracuje s objektem, jako kdyby byl nepodepsaný.

Pro systémovou hodnotu QVFYOBJRST lze nastavit několik hodnot, od ignorování všech podpisů až po vyžadování platných podpisů u všech objektů, které systém obnovuje. Tato systémová hodnota ovlivňuje pouze spustitelné objekty, které jsou obnovovány, nikoliv záložní soubory nebo soubory integrovaného systému souborů. Další informace o použití této a dalších systémových hodnot najdete ve Vyhledávači systémových hodnot v rámci aplikace iSeries Information Center.

Pomocí produktu DCM (Digital Certificate Manager) můžete implementovat svá rozhodnutí ve věci důvěryhodných certifikátů i CA a spravovat certifikáty, které používáte k ověřování podpisů na objektech. Produkt DCM můžete rovněž využít k podepisování objektů a ověřování podpisů na objektech.

Související pojmy

"Digitální certifikáty pro podepisování objektů" na stránce 34
Tato část vysvětluje, jak lze certifikáty používat k zajištění integrity objektů nebo k ověření digitálního podpisu na objektu za účelem ověření jeho pravosti.

Související informace

Vyhledávač systémových hodnot

Konfigurace produktu DCM

V této části jsou informace o tom, jak nakonfigurovat vše potřebné k tomu, abyste mohli pomocí produkt DCM spravovat certifikáty a jejich klíče.

Produkt DCM (Digital Certificate Manager) poskytuje uživatelské rozhraní založené na prohlížeči, pomocí kterého můžete provádět správu digitálních certifikátů pro vaše aplikace a uživatele. Uživatelské rozhraní se dělí na dva hlavní rámce: navigační lišta a rámec úloh.

Navigační lišta se používá k volbě úloh, pomocí kterých se spravují certifikáty nebo aplikace, které certifikáty používají. V hlavní navigační liště se sice objevují i některé individuální úlohy, ale většina úloh je organizována do kategorií. Například kategorie **Správa certifikátů** obsahuje různé individuální vedené úlohy, jako jsou např. úlohy Prohlížení certifikátu, Obnova certifikátu, Import certifikátu a tak dále. Pokud nějaká položka v navigační liště představuje kategorii, která obsahuje více než jednu úlohu, objeví se nalevo od položky šipka. Šipka naznačuje, že pokud vyberete tuto kategorii, zobrazí se rozšířený seznam úloh, takže si budete moci zvolit, kterou úlohu provést.

S výjimkou kategorie **Rychlá cesta** jsou všechny úlohy v navigační liště vedené úlohy, takže jste postupně prováděni sérií kroků, abyste úlohu rychle a snadno dokončili. Kategorie Rychlá cesta poskytuje sérii různých funkcí pro správu certifikátů a aplikací, které zkušeným uživatelům produktu DCM umožňují rychlý přístup k celé řadě souvisejících úloh z centrální sady stránek.

To, které úlohy jsou v navigační liště k dispozici, závisí na paměti certifikátů, ve které zrovna pracujete. Kategorie a počet úloh, které v navigační liště vidíte, se dále mění v závislosti na oprávněních vašeho uživatelského profilu v operačním systému i5/OS. Veškeré úlohy týkající se provozování CA, správy certifikátů, které používají aplikace, a další úlohy systémové úrovně jsou dostupné pouze pro správce nebo administrátory serveru iSeries. Aby si mohl správce systému nebo administrátor tyto úlohy zobrazovat a používat, musí mít zvláštní oprávnění *SECADM a *ALLOBJ. Uživatelé, kteří toto zvláštní oprávnění nemají, mají přístup pouze k funkcím týkajícím se uživatelských certifikátů.

Informace o konfigurování produktu DCM a o používání produktu při správě vašich certifikátů naleznete v tématech:

Pokud byste potřebovali podrobnější informace o použití digitálních certifikátů v prostředí Internetu za účelem zvýšení bezpečnosti vašeho systému a sítě, pak pro vás budou výborným zdrojem informací webové stránky VeriSign. Na webových stránkách VeriSign je k dispozici rozsáhlá knihovna věnovaná problematice digitálních certifikátů i řadě dalších témat týkajících se bezpečnosti Internetu. Tuto knihovnu můžete navštívit na internetové adrese VeriSign Help Desk .

Spuštění produktu Digital Certificate Manager

V této části je vysvětleno, jak ve vašem systému zpřístupníte produkt DCM.

Abyste mohli využívat funkce produktu DCM, musíte jej spustit. Chcete-li mít jistotu, že spustíte produkt DCM správně, postupujte takto:

1. Nainstalujte produkt 5722 SS1, volbu 34. To je produkt Digital Certificate Manager (DCM).
2. Nainstalujte produkt 5722 DG1. Jedná se o IBM HTTP Server for i5/OS.
3. Pomocí produktu iSeries Navigator spusťte administrační rozhraní HTTP serveru:
   a. Spusťte produkt **iSeries Navigator** .
   b. Dvakrát klepněte na váš systém v hlavním stromovém zobrazení.
   c. Rozbalte **Síť > Servery > TCP/IP**.
   d. Klepněte pravým tlačítkem myši na **Správa HTTP**.
   e. Klepněte na **Start**.
4. Spusťte váš webový prohlížeč.
5. Pomocí prohlížeče přejděte na stránku úloh na vašem serveru iSeries na adrese http://*your_system_name*:2001.
6. Vyberte volbu **Digital Certificate Manager** ze seznamu produktů na stránce úloh iSeries a spustí se uživatelské rozhraní produktu DCM.

Související pojmy

"Scénář: Použití certifikátů pro externí autentizaci" na stránce 12
V tomto scénáři je popsáno, kdy a jak použít certifikáty jako prostředek autentizace, chcete-li chránit a omezovat přístup veřejných uživatelů k veřejným nebo extranetovým prostředkům a aplikacím.

Prvotní nastavení certifikátů

V této části se dozvíte se, jak začít spravovat certifikáty od veřejného internetového vydavatele certifikátů (CA) a jak vytvořit a provozovat soukromého lokálního vydavatele certifikátu (CA) pro vydávání certifikátů.

Levá lišta v produktu DCM (Digital Certificate Manager) je navigační lišta úloh. V této liště můžete vybírat z široké škály úloh pro správu certifikátů a aplikací, které certifikáty používají. To, které úlohy jsou v této liště k dispozici, závisí na paměti certifikátů, se kterou pracujete (pokud s nějakou pracujete), a na oprávnění vašeho uživatelského profilu. Většina úloh je dostupná pouze tehdy, pokud máte zvláštní oprávnění *ALLOBJ a *SECADM. Chcete-li používat produkt DCM k ověření podpisů objektů, musí mít váš uživatelský profil zvláštní oprávnění *AUDIT.

Pokud používáte produkt Digital Certificate Manager (DCM) poprvé, paměti certifikátů ještě neexistují. Navigační okno zobrazí následující úlohy pouze v případě, že máte nezbytná oprávnění:

- Správa uživatelských certifikátů.
- Vytvoření nové paměti certifikátů.
- Vytvoření vydavatele certifikátů (CA). (Poznámka: Poté, co pomocí této úlohy vytvoříte soukromého lokálního CA, nebude se již tato úloha v seznamu objevovat.)
- Správa umístění CRL.
- Správa umístění LDAP pro uživatelské certifikáty.
- Správa míst na požadavky PKIX.
- Vraťte se k úlohám iSeries.

I v případě, že paměti certifikátů ve vašem systému existují (například při migraci z předchozí verze produktu DCM), produkt DCM zobrazí v levé navigační liště pouze omezený počet úloh nebo kategorií úloh. Úlohy a kategorie, které produkt DCM zobrazí, se liší dle paměti certifikátů, která je otevřená (pokud je nějaká otevřená), a zvláštního oprávnění vašeho uživatelského profilu.

Předtím, než můžete začít pracovat s většinou úloh pro správu certifikátů a aplikací, totiž musíte do příslušné paměti certifikátů vstoupit. Chcete-li otevřít určitou paměť certifikátů, klepněte na volbu **Výběr paměti certifikátů** v navigační liště.

V navigační liště produktu DCM je k dispozici také tlačítko **Zabezpečené spojení**. Pomocí tlačítka můžete otevřít další okno prohlížeče a inicializovat zabezpečené spojení prostřednictvím SSL (Secure Sockets Layer). Chcete-li tuto funkci úspěšně používat, musíte nejprve nakonfigurovat produkt IBM HTTP Server for i5/OS tak, aby používal SSL a fungoval v režimu zabezpečení. Pak musíte spustit HTTP server v režimu zabezpečení. Pokud jste nenakonfigurovali a nespustili HTTP server v režimu SSL, zobrazí se vám chybová zpráva a prohlížeč nespustí zabezpečenou relaci.

Jak začít

I když zřejmě budete chtít používat certifikáty k zajištění řady cílů v oblasti zabezpečení, to, co budete dělat nejdříve, záleží především na tom, jakým způsobem chcete certifikáty získávat. Existují v zásadě dvě cesty, které můžete při prvotním použití produktu DCM zvolit, a to v závislosti na tom, zda hodláte používat veřejné certifikáty nebo vydávat soukromé certifikáty.

Související pojmy

"Používání veřejných certifikátů versus vydávání soukromých certifikátů" na stránce 28
V této části je vysvětleno, jak určit, který typ certifikátu (veřejný nebo soukromý) bude optimální vzhledem k vašim obchodním potřebám.

Vytvoření a provozování lokálního CA

Toto téma popisuje, jak vytvořit a provozovat lokálního CA k vydávání souktomých certifikátů pro vaše aplikace.

Po důkladném zvážení vašich požadavků a strategií v oblasti zabezpečení jste se rozhodli provozovat lokálního vydavatele certifikátů (CA) a vydávat pro své aplikace soukromé certifikáty. Prostřednictvím produktu DCM (Digital Certificate Manager) můžete vytvořit a provozovat vlastního lokálního CA. Produkt DCM nabízí cestu vedených úloh, kterou projdete procesem vytvoření CA a použití CA při vydávání certifikátů pro vaše aplikace. Forma vedených úloh zajišťuje, že budete mít všechno nezbytné k tomu, abyste mohli začít pomocí digitálních certifikátů konfigurovat aplikace (aby používaly SSL), podepisovat objekty a ověřovat podpisy objektů.

Poznámka: Chcete-li používat certifikáty v kombinaci s produktem IBM HTTP Server for i5/OS, musíte ještě před zahájením práce s produktem DCM vytvořit a nakonfigurovat webový server. Když konfigurujete webový server pro použití SSL, vygeneruje se pro server určité ID aplikace. Tento ID aplikace si musíte poznamenat, abyste pak mohli v produktu DCM specifikovat, který certifikát bude tato aplikace používat při SSL.

Server neukončujte a nerestartujte, dokud mu pomocí produktu DCM nepřiřadíte certifikát. Pokud ukončíte a restartujete instanci *ADMIN webového serveru předtím, než mu přiřadíte certifikát, server se nerestartuje a nebudete moci pomocí produktu DCM serverový certifikát přiřadit.

Chcete-li prostřednictvím produktu DCM vytvořit a provozovat lokálního CA, postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště produktu DCM vyberte volbu Vytvoření vydavatele certifikátů (CA) a zobrazí se vám série formulářů. Tyto formuláře vás provedou procesem vytvoření lokálního CA a dalšími úlohami potřebnými k zahájení používání digitálních certifikátů pro SSL, podepisování objektů a ověřování podpisů.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (?) v horní části stránky, čímž se dostanete do online nápovědy.
3. Vyplňte všechny formuláře v této vedené úloze. V rámci vyplňování těchto formulářů provádíte všechny úlohy nutné pro nastavení funkčního vydavatele certifikátů (CA), a to konkrétně:
   a. Zvolíte způsob uložení soukromého klíče certifikátu lokálního CA. (Tento krok je k dispozici pouze tehdy, pokud máte nainstalovaný produkt IBM Cryptographic Coprocessor ve vašem systému. Pokud váš systém nemá šifrovací koprocesor, produkt DCM uloží certifikát a jeho soukromý klíč automaticky do paměti certifikátů lokálního CA.)

b. Zadáte identifikační informace pro lokálního CA.
c. Nainstalujete certifikát lokálního CA na váš PC nebo do prohlížeče, aby váš software mohl rozpoznat lokálního CA a potvrzovat certifikáty, které lokální CA vydá.
d. Zvolíte strategická data pro lokálního CA.
e. Pomocí nového lokálního CA vydáte serverový nebo klientský certifikát, který vaše aplikace budou moci používat pro připojení přes SSL. (Pokud je v systému nainstalován produkt IBM Cryptographic Coprocessor, můžete v rámci tohoto kroku zvolit způsob uložení soukromého klíče serverového nebo klientského certifikátu. Pokud váš systém koprocesor nemá, produkt DCM automaticky uloží certifikát a jeho soukromý klíč do paměti certifikátů *SYSTEM. Produkt DCM vytváří paměť certifikátů *SYSTEM jako součást této dílčí úlohy.)
f. Vyberete aplikace, které mohou používat serverový nebo klientský certifikát pro připojení přes SSL.

   Poznámka: Jestliže jste již dříve prostřednictvím produktu DCM vytvořili paměť certifikátů *SYSTEM při správě certifikátů pro SSL od veřejného internetového CA, neprovádíte tento ani předchozí krok.
g. Pomocí nového lokálního CA vydáte certifikát pro podepisování objektů, který aplikace budou moci používat k digitálnímu podepisování objektů. Tato dílčí úloha vytvoří paměť certifikátů *OBJECTSIGNING. Tuto paměť certifikátů budete používat při správě certifikátů pro podepisování objektů.
h. Vyberete aplikace, které mohou certifikát pro podepisování objektů používat k umístění digitálního podpisu na objekty.

   Poznámka: Jestliže jste již dříve pomocí produktu DCM vytvořili paměť certifikátů *OBJECTSIGNING při správě certifikátů pro podepisování objektů od veřejného internetového CA, neprovádíte tento ani předchozí krok.
i. Vyberete aplikace, které vašemu lokálnímu CA budou důvěřovat.

Po dokončení této vedené úlohy budete mít hotovo vše potřebné k tomu, abyste mohli u vašich aplikací nakonfigurovat SSL pro zabezpečenou komunikaci.

Poté, co takto nakonfigurujete své aplikace, musí si uživatelé, kteří přistupují k aplikacím prostřednictvím připojení přes SSL, pomocí produktu DCM nainstalovat kopii certifikátu lokálního CA. Každý uživatel musí mít kopii tohoto certifikátu, aby ho jeho klientský software mohl použít při autentizaci identity serveru jakožto součást navazování spojení přes SSL. Uživatelé mohou pomocí produktu DCM buď zkopírovat certifikát CA do souboru, nebo certifikát stáhnout do svých prohlížečů. Způsob, jakým uživatelé ukládají certifikát lokálního CA, závisí na typu klientského softwaru, který používají k navázání spojení s aplikací přes SSL.

Pomocí lokálního CA můžete také vydávat certifikáty pro aplikace na jiných serverech iSeries v rámci vaší sítě.

Další informace o tom, jak používat DCM při správě uživatelských certifikátů a jak mohou uživatelé získat kopii certifikátu lokálního CA, aby byli schopni autentizovat certifikáty vydané lokálním CA, najdete v tématech:

Související pojmy

“Používání veřejných certifikátů versus vydávání soukromých certifikátů” na stránce 28
V této části je vysvětleno, jak určit, který typ certifikátu (veřejný nebo soukromý) bude optimální vzhledem k vašim obchodním potřebám.

“Správa uživatelských certifikátů” na stránce 40
Pro získání certifikátů s SSL nebo přidružení existujících certifikátů k jejich uživatelským profilům na serveru iSeries můžete využít produkt DCM.

Související úlohy

“Použití lokálního CA k vydávání certifikátů pro jiné servery iSeries” na stránce 53
V této části najdete informace o tom, jak pomocí soukromého lokálního CA vydávat certifikáty, které se budou používat na jiných serverech iSeries.

“Získání kopie certifikátu soukromého CA” na stránce 44
Tato část vysvětluje, jak získat kopii certifikátu soukromého CA a jak ji nainstalovat na vaše PC tak, abyste mohli autentizovat libovolný serverový certifikát, který tento CA vydá.

Související odkazy

“Vydávání certifikátů jiným uživatelům než uživatelům systému iSeries pomocí rozhraní API” na stránce 43
V této části je vysvětleno, jak lze pomocí lokálního CA vydávat uživatelům soukromé certifikáty, aniž by se certifikáty přiřazovaly k uživatelskému profilu na serveru iSeries.

Správa uživatelských certifikátů:

Pro získání certifikátů s SSL nebo přidružení existujících certifikátů k jejich uživatelským profilům na serveru iSeries můžete využít produkt DCM.

Jestliže uživatelé přistupují na vaše veřejné nebo interní servery prostřednictvím připojení přes SSL, musí mít kopii certifikátu vydavatele certifikátů (CA), který serverový certifikát vydal. Tento certifikát CA musí mít proto, aby jejich klientský software mohl ověřit autenticitu serverového certifikátu a vytvořit připojení. Pokud server používá certifikát od veřejného CA, je možné, že uživatelský software již kopii certifikátu CA vlastní. Tudíž ani vy jako administrátor produktu DCM, ani vaši uživatelé nemusíte před zapojením do relace SSL provádět žádnou akci. Pokud však server používá certifikát od soukromého lokálního CA, musí uživatelé předtím, než vytvoří relaci SSL s tímto serverem, získat kopii certifikátu lokálního CA.

Navíc, pokud serverová aplikace podporuje a vyžaduje autentizaci klientů prostřednictvím certifikátů, musí uživatelé předložit přijatelný uživatelský certifikát, aby mohli přistupovat k prostředkům, které server poskytuje. V závislosti na vašich potřebách zabezpečení mohou uživatelé předkládat buď certifikát od veřejného internetového CA, nebo certifikát získaný od lokálního CA, kterého provozujete. Jestliže vaše serverová aplikace poskytuje přístup k prostředkům interním uživatelům, kteří v současné době mají uživatelský profil v systému iSeries , můžete pomocí produktu DCM přidat jejich certifikát k jejich uživatelským profilům. Tímto přiřazením zajistíte, aby uživatelé měli při předkládání certifikátu stejná přístupová práva a omezení k prostředkům, jaká jim zaručuje nebo omezuje jejich uživatelský profil.

Pomocí produktu DCM můžete spravovat certifikáty, které jsou přiřazeny k uživatelskému profilu na serveru iSeries. Pokud máte uživatelský profil se zvláštními oprávněními *SECADM a *ALLOBJ, můžete spravovat přiřazení certifikátů jak pro svůj uživatelský profil, tak pro uživatelské profily ostatních uživatelů. Když není otevřena žádná paměť certifikátů nebo když je otevřena paměť certifikátů lokálního CA, pak v navigační liště můžete vybrat volbu **Správa uživatelských certifikátů** a dostanete se tak k příslušným úlohám. Jestliže je otevřena jiná paměť certifikátů, pak jsou úlohy týkající se uživatelských certifikátů integrovány do úloh v rámci volby **Správa certifikátů**.

Uživatelé, kteří nemají zvláštní oprávnění uživatelských profilů *SECADM a *ALLOBJ, mohou spravovat pouze přiřazení svých vlastních certifikátů. Přes volbu **Správa uživatelských certifikátů** se dostanou k úlohám, které jim umožní zobrazit certifikáty přiřazené k jejich uživatelskému profilu, odstranit certifikát ze svého uživatelského profilu nebo přiřadit k uživatelskému profilu certifikát od jiného CA. Uživatelé, bez ohledu na zvláštní oprávnění svých uživatelských profilů, mohou získat uživatelský certifikát od lokálního CA tak, že použijí úlohu **Vytvoření certifikátu** v hlavní navigační liště.

Další informace o použití produktu DCM při správě a vytváření uživatelských certifikátů naleznete v těchto tématech:

Související úlohy

“Vytvoření a provozování lokálního CA” na stránce 38
Toto téma popisuje, jak vytvořit a provozovat lokálního CA k vydávání souktomých certifikátů pro vaše aplikace.

“Získání kopie certifikátu soukromého CA” na stránce 44
Tato část vysvětluje, jak získat kopii certifikátu soukromého CA a jak ji nainstalovat na vaše PC tak, abyste mohli autentizovat libovolný serverový certifikát, který tento CA vydá.

Vytvoření uživatelského certifikátu:

Tato část popisuje, jak mohou uživatelé pomocí lokálního CA vydat certifikát pro účely autentizace klienta.

Chcete-li používat digitální certifikáty k autentizaci uživatelů, musí mít uživatelé certifikáty. Pokud pomocí produktu Digital Certificate Manager (DCM) provozujete soukromého lokálního vydavatele certifikátů (CA), můžete tohoto CA použít i k vydávání certifikátu jednotlivým uživatelům. Každý uživatel, který chce získat certifikát, musí v rámci

produktu DCM použít úlohu **Vytvoření certifikátu**. Aby mohl uživatel získat certifikát od lokálního CA, musí strategie CA povolovat danému CA vydávání uživatelských certifikátů.

Chcete-li získat certifikát od lokálního CA, postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště vyberte volbu **Vytvoření certifikátu**.
3. Vyberte **Uživatelský certifikát** jako typ certifikátu, který budete vytvářet. Zobrazí se formulář, do kterého zadáte identifikační informace pro certifikát.
4. Vyplňte formulář a klepněte na **Pokračovat**.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
5. V tomto bodě produkt DCM ve spolupráci s vaším prohlížečem vytvoří soukromý a veřejný klíč certifikátu. Prohlížeč pravděpodobně zobrazí okna, aby vás tímto procesem provedl. Postupujte podle instrukcí, které vám pro tyto úlohy poskytne prohlížeč. Když prohlížeč vygeneruje klíče, zobrazí se potvrzující stránka, která oznamuje, že produkt DCM vytvořil certifikát.
6. Nainstalujte nový certifikát do prohlížeče. Prohlížeč pravděpodobně zobrazí okna, aby vás tímto procesem provedl. Při provádění této úlohy postupujte podle instrukcí, které vám poskytne prohlížeč.
7. Klepnutím na **OK** úlohu dokončíte.

Během zpracování produkt DCM automaticky přiřadí certifikát k vašemu uživatelskému profilu na serveru iSeries.

Pokud byste chtěli, aby certifikát od jiného CA, který uživatel předkládá při autentizaci klienta, měl stejná oprávnění jako jeho uživatelský profil, může uživatel pomocí produktu DCM přiřadit certifikát ke svému uživatelskému profilu.

Související pojmy

"Používání veřejných certifikátů versus vydávání soukromých certifikátů" na stránce 28
V této části je vysvětleno, jak určit, který typ certifikátu (veřejný nebo soukromý) bude optimální vzhledem k vašim obchodním potřebám.

