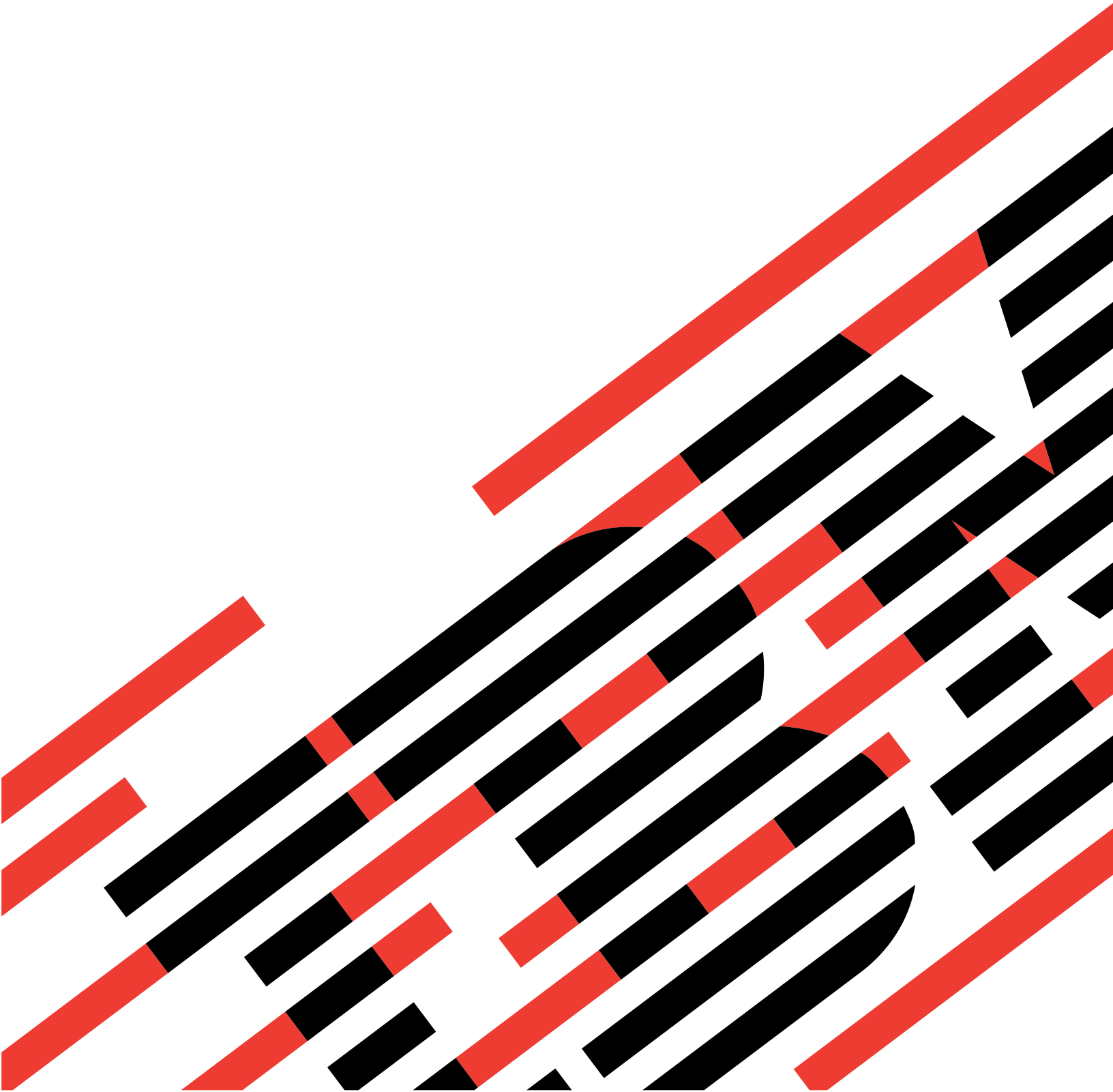
IBM

eserver

iSeries

Digital Certificate Manager



IBM

@server

iSeries

Digital Certificate Manager

Obsah

Část 1. Produkt Digital Certificate Manager

Digitální certifikát je elektronický prostředek pro ověřování, který lze použít, pokud je nutno v elektronické transakci provádět prokazování identity. 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. Podporu SSL dnes v rámci zajišťování privátnosti dat poskytují mnohé služby a aplikace iSeries, např. FTP, Telnet, HTTP Server for iSeries, i mnoho dalších produktů.

Systém 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 v systému iSeries je snadné, jestliže k centrální správě certifikátů pro vaše aplikace použijete Digital Certificate Manager (DCM), bezplatně dodávanou funkci systému iSeries. 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:

Co je nového ve verzi V5R2
Tato část obsahuje informace o tom, k jakým funkčním změnám došlo v novém vydání produktu Digital Certificate Manager a k jakým změnám došlo v rozsahu a struktuře informací pro toto téma.

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

Migrace z předcházející verze produktu DCM
V této části jsou vysvětleny úlohy, které musíte provést při migraci z vaší existující verze produktu DCM na současnou verzi produktu, a další aspekty, které je při migraci nutno uvážit.

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 strategie zabezpečení systému iSeries. U každého scénáře jsou uvedeny rovněž všechny potřebné konfigurační úlohy, které musíte provést, aby bylo možno scénář použít tak, jak bylo popsáno.

Princip digitálních certifikátů
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.

Plánování použití produktu DCM
Tato část obsahuje informace, které vám pomohou při rozhodování, jak a kdy byste měli 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.

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.

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).

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

Související informace o produktu DCM
Na této straně jsou odkazy na další zdroje, kde je možno získat informace o digitálních certifikátech, infrastruktuře veřejných klíčů, produktu Digital Certificate Manager a dalších souvisejících tématech.

Kapitola 1. Co je nového ve verzi V5R2

K funkčním zdokonalením verze V5R2 produktu Digital Certificate Manager (DCM) a systému iSeries v oblasti digitálních certifikátů patří:

- **Funkce Přiřazení certifikátu**
  Tato nová úloha v produktu DCM vám umožní rychleji a snadněji přiřadit certifikát k jedné nebo více aplikacím. Tuto úlohu můžete spustit buď ze seznamu úloh **Správa certifikátů**, nebo ze stránek **Práce se serverem a certifikáty** a **Práce s certifikáty pro podepisování objektů**. Tato funkce je dostupná pouze pro paměti certifikátů *SYSTEM a *OBJECTSIGNING.
- **Podepisování příkazových objektů (*CMD)**
  Nyní můžete produkt DCM použít i k vytvoření digitálního podpisu na příkazových objektech (*CMD), čímž získáte prostředek pro ověřování jejich integrity. Můžete také zvolit rozsah podpisu pro objekty *CMD: buď můžete podepsat celý objekt *CMD, nebo můžete podepsat pouze základní komponenty objektu *CMD. Jestliže pomocí produktu DCM zobrazujete podpis na objektech *CMD, produkt DCM poskytne informace o rozsahu podpisu.
- **API pro vytvoření uživatelského certifikátu podepsaného lokálním vydavatelem certifikátů bez použití produktu DCM**
  K dispozici jsou dvě nová API, která můžete použít k programovému vydávání certifikátů podepsaných vaším lokálním vydavatelem certifikátů pro jiné uživatele než uživatele systému iSeries. Tato API vám umožní vydávat certifikáty pro uživatele bez uživatelského profilu iSeries. Uživatelé tak mohou získat certifikát pro autentizaci klienta, aniž by museli používat produkt DCM.

Nové nebo zdokonalené informace o tomto tématu zahrnují:

- Dva nové scénáře, které vám mohou pomoci při stanovení optimálního způsobu použití certifikátů tak, aby byly splněny vaše cíle v oblasti zabezpečení.
- Témata jsou reorganizována tak, abyste byli schopni rychle vyhledat ty informace, které při používání produktu DCM právě potřebujete.

Další informace o tom, co je nového nebo co bylo změněno v této verzi produktu, naleznete v tématu Memo to Users  .

Kapitola 2. Tisk tohoto tématu

Pokud chcete soubor typu PDF prohlížet nebo stáhnout, zvolte Digital certificate Manager

 (velikost souboru je cca 468 KB nebo cca 110 stran).
Pokud chcete soubor typu PDF uložit na svou pracovní stanici za účelem prohlížení nebo tisku:

1. Otevřete soubor typu PDF pomocí svého prohlížeče (klepněte na výše uvedený odkaz).
2. V menu vašeho prohlížeče klepněte na volbu **Soubor**.
3. Klepněte na **Uložit jako...**
4. Vyhledejte adresář, do něhož chcete soubor typu PDF uložit.
5. Klepněte na **Uložit**.

Pokud potřebujete ke stažení nebo prohlížení souboru typu PDF produkt Adobe Acrobat Reader, můžete si kopii tohoto produktu stáhnout z domovské stránky firmy Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Kapitola 3. Migrace z předchozí verze produktu DCM

Když migrujete z verze V4R3 produktu Digital Certificate Manager (DCM) na verzi V5R2, produkt DCM provede automaticky aktualizaci vašeho existujícího lokálního vydavatele certifikátu (CA) a souborů klíčového řetězce systémových certifikátů. Produkt DCM tyto soubory, které se jmenují default.kyr, aktualizuje na odpovídající paměti certifikátů, které se jmenují default.kdb. Produkt DCM také provede migraci všech platných certifikátů v souborech klíčového řetězce, které jsou asociované se servery HTTP (Hypertext Transfer Protocol) a LDAP (Lightweight Directory Access Protocol). Produkt DCM provede migraci platných certifikátů do paměti certifikátů *SYSTEM (default.kdb).

Poznámka: Pokud migrujete z verzí V4R4, V4R5 nebo V5R1 produktu DCM, nemusíte žádné migrační úlohy provádět, protože soubory certifikátů z těchto verzí jsou kompatibilní s verzí V5R2 produktu DCM.

Migrace klíčového řetězce na paměť certifikátů – migrace z verze V4R3

V průběhu instalace verze V5R2 produktu DCM provede systém migraci následujících souborů klíčového řetězce:
- Soubory předvoleného klíčového řetězce produktu DCM.
- Klíčové řetězce používané konfiguračními soubory serveru HTTP.
- Klíčové řetězce používané konfiguračními soubory serveru LDAP.

Pokud používáte nějaký soubor .kyr, který produkt DCM automaticky neaktualizoval, produkt DCM jej konvertuje na soubor kyr.kdb, když s ním budete v produktu DCM poprvé pracovat. Když například v uživatelském rozhraní DCM poprvé zadáte soubor secure.kyr, produkt DCM provede konverzi souboru na novou paměť certifikátů se jménem souboru secure.kyr.kdb.

Poznámka: Klíčové řetězce se od pamětí certifikátů liší, proto musíte soubory klíčových řetězců, které produkt DCM neaktualizuje automaticky, konvertovat zvlášť pomocí uživatelského rozhraní DCM. Pouhá manuální změna přípony jména souborů na .kdb by měla za následek chybový stav, když byste se následně pokoušeli s těmito soubory pracovat v uživatelském rozhraní produktu DCM.

Jestliže se pokusíte vymazat soubor secure.kyr, když pracujete s produktem DCM, produkt DCM ve skutečnosti tento soubor zaarchivuje a vymaže soubor secure.kyr.kdb.

Předvolené heslo místa uložení certifikátů

Jestliže soubor /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR existuje, systém provede migraci tohoto souboru klíčového řetězce a všech ostatních způsobilých souborů klíčového řetězce do místa uložení certifikátů *SYSTEM. Původní heslo, přiřazené k souboru /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR, je použito jako heslo pro paměť certifikátů *SYSTEM.

Jestliže soubor /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR neexistuje, ale existují jiné soubory klíčových řetězců způsobilé pro migraci (např. soubory klíčového řetězce používané konfiguračními soubory serveru HTTP), systém vytvoří paměť certifikátů *SYSTEM s heslem DEFAULT (všechna písmena velká) a dokončí migraci.

Bližší informace k chybám, které se mohou vyskytnout během procesu migrace souborů, a informace jak tyto chybové stavy řešit viz Řešení chybových stavů a obnovy při migraci.

Kapitola 4. Scénáře použití produktu DCM

Produkt Digital Certificate Manager (DCM) a podpora pro digitální certifikáty, kterou poskytuje váš systém iSeries, vám umožňuje 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 spojení s vašimi 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 dále použít pro přiřazení certifikátu uživatele k jeho uživatelskému profilu v systému iSeries. Certifikát má pak stejné oprávnění a povolení jako přiřazený 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 pro použití digitálních certifikátů 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. Prostudování těchto scénářů vám může pomoci určit takový způsob použití certifikátů, který vzhledem k vašim potřebám optimálně zvýší zabezpečení vašeho systému:

Scénář: Použití certifikátů za účelem ochrany přístupu k veřejným aplikacím a zdrojům
V tomto scénáři je popsáno, kdy a jak použít certifikáty, chcete-li chránit a omezovat přístup veřejných uživatelů k veřejným nebo extranetovým zdrojům a aplikacím.

Scénář: Použití certifikátů za účelem ochrany přístupu k interním aplikacím a zdrojům
V tomto scénáři je popsáno, kdy a jak použít certifikáty, chcete-li chránit zdroje a aplikace na interních serverech a omezit v tomto smyslu přístupy interních uživatelů.

Scénář: Použití certifikátů za účelem ochrany přístupu k veřejným aplikacím a zdrojům

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 uživatelského přístupu k aplikaci, než je vaše současná metoda využívající uživatelská jména a hesla. Máte obavy, že by neautorizovaní uživatelé mohli tuto informaci zachytit při jejím přenosu přes nedůvěryhodnou síť. Někteří pojišťovací agenti by také 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. Certifikáty 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. V této době bude možno k autentizaci používat ještě současných uživatelských jmen a hesel, protože SSL poskytuje citlivým datům při přenosu dostatečnou ochranu.

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

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 privátní.
- Použitím digitálních certifikátů pro autentizaci klientů, v co největší míře to bude možné, poskytnete autorizovaným uživatelům bezpečnější metodu identifikace. A i když to nebude možné, autentizace na základě uživatelského jména a hesla bude díky relaci SSL chráněna a zachována privátní, takže výměna těchto citlivých dat bude bezpečnější.
- Použití *veřejných* digitálních certifikátů pro omezení nebo povolení přístupu k vašim aplikacím a datům 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 (CA) kvůli velkému počtu uživatelů, kteří přistupují k vašim aplikacím a zdrojům, nebo z jiných administrativních důvodů.
- 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. Většina klientských softwarů obsahuje certifikáty CA pro většinu známých vydavatelů certifikátu.

