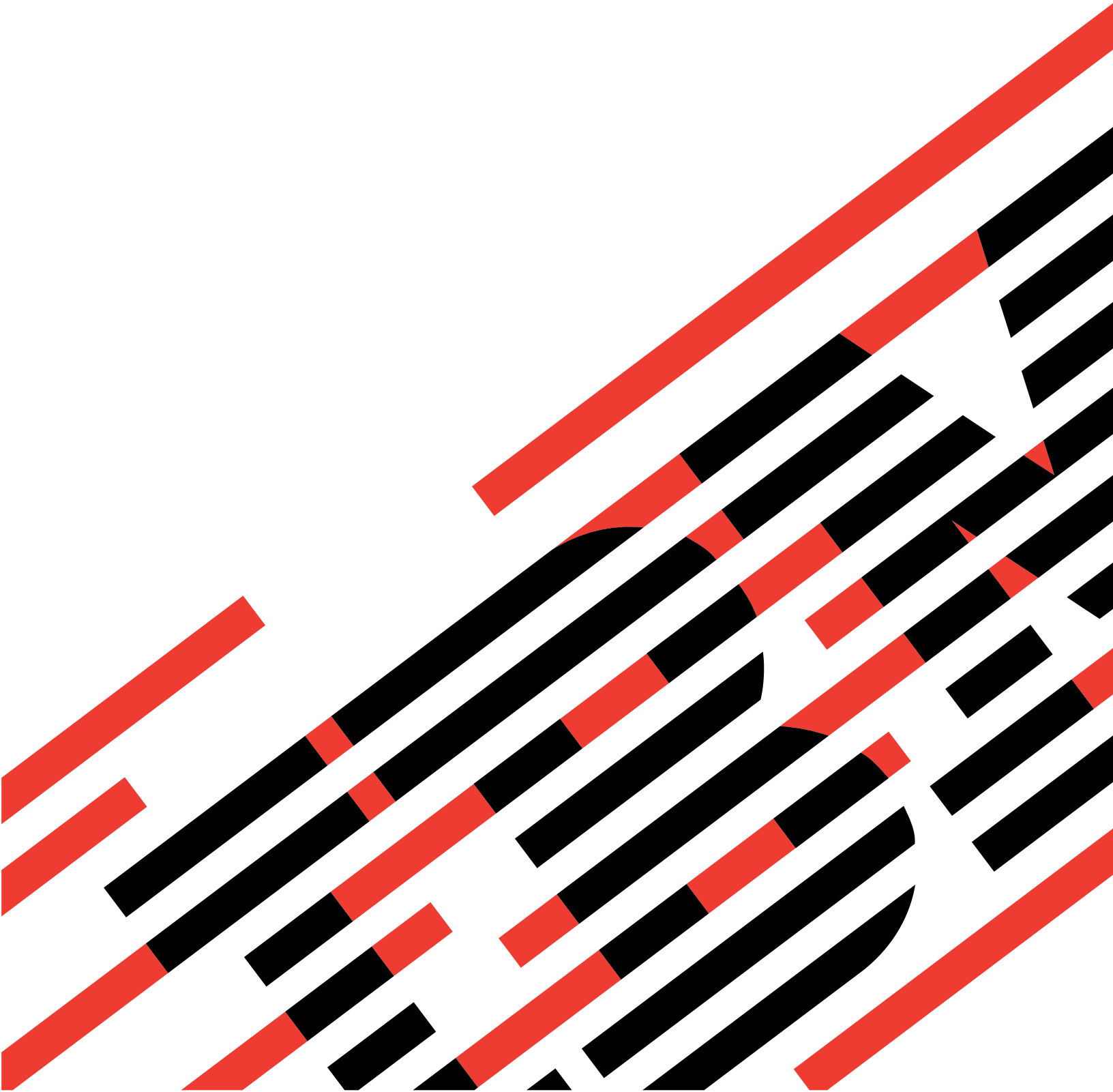
IBM

eserver

iSeries

Upravitelj digitalnih certifikata



IBM

@server

iSeries

Upravitelj digitalnih certifikata

Sadržaj

Dio 1. Upravitelj digitalnih certifikata

Digitalni certifikat je elektronska vjerodajnica koju možete koristiti za postavljanje dokaza identiteta u elektronskoj transakciji. Digitalni certifikati se koriste sve više u poboljšanim mjerama sigurnosti mreže. Na primjer, digitalni certifikati su bitni za konfiguriranje i korištenje Sloja sigurnih utičnica (SSL). Korištenjem SSL-a omogućeno vam je kreiranje sigurnih veza između korisnika i poslužiteljskih aplikacija na nepouzdanoj mreži, kao što je Internet. SSL omogućuje jedno od najboljih rješenja za zaštitu privatnosti osjetljivih podataka, kao što su korisnička imena i lozinke, putem Interneta. Mnoge iSeries usluge i aplikacije, kao FTP, Telnet, HTTP poslužitelj za iSeries i mnoge druge, pružaju SSL podršku da bi osigurale privatnost podataka.

iSeries pruža opsežnu podršku digitalnog certifikata koja vam dozvoljava da koristite digitalne certifikate kao preporuke u mnogim sigurnosnim aplikacijama. Osim korištenja certifikata za konfiguraciju SSL-a, možete ih koristiti kao vjerodajnice u SSL-u i transakcijama na virtualnim privatnim mrežama. Također, možete koristiti digitalne certifikate i njima pridružene sigurnosne ključeve za označavanje objekata. Označavanje objekata vam dozvoljava da otkrijete promjene ili moguće nedozvoljeno mijenjanje sadržaja objekta provjeravanjem potpisa na objektima da bi osigurali njihovu cjelovitost.

Kapitaliziranjem iSeries podrške za certifikate je jednostavno kada koristite Upravitelj digitalnih certifikata (DCM), besplatno iSeries svojstvo za centralno upravljanje certifikatima za vaše aplikacije. DCM vam dopušta da upravljate certifikatima koje dobivate od svakog Izdavača certifikata (CA). Možete koristiti DCM za stvaranje i rad na vašem vlastitom Lokalnom CA za izdavanje privatnih certifikata aplikacijama i korisnicima u vašoj organizaciji.

Pravo planiranje i procjena su ključevi učinkovitog korištenja certifikata za njihove dodatne sigurnosne koristi. Trebate ponovo pregledati ova poglavlja da više naučite o radu certifikata i korištenju DCM-a za njihovo upravljanje i aplikacije koje ih koriste:

Što je novo za V5R2
Koristite ovu informaciju da bi doznali o promjenama na svojstvu Upravitelja digitalnih certifikata i promjenama u poglavlju informacija za ovo izdanje.

Ispis teme na pisač
Koristite ovu stranicu da saznate kako ispisati cijelo poglavlje kao PDF datoteku.

Migriranje na DCM sa ranijeg izdanja
Koristite ovu informaciju da saznate koje zadatke morate izvesti i druga razmatranja koja trebate uzeti u obzir ako migrirate postojeću verziju DCM-a na trenutno izdanje.

DCM scenariji
Koristite ove informacije da pregledate dva scenarija koja ilustriraju tipične sheme implementacije certifikata da vam pomognu planirati vlastitu implementaciju certifikata kao dio vaše iSeries politike sigurnosti. Svaki scenario također daje sve potrebne zadatke konfiguracije koje morate izvesti da upotrijebite scenario kako je opisano.

Koncepti digitalnog certifikata
Upotrijebite ovaj koncept i referentne informacije da bolje razumijete što su digitalni certifikati i kako rade. Naučite o različitim tipovima certifikata i kao ih možete koristiti kao dio vaše politike sigurnosti.

Plan za DCM
Upotrijebite ove informacije da vam pomognu kako i kada trebate koristiti digitalne certifikate za postizanje vašeg sigurnosnog cilja. Koristite ovu informaciju da naučite o preduvjetima koje trebate instalirati kao i ostalim zahtjevima koje morate uzeti u obzir prije korištenja DCM-a.

Konfiguriraj DCM
Upotrijebite ove informacije da naučite kako konfigurirati sve što trebate da osigurate da možete koristiti DCM za upravljanje vašim certifikatima i njihovim ključevima.

Upravljanje DCM-om
Upotrijebite ove informacije da naučite kako se koristi DCM za upravljanje vašim certifikatima i aplikacijama koje ga koriste. Možete također naučiti o tome kako digitalno potpisati objekte i kako kreirati i raditi sa vašim vlastitim Izdavačima certifikata.

Rješavanje pogrešaka u DCM
Upotrijebite ovu informaciju da naučite kako riješiti neke od najčešćih grešaka koje mogu nastati u korištenju DCM-a.

Povezane informacije za DCM
Koristite ovu stranicu za pronalaženje veza na druge resurse da bi naučili više o digitalnim certifikatima, infrastrukturi javnog ključa, Upravitelju digitalnih certifikata i drugim povezanim infomacijama.

Poglavlje 1. Što je novo za V5R2

Poboljšanja u V5R2 Upravitelju digitalnih certifikata (DCM) i mogućnostima iSeries digitalnih certifikata uključuju:

- **Dodjeljivanje funkcija certifikata**
  Ovaj novi DCM zadatak omogućava vam brže i jednostavnije dodjeljivanje certifikata jednoj ili više aplikacija. Možete pristupiti zadacima ili iz popisa zadataka **Upravljanje certifikatima** ili iz stranica brze staze **Rad sa poslužiteljem i certifikatima** i **Rad sa certifikatima potpisivanja objekata**. Ova funkcija je dostupna samo za *SYSTEM i *OBJECTSIGNING memorije certifikata.
- **Potpisivanje objekata naredbi (*CMD)**
  Sada možete koristiti DCM za kreiranje digitalnih potpisa na objektima naredbe (*CMD) za omogućavanje načina provjeravanja njihovog integriteta. Također, možete izabrati djelokrug potpisa za *CMD objekte; možete izabrati potpisivanje *CMD objekata u cijelosti ili potpisivanje samo glavnih komponenti objekta *CMD-a. Kada koristite DCM za gledanje potpisa na *CMD objektima, DCM pruža informacije o djelokrugu potpisa.
- **APIji za kreiranje certifikata korisnika potpisanih od Lokalnog CA bez korištenja DCM-a**
  Sada postoje dva nova APIja koje možete koristiti da programatski izdate certifikate potpisane od vašeg Lokalnog Izdavača certifikata (CA) ne-iSeries korisnicima. Ovi APIji vam dozvoljavaju da izdate certifikate korisnicima bez iSeries profila korisnika bez da korisnici koriste DCM da pojedinačno dobivaju certifikata za provjeru autentičnosti klijenta.

Nove ili poboljšane informacije za ovu temu uključuju:

- Dva nova scenarija koja možete koristiti da vam pomognu odrediti kako najbolje upotrijebiti certifikate za ispunjavanje vaših ciljeva sigurnosti.
- Reorganizirane informacije koje olakšavaju brzo pronalaženje informacija koje trebate za korištenje DCM-a.

Da pronađete druge informacije o tome što je novo ili promijenjeno u ovom izdanju, pogledajte vezu Memorandum korisnicima  .

Poglavlje 2. Ispiši ovo poglavlje

Za gledanje ili spuštanje PDF verzije, izaberite Upravitelj digitalnih certifikata  (veličina datoteke je oko 468 KB ili oko 110 stranica).

Da bi spremili PDF na vašu radnu stanicu za gledanje ili ispis:

1. Otvorite PDF u vašem pretražitelju (kliknite na gornju vezu).
2. U izborniku vašeg pretražitelja, kliknite **Datoteka**.
3. Kliknite **Spremi kao...**
4. Idite do direktorija u koji želite pohraniti PDF dokument.
5. Pritisnite **Spremi**.

Ako trebate Adobe Acrobat Reader za gledanje ili ispis PDF-a, možete spustiti kopiju sa Adobe Web stranice (www.adobe.com/prodindex/acrobat/readstep.html)  .

Poglavlje 3. Migrirajte sa ranije verzije DCM-a

Kada migrirate sa V4R3 verzije Upravitelja digitalnih certifikata (DCM) na V5R2, DCM automatski nadograđuje vaš postojeći lokalni Izdavač certifikata (CA) i datoteke prstenastih ključeva certifikata sistema. DCM ažurira te datoteke, koje se nazivaju default.kyr, u odgovarajuće datoteke memorije certifikata, koje se nazivaju default.kdb. DCM također migrira sve važeće certifikate u datoteke prstenova ključeva pridružene sa Hypertext Transfer Protocol (HTTP) i Lightweight Directory Access Protocol (LDAP) poslužiteljima. DCM migrira važeći certifikat u *SYSTEM memoriju certifikata default.kdb).

Bilješka: Ako migrirate sa V4R4, V4R5 ili V5R1 verzije DCM-a, ne morate izvoditi nikakve zadatke migracije jer su datoteke certifikata sa tih verzija kompatibilne sa V5R2 verzijom DCM-a.

Migracija prstenastog ključa u memoriju certifikata – V4R3 migracija

Za vrijeme V5R2 DCM instalacije, sistem migrirat sljedeće datoteke prstenastih ključeva:
- DCM-ove defaultne datoteke prstenova ključeva.
- Prstenovi ključeva koje koriste konfiguracijske datoteke HTTP poslužitelja.
- Prstenovi ključeva koje koriste konfiguracijske datoteke LDAP poslužitelja.

Ako koristite .kyr datoteku koju DCM nije automatski ažurirao, DCM ju konvertira u kyr.kdb datoteku kad s njom radite prvi put u DCM-u. Na primjer, kad prvi put specificirate datoteku secure.kyr u DCM korisničkom sučelju, DCM konvertira datoteku u novu memoriju certifikata sa imenom datoteke secure.kyr.kdb.

Bilješka: Prstenovi ključeva se razlikuju od memorija certifikata, tako da trebate konvertirati datoteke prstenova ključeva koje DCM nije automatski ažurirao tijekom rada sa njima preko DCM korisničkog sučelja. Ručna promjena proširenja imena datoteke u .kdb rezultira u greškama kad kasnije pokušate raditi sa tim datotekama preko DCM korisničkog sučelja.

Ako pokušate izbrisati secure.kyr datoteku tijekom korištenja DCM-a, DCM je u stvari arhivira i briše secure.kyr.kdb datoteku.

Default lozinka za memoriju certifikata

Ako postoji datoteka/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR, sistem migrira tu datoteku prstenova ključeva i sve druge prihvatljive datoteke prstenova ključeva u memoriju *SYSTEM certifikata. Originalna lozinka pridružena /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR datoteci se koristi kao lozinka za memoriju *SYSTEM certifikata.

Ako ne postoji datoteka /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR ali postoje druge datoteke prstenova ključeva prihvatljive za migraciju (na primjer, datoteke prstenova ključeva koje koriste datoteke za konfiguraciju HTTP poslužitelja), sistem kreira memoriju *SYSTEM certifikata sa lozinkom DEFAULT (sve velika slova) i dovršava migraciju.

Za više informacija o greškama koje se mogu desiti za vrijeme procesa migracije datoteke i informacije kako ih riješiti, pogledajte: Greške migracije i rješenja za obnavljanje.

Poglavlje 4. DCM scenariji

Upravitelj digitalnih certifikata i podrška digitalnog certifikata koji vaš iSeries omogućava dozvoljava vam da koristite certifikate da unaprijedite vašu politiku sigurnosti na više različitih načina. Kako izaberete koristiti certifikate razlikuje se i po vašim poslovnim ciljevima i vašim sigurnosnim potrebama.

Korištenje digitalnih certifikata vam može pomoći da unaprijedite vašu sigurnost na mnogo načina. Digitalni certifikati vam dopuštaju korištenje Sloja sigurnih utičnica (SSL) za sigurni pristup Web stranicama i drugim Internet uslugama. Digitalne certifikate možete koristiti za konfiguraciju veza vaše virtualne privatne mreže (VPN). Možete također koristiti certifikatov ključ za digitalno potpisivanje objekata ili da provjerite digitalne potpise da budete sigurni u autentičnost objekata. Takvi digitalni potpisi osiguravaju pouzdanost porijekla objekta i štite cjelovitost objekta.

Možete i dalje povećavati sistemsku sigurnost upotrebom digitalnih certifikata (umjesto korisničkih imena i lozinki) za provjeru identiteta i ovlaštenje sesije između poslužitelja i korisnika. Također, možete koristiti DCM da pridružite korisnikov certifikat njegovom ili njezinom iSeries korisničkom profilu. Certifikat ima iste autorizacije i dozvole kao pridruženi profil.

Kao posljedica, način na koji koristite certifikate može biti kompliciran i ovisi o raznim faktorima. Scenariji dani u ovom poglavlju opisuju neke od uobičajenijih ciljeva sigurnosti digitalnih certifikata unutar tipičnog poslovnog konteksta. Svaki scenario također opisuje sve potrebne sistemske i softverske preduvjete i sve zadatke konfiguracije koje morate izvoditi da bi implementirali scenario. Pregledajte te scenarije da vam pomognu odrediti kako korištenje certifikata za povećanu sigurnost može najbolje odgovarati vašim potrebama:

Scenario: Koristite certifikate za zaštitu pristupa javnim aplikacijama i resursima
Ovaj scenario opisuje kada i kako koristiti certifikate za zaštitu i ograničavanje pristupa od javnih korisnika na javne ekstranet resurse i aplikacije.

Scenario: Koristite certifikate za zaštitu pristupa unutarnjim aplikacijama i resursima
Ovaj scenario opisuje kada i kako koristiti certifikate za zaštitu i ograničavanje kojim resursima i aplikacijama interni korisnici mogu pristupati na vašim internim poslužiteljima.

Scenario: Koristite certifikate za zaštitu pristupa javnim aplikacijama i resursima

Situacija

Radite za osiguravajuće društvo (MyCo., Inc) i odgovorni ste za održavanje raznih aplikacija na intranet i ekstranet stranicama vašeg poduzeća. Jedna posebna aplikacija za koju ste odgovorni je aplikacija računanja rata koja dozvoljava stotinama nezavisnih agenata da generiraju kvote za svoje klijente. Zato što je informacija koju ova aplikacija pruža donekle osjetljiva, želite osigurati da je koriste samo registrirani agenti. Nadalje, želite eventualno pružiti sigurniju metodu za korisnički pristup aplikaciji nego što je to trenutna metoda korisničkog imena i lozinke. Zabrinuti ste da neovlašteni korisnici mogu uhvatiti ovu informaciju kada se prenosi preko nepouzdane mreže. Također, različiti agenti mogu dijeliti ovu informaciju međusobno bez ovlaštenja da to učine.

Nakon nešto istraživanja, odlučite da vam korištenje digitalnih certifikata može pružiti potrebnu sigurnost. Korištenje certifikata vam omogućava da koristite Sloj sigurnih utičnica (SSL) za zaštitu prijenosa podataka. Iako ćete kasnije htjeti da svi agenti koriste certifikat za pristup aplikaciji, znate da vaše poduzeće i vaši agent trebaju neko vrijeme prije nego taj cilj može biti postignut. Trenutno, planirate nastaviti trenutnu provjeru ovlaštenja pomoću korisničkog imena i lozinke zato što SSL štiti privatnost tih osjetljivih podataka u prijenosu.

Na osnovi tipa aplikacije i njihovih korisnika i vašeg budućeg cilja za provjeru autentičnosti certifikatima za korisnike, odlučite koristiti javni certifikat od vrlo poznatog Izdavača certifikata (CA) da konfigurirate SSL za vaše aplikacije.

Prednosti scenarija

Ovaj scenario ima sljedeće prednosti:
- Korištenje digitalnih certifikata za konfiguriranje SSL pristupa na vašu aplikaciju izračuna rata osigurava da je informacija koja je prenesena između poslužitelja i klijenta zaštićena i privatna.
- Korištenje digitalnih certifikata kad god je moguće za provjeru ovlaštenja klijenta pruža sigurniji način identificiranja ovlaštenih korisnika. Čak i kada nije moguće, provjera autentičnosti klijenta pomoću korisničkog imena i lozinke je zaštićena i zadržana privatnom od SSL sesije, čineći razmjenu tako osjetljivih podataka sigurnijom.
- Korištenje *javnih* digitalnih certifikata za ograničavanjem pristupa vašim aplikacijama i podacima je praktičan izbor pod ovim ili sličnim uvjetima:
  - Podaci i aplikacije iziskuju različite stupnjeve zaštite.
  - Stopa prometa među pouzdanim korisnicima je vrlo velika.
  - Vi pružate javni pristup aplikacijama i podacima, kao na Internet web stranici ili aplikaciji na ekstranetu.
  - Ne želite sami upravljati vašim Izdavačem certifikata (CA) zbog velikog broja korisnika koji pristupaju vašim aplikacijama i resursima ili zbog drugih administrativnih razloga.
- Korištenje javnog certifikata za konfiguriranje aplikacije za konfiguriranje rata za SSL u ovom scenariju smanjuje količinu konfiguracije koju korisnici moraju izvoditi za pristupanje aplikaciji. Većina softvera klijenta sadrži CA certifikate za većinu poznatih CA.

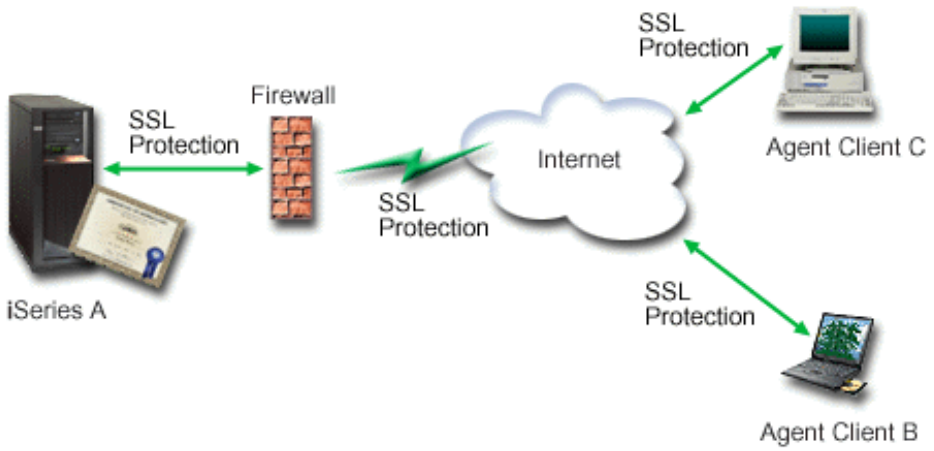
Ciljevi

U ovom scenariju, MyCo., Inc. želi koristiti digitalne certifikate za zaštitu informacija o izračunu rata koji njihova aplikacija pruža ovlaštenim javnim korisnicima. Poduzeće također želi sigurniju metodu autentificiranja onih korisnika kojima je dozvoljeno pristupiti tim aplikacijama.

Ciljevi ovog scenarija su sljedeći:
- Aplikacija izračuna rata poduzeća mora koristiti SSL za zaštitu privatnosti podataka koje daje korisnicima.
- SSL konfiguracija mora biti postignuta javnim certifikatima od poznatog javnog Internet izdavača certifikata (CA).
- Ovlašteni korisnici moraju pružati valjano korisničko ime i lozinku za pristupanje aplikaciji u SSL načinu. S vremenom, ovlašteni korisnici moraju biti sposobni koristiti jednu od dvije metode sigurne provjere autentičnosti da im bude dopušten pristup aplikaciji. Agenti moraju pokazati ili javni digitalni certifikat od poznatog Izdavača certifikata (CA) ili valjano korisničko ime i lozinku.

Detalji

Sljedeća slika objašnjava situaciju konfiguracije mreže za ovaj scenario:



Slika prikazuje sljedeće informacije o situaciji za ovaj scenario:

Javni poslužitelj poduzeća – iSeries A
- iSeries A je poslužitelj koji poslužuje aplikaciju poduzeća za izračun rata.
- iSeries A izvodi OS/400 Verziju 5 Izdanje 2 (V5R2).
- iSeries A ima instaliran dobavljač kriptografičkog pristupa (5722–AC3).
- iSeries A ima instaliran i konfiguriran Upravitelj digitalnih certifikata (OS/400 opcija 34) i IBM HTTP poslužitelj za iSeries (5722–DG1).
- iSeries A izvodi aplikaciju izračuna rata, koja je konfigurirana tako da:
  - Zahtijeva SSL način.
  - Koristi javni certifikat od poznatog Izdavača certifikata (CA) za SSL konfiguraciju.
  - Zahtijeva provjeru autentičnosti korisnika pomoću korisničkog imena i lozinke.
- iSeries A pokazuje svoj certifikat da započne SSL sesiju kada Klijenti B i C pristupaju aplikaciji.
- Nakon inicijaliziranja SSL sesije, iSeries A traži da Klijenti B i C pribave valjano korisničko ime i lozinku prije dopuštanja pristupa aplikaciji za izračunavanje rata.

Sistemi klijenta agenta – Klijent B i Klijent C
- Klijenti B i C su nezavisni agenti koji pristupaju aplikaciji za izračunavanje rata.
- Klijenti B i C imaju kopiju poznatog CA certifikata koji je izdao certifikat aplikacije koja je instalirana na njihovom softveru klijenta.
- Klijenti B i C pristupaju aplikaciji izračuna rata na iSeries A, koji pokazuje svoj certifikat softveru njihovih klijenata da bi provjerio njihov identitet i započeo SSL sesiju.
- Softver klijenata na Klijentima B i C je konfiguriran da prihvaća certifikat od iSeries A i SSL sesija počinje.
- Nakon što SSL sesija započne, Klijenti B i C moraju pribaviti valjano korisničko ime i lozinku prije nego iSeries A dopusti pristup aplikaciji.

Preduvjeti i pretpostavke

Ovaj scenario ovisi o sljedećim preduvjetima i pretpostavkama:
1. Aplikacija za izračunavanje rata na iSeries A je generička aplikacija koja može biti konfigurirana da koristi SSL. Većina aplikacija, uključujući mnoge iSeries aplikacije, pružaju SSL podršku. SSL koraci konfiguracije razlikuju se prilično među aplikacijama. Kao posljedica, ovaj scenario ne pruža specifične instrukcije za konfiguriranje aplikacije za izračun rata da koristi SSL. Ovaj scenario pruža instrukcije za konfiguriranje i upravljanje certifikatima koji su potrebni da bi bilo koja aplikacija koristila SSL.
2. *Opcijski*, aplikacija za izračun rata može pružiti mogućnost zahtijevanja certifikata za provjeru autentičnosti klijenta. Ovaj scenario pruža instrukcije kako koristiti Upravitelj

digitalnih certifikata (DCM) za konfiguriranje povjerenje certifikata za one aplikacije koje pružaju ovu podršku. Zato što se koraci konfiguracije poprilično razlikuju među aplikacijama, ovaj scenario ne pruža specifične instrukcije za konfiguriranje provjere autentičnosti certifikata klijenata za aplikaciju izračuna rata.

3. iSeries A odgovara zahtjevima za instaliranje i korištenje Upravitelja digitalnih certifikata (DCM).
4. Nitko nije prethodno konfigurirao ili koristio DCM na iSeries A.
5. Tkogod koristi DCM za izvođenje zadataka u ovom scenariju mora imati *SECADM i *ALLOBJ posebna ovlaštenja za svoj korisnički profil.
6. iSeries A nema instaliran IBM 4758-023 PCI kriptografički koprocesor.

Koraci zadatka

Za primjenu ovog scenarija, morate obaviti ove zadatke na iSeries A:

1. Dovršite sve korake preduvjeta za instaliranje i konfiguriranje svih potrebnih iSeries proizvoda.
2. Koristite Upravitelj digitalnih certifikata (DCM) za zahtjev kreiranja certifikata poslužitelja.
3. Konfigurirajte vašu aplikaciju da koristi Sloj sigurnih utičnica (SSL).
4. Koristite DCM da importirate i dodijelite potpisani certifikat poslužitelja ili klijenta ID-u aplikacije za vašu aplikaciju.
5. Pokrenite aplikaciju u SSL načinu, ako je potrebno.
6. *Opcijski zadatak*: Koristite DCM da definirate CA listu povjerenja da omogućite provjeru autentičnosti klijenta na temelju certifikata za aplikacije koje pružaju ovu podršku.

   Bilješka: Situacija koju ovaj scenario opisuje ne traži da aplikacija za izračun rata koristi certifikate za provjeru autentičnosti klijenta. Mnoge aplikacije pružaju podršku provjere autentičnosti certifikata klijenta; kako konfigurirate ovu podršku razlikuje se prilični između aplikacija. Ovaj opcijski zadatak vam je dan da vam pomogne razumjeti kako koristiti DCM za omogućavanje povjerenja certifikata za provjeru autentičnosti klijenta kao temelj za konfiguriranje podrške provjere autentičnosti certifikata klijenta za vašu aplikaciju.

Detalji konfiguracije

Dovršite sljedeće korake zadatka da koristite certifikate za konfiguriranje zaštićenog javnog pristupa aplikacijama i resursima kako ovaj scenario opisuje.

Korak 1: Dovršite zadatke koji su preduvjet za instaliranje svih potrebnih iSeries proizvoda

Morate dovršiti sve preduvjete za instaliranje i konfiguriranje svih potrebnih iSeries proizvoda prije nego možete izvoditi zadatke posebne konfiguracije za implementiranje ovog scenarija.