Související úlohy

"Přiřazení uživatelského certifikátu"
Uživatelský certifikát, který vlastníte, můžete přiřadit k vašemu uživatelskému profilu v operačním systému i5/OS nebo k identitě uživatele. Certifikát může pocházet i od soukromého lokálního CA v jiném systému, nebo od veřejného CA. Abyste mohli přiřadit certifikát k totožnosti uživatele, musí server vydávajícímu CA důvěřovat a tento certifikát nesmí být přiřazen k jinému uživatelskému profilu nebo totožnosti uživatele v systému.

"Získání kopie certifikátu soukromého CA" na stránce 44
Tato část vysvětluje, jak získat kopii certifikátu soukromého CA a jak ji nainstalovat na vaše PC tak, abyste mohli autentizovat libovolný serverový certifikát, který tento CA vydá.

Přiřazení uživatelského certifikátu:

Uživatelský certifikát, který vlastníte, můžete přiřadit k vašemu uživatelskému profilu v operačním systému i5/OS nebo k identitě uživatele. Certifikát může pocházet i od soukromého lokálního CA v jiném systému, nebo od veřejného CA. Abyste mohli přiřadit certifikát k totožnosti uživatele, musí server vydávajícímu CA důvěřovat a tento certifikát nesmí být přiřazen k jinému uživatelskému profilu nebo totožnosti uživatele v systému.

Někteří uživatelé mohou vlastnit certifikáty od externích CA (vydavatelů certifikátů) nebo od místního vydavatele certifikátů na jiném serveru iSeries , které chcete z pozice administrátora zpřístupnit pro produkt DCM. To umožní vám i uživatelům spravovat pomocí produktu DCM tyto certifikáty, které jsou nejčastěji používané pro autentizaci klienta. Úloha **Přiřazení uživatelského certifikátu** poskytuje mechanismus, kterým lze povolit uživateli vytvořit přiřazení DCM pro certifikáty získané od externího CA (vydavatele certifikátů).

Pokud uživatel přidělí certifikát, má produkt DCM na výběr z těchto dvou možností zpracování přiděleného certifikátu.

- Uloží certifikát lokálně k uživatelskému profilu uživatele na serveru iSeries. Pokud není pro produkt DCM definováno umístění LDAP, umožní úloha **Přiřazení uživatelského certifikátu** uživateli přidělit externí certifikát uživatelskému profilu v operačním systému i5/OS. Přiřazení certifikátu k uživatelskému profilu umožní, že lze certifikát v systému použít s aplikacemi vyžadujícími certifikáty pro autentizaci klienta.
- Uloží certifikát do umístění LDAP (Lightweight Directory Access Protocol) pro použití s EIM (Enterprise Identity Mapping). Pokud je definováno umístění LDAP a server iSeries je konfigurován pro práci s EIM, umožní úloha **Přiřazení uživatelského certifikátu** uživateli uložit kopii externího certifikátu do zadaného adresáře LDAP. Produkt DCM také vytvoří pro certifikát zdrojové přidružení v EIM. Takový způsob ukládání certifikátů dovoluje administrátorovi EIM rozeznávat certifikáty jako platné totožnosti uživatelů, které mohou pracovat s EIM.

  Poznámka: Předtím, než může uživatel přiřadit certifikát totožnosti uživatele v konfiguraci EIM, musí být EIM pro uživatele náležitě konfigurován. Tato konfigurace EIM vyžaduje vytvoření identifikátoru EIM pro uživatele a vytvoření cílového přidružení identifikátoru EIM a uživatelského profilu. V opačném případě nemůže produkt DCM vytvořit pro certifikát odpovídající zdrojové přidružení s identifikátorem EIM.

K tomu, aby uživatel mohl použít úlohu **Přiřazení uživatelského certifikátu**, musí splňovat tyto požadavky:

1. Musí mít zabezpečenou relaci s HTTP serverem, jejímž prostřednictvím přistupuje k produktu DCM.

   To, zda máte zabezpečenou relaci, je určeno číslem portu v adrese URL, který používáte pro přístup do produktu DCM. Jestliže jste použili port 2001, což je předvolený port pro přístup do produktu DCM, pak nemáte zabezpečenou relaci. Než budete moci přepnout na zabezpečenou relaci, musí být také HTTP server nakonfigurován pro použití SSL.

   Pokud uživatel zvolí tuto úlohu, zobrazí se nové okno prohlížeče. Jestliže uživatel nemá zabezpečenou relaci, vyzve jej produkt DCM, aby klepl na **Přiřazení uživatelského certifikátu** a relaci tak vytvořil. Produkt DCM pak iniciuje navázání spojení přes SSL (Secure Sockets Layer) s prohlížečem uživatele. V rámci navázání tohoto spojení může prohlížeč uživatele vyzvat, aby specifikoval, zda se má důvěřovat vydavateli certifikátů (CA), jenž vydal certifikát, který identifikuje HTTP server. Prohlížeč také může uživatele vyzvat, aby specifikoval, zda lze přijmout samotný serverový certifikát.
2. Musí předložit certifikát pro autentizaci klienta.

   V závislosti na konfiguraci nastavení prohlížeče vás může prohlížeč vyzvat, abyste vybrali certifikát, který použijete k autentizaci. Jestliže prohlížeč předloží certifikát od CA, který systém přijme jako důvěryhodný, zobrazí produkt DCM v samostatném okně informace o certifikátu. Jestliže nepředložíte přijatelný certifikát, server vás může namísto toho vyzvat, abyste předtím, než vám povolí přístup, zadali vaše uživatelské jméno a heslo.
3. Musí mít v prohledávacím programu certifikát, který není přidružen k totožnosti uživatele, jenž úlohu provádí. (Nebo pokud je DCM konfigurován pro práci společně s EIM, musí mít uživatel v prohledávacím programu certifikát, který ještě není v umístění LDAP pro DCM uložen.)

   Jakmile vytvoříte zabezpečenou relaci, produkt DCM se pokusí načíst příslušný certifikát z vašeho prohlížeče, aby ho mohl přiřadit k vaší totožnosti uživatele. Jestliže produkt DCM úspěšně načte jeden nebo více certifikátů, můžete si prohlédnout informace o certifikátu a rozhodnout se přiřadit certifikát k vašemu uživatelskému profilu.

   Pokud produkt DCM nezobrazí informace z certifikátu, znamená to, že jste neposkytli certifikát, který by produkt DCM mohl přiřadit k vaší totožnosti uživatele. Příčinou by mohl být některý z problémů s uživatelskými certifikáty. Například certifikáty, které obsahuje váš prohlížeč, již mohou být k vaší totožnosti uživatele přiřazeny.

   Související úlohy

   “Vytvoření uživatelského certifikátu” na stránce 40
   Tato část popisuje, jak mohou uživatelé pomocí lokálního CA vydat certifikát pro účely autentizace klienta.

   “Odstraňování problémů s přiřazením uživatelského certifikátu” na stránce 78

   Související informace

   Přehled tématu EIM (Enterprise Identity Mapping) v rámci aplikace Information Center

Správa uživatelských certifikátů prostřednictvím data ukončení platnosti:

Produkt DCM poskytuje podporu správy certifikátů prostřednictvím ukončení jejich platnosti, což administrátorům umožňuje ověřovat data ukončení platnosti uživatelských certifikátů na lokálním serveru iSeries. Uživatelská služba

produktu DCM pro správu ukončení platnosti certifikátů může být používána společně s produktem EIM (Enterprise Identity Mapping), proto aby administrátoři mohli produkt DCM používat ke kontrole ukončení platnosti uživatelských certifikátů na podnikové úrovni.

Aby mohla být služba pro správu ukončení platnosti využita pro uživatelské certifikáty na úrovni podniku, musí být v podniku nakonfigurován produkt EIM, který navíc musí obsahovat pro uživatelské certifikáty odpovídající informace o mapování. Ke kontrole ukončení platnosti uživatelských certifikátů, které nejsou přidruženy vašemu uživatelskému profilu, budete potřebovat speciální oprávnění *ALLOBJ a *SECADM.

Použití DCM k zobrazení certifikátů na základě ukončení platnosti vám umožňuje rychle a snadno vymezit ty certifikáty, jejichž platnost bude brzy ukončena, abyste je mohli včas obnovit.

Chcete-li zobrazit a spravovat uživatelské certifikáty na základě data ukončení platnosti, proveďte následující kroky:

1. Spusťte produkt DCM.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit v průběhu práce s produktem DCM určitý formulář, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
2. V navigační liště vyberte volbu **Správa uživatelských certifikátů**. Zobrazí se seznam úloh .

   Poznámka: Pokud právě pracujete s pamětí certifikátů a chcete zobrazit seznam úloh, vyberte volbu **Správa certifikátů** čímž zobrazíte seznam úloh, poté vyberte volbu **Zkontrolovat ukončení platnosti** a vyberte volbu **Uživatel**.
3. Pokud má váš uživatelský profil speciální oprávnění *ALLOBJ a *SECADM, můžete vybrat metodu výběru uživatelských certifikátů, které chcete zobrazit a spravovat na základě data ukončení platnosti. (Pokud váš uživatelský profil nemá tato speciální oprávnění, vyzve vás produkt DCM k zadání rozsahu dat ukončení platnosti, jak je popsáno v následujícím kroku.) Můžete zadat jednu z následujících voleb:
   - **Uživatelský profil**, chcete-li zobrazit a spravovat uživatelské certifikáty přidělené specifickému uživatelskému profilu operačního systému i5/OS. Zadejte **Jméno uživatelského profilu** a klepněte na **Pokračovat**.

     Poznámka: Jiný uživatelský profil než svůj vlastní můžete uvést pouze tehdy, pokud máte speciální oprávnění *ALLOBJ a *SECADM.
   - **Všechny uživatelské certifikáty**, chcete-li zobrazit a spravovat uživatelské certifikáty všech totožností uživatelů.
4. Do pole **Rozsah dat ukončení platnosti ve dnech (1-365)** zadejte počet dnů odpovídající ukončení platnosti certifikátů, které chcete zobrazit dle data ukončení platnosti, a klepněte na **Další**. Produkt DCM zobrazí všechny uživatelské certifikáty zadaného uživatelského profilu, jejichž platnost končí mezi dnešním dnem a datem, které odpovídá hodnotě zadaných dnů. Produkt DCM také zobrazí všechny uživatelské certifikáty, jejichž platnost končí před dnešním datem.
5. Vyberte uživatelský certifikát, který chcete spravovat. Můžete se rozhodnout, že si prohlédnete podrobné informace certifikátu nebo že odstraníte certifikát z přiřazené totožnosti uživatele.
6. Až dokončíte práci s certifikáty na seznamu, klepněte na **Zrušit** a opustíte seznam úloh.

Související úlohy

“Digitální certifikáty a produkt EIM (Enterprise Identity Mapping)” na stránce 32
Produkt EIM společně s produktem DCM vám umožní použít certifikát jako zdroj pro operaci vyhledávání během mapování EIM za účelem mapování z certifikátu na cílovou totožnost uživatele, která je přidružena ke stejnému identifikátoru EIM.

Související informace

Přehled tématu EIM (Enterprise Identity Mapping) v rámci aplikace Information Center

Vydávání certifikátů jiným uživatelům než uživatelům systému iSeries pomocí rozhraní API:

V této části je vysvětleno, jak lze pomocí lokálního CA vydávat uživatelům soukromé certifikáty, aniž by se certifikáty přiřazovaly k uživatelskému profilu na serveru iSeries.

Počínaje verzí V5R3 jsou k dispozici dvě nová rozhraní API, pomocí kterých můžete vydávat certifikáty i jiným uživatelům, než jsou uživatelé systému i5/OS. Když jste vydávali certifikáty uživatelům pomocí lokálního vydavatele certifikátů (CA) v předchozích verzích, byly tyto certifikáty automaticky přiřazeny k jejich uživatelskému profilu na serveru iSeries. Pokud jste tudíž chtěli pomocí lokálního CA vydat nějakému uživateli certifikát pro autentizaci klienta, museli jste tomuto uživateli vytvořit uživatelský profil na serveru iSeries. A když uživatel potřeboval získat od lokálního CA certifikát pro autentizaci klienta, musel k tomu použít produkt DCM (Digital Certificate Manager). Takže každý uživatel musel mít uživatelský profil na serveru iSeries , který byl hostitelským systémem produktu DCM a platný prostředek pro přihlášení na tento server iSeries.

Přiřazení certifikátu k uživatelskému profilu má své výhody, zejména pokud jde o interní uživatele. Kvůli výše uvedeným požadavkům a omezením však bylo poněkud nepraktické používat lokálního CA k vydávání uživatelských certifikátů velkému počtu uživatelů, zvláště když nechcete, aby tito uživatelé měli uživatelský profil na serveru iSeries. Abyste nemuseli těmto uživatelům zřizovat uživatelský profil, museli uživatelé zaplatit za certifikát od nějakého veřejného CA, když jste vyžadovali při autentizaci uživatelů vašich aplikací certifikáty.

Tato dvě nová rozhraní API vám umožní poskytovat rozhraní pro vytvoření uživatelského certifikátu podepsaného certifikátem lokálního CA pro jakékoliv uživatelské jméno. Certifikát pak nebude přiřazen k určitému uživatelskému profilu. Uživatel nemusí existovat na serveru iSeries , který je hostitelským systémem produktu DCM, a uživatel nepotřebuje k vytvoření certifikátu produkt DCM.

K dispozici jsou dvě různá API pro dva nejběžnější typy prohlížečů, která vyvoláte, když budete pomocí produktu Net.Data vytvářet program pro vydávání certifikátů uživatelům. Aplikace, kterou vytvoříte, musí poskytovat kód grafického uživatelského rozhraní (GUI) potřebný k tomu, abyste vytvořili uživatelský certifikát a vyvolali jedno z vhodných API, pomocí něhož se zajistí, že certifikát bude podepisovat lokální CA.

Další informace o použití těchto API uvádí stránky:

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

Související pojmy

“Používání veřejných certifikátů versus vydávání soukromých certifikátů” na stránce 28
V této části je vysvětleno, jak určit, který typ certifikátu (veřejný nebo soukromý) bude optimální vzhledem k vašim obchodním potřebám.

“Digitální certifikáty pro autentizaci uživatelů” na stránce 31
V této části naleznete informace o možném použití certifikátů jako prostředku pro přísnější autentizaci uživatelů, kteří přistupují k prostředkům serveru iSeries.

Související úlohy

“Vytvoření a provozování lokálního CA” na stránce 38
Toto téma popisuje, jak vytvořit a provozovat lokálního CA k vydávání souktomých certifikátů pro vaše aplikace.

Získání kopie certifikátu soukromého CA:

Tato část vysvětluje, jak získat kopii certifikátu soukromého CA a jak ji nainstalovat na vaše PC tak, abyste mohli autentizovat libovolný serverový certifikát, který tento CA vydá.

Když přistupujete na server, který používá připojení přes SSL (Secure Sockets Layer), předloží server vašemu klientskému softwaru certifikát jako důkaz své totožnosti. Váš klientský software musí předtím, než server vytvoří relaci, potvrdit serverový certifikát. Aby mohl klientský software serverový certifikát potvrdit, musí mít přístup k lokálně uložené kopii certifikátu pro toho vydavatele certifikátů (CA), který serverový certifikát vydal. Pokud server předkládá certifikát od veřejného internetového CA, je možné, že váš prohlížeč nebo jiný klientský software již kopii certifikátu CA má. Pokud ale server předloží certifikát od soukromého lokálního CA, musíte pomocí produktu DCM (Digital Certificate Manager) získat kopii certifikátu CA.

Pomocí produktu DCM lze stáhnout certifikát lokálního CA přímo do vašeho prohlížeče nebo lze certifikát lokálního CA zkopírovat do souboru, aby jiný klientský software k němu mohl přistupovat a používat jej. Jestliže používáte pro

zabezpečené komunikace váš prohlížeč i jiné aplikace, budete zřejmě muset použít obě metody instalace certifikátu lokálního CA. Při použití obou metod proveďte nejprve instalaci certifikátu do svého prohlížeče, a pak jej zkopírujte a vložte do souboru.

Pokud serverová aplikace vyžaduje, abyste provedli svou autentizaci prostřednictvím předložení certifikátu od lokálního CA, musíte předtím, než budete požadovat uživatelský certifikát od lokálního CA, stáhnout certifikát lokálního CA do svého prohlížeče.

Chcete-li pomocí produktu DCM získat kopii certifikátu lokálního CA, postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště vyberte volbu **Instalace certifikátu lokálního CA na počítač** a zobrazí se stránka, pomocí níž můžete stáhnout certifikát lokálního CA do prohlížeče nebo jej uložit do souboru ve vašem systému.
3. Vyberte metodu získání certifikátu lokálního CA.
   a. Vybráním volby **Instalovat certifikát** stáhnete certifikát lokálního CA jako důvěryhodný zdroj do svého prohlížeče. Tím zajistíte, že prohlížeč bude umět vytvářet zabezpečené komunikační relace se servery, které používají certifikát od tohoto CA. Prohlížeč zobrazí sérii oken, která vám pomohou dokončit instalaci.
   b. Vyberte volbu **Kopírovat a vložit certifikát**, čímž zobrazíte stránku, která obsahuje speciálně kódovanou kopii certifikátu CA. Zkopírujte textový objekt zobrazený na této stránce do schránky. Později musíte tuto informaci vložit do souboru. Tento soubor používá obslužný program PC (jako je např. MKKF nebo IKEYMAN) k uložení certifikátů, které používají klientské programy na PC. Předtím, než budou vaše klientské aplikace schopny při autentizaci rozpoznávat a používat certifikát lokálního CA, musíte nakonfigurovat aplikace tak, aby rozpoznávaly certifikát jako důvěryhodný zdroj. Postupujte přitom podle pokynů k používání uvedeného souboru, které poskytují tyto aplikace.
4. Klepněte na **OK** a vrátíte se na domovskou stránku produktu DCM.

Související pojmy

"Správa uživatelských certifikátů" na stránce 40
Pro získání certifikátů s SSL nebo přidružení existujících certifikátů k jejich uživatelským profilům na serveru iSeries můžete využít produkt DCM.

Související úlohy

"Vytvoření a provozování lokálního CA" na stránce 38
Toto téma popisuje, jak vytvořit a provozovat lokálního CA k vydávání souktomých certifikátů pro vaše aplikace.

"Vytvoření uživatelského certifikátu" na stránce 40
Tato část popisuje, jak mohou uživatelé pomocí lokálního CA vydat certifikát pro účely autentizace klienta.

Správa certifikátů od veřejného internetového CA

V této části naleznete informace o správě certifikátů od internetových CA pomocí vytvoření paměti certifikátů.

Po důkladném zvážení vašich požadavků a strategií v oblasti zabezpečení jste se rozhodli, že budete používat certifikáty od veřejného internetového vydavatele certifikátů, jakým je např. VeriSign. Například provozujete veřejné webové stránky a chcete používat SSL (Secure Sockets Layer) pro zabezpečené komunikační relace, abyste zajistili soukromost určitých informačních transakcí. Protože jsou webové stránky přístupné široké veřejnosti, chcete používat certifikáty, které většina webových prohlížečů snadno rozpozná.

Nebo vyvíjíte aplikace pro externí zákazníky a chcete pomocí veřejného certifikátu digitálně podepisovat aplikační balíky. Když aplikační balík obsahuje váš digitální podpis, může si být zákazník jist, že balík pochází z vaší společnosti a že v průběhu přenosu žádná neautorizovaná strana nezměnila kód. Veřejný certifikát chcete používat proto, aby vaši zákazníci mohli jednoduše a levně ověřit digitální podpis na balíku programů. Tento certifikát můžete používat také k ověření podpisu před odesláním balíku zákazníkovi.

Pomocí vedených úloh v produktu DCM (Digital Certificate Manager) můžete centrálně spravovat tyto veřejné certifikáty i aplikace, které je používají k vytváření připojení přes SSL, podepisování objektů nebo ověřování autenticity digitálních podpisů na objektech.

Správa veřejných certifikátů

Jestliže chcete pomocí produktu DCM spravovat certifikáty od veřejného internetového CA, musíte si nejprve vytvořit paměť certifikátů. Paměť certifikátů je zvláštní soubor databáze klíčů, který DCM používá k uložení digitálních certifikátů a jejich přiřazených soukromých klíčů. Pomocí produktu DCM můžete vytvořit a spravovat několik typů pamětí certifikátů podle typu certifikátů, které obsahují.

Typ paměti certifikátů, kterou vytvoříte, a následně i úlohy, jež provádíte při správě certifikátů a aplikací, které certifikáty používají, závisí na tom, jakým způsobem budete chtít certifikáty používat.

Poznámka: Produkt DCM vám také umožní spravovat certifikáty, které získáte od vydavatelů certifikátů, kteří podporují infrastrukturu veřejného klíče pro vydavatele certifikátu X.509 (PKIX).

Další informace o tom, jak pomocí DCM vytvořit příslušné paměti certifikátů a jak spravovat veřejné internetové certifikáty pro vaše aplikace, naleznete v těchto tématech:

Související pojmy

"Používání veřejných certifikátů versus vydávání soukromých certifikátů" na stránce 28
V této části je vysvětleno, jak určit, který typ certifikátu (veřejný nebo soukromý) bude optimální vzhledem k vašim obchodním potřebám.

Související úlohy

"Správa umístění požadavků pro vydavatele certifikátů PKIX" na stránce 68
Vydavatel certifikátů (CA) typu PKIX (Public Key Infrastructure X.509) je takový vydavatel certifikátů, který vydává certifikáty založené na nejnovějších internetových standardech pro implementaci infrastruktury veřejných klíčů X.509.

Správa veřejných internetových certifikátů pro komunikační relace SSL:

Produkt Digital Certificate Manager (DCM) můžete použít pro správu veřejných internetových certifikátů, které vaše aplikace budou využívat k vytváření zabezpečených komunikačních relací prostřednictvím SSL (Secure Sockets Layer).

Jestliže pomocí produktu DCM neprovozujete vlastního lokálního CA, musíte nejprve vytvořit příslušnou paměť certifikátů pro správu veřejných certifikátů používaných pro SSL. Jedná se o paměť certifikátů *SYSTEM. Když vytváříte paměť certifikátů, provede vás produkt DCM procesem vytvoření informací pro požadavek na certifikát, které musíte poskytnout veřejnému CA, abyste certifikát obdrželi.

Chcete-li pomocí produktu DCM spravovat a používat veřejné internetové certifikáty k tomu, aby vaše aplikace mohly vytvářet zabezpečené komunikační relace SSL, postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště produktu DCM vyberte volbu **Vytvoření nové paměti certifikátů**, čímž spustíte úlohu s průvodcem a zobrazí se série formulářů. Pomocí těchto formulářů budete provedeni procesem vytvoření paměti certifikátů a certifikátu, které vaše aplikace budou používat pro relace SSL.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
3. Vyberte ***SYSTEM** jako paměť certifikátů, kterou chcete vytvořit, a klepněte na **Pokračovat**.
4. Vyberte **Ano**, abyste v rámci vytvoření paměti certifikátů *SYSTEM vytvořili i certifikát, a klepněte na **Pokračovat**.
5. Vyberte **VeriSign nebo jiného internetového vydavatele certifikátů (CA)** jako toho, kdo bude podepisovat nové certifikáty, a klepněte na **Pokračovat**, čímž se vám zobrazí formulář na vložení identifikačních informací pro nový certifikát.