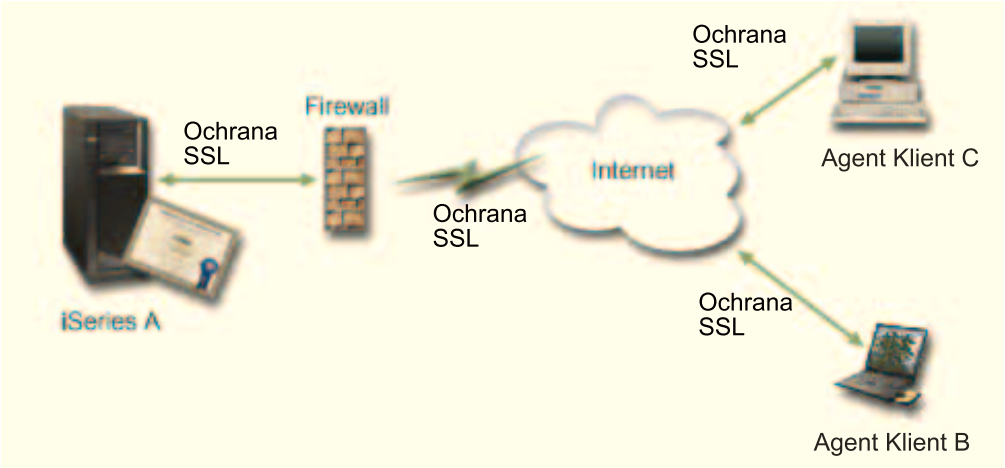
Cíle

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 se zajistila ochrana a privátnost dat, které aplikace uživatelům poskytuje.
- Konfigurace SSL musí být provedena pomocí veřejného certifikátu od známého veřejného internetového vydavatele certifikátů (CA).
- 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 (CA), nebo platné uživatelské jméno a heslo.

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.
- Na serveru iSeries A běží operační systém OS/400 verze 5, vydání 2 (V5R2).
- Server iSeries A má nainstalovanou komponentu pro kryptografický přístup (5722–AC3).
- Server iSeries A má nainstalovaný a nakonfigurovaný produkt Digital Certificate Manager (OS/400 volba 34) a server IBM HTTP Server for iSeries (5722–DG1).
- Na serveru iSeries A běží aplikace pro výpočet pojistných sazeb, která je nakonfigurovaná tak, že:
  - Vyžaduje režim SSL.
  - Používá pro konfiguraci SSL veřejný certifikát od známého vydavatele certifikátů (CA).
  - Vyžaduje autentizaci uživatelů pomocí uživatelského jména a hesla.
- Když se klienti B a C přihlašují k aplikaci, 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 ověřil svoji identitu a inicializoval relaci SSL.
- Klientský software na klientech B a C je konfigurovaný tak, aby byl schopen akceptovat certifikát ze serveru iSeries A a zahájit relaci 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:
1. Aplikace pro výpočet pojistných sazeb na serveru iSeries A je generická aplikace, která může být nakonfigurovaná pro použití SSL. Většina aplikací, včetně mnohých aplikací iSeries, poskytují podporu pro 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.
2. *Volitelně* může být aplikace nastavena tak, aby požadovala při autentizaci klientů certifikáty. Tento scénář poskytuje instrukce k tomu, jak pomocí produktu Digital Certificate Manager (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.
3. Server iSeries A splňuje požadavky pro nainstalování a použití produktu Digital Certificate Manager (DCM).
4. Na serveru iSeries A doposud nikdo nekonfiguroval a nepoužíval produkt DCM.
5. 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.
6. Server iSeries A nemá nainstalovaný kryptografický koprocesor IBM 4758-023 PCI Cryptographic Coprocessor.

Kroky scénáře

Při realizaci tohoto scénáře musíte provést na serveru iSeries A tyto úlohy:

1. Zajistěte všechny nezbytné podmínky týkající se instalace a konfigurace všech potřebných produktů na serveru iSeries.
2. Pomocí produktu Digital Certificate Manager (DCM) vytvořte žádost o serverový certifikát.
3. Nakonfigurujte vaši aplikaci pro použití SSL (Secure Sockets Layer).
4. Pomocí produktu DCM proveďte import a přiřazení podepsaného serverového nebo klientského certifikátu k ID vaší aplikace.
5. Spusťte aplikaci v režimu SSL, je-li to nezbytné.
6. *Volitelná úloha*: Pomocí produktu DCM definujte seznam důvěryhodných CA, čímž umožníte aplikacím, které tuto podporu poskytují, autentizaci klientů na základě certifikátů.

Poznámka: Situace, kterou popisuje tento scénář, nevyžaduje, aby aplikace pro výpočet pojistných sazeb používala při autentizaci klientů certifikáty. 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.

Podrobnosti konfigurace

Chcete-li používat certifikáty pro konfiguraci chráněného veřejného přístupu k aplikacím a zdrojům způsobem, který je popsán v tomto scénáři, postupujte takto:

Krok 1: Proveďte nezbytné předchozí úlohy a instalujte všechny potřebné produkty na serveru iSeries

Abyste mohli začít s konkrétními úlohami při realizaci tohoto scénáře, musíte nejprve splnit všechny nezbytné podmínky týkající se instalace a konfigurace potřebných produktů na serveru iSeries.

Krok 2: Vytvořte žádost o serverový nebo klientský certifikát

Předtím, než budete moci začít používat SSL (Secure Sockets Layer) pro ochranu datové komunikace aplikace tak, jak popisuje tento scénář, musíte získat digitální certifikát od veřejného vydavatele certifikátů (CA). K vytvoření informace, kterou veřejný vydavatel certifikátů vyžaduje pro vydání certifikátu, použijete produkt Digital Certificate Manager (DCM).

Chcete-li získat certifikát, postupujte takto:

1. Spusťte produkt DCM.
2. V navigačním rámu produktu DCM vyberte volbu **Vytvoření nové paměti certifikátů**, čímž spustíte vedenou úlohu a zobrazí se vám 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 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.
8. Pošlete formulář žádosti nebo soubor vydavateli CA, kterého jste si zvolili pro vydání a podepsání vašeho certifikátu.
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.

Krok 3: Nakonfigurujte aplikaci pro použití SSL

Když obdržíte podepsaný certifikát od veřejného vydavatele certifikátů (CA), můžete pokračovat v procesu nastavení SSL komunikace u vaší veřejné aplikace. Aplikaci byste měli 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 Digital Certificate Manager (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 applications with SSL v rámci aplikace Information Center.

Krok 4: Importujte a přiřaďte podepsaný veřejný certifikát

Jestliže jste nakonfigurovali aplikaci pro použití SSL, můžete nyní pomocí produktu Digital Certificate Manager (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 navigačním rámu 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 rám, 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 příslušný certifikát a klepněte na volbu **Přiřazení k aplikacím**. Zobrazí se seznam definicí 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 privátnosti dat, které aplikace poskytuje.

Krok 5: Spusťte aplikaci v režimu SSL

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

Volitelný krok 6: Pro aplikaci, která vyžaduje při autentizaci klientů certifikáty, definujte seznam důvěryhodných CA

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

V situaci, kterou popisuje tento scénář, se nevyžaduje, aby aplikace pro výpočet pojistných sazeb používala při autentizaci klientů certifikáty. 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 navigačním rámu 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 rám, 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 certifikát CA, kterému by aplikace měla důvěřovat, a klepněte na **Povolit**. Zobrazí se seznam aplikací, které používají seznam důvěryhodných CA.
7. Vyberte ze seznamu aplikaci, které 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 za účelem ochrany přístupu k interním aplikacím a zdrojům

Situace

Jste správcem sítě v nějaké společnosti (MyCo., Inc.), jejíž personální oddělení řeší problémy právních otázek a privátnosti 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. A vy máte na starosti správu těchto interních webových stránek.

Protože se zaměstnanci nacházejí na dvou různých pracovištích a někteří zaměstnanci často cestují, musíte zajistit, aby se zachovala privátnost informací při jejich přenosu po Internetu. Při omezování přístupu k podnikovým datům tradičně používáte autentizaci pomocí uživatelského jména a hesla. Vzhledem k citlivosti a privátnosti těchto informací si však uvědomujete, že omezení přístupu k informacím na základě hesla nebude 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 CA, vydávat certifikáty všem zaměstnancům a přiřadit certifikáty zaměstnanců k jejich uživatelským profilům v systému iSeries. Tento typ implementace soukromých certifikátů vám umožní pevněji řídit přístup k citlivým datům a také zajistit privátnost 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 přenášená mezi serverem a klientem bude chráněná a privátní.
- Použitím digitálních certifikátů při autentizaci klientů poskytnete autorizovaným uživatelům bezpečnější metodu identifikace.
- Použití *soukromých* digitálních certifikátů pro omezení nebo povolení přístupu 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 v systému 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 uživatelskému profilu v systému 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.

Cíle

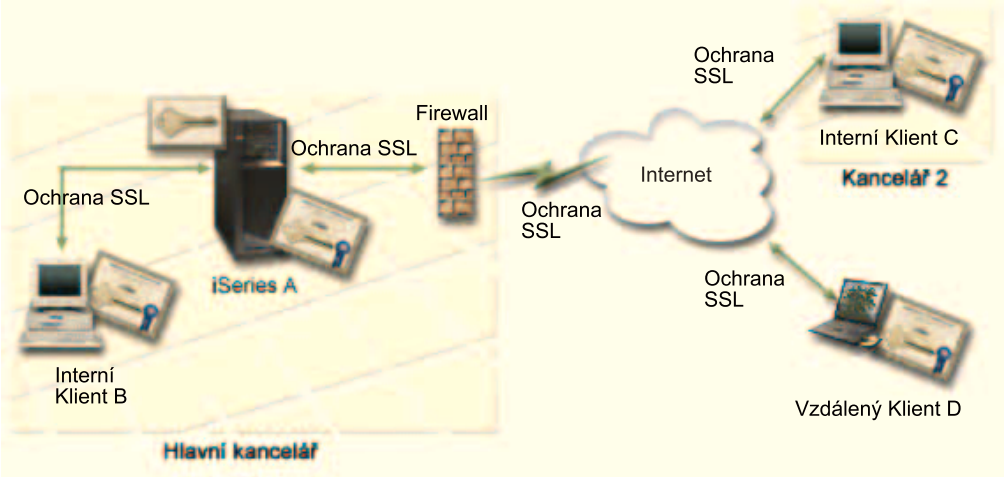
V tomto scénáři chce společnost MyCo., Inc. pomocí digitálních certifikátů zajistit ochranu personálních informací, které jejich interní webové stránky poskytují podnikovým zaměstnancům. Společnost chce také bezpečnější metodu autentizace těch uživatelů, kteří mají k těmto webovým stránkám oprávněný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

Cíle tohoto scénáře jsou následující:

- Interní podnikové webové stránky s personálními informacemi musí používat SSL, aby se zajistila ochrana a privátnost 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 webový server pro personální informace – iSeries A
- Server iSeries A je hostitelský server podnikové webové aplikace pro personální informace.
- Na serveru iSeries A běží operační systém OS/400 verze 5, vydání 2 (V5R2).
- Server iSeries A má nainstalovanou komponentu pro kryptografický přístup (5722–AC3).
- Server iSeries A má nainstalovaný a nakonfigurovaný produkt Digital Certificate Manager (OS/400 volba 34) a server IBM HTTP Server for iSeries (5722–DG1).
- Na serveru iSeries A běží aplikace pro personální informace, která je nakonfigurovaná tak, že:
  - Vyžaduje režim SSL.
  - Používá pro konfiguraci SSL soukromý certifikát od lokálního vydavatele certifikátů (CA).
  - Vyžaduje při autentizaci klientů certifikáty.
- Když se klienti B, C a D přihlašují k aplikaci, server iSeries A předkládá svůj certifikát, aby zahájil relaci SSL.
- Když se spustí relace SSL, požaduje server iSeries A předtím, než povolí přístup k aplikaci pro personální informace, aby klienti B, C a D předložili platný certifikát. Výměna certifikátů je pro uživatele klientů B, C a D transparentní.

Klientské systémy uživatelů – klient B, klient C a klient D
- Klient B je zaměstnanec, který pracuje na ředitelství společnosti MyCo, kde se nachází i server iSeries A.
- Klient C je zaměstnanec, který pracuje na pobočce společnosti MyCo, která se nachází na jiném místě než ředitelství společnosti.
- Klient D je zaměstnanec, který pracuje v terénu, často jezdí na pracovní cesty a musí mít zajištěn bezpečný přístup na webové stránky s personálními informacemi bez ohledu na místo, kde se nachází.

- Klienti B, C a D jsou zaměstnanci podniku, kteří mají přístup k aplikaci pro personální informace.
- Klienti B, C, a D mají ve svém klientském softwaru nainstalovánu kopii lokálního certifikátu vydavatele certifikátů (CA), který vydal certifikát aplikace.
- Klienti B, C, a D přistupují k aplikaci pro personální informace na serveru iSeries A, který jejich klientskému softwaru předkládá svůj certifikát, aby ověřil svoji identitu a inicializoval relaci SSL.
- Klientský software na klientech B, C a D je konfigurovaný tak, aby byl schopen akceptovat certifikát ze serveru iSeries A a zahájit relaci SSL.
- Když se spustí relace SSL, klienti B, C a D musí předložit platný certifikát, a pak teprve server iSeries A povolí přístup k aplikaci a jejím zdrojům.

Nezbytné podmínky a předpoklady

Nezbytné podmínky a předpoklady pro realizaci uvedeného scénáře jsou tyto:

1. Aplikace pro personální informace běží na serveru IBM HTTP Server for iSeries v systému iSeries A. Existují dva typy serveru HTTP Server for iSeries (původní verze a verze provozovaná na bázi Apache) a po publikaci těchto informací bude dostupná značně zrevidovaná verze HTTP serveru. V tomto scénáři proto 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.
2. HTTP server musí mít schopnost požadovat při autentizaci klientů certifikáty. Tento scénář poskytuje pokyny k tomu, jak pomocí produktu Digital Certificate Manager (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.
3. HTTP server personálních informací v systému iSeries A již používá zabezpečení formou hesel.
4. Server iSeries A splňuje požadavky pro nainstalování a použití produktu Digital Certificate Manager (DCM).
5. Na serveru iSeries A doposud nikdo nekonfiguroval a nepoužíval produkt DCM.
6. 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.
7. Server iSeries A nemá nainstalovaný kryptografický koprocesor IBM 4758-023 PCI Cryptographic Coprocessor.

Kroky scénáře

Při realizaci tohoto scénáře musíte provést dvě skupiny úloh: V první skupině budete nastavovat aplikaci pro personální informace v systému iSeries tak, aby používala SSL a požadovala při autentizaci klientů certifikáty. Druhá skupina úloh umožní uživatelům klientů B, C a D, aby se mohli podílet na relacích SSL s aplikací pro personální informace a aby získali certifikáty pro autentizaci uživatelů.

Úlohy na webovém serveru aplikace pro personální informace

Při realizaci tohoto scénáře musíte provést na serveru iSeries A tyto úlohy:

1. Zajistěte všechny nezbytné podmínky týkající se instalace a konfigurace všech potřebných produktů na serveru iSeries.
2. Nakonfigurujte HTTP server personálních informací pro použití SSL a poznamenejte si ID aplikace pro instanci serveru.
3. Pomocí produktu Digital Certificate Manager (DCM) vytvořte lokálního CA a použijte ho k vydání certifikátu pro HTTP server personálních informací. V rámci této vedené

úlohy rovněž přiřadíte certifikát aplikaci webového serveru a přidáte lokálního CA do seznamu těch CA, kterým má aplikace důvěřovat.
4. Nakonfigurujte webový server personálních informací tak, aby požadoval certifikáty při autentizaci klientů.
5. Spusťte HTTP server personálních informací v režimu SSL.