Korak 2: Kreirajte zahtjev certifikata poslužitelja ili klijenta

Da započnete proces korištenja Sloja sigurnih utičnica (SSL) za zaštitu komunikacije podataka aplikacije kako scenario opisuje, morate prvo dobiti digitalni certifikat od javnog Izdavača certifikata (CA). Koristite Upravitelj digitalnih certifikata (DCM) za kreiranje informacija koje javni CA zahtijeva za izdavanje certifikata.

Za započinjanje procesa dobivanja certifikata, dovršite ove korake:

1. Start DCM.

2. U navigacijskom okviru DCM-a odaberite **Kreiraj novu memoriju certifikata** da dovršite vođeni zadatak i popunite seriju obrazaca. Ovi obrasci vas vode kroz postupak kreiranja memorije certifikata i certifikata kojeg vaš administrator može koristiti za SSL sesije.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku, izaberite upitnik **?**) na vrhu stranice za pristup online pomoći.
3. Izaberite ***SYSTEM** kao memoriju certifikata za kreiranje i kliknite **Nastavi**.
4. Odaberite **Da** za kreiranje certifikata kao dijela kreiranja memorije *SYSTEM certifikata i klikniteNastavi.
5. Odaberite **VeriSign ili drugog Internet izdavača certifikata (CA)** kao potpisnika novog certifikata i klikniteNastavi za prikaz obrasca koji vam omogućuje da dadete informacije o identifikaciji za novi certifikat.
6. Popunite obrazac i klikniteNastavi za prikaz stranice certifikata. Stranica potvrde prikazuje podatke zahtjeva certifikata koje morate dostaviti javnom Izdavaču certifikata (CA) koji će izdati vaš certifikat. Podaci za zahtjev za potpisivanje certifikata sastoje se od javnog ključa i drugih informacija koje ste naveli za novi certifikat.
7. Pažljivo kopirajte i preslikajte CSR podatke u obrazac molbe za certifikat ili u posebnu datoteku, što CA traži kod zahtjeva za certifikat. Morate upotrijebiti sve CSR podatke, uključujući početne i krajnje linije zahtjeva za novi certifikat. Kad napustite ovu stranicu, podaci se gube i ne možete ih obnoviti.
8. Pošaljite obrazac molbe ili datoteku CA-u kojeg ste odabrali da izdaje i potpisuje vaše certifikate.
9. Čekajte da CA vrati potpisan, dovršen certifikat prije nego nastavite na sljedeći korak zadatka za ovaj scenario.

Nakon što CA vrati potpisan dovršen certifikat, možete konfigurirati vašu aplikaciju da koristi SSL, importirajte certifikat u *SYSTEM memoriju certifikata i pridružite je vašoj aplikaciji da koristi za SSL.

Korak 3: Konfigurirajte aplikaciju da koristi SSL

Kada dobijete vaš potpisani certifikat nazad od javnog Izdavača certifikata (CA), možete nastaviti proces omogućavanja komunikacije kroz Sloj sigurnih utičnica (SSL) za vašu javnu aplikaciju. Trebate konfigurirati vašu aplikaciju da koristi SSL prije rada sa vašim potpisanim certifikatom. Neke aplikacije, kao HTTP poslužitelj za iSeries generiraju jedinstveni ID aplikacije i registriraju ID sa Upraviteljem digitalnih certifikata (DCM) kada konfigurirate aplikaciju da koristi SSL. Morate znati ID aplikacije prije nego možete koristiti DCM da joj dodijeli vaš potpisani certifikat i dovršiti proces SSL konfiguracije.

Kako konfigurirati vašu aplikaciju da koristi SSL razlikuje se ovisno o aplikaciji. Ovaj scenario ne pretpostavlja specifičan izvor za aplikaciju za izračun rata koji opisuje jer postoji mnogo načina na koji MyCo., Inc. može pružati ovu aplikaciju svojim agentima.

Da konfigurirate vašu aplikaciju da koristi SSL, slijedite instrukcije koje vaša dokumentacija za aplikaciju pruža. Također, možete naučiti više o konfiguriranju mnogih uobičajenih IBM aplikacija da koriste SSL pregledavanjem poglavlja u Informacijskom Centru Sigurne aplikacije s SSL-om.

Korak 4: Importiranje i dodjela potpisanog javno certifikata

Nakon što ste konfigurirali vašu aplikaciju da koristi SSL, možete koristiti Upravitelj digitalnih certifikata (DCM) da importirate vaš potpisani certifikat pridružite ga vašoj aplikaciji.

Da importirate vaš certifikat i dodijelite ga vašoj aplikaciji da dovrši proces konfiguriranja SSL-a slijedite ove korake:

1. Start DCM.
2. U navigacijskom okviru kliknite **Izaberi memoriju certifikata** i izaberite ***SYSTEM** da se otvori memorija certifikata.
3. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za memoriju certifikata kad ste je kreirali i kliknite **Nastavi**.
4. Nakon osvježenja navigacijskog okvira izaberite**Upravljaj certifikatima** za prikaz popisa zadataka.
5. Sa popisa zadataka izaberite**Importiraj certifikat** da započnete postupak importiranja potpisanog certifikata u memoriju *SYSTEM certifikata.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku, izaberite upitnik **?**) na vrhu stranice za pristup online pomoći.
6. Sa popisa zadataka izaberite **Pridruži certifikat** iz liste zadataka **Upravljaj certifikatima** da prikažete listu certifikata u trenutnoj memoriji certifikata.
7. Izaberite certifikat sa popisa i kliknite**Dodijeli aplikacijama** da prikažete listu definicija aplikacija za trenutnu memoriju certifikata.
8. Izaberite vašu aplikaciju sa popisa i kliknite **Nastavi**. Prikazuje se stranica sa ili porukom potvrde za vaš izbor dodjela ili poruka o grešci ako se dogodio problem.

Kada su ovi zadaci dovršeni, možete započeti vašu aplikaciju u SSL načinu i započeti štititi privatnost podataka koje pruža.

Korak 5: Pokrenite aplikaciju u SSL načinu

Nakon što dovršite proces importiranja i dodjeljivanja certifikata vašoj aplikaciji, možda ćete trebati završiti i ponovno pokrenuti vašu aplikaciju u SSL načinu. To je potrebno u nekim slučajevima jer aplikacija ne može odrediti da postoji dodjela certifikata dok se aplikacija izvodila. Pregledajte dokumentaciju za vašu aplikaciju da odredite trebate li ponovo pokrenuti aplikaciju ili zbog drugih specifičnih informacija o pokretanju aplikacije u SSL načinu.

Opcijski korak 6: Definirajte popis pouzdanih CA-ova za aplikaciju koja zahtijeva certifikate za provjeru autentičnosti klijenta

Aplikacije koje podržavaju korištenje certifikata za provjeru autentičnosti klijenta tijekom sesije Sloja sigurnih utičnica (SSL) moraju odrediti da li prihvaćaju certifikat kao važeći dokaz identiteta. Jedan od kriterija kojeg aplikacija koristi za provjeru autentičnosti certifikata je da li aplikacija ima povjerenja u Izdavača certifikata (CA) koji je izdao certifikat.

Situacija koju ovaj scenario opisuje ne traži da aplikacija za izračun rata koristi certifikate za provjeru autentičnosti klijenta. Mnoge aplikacije pružaju podršku provjere autentičnosti certifikata klijenta; kako konfigurirate ovu podršku razlikuje se prilični između aplikacija. Ovaj opcijski zadatak vam je dan da vam pomogne razumjeti kako koristiti DCM za omogućavanje povjerenja certifikata za provjeru autentičnosti klijenta kao temelj za konfiguriranje vaših aplikacija da koriste certifikate za provjeru autentičnosti klijenta.

Prije nego što možete definirati popis pouzdanih CA, moraju se ispuniti nekoliko uvjeta:

- Aplikacija mora podržavati korištenje certifikata za provjeru autentičnosti klijenta.
- DCM definicija za aplikaciju mora navesti da aplikacija koristi popis pouzdanih CA.

Ako definicija za aplikaciju navede da aplikacija koristi popis pouzdanih CA morate definirati taj popis prije da aplikacija može uspješno izvesti provjeru autentičnosti klijenta certifikata. Time se osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA-ova,

koje ste naveli kao pouzdane. Ako korisnici ili klijentova aplikacija predoči certifikat od CA, koji nije naveden kao pouzdan na popisu pouzdanih CA-ova, ta aplikacija ga neće prihvatiti kao temelj za važeću provjeru autentičnosti.

Da koristite DCM da definirate popis pouzdanih CA-ova za neku aplikaciju, dovršite ove korake:

1. Start DCM.
2. U navigacijskom okviru kliknite **Izaberi memoriju certifikata** i izaberite ***SYSTEM** da se otvori memorija certifikata.
3. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za memoriju certifikata kad ste je kreirali i kliknite **Nastavi**.
4. Nakon osvježenja navigacijskog okvira izaberite**Upravljaj certifikatima** za prikaz popisa zadataka.
5. Sa popisa zadataka izaberite **Postavi CA status** da prikažete listu CA certifikata.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku, izaberite upitnik **?**) na vrhu stranice za pristup online pomoći.
6. Izaberite CA certifikat iz liste kojoj vaša aplikacija treba vjerovati i kliknite **Omogući** da prikažete listu aplikacija koje koriste CA listu povjerenja.
7. Izaberite aplikaciju sa popisa koja treba dodati izabrani CA na svoju list povjerenja i kliknite **OK**. Prikazuje se poruka na vrhu stranice koja pokazuje da će aplikacije koje ste izabrali vjerovati CA i certifikatima koje on izdaje.

Sada možete konfigurirati vašu aplikaciju da zahtijeva certifikate za provjeru autentičnosti klijenta. Slijedite upute koje su zadane dokumentacijom za vašu aplikaciju.

Scenario: Koristite certifikate za zaštitu pristupa unutarnjim aplikacijama i resursima

Situacija

Vi ste mrežni administrator za poduzeće (MyCo., Inc.) čiji odjel za ljudske potencijale je zabrinut zbog pravnih stvari i privatnosti zapisa. Zaposlenici poduzeća su zahtijevali da žele imati online pristup informacijama o svojim osobnim koristima i zdravstvenoj njezi. Poduzeće je odgovorilo na taj zahtjev kreiranjem interne web stranice da omogući te informacije zaposlenicima. Vi ste odgovorni za administriranje te interne web stranice.

Kako su zaposlenici smješteni u dva zemljopisno odvojena ureda i neki zaposlenici često putuju, zabrinuti ste za čuvanje privatnosti tih informacija jer putuju Internetom. Također, tradicionalno koristite korisničko ime i lozinku kao provjeru autentičnosti za ograničavanje pristupa podacima poduzeća. Zbog osjetljivosti i privatne prirode tih podataka, shvaćate da ograničavanje pristupa tim podacima na osnovi lozinki može biti nedovoljno. Konačno, ljudi mogu dijeliti, zaboraviti i čak ukrasti lozinke.

Nakon nešto istraživanja, odlučite da vam korištenje digitalnih certifikata može pružiti potrebnu sigurnost. Korištenje certifikata vam omogućava da koristite Sloj sigurnih utičnica (SSL) za zaštitu prijenosa podataka. Dodatno, možete koristiti certifikate umjesto lozinki da sigurnije provjeravate autentičnost korisnika i ograničite informacije odjela ljudskih potencijala kojima mogu pristupiti.

Zato, odlučujete postaviti privatni Lokalni Izdavač certifikata (CA) i izdavati certifikate svim zaposlenicima i da zaposlenici pridruže svoje certifikate svojim iSeries profilima korisnika. Ovaj tip implementacije privatnih certifikata vam dozvoljava da još pomnije nadgledate

pristup osjetljivim podacima, kao i kontrolirate privatnost podataka korištenjem SSL-a. Konačno, izdavanjem certifikata samom sebi, vjerojatnije je da vaši podaci ostanu sigurni i da su pristupni samo određenim osobama.

Prednosti scenarija

Ovaj scenario ima sljedeće prednosti:
- Korištenje digitalnih certifikata za konfiguriranje SSL pristupa na vaš web poslužitelj ljudskih potencijala osigurava da je informacija koja je prenesena između poslužitelja i klijenta zaštićena i privatna.
- Korištenje digitalnih certifikata za provjeru ovlaštenja klijenta pruža sigurniji način identificiranja ovlaštenih korisnika.
- Korištenje *privatnih* digitalnih certifikata za ograničavanjem pristupa vašim aplikacijama i podacima je praktičan izbor pod ovim ili sličnim uvjetima:
  - Zahtijevate visoki stupanj sigurnosti, posebno u odnosu na provjeru autentičnosti korisnika.
  - Vjerujete pojedincima kojima izdajete certifikate.
  - Vaši korisnici već imaju iSeries korisničke profile za kontroliranje njihovih pristupa aplikacijama i podacima.
  - Želite raditi sa vlastitim izdavačem certifikata (CA).
- Korištenje privatnih certifikata za provjeru autentičnosti klijenta vam omogućava da jednostavnije pridružujete certifikat sa korisničkim profilom ovlaštenog iSeries korisnika. Ovo pridruživanje certifikata profilu korisnika omogućava HTTP poslužitelju da odredi profil korisnika vlasnika certifikata za vrijeme provjere autentičnosti. HTTP poslužitelj ih tada može zamijeniti i izvoditi pod tim profilom korisnika ili izvoditi akcije za tog korisnika na osnovi informacija u profilu korisnika.

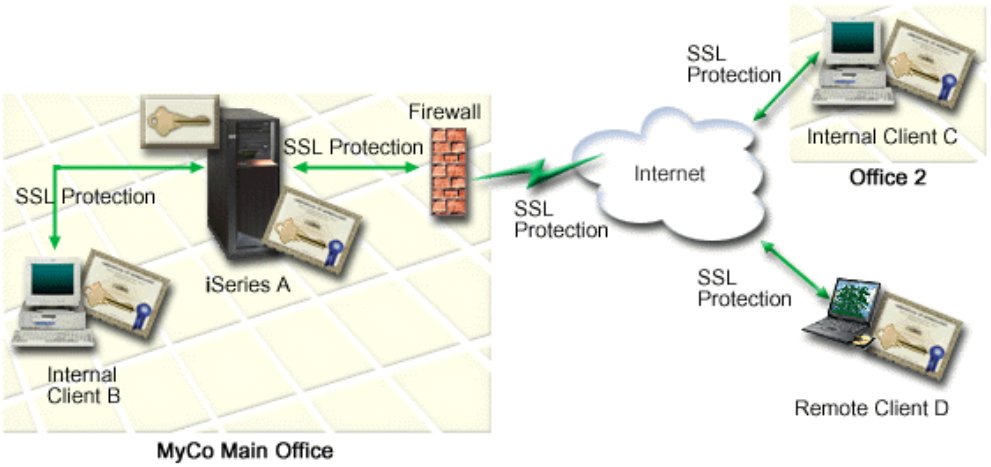
Ciljevi

U ovom scenariju, MyCo., Inc. želi koristiti digitalne certifikate za zaštitu osjetljivih osobnih informacija koji njihova interna web stranica ljudskih potencijala zaposlenicima poduzeća. Poduzeće također želi sigurniju metodu autentificiranja onih korisnika kojima je dozvoljeno pristupiti toj web stranici.

Ciljevi ovog scenarija su sljedeći:
- Interna web stranica ljudskih potencijala mora koristiti SSL za zaštitu privatnosti podataka koje daje korisnicima.
- SSL konfiguracija mora bit postignuta privatnim certifikatima od internog Lokalnog izdavača certifikata (CA).
- Ovlašteni korisnici moraju pružati valjani certifikat za pristupanje web stranici u SSL načinu.

Detalji

Sljedeća slika objašnjava situaciju konfiguracije mreže za ovaj scenario:



Slika prikazuje sljedeće informacije o situaciji za ovaj scenario:

Web poslužitelj ljudskih potencijala poduzeća – iSeries A
- iSeries A je poslužitelj koji poslužuje web aplikaciju poduzeća ljudskih potencijala.
- iSeries A izvodi OS/400 Verziju 5 Izdanje 2 (V5R2).
- iSeries A ima instaliran dobavljač kriptografičkog pristupa (5722–AC3).
- iSeries A ima instaliran i konfiguriran Upravitelj digitalnih certifikata (OS/400 opcija 34) i IBM HTTP poslužitelj za iSeries (5722–DG1).
- iSeries A izvodi aplikaciju ljudskih potencijala, koja je konfigurirana tako da:
  - Zahtijeva SSL način.
  - Koristi privatni certifikat od Lokalnog Izdavača certifikata (CA) za SSL konfiguraciju.
  - Zahtijeva certifikate za provjeru autentičnosti klijenta.
- iSeries A pokazuje svoj certifikat da započne SSL sesiju kada Klijenti B, C i D pristupaju aplikaciji.
- Nakon inicijaliziranja SSL sesije, iSeries A traži da Klijenti B, C i D pribave valjani certifikat prije dopuštanja pristupa aplikaciji ljudskih potencijala. Ova razmjena certifikata je vidljiva korisnicima Klijenata B, C i D.

Sistemi klijenata zaposlenika– Klijent B, Klijent C i Klijent D
- Klijent B je zaposlenik koji radi u glavnom uredu MyCo gdje je smješten iSeries A.
- Klijent C je zaposlenik koji radi u drugom uredu MyCo koji je zemljopisno odijeljen od glavnog ureda.
- Klijent D je zaposlenik koji radi udaljeno i često putuje zbog posla poduzeća i mora moći sigurno pristupiti web stranici ljudskih potencijala bez obzira na fizičku lokaciju.
- Klijenti B, C i D su zaposlenici poduzeća koji pristupaju aplikaciji ljudskih potencijala.
- Klijenti B, C i D imaju kopiju Lokalnog CA certifikata koji je izdao certifikat aplikacije koja je instalirana na njihovom softveru klijenta.
- Klijenti B, C i D pristupaju aplikaciji ljudskih potencijala na iSeries A, koji pokazuje svoj certifikat softveru njihovih klijenata da bi provjerio njihov identitet i započeo SSL sesiju.
- Softver klijenata na Klijentima B, C i D je konfiguriran da prihvaća certifikat od iSeries A i SSL sesija počinje.
- Nakon što SSL sesija započne, Klijenti B, C i D moraju pribaviti valjani certifikat prije nego iSeries A dopusti pristup aplikaciji.

Preduvjeti i pretpostavke

Ovaj scenario ovisi o sljedećim preduvjetima i pretpostavkama:

1. IBM HTTP poslužitelj za iSeries izvodi aplikaciju ljudskih potencijala na iSeries A. Dvije su vrste HTTP poslužitelja za iSeries (original i Apache podržan) i značajno revidirana verzija HTTP poslužitelja će biti dostupna nakon izdavanja ovih informacija. Kao posljedica, ovaj scenario ne pruža *specifične* upute za konfiguriranje HTTP poslužitelja da koristi SSL. Ovaj scenario pruža instrukcije za konfiguriranje i upravljanje certifikatima koji su potrebni da bi bilo koja aplikacija koristila SSL.
2. Http poslužitelj može pružiti mogućnost zahtijevanja certifikata za provjeru autentičnosti klijenta. Ovaj scenario pruža instrukcije kako koristiti Upravitelj digitalnih certifikata (DCM) za konfiguriranje zahtjeva upravljanja certifikatima za ovaj scenario. Ipak, ovaj scenario ne pruža *specifične* korake konfiguracije za konfiguriranje provjere autentičnosti certifikata klijenta za HTTP poslužitelj.
3. HTTP poslužitelj ljudskih potencijala na iSeries A već koristi zaštitu lozinkom.
4. iSeries A odgovara zahtjevima za instaliranje i korištenje Upravitelja digitalnih certifikata (DCM).
5. Nitko nije prethodno konfigurirao ili koristio DCM na iSeries A.
6. Tkogod koristi DCM za izvođenje zadataka u ovom scenariju mora imati *SECADM i *ALLOBJ posebna ovlaštenja za svoj korisnički profil.
7. iSeries A nema instaliran IBM 4758-023 PCI kriptografički koprocesor.

Koraci zadatka

Dva su skupa zadataka koje morate dovršiti za implementiranje ovog scenarija: Jedan skup zadataka vam dozvoljava da postavite aplikaciju ljudskih potencijala na iSeries A da koristi SSL i zahtijeva certifikate za provjeru autentičnosti korisnika. Drugi skup zadataka dozvoljava vašim korisnicima na Klijentima B, C i D da sudjeluju u SSL sesijama sa aplikacijom ljudskih potencijala i dobivaju certifikate za provjeru autentičnosti korisnika.

Koraci zadatka aplikacije Web poslužitelja ljudskih potencijala

Za primjenu ovog scenarija, morate obaviti ove zadatke na iSeries A:
1. Dovršite sve korake preduvjeta za instaliranje i konfiguriranje svih potrebnih iSeries proizvoda.
2. Konfigurirajte vaš HTTP poslužitelj ljudskih potencijala da koristi SSL i zabilježite ID aplikacije za instancu poslužitelja.
3. Koristite Upravitelj digitalnih certifikata (DCM) da kreirate i koristite Lokalni CA i koristite ga da izdate certifikate za HTTP poslužitelj ljudskih potencijala. Ovaj vođeni zadatak također osigurava da dodijelite certifikat Web poslužitelj aplikaciji i dodate CA na popis onih kojima aplikacija vjeruje.
4. Konfigurirajte Web poslužitelj ljudskih potencijala da zahtijeva certifikate za provjeru autentičnosti klijenta.
5. Pokrenite HTTP poslužitelj ljudskih potencijala u SSL načinu.

Koraci zadatka konfiguracije klijenta

Da implementirate ovaj scenario, svaki korisnik (Klijenti B, C i D) koji će pristupiti web poslužitelju na iSeries A moraju izvesti ove zadatke:
6. Instalirati kopiju Lokalnog CA certifikata u svoj softver pretražitelja.
7. Zatražiti certifikat od Lokalnog CA.

Detalji konfiguracije

Dovršite sljedeće korake zadatka da koristite certifikate za konfiguriranje zaštićenog pristupa internim aplikacijama i resursima kako ovaj scenario opisuje.

Korak 1: Dovršite zadatke koji su preduvjet za instaliranje svih potrebnih iSeries proizvoda

Morate dovršiti sve preduvjete za instaliranje i konfiguriranje svih potrebnih iSeries proizvoda prije nego možete izvoditi zadatke posebne konfiguracije za implementiranje ovog scenarija.

Korak 2: Konfigurirajte HTTP poslužitelj ljudskih potencijala da koristi SSL

Koraci konfiguracije Sloja sigurnih utičnica (SSL) za HTTP poslužitelj ljudskih potencijala na iSeries A ovisi o tome koristite li originalnu ili Apache podržanu verziju.

Za određenije informacije o konfiguriranju HTTP poslužitelja (original) da koristi SSL, pogledajte Konfiguriraj sigurni poslužitelj na HTTP poslužitelju.

Za određene informacije o konfiguriranju HTTP poslužitelja (Apache podržan) da koristi SSL, pogledajte Scenario: JKL omogućuje zaštitu sloja sigurnih utičnica (SSL) na svojem HTTP poslužitelju (Apache podržan). Ovaj scenario pruža sve korake zadatka za kreiranje virtualnog hosta i konfiguriranje da koristi SSL. Za specifične korake za konfiguriranje SSL-a, pogledajte naslov ″Omogući SSL za virtualni host.″

Za dodatne informacije o konfiguriranju trenutne i budućih verzija HTTP poslužitelja za iSeries (original ili Apache podržan), pogledajte poglavlje Web posluživanje.

Korak 3: Kreirajte i koristite Lokalni CA

Nakon što konfigurirate HTTP poslužitelj ljudskih potencijala da koristi sloj sigurnih utičnica (SSL), morate konfigurirati certifikat da bi ga poslužitelj koristio da inicira SSL. Na osnovi ciljeva za ovaj scenario, izabrali ste kreiranje i korištenje Lokalnog Izdavača certifikata (CA) da izda certifikat poslužitelju.

Kada koristite Upravitelj digitalnih certifikata (DCM) za kreiranje Lokalnog CA, vođeni ste kroz proces koji osigurava da konfigurirate sve što trebate da bi omogućili SSL za vašu aplikaciju. To uključuje dodjeljivanje certifikata koje Lokalni CA izdaje vašoj Web poslužitelj aplikaciji. Također, dodajete Lokalni CA pouzdanoj listi CA za Web poslužitelj aplikaciju. To što je Lokalni CA u listi pouzdanosti aplikacije osigurava da aplikacija može prepoznati i ovlastiti korisnike koji pokažu certifikate koje Lokalni CA izdaje.

Za korištenje Upravitelja digitalnih certifikata (DCM) da kreira i koristi CA i izdaje certifikat vašoj poslužiteljskoj aplikaciji ljudskih potencijala, dovršite ove korake:

1. Start DCM.
2. U navigacijskom okviru DCM-a odaberite **Kreiraj Izdavača certifikata (CA)** za prikaz slijeda obrazaca. Ovi obrasci vas vode kroz proces kreiranja Lokalnog CA i dovršavanja drugih zadataka koji su potrebni za započinjanje korištenja digitalnih certifikata za SSL, potpisivanje objekata i provjeru potpisa.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku, izaberite upitnik **?**) na vrhu stranice za pristup online pomoći.
3. Dovršite obrasce za ovaj vođeni zadatak. Kod korištenja ovih obrazaca za izvođenje svih zadataka koji su potrebni za postavljanje Lokalnog Izdavača certifikata (CA), vi:
   a. Dajete informaciju identifikacije za Lokalni CA.
   b. Instalirate Lokalni CA certifikat na vaš PC ili na vaš pretražitelj tako da vaš softver može prepoznati provjeriti Lokalni CA i provjeriti certifikate koje Lokalni CA izdaje.
   c. Izaberite politiku podataka za vaš Lokalni CA.

      Bilješka: Budite sigurni da ste izabrali da Lokalni CA može izdati certifikate korisnika.
   d. Koristite novi Lokalni CA da izdate certifikat poslužitelja ili klijenta koje vaše aplikacije mogu koristiti za SSL veze.

e. Izabrati aplikacije koje mogu koristiti poslužiteljski ili klijentski certifikat za SSL veze.

   Bilješka: Budite sigurni da ste izabrali ID aplikacije za vaš HTTP poslužitelj ljudskih potencijala.

f. Koristite novi Lokalni CA da izdate certifikat potpisivanja objekata koje vaše aplikacije mogu koristiti za digitalno potpisivanje objekata. Ovaj podzadatak kreira memoriju *OBJECTSIGNING certifikata; to je memorija certifikata koju koristite za upravljanje certifikatima za potpisivanje objekata.

   Bilješka: Iako ovaj scenarij ne koristi certifikate potpisivanja objekata, obavezno dovršite ovaj korak. Ako odustanete na ovom mjestu u zadatku, zadatak završava i morate izvoditi zasebne zadatke za dovršenje vaše konfiguracije SSL certifikata.

g. Izaberite aplikacije koje trebaju imati povjerenje u Lokalni CA.

   Bilješka: Budite sigurni da ste izabrali ID aplikacije za vaš HTTP poslužitelj ljudskih potencijala kao jednu od aplikacija koja vjeruje Lokalnom CA.

Sada kada ste dovršili konfiguraciju certifikata koju vaša Web poslužitelj aplikacija zahtijeva za korištenje SSL-a, možete konfigurirati Web poslužitelj aplikaciju da zahtijeva certifikate za provjeru autentičnosti korisnika.

Korak 4: Konfigurirajte Web poslužitelj ljudskih potencijala da zahtijeva certifikate za provjeru autentičnosti klijenta

Koraci konfiguracije Sloja sigurnih utičnica (SSL) za zahtijevanje certifikata za provjeru autentičnosti klijenta za HTTP poslužitelj na iSeries A ovisi o tome koristite li originalnu ili Apache podržanu verziju aplikacije.

za određenije informacije o konfiguriranju HTTP poslužitelja (original) da zahtijeva certifikate za provjeru autentičnosti klijenta, pogledajte Kreiraj postave zaštite na HTTP poslužitelju (original).

Za određene informacije o konfiguriranju HTTP poslužitelja (Apache podržan) da koristi certifikate za provjeru autentičnosti klijenta, pogledajte Scenario: JKL omogućuje zaštitu sloja sigurnih utičnica (SSL) na svojem HTTP poslužitelju (Apache podržan). Ovaj scenario HTTP poslužitelja pruža sve korake zadatka za kreiranje virtualnog hosta i konfiguriranje da koristi SSL i certifikate za provjeru autentičnosti klijenta. Za specifične korake za konfiguriranje SSL-a i certifikata za provjeru autentičnosti klijenta, pogledajte naslov ″Omogući SSL za virtualni host.″

Za dodatne informacije o konfiguriranju trenutne i budućih verzija HTTP poslužitelja za iSeries (original ili Apache podržan), pogledajte poglavlje Web posluživanje.

Korak 5: Pokrenite Web poslužitelj ljudskih potencijala u SSL načinu

Možda ćete trebati zaustaviti i ponovo pokrenuti vaš HTTP poslužitelj da osigurate da poslužitelj može odrediti da postoji dodjela certifikata i koristiti ga za pokretanje SSL sesije.