   Poznámka: Pokud má váš systém nainstalovaný produkt IBM Cryptographic Coprocessor, umožní vám produkt DCM v další úloze zvolit způsob uložení soukromého klíče tohoto certifikátu. Pokud váš systém

koprocesor nemá, produkt DCM automaticky uloží soukromý klíč do paměti certifikátů *SYSTEM. Potřebujete-li poradit při volbě způsobu uložení soukromého klíče, podívejte se do online nápovědy v produktu DCM.

6. Vyplňte formulář a klepněte na **Pokračovat**. Zobrazí se potvrzující stránka. Tato potvrzující stránka zobrazuje údaje žádosti o certifikát, které musíte poskytnout veřejnému vydavateli certifikátů (CA), jenž bude certifikát vydávat. Data tohoto tzv. požadavku na podepisovací certifikát (Certificate Signing Request, CSR) zahrnují veřejný klíč a další informace, které jste uvedli pro nový certifikát.
7. Pečlivě zkopírujte a vložte data CSR do formuláře žádosti o certifikát nebo do zvláštního souboru, který veřejný CA požaduje při žádostech o certifikát. Musíte použít veškerá data CSR, včetně řádek Begin a End New Certificate Request. Jakmile tuto stránku opustíte, budou data ztracena a nebude možné je obnovit. Pošlete formulář žádosti nebo soubor vydavateli CA, kterého jste si zvolili pro vydání a podepsání vašeho certifikátu.

   Poznámka: Než budete moci pokračovat, musíte počkat, až vám CA vrátí podepsaný dokončený certifikát.

   Chcete-li používat certifikát v kombinaci s HTTP serverem, musíte ještě před zahájením práce s produktem DCM vytvořit a nakonfigurovat váš webový server. Když konfigurujete webový server pro použití SSL, vygeneruje se pro server určité ID aplikace. Toto ID aplikace si musíte poznamenat, abyste mohli pomocí produktu DCM specifikovat, který certifikát bude tato aplikace používat pro SSL.

   Server neukončujte ani nerestartujte, dokud mu pomocí produktu DCM nepřiřadíte podepsaný dokončený certifikát. Pokud ukončíte a restartujete instanci *ADMIN webového serveru předtím, než mu přiřadíte certifikát, server se nerestartuje a nebudete moci prostřednictvím produktu DCM serverový certifikát přiřadit.
8. Když vám veřejný CA zašle zpět podepsaný certifikát, spusťte produkt DCM.
9. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***SYSTEM**.
10. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte heslo, které jste pro danou paměť certifikátů uvedli, když jste ji vytvářeli, a klepněte na **Pokračovat**.
11. Když se obnoví navigační lišta, vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
12. Ze seznamu úloh vyberte volbu **Import certifikátů**, čímž zahájíte proces importu podepsaného certifikátu do paměti certifikátů *SYSTEM. Když dokončíte import certifikátu, můžete specifikovat aplikace, které tento certifikát musí používat při komunikaci SSL.
13. V navigační liště vyberte volbu **Správa aplikací**. Zobrazí se seznam úloh.
14. Ze seznamu úloh vyberte volbu **Aktualizace přiřazení certifikátu**. Zobrazí se seznam aplikací využívajících SSL, kterým můžete přiřadit certifikát.
15. Vyberte ze seznamu aplikaci a klepněte na **Aktualizace přiřazení certifikátu**.
16. Vyberte certifikát, který jste importovali, a klepněte na **Přiřadit nový certifikát**. Produkt DCM zobrazí zprávu, která bude potvrzovat váš výběr certifikátu pro danou aplikaci.

    Poznámka: Některé aplikace využívající SSL podporují autentizaci klientů založenou na certifikátech. Pokud chcete, aby aplikace s touto podporou byla schopna autentizovat certifikáty předtím, než poskytne přístup k prostředkům, musíte pro tuto aplikaci definovat seznam důvěryhodných CA. Tím zajistíte, že aplikace bude potvrzovat pouze certifikáty těch CA, které v seznamu uvedete jako důvěryhodné. Pokud uživatel nebo klientská aplikace předloží certifikát od CA, který není uveden jako důvěryhodný v seznamu důvěryhodných CA, aplikace certifikát nepřijme za základ pro platnou autentizaci.

Po dokončení této vedené úlohy budete mít hotovo vše potřebné k tomu, abyste mohli u vašich aplikací nakonfigurovat SSL pro zabezpečenou komunikaci. Předtím, než mohou uživatelé přistupovat k aplikacím prostřednictvím relace SSL, musí mít kopii certifikátu CA od toho CA, který vydal serverový certifikát. Jestliže váš certifikát pochází od známého internetového CA, klientský software vašich uživatelů bude pravděpodobně mít kopii potřebného certifikátu CA. Pokud uživatelé potřebují certifikát CA získat, musí navštívit webové stránky daného CA a řídit se instrukcemi, které stránky poskytují.

Správa veřejných internetových certifikátů k podepisování objektů:

Pomocí produktu DCM (Digital Certificate Manager) můžete spravovat veřejné internetové certifikáty pro digitální podepisování objektů.

Jestliže pomocí produktu DCM neprovozujete vlastního lokálního CA, musíte nejprve vytvořit příslušnou paměť certifikátů pro správu veřejných certifikátů používaných k podepisování objektů. Jedná se o paměť certifikátů *OBJECTSIGNING. Když vytvoříte paměť certifikátů, provede vás produkt DCM procesem vytvoření informací pro požadavek na certifikát, které musíte poskytnout veřejnému internetovému CA, abyste certifikát obdrželi.

Chcete-li pomocí certifikátu podepisovat objekty, musíte také definovat ID aplikace. Toto ID aplikace určuje, jaká oprávnění musí mít uživatel, který bude podepisovat objekty pomocí určitého certifikátu, a rozšiřuje tak řízení přístupu k těm, které produkt DCM poskytuje, o další úroveň. Definice aplikace obvykle vyžaduje, aby uživatel, který má mít povolení používat certifikát k podepisování objektů, měl zvláštní oprávnění *ALLOBJ. (Oprávnění, které ID aplikace vyžaduje, lze však změnit pomocí produktu iSeries Navigator.)

Chcete-li pomocí produktu DCM spravovat a používat veřejné internetové certifikáty pro podepisování objektů, postupujte takto:

1. Spusťte produkt DCM.
2. V levé navigační liště produktu DCM vyberte volbu **Vytvoření nové paměti certifikátů**, čímž spustíte úlohu s průvodcem a zobrazí se série formulářů. Pomocí těchto formulářů budete provedeni procesem vytvoření paměti certifikátů a certifikátu, který můžete používat k podepisování objektů.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
3. Vyberte ***OBJECTSIGNING** jako paměť certifikátů, kterou chcete vytvořit, a klepněte na **Pokračovat**.
4. Vyberte **Ano**, abyste v rámci vytvoření paměti certifikátů vytvořili i certifikát, a klepněte na **Pokračovat**.
5. Vyberte **VeriSign nebo jiného internetového vydavatele certifikátů (CA)** jako toho, kdo bude podepisovat nové certifikáty, a klepněte na **Pokračovat**. Zobrazí se vám formulář na vložení identifikačních informací pro nový certifikát.
6. Vyplňte formulář a klepněte na **Pokračovat**. Zobrazí se potvrzující stránka. Tato potvrzující stránka zobrazuje údaje žádosti o certifikát, které musíte poskytnout veřejnému vydavateli certifikátů (CA), jenž bude certifikát vydávat. Data tohoto tzv. požadavku na podepisovací certifikát (Certificate Signing Request, CSR) zahrnují veřejný klíč a další informace, které jste uvedli pro nový certifikát.
7. Pečlivě zkopírujte a vložte data CSR do formuláře žádosti o certifikát nebo do zvláštního souboru, který veřejný CA požaduje při žádostech o certifikát. Musíte použít veškerá data CSR, včetně řádek Begin a End New Certificate Request. Jakmile tuto stránku opustíte, budou data ztracena a nebude možné je obnovit. Pošlete formulář žádosti nebo soubor vydavateli CA, kterého jste si zvolili pro vydání a podepsání vašeho certifikátu.

   Poznámka: Než budete moci pokračovat, musíte počkat, až vám CA vrátí podepsaný dokončený certifikát.
8. Když vám veřejný CA zašle zpět podepsaný certifikát, spusťte produkt DCM.
9. V levé navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***OBJECTSIGNING**.
10. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte heslo, které jste pro danou paměť certifikátů uvedli, když jste ji vytvářeli, a klepněte na **Pokračovat**.
11. V navigační liště vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
12. Ze seznamu úloh vyberte volbu **Import certifikátů**, čímž zahájíte proces importu podepsaného certifikátu do paměti certifikátů *OBJECTSIGNING. Když dokončíte import certifikátu, můžete vytvořit definici aplikace tak, aby používala certifikát k podepisování objektů.
13. Když se obnoví levá navigační lišta, vyberte volbu **Správa aplikací**. Zobrazí se seznam úloh.
14. Ze seznamu úloh vyberte volbu **Přidání aplikace**, čímž zahájíte proces vytvoření definice aplikace pro podepisování objektů tak, aby používala certifikát k podepisování objektů.

15. Vyplňte formulář, abyste nadefinovali aplikaci pro podepisování objektů, a klepněte na **Přidat**. Tato definice aplikace nepopisuje žádnou skutečnou aplikaci, ale popisuje spíše typ objektů, které hodláte pomocí určitého certifikátu podepisovat. Chcete-li poradit s vyplněním formuláře, použijte online nápovědu.
16. Klepněte na **OK**, abyste potvrdili zprávu o definici aplikace. Zobrazí se seznam úloh Správa aplikací.
17. Ze seznamu úloh vyberte volbu **Aktualizace přiřazení certifikátu** a klepněte na **Pokračovat**, aby se zobrazil seznam ID aplikací pro podepisování objektů, kterým můžete certifikát přiřadit.
18. Vyberte ze seznamu ID vaší aplikace a klepněte na **Aktualizace přiřazení certifikátu**.
19. Vyberte certifikát, který jste importovali, a klepněte na **Přiřadit nový certifikát**.

Po dokončení těchto úloh máte připraveno vše potřebné k tomu, abyste mohli zahájit podepisování objektů a zajišťovat tak jejich integritu.

Pokud distribuujete podepsané objekty, tak ti, kteří objekty dostávají a chtějí si ověřit totožnost odesílatele a to, že data jsou nezměněna, musí pomocí verze produktu DCM V5R1 nebo novější ověřit podpis na objektech. Aby mohl příjemce ověřit podpis, musí mít kopii certifikátu pro ověřování podpisů. Jako součást dodávky podepsaných objektů musíte poskytnout kopii tohoto certifikátu.

Příjemce musí mít také kopii certifikátu CA pro toho CA, který certifikát, jenž jste použili k podepsání objektu, vydal. Jestliže jste podepsali objekty pomocí certifikátu od nějakého známého internetového CA, pak by uživatelova verze produktu DCM již kopii potřebného certifikátu CA mohla mít. Pokud si však nejste jisti, zda příjemce kopii tohoto certifikátu má, můžete kopii certifikátu CA poskytnout příjemci spolu s podepsanými objekty. Musíte například poskytnout kopii certifikátu lokálního CA, pokud jste podepsali objekty pomocí certifikátu od soukromého lokálního CA. Z bezpečnostních důvodů musíte zaslat certifikát CA samostatně, nebo dát certifikát CA k dispozici veřejně na vyžádání těch, kteří jej potřebují.

Související pojmy

“Digitální certifikáty pro podepisování objektů” na stránce 34
Tato část vysvětluje, jak lze certifikáty používat k zajištění integrity objektů nebo k ověření digitálního podpisu na objektu za účelem ověření jeho pravosti.

Správa certifikátů pro ověřování podpisů na objektech:

Pomocí produktu DCM (Digital Certificate Manager) můžete spravovat certifikáty pro ověřování podpisů, které používáte při ověření platnosti digitálního podpisu na objektech.

Chcete-li podepsat objekt, musíte pomocí soukromého klíče certifikátu vytvořit podpis. Když někomu posíláte podepsaný objekt, musíte poslat také kopii certifikátu, který objekt podepsal. To provedete, když pomocí produktu DCM exportujete certifikát pro podepisování objektů (bez soukromého klíče certifikátu) jako certifikát pro ověřování podpisů. Certifikát pro ověřování podpisů lze exportovat do souboru, který pak můžete distribuovat ostatním. Anebo, pokud chcete ověřovat podpisy, které budete vytvářete, můžete exportovat certifikát pro ověřování podpisů do paměti certifikátů *SIGNATUREVERIFICATION.

Chcete-li ověřit platnost podpisu na objektu, musíte mít kopii certifikátu, který objekt podepsal. Pomocí veřejného klíče podepisujícího certifikátu, který je součástí certifikátu, prozkoumáte a ověříte podpis, který byl vytvořen odpovídajícím soukromým klíčem. Takže předtím, než můžete ověřit podpis na objektu, musíte získat kopii podepisujícího certifikátu od toho, kdo vám podepsaný objekt poskytl.

Musíte mít také kopii certifikátu CA pro toho CA, jenž vydal certifikát, kterým je objekt podepsaný. Pomocí certifikátu CA si ověříte autenticitu certifikátu, který podepsal objekt. Produkt DCM obsahuje kopie certifikátů CA pro většinu známých CA. Pokud byl ale objekt podepsán certifikátem od jiného veřejného CA nebo od nějakého soukromého lokálního CA, musíte předtím, než budete moci ověřit podpis objektu, získat kopii certifikátu CA.

Chcete-li pomocí produktu DCM ověřovat podpisy objektů, musíte nejprve vytvořit příslušnou paměť certifikátů pro správu potřebných certifikátů pro ověřování podpisů. Jedná se o paměť certifikátů *SIGNATUREVERIFICATION. Když tuto paměť certifikátů vytvoříte, produkt DCM ji automaticky zaplní kopiemi certifikátů CA většiny známých veřejných CA.

Poznámka: Pokud chcete ověřovat podpisy, které vytvoříte pomocí vlastních certifikátů pro podepisování objektů, musíte vytvořit paměť certifikátů *SIGNATUREVERIFICATION a zkopírovat do ní certifikáty z paměti *OBJECTSIGNING. Toto platí i tehdy, pokud hodláte provádět ověřování podpisů v rámci paměti certifikátů *OBJECTSIGNING.

Chcete-li pomocí produktu DCM spravovat certifikáty pro ověřování podpisů, postupujte takto:

1. Spusťte produkt DCM.
2. V levé navigační liště produktu DCM vyberte volbu **Vytvoření nové paměti certifikátů**, čímž spustíte úlohu s průvodcem a zobrazí se série formulářů.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
3. Vyberte ***SIGNATUREVERIFICATION** jako paměť certifikátů, kterou chcete vytvořit, a klepněte na **Pokračovat**.

   Poznámka: Pokud již existuje paměť certifikátů *OBJECTSIGNING, produkt DCM vás v tomto místě vyzve, abyste uvedli, zda má zkopírovat certifikáty pro podepisování objektů do této nové paměti certifikátů jako certifikáty pro ověřování podpisů. Chcete-li používat vaše existující certifikáty pro podepisování objektů také k ověřování podpisů, vyberte **Ano** a klepněte na **Pokračovat**. Abyste mohli certifikáty z paměti certifikátů *OBJECTSIGNING kopírovat, musíte znát heslo k této paměti.
4. Uveďte heslo pro novou paměť certifikátů a klepněte na **Pokračovat**, abyste vytvořili paměť certifikátů. Zobrazí se potvrzující stránka, která oznamuje, že paměť certifikátů byla úspěšně vytvořena. Nyní můžete pomocí této paměti certifikátů spravovat a používat certifikáty k ověřování podpisů objektů.

   Poznámka: Jestliže jste tuto paměť vytvořili za účelem ověřování podpisů na objektech, které budete podepisovat vy sami, můžete nyní skončit. Když pak budete vytvářet nové certifikáty pro podepisování objektů, musíte je exportovat z paměti certifikátů *OBJECTSIGNING do této paměti certifikátů. Pokud je nevyexportujete, nebudete schopni ověřovat podpisy, které jste pomocí těchto certifikátů vytvořili. Jestliže jste tuto paměť vytvořili za účelem ověřování podpisů na objektech, které budete dostávat z jiných zdrojů, musíte podle tohoto postupu pokračovat dál, abyste byli schopni do této paměti certifikátů importovat certifikáty, které budete potřebovat.
5. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***SIGNATUREVERIFICATION**.
6. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte heslo, které jste pro danou paměť certifikátů uvedli, když jste ji vytvářeli, a klepněte na **Pokračovat**.
7. Když se obnoví navigační lišta, vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
8. Ze seznamu úloh vyberte volbu **Import certifikátů**. Tato vedená úloha vás provede procesem importu certifikátů, které potřebujete mít v paměti certifikátů, abyste mohli ověřovat podpis na objektu, jenž obdržíte.
9. Vyberte typ certifikátu, který chcete importovat. Vyberte **Ověřování podpisu**, abyste importovali certifikát, který jste obdrželi s podepsanými objekty, a dokončete úlohu.

   Poznámka: Pokud paměť certifikátů ještě neobsahuje kopii certifikátu CA od toho CA, který vydal certifikát pro ověřování podpisů, musíte *nejprve* importovat tento certifikát CA. Jestliže nenaimportujete certifikát CA předtím, než importujete certifikát pro ověřování podpisů, dostanete se pravděpodobně do chybového stavu.

Nyní můžete tyto certifikáty používat při ověřování podpisů na objektech.

Související pojmy

“Digitální certifikáty pro podepisování objektů” na stránce 34
Tato část vysvětluje, jak lze certifikáty používat k zajištění integrity objektů nebo k ověření digitálního podpisu na objektu za účelem ověření jeho pravosti.

Související úlohy

"Ověřování podpisu objektů" na stránce 71
Pomocí produktu DCM (Digital Certificate Manager) lze ověřovat autenticitu digitálních podpisů na objektech. Když ověříte podpis, budete mít jistotu, že data v objektu nebyla změněna poté, co vlastník objektu objekt podepsal.

Obnovení existujícího certifikátu

Proces obnovení certifikátu, který používá produkt DCM, se liší dle typu vydavatele certifikátů (CA), který příslušný certifikát vydal.

Můžete obnovit certifikát s lokálním CA nebo internetovým CA.

Obnovení certifikátu lokálního CA

Pokud použijete lokálního CA k podepsání obnoveného certifikátu, použije produkt DCM poskytnuté informace k vytvoření nového certifikátu v aktuální paměti certifikátů a dřívější certifikát zachová.

Při obnovení certifikátu od lokálního CA postupujte takto:

1. V navigační liště klepněte na **Výběr paměti certifikátů**, poté vyberte paměť certifikátů, ve které se nachází certifikát, který chcete obnovit.
2. V navigační liště vyberte volbu **Správa certifikátů**.
3. V navigační liště vyberte volbu **Obnovit certifikát**.
4. Vyberte certifikát, který chcete obnovit, a klepněte na **Obnovit**.
5. Vyberte **Lokální vydavatel certifikátů (CA)** a klepněte na **Pokračovat**.
6. Vyplňte formulář identifikace certifikátu. Musíte změnit pole **Návěští nového certifikátu**, ale všechny ostatní pole mohou zůstat stejné.
7. K dokončení obnovy certifikátu vyberte všechny aplikace ve kterých chcete obnovený certifikát použít a klepněte na **Pokračovat**.

   Poznámka: Aplikaci, ve které používáte certifikát, nemusíte vybrat.

Obnovení certifikátu internetového CA

Pokud k vydání certifikátu používáte známého internetového CA, můžete obnovu certifikátu zařídit dvěma způsoby.

Certifikát můžete obnovit přímo s internetovým CA a poté jej můžete importovat ze souboru, který získáte od podepisujícího CA. Nebo pomocí produktu DCM vytvoříte novou dvojici soukromého a veřejného klíče a CSR (Certificate Signing Request) a tyto informace zašlete internetovému CA za účelem získání nového certifikátu. Po obdržení certifikátu od CA můžete dokončit proces obnovení.

Import a obnovení certifikátu získaného přímo od internetového CA:

Chcete-li importovat a obnovit certifikát, který jste získali přímo od internetového CA, postupujte takto:

1. V navigační liště klepněte na **Výběr paměti certifikátů**, poté vyberte paměť certifikátů, ve které se nachází certifikát, který chcete obnovit.

   Poznámka: Klepněte na "?" na kterémkoliv panelu, pokud máte další dotazy ohledně dokončení panelu.
2. V navigační liště vyberte volbu **Správa certifikátů**.
3. V navigační liště klepněte na **Obnovit certifikát**.
4. Vyberte certifikát, který chcete obnovit, a klepněte na **Obnovit**.
5. Vyberte **VeriSign** nebo jiného **internetového CA** a klepněte na **Pokračovat**.
6. Vyberte **Ne - Import obnoveného podepsaného certifikátu z existujícího souboru**.
7. Pro import certifikátu dokončete vedenou úlohu. Pokud si vyberete obnovu certifikátu prostřednictvím vydávajícího CA, pak vám CA obnovený certifikát vrátí v souboru. Při importu certifikátu se ujistěte, že jste uvedli

správnou absolutní cestu na které je certifikát na serveru uložen. Soubor, který obsahuje obnovený certifikát, může být uložen v jakémkoliv adresáři integrovaného systémuu souborů.

8. Klepnutím na **OK** úlohu dokončíte.

Obnovení certifikátu pomocí vytvoření dvojice soukromého a veřejného klíče a CSR:

Chcete-li obnovit certifikát prostřednictvím lokálního CA pomocí vytvoření nové dvojice soukromého a veřejného klíče a CSR, postupujte takto:

1. V navigační liště klepněte na **Výběr paměti certifikátů**, poté vyberte paměť certifikátů, ve které se nachází certifikát, který chcete obnovit.

   Poznámka: Klepněte na "?" na kterémkoliv panelu, pokud máte další dotazy ohledně dokončení panelu.

2. V navigační liště vyberte volbu **Správa certifikátů**.
3. V navigační liště klepněte na **Obnovit certifikát**
4. Vyberte certifikát, který chcete obnovit, a klepněte na **Obnovit**.
5. Vyberte **VeriSign** nebo jiného **internetového CA** a klepněte na **Pokračovat**.
6. Klepněte na **Ano - Vytvoření nové dvojice klíčů pro tento certifikát a klepněte na Pokračovat**.
7. Vyplňte formulář identifikace certifikátu. Musíte změnit pole Návěští nového certifikátu, ale všechny ostatní pole mohou zůstat stejné. Poznámka: Klepněte na "?" na kterémkoliv panelu, pokud máte další dotazy ohledně dokončení panelu.
8. Klepnutím na **OK** úlohu dokončíte.

Import certifikátu

Tyto informace popisují, jak lze použít produkt DCM k importu certifikátů, které jsou umístěny v souborech na vašem serveru.