Úlohy na klientech

Chcete-li realizovat tento scénář, je nutno, aby každý uživatel (klienti B, C a D), který bude mít přístup k webovému serveru personálních informací v systému iSeries, provedl tyto úlohy:
6. Nainstalujte kopii certifikátu lokálního CA do svého prohlížeče.
7. Vyžádejte si certifikát od lokálního CA.

Podrobnosti konfigurace

Chcete-li používat certifikáty pro konfiguraci chráněného přístupu k interním aplikacím a zdrojům způsobem, který je popsán v tomto scénáři, postupujte takto:

Krok 1: Proveďte nezbytné předchozí úlohy a instalujte všechny potřebné produkty na serveru iSeries

Abyste mohli začít s konkrétními úlohami při realizaci tohoto scénáře, musíte nejprve splnit všechny nezbytné podmínky týkající se instalace a konfigurace potřebných produktů na serveru iSeries.

Krok 2: Nakonfigurujte HTTP server personálních informací pro použití SSL

Konfigurace SSL (Secure Sockets Layer) u HTTP serveru personálních informací v systému iSeries A se bude lišit podle toho, zda používáte původní verzi HTTP serveru nebo verzi provozovanou na bázi Apache.

Podrobné informace o konfiguraci HTTP serveru (původní verze) pro použití SSL uvádí téma Konfigurování zabezpečeného serveru na HTTP serveru.

Podrobné informace o konfiguraci HTTP serveru (provozovaného na bázi Apache) pro použití SSL uvádí téma Scénář: JKL aktivuje ochranu pomocí SSL na HTTP serveru (provozovaném na bázi Apache). V tomto scénáři je uveden kompletní postup vytvoření virtuálního hostitelského systému a jeho konfigurace pro použití SSL. Konkrétní postup při konfiguraci SSL uvádí téma ″Aktivace SSL pro virtuální hostitelský systém.″

Další informace o konfigurování jak současných, tak budoucích verzí produktu HTTP Server for iSeries (původních verzí nebo verzí provozovaných na bázi Apache) uvádí téma Služby Web.

Krok 3: Vytvořte a provozujte lokálního vydavatele certifikátů (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 kterého vydáte certifikát pro server.

Když pomocí produktu DCM vytvářítе lokálního CA, provádíte 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 navigačním rámu 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), a to konkrétně:
   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, že lokální CA může 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 podúloha 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 by měly 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.

Nyní, když jste provedli konfiguraci certifikátu, který vaše aplikace webového serveru potřebuje pro SSL, můžete nakonfigurovat aplikaci webového serveru tak, aby požadovala při autentizaci uživatelů certifikáty.

Krok 4: Nakonfigurujte webový server personálních informací tak, aby požadoval při autentizaci klientů certifikáty

Konfigurace SSL u HTTP serveru personálních informací na serveru iSeries A tak, aby požadoval při autentizaci uživatelů certifikáty, se bude lišit podle toho, zda používáte původní verzi HTTP serveru nebo verzi provozovanou na bázi Apache.

Podrobné informace o konfiguraci HTTP serveru (původní verze) tak, aby požadoval při autentizaci klientů certifikáty, uvádí téma Nastavení ochrany na HTTP serveru (původní).

Podrobné informace o konfiguraci HTTP serveru (provozovaného na bázi Apache) pro použití certifikátů při autentizaci uživatelů uvádí téma Scénář: JKL aktivuje ochranu pomocí SSL na HTTP serveru (provozovaném na bázi Apache). V tomto scénáři je uveden kompletní postup vytvoření virtuálního hostitelského systému a jeho konfigurace pro použití SSL a certifikátů při autentizaci klientů. Konkrétní postup při konfiguraci SSL a použití certifikátů při autentizaci klientů uvádí téma ″Aktivace SSL pro virtuální hostitelský systém″.

Další informace o konfigurování jak současných, tak budoucích verzí produktu HTTP Server for iSeries (původních verzí nebo verzí provozovaných na bázi Apache) uvádí téma Služby Web.

Krok 5: Spusťte webový server personálních informací 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 znovu spustit.

Při zastavení a opětovném spuštění HTTP serveru (původní verze) použijte formuláře Configuration and Administration a postupujte takto:
1. Klepněte na **Administration**.
2. Klepněte na **Manage HTTP servers**.
3. Vyberte server.
4. Do pole formuláře zadejte volitelné parametry spuštění.
5. Klepněte na **Start**.

Poznámka: Jestliže byl server spuštěný, když jste prováděli přiřazení certifikátu, měli byste server zastavit a spustit. Použijete-li volbu **Restart**, není zaručeno, že bude server schopen určit změny certifikátů, ke kterým došlo, když byl spuštěný.

Při zastavení a opětovném spuštění HTTP serveru provozovaném na bázi Apache použijte formuláře Configuration and Administration a postupujte takto:
1. Klepněte na **Administration**.
2. V menu nalevo klepněte na **Manage HTTP Servers** v rámci **General Server Administration**.
3. Vyberte server, se kterým chcete pracovat, pak klepněte na **Start** nebo **Stop**. V online nápovědě získáte další informace o parametrech spuštění.

Další informace o správě současných a budoucích verzí produktu HTTP Server for iSeries (původní verze nebo verze provozované na bázi Apache) uvádí téma Služby Web.

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

Krok 6: Uživatelé si nainstalují kopii certifikátu lokálního CA do svého prohlížeče

Když uživatelé přistupují na server, který používá připojení přes SSL (Secure Sockets Layer), předloží server klientskému softwaru uživatele certifikát jako důkaz své identity. Klientský software musí certifikát serveru 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, měl by prohlížeč nebo jiný klientský software uživatele již kopii certifikátu CA mít. Pokud ale, jak je tomu v tomto scénáři, server

předloží certifikát od soukromého lokálního CA, musí si každý uživatel pomocí produktu Digital Certificate Manager (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 navigačním rámu 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. Tak 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 Digital Certificate Manager.

Krok 7: Uživatelé si vyžádají 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 produkt Digital Certificate Manager (DCM) a v něm 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 navigačním rámu 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 Digital Certificate Manager automaticky přiřadí certifikát k vašemu uživatelskému profilu v systému iSeries.

Kapitola 5. Princip digitálních certifikátů

Předtím, než začnete používat digitální certifikáty v rámci rozšíření strategie zabezpečení vašeho systému a sítě, měli byste dobře chápat význam certifikátů a jaké bezpečnostní přínosy poskytují.

Digitální certifikát je digitální doklad, který potvrzuje platnost identity vlastníka certifikátu, podobně jako např. cestovní pas. Důvěryhodná strana, zvaná vydavatel certifikátů (CA), vydává digitální certifikáty uživatelům a serverovým nebo klientským aplikacím. Důvěra ve vydavatele certifikátů je základem důvěry v certifikát jako platný doklad.

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

Rozpoznané jméno
V této části najdete bližší informace o identifikačních charakteristikách digitálních certifikátů.

Digitální podpisy
V této části je vysvětleno, co to jsou digitální podpisy a jak fungují při zajišťování integrity objektů.

Dvojice veřejného a soukromého klíče
Tato část obsahuje informace o bezpečnostních klíčích přidružených k digitálním certifikátům.

Vydavatel certifikátů (CA)
V této části jsou informace o vydavatelích certifikátů, to jest entitách, které vydávají digitální certifikáty.

Umístění CRL
Tato část vysvětluje, co je to seznam odvolaných certifikátů (Certificate Revocation List, CRL) a jak se tyto seznamy využívají v procesu potvrzování a autentizace certifikátů.

Paměti certifikátů
V této části je vysvětleno, co je to paměť certifikátů a jak používat produkt DCM při práci s nimi a s certifikáty, které obsahují.

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

SSL (Secure Sockets Layer)
V této části naleznete stručné informace o šifrovací technologii SSL.

Rozpoznané jméno

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.

Rozpoznané jméno (Distinguished name, DN) je termín, který popisuje identifikační informace vlastníka certifikátu a je součástí certifikátu samotného. 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
- město
- stát
- země

Pokud pomocí produktu DCM vydáváte soukromé certifikáty, můžete pro certifikát uvádět v DN další informace:
- duplicitní IP adresa
- plně kvalifikované jméno domény
- adresa elektronické pošty

Tyto dodatečné informace jsou užitečné, pokud plánujete používat certifikáty ke konfiguraci spojení s VPN (virtual private network).

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 identitou 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 systém iSeries 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, ve skutečnosti však 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.

Dvojice veřejného a soukromého klíče

Každý digitální certifikát má dvojici přiřazených šifrovacích klíčů. Tato dvojice klíčů obsahuje jeden soukromý klíč a jeden veřejný klíč. (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.

Vydavatel certifikátů (CA)

Vydavatel certifikátů (CA) je důvěryhodná centrální administrativní 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 spravovat certifikáty jak od veřejných, tak od soukromých CA.

Produkt DCM můžete také použít k tomu, abyste provozovali vlastního soukromého CA a vydávali soukromé certifikáty pro systémy a uživatele. Když CA vydá certifikát uživatele, produkt DCM automaticky přiřadí tento certifikát k uživatelskému profilu daného uživatele v systému iSeries. 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 v paměti certifikátů. 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 vydavatele certifikátů (CA) pomocí programu Digital Certificate Manager, můžete uvést pro CA strategická data. Strategická data CA popisují podepisovací oprávnění, která CA má. Strategická data určují:
- Zda může CA vydávat a podepisovat uživatelské certifikáty.
- Jak dlouho jsou certifikáty vydané vydavatelem certifikátů platné.

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.

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.

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 v kryptografickém koprocesoru (produkt 4758 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 IFS a souborům IFS, z nichž se skládá paměť 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 ke zdrojům.

***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 pro systém 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 na serveru iSeries nainstalovaný kryptografický koprocesor 4758 PCI Cryptographic Coprocessor, můžete si zvolit jiné možnosti pro uložení soukromých klíčů 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.

Šifrování

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 **veřejnými 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.

SSL (Secure Sockets Layer)

SSL (Secure Sockets Layer), původně vytvořený firmou Netscape, je průmyslový standard 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.

Kapitola 6. Plánování použití produktu DCM

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 použití produktu DCM
Tato část popisuje, jaký software musíte mít nainstalován, a obsahuje další informace týkající se nastavení vašeho systému tak, abyste mohli používat produkt DCM.

Typy digitálních certifikátů
V této části najdete informace o různých typech certifikátů, které můžete pomocí produktu DCM spravovat.

Používání veřejných certifikátů versus vydávání soukromých certifikátů
V této části je vysvětleno, jak určit, který typ certifikátu bude optimální vzhledem k vašim obchodním potřebám, poté co se rozhodnete, že chcete certifikáty používat a využít výhod dodatečného zabezpečení, jež poskytují. 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.

Digitální certifikáty pro komunikaci SSL (Secure Sockets Layer)
Tato část vysvětluje, jak certifikáty používat k tomu, aby vaše aplikace mohly vytvářet zabezpečené komunikační relace.

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

Digitální certifikáty pro autentizaci spojení s VPN (virtual private network)
V této části je vysvětleno, jak lze certifikáty používat jako součást konfigurace spojení s 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.

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.

Požadavky pro nastavení produktu DCM

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

- Nainstalujte licencovaný program pro kryptografický přístup (5722–AC3). Tento šifrovací produkt určuje maximální délku klíčů, která je povolena pro šifrovací algoritmus na základě omezení exportu a importu. Tento produkt musíte mít nainstalován předtím, než můžete vytvářet certifikáty.
- V operačním systému OS/400 nainstalujte volbu 34. Tato volba obsahuje produkt DCM založený na prohlížeči.
- Nainstalujte produkt IBM HTTP Server for iSeries (5722–DG1) a spusťte instanci serveru *ADMIN.

- Ujistěte se, že je v systému nakonfigurován protokol TCP, abyste mohli pro přístup k funkci DCM používat webový prohlížeč a instanci HTTP Server *ADMIN.

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.

Typy digitálních certifikátů

Existuje několik kategorií digitálních certifikátů. Tyto kategorie vycházejí ze způsobu použití certifikátů. Pomocí produktu DCM (Digital Certificate Manager) můžete spravovat tyto typy certifikátů:

Certifikáty vydavatele certifikátů (CA)
Certifikát vydavatele certifikátů je digitální doklad identity vydavatele certifikátů (CA), který vlastní certifikát. Certifikát CA obsahuje identifikační informace o daném CA a také jeho veřejný klíč. Ostatní mohou použít veřejný klíč certifikátu CA k tomu, aby si ověřili autenticitu certifikátů, které tento CA vydává a podepisuje. Certifikát vydavatele certifikátů může být podepsán jiným CA, jako je např. VeriSign, nebo může být podepsán sám sebou, jedná-li se o nezávislou entitu. CA vytvořený pomocí produktu Digital Certificate Manager je nezávislý. Ostatní mohou použít veřejný klíč certifikátu CA k tomu, aby si ověřili autenticitu certifikátů, které tento CA vydává a podepisuje. Chcete-li určitý certifikát použít pro SSL, podepisování objektů nebo ověřování podpisů na objektech, musíte mít také kopii certifikátu pro toho 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. rozpoznané 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 certifikát serveru 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 identity 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 uživatelů v systému iSeries. Pomocí produktu DCM můžete rovněž k uživatelskému profilu v systému iSeries přiřadit certifikát vydaný jiným vydavatelem certifikátů.

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

Poznámka: Jestliže máte na serveru iSeries nainstalován kryptografický koprocesor IBM 4758 PCI, můžete se rozhodnout pro jinou možnost uložení soukromých klíčů certifikátů (s výjimkou certifikátů pro podepisování objektů). Můžete si zvolit uložení soukromých klíčů do koprocesoru samotného. Nebo můžete pomocí 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.

Používání veřejných certifikátů versus vydávání soukromých certifikátů

Jakmile se rozhodnete používat certifikáty, měli byste 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 CA a vydávat soukromé certifikáty pro své uživatele a aplikace.
- Používat kombinaci certifikátů od veřejných internetových CA a vašeho vlastního 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 novější 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 vydávat certifikáty jen 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 byste měli rovněž brát v úvahu administrativní 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 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 CA vám umožňuje vydávat certifikáty pouze těm uživatelům, kteří jsou důvěryhodnými členy vaší pracovní skupiny. To poskytuje lepší zabezpečení, protože můžete s větší přísností řídit, kdo má certifikáty a kdo má tudíž přístup k vašim zdrojům. Potenciální nevýhodou udržování lokálního CA je množství času a zdrojů, 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, zda budete chtít, aby certifikáty uživatelů byly přidruženy k jejich uživatelskému profilu v systému iSeries. Jestliže zvolíte variantu, že certifikáty budou přidruženy k uživatelskému profilu v systému iSeries, uživatelé budou moci získávat certifikáty od lokálního CA pomocí produktu DCM. Nebo můžete, počínaje verzí V5R2, pomocí rozhraní API vydávat certifikáty jiným uživatelům než uživatelům systému iSeries, takže uživatelé nemusí mít uživatelský profil v systému iSeries, aby mohli při autentizaci klientů používat soukromé certifikáty.