Da zaustavite i pokrenete HTTP poslužitelj (original), koristite obrasce Konfiguracija i administracija i slijedite ove korake:

1. Kliknite **Administracija**.
2. Kliknite **Upravljaj HTTP poslužiteljima**.
3. Izaberite poslužitelj.
4. Unesite opcijske parametre za pokretanje u polju koje je dano na obrascu.

5. Kliknite **Pokreni**.

   Bilješka: Ako je poslužitelj bio pokrenut kada ste napravili dodjele certifikata, trebate pritisnuti Stop, i Pokrenuti poslužitelj. Klikom na **Ponovo pokreni** ne osigurava uvijek da je poslužitelj u stanju odrediti promjene certifikata koje su se dogodile za vrijeme izvođenja.

Da zaustavite i pokrenete HTTP poslužitelj (podržan), koristite obrasce Konfiguracija i administracija i slijedite ove korake:
1. Kliknite **Administracija**.
2. U izborniku lijevo, kliknite **Upravljaj HTTP poslužiteljima** pod **Opća administracija poslužitelja**.
3. Izaberite poslužitelj sa kojim želite raditi i kliknite **Start** ili **Stop**. Obratite se na online pomoć za više informacija o parametrima pokretanja.

Za dodatne informacije o upravljanju trenutnom i budućim verzijama HTTP poslužitelja za iSeries (original ili Apache podržan), pogledajte poglavlje Web posluživanje.

Kada su ovi zadaci dovršeni, možete započeti vašu aplikaciju ljudskih potencijala u SSL načinu i započeti štititi privatnost podataka koje pruža.

Korak 6: Neka korisnici instaliraju kopiju Lokalnog CA certifikata na svoj softver pretražitelja.

Kad korisnici pristupaju poslužitelju koji pruža vezu Sloja sigurnih utičnica (SSL), poslužitelj predočava certifikat korisnikovom klijentovom softveru kao dokaz njegovog identiteta. Softver klijenta mora zatim provjeriti poslužiteljev certifikat da poslužitelj može uspostaviti sesiju. Da provjerite valjanost certifikata poslužitelja, klijentov softver mora imati pristup lokalno pohranjenoj kopiji certifikata za Izdavača certifikata (CA), koji je izdao poslužiteljev certifikat. Ako poslužitelj pokazuje certifikate os javnog Internet CA, tada bi korisnikov pretražitelj ili drugi softver klijenta trebao već imati kopiju CA certifikata. Ako, kao u ovom scenariju, poslužitelj pokazuje certifikat od privatnog Lokalnog CA, svaki korisnik mora koristiti Upravitelj digitalnih certifikata (DCM) za instaliranje kopije Lokalnog CA certifikata.

Svaki korisnik (Klijenti B, C i D) moraju dovršiti ove korake da dobiju kopiju Lokalnog CA certifikata:
1. Start DCM.
2. U navigacijskom okviru, izaberite **Instalirajte Lokalni CA certifikat na vaš PC** da bi prikazali stranicu koja vam dozvoljava da spustite Lokalni CA certifikat na vaš pretražitelj ili ga spremite u datoteku na vašem sistemu.
3. Izaberite opciju za instaliranje certifikata. Ova opcija spušta Lokalni CA certifikat kao pouzdano ishodište u vašem pretražitelju. Time se osigurava da vaš pretražitelj može postaviti sesije sigurnih komunikacija sa web poslužiteljima koji koriste certifikat od tih CA-ova. Vaš pretražitelj će prikazati seriju prozora da vam pomogne dovršiti instalaciju.
4. Kliknite **OK** za vraćanje na početnu stranicu Upravitelj digitalnih certifikata.

Korak 7: Neka svaki korisnik zatraži certifikat od Lokalnog CA

U ranijim koracima, konfigurirali ste web poslužitelj ljudskih potencijala da zahtijeva certifikate za provjeru autentičnosti korisnika. Sada korisnici moraju pokazati valjani certifikat od Lokalnog CA prije nego im je dozvoljeno pristupiti web poslužitelju. Svaki korisnik mora koristiti Upravitelj digitalnih certifikata (DCM) da dobije certifikat korištenjem zadatka **Kreiraj certifikat**. Da bi dobio certifikat od Lokalnog CA, politika Lokalnog CA mora dozvoliti da CA izda certifikate korisnika.

Svaki korisnik (Klijenti B, C i D) moraju dovršiti ove korake da dobiju certifikat:

1. Start DCM.
2. U navigacijskom okviru odaberite **Kreiraj certifikat**.
3. Odaberite **Korisnički certifikat** kao tip certifikata za kreiranje. Prikaže se obrazac tako da možete unijeti informacije o identifikaciji za certifikat.
4. Popunite obrazac i kliknite **Nastavi**.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku, izaberite upitnik **?**) na vrhu stranice za pristup online pomoći.
5. U ovom trenutku DCM radi sa vašim pretražiteljem na kreiranju privatnog i javnog ključa za certifikat. Preglednik može prikazati i prozor koji će vas voditi kroz ovaj postupak. Slijedite upute pretražitelja za ove poslove. Nakon što pretražitelj generira ključeve, stranica potvrde pokazuje da je DCM kreirao certifikat.
6. Instalirajte novi certifikat na vaš softver preglednika. Preglednik može prikazati i prozor koji će vas voditi kroz ovaj postupak. Slijedite upute koje vam daje pretražitelj i završite posao.
7. Kliknite **OK** da dovršite zadatak.

Tijekom obrade, Upravitelj digitalnih certifikata automatski pridružuje certifikat vašem iSeries korisničkom profilu.

Poglavlje 5. Koncepti digitalnog certifikata

Prije nego što počnete koristiti digitalne certifikate za povećanje sigurnosne politike vašeg sistema i mreže, trebate shvatiti što su oni i koje prednosti u sigurnosti oni daju.

Digitalni certifikat je digitalna vjerodajnica koja provjerava valjanost identiteta vlasnika certifikata, slično kao putovnica. Pouzdana strana, nazvana Izdavač certifikata (CA) izdaje digitalne certifikate korisnicima i aplikacijama poslužitelja ili klijenta. Povjerenje u CA je temelj povjerenja u certifikat kao valjanu vjerodajnicu.

Da naučite više o konceptima digitalnih certifikata, pregledajte ova poglavlja:

Razlikovno ime
Pročitajte ove informacije da više naučite o osobinama identifikacije digitalnih certifikata.

Digitalni potpisi
Pročitajte ove informacije da naučite što su digitalni certifikati i kako rade da osiguraju cjelovitost objekata.

Javni privatni par ključeva
Pročitajte ove informacije da više naučite o sigurnosnim ključevima pridruženim digitalnim certifikatima.

Izdavač certifikata (CA)
Pročitajte ove informacije da više naučite o CA-ovima, cjelinama koje izdaju digitalne certifikate.

CRL lokacije
Pročitajte ove informacije da naučite što je Popis opozvanih certifikata (CRL) i kako se oni koriste u postupku provjere valjanosti i provjere autentičnosti certifikata.

Memorije certifikata
Pročitajte ove informacije da naučite što je memorija certifikata i kako se treba koristiti Upravitelja digitalnih certifikata da se radi s njima i certifikatima koje oni sadrže.

Kriptografija
Pročitajte ove informacije da naučite što je kriptografija i kako digitalni certifikati koriste kriptografičke funkcije za omogućavanje sigurnosti.

Sloj sigurnih utičnica (SSL)
Pročitajte ove informacije za kratak opis SSL-a.

Razlikovno ime

Svaki CA ima politiku kojom određuje koje informacije za identificiranje zahtjeva CA da može izdati certifikat. Neki javni Internet izdavači certifikata zahtijevaju malo informacija, kao što je ime i adresa e-pošte. Drugi javni CA-ovi mogu prije izdavanja certifikata, zahtijevati više informacija i zahtijevati točan dokaz tih informacija za identificiranje. Na primjer, CA-ovi koji podržavaju Public Key Infrastructure Exchange (PKIX) standarde, mogu zatražiti prije izdavanja certifikata, da zahtjevatelj provjeri informacije identiteta putem Izdavača registracije (RA). Prema tome, ako planirate prihvatiti i koristiti certifikate kao vjerodajnice, trebate pregledati zahtjeve identifikacije za CA da odredite da li su njihovi zahtjevi u skladu sa vašim sigurnosnim potrebama.

Razlikovno ime (DN) je pojam koji opisuje identifikacijske informacije vlasnika certifikata i dio je samog certifikata. Ovisno o politici identificiranja od CA, koji izdaje certifikat, DN može uključiti razne informacije. Možete koristiti Upravitelja digitalnih certifikata (DCM) za rad sa privatnim Izdavačem certifikata i izdavanje privatnih certifikata. Također, možete

koristiti DCM za generiranje DN informacija i parova ključeva za certifikate koje izdaje javni Internet CA za vašu organizaciju. DN informacije koje možete pribaviti za oba tipa certifikata uključuju:
- Obično ime vlasnika certifikata
- Organizacija
- Organizacijska jedinica
- Grad
- Država
- Zemlja

Kad koristite DCM za izdavanje privatnih certifikata možete pribaviti dodatne DN informacije za certifikat, uključujući:
- Verzija 4 IP adresa
- Potpuno kvalificirano ime domene
- Adresa e-pošte

Ove dodatne informacije su korisne ako planirate koristiti certifikat za konfiguriranje veze virtualne privatne mreže (VPN).

Digitalni potpisi

Digitalni potpis na elektroničkom dokumentu ili drugom objektu kreira se korištenjem obrasca šifriranja i ekvivalentan je osobnom potpisu na pisanom dokumentu. Digitalni potpis daje dokaz o porijeklu objekta i način kako provjeriti cjelovitost objekta. Vlasnik digitalnog certifikata potpisuje objekt korištenjem privatnog ključa certifikata. Primatelj objekta koristi odgovarajući javni ključ certifikata za dešifriranje potpisa, koji ovjerava cjelovitost potpisanog objekta i ovjerava odašiljatelja kao izvora.

Izdavač certifikata (CA) potpisuje certifikate koje izdaje. Ovaj potpis se sastoji od podatkovnog niza koji se šifrira privatnim ključem izdavača certifikata. Svaki korisnik može potom provjeriti potpis na certifikatu koristeći se javnim ključem Izdavača certifikata za dešifriranje potpisa.

Digitalni potpis je elektronički potpis koji vi ili aplikacija kreirate na objektu korištenjem privatnog ključa digitalnog certifikata. Digitalni potpis na objektu daje jedinstveno elektroničko vezivanje identiteta potpisnika (vlasnika ključa potpisivanja) sa porijeklom objekta. Kada pristupite objektu koji sadrži digitalni potpis, možete provjeriti potpis na objektu da provjerite porijeklo objekta kao valjano (na primjer, da aplikacija koju spuštate zaista dolazi od ovlaštenog izvora kao IBM). Ovaj proces provjere također vam omogućava da odredite je li bilo neovlaštenih promjena na objektu od kada je potpisan.

Primjer kako radi digitalni potpis

Razvijač softvera je kreirao iSeries aplikaciju koju želi distribuirati preko Interneta kao prikladan isplativ način za svoje korisnike. Ipak, zna da su korisnici opravdano zabrinuti kada se radi o spuštanju programa preko Interneta zbog rastućeg problema objekata koji se prikazuju kao legitimni programi ali stvarno sadrže štetne programe, kao virusi.

Kao posljedica, odlučuje digitalno potpisati aplikaciju tako da korisnici mogu provjeriti da je njegovo poduzeće legitimni izvor aplikacije. Koristi privatni ključ od digitalnog certifikata koji je dobio od poznatog javnog Izdavača certifikata da potpiše aplikaciju. Tada je čini dostupnom za spuštanje korisnicima. Kao dio paketa koji se spušta uključuje kopiju digitalnog certifikata koji je koristio za potpisivanje objekta. Kada korisnik spušta aplikacijski paket, korisnik može koristiti javni ključ certifikata da provjeri potpis aplikacije. Ovaj proces dozvoljava korisniku da identificira i provjeri aplikaciju, kao i da osigura da sadržaj aplikacije nije mijenjan od kada je potpisan.

Javni privatni par ključeva

Svaki digitalni certifikat ima par pridruženih kriptografičkih ključeva. Par ključeva se sastoji od privatnog ključa i javnog ključa. (Certifikati za provjeru potpisa su izuzetak ovom pravilu i imaju pridružen samo javni ključ.)

Javni ključ je dio digitalnog certifikata vlasnika i dostupan je bilo kome na korištenje. Privatni ključ je međutim zaštićen i dostupan samo vlasniku ključa. Ovako ograničeni pristup osigurava da komunikacije koje koriste taj ključ ostanu sigurne i zaštićene.

Vlasnik certifikata može koristiti te ključeve da iskoristi svojstva kriptografičke sigurnosti koje pružaju ključevi. Na primjer, vlasnik certifikata može koristiti privatni ključ certifikata da potpiše i šifrira podatke koji su poslani između korisnika i poslužitelja, kao poruke, dokumente i kodirane objekte. Primaoc potpisanog objekta može tada koristiti javni ključ sadržan u certifikatu potpisnika za dešifriranje potpisa. Takvi digitalni potpisi osiguravaju pouzdanost porijekla objekta i daju način provjere cjelovitosti objekta.

Izdavač certifikata (CA)

Izdavač certifikata (CA) je pouzdani centralni administrativan entitet koji može izdati digitalne certifikate korisnicima i poslužiteljima. Povjerenje u CA je osnova povjerenja u certifikat kao valjanu vjerodajnicu. CA koristi svoje privatne ključeve za kreiranje digitalnog potpisa na certifikatu koji izdaje za provjeru valjanosti porijekla certifikata. Drugi mogu koristiti javni ključ CA certifikata za provjeru autentičnosti certifikata koje CA izdaje i potpisuje.

CA može biti bilo javna komercijalna cjelina, kao što je VeriSign ili može biti privatna cjelina s kojom radi neka organizacija za interne svrhe. Neke tvrtke pružaju komercijalne usluge za izdavanje potvrda korisnicima Interneta. Upravitelj digitalnog certifikata (DCM) vam dopušta upravljanje certifikatima sa javnih i privatnih CA.

Možete koristiti DCM za rad i na vašem vlastitom privatnom CA za izdavanje privatnih certifikata sistemima i korisnicima. Kada CA izda korisnički certifikat, DCM automatski pridružuje certifikat sa korisnikovim iSeries sistemskim profilom korisnika. Time se osigurava da pristup i privilegije ovlaštenja tog certifikata budu iste kao one kod vlasnikovog korisničkog profila.

Stanje pouzdanog korijena

Izraz pouzdani korijen upućuje na posebno označavanje koje se daje certifikatu Izdavača certifikata. To označavanje pouzdanog korijena dopušta pretražitelju ili drugoj aplikaciji provjeru autentičnosti i prihvaćanje certifikata koje izdaje Izdavač certifikata (CA).

Kad učitate certifikat Izdavača certifikata u vaš pretražitelj, pretražitelj vam dopušta da certifikat označite kao pouzdani korijen. Druge aplikacije koje podržavaju upotrebu certifikata moraju također biti konfigurirane za povjerenje CA prije nego što aplikacija može provjeriti autentičnost i povjerenje certifikatima koje izdaje specifični CA.

Možete upotrijebiti DCM da omogućite ili onemogućite status povjerenja za certifikate Izdavača certifikata (CA) u memoriji za certifikate. Kad omogućite CA certifikat možete odrediti da ga aplikacije mogu koristiti za provjeru autentičnosti i prihvatiti certifikate koje izdaje CA. Kad onemogućite CA certifikat ne možete odrediti da ga koriste aplikacije za provjeru autentičnosti i prihvat certifikata koje izdaje CA.

Podaci o politici Izdavača certifikata

Kad kreirate Izdavača certifikata (CA) pomoću DCM-a, možete odrediti podatke o politici toga CA. Podaci o politici nekog Izdavača certifikata opisuju prava na potpis koja taj izdavač ima. Podaci o politici određuju:

- Da li CA može izdati i potpisati korisničke certifikate.
- Kako dugo su certifikati, koje CA izdaje, valjani.

Lokacije popisa opoziva certifikata (CRL)

Popis opoziva certifikata (CRL) je datoteka koja popisuje sve nevažeće i opozvane certifikate za određenog Izdavača certifikata (CA). CA-ovi povremeno ažuriraju svoje CRL-ove i čine ih dostupnim za ostale za objavu u Lightweight Directory Access Protocol (LDAP) direktorijima. Nekoliko CA-ova, kao SSH u Finskoj, objavljuju sami CRL-ove u LDAP direktorijima, kojima možete direktno pristupiti. Ako CA objavljuje svoje vlastite CRL-ove, certifikat to označava uključivanjem ekstenzije u CRL distribucijskoj točki u obliku Uniform Resource Identifier-a (URI).

Upravitelj digitalnih certifikata (DCM) vam dozvoljava da definirate i upravljate CRL lokacijskim informacijama da osigurate bolju provjeru autentičnosti za certifikate koje koristite ili prihvaćate od drugih. Definicija CRL lokacije opisuje lokaciju od i informaciju o pristupu za poslužitelja Lightweight Directory Access Protocol-a (LDAP), koji pohranjuje CRL.

Aplikacije, koje izvode provjeru autentičnosti certifikata, pristupaju CRL lokaciji, ako je definirana, za određeni CA da se jamči da CA nije opozvao određeni certifikat. DCM vam dopušta definiranje i upravljanje informacijama o CRL lokaciji koje aplikacije trebaju za izvođenje CRL obrade tijekom provjere autentičnosti certifikata. Primjeri aplikacija i obrada koje mogu obrađivati CRL za provjeru autentičnosti su: Internet Key Exchange (IKE) poslužitelj za virtualno privatno umrežavanje, Sloj sigurnih utičnica (SSL) omogućene aplikacije i postupak potpisivanja objekata. Osim toga, kad definirate CRL lokaciju i pridružite je CA certifikatu, DCM izvodi CRL obradu kao dio validacionog postupka za certifikate, koje izdaje određeni CA. .

Memorije certifikata

Memorija certifikata je posebna datoteka baze podataka ključa koju Upravitelj digitalnih certifikata (DCM) koristi za pohranjivanje digitalnih certifikata. Memorija certifikata također sadrži privatni ključ certifikata osim ako ne odlučite koristiti 4758 kriptografički koprocesor za spremanje ključa. DCM vam omogućuje kreiranje i upravljanje sa nekoliko tipova memorija certifikata. DCM kontrolira pristup memorijama certifikata kroz lozinke u spoju sa kontrolom pristupa IFS direktorija i IFS datoteka koje čine memoriju certifikata.

Memorije certifikata su klasificirane na temelju tipova certifikata koje one sadrže. Zadaci upravljanja koje možete obaviti za svaku memoriju certifikata se mijenjaju ovisno o tipu certifikata kojeg sadrži memorija certifikata. DCM pruža sljedeće predefinirane memorije certifikata koje možete kreirati i upravljati:

Lokalni Izdavač certifikata (CA)
DCM koristi ovu memoriju certifikata za pohranjivanje certifikata lokalnog CA i njegovog privatnog ključa ako vi kreirate lokalnog CA. Možete koristiti certifikat u toj memoriji certifikata za potpis certifikata koje koristite i koje izdaje lokalni CA. Kad lokalni CA izda certifikat, DCM stavlja njegovu kopiju (bez privatnog ključa) u odgovarajuću memoriju certifikata (na primjer, *SYSTEM) za svrhe provjere autentičnosti. Aplikacije koriste CA certifikati za provjeru porijekla certifikata, koje moraju provjeriti kao dio SSL pregovora za dodjelu autorizacije resursima.

***SYSTEM**
DCM pribavlja ovu memoriju certifikata za upravljanje poslužiteljevim ili klijentovim certifikatima koje koriste aplikacije za sudjelovanje u komunikacijskim sesijama Sloja sigurnih utičnica (SSL). IBM iSeries aplikacije (i mnoge druge aplikacije razvijatelja softvera) su pisane za korištenje certifikata samo u *SYSTEM memoriji certifikata. Kada koristite DCM za kreiranje lokalnog CA, DCM kreira ovu memoriju certifikata kao dio procesa. Kada izaberete dobivanje certifikata od javnog CA, kao VeriSign, za korištenje od vaših aplikacija poslužitelja ili klijenata, morate kreirati ovu memoriju certifikata.

***OBJECTSIGNING**
DCM omogućuje ovu memoriju certifikata za upravljanje certifikatima koje koristite za digitalno potpisivanje objekata. Također, zadaci u ovoj memoriji certifikata vam omogućavaju kreiranja digitalnih potpisa na objektima, kao i gledanje i provjeru potpisa na objektima. Kada koristite DCM za kreiranje lokalnog CA, DCM kreira ovu memoriju certifikata kao dio procesa. Kada izaberete dobivanje certifikata od javnog CA, kao VeriSign, za potpisivanje objekata, morate kreirati ovu memoriju certifikata.

***SIGNATUREVERIFICATION**
DCM omogućuje ovu memoriju certifikata za upravljanje certifikatima koje koristite za provjeru autentičnosti digitalnih potpisa na objektima. Za provjeru digitalnog potpisa, ovaj certifikat mora sadržavati kopiju certifikata koji je potpisao objekt. Memorija certifikata mora također sadržavati kopiju CA certifikata za CA koji je izdao certifikat potpisivanja objekta. Dobivate ove objekte ili eksportiranjem objekata na trenutni sistem u memoriju ili importiranjem certifikata koje primite od potpisnika objekta.

Memorija certifikata drugog sistema
Ova memorija certifikata omogućuje alternativnu memorijsku lokaciju za poslužiteljeve ili klijentove certifikate koje koristite za SSL sesije. Druge sistemske memorije certifikata su korisnički definirane sekundarne memorije certifikata za SSL certifikate. Opcija druge sistemske memorije certifikata vam dopušta upravljanje certifikatima za aplikacije koje pišete vi ili drugi, koje koriste SSL_Init API za programski pristup i korištenje certifikata za postavljanje SSL sesije. Ovaj API omogućuje aplikaciji korištenje defaultnog certifikata za memoriju certifikata radije nego certifikat kojeg ste specifično identificirali. Najuobičajenije je da ovu memoriju certifikata koristite kad premještate certifikate od prethodnog izdanja DCM-a ili za kreiranje posebnog podskupa certifikata za SSL korištenje.

Bilješka: Ako imate instaliran 4758 PCI kriptografički koprocesor na vašem iSeries poslužitelju, možete izabrati druge opcije memorije privatnog ključa (sa iznimkom certifikata potpisivanja objekata). Možete pohraniti privatni ključ u sam koprocesor ili koprocesor upotrijebiti za šifriranje privatnog ključa i njegovo pohranjivanje u posebnu datoteku ključa umjesto u memoriju certifikata.

DCM kontrolira pristup memorijama certifikata putem lozinki. DCM također održava kontrolu pristupa direktorija integriranog sistema datoteka i datoteka koje sačinjavaju memoriju certifikata. Lokalni izdavač certifikata (CA) i memorije *SYSTEM, *OBJECTSIGNING i *SIGNATUREVERIFICATION certifikata moraju biti smještene u posebnu stazu unutar integriranog sistema datoteka. Druge sistemske memorije certifikata mogu biti smještene bilo gdje u integriranom sistemu datoteka.

Kriptografija

Kriptografija je znanost o čuvanju podataka na sigurnom. Kriptografija vam dopušta pohranjivanje informacija ili komunikaciju sa drugim strankama sprečavajući da neovlaštene stranke razumiju pohranjene informacije ili da razumiju komunikacije. Enkripcija pretvara razumljiv tekst u nečitljive podatke (ciphertext). Dešifriranjem se nerazumljivi podaci vraćaju u razumljivi tekst. Oba procesa uključuju matematičku formulu ili algoritam i tajni slijed podataka (ključ).

Postoje dva tipa kriptografije:

- U **kriptografiji sa podijeljenim ili tajnim ključem (simetričan)** jedan ključ se tajno dijeli među dvije komunikacijske stranke. Šifriranje i dešifriranje koriste isti ključ.
- U **kriptografiji sa javnim ključem (asimetrično)** šifriranje i dešifriranje koriste različite ključeve. Suprotna strana ima par ključeva koji se sastoje od javnog ključa i privatnog ključa. Javni ključ se slobodno distribuira, obično unutar digitalnog certifikata, dok privatni ključ vlasnik drži na sigurnom. Ova su dva ključa matematički srodna, ali je uistinu nemoguće izvesti privatni ključ iz javnog ključa. Objekt, kao što je poruka, koji je šifriran nečijim javnim ključem može se dešifrirati samo sa pridruženim privatnim ključem. Alternativno može poslužitelj ili korisnik upotrijebiti privatni ključ da ″potpiše″ objekt a primatelj može upotrijebiti javni ključ za dešifriranje digitalnog potpisa da provjeri izvor objekta i cjelovitost.

Sloj sigurnih utičnica (SSL)

Sloj sigurnih utičnica (SSL), koje je izvorno proizveo Netscape, je industrijski standard za enkripciju sesija između klijenata i poslužitelja. SSL koristi asimetrički ili javni ključ šifriranja za dešifriranje sesije između poslužitelja i klijenta. Aplikacije poslužitelja i klijenta dogovaraju ovu sesiju za vrijeme razmjene digitalnih certifikata. Ključ ističe automatski nakon 24 sata i SSL obrada kreira različit ključ za svaku poslužiteljsku vezu i svakog klijenta. Sukladno tomu, čak i ako neovlašteni korisnici presretnu i dešifriraju ključ sesije (što je malo vjerojatno), ne mogu ga koristiti za prisluškivanje kasnijih seansi.

Poglavlje 6. Plan za DCM

Za korištenje Upravitelja digitalnih certifikata (DCM) za efektivno upravljanje digitalnim certifikatima vaše kompanije, morate imati ukupni plan kako ćete koristiti digitalne certifikate kao dio vaše politike sigurnosti.

Da naučite više o planiranju korištenja DCM-a i bolje razumijevanje kako se digitalni certifikati mogu smjestiti u vašu politiku sigurnosti, pregledajte ova poglavlja:

Zahtjevi za korištenje DCM-a
Pročitajte ovo da naučite koji softver morate instalirati i druge informacije koje trebate za postavljanje vašeg sistema za korištenje DCM-a.

Tipovi digitalnih certifikata
Upotrijebite ove informacije da naučite o različitim tipovima certifikata za koje možete koristiti DCM da im upravlja.

Javni certifikati protiv privatnih certifikata
Upotrijebite ove informacije da naučite kako odrediti koji tip certifikata je najprikladniji vašim poslovnim potrebama nakon što odlučite kako želite koristiti certifikate da iskoristite prednosti od dodatne sigurnosti koju vam oni pružaju. Možete koristiti certifikate od javnih CA ili možete kreirati i raditi na privatnom CA za izdavanje certifikata. Kako ćete odabrati dobivanje vaših certifikata ovisi o tome kako ih planirate koristiti.

Digitalni certifikati za komunikaciju Sloja sigurnih utičnica (SSL)
Upotrijebite ove informacije da naučite kako se koriste certifikati da vaše aplikacije mogu postaviti sigurne komunikacijske sesije.

Digitalni certifikati za provjeru korisnika
Koristite ove informacije da naučite kako koristiti certifikate za pružanje bolje provjere autentičnosti korisnika koji mogu pristupiti resursima iSeries poslužitelja.

Digitalni certifikati za provjeru autentičnosti veza virtualne privatne mreže (VPN)
Upotrijebite ove informacije da naučite kako se koriste certifikati kao dio konfiguriranja VPN veze.

Digitalni certifikati za potpisivanje objekata
Upotrijebite ove informacije da naučite kako se koriste certifikati za osiguranje cjelovitosti objekta ili za provjeru digitalnog potpisa na objektu da se provjeri njegova autentičnost.

Digitalni certifikati za provjeravanje potpisa objekata
Upotrijebite ove informacije da naučite kako se koriste certifikati za provjeru digitalnog potpisa na objektu da se provjeri njegova autentičnost.

DCM zahtjevi za postav

Upravitelj digitalnih certifikata (DCM) je besplatno iSeries svojstvo koje vam dozvoljava da centralno upravljate digitalnim certifikatima za vaše aplikacije. Da bi uspješno koristili DCM, osigurajte da ste učinili sljedeće:

- Instalirali licencirani program dobavljača kriptografičkog pristupa (5722–AC3). Ovaj kriptografički proizvod određuje maksimalnu duljinu ključa koja je dozvoljena za kriptografičke algoritme na temelju pravila eksportiranja i importiranja. Morate instalirati ova proizvod prije nego možete kreirati certifikate.
- Instalirajte opciju 34 iz OS/400. Ovo je DCM funkcija osnovana na pretražitelju.
- Instalirajte IBM HTTP poslužitelj za iSeries (5722–DG1) i pokrenite *ADMIN instancu poslužitelja.
- Pobrinite se da je TCP konfiguriran za vaš sistem tako da možete koristiti web pretražitelja i HTTP poslužitelja *ADMIN instance za pristup DCM funkciji.

Bilješka: Neće biti u stanju kreirati certifikate, ako ne instalirate sve tražene proizvode. Ako zahtijevani proizvod nije instaliran, DCM će prikazati poruku o greški upućujući vas da instalirate komponentu koja nedostaje.