Místo toho, abyste znovu vytvářeli certifikát na aktuálním serveru, můžete použít import certifikátu z jiného serveru. Například na serveru iSeries A používáte lokálního CA k vytvoření certifikátu pro vaši webovou aplikaci pro maloobchod k zahájení připojení SSL. Váš obchod se v poslední době rozvíjel a nainstalovali jste nový iSeries server (iSeries B), aby se stal hostitelem pro další instance této velmi vytížené obchodní aplikace. Chcete, aby všechny instance aplikace pro maloobchod používaly identický certifikát pomocí kterého by bylo možné je identifikovat a zahajovat SSL spojení. Proto se můžete rozhodnout, že raději naimportujete jak certifikáty lokálního CA, tak certifikáty serveru, ze serveru iSeries A na server iSeries B, než abyste použili lokálního CA na serveru iSeries A k vytvoření nového, odlišného certifikátu pro server iSeries B.

Chcete-li pro import certifikátu použít produkt DCM, postupujte takto:

1. V navigačním podokně na levé straně, klepněte na volbu **Vybrat paměť certifikátů** a vyberte paměť certifikátů, do které chcete certifikát importovat. Paměť certifikátů, do které certifikát importujete, musí obsahovat certifikáty stejného typu jako certifikát, který jste exportovali v jiném systému. Pokud například importujete certifikát serveru, pak jej importujte do paměti certifikátů, která obsahuje certifikáty pro server, jako například *SYSTEM nebo jiná systémová paměť certifikátů.
2. V navigační liště vyberte volbu **Správa certifikátů**.
3. V navigační liště vyberte volbu **Import certifikátu**.
4. Vyberte typ certifikátu, který chcete importovat a klepněte na **Pokračovat**. Certifikát, který importujete, musí být stejného typu jako certifikát, který jste exportovali. Pokud jste například exportovali certifikát serveru, vyberte při importu certifikát serveru.

   Poznámka: Pokud produkt DCM exportuje certifikát ve formátu pkcs12, pak vydání CA je zahrnuto v řetězci exportovaného certifikátu a je tedy importováno automaticky, pokud je certifikát sám pomocí produktu DCM importován do paměť certifikátů. Pokud však certifikát není exportován ve formátu pkcs12 a nemáte certifikát CA v paměti certifikátů do které importujete, pak musíte importovat vydání certifikátu CA předtím, než můžete importovat certifikát.

5. Pro import certifikátu dokončete vedenou úlohu. Při importu certifikátu se ujistěte, že jste uvedli správnou absolutní cestu na které je certifikát na serveru uložen.

Správa produktu DCM

Tato část popisuje, jak používat produkt DCM při správě vašich certifikátů a aplikací, které certifikáty používají. Dovíte se také, jak digitálně podepisovat objekty a jak vytvořit a provozovat svého vlastního vydavatele certifikátů (CA).

Poté, co jste nakonfigurovali produkt DCM (Digital Certificate Manager), budete v průběhu doby potřebovat provést řadu úloh týkajících se správy certifikátů. Další informace o použití produktu DCM při správě vašich digitálních certifikátů naleznete v těchto tématech:

Použití lokálního CA k vydávání certifikátů pro jiné servery iSeries

V této části najdete informace o tom, jak pomocí soukromého lokálního CA vydávat certifikáty, které se budou používat na jiných serverech iSeries.

Předpokládejme, že již používáte soukromého lokálního vydavatele certifikátů (CA) na některém serveru v rámci vaší sítě. Nyní chcete rozšířit použití tohoto CA i na další server v síti. Chcete například, aby váš současný lokální CA vydával serverový nebo klientský certifikát pro aplikaci v jiném systému, který by tato aplikace použila při komunikační relaci SSL. Nebo chcete použít certifikáty od vašeho lokálního CA v jednom systému k podepsání objektů, které máte uloženy na jiném serveru.

Tyto záměry lze splnit pomocí produktu DCM (Digital Certificate Manager). Některé z úloh budete provádět na serveru, kde provozujete lokálního CA, jiné budete provádět na sekundárním serveru, který je hostitelským systémem aplikací pro něž chcete certifikáty vydávat. Tento sekundární systém se nazývá cílový systém. Úlohy, které musíte provádět v cílovém systému, závisí na úrovni vydání tohoto systému.

Poznámka: Pokud systém, ve kterém provozujete lokálního CA, používá produkt Cryptographic Access Provider se silnějším šifrováním, než má cílový systém, pak je možné, že se vyskytnou problémy. Ve verzích operačního systému OS/400 V5R2 a OS/400 V5R3 je k dispozici pouze produkt Cryptographic Access Provider 5722–AC3, což je nejsilnější dostupný produkt. V dřívějších vydáních však bylo možno instalovat jiné, slabší produkty Cryptographic Access Provider (5722–AC1 nebo 5722–AC2), které poskytovaly nižší úroveň funkcí šifrování. Když exportujete certifikát (s jeho soukromým klíčem), systém soubor zašifruje, aby chránil jeho obsah. Pokud systém používá silnější šifrovací produkt než cílový systém, nemůže cílový systém v průběhu procesu importu soubor dešifrovat. V důsledku toho se nemusí import zdařit, nebo certifikát nemusí být použitelný pro ustanovení relace SSL. To platí dokonce i tehdy, když použijete pro nový certifikát takovou velikost klíče, která odpovídá použití pro šifrovací produkt cílového systému.

Pomocí lokálního CA můžete vydávat certifikáty jiným systémům, které pak můžete použít k podepisování objektů nebo které mohou aplikace tohoto systému používat při vytváření relací SSL. Když pomocí lokálního CA vytvoříte certifikát pro použití v jiném systému, soubory vytvořené produktem DCM budou obsahovat kopii certifikátu CA tohoto lokálního CA i kopie certifikátů CA mnoha veřejných internetových CA.

Úlohy, které musíte provést v produktu DCM, se mírně liší podle typu certifikátu, který lokální CA vydává, a podle úrovně vydání a podmínek cílového systému.

Vydávání soukromých certifikátů pro použití na jiném serveru než iSeries

Chcete-li pomocí lokálního CA vydávat certifikáty, které se budou používat v jiném systému, proveďte v systému, který je hostitelem lokálního CA, následující:

1. Spuštění produktu DCM
2. V navigační liště vyberte volbu **Vytvoření certifikátu**. Zobrazí se seznam typů certifikátů, které můžete pomocí lokálního CA vytvořit.

Poznámka: Před vykonáním této úlohy nemusíte otevírat určitou paměť certifikátů. Tyto pokyny předpokládají, že buď nepracujete s konkrétní pamětí certifikátů, anebo že pracujete v rámci paměti certifikátů Lokální vydavatel certifikátů (CA). Než můžete provést tyto úlohy, musí v daném systému existovat lokální CA. Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.

3. Vyberte požadovaný typ certifikátu, který má lokální CA vydat, a klepněte na **Pokračovat**, čímž spustíte úlohu s průvodcem a zobrazí se série formulářů.
4. Vyberte vytvořit **serverový nebo klientský certifikát pro jiný server iSeries** (pro relace SSL), nebo **certifikát pro podepisování objektů pro jiný server iSeries** (pro použití v jiném systému).

   Poznámka: Pokud vytváříte certifikát pro podepisování objektů, který se bude používat v jiném systému, musí tento systém provozovat verzi OS/400 V5R1 nebo vyšší verzi, aby mohl certifikát používat. Protože cílový systém musí mít verzi OS/400 V5R1 nebo vyšší, nevyzve vás produkt DCM v lokálním hostitelském systému, abyste u nového certifikátu pro podepisování objektů vybrali formát cílového vydání.
5. Vyplňte formulář a klepněte na **Pokračovat**. Zobrazí se potvrzující stránka.

   Poznámka: Jestliže v cílovém systému existuje paměť certifikátů *OBJECTSIGNING nebo *SYSTEM, ujistěte se, že zadáváte jedinečné návěští certifikátu a jedinečné jméno souboru pro certifikát. Zadání jedinečného návěští certifikátu a jména souboru je důležité proto, abyste mohli snadno importovat certifikát do existující paměti certifikátů v cílovém systému. Tato potvrzující stránka zobrazí jména souborů, které produkt DCM vytvořil a které budete přenášet do cílového systému. Produkt DCM tyto soubory vytváří na základě úrovně vydání cílového systému, kterou jste zadali. Produkt DCM do těchto souborů automaticky vkládá kopii certifikátu lokálního CA.

   Produkt DCM vytváří nový certifikát ve své vlastní paměti certifikátů a vygeneruje dva soubory, které musíte přenést: soubor paměti certifikátů (přípona .KDB) a soubor požadavku na certifikát (přípona .RDB).
6. Prostřednictvím binárního protokolu FTP (File Transfer Protocol) nebo jiné metody proveďte přenos souborů do cílového systému.

Související pojmy

“Pokyny pro zálohování a obnovu dat produktu DCM” na stránce 26
Toto téma obsahuje informace o tom, jak lze zajistit, aby byla důležitá data produktu DCM přidána do plánu zálohování a obnovy vašeho systému.

“Používání veřejných certifikátů versus vydávání soukromých certifikátů” na stránce 28
V této části je vysvětleno, jak určit, který typ certifikátu (veřejný nebo soukromý) bude optimální vzhledem k vašim obchodním potřebám.

Související úlohy

“Vytvoření a provozování lokálního CA” na stránce 38
Toto téma popisuje, jak vytvořit a provozovat lokálního CA k vydávání souktomých certifikátů pro vaše aplikace.

Použití soukromého certifikátu pro SSL

Správu certifikátů, které vaše aplikace používají pro relace SSL, provádíte z paměti certifikátů *SYSTEM v produktu DCM (Digital Certificate Manager). Pokud jste produkt DCM v cílovém systému nikdy nepoužívali ke správě certifikátů pro SSL, pak tato paměť certifikátů v cílovém systému neexistuje.

Úlohy týkající se použití přenesených souborů paměti certifikátů, které jste vytvořili v hostitelském systému lokálního vydavatele certifikátů (CA), se liší podle toho, zda paměť certifikátů *SYSTEM existuje, či nikoliv. Pokud paměť certifikátů *SYSTEM neexistuje, můžete přenesené soubory certifikátů použít jako prostředek pro vytvoření paměti certifikátů *SYSTEM. Pokud paměť certifikátů *SYSTEM v cílovém systému neexistuje, pak můžete použít přenesené soubory jako paměť certifikátů v jiném systému nebo importovat přenesené soubory do existující paměti certifikátů *SYSTEM.

Paměť certifikátů *SYSTEM neexistuje:

Pokud paměť certifikátů *SYSTEM v systému, ve kterém chcete používat přenesené soubory paměti certifikátů, neexistuje, pak můžete použít přenesené soubory certifikátů jako paměť certifikátů *SYSTEM. Chcete-li vytvořit paměť certifikátů *SYSTEM a použít soubory certifikátů v cílovém systému, postupujte takto:

1. Ujistěte se, že soubory paměti certifikátů (dva soubory: jeden s příponou .KDB a jeden s příponou .RDB), které jste vytvořili v hostitelském systému lokálního CA, jsou v adresáři /QIBM/USERDATA/ICSS/CERT/SERVER .
2. Jakmile jsou přenesené soubory certifikátů v adresáři /QIBM/USERDATA/ICSS/CERT/SERVER, přejmenujte tyto soubory na soubory DEFAULT.KDB a DEFAULT.RDB. Přejmenováním těchto souborů v příslušném adresáři vytvoříte komponenty, které obsahují paměť certifikátů *SYSTEM pro cílový systém. Soubory paměti certifikátů již obsahují kopie certifikátů pro řadu veřejných internetových CA. Produkt DCM tyto kopie a rovněž i kopii certifikátu lokálního CA do souborů paměti certifikátů přidal, když jste tyto soubory vytvářeli.

   Upozornění: Jestliže cílový systém již soubory DEFAULT.KDB a DEFAULT.RDB v adresáři /QIBM/USERDATA/ICSS/CERT/SERVER obsahuje, pak v cílovém systému paměť certifikátů *SYSTEM existuje. Nesmíte tedy přejmenovávat přenesené soubory tak, jak je výše popsáno. Přepsání předvolených souborů způsobí problémy při používání produktu DCM, přenesené paměti certifikátů a jejího obsahu. Namísto toho musíte zajistit, aby měly soubory jedinečné jméno, a použít přenesenou paměť certifikátů jako **Jinou systémovou paměť certifikátů**. Použijete-li však soubory jako Jinou systémovou paměť certifikátů, nemůžete pomocí produktu DCM specifikovat, které aplikace budou certifikát používat.
3. Spusťte produkt DCM.Nyní musíte změnit heslo pro paměť certifikátů *SYSTEM, kterou jste vytvořili přejmenováním přenesených souborů. Při změně hesla produkt DCM uloží nové heslo tak, že budete moci v této paměti používat všechny funkce produktu DCM pro správu certifikátů.
4. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***SYSTEM**.
5. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte heslo, které jste pro tuto paměť certifikátů uvedli v *hostitelském* systému, když jste vytvářeli certifikát pro cílový systém, a klepněte na **Pokračovat**.
6. V navigační liště vyberte volbu **Správa paměti certifikátů** a ze seznamu úloh pak vyberte **Změna hesla**. Vyplňte formulář pro změnu hesla k této paměti certifikátů. Když změníte heslo, musíte paměť certifikátů znovu otevřít, abyste mohli pracovat s certifikáty, které v paměti jsou. Nyní můžete specifikovat, které aplikace budou certifikát pro relace SSL používat.
7. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***SYSTEM**.
8. Když se zobrazí stránka **Paměť certifikátů a heslo**, zadejte nové heslo a klepněte na **Pokračovat**.
9. Když se obnoví navigační lišta, vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
10. Ze seznamu úloh vyberte volbu **Přiřazení certifikátu**. Zobrazí se seznam certifikátů v aktuální paměti certifikátů.
11. Vyberte certifikát, který jste vytvořili v *hostitelském* systému, a klepněte na **Přiřadit k aplikacím**. Zobrazí se seznam aplikací využívajících SSL, kterým můžete přiřadit tento certifikát.
12. Vyberte aplikace, které budou používat certifikát pro relace SSL, a klepněte na **Pokračovat**. Produkt DCM zobrazí zprávu, která bude potvrzovat výběr certifikátu pro určité aplikace.

    Poznámka: Některé aplikace využívající SSL podporují autentizaci klientů založenou na certifikátech. Aplikace s touto podporou musí být schopna autentizovat certifikáty předtím, než poskytne přístup k prostředkům. Pro tuto aplikaci tudíž musíte definovat seznam důvěryhodných CA. Tím zajistíte, že aplikace bude potvrzovat pouze certifikáty těch CA, které v seznamu uvedete jako důvěryhodné. Pokud uživatelé nebo klientská aplikace předloží certifikát od CA, který není uveden jako důvěryhodný v seznamu důvěryhodných CA, aplikace certifikát nepřijme za základ pro platnou autentizaci.

Po provedení výše uvedených úloh budou moci aplikace v cílovém systému používat certifikát vydaný lokálním CA v jiném systému. Avšak předtím, než pro tyto aplikace začnete používat SSL, musíte je nakonfigurovat tak, aby používaly SSL.

Dříve, než bude uživatel moci přistupovat k vybraným aplikacím přes SSL, musí pomocí produktu DCM získat kopii certifikátu lokálního CA z hostitelského systému. Certifikát lokálního CA se musí zkopírovat do souboru na počítači uživatele nebo stáhnout do prohlížeče uživatele, což závisí na požadavcích aplikace, která používá SSL.

Paměť certifikátů *SYSTEM existuje — použití souborů jako jiný systémový certifikát:

Jestliže cílový systém již paměť certifikátů *SYSTEM má, musíte se rozhodnout, jak budete se soubory certifikátu, které jste přenesli na cílový systém, pracovat. Můžete se rozhodnout, že použijete přenesené soubory certifikátu jako **Jinou systémovou paměť certifikátů**. Nebo se můžete rozhodnout, že naimportujete soukromý certifikát a odpovídající certifikát lokálního CA do existující paměti certifikátů *SYSTEM.

Jiné systémové paměti certifikátů jsou uživatelsky definované sekundární paměti certifikátů pro certifikáty SSL. Můžete je vytvořit a používat tehdy, když potřebujete poskytnout certifikáty pro uživatelsky programované aplikace používající SSL, které nepoužívají rozhraní API produktu DCM pro registraci ID aplikace pomocí obslužného programu DCM. Volba Jiná systémová paměť certifikátů vám umožní správu certifikátů pro aplikace, které naprogramujete vy nebo někdo jiný a které používají rozhraní SSL_Init API k programovanému přístupu a použití certifikátů při vytváření relace SSL. Díky tomuto rozhraní API může aplikace používat předvolený certifikát pro určitou paměť certifikátů namísto certifikátu, který konkrétně určíte.

Aplikace společnosti IBM iSeries (a aplikace mnohých dalších vývojářů softwaru) jsou naprogramovány tak, že používají pouze certifikáty uložené v paměti certifikátů *SYSTEM. Pokud se rozhodnete, že přenesené soubory použijete jako Jinou systémovou paměť certifikátů, nemůžete pomocí produktu DCM specifikovat, které aplikace budou certifikát používat. Nemůžete tudíž nakonfigurovat standardní aplikace serveru iSeries využívající SSL tak, aby používaly tento certifikát. Pokud hodláte používat certifikát pro aplikace serveru iSeries, musíte certifikát z vašich přenesených souborů paměti certifikátů naimportovat do paměti certifikátů *SYSTEM.

Chcete-li pracovat s přenesenými soubory certifikátu jako s Jinou systémovou pamětí certifikátů, postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, zadejte volbu **Jiná systémová paměť certifikátů**.
3. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte úplnou cestu a jméno souboru pro soubor paměti certifikátů (soubor s příponou .KDB), který jste přenesli z hostitelského systému. Dále zadejte heslo, které jste pro tuto paměť certifikátů uvedli v *hostitelském* systému, když jste vytvářeli certifikát pro cílový systém, a klepněte na **Pokračovat**.
4. V navigační liště vyberte volbu **Správa paměti certifikátů** a ze seznamu úloh pak vyberte **Změna hesla**. Vyplňte formulář pro změnu hesla k této paměti certifikátů.

   Poznámka: Když měníte heslo pro paměť certifikátů, vždy vyberte volbu **Automatické přihlašování**. Tím umožníte, aby produkt DCM uložil nové heslo tak, že budete moci v nové paměti používat všechny funkce produktu DCM pro správu certifikátů.

   Když změníte heslo, musíte paměť certifikátů znovu otevřít, abyste mohli pracovat s certifikáty, které v paměti jsou. Nyní můžete specifikovat, že certifikát v této paměti certifikátů bude používán jako předvolený certifikát.
5. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte **Jiná systémová paměť certifikátů**.
6. Když se zobrazí stránka **Paměť certifikátů a heslo**, zadejte úplnou cestu a jméno souboru pro soubor paměti certifikátů, zadejte nové heslo a klepněte na **Pokračovat**.
7. Když se obnoví navigační lišta, vyberte volbu **Správa paměti certifikátů** a ze seznamu úloh vyberte **Nastavení předvoleného certifikátu**.

Nyní když jste vytvořili a nakonfigurovali Jinou systémovou paměť certifikátů, může každá aplikace používající rozhraní SSL_Init API použít certifikát v této paměti k vytváření relací SSL.

*Paměť certifikátů *SYSTEM existuje — použití certifikátů v existující paměti certifikátů *SYSTEM:*

Můžete použít certifikáty v přenesených souborech paměti certifikátů můžete použít v existující paměti certifikátů *SYSTEM v systému. Chcete-li zvolit tuto variantu, musíte certifikáty ze souborů paměti certifikátů naimportovat do existující paměti certifikátů *SYSTEM. Certifikáty však nemůžete importovat přímo ze souborů .KDB a .RDB, protože tyto soubory nejsou ve formátu, který funkce importu produktu DCM umí rozpoznat a použít. Chcete-li přenesené certifikáty použít v existující paměti certifikátů *SYSTEM, musíte soubory otevřít jako Jinou systémovou paměť certifikátů a pak je exportovat do paměti certifikátů *SYSTEM.

Chcete-li exportovat certifikáty ze souborů paměti certifikátů do paměti certifikátů *SYSTEM, postupujte v cílovém systému takto:

1. Spusťte produkt DCM.
2. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, zadejte volbu **Jiná systémová paměť certifikátů**.
3. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte úplnou cestu a jméno souboru pro soubor paměti certifikátů (soubor s příponou .KDB), který jste přenesli z hostitelského systému. Dále zadejte heslo, které jste pro tuto paměť certifikátů uvedli v *hostitelském* systému, když jste vytvářeli certifikát pro cílový systém, a klepněte na **Pokračovat**.
4. V navigační liště vyberte volbu **Správa paměti certifikátů** a ze seznamu úloh pak vyberte **Změna hesla**. Vyplňte formulář pro změnu hesla k této paměti certifikátů. Když změníte heslo, musíte paměť certifikátů znovu otevřít, abyste mohli pracovat s certifikáty, které v paměti jsou.

   Poznámka: Když měníte heslo pro paměť certifikátů, vždy vyberte volbu **Automatické přihlašování**. Tím umožníte, aby produkt DCM uložil nové heslo tak, že budete moci v nové paměti používat všechny funkce produktu DCM pro správu certifikátů. Pokud nezměníte heslo a nevyberete volbu Automatické přihlašování, mohli byste se při exportu certifikátů z této paměti do paměti certifikátů *SYSTEM dostat do chybového stavu.
5. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte **Jiná systémová paměť certifikátů**.
6. Když se zobrazí stránka **Paměť certifikátů a heslo**, zadejte úplnou cestu a jméno souboru pro soubor paměti certifikátů, zadejte nové heslo a klepněte na **Pokračovat**.
7. Když se obnoví navigační lišta, vyberte volbu **Správa certifikátů** a ze zobrazeného seznamu úloh vyberte **Export certifikátu**.
8. Vyberte **Vydavatel certifikátů (CA)** jako typ certifikátu, který budete exportovat, a klepněte na **Pokračovat**.

   Poznámka: Předtím, než budete do paměti certifikátů exportovat serverový nebo klientský certifikát, musíte do ní exportovat certifikát lokálního CA. Kdybyste exportovali nejdříve serverový nebo klientský certifikát, mohli byste se dostat do chybového stavu způsobeného právě tím, že v paměti certifikátů neexistuje certifikát lokálního CA.
9. Vyberte certifikát lokálního CA, který chcete exportovat, a klepněte na **Exportovat**.
10. Vyberte **Paměť certifikátů** jako místo určení pro exportovaný certifikát a klepněte na **Pokračovat**.
11. Zadejte *SYSTEM jako cílovou paměť certifikátů, zadejte heslo pro paměť certifikátů *SYSTEM a klepněte na **Pokračovat**. Zobrazí se zpráva, která bude oznamovat, že certifikát byl úspěšně exportován, nebo v případě, že se export nepodařil, poskytne informace o chybách.
12. Nyní můžete exportovat do paměti certifikátů *SYSTEM serverový nebo klientský certifikát. Znovu vyberte úlohu **Export certifikátu**.
13. Vyberte volbu **Server nebo klient** jako typ certifikátu, který budete exportovat, a klepněte na **Pokračovat**.
14. Vyberte příslušný serverový nebo klientský certifikát, který chcete exportovat, a klepněte na **Exportovat**.
15. Vyberte **Paměť certifikátů** jako místo určení pro exportovaný certifikát a klepněte na **Pokračovat**.
16. Zadejte *SYSTEM jako cílovou paměť certifikátů, zadejte heslo pro paměť certifikátů *SYSTEM a klepněte na **Pokračovat**. Zobrazí se zpráva, která bude oznamovat, že certifikát byl úspěšně exportován, nebo v případě, že se export nepodařil, poskytne informace o chybách.
17. Nyní můžete přiřadit certifikát k aplikaci, která jej bude používat při SSL. V navigační liště klepněte na volbu **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***SYSTEM**.

18. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte heslo pro paměť certifikátů *SYSTEM a klepněte na **Pokračovat**.
19. Když se obnoví navigační lišta, vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
20. Ze seznamu úloh vyberte volbu **Přiřazení certifikátu**. Zobrazí se seznam certifikátů v aktuální paměti certifikátů.
21. Vyberte certifikát, který jste vytvořili v *hostitelském* systému, a klepněte na **Přiřadit k aplikacím**. Zobrazí se seznam aplikací využívajících SSL, kterým můžete přiřadit tento certifikát.
22. Vyberte aplikace, které budou používat certifikát pro relace SSL, a klepněte na **Pokračovat**. Produkt DCM zobrazí zprávu, která bude potvrzovat výběr certifikátu pro určité aplikace.

    Poznámka: Některé aplikace využívající SSL podporují autentizaci klientů založenou na certifikátech. Aplikace s touto podporou musí být schopna autentizovat certifikáty předtím, než poskytne přístup k prostředkům. Pro tuto aplikaci tudíž musíte definovat seznam důvěryhodných CA. Tím zajistíte, že aplikace bude potvrzovat pouze certifikáty těch CA, které v seznamu uvedete jako důvěryhodné. Pokud uživatelé nebo klientská aplikace předloží certifikát od CA, který není uveden jako důvěryhodný v seznamu důvěryhodných CA, aplikace certifikát nepřijme za základ pro platnou autentizaci.

Po provedení výše uvedených úloh budou moci aplikace v cílovém systému používat certifikát vydaný lokálním CA v jiném systému system. Avšak předtím, než pro tyto aplikace začnete používat SSL, musíte je nakonfigurovat tak, aby používaly SSL.

Dříve, než bude uživatel moci přistupovat k vybraným aplikacím přes SSL, musí pomocí produktu DCM získat kopii certifikátu lokálního CA z hostitelského systému. Certifikát lokálního CA se musí zkopírovat do souboru na počítači uživatele nebo stáhnout do prohlížeče uživatele, což závisí na požadavcích aplikace, která používá SSL.

Použití soukromého certifikátu pro podepisování objektů v cílovém systému

Správa certifikátů, které používáte k podepisování objektů, se provádí z paměti certifikátů *OBJECTSIGNING v produktu DCM (Digital Certificate Manager). Pokud jste produkt DCM v cílovém systému nikdy nepoužívali ke správě certifikátů pro podepisování objektů, pak tato paměť certifikátů v cílovém systému neexistuje.

Úlohy, které musíte provést, abyste mohli použít přenesené soubory paměti certifikátů, které jste vytvořili v hostitelském systému lokálního CA, se liší podle toho, zda paměť certifikátů *OBJECTSIGNING existuje, či nikoliv. Pokud paměť certifikátů *OBJECTSIGNING neexistuje, můžete přenesené soubory certifikátů použít jako prostředek pro vytvoření paměti certifikátů *OBJECTSIGNING. Pokud paměť certifikátů *OBJECTSIGNING v cílovém systému existuje , musíte importovat přenesené certifikáty do této paměti.

Paměť certifikátů *OBJECTSIGNING neexistuje:

Úlohy, jež budete provádět, abyste mohli použít soubory paměti certifikátů, které jste vytvořili v hostitelském systému lokálního CA, se liší podle toho, zda jste již někdy produkt DCM v cílovém systému používali ke správě certifikátů pro podepisování objektů.

Pokud paměť certifikátů *OBJECTSIGNING v cílovém systému, kam jste přenesli soubory paměti certifikátů, neexistuje, postupujte takto:

1. Ujistěte se, že soubory paměti certifikátů (dva soubory: jeden s příponou .KDB a jeden s příponou .RDB), které jste vytvořili v hostitelském systému lokálního CA, jsou v adresáři /QIBM/USERDATA/ICSS/CERT/SIGNING .
2. Jakmile jsou přenesené soubory certifikátů v adresáři /QIBM/USERDATA/ICSS/CERT/SIGNING, přejmenujte tyto soubory na soubory SGNOBJ.KDB a SGNOBJ.RDB, pokud je to nutné. Přejmenováním těchto souborů vytvoříte komponenty, které obsahují paměť certifikátů *OBJECTSIGNING pro cílový systém. Soubory paměti certifikátů již obsahují kopie certifikátů pro řadu veřejných internetových CA. Produkt DCM tyto kopie a rovněž i kopii certifikátu lokálního CA do souborů paměti certifikátů přidal, když jste tyto soubory vytvářeli.

   Upozornění: Jestliže cílový systém již soubory SGNOBJ.KDB a SGNOBJ.RDB v adresáři /QIBM/USERDATA/ICSS/CERT/SIGNING obsahuje, pak v tomto cílovém systému paměť

certifikátů *OBJECTSIGNING existuje. Nesmíte tedy přejmenovávat přenesené soubory tak, jak je výše popsáno. Přepsání předvolených souborů podepisování objektů způsobí problémy při používání produktu DCM, přenesené paměti certifikátů a jejího obsahu. Pokud paměť certifikátů *OBJECTSIGNING již existuje, musíte použít jiný proces, chcete-li certifikáty dostat do této existující paměti.

3. Spusťte produkt DCM. Nyní musíte změnit heslo pro paměť certifikátů *OBJECTSIGNING. Při změně hesla produkt DCM uloží nové heslo tak, že budete moci v této paměti používat všechny funkce produktu DCM pro správu certifikátů.
4. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***OBJECTSIGNING**.
5. Když se zobrazí stránka pro heslo, zadejte heslo, které jste pro tuto paměť certifikátů uvedli, když jste ji v hostitelském systému vytvářeli, a klepněte na **Pokračovat**.
6. V navigační liště vyberte volbu **Správa paměti certifikátů** a ze seznamu úloh pak vyberte **Změna hesla**. Vyplňte formulář pro změnu hesla k této paměti certifikátů. Když změníte heslo, musíte paměť certifikátů znovu otevřít, abyste mohli pracovat s certifikáty, které v paměti jsou. Nyní můžete vytvořit definici aplikace, na jejímž základě bude aplikace používat certifikát k podepisování objektů.
7. Když znovu otevřete paměť certifikátů, vyberte v navigační liště volbu **Správa aplikací**. Zobrazí se seznam úloh.
8. Ze seznamu úloh vyberte volbu **Přidání aplikace**, čímž zahájíte proces vytvoření definice aplikace pro podepisování objektů tak, aby používala certifikát k podepisování objektů.
9. Vyplňte formulář, abyste nadefinovali aplikaci pro podepisování objektů, a klepněte na **Přidat**. Tato definice aplikace nepopisuje žádnou skutečnou aplikaci, ale popisuje spíše typ objektů, které hodláte pomocí určitého certifikátu podepisovat. Chcete-li poradit s vyplněním formuláře, použijte online nápovědu.
10. Klepněte na **OK**, abyste potvrdili definici aplikace. Zobrazí se seznam úloh **Správa aplikací**.
11. Ze seznamu úloh vyberte volbu **Aktualizace přiřazení certifikátu**. Zobrazí se seznam ID aplikací pro podepisování objektů, kterým můžete certifikát přiřadit.
12. Vyberte ze seznamu ID vaší aplikace a klepněte na **Aktualizace přiřazení certifikátu**.
13. Vyberte certifikát, který vydal lokální CA v hostitelském systému, a klepněte na **Přiřadit nový certifikát**.

Po dokončení těchto úloh máte připraveno vše potřebné k tomu, abyste mohli zahájit podepisování objektů a zajišťovat tak jejich integritu.

Pokud distribuujete podepsané objekty, tak ti, kteří objekty dostávají a chtějí si ověřit totožnost odesílatele a to, že data jsou nezměněna, musí pomocí produktu DCM ověřit podpis na objektu. Aby mohl příjemce ověřit podpis, musí mít kopii certifikátu pro ověřování podpisů. Jako součást dodávky podepsaných objektů musíte poskytnout kopii tohoto certifikátu.

Příjemce musí mít také kopii certifikátu CA pro toho CA, který certifikát, jenž jste použili k podepsání objektu, vydal. Jestliže jste podepsali objekty pomocí certifikátu od nějakého známého internetového CA, pak uživatelova verze produktu DCM již má kopii potřebného certifikátu CA. Musíte však kopii certifikátu CA příjemci spolu s podepsanými objekty zaslat samostatně. Musíte například poskytovat kopii certifikátu lokálního CA, pokud jste podepsali objekty pomocí certifikátu od lokálního CA. Z bezpečnostních důvodů musíte zaslat certifikát CA samostatně, nebo dát certifikát CA k dispozici veřejně na vyžádání těch, kteří jej potřebují.

Paměť certifikátů *OBJECTSIGNING existuje:

Certifikáty v přenesených souborech paměti certifikátů můžete použít v existující paměti certifikátů *OBJECTSIGNING v systému. Chcete-li zvolit tuto variantu, musíte certifikáty ze souborů paměti certifikátů naimportovat do existující paměti certifikátů *OBJECTSIGNING. Certifikáty však nemůžete importovat přímo ze souborů .KDB a .RDB, protože tyto soubory nejsou ve formátu, který funkce importu produktu DCM umí rozpoznat a použít. Certifikáty můžete do existující paměti certifikátů *OBJECTSIGNING přidat tak, že přenesené soubory v cílovém systému otevřete jako Jinou systémovou paměť certifikátů. Pak můžete certifikáty exportovat přímo do paměti certifikátů *OBJECTSIGNING. Z přenesených souborů musíte exportovat jak vlastní certifikát pro podepisování objektů, tak certifikát lokálního CA.

Chcete-li exportovat certifikáty ze souborů paměti certifikátů přímo do paměti certifikátů *OBJECTSIGNING, postupujte v cílovém systému takto:

1. Spusťte produkt DCM.
2. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, zadejte volbu **Jiná systémová paměť certifikátů**.
3. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte úplnou cestu a jméno souboru pro soubory paměti certifikátů. Zadejte také heslo, které jste uvedli pro tuto paměť certifikátů, když jste ji v hostitelském systému vytvářeli, a klepněte na **Pokračovat**.
4. V navigační liště vyberte volbu **Správa paměti certifikátů** a ze seznamu úloh pak vyberte **Změna hesla**. Vyplňte formulář pro změnu hesla k této paměti certifikátů.

   Poznámka: Když měníte heslo pro paměť certifikátů, vždy vyberte volbu **Automatické přihlašování**. Tím umožníte, aby produkt DCM uložil nové heslo tak, že budete moci v nové paměti používat všechny funkce produktu DCM pro správu certifikátů. Pokud nezměníte heslo a nevyberete volbu Automatické přihlašování, mohli byste se při exportu certifikátů z této paměti do paměti certifikátů *OBJECTSIGNING dostat do chybového stavu.

   Když změníte heslo, musíte paměť certifikátů znovu otevřít, abyste mohli pracovat s certifikáty, které v paměti jsou.
5. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte **Jiná systémová paměť certifikátů**.
6. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte úplnou cestu a jméno souboru pro soubor paměti certifikátů, zadejte nové heslo a klepněte na **Pokračovat**.
7. Když se obnoví navigační lišta, vyberte volbu **Správa certifikátů** a ze zobrazeného seznamu úloh vyberte **Export certifikátu**.
8. Vyberte **Vydavatel certifikátů (CA)** jako typ certifikátu, který budete exportovat, a klepněte na **Pokračovat**.

   Poznámka: Znění této úlohy předpokládá, že když pracujete s Jinou systémovou pamětí certifikátů, pracujete se serverovým nebo klientským certifikátem. Je tomu tak proto, že tento typ paměti certifikátů je určen pro použití jako sekundární paměť certifikátů k paměti certifikátů *SYSTEM. Avšak použití úlohy exportu v této paměti certifikátů představuje nejjednodušší způsob, jak dostat certifikáty z přenesených souborů do existující paměti certifikátů *OBJECTSIGNING.
9. Vyberte certifikát lokálního CA, který chcete exportovat, a klepněte na **Exportovat**.

   Poznámka: Certifikát CA musíte do paměti certifikátů exportovat předtím, než budete do paměti certifikátů exportovat certifikát pro podepisování objektů. Kdybyste exportovali nejdříve certifikát pro podepisování objektů, můžete se dostat do chybového stavu způsobeného právě tím, že v paměti certifikátů neexistuje certifikát CA.
10. Vyberte **Paměť certifikátů** jako místo určení pro exportovaný certifikát a klepněte na **Pokračovat**.
11. Zadejte *OBJECTSIGNING jako cílovou paměť certifikátů, zadejte heslo pro paměť certifikátů *OBJECTSIGNING a klepněte na **Pokračovat**.
12. Nyní můžete do paměti certifikátů *OBJECTSIGNING naexportovat certifikát pro podepisování objektů. Znovu vyberte úlohu **Export certifikátu**.
13. Vyberte volbu **Server nebo klient** jako typ certifikátu, který budete exportovat, a klepněte na **Pokračovat**.
14. Vyberte příslušný certifikát, který chcete exportovat, a klepněte na **Exportovat**.
15. Vyberte **Paměť certifikátů** jako místo určení pro exportovaný certifikát a klepněte na **Pokračovat**
16. Zadejte *OBJECTSIGNING jako cílovou paměť certifikátů, zadejte heslo pro paměť certifikátů *OBJECTSIGNING a klepněte na **Pokračovat**. Zobrazí se zpráva, která bude oznamovat, že certifikát byl úspěšně exportován, nebo v případě, že se export nepodařil, poskytne informace o chybách.

    Poznámka: Abyste mohli pomocí tohoto certifikátu podepisovat objekty, musíte nyní přiřadit certifikát k aplikaci pro podepisování objektů.

Správa aplikací v produktu DCM

Jsou zde uvedeny informace o tvorbě definic aplikací a o tom, jak spravovat přiřazování certifikátů k aplikaci. Dále je zde vysvětleno definování seznamů důvěryhodných CA, které aplikace používají jako základ pro schválení certifikátu při autentizaci klienta.

Pomocí produktu DCM lze provádět různé správní úlohy pro aplikace využívající SSL a aplikace pro podepisování objektů. Můžete například určovat, které certifikáty budou vaše aplikace používat pro komunikační relace SSL (Secure Sockets Layer). Úlohy pro správu aplikací, jež lze provádět, se liší podle typu aplikace a podle toho, ve které paměti certifikátů pracujete. Správu aplikací můžete provádět pouze z paměti certifikátů *SYSTEM nebo *OBJECTSIGNING.

Většina úloh pro správu aplikací, které produkt DCM poskytuje, je snadno pochopitelných, s některými z nich však možná nebudete obeznámeni. Další informace o těchto úlohách obsahují tato témata:

Související pojmy

"Definice aplikace" na stránce 9
Tato část obsahuje informace o tom, co jsou to definice aplikací v rámci produktu DCM a jak s nimi lze pracovat při konfiguraci SSL a podepisování objektů.

Vytvoření definice aplikace

V tomto tématu se můžete dozvědět o dvou odlišných typech aplikací, které můžete definovat a se kterými můžete pracovat.

Existují dva typy definic aplikací, se kterými lze v produktu DCM pracovat: definice aplikací pro serverové nebo klientské aplikace, které používají SSL, a definice aplikací, které používáte při podepisování objektů.

Chcete-li v produktu DCM pracovat s definicemi aplikací pro SSL a jejich certifikáty, musí být aplikace nejdříve v produktu DCM zaregistrována jako definice aplikace tak, aby měla jedinečné ID aplikace. Vývojáři aplikací provádějí registraci aplikací využívajících SSL pomocí rozhraní API (QSYRGAP, QsyRegisterAppForCertUse), takže ID aplikace se v produktu DCM vytvoří automaticky. Všechny aplikace IBM iSeries využívající SSL jsou takto registrovány produktem DCM, takže k nim můžete pomocí produktu DCM snadno přiřadit certifikát a aplikace pak mohou vytvářet relace SSL. Také pro aplikace, které naprogramujete nebo zakoupíte, můžete definovat definici aplikace a vytvořit pro ni ID aplikace v rámci samotného produktu DCM. Chcete-li definici aplikace pro SSL vytvořit pro klientskou nebo serverovou aplikaci, musíte pracovat v paměti certifikátů *SYSTEM.

Chcete-li pomocí nějakého certifikátu podepisovat objekty, musíte nejprve nadefinovat aplikaci, kterou bude certifikát používat. Na rozdíl od definice aplikace v rámci SSL nepopisuje aplikace pro podepisování objektů žádnou skutečnou aplikaci. Definice aplikace, kterou vytvoříte, může namísto toho popisovat typ nebo skupinu objektů, které hodláte podepisovat. Při tvorbě definice aplikace pro podepisování objektů musíte pracovat v paměti certifikátů *OBJECTSIGNING.

Chcete-li vytvořit definici aplikace, postupujte takto:

1. Spusťte produkt DCM.
2. Klepněte na **Výběr paměti certifikátů** a vyberte příslušnou paměť certifikátů. (To je buď paměť certifikátů *SYSTEM, nebo *OBJECTSIGNING, podle toho, který typ definice aplikace chcete vytvořit.)

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
3. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte heslo, které jste pro danou paměť certifikátů uvedli, když jste ji vytvářeli, a klepněte na **Pokračovat**.
4. V navigační liště vyberte volbu **Správa aplikací**. Zobrazí se seznam úloh.
5. Ze seznamu úloh vyberte volbu **Přidání aplikace** a zobrazí se formulář pro definici aplikace.

   Poznámka: Pokud pracujete v paměti certifikátů *SYSTEM, vyzve vás na tomto místě produkt DCM, abyste zvolili, zda budete přidávat definici serverové aplikace nebo definici klientské aplikace.

6. Vyplňte formulář a klepněte na **Přidat**. Informace, které zadáváte do definice aplikace, se liší podle typu aplikace, kterou definujete. Jestliže definujete serverovou aplikaci, můžete také specifikovat, zda aplikace může používat certifikáty pro autentizaci klientů a zda musí vyžadovat autentizaci klientů. Můžete také specifikovat, že aplikace bude při autentizaci certifikátů používat seznam důvěryhodných CA.

Související pojmy

"Definice aplikace" na stránce 9
Tato část obsahuje informace o tom, co jsou to definice aplikací v rámci produktu DCM a jak s nimi lze pracovat při konfiguraci SSL a podepisování objektů.

Správa přiřazení certifikátu k aplikaci

Předtím, než může aplikace vykonávat funkce zabezpečení, jako je vytváření relací SSL nebo podepisování objektů, musíte pomocí produktu Digital Certificate Manager (DCM) přiřadit aplikaci určitý certifikát.

Chcete-li přiřadit aplikaci certifikát nebo změnit přiřazení certifikátu k aplikaci, postupujte takto:

1. Spusťte produkt DCM.
2. Klepněte na **Výběr paměti certifikátů** a vyberte příslušnou paměť certifikátů. (To jest buď paměť certifikátů *SYSTEM, nebo *OBJECTSIGNING, podle toho, pro který typ aplikace chcete přiřadit certifikát.)

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
3. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte heslo, které jste pro danou paměť certifikátů uvedli, když jste ji vytvářeli, a klepněte na **Pokračovat**.
4. V navigační liště vyberte volbu **Správa aplikací**. Zobrazí se seznam úloh.
5. Jestliže jste v paměti certifikátů *SYSTEM, vyberte typ aplikace, se kterou budete pracovat. (Podle situace vyberete buď aplikaci typu **Server**, nebo **Klient**.)
6. Ze seznamu úloh vyberte volbu **Aktualizace přiřazení certifikátu**. Zobrazí se seznam aplikací, kterým můžete přiřadit certifikát.
7. Vyberte ze seznamu aplikaci a klepněte na **Aktualizace přiřazení certifikátu**, abyste zobrazili seznam certifikátů, které můžete aplikaci přiřadit.
8. Vyberte ze seznamu certifikát a klepněte na **Přiřadit nový certifikát**. Produkt DCM zobrazí zprávu, která bude potvrzovat váš výběr certifikátu pro danou aplikaci.

   Poznámka: Pokud přiřazujete certifikát k aplikaci využívající SSL, která podporuje použití certifikátů při autentizaci klientů, musíte aplikaci definovat seznam důvěryhodných CA. Tím zajistíte, že aplikace bude potvrzovat pouze certifikáty těch CA, které v seznamu uvedete jako důvěryhodné. Pokud uživatelé nebo klientská aplikace předloží certifikát od CA, který není uveden jako důvěryhodný v seznamu důvěryhodných CA, aplikace certifikát nepřijme za základ pro platnou autentizaci.

Když měníte nebo odstraňujete přiřazení certifikátu k aplikaci, aplikace může, ale nemusí být schopna tuto změnu zaregistrovat, pokud je v době, kdy změnu provádíte, spuštěná. Například servery iSeries Access for Windows použijí změny v certifikátech, které provedete, automaticky. Avšak servery Telnet, IBM HTTP Server for i5/OS, nebo jiné aplikace budete muset zastavit a spustit, aby mohly provedenou změnu certifikátu aplikovat.

Počínaje verzí V5R2 operačního systému OS/400 můžete pomocí úlohy Přiřazení certifikátu přiřadit certifikát k několika aplikacím najednou.

Definování seznamu důvěryhodných CA pro aplikaci

Aplikace, které podporují použití certifikátů při autentizaci klientů během relace SSL (Secure Sockets Layer), musí určovat, zda přijmout určitý certifikát jako platný průkaz totožnosti. Jedním z kritérií, které aplikace používá při autentizaci certifikátu, je to, zda aplikace důvěřuje vydavateli certifikátů (CA), jenž certifikát vydal.

Pomocí produktu Digital Certificate Manager (DCM) lze definovat, kterým CA může aplikace důvěřovat, když provádí autentizaci klienta prostřednictvím certifikátů. Ty CA, kterým může aplikace důvěřovat, určujete prostřednictvím tzv. seznamu důvěryhodných CA.

Předtím, než můžete definovat seznam důvěryhodných CA pro určitou aplikaci, musí být splněno několik podmínek:

- Aplikace musí podporovat použití certifikátů při autentizaci klientů.
- V definici pro tuto aplikaci musí být specifikováno, že aplikace používá seznam důvěryhodných CA.