Poznámka: Bez ohledu na to, kterého CA zvolíte pro vydávání certifikátů, řídí systémový administrátor, kterým CA by měly 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. Jestliže však certifikát tohoto CA není uložen v paměti certifikátů *SYSTEM, nemůže váš server důvěřovat uživatelskému nebo klientskému certifikátu, který byl tímto CA vydán. Má-li uživatelskému certifikátu vydanému určitým CA důvěřovat, musíte od CA obdržet kopii certifikátu 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:

- Vytváření 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.
- Použití lokálního CA na jiných serverech iSeries popisuje úlohy, které musíte provést, pokud budete používat certifikáty od soukromého CA ve více systémech než v jednom.

Digitální certifikáty pro bezpečnou komunikaci SSL

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 privátnosti 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 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 zdrojům, prokázal svoji identitu. Aby bylo možno k prokázání identity 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.

Digitální certifikáty pro autentizaci uživatelů

Tradičně uživatelé získávají přístup ke zdrojům 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 certifikát uživatele k jeho uživatelskému profilu v systému iSeries. Certifikát má pak stejná oprávnění a povolení jako přiřazený profil. Počínaje verzí V5R2 můžete používat rozhraní API a pomocí soukromého lokálního vydavatele certifikátů vydávat certifikáty i uživatelům jiných systémů než systému iSeries. Tato API vám umožní vydávat soukromé certifikáty uživatelům v případech, kdy nebudete chtít, aby tito uživatelé měli uživatelský profil v systému iSeries.

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 identitu 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 poskytují podporu pro autentizaci klientů prostřednictvím certifikátů tyto aplikace iSeries:

- Telnet server
- IBM HTTP server (původní i provozovaný na bázi Apache)
- LDAP (Directory Services) server

- Management Central
- Client Access Express (včetně produktu iSeries 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 privátnosti 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 privátnosti přenosu dat použitím SSL (Secure Sockets Layer) při zašifrování komunikačních relací.

Další informace o tom, jak nakonfigurovat aplikace systému iSeries, aby během relací SSL používaly při autentizaci klientů certifikáty, uvádí téma Zabezpečení aplikací pomocí SSL.

Digitální certifikáty pro spojení s VPN

Digitální certifikáty můžete použít jako prostředek pro vytvoření spojení s VPN (virtual private network) systému 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.

Před verzí V5R1 se servery IKE mohly navzájem autentizovat pouze prostřednictvím předem sdílených klíčů. Použití předem sdílených klíčů je 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 spojení s 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 rozpoznaném jménu i informaci o alternativním jménu subjektu, jako je např. jméno domény nebo adresa elektronické pošty. Pokud použijete k vydání certifikátu funkci soukromého vydavatele certifikátů, obsaženou v produktu DCM, můžete u certifikátu specifikovat informaci o alternativním jménu subjektu. Specifikací této informace zajistíte, že bude spojení s VPN systému iSeries kompatibilní s jinými implementacemi VPN, které by mohly tuto informaci při autentizaci vyžadovat.

Další informace o správě certifikátů při spojení s 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 pro 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).

Digitální certifikáty pro podepisování objektů

Počínaje verzí V5R1 poskytuje operační systém OS/400 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 iSeries pro 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 detekování 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 jejich privátnosti, 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 si dále vyhodnotit, zda používat veřejné certifikáty nebo vydávat soukromé certifikáty. Hodláte-li distribuovat objekty uživatelům

z řad široké veřejnosti, měli byste 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.

Digitální certifikáty pro ověřování podpisů na objektech

Počínaje verzí V5R1 poskytuje systém iSeries 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, 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.

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. Když se rozhodnete důvěřovat určitému CA, 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.

Ověření systémové hodnoty pro obnovu objektů (QVFYOBJRST)

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. 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 IFS. Další informace o použití této systémové hodnoty uvádí téma System Value Finder v rámci aplikace 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.

Kapitola 7. Konfigurace produktu DCM

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 rámy: navigační rám a rám úloh.

Navigační rám se používá k volbě úloh, pomocí kterých se spravují certifikáty nebo aplikace, které certifikáty používají. V hlavním navigačním rámu 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 navigačním rámu 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 navigačním rámu 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 navigačním rámu k dispozici, závisí na paměti certifikátů, ve které zrovna pracujete. Kategorie a počet úloh, které v navigačním rámu vidíte, se dále mění v závislosti na oprávněních vašeho uživatelského profilu v systému iSeries. Veškeré úlohy týkající se provozování CA, správy certifikátů, které používají aplikace, a další úlohy systémové úrovně jsou dostupné pouze pro správce systému nebo administrátory systému 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:

Spuštění produktu DCM
V této části je vysvětleno, jak se dostanete k funkci Digital Certificate Manager v systému iSeries.

Prvotní nastavení certifikátů
Tato část popisuje, jak v produktu DCM provést veškerá prvotní nastavení tak, abyste mohli začít používat certifikáty. Dovíte se, jak začít spravovat certifikáty od veřejného internetového vydavatele certifikátů (CA) a jak vytvořit a provozovat soukromého CA pro vydávání certifikátů.

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

Abyste mohli začít používat funkce produktu Digital Certificate Manager (DCM), musíte DCM 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).

   Nainstalujte produkt 5722 DG1. Toto je IBM HTTP Server for iSeries.

   Nainstalujte produkt 5722 AC3. Toto je šifrovací produkt, který produkt DCM verze V5R2 používá ke generování dvojic veřejných a soukromých klíčů certifikátů, aby se mohly zašifrovat soubory exportovaných certifikátů a dešifrovat soubory importovaných certifikátů.
2. Pomocí produktu iSeries Navigator spusťte instanci HTTP Server *ADMIN:
   a. Spusťte produkt **iSeries Navigator**.
   b. Dvakrát klepněte na váš server iSeries v hlavním stromovém zobrazení.
   c. Dvakrát klepněte na **Síť**.
   d. Dvakrát klepněte na **Servery**.
   e. Dvakrát klepněte na **TCP/IP**.
   f. Klepněte pravým tlačítkem myši na **Správa HTTP**.
   g. Klepněte na **Start**.
3. Spusťte váš webový prohlížeč.
4. Pomocí prohlížeče přejděte na stránku úloh ve vašem systému iSeries na adrese http://*jméno_vašeho_systému*:2001.
5. Když vyberete volbu **Digital Certificate Manager** ze seznamu produktů na stránce úloh systému iSeries, spustí se produkt DCM.

Pokud migrujete z předchozích verzí produktu DCM, získáte na této stránce podrobnosti, které budete potřebovat při přechodu na vyšší verzi vašeho systému.

Prvotní nastavení certifikátů

Levý rám v produktu Digital Certificate Manager (DCM) je navigační rám úloh. V tomto rámu můžete vybírat z široké škály úloh pro správu certifikátů a aplikací, které certifikáty používají. To, které úlohy jsou v tomto rámu k dispozici, závisí na paměti certifikátů, kterou jste otevřeli (pokud jste nějakou otevřeli), a na oprávnění vašeho uživatelského profilu. Většina úloh je dostupná pouze tehdy, pokud máte zvláštní oprávnění *ALLOBJ a *SECADM.

Když používáte produkt Digital Certificate Manager (DCM) poprvé, paměti certifikátů ještě neexistují (pokud nemigrujete z předchozí verze produktu DCM). Máte-li potřebná oprávnění, zobrazuje navigační rám tudíž pouze tyto úlohy:

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

I v případě, že paměti certifikátů ve vašem systému existují (například při migraci z předchozí verze produktu DCM), produkt DCM zobrazí v levém navigačním rámu pouze omezený počet úloh nebo kategorií úloh. 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 navigačním rámu.

V navigačním rámu 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 iSeries tak, aby používal SSL a fungoval v režimu zabezpečení. Pak musíte spustit HTTP server v režimu zabezpečení. Pokud jste nenakonfigurovali a nespustili server HTTP v režimu SSL, zobrazí se vám chybová zpráva a prohlížeč nespustí zabezpečenou relaci.

Jak začít

I když zřejmě budete chtít používat certifikáty pro 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:

Vytvořit a provozovat lokálního CA, pomocí kterého budete vydávat certifikáty svým aplikacím.

Spravovat certifikáty od veřejného internetového CA, které pak budou vaše aplikace používat.

Vytvoření a provozování lokálního CA

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. Pomocí 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 iSeries, měli byste ještě před zahájením práce s produktem DCM webový server vytvořit a nakonfigurovat. Když konfigurujete webový server, aby používal SSL, vygeneruje se pro server určitý 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 znovu nespouštějte, dokud mu pomocí DCM nepřiřadíte certifikát. Pokud ukončíte a znovu spustíte instanci *ADMIN webového serveru předtím, než mu přiřadíte certifikát, server se nespustí a nebudete moci pomocí produktu DCM certifikát serveru přiřadit.

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

1. Spusťte produkt DCM.
2. V navigačním rámu 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 v systému iSeries nainstalován kryptografický koprocesor IBM 4758–023 PCI Cryptographic Coprocessor. Pokud váš systém nemá kryptografický koprocesor, produkt DCM uloží certifikát a jeho soukromý klíč automaticky do paměti certifikátů Lokální 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 iSeries nainstalován kryptografický koprocesor IBM 4758–023 PCI 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 podúlohy.)
f. Vyberete aplikace, které mohou používat serverový nebo klientský certifikát pro připojení přes SSL.

   Poznámka: Jestliže jste již dříve pomocí 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 podúloha 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 by měly důvěřovat vašemu lokálnímu CA.

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 v jiných systémech 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, naleznete v tématech:

Správa uživatelských certifikátů
Tato část popisuje, jak mohou uživatelé získat certifikáty nebo přiřadit existující certifikáty ke svému uživatelskému profilu v systému iSeries.

Vydávání certifikátů uživatelům jiných systémů než 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 v systému iSeries.

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

Správa uživatelských certifikátů

Vy i vaši uživatelé můžete pomocí produktu Digital Certificate Manager (DCM) spravovat certifikáty, které vaši uživatelé potřebují a používají k tomu, aby se zúčastnili relací SSL (Secure Sockets Layer).

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, měl by uživatelský software již kopii certifikátu CA vlastnit. Tudíž ani vy jako administrátor produktu DCM, ani vaši uživatelé nemusí před zapojení 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 ke zdrojům, 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 ke zdrojům interním uživatelům, kteří v současné době mají uživatelský profil v systému iSeries, můžete pomocí produktu DCM přidat jejich certifikát k jejich uživatelskému profilu. Tímto přiřazením zajistíte, aby uživatelé měli při předkládání certifikátu stejná přístupová práva a omezení ke zdrojům, jaká jim zaručuje nebo omezuje jejich uživatelský profil.

Pomocí produktu DCM můžete spravovat certifikáty, které jsou přiřazeny k uživatelskému profilu v systému 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 v produktu DCM otevřena žádná paměť certifikátů nebo když je otevřena paměť certifikátů lokálního CA, pak v navigačním rámu 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 hlavním navigačním rámu.

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

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

Přiřazení uživatelského certifikátu
V této části je vysvětleno, jak přiřadit certifikát, který vlastníte, k vašemu uživatelskému profilu. Certifikát může pocházet i od soukromého lokálního CA v jiném systému, nebo od veřejného CA. Abyste mohli přiřadit certifikát ke svému uživatelskému profilu, musí server vydávajícímu CA důvěřovat a tento certifikát nesmí být přiřazen k nějakému jinému uživatelskému profilu v systému.

Vytvoření uživatelského certifikátu: 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 navigačním rámu 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 (Digital Certificate Manager) automaticky přiřadí certifikát k vašemu uživatelskému heslu v systému 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.

Přiřazení uživatelského certifikátu: Chcete-li používat digitální certifikáty k autentizaci uživatelů, musí mít uživatelé certifikáty. Jestliže musí vaši uživatelé předkládat certifikáty od veřejného internetového vydavatele certifikátů (CA), mohou pomocí produktu DCM přiřadit tyto certifikáty ke svým uživatelským profilům. To umožní vám i uživateli spravovat tyto certifikáty pomocí produktu DCM.

Chcete-li použít úlohu **Přiřazení uživatelského certifikátu**, musíte mít zabezpečenou relaci se serverem HTTP, prostřednictvím které přistupujete 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.

Když zvolíte tuto úlohu, zobrazí se nové okno prohlížeče. Jestliže nemáte zabezpečenou relaci, vyzve vás produkt DCM, abyste klepli na **Přiřadit uživatelský certifikát** a relaci tak vytvořili. Produkt DCM pak iniciuje navázání spojení přes SSL (Secure Sockets Layer) s vaším prohlížečem.

V rámci navázání tohoto spojení vás může prohlížeč vyzvat, abyste specifikovali, zda se má důvěřovat vydavateli certifikátů (CA), jenž vydal certifikát, který identifikuje HTTP server. Prohlížeč vás také může vyzvat, abyste specifikovali, zda lze přijmout samotný serverový certifikát.

Když povolíte prohlížeči, aby důvěřoval CA a přijal serverový certifikát, může server vyžadovat, abyste předložili 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.

Jakmile vytvoříte zabezpečenou relaci, produkt DCM se pokusí načíst příslušný certifikát z vašeho prohlížeče, aby ho mohl přiřadit k vašemu uživatelskému profilu. 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 vašemu uživatelskému profilu. Příčinou by mohl být některý z problémů s uživatelskými certifikáty. Například certifikáty, které obsahuje váš prohlížeč, již mohou být k vašemu uživatelskému profilu přiřazeny.

Dáváte-li přednost tomu, aby byly certifikáty vydávány uživatelům pomocí lokálního CA, musí si uživatelé vytvořit uživatelský certifikát.

Vydávání certifikátů uživatelům jiných systémů než systému iSeries pomocí rozhraní API

Počínaje verzí V5R2 jsou k dispozici dvě nová rozhraní API, pomocí kterých můžete vydávat certifikáty i uživatelům jiných systémů než systému iSeries. Když jste vydávali certifikáty uživatelům pomocí lokálního vydavatele certifikátů (CA) v předchozích verzích, byly tyto certifikáty automaticky přiřazeny k jejich uživatelskému profilu v systému iSeries. Pokud jste tudíž chtěli pomocí lokálního CA vydat nějakému uživateli certifikát pro autentizaci klienta, museli jste tomuto uživateli vytvořit uživatelský profil v systému 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 v systému 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 pro produkt 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 kterého 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.

Získání kopie certifikátu soukromého CA

Když přistupujete na server, který používá připojení přes SSL (Secure Sockets Layer), předloží server vašemu klientskému softwaru certifikát jako důkaz své identity. Váš klientský software musí předtím, než server vytvoří relaci, potvrdit certifikát serveru. 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, měl by váš prohlížeč nebo jiný klientský software již kopii certifikátu CA mít. 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, měli byste stáhnout certifikát lokálního CA do svého prohlížeče předtím, než budete požadovat uživatelský certifikát od lokálního CA.

Chcete-li pomocí produktu DCM získat kopii certifikátu lokálního CA, postupujte takto:
1. Spusťte produkt DCM.
2. V navigačním rámu 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. Vybráním volby **Kopírovat a vložit certifikát** 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.