Tipovi digitalnih certifikata

Postoji nekoliko klasifikacija digitalnih certifikata. Te klasifikacije opisuju kako se certifikat koristi. Možete koristiti Upravitelj digitalnih certifikata (DCM) da upravlja sljedećim tipovima certifikata:

Certifikati Izdavača certifikata (CA)
Certifikat Izdavača certifikata je digitalna vjerodajnica koja provjerava identitet Izdavača certifikata (CA) koji je vlasnik certifikata. Certifikat Izdavača certifikata sadrži identifikacijske informacije o Izdavača certifikata, kao i njegov javni ključ. Drugi mogu koristiti javni ključ CA certifikata za provjeru autentičnosti certifikata koje CA izdaje i potpisuje. Certifikat Izdavača certifikata mogu potpisati drugi CA, kao VeriSign ili mogu biti samo-potpisani ako je to nezavisna cjelina. CA, koji vi kreirate u Upravitelju digitalnih certifikata, je nezavisna cjelina. Drugi mogu koristiti javni ključ CA certifikata za provjeru autentičnosti certifikata koje CA izdaje i potpisuje. Da koristite certifikat za SSL, potpisivanje objekata ili provjeru potpisa objekata, morate također imati kopiju CA certifikata za CA koji je izdao certifikat.

Certifikati poslužitelja ili klijenta
Certifikat poslužitelja ili klijenta je digitalna vjerodajnica koja identificira aplikaciju poslužitelja ili klijenta, koja koristi certifikat za sigurne komunikacije. Certifikati poslužitelja ili klijenta sadrže informacije identifikacije o organizaciji koja posjeduje aplikaciju, kao što je sistemsko razlikovno ime. Certifikat također sadrži i javni ključ sistema. Svaki poslužitelj mora imati digitalnu potvrdu ako želi koristiti Sloj sigurnih utičnica (SSL) za zaštićenu komunikaciju. Aplikacija koja podržava digitalne certifikate može pregledati certifikat poslužitelja za provjeru identiteta poslužitelja kad klijent pristupa poslužitelju. Aplikacija zatim može koristiti provjeru autentičnosti certifikata kao osnovu za iniciranje SSL šifrirane sesije između klijenta i poslužitelja. Možete upravljati ovim tipovima certifikata samo iz *SYSTEM memorije certifikata.

Certifikati potpisivanja objekata
Certifikat potpisivanja objekta je certifikat koji koristite za digitalno potpisivanje objekta. Potpisivanjem objekta, dajete način kojim možete provjeriti i cjelovitost objekta i izvorište ili vlasništvo nad objektom. Možete koristiti certifikat za potpisivanje raznih objekata, uključujući većinu objekata u Integriranom sistemu datoteka (IFS) i *CMD objekte. Možete naći potpun popis objekata koji se mogu potpisati u poglavlju Potpisivanje objekata i provjera potpisa. Kad koristite privatni ključ certifikata za potpisivanje objekta da potpišete objekt, primatelj objekta mora imati pristup kopiji odgovarajućeg certifikata za provjeru potpisa da ispravno provjeri autentičnost potpisa objekta. Možete upravljati ovim tipovima certifikata samo iz *OBJECTSIGNING memorije certifikata.

Certifikati provjere potpisa
Certifikat za provjeru potpisa je kopija certifikata za potpisivanje objekta bez privatnog ključa certifikata. Koristite javni ključ certifikata provjere potpisa za provjeru autentičnosti digitalnog potpisa koji je kreiran sa certifikatom potpisivanja objekta. Provjeravanje potpisa će vam dozvoliti da odredite porijeklo objekta i je li mijenjan od kada je potpisan. Možete upravljati ovim tipovima certifikata samo iz *SIGNATUREVERIFICATION memorije certifikata.

Certifikati korisnika
Korisnički certifikat je digitalna vjerodajnica kojom se provjerava valjanost identiteta klijenta ili korisnika koji posjeduje certifikat. Mnoge aplikacije danas omogućuju podršku koja vam dopušta upotrebu certifikata za provjeru autentičnosti korisnika za resurse umjesto korisničkih imena i lozinki. Upravitelj digitalnih certifikata (DCM) automatski pridružuje certifikate korisnika koje vaš privatni CA izdaje sa korisnikovim iSeries profilom korisnika. Možete također koristiti DCM za pridruživanje certifikata korisnika koje drugi Izdavač certifikata izdaje sa korisnikovim iSeries profilom korisnika.

Kad koristite Upravitelja digitalnih certifikata (DCM) za upravljanje vašim certifikatima, DCM ih organizira po ovim klasifikacijama i smješta njih i njihove pridružene privatne ključeve u memoriju certifikata.

Bilješka: Ako imate instaliran IBM 4758 PCI kriptografički koprocesor na vašem iSeries poslužitelju, možete izabrati druge opcije memorije privatnog ključa za vaše certifikate (sa iznimkom certifikata potpisivanja objekata). Možete pohraniti privatni ključ i na samom koprocesoru. Ili možete upotrijebiti koprocesor za šifriranje privatnog ključa i njegovo pohranjivanje u posebnu datoteku ključa umjesto u memoriju certifikata. Korisnički certifikati i njihovi privatni ključevi su, međutim, pohranjeni na korisnikovom sistemu, bilo u pretražiteljevom softveru ili u datoteci da ga koriste drugi paketi klijentovih softvera.

Javni certifikati protiv privatnih certifikata

Kad odlučite koristiti certifikate, trebali biste izabrati tip primjene certifikata koji najbolje odgovara vašim sigurnosnim potrebama. Izbori koje imate za dobivanje vaših certifikata uključuju:

- Kupnja vaših certifikata od javnog Internet izdavača certifikata (CA).
- Rad sa vašim vlastitim CA za izdavanje privatnih certifikata za vaše korisnike i primjene.
- Korištenje kombinacije certifikata od javnih Internet CA-ova i vaših vlastitih CA-ova.

Koju ćete implementaciju izabrati ovisi o nekoliko faktora, od kojih je jedan od najvažnijih okolina u kojoj se certifikati koriste. Evo nekoliko informacija da vam pomognu da bolje odredite koja je implementacija prava za vaše poslovne i sigurnosne potrebe.

Korištenje javnih certifikata

Javni Internet CA-ovi izdaju certifikate svakom tko plati potrebnu pristojbu. Međutim, Internet CA zahtjeva još neki dokaz identiteta prije nego što izda certifikat. Ova razina dokaza se ipak mijenja, ovisno o politici identifikacije od CA. Prije odluke o dobivanju certifikata od CA ili o povjerenju certifikatima koje on izdaje, trebate procijeniti da li strogost politike identifikacije od CA odgovara vašim sigurnosnim potrebama. Kako su standardi Infrastrukture javnog ključa za X.509 (PKIX) evoluirali, neki noviji javni CA sada pružaju bolje standarde identifikacije za izdavanje certifikata. Dok je postupak dobivanja certifikata od takvih PKIX CA-ova kompliciraniji, certifikati koje izdaje CA omogućuje bolje osiguranje za sigurni pristup posebnih korisnika aplikacijama. Upravitelj digitalnog certifikata (DCM) vam dopušta upravljanje certifikatima od PKIX CA-ova, koji koriste te nove standarde certifikata.

Trebate također razmotriti cijenu korištenja javnog CA za izdavanje certifikata. Ako trebate da se certifikati izdaju ograničenom broju poslužiteljskih ili klijentskih aplikacija i korisnika, tada cijena možda nije za vas važan faktor. Međutim, cijena može biti naročito važna ako imate veliki broj *privatnih* korisnika koji trebaju javne certifikate za provjeru autentičnosti klijenata. U tom slučaju trebate razmotriti i administrativna i programska nastojanja za konfiguraciju poslužiteljskih aplikacija da se prihvati samo specifični podskup certifikata koje izdaje javni CA.

Korištenje certifikata od javnog CA može vam uštediti vrijeme i resurse jer mnoge aplikacije poslužitelja, klijenata i korisnika su konfigurirane tako da prepoznaju većinu dobro poznatih javnih CA-ova. Također i druge tvrtke i korisnici mogu prepoznati i imati povjerenje u certifikate, koje izdaju dobro poznati CA-ovi više nego u one koje izdaje vaš privatni CA.

Korištenje privatnih certifikata

Ako kreirate vlastiti Lokalni CA, morate izdavati certifikate sistemima i korisnicima unutar ograničenijeg djelokruga, kao unutar vašeg poduzeća ili organizacije. Kreiranje i održavanje vlastitoga CA omogućuje vam izdavanje certifikata samo onim korisnicima koji su pouzdani članovi vaše skupine. Time je osigurana bolja zaštita jer možete strože i bolje kontrolirati tko ima certifikat, pa tako i tko ima pristup vašim resursima. Potencijalni nedostaci održavanja vlastitog Lokalnog CA je količina vremena i resursa koje morate uložiti. Međutim, Upravitelj digitalnih certifikata (DCM) čini za vas taj postupak lakšim.

Kada koristite Lokalni CA za izdavanje certifikata korisnicima za provjeru autentičnosti klijenta, trebate odrediti želite li da certifikati korisnika budu pridruženi iSeries korisničkim profilima. Možete odrediti da korisnici primaju svoje certifikate od Lokalnog CA kroz DCM ako želite da njihovi certifikati budu pridruženi iSeries korisničkom profilu. Počevši sa V5R2, možete koristiti APIje da programatski izdaju certifikate ne-iSeries korisnicima tako da ti korisnici ne moraju imati iSeries korisnički profil da koristi privatne certifikate za provjeru autentičnosti klijenta.

Bilješka: Nije važno koje CA-ove koristite za izdavanje vaših certifikata, sistemski administrator pomoću aplikacija na svom sistemu kontrolira koji CA-ovi trebaju biti pouzdani. Ako se u vašem pretražitelju nalazi kopija certifikata poznatoga CA, pretražitelj možete podesiti da vjeruje poslužiteljskim certifikatima koje je izdao taj CA. Međutim, ako taj CA certifikat nije u vašoj memoriji *SYSTEM certifikata, vaš poslužitelj ne može imati povjerenje u certifikate korisnika ili klijenta koje je izdao taj CA. Ako želite vjerovati korisničkim certifikatima koje izdaje neki CA, potrebna vam je kopija CA certifikata od toga CA. Ona mora biti u ispravnom formatu datoteke i taj certifikat morate dodati vašem DCM certifikatu.

Možete misliti da je korisno da pregledate neke uobičajene scenarije upotrebe certifikata da vam pomogne izabrati odgovara li bilje korištenje javnih ili privatnih certifikata vašem poslu ili sigurnosnim potrebama.

Srodni zadaci

Nakon što odlučite kako koristiti certifikate i koje tipove koristiti, pogledajte ove postupke da više naučite o tome kako koristiti Upravitelja digitalnih certifikata za aktiviranje vašeg plana.

- Kreiranje i rad sa privatnim CA opisuje zadatke koje morate izvršiti ako ste odlučili da radite sa CA za izdavanje privatnih certifikata.
- Upravljanje certifikatima od javnog Internet CA opisuje zadatke koje morate izvršiti za korištenje certifikata od dobro poznatih javnih CA-ova, uključujući PKIX CA.
- Korištenje Lokalnog CA na drugim iSeries poslužiteljima opisuje zadatke koje morate izvesti ako želite koristiti certifikate sa privatnog CA na više od jednog sistema.

Digitalni certifikati za SSL sigurne komunikacije

Možete koristiti digitalne certifikate za konfiguriranje aplikacija da koriste Sloj sigurnih utičnica (SSL) za sigurne sesije komunikacije. Za postavljanje SSL sesije, vaš poslužitelj uvijek pribavlja kopiju svog certifikata da klijent, koji zahtijeva vezu, provjeri valjanost. Korištenje SSL veze:

- Uvjerava klijenta ili krajnjeg korisnika da je vaša stranica autentična.
- Omogućuje šifriranu komunikacijsku sesiju da se osigura privatnost podataka koji prođu vezom.

Aplikacije poslužitelja i klijenta rade zajedno kako slijedi da osiguraju sigurnost podataka:

1. Aplikacija poslužitelja predočava certifikat aplikaciji klijenta (korisnik) kao dokaz poslužiteljevog identiteta.

2. Aplikacija klijenta provjerava poslužiteljev identitet prema kopiji certifikata kojeg je izdao Izdavač certifikata. (Aplikacija klijenta mora imati pristup lokalno pohranjenoj kopiji relevantnog CA certifikata.)
3. Aplikacije poslužitelja i klijenta dogovore se o simetričnom ključu za šifriranje i koriste ga za šifriranje komunikacijskih sesija.
4. Poslužitelj može sada neobvezno zahtijevati od klijenta da pribavi dokaz o identitetu prije nego što dopusti pristup zatraženom resursu. Za korištenje certifikata kao dokaza identiteta, komunikacijske primjene moraju podržavati korištenje certifikata za provjeru autentičnosti korisnika. .

SSL koristi algoritme asimetričnog ključa (javni ključ) tijekom SSL handshake obrade za pregovaranje o simetričnom ključu, koji se kasnije koristi za šifriranje i dešifriranje aplikacijskih podataka za tu posebnu SSL sesiju. To znači da klijent i poslužitelj koriste različite ključeve u sesiji, koji automatski prestaju važiti nakon nekog vremena, određenog za svaku vezu. Da se u nekom malo vjerojatnom slučaju desi da se dešifrira ključ određene sesije, taj ključ sesije se ne može više koristiti za izvođenje nikakvih budućih ključeva.

Digitalni certifikati za provjeru korisnika

Korisnici tradicionalno primaju pristup resursima od neke aplikacije ili sistema, na osnovi njihovog korisničkog imena i lozinke. Možete i dalje povećavati sistemsku sigurnost upotrebom digitalnih certifikata (umjesto korisničkih imena i lozinki) za provjeru autentičnosti i autorizirati sesije između mnogih aplikacija i korisnika. Također, možete koristiti Upravitelj digitalnih certifikata (DCM) za pridruživanje certifikata korisnika sa tim korisnikovim iSeries korisničkim profilom. Tada certifikat ima iste autorizacije i dozvole kao pridruženi profil. Počevši sa V5R2, možete koristiti APIje da programatski koristite vaš privatni Lokalni Izdavač certifikata za izdavanje certifikata ne-iSeries korisnicima. Ovi APIji vam daju mogućnost izdavanje privatnih certifikata korisnicima kada ne želite da ti korisnici imaju iSeries korisnički profil.

Digitalni certifikat djeluje kao elektronička vjerodajnica i potvrđuje da je osoba koja predočava taj certifikat uistinu ta koja se predstavlja. U tom smislu, certifikat je sličan putovnici. Oboje predočavaju identitet pojedinca, sadrže jedinstveni broj za svrhe identifikacije i imaju prepoznatljivo ovlaštenje za izdavanje koje potvrđuje vjerodajnicu autentičnom. Što se tiče certifikata, Izdavač certifikata funkcionira kao pouzdana, treća stranka koja izdaje certifikat i potvrđuje ga kao autentičnu vjerodajnicu.

Za svrhe provjere autentičnosti, certifikati koriste javni ključ i srodni privatni ključ. Izdavački CA veže ove ključeve, zajedno sa drugim informacijama o vlasniku certifikata, na sam certifikat za svrhe identifikacije.

Danas sve veći broj aplikacija daje podršku za korištenje certifikata za provjeru autentičnosti klijenta tijekom SSL sesije. Trenutno, te iSeries aplikacije pružaju podršku provjere certifikata klijenta:

- Telnet poslužitelj
- IBM HTTP poslužitelj (originalni i podržan od Apache)
- Poslužitelj (LDAP) Usluga Direktorija
- Središnje upravljanje
- Client Access Express (uključujući iSeries Navigator)
- FTP poslužitelj

S vremenom, dodatne aplikacije mogu pružiti podršku provjere autentičnosti certifikata klijenta; pregledajte dokumentaciju za specifične aplikacije da odredite pružaju li tu podršku.

Certifikati mogu omogućiti strožu provjeru autentičnosti korisnika radi nekoliko razloga:

- Postoji mogućnost i da netko zaboravi svoju lozinku. Stoga, korisnici moraju upamtiti ili zapisati svoja korisnička imena i lozinke da ih se mogu sjetiti. Kao rezultat, neovlašteni korisnici mogu odmah dobiti korisnička imena i lozinke od ovlaštenih korisnika. Budući da su certifikati pohranjeni u datoteci ili drugim elektroničkim lokacijama, klijentove aplikacije (radije nego korisnik) rukuju pristupanjima i predočenjima certifikata za provjeru autentičnosti. Na taj način je manje vjerojatno da korisnici dijele certifikate sa neovlaštenim korisnicima, ukoliko neovlašteni korisnici nemaju pristup korisnikovom sistemu. Certifikati mogu također biti instalirani na pametnim karticama kao dodatno sredstvo njihove zaštite od neovlaštenog korištenja.
- Certifikat sadrži privatni ključ, kojeg se nikad ne šalje sa certifikatom za identifikaciju. Umjesto toga sistem koristi taj ključ tijekom obrade šifriranja i dešifriranja. Drugi mogu koristiti odgovarajući javni certifikatov ključ za provjeru identiteta odašiljatelja objekata, koji su potpisani sa privatnim ključem.
- Mnogi sistemi zahtijevaju 8-znakovne ili kraće lozinke, čime su te lozinke više povredive na slučajne napade. Kriptografski ključevi certifikata su dugi stotine znakova. Zbog ove duljine, zajedno sa njihovom nasumičnom prirodom, teže je pogoditi kriptografske ključeve nego lozinke.
- Ključevi digitalnih certifikata omogućuju nekoliko potencijalnih koristi koje lozinke ne mogu dati, kao što je cjelovitost podataka i privatnost. Možete koristiti certifikate i njihove pridružene ključeve za:
  - Osiguranje cjelovitosti podataka otkrivanjem promjena u podacima.
  - Dokaz da je određena akcija stvarno izvedena. To se naziva nonrepudiation.
  - Jamčenje privatnosti prijenosa podataka korištenjem Sloja sigurnih utičnica (SSL) za šifriranje komunikacijskih sesija.

Da naučite više o konfiguriranju iSeries poslužitelj aplikacija da koriste certifikate za provjeru autentičnosti klijenta za vrijeme SSL sesije, pogledajte Osiguravanje aplikacija sa SSL-om.

Digitalni certifikati za VPN veze

Možete koristiti digitalne certifikate kao način uspostavljanja iSeries veze virtualne privatne mreže (VPN). Obje krajnje točke dinamičke VPN veze moraju biti sposobne za međusobno provjeravanje autentičnost prije aktiviranja veze. Provjera krajnjih točaka se vrši pomoću Internet Key Exchange (IKE) poslužitelja na svakom kraju. Nakon uspješne provjere autentičnosti, IKE poslužitelji zatim dogovaraju metodologiju šifriranja i algoritme koje će koristiti za osiguranje VPN veze.

U izdanjima ranijim od V5R1, IKE poslužitelji su mogli međusobno provjeravati autentičnost samo pomoću prethodno podijeljenog ključa. Korištenje prethodno podijeljenog ključa je manje sigurno jer morate manualno komunicirati taj ključ sa administratorom druge krajnje točke vašeg VPN-a. Prema tome, postoji mogućnost da ključ bude izložen drugim korisnicima tijekom postupka komunikacije sa ključem.

Možete izbjeći ovaj rizik korištenjem digitalnih certifikata za provjeru autentičnosti krajnjih točaka umjesto korištenja pred-dijeljenog ključa. IKE poslužitelj može provjeriti certifikat drugog poslužitelja za postavljanje veze i dogovor o metodologiji šifriranja i algoritmima koje će koristiti poslužitelji za osiguranje veze.

Možete koristiti Upravitelja digitalnih certifikata (DCM) za upravljanje certifikatima, koje koristi vaš IKE poslužitelj za postavljanje dinamičke VPN veze. Prvo, morate odlučiti da li ćete koristiti javne certifikate ili izdavati privatne certifikate za vašeg IKE poslužitelja.

Neke VPN primjene zahtijevaju da certifikat osim informacije o standardnom razlikovnom imenu, sadrži i informacije o alternativnom imenu subjekta, kao ime domene ili adresu e-pošte. Kad koristite privatni CA od DCM-ovog pomoćnog programa za izdavanje certifikata, možete specificirati informaciju o alternativnom imenu subjekta za taj certifikat.

Specificiranje ove informacije osigurava da je vaša iSeries VPN veza kompatibilna sa drugim VPN implementacijama koje je mogu tražiti za provjeru autentičnosti.

Da više naučite o tome kako upravljati certifikatima za vašu VPN vezu pogledajte ove resurse:

- Ako nikad niste koristili DCM za upravljanje certifikatima, ova poglavlja će vam u početku pomoći:
  - Kreiranje i upravljanje Lokalnim, privatnim CA opisuje kako koristiti DCM za izdavanje privatnih certifikata za vaše aplikacije
  - Upravljanje certifikatima od javnog Internet CA opisuje kako koristiti DCM za rad sa certifikatima od javnog CA.
- Ako trenutno koristite DCM za upravljanje certifikatima za druge aplikacije, pogledajte ove resurse da naučite kako specificirati da aplikacija koristi postojeći certifikat i koje certifikate aplikacija može prihvatiti i provjeriti njihovu autentičnost:
  - Upravljanje dodjelom certifikata za aplikaciju opisuje kako koristiti DCM za dodjelu postojećeg certifikata aplikaciji, kao što je vaš IKE poslužitelj.
  - Definiranje popisa pouzdanih CA za aplikaciju opisuje kako odrediti kojim CA-ovima aplikacija može vjerovati kad aplikacija prihvaća certifikate za provjeru autentičnosti klijenta (ili VPN-a).

Digitalni certifikati za potpisivanje objekata

Počevši sa V5R1, OS/400 pruža podršku za korištenje certifikata za digitalno potpisivanje objekata. Digitalno potpisivanje objekata pruža način provjere cjelovitosti sadržaja objekta i izvora porijekla. Podrška potpisivanja objekata pojačava tradicionalne iSeries sistemske alate za kontroliranje tko može mijenjati objekte. Tradicionalna kontrola ne može zaštititi objekt od neovlaštenog miješanja dok se objekt prenosi preko Interneta ili druge nepouzdane mreže ili dok je objekt pohranjen na ne-iSeries sistemu. Također, tradicionalne kontrole ne mogu uvijek odrediti je li došlo do neovlaštenih promjena ili zlonamjernog mijenjanja objekta. Korištenjem digitalnih potpisa na objektima daje se pouzdan način otkrivanja promjena na potpisanim objektima.

Stavljanje digitalnog potpisa na objekt sastoji se od korištenja certifikatovog privatnog ključa za dodavanje šifriranog matematičkog sažetka podataka u objekt. Potpis štiti podatke od neovlaštenih promjena. Objekt i njegov sadržaj nisu šifrirani i nisu sa digitalnim popisom postali privatni; međutim, sam sažetak je šifriran da spriječi u njemu neovlaštene promjene. Svatko tko želi zaštititi objekt od promjena u prijenosu te da objekt proizveden od prihvaćenog, legitimnog izvora može koristiti certifikatov javni ključ za provjeru originalnog digitalnog potpisa. Ako potpis nije više usklađen, podaci su možda promijenjeni. U takvom slučaju, primaoc može izbjeći korištenje objekta i umjesto toga kontaktirati potpisnika da dobije drugu kopiju potpisanog objekta.

Ako odlučite da je korištenje digitalnih potpisa u skladu sa vašim sigurnosnim potrebama i politikom, trebate ocijeniti trebate li koristiti javne certifikate a ne izdavati privatne certifikate. Ako želite distribuirati objekte korisnicima u javnosti, trebate uzeti u obzir korištenje certifikata od poznatog Izdavača certifikata (CA) za potpisivanje objekata. Korištenjem javnih certifikata jamči se da ostali mogu lako i jeftino provjeriti potpise koje stavljate na objekte koje ih njima distribuirate. Ako, ipak, namjeravate distribuirati objekte samo unutar organizacije, možete dati prednost korištenju Upravitelja digitalnih certifikata (DCM) za upravljanje vašim lokalnim CA za izdavanje certifikata za potpisivanje objekata. Korištenje privatnih certifikata sa Lokalnog CA za potpisivanje objekata je jeftinije od kupovanja certifikata od poznatog javnog CA.

Potpis na objektu predstavlja sistem koji je potpisao objekt a ne određenog korisnika na tom sistemu (iako korisnik mora imati odgovarajuće ovlaštenje za korištenje certifikata za potpisivanje objekata). Koristite Upravitelja digitalnih certifikata (DCM) za upravljanje certifikatima koje koristite za potpisivanje i provjeru potpisa na objektima. Možete također koristiti DCM za potpisivanje objekata i provjeru potpisa objekata.

Digitalni certifikati za provjeravanje potpisa objekata

Počevši sa V5R1, iSeries pruža podršku za korištenje certifikata za provjeru digitalnih potpisa na objektima. Svatko tko želi biti siguran da potpisani objekt nije bio promijenjen u prijenosu te da je objekt proizveden od prihvaćenog, legitimnog izvora može koristiti certifikatov javni ključ za provjeru originalnog digitalnog potpisa. Ako potpis nije više usklađen, podaci su možda promijenjeni. U takvom slučaju, primaoc može izbjeći korištenje objekta i umjesto toga kontaktirati potpisnika da dobije drugu kopiju potpisanog objekta.

Potpis na objektu predstavlja sistem koji je potpisao objekt a ne određenog korisnika na tom sistemu. Kao dio postupka provjeravanja digitalnih potpisa, morate odlučiti kojem Izdavaču certifikata vjerujete i kojim certifikatima za potpisivanje objekata vjerujete. Kad odlučite vjerovati CA-u, možete razmisliti da li vjerovati potpisima koje je netko kreirao koristeći certifikat kojeg je izdao pouzdani CA. Kad odlučite da ne vjerujete CA-u, odlučujete također da ne vjerujete certifikatima koje taj CA izdaje ili potpisima koje netko kreira koristeći te certifikate.

Provjeri sistemske vrijednosti vraćanja objekta (QVFYOBJRST)

Ako odlučite izvesti provjeru potpisa, jedna od prvih važnih odluka koje morate napraviti je odluka koliko su važni potpisi za objekte koji se vraćaju na vaš sistem. To kontrolirate sistemskom vrijednosti nazvanom QVFYOBJRST. Defaultna postavka za tu sistemsku vrijednost omogućuje vraćanje nepotpisanih objekata, ali osigurava da se potpisani objekti mogu vratiti samo ako objekti imaju važeći potpis. Sistem definira objekt potpisanim samo ako objekt ima potpis kojem vaš sistem vjeruje; sistem zanemaruje druge ″nepouzdane″ potpise na objektu i ponaša se prema tom objektu kao da nije potpisan.

Nekoliko je vrijednosti koje možete koristiti za QVFYOBJRST sistemsku vrijednost, u rasponu od zanemarivanja svih potpisa da zahtijevanja valjanih potpisa za sve objekte koje sistem vraća. Ova sistemska vrijednost utječe samo na izvedive objekte koji su vraćeni a ne na spremljene datoteke ili IFS datoteke. Da naučite više o korištenju ove i drugih sistemskih vrijednosti, pogledajte Pronalazač sistemskih vrijednosti u Informacijskom Centru.

Koristite Upravitelja digitalnih certifikata (DCM) za implementiranje certifikata i odluke o povjerenju CA kao i za upravljanje certifikatima koje koristite za provjeru potpisa na objektima. Možete također koristiti DCM za potpisivanje objekata i provjeru potpisa objekata
.

Poglavlje 7. Konfiguriraj DCM

Upravitelj digitalnih certifikata (DCM) pruža korisničko sučelje temeljeno na pretražitelju koje možete koristiti za upravljanje digitalnih certifikata za vaše aplikacije i korisnike. Korisničko sučelje se dijeli na dva glavna okvira: navigacijski okvir i okvir zadatka.

Navigacijski okvir se koristi za izbor zadataka za upravljanje certifikatima ili aplikacijama koje ih koriste. Dok se neki pojedinačni zadaci pojavljuju neposredno u glavnom navigacijskom okviru, većina zadataka u navigacijskom okviru se organiziraju u kategorije. Na primjer, **Upravljaj certifikatima** je kategorija zadatka koja sadrži raznolikost individualno vođenih zadataka, kao što je Pogledaj certifikat, Obnovi certifikat, Importiraj certifikat i tako dalje. Ako je neka stavka u navigacijskom okviru kategorija, koja sadrži više od jednog zadatka, sa njegove lijeve strane se pojavi strelica. Ta strelica označava da kad izaberete vezu na tu kategoriju, pojavit će se proširena lista tako da možete birati zadatak koji ćete izvoditi.

Sa izuzetkom **Fast Path** kategorije svaki zadatak u navigacijskom okviru je vođeni zadatak koji vas brzo i lako vodi kroz slijed koraka do završetka zadatka. Fast Path kategorija omogućuje skupinu funkcija za upravljanje certifikatima i aplikacijama koji dopušta iskusnom DCM korisniku brzi pristup različitim srodnim zadacima sa centralnog skupa stranica.