Jestliže v definici aplikace je specifikováno, že aplikace používá seznam důvěryhodných CA, musíte tento seznam definovat předtím, než bude aplikace moci úspěšně provádět autentizaci klientů na základě certifikátů. Tím zajistíte, že aplikace bude potvrzovat pouze certifikáty těch CA, které v seznamu uvedete jako důvěryhodné. Pokud uživatelé nebo klientská aplikace předloží certifikát od CA, který není uveden jako důvěryhodný v seznamu důvěryhodných CA, aplikace certifikát nepřijme za základ pro platnou autentizaci.

Když přidáváte do seznamu důvěryhodných CA aplikace nějakého CA, ověřte si rovněž, že je tento CA aktivní.

Chcete-li definovat seznam důvěryhodných CA pro aplikaci, postupujte takto:

1. Spusťte produkt DCM.
2. Klepněte na **Vybrat paměť certifikátů** a jako paměť certifikátů, která se má otevřít, vyberte ***SYSTEM**.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
3. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte heslo, které jste pro danou paměť certifikátů uvedli, když jste ji vytvářeli, a klepněte na **Pokračovat**.
4. V navigační liště vyberte volbu **Správa aplikací**. Zobrazí se seznam úloh.
5. Ze seznamu úloh vyberte volbu **Definování seznamu důvěryhodných CA**.
6. Vyberte typ aplikace (serverová nebo klientská), pro kterou chcete definovat seznam, a klepněte na **Pokračovat**.
7. Ze seznamu vyberte aplikaci a klepněte na **Pokračovat**. Zobrazí se seznam certifikátů CA, ze kterého budete vybírat CA do seznamu důvěryhodných CA.
8. Vyberte ty CA, kterým aplikace bude důvěřovat, a klepněte na **OK**. Produkt DCM zobrazí zprávu, která bude potvrzovat váš výběr CA pro seznam důvěryhodných CA.

   Poznámka: Ze seznamu můžete buď vybrat jednotlivé CA, nebo můžete specifikovat, že aplikace bude důvěřovat všem CA ze seznamu, nebo žádnému CA ze seznamu. Certifikát CA si také můžete předtím, než ho přidáte do seznamu důvěryhodných CA, prohlédnout nebo ověřit.

Správa certifikátů prostřednictvím data ukončení platnosti

Produkt DCM (Digital Certificate Manager) poskytuje podporu správy certifikátů prostřednictvím ukončení jejich platnosti, což administrátorům umožňuje spravovat serverové nebo klientské certifikáty, certifikáty pro podepisování objektů a uživatelské certifikáty v lokálním systému.

Poznámka: Pokud produkt DCM nakonfigurujete tak, aby spolupracoval s produktem EIM, můžete spravovat uživatelské certifikáty dle data ukončení platnosti v celém podniku.

Použití DCM k zobrazení certifikátů na základě ukončení platnosti vám umožňuje rychle a snadno vymezit ty certifikáty, jejichž platnost bude brzy ukončena, proto abyste je mohli včas obnovit.

Poznámka: Protože můžete k ověření podpisů na objektech používat certifikát pro ověřování podpisu, i když platnost certifikátu končí, neposkytuje DCM službu pro kontrolu ukončení platnosti těchto certifikátů.

Chcete-li zobrazit a spravovat serverové a klientské certifikáty na základě data ukončení platnosti, postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště klepněte na volbu **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte buď ***OBJECTSIGNING** nebo ***SYSTEM**.

Poznámka: Jestliže máte dotazy k tomu, jak vyplnit v průběhu práce s produktem DCM určitý formulář, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.

3. Zadejte heslo pro paměť certifikátů a klepněte na **Pokračovat**.
4. Když se obnoví navigační liště, vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
5. Ze seznamu úloh vyberte volbu **Kontrola data ukončení platnosti**.
6. Vyberte typ certifikátu, který chcete zkontrolovat. Jestliže jste v paměti certifikátů *SYSTEM, vyberte volbu **Serverový nebo klientský**. Jestliže jste v paměti certifikátů *OBJECTSIGNING, vyberte volbu **Podepisování objektů**.
7. Do pole **Rozsah dat ukončení platnosti ve dnech (1-365)** zadejte počet dnů odpovídající ukončení platnosti certifikátů, které chcete zobrazit dle data ukončení platnosti, a klepněte na **Další**. Produkt DCM zobrazí všechny certifikáty, jejichž platnost končí mezi dnešním dnem a datem, které odpovídá hodnotě zadaných dnů. Produkt DCM také zobrazí všechny certifikáty, jejichž platnost končí před dnešním datem.
8. Vyberte certifikát, který chcete spravovat. Můžete se rozhodnout, že si prohlédnete podrobné informace certifikátu, že certifikát vymažete nebo naopak obnovíte.
9. Až dokončíte práci s certifikáty na seznamu, klepněte na **Zrušit**.

Potvrzování certifikátů a aplikací

Pomocí produktu DCM (Digital Certificate Manager) můžete potvrzovat jednotlivé certifikáty nebo aplikace, které je používají. Seznam věcí, které produkt DCM kontroluje, se mírně liší podle toho, zda se potvrzuje certifikát nebo aplikace.

Potvrzování aplikace

Jestliže pomocí produktu DCM potvrzujete definice aplikací, napomáhá to předcházet problémům s certifikáty, k nimž může dojít, když aplikace vykonává funkci, která certifikáty vyžaduje. Tyto problémy mohou u aplikace způsobit, že se nebude moci úspěšně účastnit relace SSL (Secure Sockets Layer) nebo nebude moci úspěšně podepisovat objekty.

Když potvrzujete určitou aplikaci, produkt DCM ověřuje, že pro tuto aplikaci existuje přiřazení certifikátu, a zjišťuje, zda je přiřazený certifikát platný. Produkt DCM dále zjišťuje, zda v případě, že je aplikace konfigurována pro použití seznamu důvěryhodných CA, obsahuje tento seznam alespoň jeden certifikát CA. Produkt DCM pak ověřuje, zda certifikáty CA v seznamu důvěryhodných CA pro danou aplikaci jsou platné. Pokud definice aplikace uvádí, že se má provádět zpracování seznamu odvolaných certifikátů (CRL), a je definováno umístění CRL pro daného CA, pak produkt DCM v rámci ověřovacího procesu kontroluje i CRL.

Potvrzování certifikátu

Když potvrzujete certifikát, produkt DCM ověřuje řadu položek týkajících se certifikátu, aby zajistil autenticitu a platnost certifikátu. Potvrzováním certifikátu se zajistí, že aplikace, které používají certifikát k zabezpečené komunikaci nebo k podepisování objektů, pravděpodobně nenarazí při použití certifikátů na nějaké problémy.

Jako součást procesu potvrzení produkt DCM kontroluje, zda vybranému certifikátu nevypršela platnost. Produkt DCM také kontroluje, zda certifikát není uveden v seznamu odvolaných certifikátů (CRL) jako odvolaný, pokud pro CA, který certifikát vydal, existuje umístění CRL. Navíc produkt DCM kontroluje, zda certifikát CA pro vydávajícího CA je v aktuální paměti certifikátů a zda je certifikát CA aktivní a tudíž důvěryhodný. Jestliže má certifikát soukromý klíč (např. serverový certifikát, klientský certifikát nebo certifikát pro podepisování objektů), pak produkt DCM také prověřuje dvojici veřejného a soukromého klíče, aby zajistil, že si dvojice veřejného a soukromého klíče odpovídá. Jinými slovy, produkt DCM zašifruje data pomocí veřejného klíče a pak zjistí, zda se data mohou dešifrovat pomocí soukromého klíče.

Související pojmy

"Umístění seznamu odvolaných certifikátů (CRL)" na stránce 6
Seznam odvolaných certifikátů (CRL) je soubor, který obsahuje všechny neplatné a odvolané certifikáty pro určitého vydavatele certifikátů (CA).

“Ověření platnosti” na stránce 10
Produkt DCM poskytuje úlohy, prostřednictvím kterých lze potvrdit platnost certifikátu nebo aplikace a ověřit tak různé vlastnosti, které musí mít.

Přiřazení certifikátu k aplikacím

Produkt DCM vám umožňuje přiřazovat certifikáty rychle a snadno k více aplikacím najednou. Přiřazení certifikátu k více aplikacím můžete provádět pouze v paměti certifikátů *SYSTEM nebo *OBJECTSIGNING.

Chcete-li přiřadit certifikát k jedné nebo více aplikacím, postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště klepněte na volbu **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte buď ***OBJECTSIGNING** nebo ***SYSTEM**.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit v průběhu práce s produktem DCM určitý formulář, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
3. Zadejte heslo pro paměť certifikátů a klepněte na **Pokračovat**.
4. Když se obnoví navigační lišta, vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
5. Ze seznamu úloh vyberte volbu **Přiřazení certifikátu**. Zobrazí se seznam certifikátů v aktuální paměti certifikátů.
6. Vyberte ze seznamu příslušný certifikát a klepněte na volbu **Přiřazení k aplikacím**. Zobrazí se seznam definicí aplikací pro aktuální paměť certifikátů.
7. Vyberte ze seznamu jednu nebo více aplikací a klepněte na **Pokračovat**. Zobrazí se stránka buď se zprávou potvrzující zvolené přiřazení, nebo s chybovou zprávou v případě nějakého problému.

Správa umístění CRL

Pomocí produktu DCM (Digital Certificate Manager) můžete definovat a spravovat informace o umístění seznamu odvolaných certifikátů (CRL) pro určitého vydavatele certifikátů (CA), který se pak používá v rámci procesu potvrzování certifikátu.

Produkt DCM nebo aplikace, která vyžaduje zpracování CRL, mohou pomocí CRL určit, zda CA, který konkrétní certifikát vydal, tento certifikát neodvolal. Když nadefinujete umístění CRL pro určitého CA, mohou pak aplikace, které podporují použití certifikátů při autentizaci klientů, k CRL přistupovat.

Aplikace, které podporují použití certifikátů při autentizaci klientů, mohou pomocí zpracování CRL provádět přísnější autentizaci certifikátů, které přijímají jako platný průkaz totožnosti. Aby aplikace mohla použít definovaný CRL jako součást procesu potvrzování certifikátu, musí být v definici aplikace v rámci produktu DCM specifikováno, že má aplikace provádět zpracování CRL.

Jak zpracování CRL funguje

Když pomocí produktu DCM potvrzujete certifikát nebo aplikaci, produkt DCM provádí zpracování CRL standardně v rámci procesu ověřování. Pokud pro CA, který vydal ověřovaný certifikát, není definováno umístění CRL, produkt DCM nemůže kontrolu CRL provést. Produkt DCM se však může pokusit ověřit jiné důležité informace o certifikátu, například zda je podpis CA na konkrétním certifikátu platný nebo zda CA, který certifikát vydal, je důvěryhodný.

Definování umístění CRL

Chcete-li definovat umístění CRL pro určitého CA, postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště vyberte volbu **Správa umístění CRL**. Zobrazí se seznam úloh.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit určitý formulář v této vedené úloze, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.

3. Ze seznamu úloh vyberte volbu **Přidání umístění CRL** a zobrazí se formulář, pomocí něhožpopíšete umístění CRL a zadáte, jak bude produkt DCM nebo aplikace k umístění přistupovat.
4. Vyplňte formulář a klepněte na **OK**. Umístění CRL musíte přiřadit jedinečné jméno, dále musíte identifikovat server LDAP, který je hostitelským systémem pro daný CRL, a zadat informace o spojení, které popisují přístup na server LDAP. Nyní musíte přiřadit definici umístění CRL ke konkrétnímu CA.
5. V navigační liště vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
6. Ze seznamu úloh vyberte **Aktualizace přiřazení umístění CRL**. Zobrazí se seznam certifikátů CA.
7. Vyberte ze seznamu certifikát CA, kterému chcete přiřadit definici umístění CRL, kterou jste vytvořili, a klepněte na **Aktualizovat přiřazení umístění CRL**. Zobrazí se seznam umístění CRL.
8. Vyberte ze seznamu umístění CRL, které chcete přiřadit k tomuto CA, a klepněte na **Aktualizovat přiřazení**. V horní části stránky se zobrazí se zpráva, která informuje, že umístění CRL bylo přiřazeno k vybranému certifikátu CA.

Poznámka: Pokud potřebujete anonymní přístup k serveru LDAP, pak musíte použít nástroj Directory Server Web Administration Tool a vybrat úlohu ″Správa schématu″ za účelem změny třídy zabezpečení (která je nazývána rovněž jako ″přístupová třída″) u atributů certificateRevocationList a authorityRevocationList z hodnoty ″kritický″ na hodnotu ″normální″. Pole **Rozlišovací jméno přihlášení** a **Heslo** ponechte prázdná.

Když máte nadefinováno umístění CRL pro určitého CA, může produkt DCM nebo jiné aplikace toto umístění používat při provádění zpracování CRL. Aby však mohlo zpracování CRL fungovat, musí server adresářů obsahovat příslušný CRL. Musíte také nakonfigurovat jak server adresářů (LDAP), tak klientské aplikace, aby používaly SSL, a pomocí produktu přiřadit aplikacím v DCM certifikát.

Související pojmy

“Umístění seznamu odvolaných certifikátů (CRL)” na stránce 6
Seznam odvolaných certifikátů (CRL) je soubor, který obsahuje všechny neplatné a odvolané certifikáty pro určitého vydavatele certifikátů (CA).

Související informace

IBM Directory Server for iSeries (LDAP)

Povolení SSL na serveru adresářů

Uložení klíčů certifikátů do produktu IBM Cryptographic Coprocessor

V této části je vysvětleno, jak lze pomocí nainstalovaného koprocesoru zajistit bezpečnější uložení soukromých klíčů certifikátů.

Pokud máte nainstalován produkt IBM Cryptographic Coprocessor ve vašem systému, můžete pomocí něj zajistit bezpečnější uložení soukromých klíčů certifikátů. Do koprocesoru lze uložit soukromý klíč serverového certifikátu, klientského certifikátu nebo certifikátu lokálního vydavatele certifikátů (CA). Koprocesor však nelze použít pro uložení soukromého klíče uživatelského certifikátu, neboť tento klíč musí být uložen v systému uživatele. V současné době také nelze pomocí koprocesoru uložit soukromý klíč certifikátu pro podepisování objektů.

Pomocí koprocesoru lze zajistit uložení soukromých klíčů certifikátů jedním ze dvou způsobů:

- Uložení soukromého klíče certifikátu přímo v koprocesoru.
- Pomocí hlavního klíče koprocesoru zašifrovat soukromý klíč certifikátu a uložit jej ve zvláštním souboru klíčů.

Volbu uložení klíče pomocí koprocesoru lze vybrat v rámci procesu vytváření nebo obnovy certifikátu. Jestliže pomocí koprocesoru ukládáte soukromý klíč certifikátu, můžete také změnit přiřazení koprocesorového zařízení pro tento klíč.

Chcete-li používat koprocesor k uložení soukromých klíčů, musíte zajistit, aby byl koprocesor předtím, než začnete pracovat s produktem DCM (Digital Certificate Manager), logicky zapnutý. Jinak by totiž produkt DCM v rámci procesu vytváření nebo obnovy certifikátu vůbec stránku s možností volby uložení klíčů neposkytl.

Když vytváříte nebo obnovujete serverový nebo klientský certifikát, vybíráte volbu uložení soukromého klíče poté, co vyberete typ CA, který aktuální certifikát podepisuje. Jestliže vytváříte nebo obnovujete lokálního CA, vybíráte volbu uložení soukromého klíče hned jako první krok procesu.

Související pojmy

"IBM Cryptographic Coprocessors for iSeries" na stránce 9
Produkt Cryptographic Coprocessor poskytuje ověřené šifrovací služby, které zajišťují soukromí a integritu pro vznikající aplikace e-businessu.

Uložení soukromého klíče certifikátu přímo v koprocesoru

Chcete-li zajistit silnější ochranu přístupu k soukromému klíči certifikátu a jeho použití, můžete tento klíč uložit přímo do produktu IBM Cryptographic Coprocessor. Tento způsob uložení můžete zvolit v rámci procesu vytváření nebo obnovy certifikátu v produktu DCM (Digital Certificate Manager).

Chcete-li uložit soukromý klíč certifikátu přímo do koprocesoru, postupujte na stránce **Vyberte umístění klíče** takto:

1. Jako volbu uložení zvolte **Hardware**.
2. Klepněte na **Pokračovat**. Zobrazí se stránka **Vyberte popis šifrovacího zařízení**.
3. Ze seznamu zařízení vyberte to, které chcete použít pro uložení soukromého klíče certifikátu.
4. Klepněte na **Pokračovat**. Produkt DCM pokračuje v dané úloze a zobrazuje stránky, které je nutno vyplnit, např. identifikační informace pro certifikát, který vytváříte nebo obnovujete.

Použití hlavního klíče koprocesoru pro zašifrování soukromého klíče certifikátu

Chcete-li zajistit silnější ochranu přístupu k soukromému klíči certifikátu a jeho použití, můžete pomocí hlavního klíče produktu IBM Cryptographic Coprocessor soukromý klíč zašifrovat a uložit jej do zvláštního souboru klíčů. Tento způsob uložení můžete zvolit v rámci procesu vytváření nebo obnovy certifikátu v produktu DCM (Digital Certificate Manager).

Abyste mohli tuto volbu úspěšně použít, musíte pomocí webového rozhraní pro konfiguraci produktu IBM Cryptographic Coprocessor vytvořit příslušný soubor pro ukládání klíčů. Pomocí webového rozhraní pro konfiguraci koprocesoru musíte také přiřadit soubor pro ukládání klíčů k popisu koprocesorového zařízení, které chcete používat. Do webového rozhraní pro konfiguraci koprocesoru se dostanete ze Stránky úloh systému iSeries.

Jestliže má váš systém nainstalováno a logicky zapnuto více koprocesorových zařízení, můžete si zvolit, že budete sdílet soukromý klíč certifikátu mezi více zařízeními. Aby mohly popisy zařízení sdílet soukromý klíč, musejí mít všechna tato zařízení stejný hlavní klíč. Proces distribuce stejného hlavního klíče do více zařízení se nazývá *klonování*. Sdílení klíče mezi zařízeními vám umožňuje vyvažovat zatížení SSL (Secure Sockets Layer), což může zlepšit výkon při zabezpečených relacích.

Chcete-li pomocí hlavního klíče koprocesoru zašifrovat soukromý klíč certifikátu a uložit jej do zvláštního souboru pro ukládání klíčů, postupujte na stránce **Vyberte umístění klíče** takto:

1. Jako volbu uložení zvolte **Hardware šifrován**.
2. Klepněte na **Pokračovat**. Zobrazí se stránka **Vyberte popis šifrovacího zařízení**.
3. Ze seznamu zařízení vyberte to, které chcete použít při zašifrování soukromého klíče certifikátu.
4. Klepněte na **Pokračovat**. Pokud máte instalováno a logicky zapnuto více koprocesorových zařízení, zobrazí se stránka **Vyberte popisy dalších šifrovacích zařízení**.

   Poznámka: Pokud nemáte nainstalováno více koprocesorových zařízení, produkt DCM pokračuje v dané úloze a zobrazuje stránky, které je nutno vyplnit, např. identifikační informace pro certifikát, který vytváříte nebo obnovujete.
5. Ze seznamu zařízení vyberte jména jednoho nebo více popisů zařízení, která by měla sdílet soukromý klíč certifikátu.

   Poznámka: Popisy zařízení, které jste vybrali, musejí mít stejný hlavní klíč jako zařízení, které jste vybrali na předchozí stránce. Abyste ověřili, že hlavní klíč těchto zařízení je stejný, použijte úlohu Ověření

hlavního klíče v rámci webového rozhraní pro konfiguraci koprocesoru 4758. Do webového rozhraní pro konfiguraci koprocesoru se dostanete ze Stránky úloh systému iSeries.

6. Klepněte na **Pokračovat**. Produkt DCM pokračuje v dané úloze a zobrazuje stránky, které je nutno vyplnit, např. identifikační informace pro certifikát, který vytváříte nebo obnovujete.

Správa umístění požadavků pro vydavatele certifikátů PKIX

Vydavatel certifikátů (CA) typu PKIX (Public Key Infrastructure X.509) je takový vydavatel certifikátů, který vydává certifikáty založené na nejnovějších internetových standardech pro implementaci infrastruktury veřejných klíčů X.509.

CA, který používá standardy PKIX, vyžaduje předtím, než vydá certifikát, přísnější identifikaci. Obvykle vyžaduje, aby žadatel prokázal svoji totožnost prostřednictvím vydavatele registrace (Registration Authority, RA). Když žadatel dodá vydavateli registrace takový důkaz totožnosti, který RA vyžaduje, potvrdí RA totožnost žadatele. Potom buď RA, nebo žadatel (to záleží na zavedené proceduře daného CA) předá potvrzenou žádost o certifikát příslušnému CA. S tím, jak se použití těchto standardů rozšiřuje, bude k dispozici stále více CA používajících standardy PKIX. Využití CA používajícího standardy PKIX můžete zvážit v případě, že vaše potřeby v oblasti zabezpečení vyžadují přísnou kontrolu přístupu k prostředkům, které poskytují uživatelům aplikace používající SSL. Například produkt Lotus Domino poskytuje vydavatele certifikátů PKIX CA pro veřejné použití.

Pokud se rozhodnete, že vaše aplikace budou používat certifikáty vydané CA používajícím standardy PKIX, můžete tyto certifikáty spravovat pomocí produktu Digital Certificate Manager (DCM). S využitím produktu DCM nakonfigurujete adresu URL pro CA používajícího standardy PKIX. Tím se nakonfiguruje produkt DCM tak, aby nabízel CA používajícího standardy PKIX jako volbu pro získání podepsaného certifikátu.

Chcete-li pomocí produktu DCM spravovat certifikáty od CA používajícího standardy PKIX, musíte nakonfigurovat produkt DCM tak, aby používal umístění tohoto CA. Při konfiguraci postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště vyberte volbu **Správa umístění požadavků PKIX** a zobrazí se vám formulář, do kterého můžete zadat adresu URL pro CA používajícího standardy PKIX nebo jeho příslušného vydavatele registrace (RA).
3. Zadejte úplnou adresu URL pro CA používajícího standardy PKIX, od kterého chcete požadovat certifikáty, například http://www.thawte.com, a klepněte na **Přidat**. Přidáním adresy URL nakonfigurujete produkt DCM tak, že přiřadí CA používajícího standardy PKIX jako volbu pro získání podepsaných certifikátů.

Když přidáte umístění požadavků PKIX pro určitého CA, produkt DCM přidá vydavatele certifikátů PKIX jako volbu při specifikaci typu CA, kterého můžete zvolit pro vydání certifikátu, když pracujete s úlohou **Vytvoření certifikátu**.

Poznámka: Standardy PKIX jsou popsány v RFC (Request For Comments) 2560.

Související pojmy

“Správa certifikátů od veřejného internetového CA” na stránce 45
V této části naleznete informace o správě certifikátů od internetových CA pomocí vytvoření paměti certifikátů.