Správa certifikátů od veřejného internetového CA

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

- Správa veřejných internetových certifikátů pro komunikační relace SSL.
- Správa veřejných internetových certifikátů pro podepisování objektů.
- Správa internetových certifikátů pro ověřování podpisů na objektech.

Produkt DCM vám také umožní spravovat certifikáty, které získáte od vydavatelů certifikátů, kteří podporují standardy PKIX (Public Key Infrastructure for 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 navigačním rámu produktu DCM vyberte volbu **Vytvoření nové paměti certifikátů**, čímž spustíte vedenou úlohu a zobrazí se vám 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 iSeries nainstalovaný kryptografický koprocesor IBM 4758–023 PCI Cryptographic Coprocessor, produkt DCM vám v další úloze umožní 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 k vydání a podepsání vašeho certifikátu.

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

   Poznámka: Chcete-li používat certifikát v kombinaci s produktem HTTP Server for iSeries, měli byste 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 znovu nespouštějte, dokud mu pomocí DCM nepřiřadíte podepsaný dokončený certifikát. Pokud ukončíte a znovu spustíte instanci *ADMIN webového serveru předtím, než mu přiřadíte certifikát, server se nespustí a nebudete moci pomocí produktu DCM certifikát serveru přiřadit.

8. Když vám veřejný CA zašle zpět podepsaný certifikát, spusťte produkt DCM.
9. V navigačním rámu 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 rám, 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 by tento certifikát měly používat při komunikaci SSL.
13. V navigačním rámu 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 ke zdrojům, 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, měli by navštívit webové stránky daného CA a řídit se instrukcemi, které stránky poskytují.

Správa veřejných internetových certifikátů pro 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. Standardně definice aplikace vyžaduje, aby měl uživatel, který má mít povolení používat certifikát k podepisování objektů, 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 navigačním rámu produktu DCM po levé ruce vyberte volbu **Vytvoření nové paměti certifikátů**, čímž spustíte vedenou úlohu a zobrazí se vám 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 k vydání a podepsání 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 navigačním rámu po levé ruce 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 navigačním rámu 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 navigační rám, vyberte volbu **Správa aplikací** a 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 spíš 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 identitu odesílatele a to, že data jsou nezměněna, musí pomocí verze V5R1 produktu DCM nebo novější ověřit podpis na objektu. Aby mohl příjemce ověřit podpis, musí mít kopii certifikátu pro ověřování podpisů. Kopii tohoto certifikátu byste měli poskytovat jako součást dodávky podepsaných objektů.

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 měla mít. Pokud si však nejste jisti, zda příjemce kopii tohoto certifikátu má, měli byste kopii certifikátu CA poskytnout příjemci spolu s podepsanými objekty. Například byste měli poskytovat kopii certifikátu lokálního CA, pokud jste podepsali objekty pomocí certifikátu od soukromého lokálního CA. Z bezpečnostních důvodů byste měli zasílat certifikát CA samostatně, nebo dát certifikát CA k dispozici veřejně na vyžádání těch, kteří jej potřebují.

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. Při podepsání objektu se pomocí soukromého klíče certifikátu vytvoří 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 navigačním rámu produktu DCM po levé ruce vyberte volbu **Vytvoření nové paměti certifikátů**, čímž spustíte vedenou úlohu a zobrazí se vám 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, měli byste je exportovat z paměti certifikátů *OBJECTSIGNING do této paměti certifikátů. Pokud je nevyexportujete, nebudete schopni ověřovat podpisy, které jste pomocí těchto certifikátů vytvořili.

   Poznámka: Jestliže jste tuto paměť vytvořili za účelem ověřování podpisů na objektech, které budete dostávat z jiných zdrojů, měli byste podle tohoto postupu pokračovat dál, abyste byli schopni do této paměti certifikátů importovat certifikáty, které budete potřebovat.
5. V navigačním rámu 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 rám, 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.

Kapitola 8. Správa produktu DCM

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

Správa aplikací v produktu DCM
V této části naleznete popis, jak pomocí produktu DCM pracovat s definicemi aplikací u aplikací pro použití SSL a aplikací pro podepisování objektů. 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.

Potvrzování certifikátů a aplikací
Tato část popisuje, jak můžete ověřit autenticitu určitého certifikátu předtím, než jej aplikace použije nebo schválí.

Přiřazení certifikátů
V této části je vysvětleno, jak lze rychle přiřadit certifikát k jedné nebo více aplikacím, které jej budou používat pro funkce zabezpečení.

Správa umístění CRL Tato část popisuje, jak definovat a používat umístění seznamů odvolaných certifikátů (CRL), pomocí kterých si mohou aplikace ověřovat, že certifikát, který přijímají, je stále platný.

Uložení klíčů certifikátů do kryptografického koprocesoru IBM 4758 Cryptographic Coprocessor
V této části je vysvětleno, jak lze pomocí nainstalovaného koprocesoru zajistit bezpečnější uložení soukromých klíčů certifikátů.

Správa umístění požadavků pro vydavatele certifikátů PKIX
V této části je vysvětleno, jak pomocí produktu DCM spravovat certifikáty, které získáte od veřejného internetového CA, jenž certifikáty vydává podle standardů PKIX (Public Key Infrastructure for X.509).

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.

Ověřování podpisu objektů
V této části je vysvětleno, jak pomocí produktu DCM ověřovat autenticitu digitálních podpisů na objektech.

Použití lokálního CA k vydávání certifikátů pro jiné systémy iSeries

Předpokládejme, že již používáte soukromého lokálního vydavatele certifikátů (CA) v některém systému iSeries v rámci vaší sítě. Nyní chcete rozšířit použití tohoto CA i na další systém iSeries v síti. Chcete například, aby váš současný lokální CA vydával serverový nebo klientský certifikát pro aplikaci v jiném systému iSeries, 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 iSeries.

Tyto záměry lze splnit pomocí produktu DCM (Digital Certificate Manager). Některé z úloh budete provádět v systému iSeries, kde provozujete lokálního CA, jiné budete provádět v sekundárním systému iSeries, 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 iSeries, ve kterém provozujete lokálního CA, používá produkt pro poskytování kryptografického přístupu se silnějším šifrováním, než má cílový systém, pak je možné, že narazíte na problémy. (Ve verzi V5R2 je k dispozici pouze produkt pro kryptografický přístup 5722–AC3, což je nejsilnější dostupný produkt. V dřívějších vydáních však bylo možno instalovat jiné, slabší šifrovací produkty (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 iSeries, 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 v jiném systému iSeries verze V5R2 nebo V5R1

Chcete-li pomocí lokálního CA vydávat certifikáty, které se budou používat v jiném systému iSeries verze V5R2 nebo V5R1, proveďte v systému, který hostí vašeho lokálního CA, tyto úlohy:

1. Spusťte produkt DCM.

   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.
2. V navigačním rámu vyberte volbu **Vytvoření certifikátu**. Zobrazí se seznam typů certifikátů, které můžete pomocí lokálního CA vytvořit.

   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 certifikátu Lokální vydavatel certifikátů (CA). Než můžete provést tyto úlohy, musí v daném systému existovat lokální CA.
3. Vyberte požadovaný typ certifikátu, který má lokální CA vydat, a klepněte na **Pokračovat**, čímž spustíte vedenou úlohu a zobrazí se vám série formulářů. U typu certifikátu vyberte buď **serverový, nebo klientský certifikát pro jiný systém iSeries** (pro relace SSL), nebo **certifikát pro podepisování objektů pro jiný systém 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 V5R1 nebo vyšší verzi operačního systému OS/400, aby mohl certifikát používat. Protože cílový systém musí mít verzi V5R1 nebo vyšší, nevyzve vás v rámci této úlohy produkt DCM, abyste u nového certifikátu pro podepisování objektů vybrali formát cílového vydání.

4. Jestliže vytváříte serverový nebo klientský certifikát, vyberte úroveň vydání systému iSeries, pro který tento certifikát vytváříte. Klepněte na **Pokračovat** a zobrazí se vám formulář, do kterého zadáte identifikační informace pro nový certifikát.

   Poznámka: Úroveň vydání, kterou zvolíte, bude určovat formát, který produkt DCM použije k vytvoření nového certifikátu. Množství a typ identifikačních informací ve formuláři se liší podle toho, kterou úroveň vydání jste zvolili. Tím je zajištěno, že soubory certifikátu budou kompatibilní se systémem iSeries, který bude certifikáty používat.
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.

   Poznámka: 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.

Vydávání soukromých certifikátů pro použití v jiném systému iSeries verze V4R4 nebo V4R5

Chcete-li pomocí lokálního CA vydávat certifikáty, které se budou používat v jiném systému iSeries verze V4R4 nebo V4R5, proveďte v systému, který hostí vašeho lokálního CA V5R2, tyto úlohy:

1. Spusťte produkt DCM.

   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.
2. V navigačním rámu vyberte volbu **Vytvoření certifikátu**. Zobrazí se seznam typů certifikátů, které můžete pomocí lokálního CA vytvořit.

   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 certifikátu Lokální vydavatel certifikátů (CA). Než můžete provést tyto úlohy, musí v daném systému existovat lokální CA.
3. Vyberte požadovaný typ certifikátu, který má lokální CA vydat, a klepněte na **Pokračovat**, čímž spustíte vedenou úlohu a zobrazí se vám série formulářů.

   Poznámka: Protože vytváříte certifikát pro systém iSeries verze V4R4 nebo V4R5, musíte vybrat **serverový nebo klientský certifikát pro jiný systém iSeries**. Cílové systémy s úrovní vydání nižší než V5R1 nemohou používat certifikáty pro podepisování objektů.
4. Vyberte úroveň vydání systému iSeries, pro který tento certifikát vytváříte. Klepněte na **Pokračovat** a zobrazí se vám formulář, do kterého zadáte identifikační informace pro nový certifikát.

Poznámka: Úroveň vydání, kterou zvolíte, bude určovat formát, který produkt DCM použije k vytvoření nového certifikátu. Množství a typ identifikačních informací ve formuláři se liší podle toho, kterou úroveň vydání jste zvolili. Tím je zajištěno, že soubory certifikátu budou kompatibilní se systémem iSeries, který bude certifikáty používat.

5. Vyplňte formulář a klepněte na **Pokračovat**. Zobrazí se potvrzující stránka.

   Poznámka: Jestliže v cílovém systému existuje paměť certifikátů *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.

   Poznámka: 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).

Poznámka: Pokud hodláte použít certifikáty v těchto souborech v existující paměti certifikátů *SYSTEM v cílovém systému V4R4 nebo V4R5, nemůžete importovat certifikát lokálního CA přímo ze souborů .KDB a .RDB. Je tomu tak proto, že certifikát CA není ve formátu, který funkce importu produktu DCM umí rozpoznat a použít. Namísto toho musíte v hostitelském systému vyexportovat kopii certifikátu lokálního CA do samostatného souboru, což zajistí, že certifikát CA bude ve formátu, který bude fungovat s funkcí importu v nižších vydáních.

6. V navigačním rámu klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***SYSTEM**.
7. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte heslo, které jste pro danou paměť certifikátů uvedli, když jste ji v hostitelském systému vytvářeli, a klepněte na **Pokračovat**.
8. V navigačním rámu vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
9. Ze seznamu úloh vyberte volbu **Export certifikátu**.
10. Vyberte **Vydavatel certifikátů (CA)** jako typ certifikátu, který budete exportovat, a klepněte na **Pokračovat**. Zobrazí se seznam certifikátů CA.
11. Ze seznamu certifikátů vyberte certifikát lokálního CA (například LOCAL_CERTIFICATE_AUTHORITY). Klepněte na **Exportovat** a zobrazí se vám formulář, kde můžete zvolit místo určení pro certifikát CA.
12. Vyberte **Soubor** a klepněte na **Pokračovat**.
13. Zadejte úplnou cestu a jméno souboru pro exportní soubor a klepněte na **Pokračovat**. Zobrazí se potvrzující stránka, která oznamuje, že produkt DCM soubor úspěšně exportoval.

    Poznámka: Dávejte pozor na to, abyste pro soubor zadali jedinečné jméno a příponu. Soubor byste mohli pojmenovat například mycafile.exp. Při zadávání jména souboru nepoužívejte žádnou z těchto přípon: .TXT, .KDB, .RDB nebo .KYR. Kdybyste použili tyto typy přípon, mohli byste mít problémy při importu souboru v cílovém systému.
14. Prostřednictvím binárního protokolu FTP (File Transfer Protocol) nebo jiné metody proveďte přenos souborů paměti certifikátů (.KDB a .RDB), které jste vytvořili, do cílového systému V4R4 nebo V4R5. Pro přenos souboru, který obsahuje exportovaný certifikát lokálního CA, použijte FTP v režimu ASCII.

Poté, co jste soubory certifikátů přenesli, budete s nimi pracovat v cílovém systému pomocí produktu DCM. Úlohy, které musíte v produktu DCM provést, se liší podle úrovně vydání cílového systému a podle toho, které paměti certifikátů v cílovém systému existují. Také typ certifikátu, který jste vytvořili v hostitelském systému, ovlivňuje úlohy, které musíte v cílovém systému provést. Další informace o tom, jak pomocí produktu DCM pracovat v cílovém systému s přenesenými soubory certifikátů, obsahují tato témata:

- Použití soukromého certifikátu pro relace SSL v cílovém systému V5R2.
- Použití soukromého certifikátu pro relace SSL v cílovém systému V5R1.
- Použití soukromého certifikátu k podepisování objektů v cílovém systému V5R2 nebo V5R1.
- Použití soukromého certifikátu pro relace SSL v cílovém systému V4R5 nebo V4R4.

Použití soukromého certifikátu pro relace SSL v cílovém systému V5R2

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 V5R2 nikdy nepoužívali ke správě certifikátů pro SSL, pak by tato paměť certifikátů v cílovém systému neměla existovat. 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 V5R2 existuje, můžete použít přenesené soubory certifikátů jedním ze dvou způsobů:

- Použít přenesené soubory jako Jinou systémovou paměť certifikátů.
- Importovat přenesené soubory do existující paměti certifikátů *SYSTEM.

Paměť certifikátů *SYSTEM neexistuje

Pokud paměť certifikátů *SYSTEM v systému V5R2, kde chcete používat přenesené soubory paměti certifikátů, neexistuje, pak můžete přenesené soubory certifikátů použít přímo jako paměť certifikátů *SYSTEM. Chcete-li vytvořit paměť certifikátů *SYSTEM a použít soubory certifikátů v cílovém systému V5R2, 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. Neměli byste tudíž 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 byste měli 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 by měly 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 navigačním rámu 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 V5R2, a klepněte na **Pokračovat**.
6. V navigačním rámu 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 by měly certifikát používat pro relace SSL.
7. V navigačním rámu 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 rám, 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 mají 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 ke zdrojům. 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 iSeries. 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 Jiná systémová paměť certifikátů

Jestliže cílový systém V5R2 již paměť certifikátů *SYSTEM má, musíte se rozhodnout, jak budete se soubory certifikátu 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 pro systém 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 by měly certifikát používat. Nemůžete tudíž nakonfigurovat standardní aplikace systému iSeries využívající SSL tak, aby používaly tento certifikát. Pokud hodláte používat certifikát pro aplikace systému 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 navigačním rámu klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte **Jiná systémová paměť certifikátů**.
3. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte úplnou cestu a jméno souboru pro soubor paměti certifikátu (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 V5R2, a klepněte na **Pokračovat**.
4. V navigačním rámu 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 navigačním rámu 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 certifikátu, zadejte nové heslo a klepněte na **Pokračovat**.
7. Když se obnoví navigační rám, 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

Certifikáty v přenesených souborech paměti certifikátů můžete použít v existující paměti certifikátů *SYSTEM v systému V5R2. 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 V5R2 takto:

1. Spusťte produkt DCM.
2. V navigačním rámu 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 certifikátu (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 V5R2, a klepněte na **Pokračovat**.
4. V navigačním rámu 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 *SYSTEM dostat do chybového stavu.