Zadaci koji su dostupni u navigacijskom okviru se mijenjaju i ovise o memoriji certifikata u kojoj radite. Također, kategorija i broj zadataka koje vidite u navigacijskom okviru ovise o autorizacijama koji vaš iSeries korisnički profil ima. Svi zadaci za korištenje CA, upravljanje certifikatima koje koriste aplikacije i drugim sistemskim zadacima su dostupni samo iSeries službenicima sigurnosti ili administratorima. Službenik za zaštitu ili administrator mora imati *SECADM i *ALLOBJ posebna ovlaštenja, kako bi mogao pregledavati i koristiti ove zadatke. Korisnici bez ovih posebnih ovlaštenja imaju pristup samo funkcijama korisničkih certifikata.

Da naučite kako konfigurirati DCM i započeti koristiti ga da upravlja vašim certifikatima, pregledajte ova poglavlja:

Pokreni DCM
Pročitajte ovo da naučite pristupiti svojstvu Upravitelja digitalnih certifikata na vašem iSeries.

Postavite certifikate prvi put
Pročitajte ovo da naučite kako za početi koristiti DCM da postavi sve što trebate da započnete koristiti certifikate po prvi put. Naučite kako početi sa upravljanjem certifikatima sa javnog Internet Izdavača certifikata (CA) ili kako da kreirate i koristite privatni Lokalni CA da izdaje certifikate.

Ako želite još informacija o korištenju digitalnih certifikata u Internet okruženju za poboljšanje vašeg sistema i mrežne sigurnosti, VeriSign web stranica je odličan resurs. VeriSign web mjesto pruža opsežnu knjižnicu o temama digitalnih certifikata kao i određen broj drugih Internet sigurnosnih tema. Možete pristupiti njihovoj knjižnici na VeriSign Help Desk .

Pokreni Upravitelj digitalnih certifikata

Prije nego što možete koristiti bilo koju od ovih funkcija, trebate pokrenuti Upravitelja digitalnih certifikata (DCM). Dovršite ove zadatke da budete sigurni u uspješno pokretanje DCM-a.

1. Instalirajte 5722 SS1 opcija 34. Ovo je Upravitelj digitalnih certifikata (DCM).

   Instalirajte 5722 DG1. Ovo je IBM HTTP poslužitelj za iSeries.

   Instalirajte 5722 AC3. Ovo je umnožak kriptografije koje V5R2 DCM koristi za generiranje javno-privatnog para ključeva za certifikate, da šifrira eksportirane datoteke certifikata, i dešifrira importirane datoteke certifikata.
2. Koristite iSeries Navigator za pokretanje instance HTTP poslužitelja *ADMIN:
   a. Pokrenite **iSeries Navigator**.
   b. Dvaput kliknite vaš iSeries poslužitelj u pogledu glavnog stabla.
   c. Dva puta kliknite na **Mrežu**.
   d. Dva puta kliknite na **Poslužitelje**.
   e. Dva puta kliknite na **TCP/IP**.
   f. Desno kliknite na **HTTP Administraciju**.
   g. Kliknite **Pokreni**.
3. Pokrenite vaš web poslužitelj.
4. Korištenjem vašeg pretražitelja, idite na iSeries Stranicu sa zadacima na vašem sistemu na http://*ime_vašeg_sistema*:2001.
5. Izaberite **Upravitelj digitalnih certifikata** sa popisa proizvoda na iSeries Stranici zadataka da pristupite DCM svojstvu.

Ako ste migrirali sa ranije verzije DCM-a, ova stranica će vam dati detalje koji su vam potrebni za nadogradnju vašeg sistema.

Postavite certifikate prvi put

Lijevi okvir Upravitelja digitalnih certifikata (DCM) je navigacijski okvir zadatka. Ovaj okvir možete koristiti za odabir vrlo različitih zadataka za upravljanje certifikatima i aplikacijama koje ih koriste. Koji su zadaci dostupni ovisi o tome koju memoriju certifikata (i da li ijednu) ste otvorili i o ovlaštenju vašeg korisničkog profila. Većina zadataka su dostupni samo ako imate *ALLOBJ i *SECADM posebna ovlaštenja.

Kad prvi puta koristite Upravitelja digitalnih certifikata (DCM), ne postoje nikakve memorije certifikata (ako niste migrirali sa prethodne verzije DCM-a). Prema tome, navigacijski okvir prikazuje ove zadatke samo kad imate potrebna ovlaštenja:

- Upravljanje korisničkim certifikatima.
- Kreiranje nove memorije za certifikate.
- Kreiranje Izdavača certifikata(CA). (Opaska): Nakon što ste upotrijebili ovaj zadatak za kreiranje privatnog CA, taj zadatak se više ne pojavljuje na popisu.)
- Upravljanje CRL lokacijama.
- Upravljanje PKIX lokacijama za zahtjeve.

Čak i ako postoje memorije certifikata na vašem sistemu (na primjer, vi ste migrirali sa ranije verzije DCM-a), DCM prikazuje samo ograničen broj zadataka ili kategorija zadataka u lijevom navigacijskom okviru. Morate najprije pristupiti prikladnoj memoriji certifikata prije nego što počnete raditi sa većinom zadataka upravljanja aplikacijama i certifikatima. Da otvorite određenu memoriju certifikata, kliknite **Izaberi memoriju certifikata** u navigacijskom okviru.

Navigacijski okvir DCM-a omogućuje također gumb **Sigurna veza** . Možete upotrijebiti ovo dugme za otvaranje drugog pretražiteljskog prozora da inicirate sigurnosnu vezu korištenjem

Sloja sigurnih utičnica (SSL). Da bi uspješno koristili ovu funkciju, morate prvo konfigurirati IBM HTTP poslužitelj za iSeries da koristi SSL za rad u sigurnom načinu. Morate tada pokrenuti HTTP poslužitelj u sigurnom načinu. Ako niste konfigurirala i pokrenuli HTTP poslužitelj za SSL izvođenje, vidjet ćete poruku o grešci i vaš pretražitelj neće pokrenuti sigurnu sesiju.

Pokretanje

Iako možda želite upotrijebiti certifikate za postizanje izvjesnog broja sigurnosno srodnih ciljeva, ono što ćete najprije napraviti ovisi o tome kako planirate dobiti vaše certifikate. Postoje dvije primarne staze kojima možete krenuti kod prvog korištenja DCM-a, ovisno o tome da li namjeravate koristiti javne certifikate nasuprot izdavanju privatnih certifikata.

Kreiranje i korištenje Lokalnog CA da izdaje certifikate vašim aplikacijama.

Upravljanje certifikatima od javnog Internet CA da koriste vaše aplikacije.

Kreiranje i korištenje Lokalnog CA

Nakon pažljivog pregleda vaših sigurnosnih potreba i politika, odlučili ste koristiti Lokalnog izdavača certifikata (CA) da izdaje privatne certifikate za vaše aplikacije. Možete koristiti Upravitelja digitalnih certifikata (DCM) za kreiranje i korištenje vašeg vlastitog Lokalnog CA. DCM vam pribavlja stazu vođenog zadatka koji vas vodi kroz postupak kreiranja CA i njegovog korištenja za izdavanje certifikata za vaše primjene. Staza vođenog zadatka vam osigurava sve što trebate za početak korištenja digitalnih certifikata da konfigurirate aplikacije za korištenje SSL-a i potpisivanje objekata i provjeru potpisa objekata.

Bilješka: Da koristite certifikate sa IBM HTTP poslužiteljem za iSeries, trebate kreirati i konfigurirati vaš web poslužitelj prije rada sa DCM-om. Kada konfigurirate web poslužitelj da koristi SSL, ID se generira za poslužitelj. Obratite pozornost na ovaj aplikacijski ID tako da možete koristiti DCM da navedete koji certifikat ova aplikacija treba koristiti za SSL.

Ne zaustavljajte i ponovno pokrećite poslužitelj dok ne koristite DCM za dodjelu certifikata poslužitelju. Ako zaustavite i ponovno pokrenete *ADMIN instancu web poslužitelja prije dodjeljivanja certifikata, poslužitelj se neće pokrenuti i nećete moći koristiti DCM za dodjeljivanje certifikata poslužitelju.

Da koristite DCM za kreiranje i upravljanje Lokalnim CA, slijedite ove korake:

1. Pokrenite DCM.
2. U navigacijskom okviru DCM-a odaberite **Kreiraj Izdavača certifikata (CA)** za prikaz slijeda obrazaca. Ovi obrasci vas vode kroz proces kreiranja Lokalnog CA i dovršavanja drugih zadataka koji su potrebni za započinjanje korištenja digitalnih certifikata za SSL, potpisivanje objekata i provjeru potpisa.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku, izaberite gumb za upitnik **?**) na vrhu stranice za pristup online pomoći.
3. Popunite sve obrasce u ovom vođenom poslu. Kod korištenja ovih obrazaca za izvođenje svih zadataka koji su potrebni za postavljanje Lokalnog Izdavača certifikata (CA), vi:
   a. Izaberite kako ćete spremati privatni ključ za Lokalni CA certifikat. (Ovaj korak je uključen samo ako imate instaliran IBM 4758–023 PCI kriptografički koprocesor na vašem iSeries. Ako vaš sistem nema kriptografički koprocesor, DCM automatski pohranjuje certifikat i njegov privatni ključ u memoriju certifikata lokalnog izdavača certifikata (CA).)
   b. Dajte informaciju identifikacije za Lokalni CA.
   c. Instalirate Lokalni CA certifikat na vaš PC ili na vaš pretražitelj tako da vaš softver može prepoznati provjeriti Lokalni CA i provjeriti certifikate koje CA izdaje.

d. Izaberite politiku podataka za vaš Lokalni CA.
e. Koristite novi Lokalni CA da izdate certifikat poslužitelja ili klijenta koje vaše aplikacije mogu koristiti za SSL veze. (Ako vaš iSeries ima instaliran IBM 4758–023 PCI kriptografički koprocesor, ovaj korak dozvoljava da izaberete kako ćete pohraniti privatni ključ za certifikat poslužitelja ili klijenta. Ako vaš sistem nema koprocesor, DCM automatski postavlja certifikat i njegov privatni ključ u memoriju *SYSTEM certifikata. DCM kreira memoriju *SYSTEM certifikata kao dio ovog podzadatka.)
f. Izabrati aplikacije koje mogu koristiti poslužiteljski ili klijentski certifikat za SSL veze.

   Bilješka: Ako ste ranije koristili DCM za kreiranje memorije *SYSTEM certifikata da upravljate certifikatima za SSL od javnog Internet CA, nemojte izvoditi ovaj niti prethodni korak.
g. Koristite novi Lokalni CA da izdate certifikat potpisivanja objekata koje vaše aplikacije mogu koristiti za digitalno potpisivanje objekata. Ovaj podzadatak kreira memoriju *OBJECTSIGNING certifikata; to je memorija certifikata koju koristite za upravljanje certifikatima za potpisivanje objekata.
h. Izabrati aplikacije koje mogu koristiti certifikat za potpisivanje objekata za stavljanje digitalnih potpisa na objekte.

   Bilješka: Ako ste ranije koristili DCM za kreiranje memorije *OBJECTSIGNING certifikata da upravljate certifikatima za potpisivanje objekata od javnog Internet CA, nemojte izvoditi ovaj niti prethodni korak.
i. Izaberite aplikacije koje trebaju imati povjerenje u vaš Lokalni CA.

Kad završite vođeni zadatak tada imate sve što je potrebno za početakkonfiguriranja vaše aplikacije da koristite SSL za sigurne komunikacije.

Nakon što konfigurirate vaše aplikacije, korisnici koji pristupaju aplikacijama kroz SSL vezu moraju koristiti DCM da dobiju kopiju Lokalnog CA certifikata. Svaki korisnik mora imati kopiju certifikata tako da ga korisnikov klijentski softver može upotrijebiti za provjeru autentičnosti poslužiteljevog identiteta kao dijela SSL postupka za dogovaranje. Korisnici mogu koristiti DCM ili da kopiraju Lokalni CA certifikat u datoteku ili spuste certifikat u svoj pretražitelj. Kako korisnici pohranjuju Lokalni CA certifikat ovisi o softveru klijenta koji koriste za uspostavljanje SSL veze na aplikaciju.

Također, možete koristiti ovaj Lokalno CA da izdate certifikate aplikacijama na drugim iSeries sistemima u vašoj mreži.

Da naučite više o korištenju DCM-a za upravljanje certifikatima korisnika i kako korisnici mogu dobiti kopiju Lokalnog CA certifikata da provjere valjanost certifikata koje Lokalni CA izdaje, pregledajte ova poglavlja:

Upravljanje certifikatima korisnika
Naučite kako korisnici mogu koristiti DCM za dobivanje certifikata ili pridruživanje postojećih certifikata sa svojim iSeries profilima korisnika.

Korištenje API-a za programsko izdavanje certifikata ne-iSeries korisnicima
Naučite kako možete koristiti vaš Lokalni CA da izdate privatne certifikate korisnicima bez pridruživanja certifikata iSeries profilu korisnika.

Dobivanje kopije privatnog CA certifikata
Naučite kako dobiti kopiju privatnog CA certifikata i instalirate ga na vaš PC tako da možete provjeriti valjanost bilo kojeg certifikata poslužitelja koji CA izdaje.

Upravljanje certifikatima korisnika

Vi i vaši korisnici možete koristiti Upravitelja digitalnih certifikata (DCM) za upravljanje certifikatima koje vaši korisnici trebaju i koriste za sudjelovanje u sesijama Sloja sigurnih utičnica (SSL).

Ako korisnici pristupaju vašim javnim ili internim poslužiteljima putem SSL veze moraju imati kopiju certifikata Izdavača certifikata (CA) koji je izdao poslužiteljev certifikat. Oni moraju imati CA certifikat tako da njihov klijentski softver može provjeriti autentičnost poslužiteljevog certifikata da se postavi veza. Ako vaš poslužitelj koristi certifikat od javnog CA vaš korisnički softver bi trebao već posjedovati kopiju CA certifikata. Prema tome, niti vi kao DCM administrator niti vaši korisnici ne trebaju poduzeti nikakvu akciju prije sudjelovanja u SSL sesiji. Ipak, ako vaš poslužitelj koristi certifikat od privatnog Lokalnog CA, vaši korisnici moraju dobiti kopiju Lokalnog CA certifikata prije nego mogu uspostaviti SSL sesiju sa poslužiteljem.

Osim toga, ako aplikacije poslužitelja podržavaju i zahtijevaju provjeru autentičnosti klijenta putem certifikata, korisnici moraju predočiti prihvatljivi korisnički certifikat za pristup resursima koje daje poslužitelj. Ovisno o vašim sigurnosnim potrebama, korisnici mogu pokazati certifikat od javnog Internet CA ili onaj koji dobiju od Lokalnog CA kojim upravljate. Ako vaša aplikacija poslužitelja pruža pristup resursima za interne korisnike koji trenutno imaju iSeries korisničke profile, možete koristiti DCM da doda njihove certifikate njihovim profilima korisnika. To udruživanje osigurava korisnicima da imaju isti pristup i ograničenja resursima kad predoče certifikate kao kad njihov korisnički profil dodjeli ili ne prihvati.

Upravitelj digitalnog certifikata (DCM) vam dopušta upravljanje certifikatima CA-ova, koji su dodijeljeni iSeries profilu korisnika. Ako imate korisnički profil sa *SECADM i *ALLOBJ posebnim ovlaštenjem, možete upravljati dodjeljivanjem certifikata korisničkih profila za vas ili za druge korisnike. Kad nije otvorena nijedna memorija certifikata ili kad je otvorena memorija certifikata Lokalnog izdavača certifikata (CA) tada možete odabrati **Upravljaj korisničkim certifikatima** u navigacijskom okviru za pristup odgovarajućim zadacima. Ako je otvorena drugačija memorija certifikata, zadaci korisnika certifikata se integriraju u zadatke pod **Upravljaj certifikatima**.

Korisnici bez *SECADM i *ALLOBJ posebnih ovlaštenja profila korisnika mogu upravljati samo svojim vlastitim dodjelama certifikata. Mogu izabrati **Upravljanje certifikatima korisnika** za pristupanje zadacima koji im dozvoljavaju da gledaju certifikate pridružene njihovom korisničkom profilu, uklone certifikat iz svog korisničkog profila ili pridruže certifikat od drugog CA svom korisničkom profilu. Korisnici, bez obzira na posebna ovlaštenja za svoje profile korisnika, mogu dobiti certifikat korisnika od Lokalnog CA izabiranjem zadatka **Kreiraj certifikat** u glavnom navigacijskom okviru.

Da naučite više o korištenju DCM-a za upravljanje i kreiranje certifikata korisnika, pregledajte ova poglavlja:

Kreiranje certifikata korisnika
Koristite ovu informaciju da naučite kako korisnici mogu koristiti Lokalni CA za izdavanje certifikata za provjeru autentičnosti klijenta.

Dodjela certifikata korisnika
Koristite ovu informaciju da naučite kako pridružiti vaš vlastiti certifikat vašem korisničkom profilu. Certifikat može biti od privatnog Lokalnog CA na drugom sistemu ili od poznatog Internet CA. Prije nego što možete dodijeliti certifikat vašem korisničkom profilu, CA ,koji vrši izdavanje, mora dobiti povjerenje poslužitelja a certifikat ne smije još biti pridružen korisničkom profilu na sistemu.

Kreiranje certifikata korisnika: Ako želite koristiti digitalne certifikate za provjeru identiteta korisnika, korisnici moraju imati certifikate. Ako koristite Upravitelja digitalnih certifikata (DCM) za rad sa privatnim Lokalnim Izdavačem certifikata, možete koristiti Lokalni CA za izdavanje certifikata svakom korisniku. Svaki korisnik mora pristupiti DCM-u da dobije certifikat koristeći zadatak **Kreiraj certifikat**. Da bi dobio certifikat od Lokalnog CA, politika CA mora dozvoliti da CA izda certifikate korisnika.

Za dobivanje certifikata od Lokalnog CA, dovršite ove korake:
1. Pokrenite DCM.
2. U navigacijskom okviru odaberite **Kreiraj certifikat**.
3. Odaberite **Korisnički certifikat** kao tip certifikata za kreiranje. Prikaže se obrazac tako da možete unijeti informacije o identifikaciji za certifikat.
4. Popunite obrazac i kliknite **Nastavi**.

   Bilješka: Ako imate pitanja o tome kako popuniti specifični obrazac u ovom vodećem zadatku, odberite upitnik **?** na vrhu stranice za pristup online pomoći.
5. U ovom trenutku DCM radi sa vašim pretražiteljem na kreiranju privatnog i javnog ključa za certifikat. Preglednik može prikazati i prozor koji će vas voditi kroz ovaj postupak. Slijedite upute pretražitelja za ove poslove. Nakon što pretražitelj generira ključeve, stranica potvrde pokazuje da je DCM kreirao certifikat.
6. Instalirajte novi certifikat na vaš softver preglednika. Preglednik može prikazati i prozor koji će vas voditi kroz ovaj postupak. Slijedite upute koje vam daje pretražitelj i završite posao.
7. Kliknite **OK** da dovršite zadatak.

Tijekom obrade, Upravitelj digitalnih certifikata automatski pridružuje certifikat vašem iSeries korisničkom profilu.

Ako želite certifikat od drugog CA koji korisnik pokazuje za provjeru autentičnosti klijenta da ima ista ovlaštenja kao njihov profil korisnika, korisnik može koristiti DCM da dodijeli certifikat njihovom korisničkom profilu.

Dodjela certifikata korisnika: Ako želite koristiti digitalne certifikate za provjeru identiteta korisnika, korisnici moraju imati certifikate. Ako vaši korisnici moraju predočiti certifikate od javnog Internet izdavača certifikata (CA), mogu koristiti Upravitelja digitalnih certifikata za dodjelu tih certifikata njihovim korisničkim profilima. Time se dopušta vama i korisniku da koristite DCM za upravljanje tim certifikatima.

Da koristite zadatak **Dodijeli korisnički certifikat** morate imati sigurnu sesiju sa HTTP poslužiteljem putem koje pristupate Upravitelju digitalnih certifikata (DCM). Broj porta u URL-u kojeg koristite za pristup DCM-u određuje da li imate sigurnu sesiju. Ako ste koristili port 2001, koji je default port za pristup DCM-u, nemate sigurnu sesiju. Također, HTTP poslužitelj mora biti konfiguriran da koristi SSL prije nego se možete prebaciti na sigurnu sesiju.

Kada odaberete taj zadatak pokaže se novi prozor pretražitelja. Ako nemate sigurnu sesiju, DCM vas promptira da kliknete **Dodijeli korisnički certifikat** za njegovo pokretanje. DCM zatim inicira Sloj sigurnih utičnica (SSL) za pregovaranje sa vašim pretražiteljem.

Kao dio ovih pregovora vaš pretražitelj vas može promptirati pitanju da li vjerovati Izdavaču certifikata (CA) koji je izdao certifikat koji identificira HTTP poslužitelja. Pretražitelj također vas može promptirati pitanju da li prihvatiti sam certifikat poslužitelja.

Nakon što dopustite pretražitelju da vjeruje CA-u i prihvati certifikat poslužitelja, poslužitelj može zahtijevati da predočite certifikat za autentičnost klijenta. Ovisno o postavljanjima konfiguracija za vaš pretražitelj, on vas može promptirati da odaberete certifikat i da ga

predočite za provjeru autentičnosti. Ako vaš pretražitelj predoči certifikat od nekog CA kojeg sistem prihvaća sa povjerenjem, DCM će prikazati informacije o certifikatu u posebnom prozoru. Ako ne pokažete prihvatljiv certifikat, poslužitelj vas umjesto toga može pitati za korisničko ime i lozinku za provjeru autentičnosti prije nego vam dozvoli pristup.

Kad ste postavili sigurnu sesiju, DCM pokušava dohvatiti odgovarajući certifikat sa vašeg pretražitelja tako da ga može pridružiti vašem korisničkom profilu. Ako DCM uspješno dohvati jedan ili više certifikata, možete pogledati informacije o certifikatima i izabrati pridruživanje certifikata vašem korisničkom profilu.

Ako DCM ne prikaže informacije certifikata, tada niste u mogućnosti pribaviti certifikat kojeg bi DCM mogao pridružiti vašem korisničkom profilu. Jedan od nekoliko problema korisničkih certifikata može biti za to odgovoran. Na primjer, certifikati koje sadrži vaš pretražitelj mogu već biti pridruženi vašem korisničkom profilu.

Ako dajete prednost korištenju Lokalnog CA za izdavanje certifikata vašim korisnicima, korisnici moraju umjesto toga kreirati certifikat korisnika.

Korištenje API-a za programsko izdavanje certifikata ne-iSeries korisnicima

Počevši sa V5R2, postoje dva nova APIja koje možete koristiti da programatski izdate certifikate ne-iSeries korisnicima. U prethodnim izdanjima, kada ste koristili vaš Lokalni Izdavač certifikata (CA) za izdavanje certifikata korisnicima, ti certifikati su automatski pridruživani sa njihovim iSeries korisničkim profilima. Kao posljedica, da bi koristili Lokalni CA da izdaje certifikate za provjeru autentičnosti klijenta, morali ste dobaviti tog korisnika sa iSeries korisničkim profilom. Također, kada su korisnici trebali dobiti certifikat od Lokalnog CA za provjeru autentičnosti klijenta, svaki je korisnik morao koristiti Upravitelj digitalnih certifikata (DCM) za kreiranje potrebnog certifikata. Zato, svaki korisnik mora imati korisnički profil na iSeries poslužitelju koji poslužuje DCM i valjanu prijavu na taj iSeries poslužitelj.

Pridruživanje certifikata korisničkom profilu ima svojih prednosti, posebno kada se radi o internim korisnicima. Ipak, ta ograničenja i zahtjevi čine manje praktičnim korištenje Lokalnog CA da izdaje certifikate korisnika velikom broju korisnika, posebno kada ne želite da ti korisnici imaju iSeries korisnički profil. Da izbjegnete davanje profila korisnika tim korisnicima, trebali bi tražiti da korisnici plate za certifikat od poznatog CA ako želite tražiti certifikate za provjeru autentičnosti korisnika za vaše aplikacije.

Ta dva nova APIja daju podršku koja dozvoljava da date sučelje za kreiranje certifikata korisnika potpisanih od Lokalnog CA certifikata za bilo koje ime korisnika. Ovaj certifikat neće biti pridružen profilu korisnika. Korisnik ne treba postojati na iSeries poslužitelju koji poslužuje DCM i korisnik ne treba koristiti DCM za kreiranje certifikata.

Dva su APIja, jedan za svaki od programa pretražitelja, koje možete pozvati kod korištenja Net.Data za kreiranje programa za izdavanje certifikata korisnicima. Aplikacija koju kreirate mora dati Kod grafičkog korisničkog sučelja (GUI) koji je potreban za kreiranje certifikata korisnika i pozvati jedan od odgovarajućih APIja za korištenje Lokalnog CA za potpisivanje certifikata.

Za više informacija o korištenju ovih APIja, pogledajte ove stranice:
- Generiranje i potpisivanje zahtjeva certifikata korisnika(QYCUGSUC) API.
- Potpisivanje zahtjeva certifikata korisnika(QYCUSUC) API.

Dobivanje kopije privatnog CA certifikata

Kad pristupate poslužitelju koji koristi vezu Sloja sigurnih utičnica (SSL), poslužitelj predočava certifikat vašem klijentovom softveru kao dokaz njegovog identiteta. Vaš klijentov

softver mora zatim provjeriti poslužiteljev certifikat da poslužitelj može uspostaviti sesiju. Da provjerite valjanost certifikata poslužitelja, vaš klijentov softver mora imati pristup lokalno pohranjenoj kopiji certifikata za Izdavača certifikata (CA), koji je izdao poslužiteljev certifikat. Ako poslužitelj pokazuje certifikate os javnog Internet CA, tada bi vaš pretražitelj ili drugi softver klijenta trebao već imati kopiju CA certifikata. Ako, ipak, poslužitelj pokazuje certifikat od privatnog Lokalnog CA, morate koristiti Upravitelj digitalnih certifikata (DCM) za dobivanje kopije Lokalnog CA certifikata.

Možete koristiti DCM za spuštanje lokalnog CA certifikata izravno na vaš pretražitelj ili možete kopirati Lokalni CA certifikat u datoteku tako da drugi softver klijenta može pristupati i koristiti ga. Ako koristite i pretražitelj i druge aplikacije za sigurne komunikacije, možda ćete trebati koristiti obje metode za instaliranje Lokalnog CA certifikata. Ako koristite obje metode, instalirajte certifikat u vaš pretražitelj prije nego ga kopirate i preslikate u datoteku.

Ako aplikacija poslužitelja traži da se autentificirate pokazivanjem certifikata sa Lokalnog CA, trebate spustiti Lokalni CA certifikat u vaš pretražitelj prije zahtijevanja certifikata korisnika sa Lokalnog CA.

Da koristite DCM da dobijete kopiju Lokalnog CA certifikata, dovršite sljedeće korake:
1. Pokrenite DCM.
2. U navigacijskom okviru, izaberite **Instalirajte Lokalni CA certifikat na vaš PC** da bi prikazali stranicu koja vam dozvoljava da spustite Lokalni CA certifikat na vaš pretražitelj ili ga spremite u datoteku na vašem sistemu.
3. Izaberite metodu za dobivanje Lokalnog CA certifikata.
   a. Izaberite **Instaliraj certifikat** da spustite Lokalni CA certifikat kao pouzdano ishodište u vašem pretražitelju. Time se osigurava da vaš pretražitelj može postaviti sesije sigurnih komunikacija sa poslužiteljima koji koriste certifikat od tih CA-ova. Vaš pretražitelj će prikazati seriju prozora da vam pomogne dovršiti instalaciju.
   b. Izaberite **Kopiraj i zalijepi certifikat** za prikaz stranice koja sadrži posebno kodiranu kopiju Lokalnog CA certifikata. Tekstualni objekt prikazan na stranici kopirajte u memoriju isječaka. Kasnije morate te podatke preslikati u datoteku. Tu datoteku koristi pomoćni program na PC računalu (ka što je MKKF ili IKEYMAN) za spremanje certifikata koje će koristiti klijent programi na PC računalu. Prije nego aplikacije vašeg klijenta mogu prepoznati Lokalni CA certifikat za provjeru autentičnosti, morate konfigurirati aplikacije da prepoznaju certifikat kao pouzdano ishodište. Slijedite upute koje ove aplikacije pribavljaju za korištenje datoteke.
4. Kliknite **OK** za vraćanje na početnu stranicu Upravitelj digitalnih certifikata.

Upravljanje certifikatima od javnog Internet CA

Nakon pažljivog pregleda vaših sigurnosnih potreba i politika, odlučili ste koristiti certifikate od javnog Internet izdavača certifikata (CA), kao što je VeriSign. Na primjer, radite sa javnom web stranicom i želite koristiti Sloj sigurnih utičnica (SSL) za sigurne komunikacijske sesije da osigurate privatnost određenih transakcija informacija. Budući da je web stranica dostupna općoj publici, želite koristiti certifikate koje većina web pretražitelja može odmah prepoznati.