Správa umístění LDAP pro uživatelské certifikáty

Zde se dozvíte, jak konfigurovat produkt DCM tak, aby ukládal uživatelské certifikáty do umístění serveru adresářů LDAP (Lightweight Directory Access Protocol) a rozšířil tak použití EIM (Enterprise Identity Mapping) pro práci s uživatelskými certifikáty.

Standardně produkt DCM ukládá uživatelské certifikáty, které vydá lokální CA, obvykle společně s uživatelskými profily operačního systému i5/OS. Produkt DCM však můžete nakonfigurovat společně s produktem EIM, což umožňuje, aby poté, co lokální CA vydá uživatelské certifikáty, byla veřejná kopie certifikátu uložena do specifického umístění serveru adresářů LDAP. Nakonfigurování produktu EIM společně s produktem DCM umožňuje ukládat uživatelské certifikáty do umístění adresářů LDAP a umožňuje tak jiným aplikacím snadnější přístup k certifikátům LDAP. Tato společná konfigurace také umožňuje použít produkt EIM ke správě uživatelských certifikátů jako typu totožnosti uživatele v rámci vašeho podniku.

Poznámka: Pokud chcete, aby uživatel uložil certifikát od jiného CA do umístění LDAP, musí tento uživatel provést úlohu **Přiřazení uživatelského certifikátu**.

Produkt EIM představuje technologii @server , která vám ve vašem podniku umožňuje spravovat totožnost uživatelů včetně uživatelských profilů systému i5/OS a uživatelských certifikátů. Chcete-li produkt EIM využít ke správě uživatelských certifikátů, musíte dříve, než provedete jakékoliv úlohy týkající se konfigurace produktu DCM, provést níže uvedené úlohy související s konfigurací produktu EIM:

1. Chcete-li konfigurovat EIM, použijte průvodce **konfigurací EIM** v produktu iSeries Navigator.
2. Vytvořte registr X.509 v doméně produktu EIM pro použití k přidružení certifikátu.
3. Z menu Vlastnosti vyberte volbu Konfigurace pořadače v doméně EIM a zadejte jméno registru X.509.
4. Pro každého uživatele, který se má podílet na EIM, vytvořte identifikátor EIM.
5. Vytvořte cílové přidružení mezi každým identifikátorem EIM a uživatelským profilem příslušného uživatele v lokálním registru uživatelů operačního systému i5/OS. Použijte definiční jméno registru EIM pro lokální registr uživatelů operačního systému i5/OS, které jste zadali v průvodci **konfigurací EIM**.

   Poznámka: Další informace o konfiguraci EIM najdete v tématu EIM (Enterprise Identity Mapping) v rámci aplikace iSeries Information Center.

Po vykonání nezbytných úloh v oblasti konfigurace produktu EIM je nezbytné provést níže uvedené úlohy, kterými dokončíte celkovou konfiguraci, jež umožní spolupráci produktů DCM a EIM.

1. V prostředí produktu DCM použijte úlohu **Správa umístění LDAP** a zadejte adresář LDAP, který bude produkt DCM využívat pro ukládání uživatelských certifikátů, které vytvoří lokální CA. Umístění LDAP se nemusí nacházet na lokálním serveru iSeries a stejný nemusí to být ani server LDAP, který EIM používá. Pokud nakonfigurujete umístění LDAP v produktu DCM, produkt DCM použije zadaný adresář LDAP k ukládání všech uživatelských certifikátů, které lokální CA vydá. Produkt DCM rovněž využívá umístění LDAP k ukládání certifikátů zpracovaných úlohou **Přiřazení uživatelského certifikátu** namísto uložení certifikátu s uživatelským profilem.
2. Spusťte příkaz **CVTUSRCERT** (Convert User Certificates). Tento příkaz zkopíruje existující uživatelské certifikáty do příslušného umístění adresáře LDAP. Příkaz však zkopíruje pouze certifikáty pro uživatele, kteří dříve nastavili cílovou asociaci mezi identifikátorem EIM a příslušným uživatelským profilem. Příkaz poté vytvoří zdrojové přidružení pro každý certifikát a přidružený identifikátor EIM. K definování jména totožnosti uživatele pro zdrojové přidružení příkaz používá rozlišovací jméno (DN) subjektu, DN vydavatele a společně s veřejným klíčem certifikátu také přepočet klíče těchto DN.

Poznámka: Pokud potřebujete anonymní přístup k serveru LDAP, pak musíte použít nástroj Directory Server Web Administration Tool a vybrat úlohu ″Správa schématu″ za účelem změny třídy zabezpečení (která je nazývána rovněž jako ″přístupová třída″) u atributů certificateRevocationList a authorityRevocationList z hodnoty ″kritický″ na hodnotu ″normální″. Pole **Rozlišovací jméno přihlášení** a **Heslo** ponechte prázdná.

Související úlohy

“Digitální certifikáty a produkt EIM (Enterprise Identity Mapping)” na stránce 32
Produkt EIM společně s produktem DCM vám umožní použít certifikát jako zdroj pro operaci vyhledávání během mapování EIM za účelem mapování z certifikátu na cílovou totožnost uživatele, která je přidružena ke stejnému identifikátoru EIM.

Podepisování objektů

Tato část obsahuje informace o tom, jak pomocí produktu DCM spravovat certifikáty, které používáte k digitálnímu podepisování objektů s cílem zajistit integritu objektů.

Existují tři metody, pomocí kterých můžete podepisovat objekty. Můžete napsat program, který bude volat rozhraní pro podepisování objektů (rozhraní Sign Object API). Produkt DCM (Digital Certificate Manager) můžete použít k podepisování objektů. V operačním systému OS/400 V5R2 nebo novější, můžete pomocí produktu iSeries Navigator, funkce Centrální správa, podepisovat objekty, když je balíte za účelem distribuce na jiné servery.

Certifikáty, které spravujete v rámci produktu DCM, můžete použít k podepsání jakéhokoliv objektu, který je uložen v integrovaném systému souborů daného systému, s výjimkou objektů uložených v knihovnách. Podepisovat můžete pouze ty objekty, které jsou uloženy v systému souborů QSYS.LIB: *PGM, *SRVPGM, *MODULE, *SQLPKG a *FILE (pouze záložní soubory). V systému OS/400 V5R2 nebo novější můžete podepisovat i objekty typu příkaz (*CMD). Nelze podepisovat objekty, které jsou uloženy v jiných systémech.

Objekty můžete podepisovat pomocí certifikátů, které zakoupíte od veřejného internetového vydavatele certifikátů (CA) nebo které vytvoříte pomocí soukromého lokálního CA v rámci produktu DCM. Proces podepisování certifikátů je stejný, bez ohledu na to, zda použijete veřejné nebo soukromé certifikáty.

Nezbytné předpoklady pro podepisování objektů

Abyste mohli pomocí produktu DCM (nebo rozhraní Sign Object API) podepisovat objekty, musíte zajistit splnění několika nezbytných předpokladů:

- Musíte mít vytvořenou paměť certifikátů *OBJECTSIGNING, což jste provedli buď v rámci procesu vytvoření soukromého CA, nebo v rámci procesu správy certifikátů pro podepisování objektů od veřejného internetového CA.
- Paměť certifikátů *OBJECTSIGNING musí obsahovat alespoň jeden certifikát, buď ten, který jste vytvořili pomocí soukromého CA, nebo ten, který jste získali od veřejného internetového CA.
- Musíte mít vytvořenu alespoň jednu definici aplikace pro podepisování objektů, kterou budete používat při podepisování objektů.
- K definici aplikace pro podepisování objektů musíte mít přiřazen konkrétní certifikát, který hodláte používat k podepisování objektů.

Podepisování objektů pomocí produktu DCM

Chcete-li pomocí produktu DCM podepsat jeden nebo více objektů, postupujte takto:

1. Spuštění produktu DCM
2. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***OBJECTSIGNING**.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit v průběhu práce s produktem DCM určitý formulář, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.
3. Zadejte heslo pro paměť certifikátů *OBJECTSIGNING a klepněte na **Pokračovat**.
4. Když se obnoví navigační lišta, vyberte volbu **Správa podepsatelných objektů**. Zobrazí se seznam úloh.
5. Ze seznamu vyberte úlohu **Podepsání objektu**. Zobrazí se seznam definicí aplikací, které můžete použít pro podepisování objektů.
6. Vyberte aplikaci, klepněte na **Podepsat objekt** a zobrazí se formulář pro zadání umístění objektu, který chcete podepsat.

   Poznámka: Pokud aplikace, kterou jste vybrali, k sobě nemá přiřazený certifikát, nemůžete ji použít k podepsání objektu. Nejprve musíte použít úlohu **Aktualizace přiřazení certifikátu** v rámci volby **Správa aplikací** a přiřadit certifikát k definici aplikace.
7. Do nabídnutého pole zadejte úplnou cestu a jméno souboru objektu nebo adresáře objektů, které chcete podepsat, a klepněte na **Pokračovat**. Nebo zadejte umístění adresáře, klepněte na **Procházet** a zobrazí se vám obsah adresáře, abyste mohli vybrat objekty pro podepsání.

   Poznámka: Jméno objektu musíte začít úvodním lomítkem, jinak byste mohli narazit na chybu. Pro popis části adresáře, kterou chcete podepsat, můžete také použít určité zástupné znaky. Tyto zástupné znaky jsou hvězdička (*****), která udává ″jakýkoliv počet znaků″, a otazník (**?**), který udává ″jakýkoliv jednotlivý znak″. Pokud např. chcete podepsat všechny objekty v určitém adresáři, můžete zadat /mydirectory/*. Nebo když chcete podepsat všechny programy v určité knihovně, můžete zadat /QSYS.LIB/QGPL.LIB/*.PGM. Tyto zástupné znaky můžete používat pouze v poslední části jména cesty. Zadání např. /mydirectory*/filename by mělo za následek chybovou zprávu. Pokud chcete

použít funkci Procházet, abyste viděli seznam obsahu knihovny nebo adresáře, musíte zadat zástupný znak jako součást jména cesty předtím, než klepnete na **Procházet**.

8. Vyberte volbu zpracování, kterou chcete použít k podepsání vybraného objektu nebo objektů, a klepněte na **Pokračovat**.

   Poznámka: Pokud vyberete volbu, kdy se čeká na výsledky úlohy, zobrazí se soubor s výsledky přímo ve vašem prohlížeči. Výsledky pro aktuální úlohu jsou připojeny ke konci souboru s výsledky. Soubor tudíž kromě výsledků aktuální úlohy může obsahovat výsledky z kterýchkoliv předchozích úloh. Pomocí pole datumu v souboru můžete určit, které řádky souboru se týkají aktuální úlohy. Pole datumu je ve formátu YYYYMMDD. První pole v souboru může být buď ID zprávy (pokud v průběhu zpracování objektu došlo k chybě), nebo pole datumu (udává datum zpracování úlohy).

9. Uveďte úplnou cestu a jméno souboru, do kterého se mají uložit výsledky úlohy podepsání objektu, a klepněte na **Pokračovat**. Anebo zadejte umístění adresáře, klepněte na **Procházet** a zobrazí se vám obsah adresáře, abyste mohli vybrat soubor pro uložení výsledků úlohy. Zobrazí se zpráva, která oznamuje, že úloha pro podepsání objektu byla spuštěna. Výsledky úlohy si můžete prohlédnout v úloze **QOBJSGNBAT** v protokolu úlohy.

Ověřování podpisu objektů

Pomocí produktu DCM (Digital Certificate Manager) lze ověřovat autenticitu digitálních podpisů na objektech. Když ověříte podpis, budete mít jistotu, že data v objektu nebyla změněna poté, co vlastník objektu objekt podepsal.

Nezbytné předpoklady pro ověřování podpisů

Předtím, než můžete pomocí produktu DCM ověřovat podpisy na objektech, musíte zajistit splnění několika nezbytných předpokladů:

- Musíte mít vytvořenou paměť certifikátů *SIGNATUREVERIFICATION pro správu vašich certifikátů pro ověřování podpisů.

  Poznámka: Ověřování podpisu můžete provádět i tehdy, když pracujete v rámci paměti certifikátů *OBJECTSIGNING, a to v případech, kdy ověřujete podpisy pro objekty podepsané ve stejném systému. Kroky, které vykonáváte, když ověřujete podpis v produktu DCM, jsou stejné pro obě paměti certifikátů. Paměť certifikátů *SIGNATUREVERIFICATION však musí existovat a musí obsahovat kopii certifikátu, kterým je objekt podepsán, a to i v případě, že provádíte ověření podpisu v rámci paměti certifikátů *OBJECTSIGNING.

- Paměť certifikátů *SIGNATUREVERIFICATION musí obsahovat kopii certifikátu, kterým jsou objekty podepsané.
- Paměť certifikátů *SIGNATUREVERIFICATION musí obsahovat kopii certifikátu CA pro CA, který vydal certifikát, jímž jsou objekty podepsané.

***Ověřování podpisů na objektech pomocí produktu DCM**

Chcete-li pomocí produktu DCM ověřit podpisy na objektech, postupujte takto:

1. Spusťte produkt DCM.
2. V navigační liště klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***SIGNATUREVERIFICATION**.

   Poznámka: Jestliže máte dotazy k tomu, jak vyplnit v průběhu práce s produktem DCM určitý formulář, vyberte tlačítko otazník (**?**) v horní části stránky, čímž se dostanete do online nápovědy.

3. Zadejte heslo pro paměť certifikátů *SIGNATUREVERIFICATION a klepněte na **Pokračovat**.
4. Když se obnoví navigační lišta, vyberte volbu **Správa podepsatelných objektů**. Zobrazí se seznam úloh.
5. Ze seznamu úloh vyberte **Ověření podpisu objektu**, abyste specifikovali umístění objektů, jejichž podpis chcete ověřit.
6. Do nabídnutého pole zadejte úplnou cestu a jméno souboru objektu nebo adresáře objektů, u kterých chcete ověřit podpisy, a klepněte na **Pokračovat**. Nebo zadejte umístění adresáře, klepněte na **Procházet** a zobrazí se vám obsah adresáře, abyste mohli vybrat objekty pro ověření podpisu.

Poznámka: Pro popis části adresáře, kterou chcete ověřit, můžete také použít určité zástupné znaky. Tyto zástupné znaky jsou hvězdička (*****), která udává ″jakýkoliv počet znaků″, a otazník (**?**), který udává ″jakýkoliv jednotlivý znak″. Pokud např. chcete podepsat všechny objekty v určitém adresáři, můžete zadat /mydirectory/*. Nebo když chcete podepsat všechny programy v určité knihovně, můžete zadat /QSYS.LIB/QGPL.LIB/*.PGM. Tyto zástupné znaky můžete používat pouze v poslední části jména cesty. Zadání např. /mydirectory*/filename by mělo za následek chybovou zprávu. Pokud chcete použít funkci Procházet, abyste viděli seznam obsahu knihovny nebo adresáře, musíte zadat zástupný znak jako součást jména cesty předtím, než klepnete na **Procházet**.

7. Vyberte volbu zpracování, kterou chcete použít při ověření podpisu na vybraném objektu nebo objektech, a klepněte na **Pokračovat**.

   Poznámka: Pokud vyberete volbu, kdy se čeká na výsledky úlohy, zobrazí se soubor s výsledky přímo ve vašem prohlížeči. Výsledky pro aktuální úlohu jsou připojeny ke konci souboru s výsledky. Soubor tudíž kromě výsledků aktuální úlohy může obsahovat výsledky z kterýchkoliv předchozích úloh. Pomocí pole datumu v souboru můžete určit, které řádky souboru se týkají aktuální úlohy. Pole datumu je ve formátu YYYYMMDD. První pole v souboru může být buď ID zprávy (pokud v průběhu zpracování objektu došlo k chybě), nebo pole datumu (udává datum zpracování úlohy).

8. Uveďte úplnou cestu a jméno souboru, který se má použít pro uložení výsledků úlohy ověření podpisu, a klepněte na **Pokračovat**. Anebo zadejte umístění adresáře, klepněte na **Procházet** a zobrazí se vám obsah adresáře, abyste mohli vybrat soubor pro uložení výsledků úlohy. Zobrazí se zpráva, která oznamuje, že úloha pro ověření podpisů objektů byla spuštěna. Výsledky úlohy si můžete prohlédnout v úloze **QOBJSGNBAT** v protokolu úlohy.

Pomocí produktu DCM si také můžete prohlédnout informace o certifikátu, kterým je objekt podepsán. To vám umožní, abyste předtím, než s objektem začnete pracovat, zjistili, zda objekt pochází z důvěryhodného zdroje.

Související pojmy

“Digitální certifikáty pro podepisování objektů” na stránce 34
Tato část vysvětluje, jak lze certifikáty používat k zajištění integrity objektů nebo k ověření digitálního podpisu na objektu za účelem ověření jeho pravosti.

Související úlohy

“Správa certifikátů pro ověřování podpisů na objektech” na stránce 49
Pomocí produktu DCM (Digital Certificate Manager) můžete spravovat certifikáty pro ověřování podpisů, které používáte při ověření platnosti digitálního podpisu na objektech.

Odstraňování problémů s produktem DCM

V této části najdete informace o tom, jak řešit některé nejběžnější problémy, se kterými se při používání produktu DCM můžete setkat.

Při práci s produktem DCM (Digital Certificate Manager) a certifikáty se můžete setkat s chybami, které brání v dokončení vašich úloh a cílů. Mnoho z běžných chyb a problémů, na které můžete narazit, spadá do níže uvedených kategorií.

Odstraňování obecných problémů a problémů s hesly

V následující tabulce naleznete informace, které vám pomohou při odstraňování některých běžnějších problémů s hesly a při řešení jiných obecných problémů, na které můžete narazit při práci s produktem DCM.

Problém	Možné řešení
Nemůžete najít další nápovědu pro práci s produktem DCM.	V produktu DCM klepněte na ″**?**″ - ikonu nápovědy. Můžete také hledat v aplikaci Information Center a na externích webových stránkách IBM na Internetu.
Heslo pro paměť certifikátů lokálního vydavatele certifikátů (CA) nebo *SYSTEM nefunguje.	U hesel rozhoduje velikost písmen. Ověřte si, zda klávesa Caps lock je ve stejné poloze, jako byla při přiřazování hesla.

Problém	Možné řešení
Při pokusu o otevření paměti certifikátů obdržíte chybovou zprávu s tím, že vaše heslo vypršelo.	Musíte změnit heslo pro paměť certifikátů. Pro změnu hesla klepněte na tlačítko **OK**.
Nepodařilo se vám resetovat heslo v rámci úlohy **Výběr paměti certifikátů**.	Funkce resetování funguje pouze tehdy, pokud produkt DCM heslo uložil. Produkt DCM heslo automaticky uloží, když vytvoříte určitou paměť certifikátů. Avšak pokud měníte nebo resetujete heslo paměti certifikátů Jiná systémová paměť certifikátů, pak musíte vybrat volbu **Automatické přihlášení**, aby produkt DCM heslo uložil.
	Také když přesouváte paměť certifikátů z jednoho systému do jiného, musíte v novém systému změnit heslo této paměti certifikátů, abyste zajistili, že produkt DCM heslo automaticky uloží. Když chcete změnit heslo paměti certifikátů a otevíráte ji v novém systému, musíte zadat původní heslo pro tuto paměť. Volbu pro resetování a nastavení hesla nemůžete použít, dokud neotevřete paměť pomocí původního hesla, heslo nezměníte a změněné heslo se neuloží. Pokud se neprovede změna a uložení hesla, produkt DCM a SSL nemohou automaticky heslo obnovit v případech, kdy to různé funkce vyžadují. Jestliže přesouváte nějakou paměť certifikátů, která se bude používat jako Jiná systémová paměť certifikátů, musíte při změně hesla vybrat volbu **Automatické přihlášení**, čímž zajistíte, že DCM nové heslo pro tuto paměť certifikátů uloží.
	Zkontrolujte hodnotu pro atribut **Allow new digital certificates** v rámci volby **Work with system security** v SST (System Service Tools). Jestliže je tento atribut nastaven na hodnotu 2, pak heslo paměti certifikátů nelze resetovat. Hodnotu tohoto atributu si můžete prohlédnout nebo změnit pomocí příkazu STRSST a zadání ID uživatele a hesla pro uživatele SST. Poté zvolte volbu **Work with system security**. ID uživatele SST bývá totožné s ID uživatele QSECOFR.
Nemůžete najít zdroj certifikátu CA, který potřebujete přijmout do systému.	Někteří CA nedávají své certifikáty CA běžně k dispozici. Pokud nemůžete získat od CA jeho certifikát CA, kontaktujte vašeho prodejce VAR, který má možná s CA uzavřenu zvláštní nebo finanční dohodu.
Nemůžete najít paměť certifikátů *SYSTEM.	Umístění souboru s pamětí certifikátů *SYSTEM musí být /qibm/userdata/icss/cert/server/default.kdb. Pokud paměť certifikátů neexistuje, musíte pomocí produktu DCM tuto paměť certifikátů vytvořit. Použijte úlohu **Vytvoření nové paměti certifikátů**.
Obdrželi jste od produktu DCM chybové hlášení a toto hlášení se objevuje stále, i když jste již problém vyřešili.	Vymažte obsah paměti cache vašeho prohlížeče. Nastavte velikost paměti cache na 0 a ukončete a restartujte prohlížeč.
Máte problém se serverem LDAP, např. když se bezprostředně po přiřazení certifikátu zobrazila informace o zabezpečené aplikaci, neobjevilo se přiřazení certifikátu. K tomuto problému dochází častěji, pokud je pro přístup do prohlížeče Netscape Communications používán produkt iSeries Navigator. Preference pro paměť cache prohlížeče je nastavena tak, aby porovnávala dokument v paměti cache s dokumentem v síti **jednou za relaci (Once per session)**.	Změňte předvolenou preferenci tak, aby se paměť cache kontrolovala pokaždé.
Když pomocí produktu DCM importujete certifikát podepsaný nějakým externím CA, jako je např. Entrust, obdržíte chybovou zprávu, že doba platnosti neobsahuje aktuální datum nebo nespadá do doby platnosti vydavatele certifikátů.	Systém používá pro dobu platnosti formát obecného času. Počkejte den a zopakujte operaci. Ověřte také, zda má váš systém nastavenu správnou hodnotu pro ofset UTC (dspsysval qutcoffset). Pokud používáte tzv. letní čas, může být tato hodnota nastavena nesprávně.

Problém	Možné řešení
Když jste se pokoušeli importovat certifikát od CA Entrust, obdrželi jste základní chybu 64.	Certifikát je ve speciálním formátu, jako je např. formát PEM. Pokud funkce kopírování ve vašem prohlížeči nefunguje dobře, je možné, že jste zkopírovali i nějaký materiál navíc, který k certifikátu nepatří, např. prázdné mezery na začátku každé řádky. Pokud je to tento případ, pak certifikát nebude ve správném formátu, když se jej pokusíte použít v systému. Některé webové stránky tento problém způsobují. Jiné webové stránky jsou navrženy tak, aby se tohoto problému vyvarovaly. Určitě porovnejte vzhled originálního certifikátu s výsledným, protože zkopírovaná a vložená informace musí vypadat stejně.