   Když změníte heslo, musíte paměť certifikátů znovu otevřít, abyste mohli pracovat s certifikáty, které v paměti jsou.
5. V navigačním rámu 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 certifikátu, zadejte nové heslo a klepněte na **Pokračovat**.
7. Když se obnoví navigační rám, 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, měli byste do ní naexportovat certifikát lokálního CA. Kdybyste exportovali nejdříve serverový nebo klientský certifikát, mohli byste se dostat do chybového stavu způsobeného právě tím, že v paměti certifikátu 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 byl certifikát 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 byl certifikát 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 navigačním rámu 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 rám, 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 mají 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 ke zdrojům. 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 iSeries. 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 relace SSL v cílovém systému V5R1

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 V5R1 nikdy nepoužívali ke správě certifikátů pro SSL, pak by tato paměť certifikátů v cílovém systému neměla existovat. 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 V5R1 existuje, můžete použít přenesené soubory certifikátů jedním ze dvou způsobů:

- Použít přenesené soubory jako Jinou systémovou paměť certifikátů.
- Importovat přenesené soubory do existující paměti certifikátů *SYSTEM.

Paměť certifikátů *SYSTEM neexistuje

Pokud paměť certifikátů *SYSTEM v systému V5R1, ve kterém chcete používat přenesené soubory paměti certifikátů, neexistuje, pak můžete použít přenesené soubory certifikátů jako paměť certifikátů *SYSTEM. Chcete-li použít soubory certifikátů v cílovém systému V5R1, 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. Neměli byste tudíž 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 byste měli 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 by měly 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 navigačním rámu 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 V5R1, a klepněte na **Pokračovat**.
6. V navigačním rámu 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 by měly certifikát používat pro relace SSL.
7. V navigačním rámu 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 rám, vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
10. Ze seznamu úloh vyberte volbu **Aktualizace přiřazení certifikátu**. Zobrazí se seznam aplikací využívajících SSL, kterým můžete přiřadit certifikát.
11. Vyberte ze seznamu aplikaci a klepněte na **Aktualizace přiřazení certifikátu**.

12. Vyberte certifikát, který vydal lokální CA v *hostitelském* systému, 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. Aplikace s touto podporou musí být schopna autentizovat certifikáty předtím, než poskytne přístup ke zdrojům. 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 iSeries. 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 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 Jiná systémová paměť certifikátů

Jestliže cílový systém V5R1 již paměť certifikátů *SYSTEM má, musíte se rozhodnout, jak budete se soubory certifikátu 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 pro systém 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 by měly certifikát používat. Nemůžete tudíž nakonfigurovat standardní aplikace systému iSeries využívající SSL tak, aby používaly tento certifikát. Pokud hodláte používat certifikát pro aplikace systému 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 navigačním rámu klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte **Jiná systémová paměť certifikátů**.

3. Když se zobrazí stránka Paměť certifikátů a heslo, zadejte úplnou cestu a jméno souboru pro soubor paměti certifikátu (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 V5R1, a klepněte na **Pokračovat**.
4. V navigačním rámu 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 navigačním rámu 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 certifikátu, zadejte nové heslo a klepněte na **Pokračovat**.
7. Když se obnoví navigační rám, 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

Certifikáty v přenesených souborech paměti certifikátů můžete použít v existující paměti certifikátů *SYSTEM v systému V5R1. 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.

Poznámka: V následujícím postupu je popsáno, jak se pomocí Jiné systémové paměti certifikátů v cílovém systému exportují certifikáty z původních souborů paměti certifikátů do paměti certifikátů *SYSTEM. Pokud přidáte certifikáty do paměti certifikátů *SYSTEM touto metodou, vyhnete se potenciálním problémům v případech, kdy cílový systém používá slabší produkt pro poskytování kryptografického přístupu (např. 5722–AC2) než hostitelský systém.

Chcete-li exportovat certifikáty ze souborů paměti certifikátů do paměti certifikátů *SYSTEM, postupujte v cílovém systému V5R1 takto:

1. Spusťte produkt DCM.
2. V navigačním rámu 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 certifikátu (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 V5R1, a klepněte na **Pokračovat**.

4. V navigačním rámu 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 *SYSTEM dostat do chybového stavu.

   Když změníte heslo, musíte paměť certifikátů znovu otevřít, abyste mohli pracovat s certifikáty, které v paměti jsou.
5. V navigačním rámu 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 certifikátu, zadejte nové heslo a klepněte na **Pokračovat**.
7. Když se obnoví navigační rám, 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, měli byste do ní naexportovat certifikát lokálního CA. Kdybyste exportovali nejdříve serverový nebo klientský certifikát, mohli byste se dostat do chybového stavu způsobeného právě tím, že v paměti certifikátu 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**.
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 byl certifikát 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 navigačním rámu 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 rám, vyberte volbu **Správa certifikátů**. Zobrazí se seznam úloh.
20. Ze seznamu úloh vyberte volbu **Aktualizace přiřazení certifikátu**. Zobrazí se seznam aplikací využívajících SSL, kterým můžete přiřadit certifikát.
21. Vyberte ze seznamu aplikaci a klepněte na **Aktualizace přiřazení certifikátu**.
22. Vyberte certifikát, který vydal lokální CA v *hostitelském* systému, 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. Aplikace s touto podporou musí být schopna autentizovat certifikáty předtím, než poskytne přístup ke zdrojům. 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 iSeries. 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 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 k podepisování objektů v cílovém systému V5R2 nebo V5R1

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 by tato paměť certifikátů v cílovém systému neměla existovat. 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 V5R2 nebo V5R1, 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. Neměli byste tudíž 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. Certifikáty z těchto souborů můžete dostat do existující paměti certifikátů *OBJECTSIGNING jedním ze dvou způsobů. Buď můžete vyexportovat certifikáty v tomto souboru do sady nestrukturovatelných souborů, ze kterých pak certifikáty naimportujete do existující paměti certifikátů *OBJECTSIGNING. Nebo můžete otevřít přenesené soubory jako Jinou systémovou paměť certifikátů a exportovat certifikáty přímo do paměti certifikátů *OBJECTSIGNING, jak bude popsáno později. V obou případech musíte exportovat certifikáty do paměti certifikátů *OBJECTSIGNING, jestliže chcete být schopni spravovat aplikace, které certifikáty používají, tak jak je zde popsáno.

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 navigačním rámu 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 navigačním rámu 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 navigačním rámu 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 spíš 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.

Když distribuujete podepsané objekty, tak ti, kteří objekty dostávají, musí používat verzi V5R2 nebo V5R1 produktu DCM, aby mohli ověřit podpis na objektu a ujistili se tak, že data nebyla změněna, a ověřit identitu odesílatele. Aby mohl příjemce ověřit podpis, musí mít kopii certifikátu pro ověřování podpisů. Kopii tohoto certifikátu byste měli poskytovat jako součást dodávky podepsaných objektů.

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 měla mít. Pokud si však nejste jisti, zda příjemce kopii tohoto certifikátu má, měli byste kopii certifikátu CA poskytnout příjemci spolu s podepsanými objekty. Například byste měli poskytovat kopii certifikátu lokálního CA, pokud jste podepsali objekty pomocí

certifikátu od lokálního CA. Z bezpečnostních důvodů byste měli zasílat 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 V5R2 nebo V5R1. 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 dostat tak, že přenesené soubory 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 V5R2 nebo V5R1 takto:

1. Spusťte produkt DCM.
2. V navigačním rámu 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 navigačním rámu 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 navigačním rámu 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 certifikátu, zadejte nové heslo a klepněte na **Pokračovat**.
7. Když se obnoví navigační rám, 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 byste měli 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 certifikátu 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 tuto paměť certifikátů 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.

Použití soukromého certifikátu pro relace SSL v cílovém systému V4R5 nebo V4R4

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 V4R5 nebo V4R4 nikdy nepoužívali ke správě certifikátů pro SSL, pak by tato paměť certifikátů v cílovém systému neměla existovat. Přenesené soubory paměti certifikátů, které jste vytvořili v hostitelském systému lokálního CA, obsahují dva certifikáty. Je to serverový nebo klientský certifikát, který jste vytvořili, a certifikát soukromého lokálního CA, pomocí kterého jste jej podepsali.

Úlohy, které musíte provést, abyste mohli použít přenesené soubory paměti certifikátů, 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 existuje, můžete použít přenesené soubory certifikátů jedním ze dvou způsobů:

- Použít přenesené soubory jako Jinou systémovou paměť certifikátů.
- Importovat přenesené soubory do existující paměti certifikátů *SYSTEM.

Paměť certifikátů *SYSTEM neexistuje

Pokud paměť certifikátů *SYSTEM v systému V4R5 nebo V4R4, ve kterém chcete používat přenesené 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/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. Neměli byste tudíž 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 byste měli zajistit, aby měly soubory jedinečné jméno, a použít přenesenou paměť certifikátů jako **Jinou** paměť certifikátů. Použijete-li však soubory jako Jinou paměť certifikátů, nemůžete pomocí produktu DCM specifikovat, které aplikace by měly certifikát používat.

3. Spusťte produkt DCM. Nyní musíte změnit heslo pro paměť certifikátů *SYSTEM. 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 navigačním rámu se ujistěte, že v rozbalovacím seznamu je uvedena paměť certifikátů *SYSTEM, a vyberte volbu **Systémové certifikáty**. Zobrazí se seznam dostupných úloh. Zobrazí se okno **Paměť certifikátů a heslo**.
5. Do příslušných polí zadejte *SYSTEM jako paměť certifikátů, kterou chcete otevřít, a heslo, které jste použili, když jste soubory vytvářeli pomocí lokálního CA v hostitelském systému. Nyní můžete změnit heslo pro danou paměť certifikátů.
6. Ze seznamu úloh v navigačním rámu vyberte volbu **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.
7. Když znovu otevřete paměť certifikátů *SYSTEM, vyberte ze seznamu úloh **Práce se zabezpečenými aplikacemi** a zobrazí se stránka, pomocí níž můžete spravovat certifikáty přiřazené ke konkrétním aplikacím.
8. Ze seznamu aplikací vyberte aplikaci, která by měla používat přenesený soukromý certifikát pro relace SSL.
9. Klepněte na volbu **Práce se systémovým certifikátem** a vyberte certifikát, který vydal lokální CA v hostitelském systému.
10. Klepněte na **Přiřadit nový certifikát**, čímž zajistíte, že zadaná aplikace bude vybraný certifikát používat.

Poznámka: Některé aplikace využívající SSL podporují autentizaci klientů založenou na certifikátech. Použití certifikátů při autentizaci klientů zajišťuje, že aplikace předtím, než povolí přístup ke zdrojům, které řídí, musí dostat platný certifikát. Aplikace s touto podporou musí být nastavena tak, aby důvěřovala příslušnému CA předtím, než může autentizovat certifikáty, které tento CA vydá. Na stránce **Práce s vydavateli certifikátů** si můžete zjistit, zda je certifikát CA v paměti certifikátů uveden jako důvěryhodný zdroj. Pomocí úlohy **Práce se zabezpečenými aplikacemi** můžete nastavit, aby aplikace, které používají certifikát, důvěřovaly lokálnímu CA, který certifikát vydal. 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, aplikace certifikát nepřijme za základ pro platnou autentizaci.

Po provedení výše uvedených úloh budou moci aplikace v cílovém systému V4R5 nebo V4R4 používat certifikát vydaný lokálním CA v jiném systému iSeries verze V5R2. 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 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 Jiná systémová paměť certifikátů

Jestliže cílový systém V4R5 nebo V4R4 již paměť certifikátů *SYSTEM má, musíte se rozhodnout, jak budete se soubory certifikátů pracovat. Přenesené soubory paměti certifikátů obsahují dva certifikáty: serverový nebo klientský certifikát, který jste vytvořili, a certifikát lokálního CA, pomocí kterého jste jej podepsali. 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.

Pokud se rozhodnete, že přenesené soubory použijete jako **Jinou** paměť certifikátů, nebudete moci pomocí produktu DCM specifikovat, které aplikace by měly certifikát používat pro relace SSL. Můžete ale určit certifikát v této paměti certifikátů jako předvolený certifikát pro paměť certifikátů. 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 se konkrétně určí.

Pokud paměť certifikátů *SYSTEM v systému V4R5 nebo V4R4, ve kterém chcete používat přenesené soubory paměti certifikátů, existuje, postupujte takto:

1. Spusťte produkt DCM. Nyní musíte změnit heslo pro přenesenou paměť certifikátů. Při změně hesla produkt DCM uloží nové heslo tak, že budete moci v této paměti používat všechny funkce produktu DCM pro správu certifikátů.
2. V navigačním rámu se ujistěte, že v rozbalovacím seznamu je jako paměť certifikátu uvedeno JINÁ, a vyberte volbu **Systémové certifikáty**, abyste zobrazili seznam dostupných úloh. Zobrazí se okno **Paměť certifikátů a heslo**.
3. Do příslušných polí zadejte úplnou cestu a jméno souboru paměti certifikátů (soubor s příponou .KDB), který jste přenesli z hostitelského systému lokálního CA. Zadejte heslo, které jste použili, když jste soubory vytvářeli v *hostitelském* systému. Nyní můžete změnit heslo pro danou paměť certifikátů.
4. V navigačním rámu vyberte ze seznamu úloh Systémový certifikát volbu **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 navigačním rámu vyberte volbu **Práce s certifikáty** a zobrazí se stránka, na které můžete provádět řadu úloh týkajících se správy certifikátů.
6. Ze seznamu certifikátů vyberte certifikát, který chcete používat jako předvolený certifikát pro aktuální paměť certifikátů, a klepněte na volbu **Nastavit předvolbu**.

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

Dříve, než budete moci importovat certifikáty do paměti certifikátů *SYSTEM v cílovém systému V4R5 nebo V4R4, musíte vyexportovat certifikáty z paměti certifikátů, které jste vytvořili, do jiného formátu souborů. Z těchto nových souborů pak budete moci certifikáty importovat do paměti certifikátů *SYSTEM. Přenesené soubory paměti certifikátů obsahují dva certifikáty: serverový nebo klientský certifikát, který jste vytvořili, a certifikát lokálního CA, pomocí kterého jste jej podepsali. Do paměti certifikátů *SYSTEM musíte importovat jak serverový nebo klientský certifikát, který jste vytvořili, tak certifikát soukromého lokálního CA.