Ili razvijate aplikacije za vanjske korisnike i želite koristiti javne certifikate za digitalno potpisivanje aplikacijskih paketa. Potpisivanjem aplikacijskih paketa, vaši korisnici mogu biti sigurni da paketi dolaze od vaše tvrtke i da neovlaštene stranke nisu promijenile kod tijekom prijenosa. Želite koristiti javni certifikat tako da vaši korisnici mogu lako i jeftino provjeriti digitalni potpis na paketu. Ovaj certifikat možete koristiti također za provjeru potpisa prije odašiljanja paketa vašem korisniku.

Možete koristiti vođene zadatke u Upravitelju digitalnih certifikata za centralno upravljanje tih javnih certifikata i aplikacija koje ih koriste za postavljanje SSL veza, potpisivanje objekata ili provjeru autentičnosti digitalnih potpisa na objektima.

Upravljanje javnim certifikatima

Kad koristite DCM za upravljanje certifikatima od javnog Internet CA, morate prvo kreirati memoriju certifikata. Memorija certifikata je posebna datoteka baze podataka ključa koju DCM koristi za pohranjivanje digitalnih certifikata i njihovih pridruženih privatnih ključeva. DCM vam omogućuje kreiranje i upravljanje sa nekoliko tipova memorija certifikata ovisno o tipovima certifikata, koje one sadrže.

Tip memorije certifikata, koju kreirate i naredne zadatke koje morate izvršiti za upravljanje vašim certifikatima i aplikacijama koje ih koriste, ovisi o tome kako planirate koristiti vaše certifikate. Da naučite kako koristiti DCM za kreiranje odgovarajuće memorije certifikata i upravljanje javnim Internet certifikatima za vaše aplikacije, pregledajte ova poglavlja:

- Upravljanje javnim Internet certifikatima za SSL komunikacijske sesije.
- Upravljanje javnim Internet certifikatima za potpisivanje objekata.
- Upravljanje certifikatima za provjeravanje potpisa objekata.

DCM vam također dopušta da upravljate certifikatima koje dobijete od Izdavača certifikata Infrastrukture javnog ključa za X.509 (PKIX).

Upravljanje javnim Internet certifikatima za SSL komunikacijske sesije

Možete koristiti Upravitelja digitalnih certifikata (DCM) za upravljanje javnim Internet certifikatima da bi se vaše aplikacije koristile za postavljanje sigurnih komunikacijskih sesija sa Slojem sigurnih utičnica (SSL). Ako ne koristite DCM za upravljanje vašim Lokalnim Izdavačem certifikata CA), morate prvo kreirati odgovarajuću memoriju certifikata za upravljanje javnim certifikatima koje koristite za SSL. To je *SYSTEM memorija certifikata. Kad kreirate memoriju certifikata DCM vas vodi kroz postupak kreiranja informacija o zahtjevu certifikata koje morate dostaviti javnom CA-u za dobivanje certifikata.

Da koristite DCM za upravljanje i korištenje javnih Internet certifikata tako da vaše aplikacije mogu postaviti SSL komunikacijske sesije, slijedite ove korake:

1. Pokrenite DCM.
2. U navigacijskom okviru DCM-a odaberite **Kreiraj novu memoriju certifikata** da dovršite vođeni zadatak i popunite seriju obrazaca. Ovi obrasci vas vode kroz postupak kreiranja memorije certifikata i certifikata kojeg vaš administrator može koristiti za SSL sesije.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vodećem zadatku, odaberite upitnik **?** na vrhu stranice za pristup online pomoći.
3. Izaberite ***SYSTEM** kao memoriju certifikata za kreiranje i kliknite **Nastavi**.
4. Odaberite **Da** za kreiranje certifikata kao dijela kreiranja memorije *SYSTEM certifikata i klikniteNastavi.
5. Odaberite **VeriSign ili drugog Internet izdavača certifikata (CA)** kao potpisnika novog certifikata i klikniteNastavi za prikaz obrasca koji vam omogućuje da dadete informacije o identifikaciji za novi certifikat.

   Bilješka: Ako vaš iSeries ima instaliran IBM 4758–023 PCI kriptografički koprocesor, DCM dozvoljava da izaberete kako ćete pohraniti privatni ključ za certifikat kao sljedeći zadatak. Ako vaš sistem nema koprocesor, DCM automatski postavlja privatni ključ u memoriju *SYSTEM certifikata. Ako trebate pomoć kod izbora kako pohraniti privatni ključ, pogledajte online pomoć u DCM-u.
6. Popunite obrazac i kliknite **Nastavi** za prikaz stranice potvrde. Stranica potvrde prikazuje podatke zahtjeva certifikata koje morate dostaviti javnom Izdavaču certifikata

(CA) koji će izdati vaš certifikat. Podaci za zahtjev za potpisivanje certifikata sastoje se od javnog ključa i drugih informacija koje ste naveli za novi certifikat.

7. Pažljivo kopirajte i preslikajte CSR podatke u obrazac molbe za certifikat ili u posebnu datoteku, što CA traži kod zahtjeva za certifikat. Morate upotrijebiti sve CSR podatke, uključujući početne i krajnje linije zahtjeva za novi certifikat. Kad napustite ovu stranicu, podaci se gube i ne možete ih obnoviti. Pošaljite obrazac molbe ili datoteku CA-u kojeg ste odabrali da izdaje i potpisuje vaše certifikate.

   Bilješka: Prije nego završite ovaj postupak morate počekati dok CA ne vrati potpisan i dovršen certifikat.

   Bilješka: Da koristite certifikate sa HTTP poslužiteljem za iSeries, morate kreirati i konfigurirati vaš web poslužitelj prije rada sa DCM-om za rad sa potpisanim dovršenim certifikatom. Kada konfigurirate web poslužitelj da koristi SSL, ID se generira za poslužitelj. Obratite pozornost na ovaj aplikacijski ID tako da ga možete koristiti kad navodite koji certifikat ova aplikacija treba koristiti za SSL.

   Ne zaustavljajte i ponovno pokrećite poslužitelj dok ne koristite DCM za dodjelu potpisanog dovršenog certifikata poslužitelju. Ako zaustavite i ponovno pokrenete *ADMIN instancu web poslužitelja prije dodjeljivanja certifikata, poslužitelj se neće pokrenuti i nećete moći koristiti DCM za dodjeljivanje certifikata poslužitelju.
8. Nakon što javni CA vrati vaš potpisani certifikat, pokrenite DCM.
9. U navigacijskom okviru kliknite **Izaberi memoriju certifikata** i izaberite***SYSTEM** da se otvori memorija certifikata.
10. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za memoriju certifikata kad ste je kreirali i kliknite **Nastavi**.
11. Nakon osvježenja navigacijskog okvira izaberite**Upravljaj certifikatima** za prikaz popisa zadataka.
12. Sa popisa zadataka izaberite **Importiraj certifikat** da započnete postupak importiranja potpisanog certifikata u memoriju *SYSTEM certifikata. Nakon što ste završili importiranje certifikata, možete odrediti aplikacije koje ga trebaju koristiti za SSL komunikacije.
13. U navigacijskom okviru izaberite **Upravljaj aplikacijama** za prikaz popisa zadataka.
14. Sa popisa zadataka izaberite **Ažuriraj dodjelu certifikata** za prikaz popisa SSL omogućenih aplikacija kojim ste dodijelili certifikat.
15. Izaberite neku aplikaciju sa popisa i kliknite **Ažuriraj dodjelu certifikata** .
16. Izaberite certifikat kojeg ste importirali i kliknite**Dodijeli novi certifikat** . DCM prikazuje poruku da potvrđuje vaš izbor certifikata za tu aplikaciju.

    Bilješka: Neke SSL omogućene aplikacije podržavaju provjeru autentičnosti klijenta osnovanu na certifikatima. Ako želite aplikaciju sa tom podrškom da možete provjeriti autentičnost certifikata prije omogućavanja pristupa resursima, morate definirati popis pouzdanih CA-ova za tu aplikaciju. Time se osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA-ova koje ste naveli kao pouzdane. Ako korisnik ili klijentova aplikacija predoči certifikat od CA koji nije naveden kao pouzdan na popisu pouzdanih CA-ova, ta aplikacija ga neće prihvatiti kao temelj za važeću provjeru autentičnosti.

Kad završite vođeni zadatak tada imate sve što je potrebno za početak konfiguriranja vaše aplikacije da koristite SSL za sigurne komunikacije. Prije nego što korisnici mogu pristupiti ovim aplikacijama putem SSL sesije, moraju imati kopiju CA certifikata za CA koji je izdao

poslužiteljski certifikat. Ako je vaš certifikat od dobro poznatog Internet CA, vaš korisnički klijentov softver možda već ima kopiju potrebnog CA certifikata. Ako korisnici trebaju dobiti CA certifikat, trebaju pristupiti web stranici za CA i slijediti upute davatelja te web stranice.

Upravljanje javnim Internet certifikatima za potpisivanje objekata

Možete koristiti Upravitelja digitalnih certifikata (DCM) za upravljanje javnim Internet certifikatima za digitalno potpisivanje objekata. Ako ne koristite DCM za upravljanje vašim Lokalnim Izdavačem certifikata CA), morate prvo kreirati odgovarajuću memoriju certifikata za upravljanje javnim certifikatima koje koristite za potpisivanje objekata. To je *OBJECTSIGNING memorija certifikata. Kad kreirate memoriju certifikata DCM vas vodi kroz postupak kreiranja informacija o zahtjevu certifikata koje morate dostaviti javnom Internet CA-u za dobivanje certifikata.

Također, za korištenje certifikata za potpis objekata morate definirati ID aplikacije. Taj ID aplikacije kontrolira koliko ovlaštenja je potrebno da netko potpiše objekte sa specifičnim certifikatom i omogućuje drugu razinu kontrole pristupa iznad one koju omogućuje DCM. Definicija aplikacije zahtjeva, po default-u, da korisnik ima *ALLOBJ posebno ovlaštenje za korištenje certifikata za potpisivanje objekta od strane aplikacije. (Ipak, možete mijenjati ovlaštenje koje ID aplikacije traži korištenjem iSeries Navigatora.)

Da koristite DCM za upravljanje i korištenje javnih Internet certifikata za potpisivanje objekata, dovršite ove zadatke:

1. Pokrenite DCM.
2. U lijevom navigacijskom okviru DCM-a odaberite **Kreiraj memoriju novog certifikata** za pokretanje vođenog zadatka i popunjavanje serije obrazaca. Ovi obrasci vas vode kroz postupak kreiranja memorije certifikata i certifikata kojeg možete koristiti za potpisivanje objekata.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku, odaberite gumb upitnika **?** na vrhu stranice za pristup online pomoći.
3. Izaberite ***OBJECTSIGNING** kao memoriju certifikata za kreiranje i kliknite **Nastavi**.
4. Izaberite **Da** za kreiranje certifikata kao dijela kreiranja memorije certifikata i kliknite**Nastavi**.
5. Izaberite **VeriSign ili drugog Internet izdavača certifikata (CA)** kao potpisnika novog certifikata i kliknite**Nastavi** za prikaz obrasca koji vam omogućuje da dadete informacije o identifikaciji za novi certifikat. Ovo prikazuje obrazac koji vam dopušta da unesete informacije o identifikaciji za novi certifikat.
6. Popunite obrazac i kliknite **Nastavi** za prikaz stranice potvrde. Stranica potvrde prikazuje podatke zahtjeva certifikata koje morate dostaviti javnom Izdavaču certifikata (CA) koji će izdati vaš certifikat. Podaci za zahtjev za potpisivanje certifikata sastoje se od javnog ključa i drugih informacija koje ste naveli za novi certifikat.
7. Pažljivo kopirajte i preslikajte CSR podatke u obrazac molbe za certifikat ili u posebnu datoteku, što CA traži kod zahtjeva za certifikat. Morate upotrijebiti sve CSR podatke, uključujući početne i krajnje linije zahtjeva za novi certifikat. Kad napustite ovu stranicu, podaci se gube i ne možete ih obnoviti. Pošaljite obrazac molbe ili datoteku CA-u kojeg ste odabrali da izdaje i potpisuje vaše certifikate.

   Bilješka: Prije nego završite ovaj postupak morate početi dok CA ne vrati potpisan i dovršen certifikat.
8. Nakon što javni CA vrati vaš potpisani certifikat, pokrenite DCM.
9. U lijevom navigacijskom okviru kliknite**Izaberi memoriju certifikata** i izaberi***OBJECTSIGNING** da se otvori memorija certifikata.
10. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za memoriju certifikata kad ste je kreirali i kliknite **Nastavi**.

11. U navigacijskom okviru izaberite **Upravljaj aplikacijama** za prikaz popisa zadataka.
12. Sa popisa zadataka izaberite **Importiraj certifikat** da započnete postupak importiranja potpisanog certifikata u memoriju *OBJECTSIGNING certifikata. Nakon što ste završili importiranje certifikata, možete kreirati definiciju aplikacije koju certifikat koristi za potpisivanje objekata.
13. Nakon osvježenja lijevog navigacijskog okvira, odaberite **Upravljaj aplikacijama** za prikaz popisa zadataka.
14. Sa popisa zadataka izaberite **Dodaj aplikaciju** da započnete postupak kreiranja definicije aplikacije za potpis objekata da koristite certifikat za potpis objekata.
15. Popunite obrazac za definiranje vaše aplikacije za potpisivanje objekta i kliknite **Dodaj**. Ova definicija aplikacije ne opisuje stvarnu aplikaciju nego radije opisuje tip objekata koje planirate potpisivati sa specifičnim certifikatom. Koristite online pomoć za pitanja o popunjavanju obrasca.
16. Kliknite **OK** da potvrdite poruku potvrde za definiciju aplikacije i prikažite popis zadataka za Upravljanja aplikacijama.
17. Sa popisa zadataka izaberite **Ažuriraj dodjelu certifikata** i kliknite **Nastavi** za prikaz popisa IDa aplikacija koje potpisuju objekte kojima ste dodijelili certifikat.
18. Izaberite ID vaše aplikacije sa popisa i kliknite **Ažuriraj dodjelu certifikata** .
19. Izaberite certifikat kojeg ste importirali i kliknite**Dodijeli novi certifikat** .

Kad završite ove zadatke, tada imate sve što trebate za početak potpisivanja objekata da osigurate njihovu cjelovitost.

Kada distribuirate potpisane objekte, one koji primaju objekte moraju koristiti V5R1 ili kasniju verziju DCM-a da provjere potpis na objektima da osiguraju da su podaci nepromijenjeni i da provjere identitet pošiljaoca. Da provjeri potpis primatelj mora imati kopiju certifikata za provjeru potpisa. Trebate pribaviti kopiju tog certifikata kao dijela paketa potpisanih objekata.

Primatelj također mora imati kopiju CA certifikata za CA koji je izdao certifikat kojeg ste koristili za potpis objekta. Ako ste potpisali objekte sa certifikatom od dobro poznatog Internet CA, tada bi primateljeva verzija DCM-a trebala već imati kopiju potrebnog CA certifikata. Međutim, ako mislite da primatelj još nema kopiju tada trebate pribaviti kopiju CA certifikata zajedno sa potpisanim objektima. Na primjer, trebate dobaviti kopiju Lokalnog CA certifikata ako ste potpisali objekte sa certifikatom sa privatnog Lokalnog CA. Radi sigurnosnih razloga, trebate pribaviti CA certifikat u posebnom paketu ili učiniti CA certifikat javno dostupnim na zahtjev onih koji ga trebaju.

Upravljanje certifikatima za provjeravanje potpisa objekata

Možete koristiti Upravitelja digitalnih certifikata (DCM) za upravljanje certifikatima za provjeru potpisa koje koristite za provjeru digitalnih potpisa na objektima. Da potpišete objekt, koristite privatni ključ certifikata za kreiranje potpisa. Kad šaljete potpisani objekt drugima, morate uključiti i kopiju certifikata koji je potpisao objekt. To radite koristeći DCM za eksport certifikata za potpisivanje objekta (bez privatnog ključa certifikata) kao certifikata za provjeru potpisa. Certifikat za provjeru potpisa možete eksportirati u datoteku koju zatim možete distribuirati drugima. Ili, ako želite provjeriti potpis kojeg kreirate, možete eksportirati certifikat za provjeru potpisa u memoriju *SIGNATUREVERIFICATION certifikata.

Da provjerite potpis na objektu, morate imati kopiju certifikata koji je potpisao objekt. Koristite certifikatov javni ključ za potpisivanje, kojeg sadrži certifikat, za pregled i provjeru potpisa koji je kreiran sa odgovarajućim privatnim ključem. Stoga, prije nego što možete provjeriti potpis na objektu, morate dobiti kopiju certifikata za potpisivanje od onoga koji vam je pribavio potpisane objekte.

Morate također imati kopiju CA certifikata za CA koji je izdao certifikat koji je potpisao objekt. Koristite CA certifikat za provjeru autentičnosti certifikata koji je potpisao objekt. DCM pribavlja kopije CA certifikata od većine dobro poznatih CA-ova. Ako je, ipak, objekt bio potpisan certifikatom nekog drugog javnog CA ili privatnog Lokalnog CA, morate pribaviti kopiju CA certifikata prije nego možete provjeriti potpis objekta.

Da koristite DCM za provjeru potpisa objekata, prvo morate kreirati odgovarajuću memoriju certifikata za upravljanje potrebnim certifikatima za provjeru potpisa; to je memorija *SIGNATUREVERIFICATION certifikata. Kad kreirate tu memoriju certifikata, DCM je automatski popunjava kopijama certifikata većine dobro poznatih javnih CA.

Bilješka: Ako želite provjeriti potpise koje ste kreirali sa vašim vlastitim certifikatima za potpisivanje objekata, morate kreirati memoriju *SIGNATUREVERIFICATION certifikata i kopirati u nju certifikate od memorije *OBJECTSIGNING certifikata. To je istina čak i onda kad planirate izvesti provjeru potpisa sa memorije *OBJECTSIGNING certifikata.

Da koristite DCM za upravljanje vašim certifikatima za provjeru potpisa, dovršite ove zadatke:

1. Pokrenite DCM.
2. U lijevom navigacijskom okviru DCM-a odaberite **Kreiraj memoriju novog certifikata** za pokretanje vođenog zadatka i popunjavanje serije obrazaca.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vodećem zadatku, odaberite gumb upitnika **?** na vrhu stranice za pristup online pomoći.
3. Izaberite ***SIGNATUREVERIFICATION** kao memoriju certifikata za kreiranje i kliknite **Nastavi**.

   Bilješka: Ako postoji memorija *OBJECTSIGNING certifikata tada će vas DCM pitati da li ćete kopirati certifikate za potpisivanje objekata u memoriju novih certifikata kao certifikate za provjeru potpisa. Ako želite koristiti vaše postojeće certifikate za potpisivanje objekata za provjeru potpisa, trebate izabrati **Da** i kliknuti**Nastavi**. Morate znati lozinku za memoriju *OBJECTSIGNING certifikata da iz nje kopirate certifikate.
4. Odredite lozinku za memoriju novih certifikata i kliknite **Nastavi** za kreiranje memorije certifikata. Stranica potvrde pokazuje da je memorija certifikata uspješno kreirana. Sada možete koristiti memoriju da upravljate i koristite certifikate za provjeru potpisa objekata.

   Bilješka: Ako ste kreirali ovu memoriju tako da možete provjeriti potpise na objektima koje ste potpisali, tada se možete zaustaviti. Kad ste kreirali nove certifikate za potpisivanje objekata, trebate ih eksportirati iz memorije *OBJECTSIGNING certifikata u ovu memoriju certifikata. Ako ih ne eksportirate nećete moći provjeriti potpise koje ste sa njima kreirali.

   Bilješka: Ako ste kreirali ovu memoriju certifikata tako da možete provjeriti potpise na objektima koje ste primili od drugih izvora, trebate nastaviti sa tim postupkom tako da možete importirati certifikate koje trebate u memoriji certifikata.
5. U navigacijskom okviru kliknite**Odaberi memoriju certifikata** i odaberite ***SIGNATUREVERIFICATION** da se otvori memorija certifikata.
6. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za memoriju certifikata kad ste je kreirali i kliknite **Nastavi**.
7. Nakon osvježenja navigacijskog okvira izaberite**Upravljaj certifikatima** za prikaz popisa zadataka.

8. Sa popisa zadataka izaberite**Importiraj certifikat**. Ovaj vođeni zadatak vas vodi kroz proces importiranja certifikata koje trebate u memoriju certifikata tako da možete provjeriti potpis na objektima koje ste primili.
9. Izaberite tip certifikata kojeg želite importirati. Izaberite **Provjera potpisa** da importirate certifikat koji ste primili sa potpisanim objektima i dovršite zadatak importiranja.

   Bilješka: Ako memorija certifikata već ne sadrži kopiju CA certifikata za CA koji je izdao certifikat provjere potpisa, morate importirati CA certifikat *prije*. Možete primiti pogrešku kod importiranja certifikata provjere potpisa ako ne importirate CA certifikat prije importiranja certifikata provjere potpisa.

Ove certifikate možete koristiti za provjeru potpisa objekata.

Poglavlje 8. Upravljanje DCM-om

Nakon što konfigurirate Upravitelj digitalnih certifikata (DCM), postoje mnogi zadaci upravljanja certifikatom koje trebate obaviti kroz vrijeme. Da naučite kako koristiti DCM za upravljanje vašim digitalnim certifikatima, pregledajte ova poglavlja:

Koristite lokalni CA za izdavanje certifikata za druge iSeries sisteme
Naučite kako koristiti privatni Lokalni CA na jednom sistemu za izdavanje certifikata na korištenje na drugim iSeries sistemima.

Upravljanje aplikacijama u DCM-u
Naučite kako koristiti DCM za rad sa definicijama aplikacija za SSL-omogućene aplikacije ili aplikacije potpisivanja objekata. Ova poglavlja pružaju informacije o kreiranju definicija aplikacija i kako upravljati dodjelom certifikata aplikacije. Možete naučiti o definiranju CA popisa povjerenja koje koriste aplikacije kao osnovu za prihvaćanje certifikata za provjeru vjerodostojnosti.

Provjera valjanosti certifikata i aplikacija
Naučite kako provjeriti autentičnost određenog certifikata prije nego ga aplikacija koristi ili prihvati.

Dodjela certifikata
Naučite kako možete brzo dodijeliti certifikat jednoj ili više aplikacija za korištenje za sigurne funkcije.

Upravljanje CRL lokacijama Naučite kakao definirati i koristiti lokacije Popisa uskraćivanja certifikata koje aplikacije mogu koristiti za provjeru valjanosti certifikata.

Pohranite ključeve certifikata na IBM 4758 kriptografičkom koprocesoru
Naučite kako koristiti instalirani koprocesor za pružanje sigurnije memorije za privatne ključeve vaših certifikata.

Upravljanje lokacijom zahtjeva za PKIX CA
Naučite kako koristiti DCM za upravljanje certifikatima koje možete dobiti od javno Internet CA koji izdaje certifikate pod Infrastrukturom javnog ključa za X.509 (PKIX) standarde.

Potpisivanje objekata
Naučite kako koristiti DCM da upravljate certifikatima koje koristite za digitalno potpisivanje objekata za osiguravanje njihove cjelovitosti.

Provjeravanje valjanosti potpisa objekata
Naučite kako koristiti DCM za provjeru valjanosti digitalnih potpisa na objektima.

Koristite lokalni CA za izdavanje certifikata za druge iSeries sisteme

Možda već koristite privatni Lokalni Izdavač certifikata (CA) na iSeries sistemu u vašoj mreži. Sada, želite proširiti upotrebu ovog lokalnog CA na drugi iSeries sistem u vašoj mreži. Na primjer, želite da vaš trenutni Lokalni CA izda certifikat poslužitelja ili klijenta za aplikaciju na drugom iSeries sistemu za upotrebu u SSL komunikacijskim sesijama. Ili, možete koristiti certifikate sa vašeg Lokalnog CA na jednom sistemu za potpisivanje objekata koje spremate na drugom iSeries poslužitelju.

Taj cilj možete postići koristeći Upravitelja digitalnih certifikata (DCM). Izvodite neke zadatke na iSeries na kojima koristite Lokalni CA i izvodite druge na sekundarnom iSeries sistemu koji podržava aplikacije za koje želite izdati certifikate. Taj sekundarni sistem se naziva ciljni sistem. Zadaci koje morate izvesti na ciljnom sistemu ovise o razini izdanja tog sistema.

Bilješka: Možete se susresti sa problemom ako iSeries sistem na kojem izvodite Lokalni CA koristi proizvod dobavljača kriptografičkog pristupa koji pruža jače šifriranje nego ciljni sistem. (Za V5R2 jedini dostupni dobavljač kriptografičkog pristupa je 5722–AC3, koji je najjači dostupan proizvod. Ipak, u ranijim izdanjima, mogli ste instalirati druge, slabije proizvode dobavljača kriptografičkog pristupa (5722–AC1, ili 5722–AC2) koji su pružali niže razine kriptografičkih funkcija.) Kad eksportirate certifikat (sa njegovim privatnim ključem), sistem šifrira datoteku da zaštiti njen sadržaj. Ako sistem upotrebljava jači kriptografički proizvod nego ciljni sistem, ciljni sistem ne može dešifrirati datoteku tijekom postupka importiranja. Prema tome, import možda ne bi uspio ili certifikat ne bi bio upotrebljiv za postavljanje SSL sesija. To je točno i onda kad koristite onu veličinu ključa za novi certifikat, koja je prikladna za korištenje sa kriptografičkim proizvodom na ciljnom sistemu.

Možete koristiti vaš Lokalni CA da izdate certifikate drugim sistemima, koje tada možete koristiti za potpisivanje objekata ili ih aplikacije mogu koristiti za uspostavljanje SSL sesija. Kada koristite Lokalni CA da kreirate certifikat za korištenje u drugom iSeries sistemu, datoteke koje DCM kreira sadrže kopiju Lokalnog CA certifikata, kao i kopije certifikata za mnoge javne Internet CA.

Zadaci koje morate izvesti u DCM-u razlikuju se neznatno ovisno o tipu certifikata koji vaš Lokalni CA izdaje i razini izdanja i uvjetima na ciljnom sistemu.

Izdajte privatne certifikate za korištenje na drugom V5R2 ili V5R1 iSeries sistemu

Za korištenje vaših Lokalnih CA da izdaju certifikate za korištenje na drugom V5R2 ili V5R1 iSeries sistemu, načinite ove korake na sistemu koji poslužuje Lokalni CA:

1. Pokrenite DCM.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
2. U navigacionom okviru, izaberite **Kreiraj certifikat** da prikažete listu tipova certifikata za čije kreiranje možete koristiti vaš Lokalni CA.

   Ne morate otvoriti memoriju certifikata za dovršenje ovog zadatka. Ove upute pretpostavljaju bilo da ne radite u određenoj memoriji certifikata ili da radite u memoriji certifikata lokalnog Izdavača certifikata (CA). Lokalni CA mora postojati na ovom sistemu prije nego možete izvesti ove zadatke.
3. Izaberite tip certifikata koji želite da Lokalni CA izda i kliknite **Nastavi** da započnete vođeni zadatak i završite seriju obrazaca. Izaberite ili kreiranje **certifikata poslužitelja ili klijenta za drugi iSeries** (za SSL sesije), ili **certifikat potpisivanja objekata za drugi iSeries** (za upotrebu na drugom sistemu).

   Bilješka: Ako kreirate certifikat potpisivanja objekta koji treba koristiti drugi sistem, taj sistem mora izvoditi V5R1 ili kasniju verziju OS/400 za korištenje certifikata. Budući da ciljni sistem mora imati V5R1 ili kasniju verziju, DCM na host sistemu ne upućuje vas da izaberete format ciljnog izdanja za novi certifikat za potpisivanje objekta.
4. Ako kreirate certifikat poslužitelja ili klijenta, izaberite ovu razinu izdanja iSeries sistema za koji kreirate ovaj certifikat. Kliknite **Nastavi** za prikaz obrasca koji vam dopušta da pribavite identifikacijske informacije za novi certifikat.

   Bilješka: Razina izdanja, koju odaberete, određuje format kojeg koristi DCM za kreiranje novog certifikata. Količina i tip identifikacijskih informacija na obrascu varira ovisno o razini izdanja koju ste izabrali. Ovo osigurava da su datoteke certifikata kompatibilne sa iSeries sistemom koji će koristiti certifikat.

5. Popunite obrazac i kliknite **Nastavi** za prikaz stranice certifikata.

   Bilješka: Ako postoji memorija *OBJECTSIGNING ili *SYSTEM certifikata na ciljnom sistemu, svakako odredite jedinstvenu oznaku certifikata i jedinstveno ime datoteke za certifikat. Određivanjem jedinstvene oznake certifikata i imena datoteke omogućuje vam se lako importiranje certifikata u postojeću memoriju certifikata na ciljnom sistemu.

   Ova stranica certifikata prikazuje imena datoteka koje je DCM kreirao za vas za prijenos na ciljni sistem. DCM kreira ove datoteke na osnovi razine izdanja ciljnog sistema kojeg ste specificirali. DCM automatski stavlja kopiju Lokalnog CA certifikata u te datoteke.

   Bilješka: DCM kreira novi certifikat u vlastitoj memoriji certifikata i generira dvije datoteke da prenesete: datoteka memorije certifikata (.KDB ekstenzija) i datoteka zahtjeva (.RDB ekstenzija).
6. Koristite binarni Protokol za prijenos datoteke (FTP) ili drugi način prijenosa datoteka ciljnom sistemu.