Odstraňování problémů s paměťmi certifikátů a databázemi klíčů

V následující tabulce naleznete informace, které vám pomohou při odstraňování některých běžnějších problémů s paměťmi certifikátů a databázemi klíčů, na které můžete narazit při práci s produktem DCM.

Problém	Možné řešení
Systém nenašel databázi klíčů nebo zjistil, že je neplatná.	Zkontrolujte heslo a jméno souboru a zjistěte, zda nejde o typografickou chybu. Zkontrolujte, zda součástí jména souboru je cesta, včetně úvodního lomítka.

Problém	Možné řešení

Selhalo vytvoření databáze klíčů nebo vytvoření lokálního CA.	Zkontrolujte, zda nejde o konflikt jmen souborů. Konflikt se může týkat i jiného souboru, než toho, o který jste žádali. Produkt DCM se pokouší chránit uživatelská data v adresářích, které vytvoří, dokonce i tehdy, když tyto soubory zabraňují produktu DCM úspěšně vytvořit soubory, které produkt DCM potřebuje.
	
	Tento problém vyřešíte tak, že zkopírujete všechny konfliktní soubory do jiného adresáře a pokud je to možné, vymažete pomocí funkce DCM odpovídající soubory. Pokud to nemůžete provést pomocí produktu DCM, vymažte soubory manuálně z původního adresáře integrovaného systému souborů, kde způsobovaly konflikt s produktem DCM. Vždy si přesně zaznamenejte, které soubory jste přemístili a kam jste je přemístili. Tyto kopie vám umožní obnovit soubory v případě, že zjistíte, že je ještě potřebujete. Musíte vytvořit nového lokálního CA po přesunutí následujících souborů:
	`/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`
	
	Vytvořit novou paměť certifikátů *SYSTEM a systémový certifikát potřebujete po přesunutí následujících souborů:
	`/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`

	Produkt DCM vyžaduje, aby byl nainstalován nezbytný licencovaný program, který vám možná chybí. Zkontrolujte seznam nezbytných předpokladů pro produkt DCM a ujistěte se, že jsou řádně nainstalovány všechny licencované programy.

Problém	Možné řešení
Systém nepřijímá textový soubor CA přenesený binárně z jiného systému. Přijímá soubor, pokud je přenášen v ASCII (American National Standard Code for Information Interchange).	Klíčové řetězce a databáze klíčů jsou binární, a tudíž odlišné. Pro textové soubory CA musíte použít protokol FTP (File Transfer Protocol) v ASCII, a pro binární soubory, což jsou soubory s příponami .kdb, .kyr, .sth, .rdb apod., protokol FTP v binárním režimu.
Nemůžete změnit heslo u databáze klíčů. Certifikát v databázi klíčů už není platný.	Když si ověříte, že problém není ve špatně zadaném hesle, vyhledejte neplatný certifikát nebo certifikáty a vymažte je z paměti certifikátů. Pak zkuste změnit heslo. Pokud máte v paměti certifikátů certifikáty s ukončenou platností, tyto certifikáty již nejsou platné. Protože certifikáty nejsou platné, funkce změny hesla pro danou paměť certifikátů nemusí povolit změnu hesla a šifrovací proces nezašifruje soukromé klíče certifikátů s ukončenou platností. To znemožňuje provést změnu hesla a systém může hlásit, že jedním z důvodů je poškození paměti certifikátů. Musíte odstranit neplatné certifikáty (tj. certifikáty s ukončenou platností) z paměti certifikátů.
Certifikáty potřebujete použít pro internetového uživatele, a tudíž potřebujete použít ověřovací seznamy, ale produkt DCM funkce pro ověřovací seznamy neposkytuje.	Obchodní partneři, kteří programují aplikace pro použití ověřovacích seznamů, musí aplikaci naprogramovat tak, aby se ověřovací seznam přiřadil k jejich aplikaci dle očekávání. Musí také naprogramovat kód, který určuje, kdy je totožnost internetového uživatele správně prověřena tak, aby mohl být certifikát přidán do ověřovacího seznamu. V rámci aplikace Information Center si můžete prostudovat téma Rozhraní QsyAddVldlCertificate API. V dokumentaci k produktu HTTP Server for iSeries najdete informace o tom, jak konfigurovat zabezpečené instance HTTP serveru pro použití ověřovacích seznamů.

Odstraňování problémů s prohlížečem

V následující tabulce naleznete informace, které vám pomohou při odstraňování některých běžnějších problémů souvisejících s prohlížečem, na které můžete narazit při práci s produktem DCM.

Problém	Možné řešení
Prohlížeč Microsoft Internet Explorer vám neumožní vybrat jiný certifikát, dokud nespustíte novou relaci prohlížeče.	Zahajte novou relaci prohlížeče Internet Explorer.
Internet Explorer nezobrazí v seznamu pro výběr všechny klientské/uživatelské certifikáty, které jsou způsobilé pro výběr. Internet Explorer zobrazí pouze certifikáty vydané důvěryhodnými CA, které můžete použít na zabezpečeném počítači.	Daný CA musí být uveden jako důvěryhodný v databázi klíčů a rovněž mu musí důvěřovat zabezpečená aplikace. Ujistěte se, že jste se na PC přihlásili do prohlížeče Internet Explorer pomocí stejného uživatelského jména, jako je to, které uvedl uživatelský certifikát v prohlížeči. Ze systému, k němuž přistupujete, získejte další uživatelský certifikát. Systémový administrátor si musí být jist, že paměť certifikátů (databáze klíčů) ještě stále důvěřuje CA, který podepsal uživatelský a systémový certifikát.
Prohlížeč Internet Explorer 5 obdrží certifikát CA, ale nemůže soubor otevřít nebo najít disk, na který jste certifikát uložili.	Toto je nová funkce prohlížeče týkající se certifikátů, kterým ještě prohlížeč Internet Explorer nedůvěřuje. Můžete vybrat umístění na vašem PC.
Obdrželi jste varování prohlížeče, že jméno systému a systémový certifikát si neodpovídají.	Některé prohlížeče používají odlišné postupy při porovnávání jmen systému, pokud jde o velká a malá písmena. Napište adresu URL přesně stejnými písmeny, jak to ukazuje systémový certifikát. Nebo vytvořte systémový certifikát pomocí takových písmen, která odpovídají tomu, co většina uživatelů používá. Pokud si nejste jisti, je nejlepší ponechat jméno serveru nebo jméno systému tak, jak bylo. Také musíte zkontrolovat, zda je správně nastaven váš server jmen domény.

Problém	Možné řešení
Prohlížeč Internet Explorer jste spustili pomocí HTTPS namísto HTTP a obdrželi jste varování, že došlo ke smíchání zabezpečené a nezabezpečené relace.	Potvrďte a ignorujte toto varování. V dalším vydání prohlížeče Internet Explorer je již tento problém vyřešen.
Prohlížeč Netscape Communicator 4.04 for Windows konvertoval v polské kódové stránce hexadecimální hodnoty A1 a B1 na B2 a 9A.	Jde o chybu prohlížeče, která má dopad na NLS. Použijte jiný prohlížeč nebo použijte stejnou verzi tohoto prohlížeče, ale na jiné platformě, např. Netscape Communicator 4.04 for AIX.
Prohlížeč Netscape Communicator for 4.04 zobrazil v uživatelském profilu znaky NLS velkých písmen v uživatelském certifikátu správně, ale znaky malých písmen nesprávně.	Některé národní znaky zadané správně jako jeden znak nejsou ale při pozdějším zobrazení tím stejným znakem. Například u prohlížeče Netscape Communicator 4.04 pro operační systém Windows byly hexadecimální hodnoty A1 a B1 konvertovány pro polskou kódovou stránku na B2 a 9A, což má za následek zobrazení jiných znaků NLS.
Prohlížeč stále sděluje uživateli, že daný CA není důvěryhodný.	Pomocí produktu DCM nastavte **Stav CA** na **Povolený**, čímž daného CA označíte jako důvěryhodného.
Prohlížeč Internet Explorer požaduje zamítnout připojení pro HTTPS.	Jde o problém související s funkcí prohlížeče nebo jeho konfigurace. Prohlížeč se rozhodl nepřipojit k systému používajícímu systémový certifikát, který mohl být podepsaný sám sebou nebo který by nemusel být platný z nějakého jiného důvodu.
Servery a prohlížeče Netscape Communicator používají zdrojové certifikáty společností, jako je např. VeriSign, což je jedna z funkcí komunikace SSL - konkrétně autentizace. Platnost veškerých zdrojových certifikátů vždy po určitém období vyprší. Platnost některých zdrojových certifikátů prohlížečů a serverů Netscape vypršela mezi 25. prosincem 1999 a 31. prosincem 1999. Pokud jste tento problém nevyřešili do 14. prosince 1999, obdržíte chybovou zprávu.	Nižší verze prohlížeče (Netscape Communicator 4.05 nebo nižší) mají certifikáty, jejichž platnost vždy vyprší. Musíte přejít na vyšší, současnou verzi prohlížeče Netscape Communicator. Informace o zdrojových certifikátech prohlížeče jsou k dispozici na mnoha webových stránkách, včetně http://home.netscape.com/security/ a http://www.verisign.com/server/cus/rootcert/webmaster.html. Volné stažení prohlížeče je k dispozici na webových stránkách http://www.netcenter.com.

Odstraňování problémů s produktem HTTP Server for iSeries

Problém	Možné řešení
Nefunguje HTTPS (Hypertext Transfer Protocol Secure).	Ujistěte se, že je HTTP server správně nakonfigurován pro použití SSL. Ve verzi V5R1 nebo v pozdějších verzích musí mít konfigurační soubor prostřednictvím administračního rozhraní HTTP serveru nastavenu hodnotu **SSLAppName**. V konfiguraci také musí být obsažen virtuální hostitelský systém, který používá port SSL, přičemž virtuální hostitelský systém musí mít používání **SSL** nastaveno na **Povoleno**. Dále musí existovat dvě direktivy **Listen**, které specifikují dva různé porty: jeden, který používá SSL, a druhý, který nepoužívá SSL. Tyto volby se nastavují na stránce **Obecné nastavení**. Ujistěte se, že je vytvořena instance serveru a že serverový certifikát je podepsán.

Problém	Možné řešení
Potřebujete objasnit proces registrace instance HTTP serveru jako zabezpečené aplikace.	Na serveru přejděte do administračního rozhraní HTTP serveru, abyste mohli nastavit konfiguraci HTTP serveru. Nejprve musíte nadefinovat virtuální hostitelský systém, abyste povolili používání SSL. Poté, co nadefinujete virtuální hostitelský systém, musíte zadat, že virtuální hostitelský systém používá port SSL definovaný dříve v rámci direktivy pro **Listen** (na stránce **Obecné nastavení**. Dále musíte prostřednictvím stránky **SSL with Certificate Authentication** v rámci volby **Security** povolit SSL pro dříve nakonfigurovaný hostitelský systém. Všechny změny musí být zaneseny do konfiguračního souboru. Všimněte si, že při registraci instance se automaticky nevybere certifikát, který pak instance bude používat. Prostřednictvím produktu DCM musíte určitý certifikát přiřadit vaší aplikaci předtím, než se pokusíte ukončit a restartovat instanci serveru.
Máte problémy, když u HTTP serveru nastavujete ověřovací seznam a volitelnou autentizaci klientů.	V publikaci k produktu HTTP Server for iSeries najdete volby pro nastavení instance.
Prohlížeč Netscape Communicator předtím, než vám povolí vybrat jiný certifikát, čeká, až platnost konfigurační direktivy v kódu HTTP serveru vyprší.	Velká hodnota certifikátu způsobuje, že je obtížné registrovat druhý certifikát, protože prohlížeč ještě stále používá ten první.
Pokoušíte se prostřednictvím prohlížeče předložit HTTP serveru certifikát X.509, abyste ho mohli použít jako vstup pro rozhraní QsyAddVldlCertificate.	Musíte použít nastavení **SSLEnable** a **SSLClientAuth ON**, aby HTTP server zavedl proměnnou prostředí HTTPS_CLIENT_CERTIFICATE. Informace o těchto rozhraních API můžete nalézt ve Vyhledávači rozhraní API v rámci aplikace Information Center. Můžete se také podívat na tyto ověřovací seznamy nebo rozhraní API související s certifikáty: • QsyListVldlCertificates a QSYLSTVC • QsyRemoveVldlCertificate a QRMVVC • QsyCheckVldlCertificate a QSYCHKVC • QsyParseCertificate a QSYPARSC, a tak dále.
HTTP server má dlouhou dobu odezvy nebo časové prodlevy v případě, že požadujete seznam certifikátů v ověřovacím seznamu a existuje zde více než 10.000 položek.	Vytvořte dávkovou úlohu, která vyhledává a vymazává certifikáty odpovídající určitým kritériím, např. takové, kterým vypršela platnost, nebo certifikáty od určitého CA.
HTTP server se nespustí, pokud je volba **SSL** nastavena na **Povoleno** a v protokolu úlohy se zobrazí chybová zpráva HTP8351. Při selhání HTTP serveru protokol chyb HTTP serveru uvádí chybu, že operace inicializace SSL selhala s návratovým kódem chyby 107.	Chyba číslo 107 znamená, že platnost certifikátu vypršela. Pomocí produktu DCM přiřaďte aplikaci jiný certifikát, například QIBM_HTTP_SERVER_SERVER. Pokud instance serveru, kterou se nepodařilo spustit, je server *ADMIN, pak dočasně nastavte volbu **SSL** na hodnotu Zablokováno, abyste mohli použít produkt DCM na serveru *ADMIN. Poté pomocí produktu DCM přiřaďte aplikaci QIBM_HTTP_SERVER_ADMIN jiný certifikát a zkuste opět nastavit volbu **SSL** na **Povoleno**.

Odstraňování problémů s přiřazením uživatelského certifikátu

Když pracujete s úlohou **Přiřazení uživatelského certifikátu**, produkt DCM (Digital Certificate Manager) vám zobrazí informace o certifikátu, abyste je potvrdili, než se certifikát zaregistruje. Pokud produkt DCM není schopen zobrazit certifikát, mohl by být problém způsoben některou z těchto situací:

1. Váš prohlížeč nepožádal, abyste vybrali certifikát, který se předloží serveru. K tomu může dojít, jestliže má prohlížeč v paměti cache ještě předchozí certifikát (z přístupu na jiný server). Pokuste se vymazat v prohlížeči obsah paměti cache a zkuste úlohu provést znovu. Prohlížeč vás vyzve, abyste vybrali certifikát.
2. Toto se může stát také pokud nakonfigurujete váš prohlížeč tak, že nezobrazí seznam voleb, a prohlížeč obsahuje pouze jeden certifikát od CA (vydavatele certifikátů) ze seznamu vydavatelů certifikátů, kterým server důvěřuje. Ověřte nastavení konfigurace vašeho prohlížeče a pokud je to třeba, změňte jej. Prohlížeč vás poté vyzve, abyste

vybrali certifikát. Pokud nemůžete předložit certifikát od CA, kterému server dle nastavení důvěřuje, nelze certifikát přiřadit. Kontaktujte svého administrátora produktu DCM.

3. Certifikát, který chcete registrovat, již je v produktu DCM registrován.
4. Vydavatel certifikátu, který vydal daný certifikát, není v systému nebo v dané aplikaci specifikován jako důvěryhodný. Certifikát, který předkládáte, tudíž není platný. Kontaktujte svého systémového administrátora, aby určil, zda CA, který vydal váš certifikát, je vhodný. Jestliže je CA vhodný, bude muset systémový administrátor pravděpodobně **Importovat** certifikát CA do paměti certifikátů *SYSTEM. Nebo může administrátor použít volbu **Nastavit stav CA** a nastavit CA jako důvěryhodný zdroj, což problém vyřeší.
5. Nemáte certifikát pro registraci. Můžete zkontrolovat uživatelské certifikáty ve vašem prohlížeči a zjistit, zda problém není tady.
6. Platnost certifikátu, který se pokoušíte registrovat, vypršela, nebo je certifikát nekompletní. Musíte buď obnovit certifikát, nebo kontaktovat CA, který vydal certifikát, aby problém vyřešil.
7. IBM HTTP Server for i5/OS není správně nastaven, aby prováděl registraci certifikátů za použití SSL a autentizaci klientů na zabezpečené instanci administračního serveru. Pokud žádná z uvedených rad nepomůže, kontaktujte vašeho systémového administrátora a nahlaste mu svůj problém.

Abyste provedli úlohu **Přiřazení uživatelského certifikátu**, musíte se napojit na produkt Digital Certificate Manager (DCM) prostřednictvím relace SSL. Pokud při výběru úlohy **Přiřazení uživatelského certifikátu** nepoužijete SSL, produkt DCM zobrazí zprávu, že musíte SSL použít. Zpráva obsahuje tlačítko, pomocí kterého se napojíte na DCM prostřednictvím SSL. Pokud se zpráva zobrazí bez tohoto tlačítka, informujte o tomto problému vašeho systémového administrátora. Aby se zajistilo, že konfigurační direktivy pro použití SSL jsou aktivované, bude možná potřeba restartovat webový server.

Související úlohy

“Přiřazení uživatelského certifikátu” na stránce 41
Uživatelský certifikát, který vlastníte, můžete přiřadit k vašemu uživatelskému profilu v operačním systému i5/OS nebo k identitě uživatele. Certifikát může pocházet i od soukromého lokálního CA v jiném systému, nebo od veřejného CA. Abyste mohli přiřadit certifikát k totožnosti uživatele, musí server vydávajícímu CA důvěřovat a tento certifikát nesmí být přiřazen k jinému uživatelskému profilu nebo totožnosti uživatele v systému.

Související informace o produktu DCM

Na této stránce naleznete odkazy na další zdroje, kde je možno získat informace o digitálních certifikátech, infrastruktuře veřejných klíčů, produktu DCM a dalších souvisejících tématech.

S tím, jak se použití digitálních certifikátů všeobecně rozšiřuje, rozšiřují se také dostupné zdroje informací. Uvádíme zde alespoň krátký seznam dalších zdrojů, kde můžete získat informace o digitálních certifikátech a o tom, jak lze s jejich pomocí zlepšit zásady zabezpečení ve vašem systému:

- **Další informace najdete na webových stránkách VeriSign Help Desk** . Na webových stránkách je k dispozici rozsáhlá knihovna věnovaná problematice digitálních certifikátů i řadě dalších témat týkajících se bezpečnosti Internetu.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements**

  SG24-6168 Tato červená kniha IBM se zaměřuje na OS/400 vylepšení zabezpečení sítě ve verzi V5R1. Naleznete zde mnoho témat, např. jak využívat funkce pro podepisování objektů v produktu DCM v operačním systému iSeries, jak využít podporu kryptografického koprocesoru 4758 pro SSL a řadu dalších.

- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)** Tato červená kniha popisuje, jak lze využít digitální certifikáty na serveru iSeries. Je zde vysvětleno, jak nastavit různé servery a klienty, aby používaly certifikáty. Dále poskytuje informace a vzorový kód k tomu, jak pomocí rozhraní API operačního systému OS/400 spravovat a používat digitální certifikáty v uživatelských aplikacích.

- **RFC Index Search** Na těchto webových stránkách naleznete úložiště RFC (Request for Comments), ve kterém lze vyhledávat. RFC popisují standardy pro internetové protokoly jako je SSL, PKIX a další, které se týkají použití digitálních certifikátů.

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí nabízet produkty, služby a funkce popsané v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou momentálně dostupné ve vaší oblasti, můžete získat od obchodního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba IBM. Použít lze jakýkoli funkčně ekvivalentní produkt, program či službu neporušující práva IBM k duševnímu vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Vlastnictví tohoto dokumentu vám nedává k těmto patentům žádná práva. Písemné dotazy ohledně licencí můžete zaslat na adresu:

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

S dotazy ohledně licencí týkajícími se informací v dvoubajtové znakové sadě (DBCS) se obraťte na IBM Intellectual Property Department ve své zemi nebo zašlete písemně dotaz na adresu:

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

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují lokálním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, "JAKÁ JE", BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH VČETNĚ, MIMO JINÉ, ODVOZENÝCH ZÁRUK PORUŠENÍ ZÁKONŮ, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řády některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk v určitých transakcích a proto se na vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uvedené jsou pravidelně aktualizovány a v nových vydáních této publikace již budou tyto změny zahrnuty. IBM má právo kdykoliv bez upozornění zdokonalovat anebo měnit produkt(y) anebo program(y) popsané v této publikaci.

Jakékoliv odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoli závazků vůči vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

IBM poskytuje licencovaný program popsaný v těchto informacích a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě na programy, v Mezinárodní licenční smlouvě IBM na strojový kód nebo v jiné ekvivalentní smlouvě.

Veškeré údaje o výkonu, které jsou na v tomto dokumentu uvedeny, byly stanoveny v řízeném prostředí. Výsledky získané v jiných provozních prostředích se proto mohou významně lišit. Některá měření mohla být prováděna v systémech na úrovni vývoje a v těchto případech nelze zaručit, že tato měření budou stejná ve všeobecně dostupných systémech. Kromě toho mohla být některá měření odhadnuta prostřednictvím extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by si měli ověřit použitelnost dat pro svoje specifické prostředí.

Veškerá prohlášení týkající budoucích trendů nebo strategií IBM podléhají změnám bez předchozího upozornění a představují pouze cíle a záměry.

Všechny uváděné ceny IBM jsou maloobchodní ceny navržené společností IBM, jsou nyní platné a mohou se bez upozornění změnit. Ceny prodejců se mohou lišit.

Tyto publikace obsahují příklady údajů a sestav používaných v každodenních obchodních činnostech. Za účelem co nejpřesnější ilustrace obsahují tyto příklady jména osob, společností, značek a produktů. Všechna tato jména jsou smyšlená a jakákoliv podobnost se jmény a adresami používanými ve skutečném podniku je čistě náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Tyto ukázkové programy můžete bez závazků vůči IBM jakýmkoliv způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto vzorové programy nebyly důkladně testovány za všech podmínek. Proto IBM nemůže zaručit ani naznačit spolehlivost, provozuschopnost ani funkčnost těchto programů.

Každá kopie a libovolná část těchto ukázkových programů nebo jakékoli odvozené dílo musí obsahovat tuto copyrightovou výhradu:

Jestliže si prohlížíte tyto informace ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

Ochranné známky

Níže uvedené výrazy jsou ochrannými známkami společnosti International Business Machines Corporation ve Spojených státech a případně v dalších jiných zemích.

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

| Lotus
| Net.Data
| OS/400

Microsoft, Windows a logo Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

Ostatní jména společností, produktů a služeb mohou být ochrannými známkami nebo servisními značkami jiných firem.

Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

Komerční použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoliv informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN NEBO ZÁRUKY VHODNOSTI PRO URČITÝ ÚČEL.

Vytištěno v Dánsku společností IBM Danmark A/S.