Poznámka: Funkce exportu, které jsou v produktu DCM k dispozici u verze V4R5 a V4R4, nejsou tak vyvinuté jako funkce exportu ve verzi V5R2, takže když provádíte export certifikátu soukromého lokálního CA v cílovém systému, můžete narazit na problémy. Bude tudíž vhodnější, abyste v hostitelském systému V5R2 provedli export *další* kopie certifikátu lokálního CA do samostatného souboru a nepoužívali pro jeho export cílový systém V4R4 nebo V4R5. Když provedete export certifikátu lokálního CA v hostitelském systému V5R2, můžete pak manuálně převést exportní soubor certifikátu lokálního CA do cílového systému V4R4 nebo V4R5 a dále postupovat podle níže uvedeného postupu, který popisuje import certifikátu lokálního CA do paměti certifikátu *SYSTEM. Certifikát lokálního CA musíte importovat *předtím*, než importujete soukromý certifikát, který jste pomocí tohoto certifikátu CA vytvořili. Kdybyste nejprve importovali soukromý certifikát, mohli byste se dostat do chybového stavu způsobeného právě tím, že v paměti certifikátu neexistuje certifikát CA.

Chcete-li exportovat certifikát ze souborů paměti certifikátů, postupujte v cílovém systému V4R4 nebo V4R5 takto:

1. Spusťte produkt DCM.
2. V navigačním rámu se ujistěte, že v rozbalovacím seznamu je jako paměť certifikátu uvedeno JINÁ, a vyberte volbu **Systémové certifikáty**, abyste zobrazili seznam dostupných úloh. Zobrazí se okno **Paměť certifikátů a heslo**.
3. Zadejte úplnou cestu a jméno souboru pro přenesené soubory paměti certifikátů, zadejte heslo, které jste použili, když jste je vytvářeli v *hostitelském* systému, a klepněte na **OK**. Nyní můžete změnit heslo pro danou paměť certifikátů.
4. V navigačním rámu vyberte ze seznamu úloh Systémový certifikát volbu **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 dostat do chybového stavu.

   Když změníte heslo, musíte paměť certifikátů znovu otevřít, abyste mohli pracovat s certifikáty, které v paměti jsou.
5. V navigačním rámu vyberte volbu **Práce s certifikáty** . Zobrazí se seznam certifikátů.
6. Vyberte ze seznamu soukromý certifikát, klepněte na **Exportovat** a zobrazí se stránka Export certifikátu.
7. Vyplňte formulář Export certifikátu.

   Poznámka: Dávejte pozor na to, abyste souboru zadali jedinečné jméno a příponu. Soubor můžete pojmenovat například myfile.exp. Při zadávání jména souboru nepoužívejte žádnou z těchto přípon: .TXT, .KDB, .RDB nebo .KYR, protože by tyto přípony mohly způsobit problém při importování

certifikátů do souboru. Vyberte odpovídající úroveň vydání cílového systém, který bude používat tento certifikát. Úroveň vydání, kterou vyberete, ovlivní formát exportovaného certifikátu.

8. Klepněte na **OK**. V horní části stránky se zobrazí zpráva, že produkt DCM exportoval certifikát do souboru, který jste uvedli.

V tomto okamžiku byste již měli mít pomocí produktu DCM v původním hostitelském systému verze V5R2 vyexportovanou další kopii certifikátu lokálního CA a manuálně převedenou na cílový systém V4R4 nebo V4R5. Už byste také měli mít v cílovém systému proveden export soukromého serverového nebo klientského certifikátu do nějakého souboru. Nyní jste připraveni importovat tyto certifikáty do paměti certifikátů *SYSTEM. Import certifikátu lokálního CA musíte provést *předtím*, než importujete soukromý certifikát, který jste vytvořili pomocí tohoto certifikátu CA. Kdybyste nejprve importovali soukromý certifikát, mohli byste se dostat do chybového stavu způsobeného právě tím, že v paměti certifikátu neexistuje certifikát CA.

Chcete-li importovat certifikáty z těchto naexportovaných souborů a specifikovat, že aplikace využívající SSL je budou používat, postupujte v cílovém systému V4R4 nebo V4R5 takto:

1. Spusťte produkt DCM.
2. V navigačním rámu se ujistěte, že v rozbalovacím seznamu je uvedena paměť certifikátů *SYSTEM, a vyberte volbu **Systémové certifikáty**. Zobrazí se seznam dostupných úloh. Zobrazí se okno **Paměť certifikátů a heslo**.
3. Zadejte *SYSTEM jako paměť certifikátů, kterou chcete otevřít, zadejte heslo a klepněte na **Pokračovat**.
4. Nyní musíte importovat certifikát lokálního CA z exportního souboru, který jste vytvořili v hostitelském systému V5R2. V navigačním rámu vyberte volbu **Přijmout certifikát CA** a zobrazí se formulář.
5. Vyplňte formulář a klepněte na **OK**, zobrazí se stránka Příjem certifikátu byl úspěšný. Když pracujete v paměti certifikátů *SYSTEM, zobrazí se na této stránce seznam aplikací, u kterých můžete nastavit, aby důvěřovaly importovanému certifikátu CA.

   Poznámka: Některé aplikace využívající SSL podporují autentizaci klientů založenou na certifikátech. Použití certifikátů při autentizaci klientů zajišťuje, že aplikace obdrží platný certifikát předtím, než povolí přístup ke zdrojům, které aplikace řídí. Aplikace s touto podporou musí být nastavena tak, aby důvěřovala příslušnému CA předtím, než může autentizovat certifikáty, které tento CA vydá. 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, aplikace certifikát nepřijme za základ pro platnou autentizaci.
6. Vyberte aplikace, které by měly důvěřovat danému certifikátu CA a klepněte na **OK**. Zobrazí se stránka Stav zabezpečených aplikací, která potvrzuje, že vybrané aplikace byly nastaveny tak, aby důvěřovaly novému certifikátu.
7. Nyní můžete importovat serverový certifikát. V navigačním rámu vyberte volbu **Práce s certifikáty** . Zobrazí se seznam certifikátů.
8. Klepněte na **Importovat** a zobrazí se stránka Import certifikátu.
9. Vyplňte formulář Import certifikátu a klepněte na **OK**, abyste se vrátili na stránku Práce s certifikáty. Ujistěte se, že jste zadali jméno souboru, který obsahuje exportovaný serverový nebo klientský certifikát, a že jste zadali cílové vydání odpovídající tomu, které jste zadali při předchozím exportu certifikátu. V horní části stránky se zobrazí zpráva, že produkt DCM přidal certifikát do aktuální paměti certifikátů. Certifikát, který jste importovali, by se měl v seznamu certifikátů objevit také.

10. Nyní musíte specifikovat, které aplikace by měly importovaný soukromý certifikát používat pro relace SSL. V navigačním rámu vyberte volbu **Práce se zabezpečenými aplikacemi** a zobrazí se stránka, pomocí které můžete spravovat certifikáty přiřazené ke konkrétním aplikacím.
11. Vyberte ze seznamu aplikaci a klepněte na **Práce se systémovými certifikáty**, abyste zobrazili seznam certifikátů, pro něž můžete zadat, aby je daná aplikace používala při vytváření relací SSL.
12. Vyberte ze seznamu certifikát a klepněte na **Přiřadit nový certifikát**, čímž přiřadíte vybraný certifikát ke specifikované aplikaci. V horní části stránky se zobrazí potvrzující zpráva o výběru certifikátu.

Po provedení výše uvedených úloh budou moci aplikace v cílovém systému V4R4 nebo V4R5 používat certifikát vydaný lokálním CA v jiném systému iSeries. 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 CA se musí zkopírovat do souboru na počítači uživatele nebo stáhnout do prohlížeče uživatele, což závisí na požadavcích aplikace, která používá SSL.

Správa aplikací v produktu DCM

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:

Vytvoření definice aplikace popisuje typy aplikací, které můžete definovat a se kterými můžete pracovat.

Správa přiřazení certifikátu popisuje, jak přiřadit nebo změnit certifikát, který aplikace používá k vytvoření relace SSL nebo k podepisování objektů.

Definování seznamu důvěryhodných CA popisuje, kdy je možné a kdy je vhodné definovat, kterým CA může aplikace důvěřovat při potvrzování a přijímání certifikátů.

Informace o dalších úlohách DCM naleznete v online nápovědě.

Vytvoření definice aplikace

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 pro systém IBM iSeries využívající SSL jsou produktem DCM takto registrovány, 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 pro SSL nepopisuje aplikace pro podepisování objektů žádnou skutečnou aplikaci. Definice aplikace, kterou vytvoříte, by měla 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 navigačním rámu 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 by měla vyžadovat autentizaci klientů. Můžete také specifikovat, že aplikace bude při autentizaci certifikátů používat seznam důvěryhodných CA.

Správa přiřazení certifikátu pro 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 pro 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 navigačním rámu 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 pro aplikaci, aplikace může, ale nemusí být schopna tuto změnu zaregistrovat, pokud je v době, kdy změnu provádíte, spuštěná. Například servery Client Access Express použijí změny v certifikátech, které provedete, automaticky. Avšak servery Telnet, IBM HTTP Server for iSeries nebo jiné aplikace budete muset zastavit a spustit, aby mohly provedenou změnu certifikátu aplikovat.

Počínaje verzí V5R2 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 identity. 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 **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete 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 navigačním rámu 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 by aplikace měla 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.

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 aplikace, napomáhá to předcházet problémům s certifikáty, k nimž může dojít, když aplikace vykonává funkci, která certifikáty vyžaduje. Takové problémy mohou aplikaci např. zabránit, aby se úspěšně zúčastnila relace SSL (Secure Sockets Layer) nebo aby úspěšně podepsala 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 dále 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.

Přiřazení certifikátu k aplikacím

Počínaje verzí V5R2 je možno pomocí produktu DCM (Digital Certificate Manager) 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.

   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 navigačním rámu klepněte na volbu **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte buď ***OBJECTSIGNING** nebo ***SYSTEM**.
3. Zadejte heslo pro paměť certifikátů a klepněte na **Pokračovat**.
4. Když se obnoví navigační rám, 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 identity. 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 navigačním rámu vyberte volbu **Správa umístění CRL**. Zobrazí se seznam úloh.
3. Ze seznamu úloh vyberte volbu **Přidání umístění CRL** a zobrazí se formulář, pomocí kterého popíšete umístění CRL a zadáte, jak má 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.

   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.

   Nyní musíte přiřadit definici umístění CRL ke konkrétnímu CA.
5. V navigačním rámu 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.

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 adresářových služeb obsahovat příslušný CRL. Musíte také nakonfigurovat jak server adresářových služeb, tak klientské aplikace, aby používaly SSL, a pomocí produktu DCM přiřadit aplikacím certifikát.

Další informace o konfigurování a používání serveru adresářových služeb (LDAP) systému iSeries uvádějí tato témata v rámci aplikace Information Center:

- Directory Services (LDAP)
  V této části najdete všechny potřebné informace o konfigurování a používání adresářového serveru (LDAP) systému iSeries.
- Using Secure Sockets Layer (SSL) security with the LDAP directory server
  V této části je vysvětleno, jak se konfiguruje server LDAP, aby používal SSL pro zabezpečenou komunikaci.

Uložení klíčů certifikátů do kryptografického koprocesoru IBM 4758

Pokud máte v systému iSeries nainstalovaný kryptografický koprocesor IBM 4758–023 PCI Cryptographic Coprocessor, 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:

- Uložit soukromý klíč certifikátu přímo v koprocesoru samotném.
- Pomocí hlavního klíče koprocesoru zašifrovat soukromý klíč certifikátu a uložit ho ve zvláštním souboru klíče.

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 Digital Certificate Manager (DCM), 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.

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 kryptografického koprocesoru IBM 4758–023 PCI 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 kryptografického koprocesoru IBM 4758–023 PCI Cryptographic Coprocessor soukromý klíč zašifrovat a uložit jej do zvláštního souboru klíče. 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 koprocesoru IBM 4758–023 PCI 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. Standardy PKIX jsou popsány v RFC (Request For Comments) 2560.

CA, který používá standardy PKIX, vyžaduje předtím, než vydá certifikát, přísnější identifikaci. Obvykle vyžaduje, aby žadatel prokázal svoji identitu prostřednictvím vydavatele registrace (Registration Authority, RA). Když žadatel dodá vydavateli registrace takový důkaz identity, který RA vyžaduje, potvrdí RA identitu 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 byste měli zvážit v případě, že vaše potřeby v oblasti zabezpečení vyžadují přísnou kontrolu přístupu ke zdrojům, které aplikace používající SSL poskytují uživatelům. 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 navigačním rámu 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**.

Podepisování objektů

Existují tři metody, pomocí kterých můžete podepisovat objekty. Můžete napsat program, který bude vyvolávat rozhraní pro podepisování objektů Sign Object API. Můžete podepisovat objekty pomocí produktu Digital Certificate Manager (DCM). Anebo, počínaje verzí V5R2, můžete podepisovat objekty pomocí funkce Centrální správa produktu Navigator systému iSeries, když objekty balíte pro distribuci do jiných systémů iSeries.

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 souborovém systému QSYS.LIB: *PGM, *SRVPGM, *MODULE, *SQLPKG a *FILE (pouze záložní soubory). Nově ve verzi V5R2 můžete podepisovat i příkazové objekty (*CMD). Nelze podepisovat objekty, které jsou uloženy na jiných serverech iSeries.

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. 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 navigačním rámu klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***OBJECTSIGNING**.
3. Zadejte heslo pro paměť certifikátů *OBJECTSIGNING a klepněte na **Pokračovat**.
4. Když se obnoví navigační rám, 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, měli byste 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 když 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.

   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 navigačním rámu klepněte na **Výběr paměti certifikátů** a jako paměť certifikátů, kterou chcete otevřít, vyberte ***SIGNATUREVERIFICATION**.
3. Zadejte heslo pro paměť certifikátů *SIGNATUREVERIFICATION a klepněte na **Pokračovat**.
4. Když se obnoví navigační rám, 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 ověřit všechny objekty v určitém adresáři, můžete zadat /mydirectory/*. Nebo když chcete ověřit 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, měli byste 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.

Kapitola 9. Odstraňování problémů v produktu DCM

Na následujících stránkách naleznete informace, které vám pomohou při odstraňování některých běžnějších problémů, na které můžete narazit při práci s produktem DCM (Digital Certificate Manager).

Informace o problémech a jejich možných řešeních obsahují tyto stránky:

Odstraňování obecných problémů a problémů s hesly
V této části najdete informace o běžných problémech, které mohou nastat při práci s uživatelským rozhraním produktu DCM, a dovíte se, jak byste tyto problémy mohli vyřešit.

Odstraňování problémů s paměťmi certifikátů a databázemi klíčů
V této části najdete informace o běžných problémech, ke kterým dochází při práci s paměťmi certifikátů a databázemi klíčů, a dovíte se, jak byste tyto problémy mohli vyřešit.

Odstraňování problémů s prohlížečem
V této části najdete informace o běžných problémech, ke kterým dochází, když přistupujete k produktu DCM prostřednictvím prohlížeče, a dovíte se, jak byste tyto problémy mohli vyřešit.