Izdajte privatne certifikate za korištenje na V4R4 ili V4R5 iSeries sistemu

Za korištenje vaših Lokalnih CA da izdaju certifikate za korištenje na V4R4 ili V4R5 iSeries sistemu, načinite ove korake na sistemu koji poslužuje V5R2 Lokalni CA:

1. Pokrenite DCM.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
2. U navigacionom okviru, izaberite**Kreiraj certifikat** da prikažete listu tipova certifikata za čije kreiranje možete koristiti vaš Lokalni CA.

   Ne morate otvoriti memoriju certifikata za dovršenje ovog zadatka. Ove upute pretpostavljaju bilo da ne radite u određenoj memoriji certifikata ili da radite u memoriji certifikata lokalnog Izdavača certifikata (CA). Lokalni CA mora postojati na ovom sistemu prije nego možete izvesti ove zadatke.
3. Izaberite tip certifikata koji želite da Lokalni CA izda i kliknite **Nastavi** da započnete vođeni zadatak i završite seriju obrazaca.

   Bilješka: Zato što kreirate ovaj certifikat za korištenje na V4R4 ili V4R5 iSeries sistemu, morate izabrati **certifikat poslužitelja ili klijenta za drugi iSeries**. Ciljni sistemi sa razinom izdanja ranijom od V5R1 ne mogu koristiti certifikate za potpisivanje objekata.
4. Izaberite razinu izdanja za iSeries za koju kreirate ovaj certifikat. Kliknite **Nastavi** za prikaz obrasca koji vam dopušta da pribavite identifikacijske informacije za novi certifikat.

   Bilješka: Razina izdanja, koju odaberete, određuje format kojeg koristi DCM za kreiranje novog certifikata. Količina i tip identifikacijskih informacija na obrascu varira ovisno o razini izdanja koju ste izabrali. Ovo osigurava da su datoteke certifikata kompatibilne sa iSeries sistemom koji će koristiti certifikat.
5. Popunite obrazac i kliknite **Nastavi** za prikaz stranice certifikata.

   Bilješka: Ako postoji memorija *SYSTEM certifikata na ciljnom sistemu, svakako odredite jedinstvenu oznaku certifikata i jedinstveno ime datoteke za certifikat. Određivanjem jedinstvene oznake certifikata i imena datoteke omogućuje vam se lako importiranje certifikata u postojeću memoriju certifikata na ciljnom sistemu.

   Ova stranica certifikata prikazuje imena datoteka koje je DCM kreirao za vas za prijenos

na ciljni sistem. DCM kreira ove datoteke na osnovi razine izdanja ciljnog sistema kojeg ste specificirali. DCM automatski stavlja kopiju Lokalnog CA certifikata u te datoteke.

Bilješka: DCM kreira novi certifikat u vlastitoj memoriji certifikata i generira dvije datoteke da prenesete: datoteka memorije certifikata (.KDB ekstenzija) i datoteka zahtjeva (.RDB ekstenzija).

Bilješka: Ako planirate koristiti certifikate u tim datotekama u postojećoj *SYSTEM memoriji certifikata na V4R4 ili V4R5 ciljnom sistemu, ne možete importirati Lokalni CA certifikat direktno iz .KDB i .RDB datoteka. To je zbog toga što CA certifikat nije u formatu kojeg DCM importna funkcija može prepoznati i upotrijebiti. Umjesto toga, morate koristiti host sistem da eksportirate kopiju Lokalnog CA certifikata u zasebnu datoteku da osigurate da je CA certifikat u formati koji će raditi sa importiranom funkcijom za ranija izdanja.

6. U navigacijskom okviru kliknite **Izaberi memoriju certifikata** i izaberite ***SYSTEM** da se otvori memorija certifikata.
7. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za memoriju certifikata kad ste je kreirali na host sistemu i kliknite **Nastavi**.
8. U navigacijskom okviru izaberite **Upravljaj certifikata** za prikaz popisa zadataka.
9. Sa popisa zadataka izaberite **Eksportiraj certifikat**.
10. Izaberite **Izdavača certifikata (CA)** kao tip certifikata za eksport i **Nastavi** za prikaz popisa CA certifikata.
11. Iz liste certifikata, izaberite Lokalni CA certifikat (na primjer, LOCAL_CERTIFICATE_AUTHORITY). Kliknite**Eksport** za prikaz obrasca koji vam dopušta da izaberete odredište za CA certifikat.
12. Izaberite **Datoteku** i kliknite **Nastavi** .
13. Specificirajte potpuno kvalificiranu stazu i ime datoteke za eksportnu datoteku i kliknite**Nastavi** . Stranica potvrde pokazuje da je DCM uspješno eksportirao datoteku.

    Bilješka: Provjerite da li ste dali datoteci jedinstveno ime i ekstenziju. Na primjer, mogli ste datoteku nazvati mycafile.exp. Kad imenujete datoteku, nemojte za datoteku upotrijebiti nijednu od ovih ekstenzija:.TXT, .KDB, .RDB, ili .KYR. Korištenjem jednog od ovih tipova ekstenzije može kreirati problem kada importirate datoteku na ciljni sistem.
14. Koristite binarni Protokol za prijenos datoteke (FTP) ili drugi način prijenosa datoteka memorije certifikata koje ste kreirali (.KDB i .RDB) na V4R4 ili V4R5 ciljnom sistemu. Koristite ASCII FTP način za prijenos datoteke koja sadrži eksportirani Lokalni CA certifikat.

Koristite prenesene datoteke na ciljnom sistemu

Nakon što prenesete datoteke, koristite DCM na ciljnom sistemu da radite sa prenesenim datotekama certifikata. DCM zadaci, koje morate obaviti, variraju ovisno o razini izdanja ciljnog sistema i o tome koje memorije certifikata postoje na ciljnom sistemu. Tip certifikata kojeg ste kreirali na host sistemu također utječe na zadatke, koje morate obaviti na ciljnom sistemu. Da naučite kako upotrebljavati DCM na ciljnom sistemu za rad sa prenesenim datotekama certifikata, pogledajte ova poglavlja:

- Koristite privatni certifikat za SSL sesije na V5R2 ciljnom sistemu.
- Koristite privatni certifikat za SSL sesije na V5R1 ciljnom sistemu.
- Koristite privatni certifikat za potpisivanje objekata na V5R2 ili V5R1 ciljnom sistemu.
- Koristite privatni certifikat za SSL sesije na V4R5 ili V4R4 ciljnom sistemu.

Koristite privatni certifikat za SSL sesije na V5R2 ciljnom sistemu

Certifikatima, koje koriste vaše aplikacije za SSL sesije, upravljate iz memorije *SYSTEM certifikata u Upravitelju digitalnih certifikata. Ako niste nikad upotrebljavali DCM na V5R2 ciljnom sistemu za upravljanje certifikatima za SSL, tada ta memorija certifikata ne bi trebala postojati na ciljnom sistemu. Zadaci za korištenje prenesenih datoteka memorije certifikata koje ste kreirali na host sistemu Lokalnog Izdavača certifikata (CA) ovise ovisno o tome postoji li *SYSTEM memorija certifikata. Ako *SYSTEM memorija certifikata ne postoji, možete koristiti prenesene datoteke certifikata kao način kreiranja *SYSTEM memorije certifikata. Ako *SYSTEM certifikat postoji na V5R2 ciljnom sistemu, možete koristiti prenesene datoteke certifikata na jedan od dva načina:

- Koristite prenesene datoteke kao Memoriju certifikata drugog sistema.
- Importirajte prenesene datoteke u postojeću *SYSTEM memoriju certifikata.

***SYSTEM memorija certifikata ne postoji**

Ako memorija *SYSTEM certifikata ne postoji na V5R2 sistemu na kojem želite koristiti prenesene datoteke memorije certifikata, možete koristiti prenesene datoteke certifikata kao memoriju *SYSTEM certifikata. Za kreiranje *SYSTEM memorije certifikata i korištenje datoteka certifikata na vašem V5R2 ciljnom sistemu slijedite ove korake:

1. Budite sigurni da su datoteke memorije certifikata (dvije datoteke: jedna sa .KDB ekstenzijom i jedna sa .RDB ekstenzijom) koje ste kreirali na sistemu koji poslužuje Lokalni CA u /QIBM/USERDATA/ICSS/CERT/SERVER direktoriju.
2. Jednom kada su prenesene datoteke certifikata u /QIBM/USERDATA/ICSS/CERT/SERVER direktoriju, preimenujte te datoteke u DEFAULT.KDB i DEFAULT.RDB. Preimenovanjem ovih datoteka u odgovarajućem direktoriju, kreirate komponente koje sačinjavaju memoriju *SYSTEM certifikata za ciljni sistem. Datoteke memorije certifikata već sadrže kopije certifikata za mnoge javne Internet CA-ove. DCM ih je dodao, kao i kopiju Lokalnog CA certifikata, u datoteke memorije certifikata kada ste ih kreirali.

   Pozor: Ako vaš ciljni sistem već ima DEFAULT.KDB i DEFAULT.RDB datoteku u /QIBM/USERDATA/ICSS/CERT/SERVER direktoriju, *SYSTEM memorija certifikata trenutno postoji na ovom ciljnom sistemu. Prema tome, ne bi trebali, kao što je sugerirano, preimenovati prenesene datoteke. Prepisivanje defaultne datoteke će uzrokovati problem kod korištenja DCM-a, memorije prenesenih certifikata i njenog sadržaja. Umjesto toga morate biti sigurni da one imaju jedinstvena imena i da koriste memoriju prenesenih certifikata kao **Memorija certifikata drugog sistema**. Ako koristite datoteke kao Memoriju certifikata drugog sistema, ne možete upotrijebiti DCM za određivanje koja aplikacija treba koristiti certifikat.
3. Pokrenite DCM. Sada morate promijeniti lozinku za memoriju *SYSTEM certifikata koju ste kreirali preimenovanjem prenesenih datoteka. Promjenom lozinke se dopušta da DCM pohrani novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u memoriji certifikata.
4. U navigacijskom okviru kliknite **Izaberi memoriju certifikata** i izaberite ***SYSTEM** da se otvori memorija certifikata.
5. Kad se prikaže stranica memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za *host* sistem za memoriju certifikata kad ste kreirali certifikat za V5R2 ciljni sistem i kliknite **Nastavi**.
6. U navigacijskom okviru izaberite **Upravljaj memorijom certifikata** i izaberite **Promijeni lozinku** sa popisa zadataka. Popunite obrazac da promijenite lozinku za memoriju certifikata. Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima. Zatim možete odrediti koje aplikacije trebaju koristiti certifikat za SSL sesije.

7. U navigacijskom okviru kliknite **Izaberi memoriju certifikata** i izaberite ***SYSTEM** da se otvori memorija certifikata.
8. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite novu lozinku i kliknite **Nastavi**.
9. Nakon osvježenja navigacijskog okvira, izaberite **Upravljaj certifikatima** u navigacijskom okviru da se prikaže popis zadataka.
10. Sa popisa zadataka izaberite **Pridruži certifikat** da prikažete listu certifikata u trenutnoj memoriji certifikata.
11. Izaberite certifikat koji ste kreirali na *host* sistemu i kliknite **Pridruži aplikacijama** da prikažete listu SSL omogućenih aplikacija kojima možete dodijeliti certifikat.
12. Izaberite aplikacije koje trebaju koristiti certifikat za SSL sesije i kliknite **Nastavi**. DCM prikazuje poruku da potvrđuje vaš izbor certifikata za te aplikacije.

    Bilješka: Neke SSL omogućene aplikacije podržavaju provjeru autentičnosti klijenta osnovanu na certifikatima. Aplikacija sa tom podrškom mora biti sposobna za provjeru autentičnosti certifikata prije pribavljanja pristupa resursima. Prema tome, morate definirati popis pouzdanih CA za aplikaciju. Time se osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA-ova, koje ste naveli kao pouzdane. Ako korisnici ili klijentova aplikacija predoči certifikat od CA, koji nije naveden kao pouzdan na popisu pouzdanih CA-ova, ta aplikacija ga neće prihvatiti kao temelj za važeću provjeru autentičnosti.

Sa ovim dovršenim zadacima, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao Lokalni CA na drugom iSeries-u. Međutim, prije nego što počnete koristiti SSL za ove aplikacije, morate konfigurirati aplikacije za korištenje SSL-a.

Prije nego korisnik može pristupiti izabranim aplikacijama kroz SSL vezu, korisnik mora koristiti DCM da dobije kopiju Lokalnog CA certifikata od host sistema. Lokalni CA certifikat se mora kopirati u datoteku na korisnikovom PC računalu ili učitati u korisnikov pretražitelj, ovisno o zahtjevima aplikacije koja radi sa SSL.

*SYSTEM memorija certifikata postoji — korištenjem datoteka kao Memorija certifikata drugog sistema

Ako V5R2 ciljni sistem već ima memoriju *SYSTEM certifikata, morate odlučiti kako raditi sa datotekama certifikata. Možete odlučiti da radite sa prenesenim datotekama certifikata kao **Memorijom certifikata drugog sistema** . Ili, možete izabrati importiranje privatnog certifikata i njemu odgovarajućeg Lokalnog CA certifikata u postojeću *SYSTEM memoriju certifikata.

Druge sistemske memorije certifikata su korisnički definirane sekundarne memorije certifikata za SSL certifikate. Možete ih kreirati i koristiti za pribavljanje certifikata za korisnički pisane SSL omogućene aplikacije koje ne koriste DCM API za registraciju aplikacijskog ID-a sa DCM svojstvom. Opcija druge sistemske memorije certifikata vam dopušta upravljanje certifikatima za aplikacije koje pišete vi ili drugi, koje koriste SSL_Init API za programski pristup i korištenje certifikata za postavljanje SSL sesije. Ovaj API omogućuje aplikaciji korištenje defaultnog certifikata za memoriju certifikata radije nego onog certifikata kojeg ste specifično identificirali.

IBM iSeries aplikacije (i mnoge druge aplikacije razvijatelja softvera) su pisane za korištenje certifikata samo u *SYSTEM memoriji certifikata. Ako koristite prenesene datoteke kao druge sistemske memoriju certifikata, ne možete upotrijebiti DCM za određivanje koje aplikacije trebaju koristiti certifikat za SSL sesiju. Kao posljedica, ne možete konfigurirati

iSeries SSL-omogućene aplikacije da koriste ovaj certifikat. Ako želite koristiti certifikat za iSeries aplikacije, morate importirati certifikat iz vaših prenesenih datoteka memorije certifikata u *SYSTEM memoriju certifikata.

Da pristupite i radite sa prenesenim datotekama certifikata kao sa drugom sistemskom memorijom certifikata, slijedite ove korake:

1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i odaberite **Druga sistemska memorija certifikata** da se otvori memorija certifikata.
3. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite puno kvalificirano ime staze i datoteke za datoteku memorije certifikata (ona sa .KDB ekstenzijom) koju ste prenijeli sa host sistema. Također pribavite lozinku koju ste specificirali na *host* sistemu za memoriju certifikata kada ste kreirali certifikat za V5R2 ciljni sistem i kliknite **Nastavi**.
4. U navigacijskom okviru izaberite **Upravljaj memorijom certifikata** i izaberite **Promijeni lozinku** sa popisa zadataka. Popunite obrazac da promijenite lozinku za memoriju certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za memoriju certifikata. Korištenjem ove opcije osigurava se da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novoj memoriji.

   Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima. Zatim možete odrediti da se certifikat u toj memoriji može koristiti kao defaultni certifikat.
5. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i odaberite **Druga sistemska memorija certifikata** da se otvori memorija certifikata.
6. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite puno kvalificirano ime staze i datoteke za datoteku memorije certifikata, pribavite novu lozinku i kliknite **Nastavi**.
7. Nakon osvježavanja navigacijskog okvira, izaberite **Upravljaj memorijom certifikata** i izaberite **Postavi default certifikat** sa popisa zadataka.

Sada kada ste kreirali i konfigurirali drugu sistemsku memoriju certifikata, svaka aplikacija koja koristi SSL_Init API može upotrijebiti certifikat u njoj za postavljanje SSL sesije.

*SYSTEM memorija certifikata postoji — korištenjem certifikata u postojećoj *SYSTEM memoriji certifikata

Možete koristiti certifikate u prenesenim datotekama memorije certifikata u postojećoj memoriji *SYSTEM certifikata na V5R2 sistemu. Da to učinite, morate importirati certifikate od datoteka memorije certifikata u postojeću memoriju *SYSTEM certifikata. Ipak, ne možete importirati certifikate direktno iz .KDB i .RDB datoteka jer nisu u formatu koji DCM funkcija importa može prepoznati i koristiti. Za korištenje prenesenih certifikata u postojećoj *SYSTEM memoriji certifikata morate otvoriti datoteke kao Drugu memoriju sistemskih certifikata i eksportirati ih u *SYSTEM memoriju certifikata.

Za eksportiranje certifikata iz datoteka memorije certifikata u *SYSTEM memorije certifikata, dovršite ove korake na V5R2 ciljnom sistemu:

1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i specificirajte **Druga sistemska memorija certifikata** da se otvori memorija certifikata.
3. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite puno kvalificirano ime staze i datoteke za datoteku memorije certifikata (ona sa .KDB ekstenzijom) koju ste

prenijeli sa host sistema. Također pribavite lozinku koju ste specificirali na *host* sistemu za memoriju certifikata kada ste kreirali certifikat za V5R2 ciljni sistem i kliknite **Nastavi**.

4. U navigacijskom okviru izaberite **Upravljaj memorijom certifikata** i izaberite **Promijeni lozinku** sa popisa zadataka. Popunite obrazac da promijenite lozinku za memoriju certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za memoriju certifikata. Korištenjem ove opcije osigurava se da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novoj memoriji. Ako ne promijenite lozinku i izaberete opciju Automatska prijava, možete naići na pogreške kod eksportiranja certifikata iz ove memorije u *SYSTEM memoriju certifikata.

   Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima.
5. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i odaberite **Druga sistemska memorija certifikata** da se otvori memorija certifikata.
6. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite puno kvalificirano ime staze i datoteke za datoteku memorije certifikata, pribavite novu lozinku i kliknite **Nastavi**.
7. Nakon osvježenja navigacijskog okvira, izaberite **Upravljaj certifikatima** u navigacijskom okviru da se prikaže popis zadataka i izaberite **Eksportiraj certifikat**.
8. Izaberite **Izdavača certifikata (CA)** kao tip certifikata za eksport i kliknite **Nastavi**.

   Bilješka: Trebate eksportirati Lokalni CA certifikat u memoriju certifikata prije nego eksportirate certifikat poslužitelja ili klijenta u memoriju certifikata. Ako eksportirate prvo certifikat poslužitelja ili klijenta, možete naići na grešku jer Lokalni CA certifikat ne postoji u memoriji certifikata.
9. Izaberite certifikat lokalnog CA za eksport i kliknite **Eksport**.
10. Izaberite **Memoriju certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavi**.
11. Unesite *SYSTEM kao ciljnu memoriju certifikata, unesite lozinku za memoriju *SYSTEM certifikata i kliknite **Nastavi**. Poruka se prikazuje da pokaže da je certifikat uspješno eksportiran ili da dobavi informacije o grešci ako proces eksporta nije uspio.
12. Sada možete eksportirati certifikat poslužitelja ili klijenta u *SYSTEM memoriju certifikata. Ponovo izaberite zadatak **Eksportiraj certifikat**.
13. Izaberite **Poslužitelj ili klijent** kao tip certifikata za eksport i kliknite **Nastavi**.
14. Izaberite prikladan certifikat poslužitelja ili klijenta za eksport i kliknite **Eksportiraj**.
15. Izaberite **Memoriju certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavi**.
16. Unesite *SYSTEM kao ciljnu memoriju certifikata, unesite lozinku za memoriju *SYSTEM certifikata i kliknite **Nastavi**. Poruka se prikazuje da pokaže da je certifikat uspješno eksportiran ili da dobavi informacije o grešci ako proces eksporta nije uspio.
17. Sada možete pridružiti certifikat aplikacijama za korištenje za SSL. Kliknite **Izaberi memoriju certifikata** u navigacionom okviru i izaberite ***SYSTEM** kao memoriju certifikata koju treba otvoriti.
18. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku za *SYSTEM memoriju certifikata i kliknite **Nastavi**.
19. Nakon osvježenja navigacijskog okvira izaberite**Upravljaj certifikatima** za prikaz popisa zadataka.
20. Sa popisa zadataka izaberite **Pridruži certifikat** da prikažete listu certifikata u trenutnoj memoriji certifikata.
21. Izaberite certifikat koji ste kreirali na *host* sistemu i kliknite **Pridruži aplikacijama** da prikažete listu SSL omogućenih aplikacija kojima možete dodijeliti certifikat.
22. Izaberite aplikacije koje trebaju koristiti certifikat za SSL sesije i kliknite **Nastavi**. DCM prikazuje poruku da potvrđuje vaš izbor certifikata za te aplikacije.

Bilješka: Neke SSL omogućene aplikacije podržavaju provjeru autentičnosti klijenta osnovanu na certifikatima. Aplikacija sa tom podrškom mora biti sposobna za provjeru autentičnosti certifikata prije pribavljanja pristupa resursima. Prema tome, moratedefinirati popis pouzdanih CA za aplikaciju. Time se osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA-ova, koje ste naveli kao pouzdane. Ako korisnici ili klijentova aplikacija predoči certifikat od CA, koji nije naveden kao pouzdan na popisu pouzdanih CA-ova, ta aplikacija ga neće prihvatiti kao temelj za važeću provjeru autentičnosti.

Sa ovim dovršenim zadacima, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao Lokalni CA na drugom iSeries-u. Međutim, prije nego što počnete koristiti SSL za ove aplikacije, morate konfigurirati aplikacije za korištenje SSL-a.

Prije nego korisnik može pristupiti izabranim aplikacijama kroz SSL vezu, korisnik mora koristiti DCM da dobije kopiju Lokalnog CA certifikata od host sistema. Lokalni CA certifikat se mora kopirati u datoteku na korisnikovom PC računalu ili učitati u korisnikov pretražitelj, ovisno o zahtjevima aplikacije koja radi sa SSL.

Koristite privatni certifikat za SSL sesije na V5R1 ciljnom sistemu

Certifikatima, koje koriste vaše aplikacije za SSL sesije, upravljate iz memorije *SYSTEM certifikata u Upravitelju digitalnih certifikata. Ako niste nikad upotrebljavali DCM na V5R1 ciljnom sistemu za upravljanje certifikatima za SSL, tada ta memorija certifikata ne bi trebala postojati na ciljnom sistemu. Zadaci za korištenje prenesenih datoteka memorije certifikata koje ste kreirali na host sistemu Lokalnog Izdavača certifikata (CA) ovise ovisno o tome postoji li *SYSTEM memorija certifikata. Ako *SYSTEM memorija certifikata ne postoji, možete koristiti prenesene datoteke certifikata kao način kreiranja *SYSTEM memorije certifikata. Ako *SYSTEM certifikat postoji na V5R1 ciljnom sistemu, možete koristiti prenesene datoteke certifikata na jedan od dva načina:

- Koristite prenesene datoteke kao Memoriju certifikata drugog sistema.
- Importirajte prenesene datoteke u postojeću *SYSTEM memoriju certifikata.

***SYSTEM memorija certifikata ne postoji**

Ako memorija *SYSTEM certifikata ne postoji na V5R1 sistemu na kojem želite koristiti prenesene datoteke memorije certifikata, možete koristiti prenesene datoteke certifikata kao memoriju *SYSTEM certifikata. Za korištenje datoteka certifikata na vašem V5R1 ciljnom sistemu slijedite ove korake:

1. Budite sigurni da su datoteke memorije certifikata (dvije datoteke: jedna sa .KDB ekstenzijom i jedna sa .RDB ekstenzijom) koje ste kreirali na sistemu koji poslužuje Lokalni CA u /QIBM/USERDATA/ICSS/CERT/SERVER direktoriju.
2. Jednom kada su prenesene datoteke certifikata u /QIBM/USERDATA/ICSS/CERT/SERVER direktoriju, preimenujte te datoteke u DEFAULT.KDB i DEFAULT.RDB. Preimenovanjem ovih datoteka u odgovarajućem direktoriju, kreirate komponente koje sačinjavaju memoriju *SYSTEM certifikata za ciljni sistem. Datoteke memorije certifikata već sadrže kopije certifikata za mnoge javne Internet CA-ove. DCM ih je dodao, kao i kopiju Lokalnog CA certifikata, u datoteke memorije certifikata kada ste ih kreirali.

   Pozor: Ako vaš ciljni sistem već ima DEFAULT.KDB i DEFAULT.RDB datoteku u /QIBM/USERDATA/ICSS/CERT/SERVER direktoriju, *SYSTEM memorija certifikata trenutno postoji na ovom ciljnom sistemu. Prema tome, ne bi trebali, kao što je sugerirano, preimenovati prenesene datoteke. Prepisivanje defaultne datoteke će uzrokovati problem kod korištenja DCM-a, memorije prenesenih

certifikata i njenog sadržaja. Umjesto toga morate biti sigurni da one imaju jedinstvena imena i da koriste memoriju prenesenih certifikata kao **Memorija certifikata drugog sistema**. Ako koristite datoteke kao Memoriju certifikata drugog sistema, ne možete upotrijebiti DCM za određivanje koja aplikacija treba koristiti certifikat.

3. Pokrenite DCM. Sada morate promijeniti lozinku za memoriju *SYSTEM certifikata koju ste kreirali preimenovanjem prenesenih datoteka. Promjenom lozinke se dopušta da DCM pohrani novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u memoriji certifikata.
4. U navigacijskom okviru kliknite **Izaberi memoriju certifikata** i izaberite ***SYSTEM** da se otvori memorija certifikata.
5. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za *host* sistem za memoriju certifikata kad ste kreirali certifikat za V5R1 ciljni sistem i kliknite **Nastavi**.
6. U navigacijskom okviru izaberite **Upravljaj memorijom certifikata** i izaberite **Promijeni lozinku** sa popisa zadataka. Popunite obrazac da promijenite lozinku za memoriju certifikata. Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima. Zatim možete odrediti koje aplikacije trebaju koristiti certifikat za SSL sesije.
7. U navigacijskom okviru kliknite **Izaberi memoriju certifikata** i izaberite ***SYSTEM** da se otvori memorija certifikata.
8. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite novu lozinku i kliknite **Nastavi**.
9. Nakon osvježenja navigacijskog okvira, izaberite **Upravljaj aplikacijama** u navigacijskom okviru da se prikaže popis zadataka.
10. Sa popisa zadataka izaberite **Ažuriraj dodjelu certifikata** za prikaz popisa SSL omogućenih aplikacija kojima ste dodijelili certifikat.
11. Izaberite neku aplikaciju sa popisa i kliknite **Ažuriraj dodjelu certifikata** .
12. Izaberite certifikat koji je Lokalni CA na *host* sistemu izdao i kliknite **Pridruži novi certifikat**. DCM prikazuje poruku da potvrđuje vaš izbor certifikata za tu aplikaciju.

    Bilješka: Neke SSL omogućene aplikacije podržavaju provjeru autentičnosti klijenta osnovanu na certifikatima. Aplikacija sa tom podrškom mora biti sposobna za provjeru autentičnosti certifikata prije pribavljanja pristupa resursima. Prema tome, moratedefinirati popis pouzdanih CA za aplikaciju. Time se osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA-ova, koje ste naveli kao pouzdane. Ako korisnici ili klijentova aplikacija predoči certifikat od CA, koji nije naveden kao pouzdan na popisu pouzdanih CA-ova, ta aplikacija ga neće prihvatiti kao temelj za važeću provjeru autentičnosti.

Sa ovim dovršenim zadacima, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao Lokalni CA na drugom iSeries-u. Međutim, prije nego što počnete koristiti SSL za ove aplikacije, morate konfigurirati aplikacije za korištenje SSL-a.

Prije nego korisnik može pristupiti izabranim aplikacijama kroz SSL vezu, korisnik mora koristiti DCM da dobije kopiju Lokalnog CA certifikata od host sistema. CA potvrda se mora kopirati u datoteku na korisnikovom PC računalu ili učitati u korisnikov pretražitelj, ovisno o zahtjevima aplikacije koja radi sa SSL.

*SYSTEM memorija certifikata postoji — korištenjem datoteka kao Memoriju certifikata drugog sistema

Ako V5R1 ciljni sistem već ima memoriju *SYSTEM certifikata, morate odlučiti kako raditi sa datotekama certifikata. Možete odlučiti da radite sa prenesenim datotekama certifikata kao

Memorijom certifikata drugog sistema . Ili, možete izabrati importiranje privatnog certifikata i njemu odgovarajućeg Lokalnog CA certifikata u postojeću *SYSTEM memoriju certifikata.

Druge sistemske memorije certifikata su korisnički definirane sekundarne memorije certifikata za SSL certifikate. Možete ih kreirati i koristiti za pribavljanje certifikata za korisnički pisane SSL omogućene aplikacije koje ne koriste DCM API za registraciju aplikacijskog ID-a sa DCM pomoćnim programom. Opcija druge sistemske memorije certifikata vam dopušta upravljanje certifikatima za aplikacije koje pišete vi ili drugi, koje koriste SSL_Init API za programski pristup i korištenje certifikata za postavljanje SSL sesije. Ovaj API omogućuje aplikaciji korištenje defaultnog certifikata za memoriju certifikata radije nego onog certifikata kojeg ste specifično identificirali.