Odstraňování problémů s produktem HTTP Server for iSeries
V této části najdete informace o běžných problémech, ke kterým dochází při práci s HTTP serverem, a dovíte se, jak byste tyto problémy mohli vyřešit.

Řešení chybových stavů a obnovy při migraci
V této části najdete informace o běžných problémech, ke kterým dochází, když provádíte migraci produktu DCM z předchozího vydání, a dovíte se, jak byste tyto problémy mohli vyřešit.

Odstraňování problémů s přiřazením uživatelského certifikátu
V této části najdete informace o běžných problémech, ke kterým dochází, když pomocí produktu DCM registrujete uživatelský certifikát, a dovíte se, jak byste tyto problémy mohli vyřešit.

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 na Internetu.
Při pokusu o otevření paměti certifikátů obdržíte chybu NET.DATA.	Když vybíráte volbu **Výběr paměti certifikátů**, klepněte myší na tlačítko **Pokračovat**. Nepoužívejte klávesu **Enter** na klávesnici.
Heslo pro paměť certifikátu 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.
Nepodařilo se vám vynulovat a znovu nastavit heslo v rámci úlohy Výběr paměti certifikátů.	Funkce vynulování funguje pouze tehdy, pokud produkt DCM heslo uložil. Produkt DCM heslo automaticky uloží, když vytvoříte určitou paměť certifikátů. Avšak pokud měníte nebo nastavujete na původní hodnotu heslo paměti certifikátů Jiná systémová paměť certifikátů, pak musíte vybrat volbu **Automatické přihlášení**, aby produkt DCM heslo uložil.

Problém	Možné řešení
	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 vynulování 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 vynulovat a znovu nastavit. Hodnotu tohoto atributu si můžete prohlédnout nebo změnit pomocí příkazu STRSST a zadání uživatelského ID a hesla pro uživatele SST. Pak zvolte volbu ″Work with system security″. Uživatelský ID Service Tools bývá totožný s uživatelským ID QSECOFR.
Nemůžete najít zdroj certifikátu CA, který potřebujete přijmout do systému iSeries.	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 znovu spusťte 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 se používá produkt iSeries Navigator pro přístup do prohlížeče Netscape Communications. 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 iSeries nastavenu správnou hodnotu pro UTC offset (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 iSeries. 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 by měla vypadat stejně.
Provedli jste migraci z verze V4R3 produktu DCM na verzi V5R2 a migrace neobsahuje systémové certifikáty, jejichž platnost skončila.	Systémový certifikát s ukončenou platností je nyní nesprávný a nelze ho umístit do paměti certifikátů *SYSTEM. Před migrací odstraňte nebo přejmenujte staré soubory klíčového řetězce z verze V4R3, ignorujte indikátor selhání migrace nebo se pokuste migraci provést znovu.
Nemůžete najít vzorový kód pro přidávání certifikátů do ověřovacího seznamu.	Vzorový kód ještě není k dispozici.

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.
Selhalo vytvoření databáze klíčů.	Zkontrolujte, zda nejde o konflikt jmen souborů. Konflikt se může týkat i jiného souboru, než toho, o který jste žádali.
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.

Problém	Možné řešení
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. Prostudujte si v aplikaci Information Center téma QsyAddVldlCertificate API. Vyhledejte si v příručce Webmaster's Guide, jak konfigurovat zabezpečené instance 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 by si měl být jistý, 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. Měli byste také zkontrolovat, zda je správně nastaven váš server jmen domény.
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 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 koncovému uživateli sděluje, že daný CA není důvěryhodný.	Pomocí produktu DCM nastavte **Stav CA** tak, aby povoloval označení CA jako důvěryhodného.

Problém	Možné řešení
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 obsahují zdrojové certifikáty společností, jako je např. VeriSign, což je jedna z funkcí, které umožňují komunikaci SSL — konkrétně autentizaci. 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/ nebo 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

V následující tabulce naleznete informace, které vám pomohou při odstraňování některých běžnějších problémů s HTTP serverem systému iSeries, na které můžete narazit při práci s produktem DCM.

Problém	Možné řešení
Nefunguje HTTPS (Hypertext Transfer Protocol Secure).	Ujistěte se, že server HTTP je správně nakonfigurován pro použití SSL. Ve verzi V5R1 nebo v pozdějších verzích musí mít konfigurační soubor nastavenu hodnotu **SSLAppName** pomocí grafického uživatelského rozhraní (GUI) serveru HTTP. V konfiguraci také musí být obsažen virtuální hostitelský systém, který používá port SSL, přičemž virtuální hostitelský systém musí mít nastaveno **SSLEnable**. Dále musí existovat dvě direktivy pro naslouchání, které specifikují dva různé porty, jeden, který používá SSL, a druhý, který nepoužívá SSL. Ujistěte se, že je vytvořena instance serveru a že serverový certifikát je podepsán.
Potřebujete objasnit proces registrace instance HTTP serveru jako zabezpečené aplikace.	V systému iSeries přejděte do webového rozhraní HTTP serveru, abyste mohli nastavit konfiguraci HTTP serveru. Nejprve musíte nadefinovat virtuální hostitelský systém, abyste umožnili SSL. Toto se provádí na obrazovce Context Management. Musíte nadefinovat virtuální hostitelský systém tak, aby používal port SSL, nadefinovaný dříve v direktivě pro naslouchání. Dále musíte na obrazovce SSL General Settings přepnout virtuální hostitelský systém, nakonfigurovaný dříve, do režimu SSL. Všechny změny se musí zanést do konfiguračního souboru. Všimněte si, že při registrací instance se automaticky nevybere certifikát, který pak instance bude používat. Pomocí produktu DCM musíte určitý certifikát přiřadit vaší aplikaci předtím, než se pokusíte ukončit a znovu spustit instanci serveru.
Máte problémy, když u HTTP serveru nastavujete ověřovací seznam a volitelnou autentizaci klientů.	Vyhledejte si v příručce HTTP Server Webmaster's Guide volby pro nastavení instance. Tyto informace uvádí rovněž téma Web serving v rámci aplikace Information Center.
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.

Problém	Možné řešení
Pokoušíte se prostřednictvím prohlížeče předložit serveru HTTP 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 uvádí téma OS/400 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.
Nemůžete nalézt soubor požadavků, který se vytvoří, když se instaluje server HTTP. Systém používá tento soubor pro označování platných souborů klíčového řetězce nalezených v direktivě KEYFILE v konfiguračním souboru v rámci jeho adresáře.	Další informace naleznete v části Migrace z předcházející verze produktu DCM. Správný soubor pro server HTTP je /qibm/userdata/httpsvr/keyring/keymreq.crt. Správný soubor pro server LDAP je /qibm/userdata/os400/dirsrv/qdirsrv.crt.
Server HTTP 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.
Zaznamenali jste problém s paměťmi certifikátů poté, co jste nainstalovali verzi V5R2 přes verzi V4R3, a nyní existuje soubor /qibm/userdata/httpsvr/keyring/keymreq.crt nebo /qibm/usedata/os400/dirsrv/qdirsrv.crt. Systém nemohl dokončit automatickou migraci klíčového řetězce na databázi klíčů.	Specifikujte staré soubory klíčového řetězce jako paměť certifikátů a najděte a vymažte neplatný certifikát nebo certifikáty ze souborů klíčového řetězce. Teprve pak vyvolejte qicss/qyepmgrt a pokuste se znovu provést migraci. Anebo ignorujte či vymažte soubor .crt, pokud se v průběhu migrace přesunuly všechny důležité certifikáty.
HTTP server se nespustí při nastavení **SSLEnable** a v protokolu úlohy se zobrazí chybová zpráva HTP8351. Při selhání HTTP serveru protokol chyb serveru *ADMIN uvádí chybu, že operace SSL Initialization selhala s návratovým kódem chyby 107.	Chyba číslo 107 znamená, že platnost certifikátu vypršela. Pokud instance serveru je server *ADMIN, pak dočasně nastavte režim **SSLDisable**, abyste mohli použít produkt DCM na serveru *ADMIN. Pomocí produktu DCM přiřaďte aplikaci jiný certifikát, například QIBM_HTTP_SERVER_ADMIN, pokud je instance serveru *ADMIN server.

Řešení chybových stavů a obnovy při migraci

Chyby a náprava chyb

Následující indikátory vás upozorňují na chyby, ke kterým mohlo dojít během migrace:

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
Přítomnost tohoto indikátoru poté, co jste úspěšně instalovali jak volbu 34, tak 5722-DG1, znamená, že migrace klíčového řetězce, o kterou se produkt 5722-DG1 pokusil, nebyla úspěšná. Zřejmě budete muset provést migraci klíčového řetězce do paměti certifikátů *SYSTEM.

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT
Přítomnost tohoto indikátoru poté, co jste úspěšně nainstalovali volbu 34, znamená, že migrace klíčového řetězce pro server LDAP nebyla úspěšná.

Kromě těchto indikovaných chyb je možné, že při migraci došlo k dalším chybám, které systém neindikoval. Když například systém nalezne soubory klíčového řetězce, které potřebuje pro migraci do paměti certifikátů *SYSTEM, může zároveň zjistit konflikty s existujícími uživatelskými datovými soubory integrovaného systému souborů. V takovém případě systém pravděpodobně neprovedl migraci souboru klíčového řetězce, i když se vám instalace jeví jako úspěšně ukončená.

Ve výjimečných případech se také může stát, že se migrace souboru klíčového řetězce ukončí s částečným přiřazením systémového certifikátu předtím, než může chybová zpráva zabránit dokončení migrace. To pak může způsobit chybu, když spustíte instanci serveru *ADMIN IBM HTTP Server a SSLMODE je nastaven na ON. Možná vysvětlení jsou tato:

- Migrovaný soubor klíčového řetězce má jako předvolený certifikát nastaven špatný systémový certifikát.
- Produkt DCM ukončil migraci, aby ochránil uživatelská data, která již existují v kritickém jménu souboru.
- V kódu migrace se vyskytla nepředvídatelná chyba.

Server IBM HTTP Server můžete spustit bez nastavení SSLMODE na ON tak, že předtím, než spustíte instanci *ADMIN, nastavíte pro instanci *ADMIN dočasně SSLMODE na OFF. To vám umožní, abyste pomocí produktu DCM prozkoumali paměti certifikátů a vyřešili problém předtím, než ukončíte instanci *ADMIN. Když ukončíte instanci *ADMIN, můžete nastavit SSLMODE zpátky na ON a spustit instanci *ADMIN, aby se správně inicializovalo SSL.

Po provedení migrace volby 34 se mohou vyskytnout chyby v průběhu normálních požadavků produktu DCM, které pracují s paměťmi certifikátů. K těmto chybám dochází v prohlížeči. K takovým chybám patří například:

```
Chyba databáze
Chyba čtení databáze
Chyba zápisu do databáze
Porušení databáze
Porušena tabulka databáze
```

Dále by v systému mohl být soubor, který není platnou pamětí certifikátů, nazvaný default.kdb, uložený ve stejném adresáři jako /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR nebo /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR. V tomto případě musíte předtím, než budete pomocí produktu DCM vytvářet nové certifikáty, provést manuálně následující migraci:

Poznámka: Jestliže se rozhodnete neprovádět migraci souborů klíčového řetězce a vytvořit namísto toho nového CA a systémový certifikát, můžete tuto manuální migraci vynechat.

- Jestliže plánujete instalaci produktu HTTP Server for iSeries (5722-DG1), nainstalujte jej nyní, než budete pokračovat.

  Poznámky:

  1. Instalační kód volby 34 produktu 5722–SS1 se nepokusí znovu provést migraci poté, co jste nainstalovali volbu 34. Nepomůže pouze znovu nainstalovat volbu 34.
  2. Příslušné soubory jsou umístěny v adresářích uživatelských dat, které byly vytvořeny pomocí oprávnění PUBLIC *EXCLUDE. Ujistěte se, že pro tyto soubory máte správná oprávnění.

- Zkontrolujte, zda existují následující soubory:
  - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

  Jestliže existují, přejmenujte je pomocí příkazu WRKLNK a vytvořte záložní soubory.
- Z uživatelského profilu, který má oprávnění *ALLOBJ, vyvolejte z příkazové řádky program QICSS/QYEPMGRT takto:

  ```
  CALL QICSS/QYEPMGRT
  ```

  Jestliže je výsledek úspěšný, ujistěte se, že ve vašem systému neexistuje žádný z následujících souborů:

– /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
– /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

Produkt DCM obvykle uchovává záložní kopie uživatelských dat, které uložíte do souborů, jejichž jména jsou v konfliktu s těmi, které používá produkt DCM. Pokud následující soubory neexistují:

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

Avšak existují následující soubory:

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

Pak se systém pokusí je přejmenovat s použitím přípony .OLD. Pokud tyto soubory už také existují, pak systém žádné záložní kopie nevytvoří. Namísto toho jednoduše přepíše existující soubory s příponou .STH.

Různé

Pokud vaše pokusy o vytvoření CA a systémového certifikátu jsou stále neúspěšné kvůli konfliktu jmen souborů, narazili jste pravděpodobně na jeden z následujících problémů:

- **Konflikt různých jmen souboru** – 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. Vytvořit nového CA potřebujete 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
```

- **Chybějící nezbytné předpoklady** – ujistěte se, že jste správně nainstalovali nezbytné předchozí licencované programy (LPP).
- **Problém s kódem** – kontaktujte svého servisního zástupce.

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 by vás měl vyzvat, abyste vybrali certifikát.
2. Certifikát, který chcete registrovat, již je v produktu DCM registrován.
3. Vydavatel certifikátů, který vydal daný certifikát, není v systému specifikován jako důvěryhodný zdroj. 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 úlohu **Práce s certifikáty CA** a povolit CA jako důvěryhodný zdroj pro daný systém, což také problém vyřeší.
4. Nemáte certifikát pro registraci. Můžete zkontrolovat uživatelské certifikáty ve vašem prohlížeči a zjistit, zda problém není tady.
5. Platnost certifikátu, který se pokoušíte registrovat, vypršela, nebo je certifikát nekompletní. Musíte buď obnovit certifikát, nebo kontaktovat CA, který vydal certifikát, aby problém vyřešil.
6. Server IBM HTTP Server for iSeries není správně nastaven, aby prováděl registraci certifikátů za použití SSL a klientských certifikátů na zabezpečené instance serveru *ADMIN. 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 znovu spustit webový server.

Kapitola 10. Související informace o produktu DCM

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 strategii zabezpečení systému iSeries:

- **Webové stránky VeriSign Help Desk**
  Na webových stránkách VeriSign 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 Redbook) je zaměřena na možnosti zlepšení síťového zabezpečení ve verzi V5R1. Naleznete zde mnoho témat, např. jak využívat funkce pro podepisování objektů v systému iSeries, jak používat produkt Digital Certificate Manager (DCM), 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 možnosti použití digitálních certifikátů 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.
- **Webové stránky RFC Index Search**
  Na těchto webových stránkách naleznete schránku RFC (Request for Comments). RFC popisují standardy pro internetové protokoly jako je SSL, PKIX a další, které se týkají použití digitálních certifikátů.

Vytištěno v Dánsku společností IBM Danmark A/S.