IBM iSeries aplikacije (i mnoge druge aplikacije razvijatelja softvera) su pisane za korištenje certifikata samo u *SYSTEM memoriji certifikata. Ako koristite prenesene datoteke kao druge sistemske memoriju certifikata, ne možete upotrijebiti DCM za određivanje koje aplikacije trebaju koristiti certifikat za SSL sesiju. Kao posljedica, ne možete konfigurirati iSeries SSL-omogućene aplikacije da koriste ovaj certifikat. Ako želite koristiti certifikat za iSeries aplikacije, morate importirati certifikat iz vaših prenesenih datoteka memorije certifikata u *SYSTEM memoriju certifikata.

Da pristupite i radite sa prenesenim datotekama certifikata kao sa drugom sistemskom memorijom certifikata, slijedite ove korake:

1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i odaberite **Druga sistemska memorija certifikata** da se otvori memorija certifikata.
3. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite puno kvalificirano ime staze i datoteke za datoteku memorije certifikata (ona sa .KDB ekstenzijom) koju ste prenijeli sa host sistema. Također pribavite lozinku koju ste specificirali na *host* sistemu za memoriju certifikata kada ste kreirali certifikat za V5R1 ciljni sistem i kliknite **Nastavi**.
4. U navigacijskom okviru izaberite **Upravljaj memorijom certifikata** i izaberite **Promijeni lozinku** sa popisa zadataka. Popunite obrazac da promijenite lozinku za memoriju certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za memoriju certifikata. Korištenjem ove opcije osigurava se da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novoj memoriji.

   Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima. Zatim možete odrediti da se certifikat u toj memoriji može koristiti kao defaultni certifikat.
5. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i odaberite **Druga sistemska memorija certifikata** da se otvori memorija certifikata.
6. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite puno kvalificirano ime staze i datoteke za datoteku memorije certifikata, pribavite novu lozinku i kliknite **Nastavi**.
7. Nakon osvježavanja navigacijskog okvira, izaberite **Upravljaj memorijom certifikata** i izaberite **Postavi default certifikat** sa popisa zadataka.

Sada kada ste kreirali i konfigurirali drugu sistemsku memoriju certifikata, svaka aplikacija koja koristi SSL_Init API može upotrijebiti certifikat u njoj za postavljanje SSL sesije.

***SYSTEM memorija certifikata postoji — korištenjem certifikata u postojećoj *SYSTEM memoriji certifikata**

Možete koristiti certifikate u prenesenim datotekama memorije certifikata u postojećoj memoriji *SYSTEM certifikata na V5R1 sistemu. Da to učinite, morate importirati certifikate od datoteka memorije certifikata u postojeću memoriju *SYSTEM certifikata. Ipak, ne možete importirati certifikate direktno iz .KDB i .RDB datoteka jer nisu u formatu koji DCM funkcija importa može prepoznati i koristiti. Za korištenje prenesenih certifikata u postojećoj *SYSTEM memoriji certifikata morate otvoriti datoteke kao Drugu memoriju sistemskih certifikata i eksportirati ih u *SYSTEM memoriju certifikata.

Bilješka: Ova procedura opisuje kako koristiti Memoriju certifikata drugog sistema na ciljnom sistemu za eksportiranje certifikata iz originalnih datoteka memorije certifikata u *SYSTEM memoriju certifikata. Korištenjem ove metode dodavanja certifikata *SYSTEM memoriji certifikata vam pomaže da izbjegnete moguće probleme kada sistem koristi slabije proizvode pružatelja kriptografičkih usluga (kao 5722–AC2) od host sistema.

Za eksportiranje certifikata iz datoteka memorije certifikata u *SYSTEM memoriju certifikata, dovršite ove korake na V5R1 ciljnom sistemu:

1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i specificirajte **Druga sistemska memorija certifikata** da se otvori memorija certifikata.
3. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite puno kvalificirano ime staze i datoteke za datoteku memorije certifikata (ona sa .KDB ekstenzijom) koju ste prenijeli sa host sistema. Također pribavite lozinku koju ste specificirali na *host* sistemu za memoriju certifikata kada ste kreirali certifikat za V5R1 ciljni sistem i kliknite **Nastavi**.
4. U navigacijskom okviru izaberite **Upravljaj memorijom certifikata** i izaberite **Promijeni lozinku** sa popisa zadataka. Popunite obrazac da promijenite lozinku za memoriju certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za memoriju certifikata. Korištenjem ove opcije osigurava se da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novoj memoriji. Ako ne promijenite lozinku i izaberete opciju Automatska prijava, možete naići na pogreške kod eksportiranja certifikata iz ove memorije u *SYSTEM memoriju certifikata.

   Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima.
5. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i odaberite **Druga sistemska memorija certifikata** da se otvori memorija certifikata.
6. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite puno kvalificirano ime staze i datoteke za datoteku memorije certifikata, pribavite novu lozinku i kliknite **Nastavi**.
7. Nakon osvježenja navigacijskog okvira, izaberite **Upravljaj certifikatima** u navigacijskom okviru da se prikaže popis zadataka i izaberite **Eksport certifikata**.
8. Izaberite **Izdavača certifikata (CA)** kao tip certifikata za eksport i kliknite **Nastavi**.

   Bilješka: Trebate eksportirati Lokalni CA certifikat u memoriju certifikata prije nego eksportirate certifikat poslužitelja ili klijenta u memoriju certifikata. Ako eksportirate prvo certifikat poslužitelja ili klijenta, možete naići na grešku jer Lokalni CA certifikat ne postoji u memoriji certifikata.
9. Izaberite certifikat lokalnog CA za eksport i kliknite **Eksport**.
10. Izaberite **Memoriju certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavi**.
11. Unesite *SYSTEM kao ciljnu memoriju certifikata, unesite lozinku za memoriju *SYSTEM certifikata i kliknite **Nastavi**.

12. Sada možete eksportirati certifikat poslužitelja ili klijenta u *SYSTEM memoriju certifikata. Ponovo izaberite zadatak **Eksport certifikata**.
13. Izaberite **Poslužitelj ili klijent** kao tip certifikata za eksport i kliknite **Nastavi**.
14. Izaberite prikladan certifikat poslužitelja ili klijenta za eksport i kliknite **Eksportiraj**.
15. Izaberite **Memoriju certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavi**.
16. Unesite *SYSTEM kao ciljnu memoriju certifikata, unesite lozinku za memoriju *SYSTEM certifikata i kliknite **Nastavi**. Poruka se prikazuje da pokaže da je certifikat uspješno eksportiran ili da dobavi informacije o grešci ako proces eksporta nije uspio.
17. Sada možete pridružiti certifikat aplikacijama za korištenje za SSL. Kliknite **Izaberi memoriju certifikata** u navigacionom okviru i izaberite ***SYSTEM** kao memoriju certifikata koju treba otvoriti.
18. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku za *SYSTEM memoriju certifikata i kliknite **Nastavi**.
19. Nakon osvježenja navigacijskog okvira izaberite**Upravljaj certifikatima** za prikaz popisa zadataka.
20. Sa popisa zadataka izaberite **Ažuriraj dodjelu certifikata** za prikaz popisa SSL omogućenih aplikacija kojima ste dodijelili certifikat.
21. Izaberite neku aplikaciju sa popisa i kliknite **Ažuriraj dodjelu certifikata** .
22. Izaberite certifikat koji je Lokalni CA na *host* sistemu izdao i kliknite **Pridruži novi certifikat**. DCM prikazuje poruku da potvrđuje vaš izbor certifikata za tu aplikaciju.

    Bilješka: Neke SSL omogućene aplikacije podržavaju provjeru autentičnosti klijenta osnovanu na certifikatima. Aplikacija sa tom podrškom mora biti sposobna za provjeru autentičnosti certifikata prije pribavljanja pristupa resursima. Prema tome, moratedefinirati popis pouzdanih CA za aplikaciju. Time se osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA-ova, koje ste naveli kao pouzdane. Ako korisnici ili klijentova aplikacija predoči certifikat od CA, koji nije naveden kao pouzdan na popisu pouzdanih CA-ova, ta aplikacija ga neće prihvatiti kao temelj za važeću provjeru autentičnosti.

Sa ovim dovršenim zadacima, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao Lokalni CA na drugom iSeries-u. Međutim, prije nego što počnete koristiti SSL za ove aplikacije, morate konfigurirati aplikacije za korištenje SSL-a.

Prije nego korisnik može pristupiti izabranim aplikacijama kroz SSL vezu, korisnik mora koristiti DCM da dobije kopiju Lokalnog CA certifikata od host sistema. CA potvrda se mora kopirati u datoteku na korisnikovom PC računalu ili učitati u korisnikov pretražitelj, ovisno o zahtjevima aplikacije koja radi sa SSL.

Koristite privatni certifikat za potpisivanje objekata na V5R2 ili V5R1 ciljnom sistemu

Upravljate certifikatima, koje koristite za potpisivanje objekata od memorije *OBJECTSIGNING certifikata u Upravitelju digitalnih certifikata. Ako niste nikad upotrebljavali DCM na ciljnom sistemu za upravljanje certifikatima za potpisivanje objekata, tada ta memorija certifikata ne bi trebala postojati na ciljnom sistemu. Zadaci koje morate obaviti za korištenje prenesenih datoteka memorije certifikata koje ste kreirali na host sistemu Lokalnog CA ovise ovisno o tome postoji li *OBJECTSIGNING memorija certifikata. Ako *OBJECTSIGNING memorija certifikata ne postoji, možete koristiti prenesene datoteke certifikata kao način kreiranja *OBJECTSIGNING memorije certifikata. Ako *OBJECTSIGNING certifikat postoji na ciljnom sistemu, morate na njega importirati prenesene certifikate.

***OBJECTSIGNING memorija certifikata ne postoji**

Zadaci koje obavljate za korištenje datoteka memorije certifikata koje ste kreirali na host sistemu Lokalnog CA razlikuju se ovisno o tome jeste li ikad koristili DCM na ciljnom sistemu za upravljanje certifikatima potpisivanja objekata.

Ako *OBJECTSIGNING memorija certifikata ne opstoji na V5R2 ili V5R1 ciljnom sistemu sa prenesenim datotekama memorije certifikata, slijedite ove korake:

1. Budite sigurni da su datoteke memorije certifikata (dvije datoteke: jedna sa .KDB ekstenzijom i jedna sa .RDB ekstenzijom) koje ste kreirali na sistemu koji poslužuje Lokalni CA u /QIBM/USERDATA/ICSS/CERT/SIGNING direktoriju.
2. Jednom kada su prenesene datoteke certifikata u /QIBM/USERDATA/ICSS/CERT/SIGNING direktoriju, preimenujte te datoteke u SGNOBJ.KDB i SGNOBJ.RDB, ako je potrebno. Preimenovanjem ovih datoteka, kreirate komponente koje sačinjavaju memoriju *OBJECTSIGNING certifikata za ciljni sistem. Datoteke memorije certifikata već sadrže kopije certifikata za mnoge javne Internet CA-ove. DCM ih je dodao, kao i kopiju Lokalnog CA certifikata, u datoteke memorije certifikata kada ste ih kreirali.

   Pozor: Ako vaš ciljni sistem već ima SGNOBJ.KDB i SGNOBJ.RDB datoteku u /QIBM/USERDATA/ICSS/CERT/SIGNING direktoriju, *OBJECTSIGNING memorija certifikata trenutno postoji na ovom ciljnom sistemu. Prema tome, ne bi trebali, kao što je sugerirano, preimenovati prenesene datoteke. Prepisivanje defaultnih datoteka za potpisivanje objekata će uzrokovati problem kod korištenja DCM-a, memorije prenesenih certifikata i njenog sadržaja. Možete dobiti certifikate od tih datoteka u postojećoj memoriji *OBJECTSIGNING certifikata na jedan od dva načina. Možete eksportirati certifikate u ovu datoteku za postavljanje plošnih datoteka od kojih možete importirati certifikate u postojeću memoriju *OBJECTSIGNING certifikata. Ili možete otvoriti prenesene datoteke kao drugu sistemsku memoriju certifikata i eksportirati certifikate neposredno u memoriju *OBJECTSIGNING certifikata, kao što je opisano dalje u ovom materijalu. U bilo kojem slučaju, morate staviti certifikate na *OBJECTSIGNING memoriju certifikata ako želite upravljati aplikacijama koje ih koriste kako opisuje ova procedura.
3. Pokrenite DCM. Sada morate promijeniti lozinku za memoriju *OBJECTSIGNING certifikata. Promjenom lozinke se dopušta da DCM pohrani novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u memoriji certifikata.
4. U navigacijskom okviru kliknite **Izaberi memoriju certifikata** i odaberite ***OBJECTSIGNING** da se otvori memorija certifikata.
5. Kad se prikaže stranica sa lozinkom, pribavite lozinku koju ste specificirali za memoriju certifikata kad ste je kreirali na host sistemu i kliknite **Nastavi**.
6. U navigacijskom okviru izaberite **Upravljaj memorijom certifikata** i izaberite **Promijeni lozinku** sa popisa zadataka. Popunite obrazac da promijenite lozinku za memoriju certifikata. Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima. Zatim možete kreirati definiciju aplikacije koju certifikat koristi za potpisivanje objekata.
7. Nakon ponovnog otvaranja memorije certifikata izaberite **Upravljaj aplikacijama** u navigacijskom okviru da se prikaže popis zadataka.
8. Sa popisa zadataka izaberite **Dodaj aplikaciju** da započnete postupak kreiranja definicije aplikacije za potpis objekata da koristite certifikat za potpisivanje objekata.
9. Popunite obrazac za definiranje vaše aplikacije za potpisivanje objekta i kliknite **Dodaj**. Ova definicija aplikacije ne opisuje stvarnu aplikaciju nego radije opisuje tip objekata koje planirate potpisivati sa specifičnim certifikatom. Koristite online pomoć za pitanja o popunjavanju obrasca.
10. Kliknite **OK** da potvrdite poruku potvrde za definiciju aplikacije i prikažite popis zadataka **Upravljaj aplikacijama**.
11. Sa popisa zadataka izaberite **Ažuriraj dodjelu certifikata** za prikaz popisa IDa aplikacija koje potpisuju objekte kojima ste dodijelili certifikat.

12. Izaberite ID vaše aplikacije sa popisa i kliknite **Ažuriraj dodjelu certifikata** .
13. Izaberite certifikat koji je Lokalni CA na host sistemu kreirao i kliknite **Pridruži novi certifikat**.

Kad završite ove zadatke, tada imate sve što trebate za početak potpisivanja objekata da osigurate njihovu cjelovitost.

Kada distribuirate potpisane objekte, one koji primaju objekte moraju koristiti V5R2 ili V5R1 verziju DCM-a da provjere potpis na objektima da osiguraju da su podaci nepromijenjeni i da provjere identitet pošiljaoca. Da provjeri potpis, primatelj mora imati kopiju certifikata za provjeru potpisa. Trebate pribaviti kopiju tog certifikata kao dijela paketa potpisanih objekata.

Primatelj također mora imati kopiju CA certifikata za CA, koji je izdao certifikat kojeg ste koristili za potpis objekta. Ako ste potpisali objekte sa certifikatom od dobro poznatog Internet CA, tada bi primateljeva verzija DCM-a trebala već imati kopiju potrebnog CA certifikata. Međutim, ako je potrebno, trebate pribaviti kopiju CA certifikata u posebnom paketu, zajedno sa potpisanim objektima. Na primjer, trebate dobaviti kopiju Lokalnog CA certifikata ako ste potpisali objekte sa certifikatom sa Lokalnog CA. Radi sigurnosnih razloga, trebate pribaviti CA certifikat u posebnom paketu ili učiniti CA certifikat javno dostupnim na zahtjev onih koji ga trebaju.

***OBJECTSIGNING memorija certifikata postoji**

Možete koristiti certifikate u prenesenim datotekama memorije certifikata u postojećoj memoriji *OBJECTSIGNING certifikata na V5R2 ili V5R1 sistemu. Da to učinite, morate importirati certifikate od datoteka memorije certifikata u postojeću memoriju *OBJECTSIGNING certifikata. Ipak, ne možete importirati certifikate direktno iz .KDB i .RDB datoteka jer nisu u formatu koji DCM funkcija importa može prepoznati i koristiti. Možete dodati certifikate u postojeću *OBJECTSIGNING memoriju certifikata otvaranjem prenesenih datoteka kao Memorija certifikata drugog sistema na V5R2 ili V5R1 ciljnom sistemu. Možete eksportirati certifikate neposredno u memoriju *OBJECTSIGNING certifikata. Morate eksportirati kopiju certifikata potpisivanja objekta i Lokalnog CA certifikata sa prenesenih datoteka.

Za eksportiranje certifikata iz datoteka memorije certifikata direktno u *OBJECTSIGNING memoriju certifikata, dovršite ove korake na V5R1 ili V5R2 ciljnom sistemu:

1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i specificirajte **Druga sistemska memorija certifikata** da se otvori memorija certifikata.
3. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite potpuno kvalificirano ime staze i datoteke za datoteke memorije certifikata. Također pribavite lozinku koju ste koristili hada ste ih kreirali na host sistemu i kliknite **Nastavi**.
4. U navigacijskom okviru izaberite **Upravljaj memorijom certifikata** i izaberite **Promijeni lozinku** sa popisa zadataka. Popunite obrazac da promijenite lozinku za memoriju certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za memoriju certifikata. Korištenjem ove opcije osigurava se da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novoj memoriji. Ako ne promijenite lozinku i izaberete opciju Automatska prijava, možete naići na pogreške kod eksportiranja certifikata iz ove memorije u *OBJECTSIGNING memoriju certifikata.

   Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima.

5. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i odaberite **Druga sistemska memorija certifikata** da se otvori memorija certifikata.
6. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite puno kvalificirano ime staze i datoteke za datoteku memorije certifikata, pribavite novu lozinku i kliknite **Nastavi**.
7. Nakon osvježenja navigacijskog okvira, izaberite **Upravljaj certifikatima** u navigacijskom okviru da se prikaže popis zadataka i izaberite **Eksport certifikata**.
8. Izaberite **Izdavač certifikata (CA)** kao tip certifikata za eksport i kliknite **Nastavi**.

   Bilješka: Formulacija ovog zadatka podrazumijeva da kad radite sa drugom sistemskom memorijom certifikata da radite sa poslužiteljskim ili klijentskim certifikatima. To je zato što je ovaj tip memorije certifikata oblikovan za upotrebu kao sekundarna memorija certifikata u *SYSTEM memoriji certifikata. Ipak, korištenjem zadatka eksportiranja u ovoj memoriji certifikata je najlakši način dodavanja certifikata iz prenesenih datoteka u postojeću *OBJECTSIGNING memoriju certifikata.
9. Izaberite certifikat lokalnog CA za eksport i kliknite **Eksportiraj**.

   Bilješka: Trebate eksportirati Lokalni CA certifikat u memoriju certifikata prije nego eksportirate certifikat potpisivanja objekata u memoriju certifikata. Ako eksportirate prvo certifikat potpisivanja objekta, možete naići na grešku jer Lokalni CA certifikat ne postoji u memoriji certifikata.
10. Izaberite **Memoriju certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavi**.
11. Unesite *OBJECTSIGNING kao ciljnu memoriju certifikata, unesite lozinku za memoriju certifikata i kliknite **Nastavi**.
12. Sada možete eksportirati certifikat za potpisivanje objekta u memoriju *OBJECTSIGNING certifikata. Ponovo izaberite zadatak **Eksportiraj certifikat**.
13. Izaberite **Poslužitelj ili klijent** kao tip certifikata za eksport i kliknite **Nastavi**.
14. Izaberite prikladan certifikat za eksport i kliknite **Eksportiraj**.
15. Izaberite **Memoriju certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavi**.
16. Unesite *OBJECTSIGNING kao ciljnu memoriju certifikata, unesite lozinku za *OBJECTSIGNING memoriju certifikata i kliknite **Nastavi**.Poruka se prikazuje da pokaže da je certifikat uspješno eksportiran ili da dobavi informacije o grešci ako proces eksporta nije uspio.

    Bilješka: Da bi koristili ovaj certifikat za potpisivanje objekata morate sada dodijeliti certifikat aplikaciji potpisivanja objekata.

Koristite privatni certifikat za SSL sesije na V4R5 ili V4R4 ciljnom sistemu

Certifikatima, koje koriste vaše aplikacije za SSL sesije, upravljate iz memorije *SYSTEM certifikata u Upravitelju digitalnih certifikata. Ako niste nikad upotrebljavali DCM na V4R5 ili V4R4 ciljnom sistemu za upravljanje certifikatima za SSL, tada ta memorija certifikata ne bi trebala postojati na ciljnom sistemu. Prenesene datoteke memorije certifikata koje ste kreirali na host sistemu Lokalnog CA sadrže dva certifikata. Te datoteke su certifikati poslužitelja ili klijenta koje ste kreirali i privatni Lokalni CA certifikat koji ste koristili za potpisivanje.

Zadaci koje morate obaviti za korištenje prenesenih datoteka memorije certifikata ovise ovisno o tome postoji li *SYSTEM memorija certifikata. Ako *SYSTEM memorija certifikata ne postoji, možete koristiti prenesene datoteke certifikata kao način kreiranja *SYSTEM memorija certifikata. Ako *SYSTEM certifikat postoji na ciljnom sistemu, možete koristiti prenesene datoteke certifikata na jedan od dva načina:

- Koristite prenesene datoteke kao Memoriju certifikata drugog sistema.
- Importirajte prenesene datoteke u postojeću *SYSTEM memoriju certifikata.

***SYSTEM memorija certifikata ne postoji**

Ako *SYSTEM memorija certifikata ne opstoji na V4R5 ili V4R4 sistemu na kojem želite koristiti prenesene datoteke memorije certifikata, slijedite ove korake:

1. Budite sigurni da su datoteke memorije certifikata (dvije datoteke: jedna sa .KDB ekstenzijom i jedna sa .RDB ekstenzijom) koje ste kreirali na sistemu koji poslužuje Lokalni CA u /QIBM/USERDATA/ICSS/CERT/SERVER direktoriju.
2. Jednom kada su prenesene datoteke certifikata u /QIBM/USERDATA/ICSS/CERT/SERVER direktoriju, preimenujte te datoteke u DEFAULT.KDB i DEFAULT.RDB. Preimenovanjem ovih datoteka u odgovarajućem direktoriju, kreirate komponente koje sačinjavaju memoriju *SYSTEM certifikata za ciljni sistem. Datoteke memorije certifikata već sadrže kopije certifikata za mnoge javne Internet CA-ove. DCM ih je dodao, kao i kopiju Lokalnog CA certifikata, u datoteke memorije certifikata kada ste ih kreirali.

   Pozor: Ako vaš ciljni sistem već ima DEFAULT.KDB i DEFAULT.RDB datoteku u /QIBM/USERDATA/ICSS/CERT/SERVER direktoriju, *SYSTEM memorija certifikata trenutno postoji na ovom ciljnom sistemu. Prema tome, ne bi trebali, kao što je sugerirano, preimenovati prenesene datoteke. Prepisivanje defaultne datoteke će uzrokovati problem kod korištenja DCM-a, memorije prenesenih certifikata i njenog sadržaja. Umjesto toga morate biti sigurni da one imaju jedinstvena imena i da koriste memoriju prenesenih certifikata kao **Drugu sistemsku memoriju certifikata**. Ako koristite datoteke kao Drugu memoriju certifikata, ne možete upotrijebiti DCM za određivanje koja aplikacija treba koristiti certifikat.
3. Pokrenite DCM. Sada morate promijeniti lozinku za memoriju *SYSTEM certifikata. Promjenom lozinke se dopušta da DCM pohrani novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u memoriji certifikata.
4. U navigacijskom okviru, osigurajte da je *SYSTEM prikazano kao memorija certifikata u padajućoj kućici s popisom i izaberite **Certifikati sistema** za prikazivanje liste dostupnih zadataka. **Memorija certifikata i lozinka** prozorski prikazi.
5. U odgovarajućim poljima, unesite *SYSTEM za memoriju certifikata koju ćete otvoriti i lozinku koju ste koristili kada ste kreirali datoteke korištenjem Lokalnog CA na host sistemu. Sada možete promijeniti lozinku za memoriju certifikata.
6. Sa popisa zadataka u navigacijskom okviru izaberite **Promijeni lozinku**. Popunite obrazac da promijenite lozinku za memoriju certifikata. Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima.
7. Nakon ponovnog otvaranja memorije *SYSTEM certifikata, odaberite **Rad sa sigurnim aplikacijama** sa popisa zadataka za prikaz stranice koja vam dopušta upravljanje certifikatima pridružene specifičnim aplikacijama.
8. Sa popisa aplikacija, odaberite aplikaciju koja treba koristiti prenesene privatne certifikate sa SSL sesija.
9. Kliknite **Radi sa sistemskim certifikatima** i izaberite certifikat koji je izdao Lokalni CA na host sistemu.
10. Kliknite **Dodijeli novi certifikat** da navedena aplikacija može koristiti izabrani certifikat.

    Bilješka: Neke SSL omogućene aplikacije podržavaju provjeru autentičnosti klijenta osnovanu na certifikatima. Koristeći certifikate za provjeru autentičnosti klijenta osigurava se da aplikacija primi važeći certifikat prije nego što se dopusti pristup resursima koje aplikacija kontrolira. Aplikacija sa tom

podrškom mora biti postavljena tako da ima povjerenje u CA prije nego što se aplikacija osposobi za provjeru autentičnosti certifikata, koje izdaje određeni CA. Koristite stranicu **Radi sa Izdavačima certifikata** da osigurate da CA certifikat ima pouzdan status u memoriji certifikata. Tada, koristite stranicu **Radi sa Sigurnim aplikacijama** da osigurate da aplikacije koje koriste certifikate imaju povjerenja u Lokalni CA koji ih je izdao. Time se osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA-ova, koje ste naveli kao pouzdane. Ako korisnici ili klijentova aplikacija predoči certifikat od CA, koji nije naveden kao pouzdan, ta aplikacija ga neće prihvatiti kao temelj za važeću provjeru autentičnosti.

Sa ovim dovršenim zadacima, aplikacije na V4R5 ili V4R4 ciljnom sistemu mogu koristiti certifikat koji je izdao V5R2 Lokalni CA na drugom iSeries-u. Međutim, prije nego što počnete koristiti SSL za ove aplikacije, morate konfigurirati aplikacije za korištenje SSL-a.

Prije nego korisnik može pristupiti izabranim aplikacijama kroz SSL vezu, korisnik mora koristiti DCM da dobije kopiju Lokalnog CA certifikata od host sistema. CA potvrda se mora kopirati u datoteku na korisnikovom PC računalu ili učitati u korisnikov pretražitelj, ovisno o zahtjevima aplikacije koja radi sa SSL.

***SYSTEM memorija certifikata postoji — korištenjem datoteka kao Memoriju certifikata drugog sistema**

Ako V4R5 ili V4R4 ciljni sistem već ima memoriju *SYSTEM certifikata, morate odlučiti kako raditi sa datotekama certifikata. Prenesene datoteke memorije certifikata sadrže dva certifikata: certifikate poslužitelja ili klijenta koje ste kreirali i privatni Lokalni CA certifikat koji ste koristili za potpisivanje. Možete odlučiti da koristite prenesene datoteke certifikata kao **Druge** sistemske memorije certifikata. Ili, možete izabrati importiranje privatnog certifikata i njemu odgovarajućeg CA certifikata u postojeću *SYSTEM memoriju certifikata.

Ako koristite prenesene datoteke certifikata kao **Druge**sistemske memorije certifikata, ne možete koristiti DCM da odredite koje aplikacije trebaju upotrijebiti certifikat za SSL sesije. Međutim, možete označiti certifikat u toj memoriji certifikata kao defaultni certifikat za memoriju certifikata. Opcija druge sistemske memorije certifikata vam dopušta upravljanje certifikatima za aplikacije koje pišete vi ili drugi, koje koriste SSL_Init API za programski pristup i korištenje certifikata za postavljanje SSL sesije. Ovaj API omogućuje aplikaciji korištenje defaultnog certifikata za memoriju certifikata radije nego specifični certifikat.

Ako *SYSTEM memorija certifikata postoji na V4R5 ili V4R4 sistemu na kojem želite koristiti prenesene datoteke memorije certifikata, slijedite ove korake:

1. Pokrenite DCM. Sada morate promijeniti lozinku za memoriju prenesenih certifikata. Promjenom lozinke se dopušta da DCM pohrani novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u memoriji certifikata.
2. U navigacijskom okviru, osigurajte da je OTHER prikazano kao memorija certifikata u padajućoj kućici s popisom i izaberite **Certifikati sistema** za prikazivanje liste dostupnih zadataka. **Memorija certifikata i lozinka** prozorski prikazi.
3. U odgovarajućim poljima, unesite puno kvalificirano ime staze i datoteke za memoriju certifikata (.KDB ekstenzija) koju ste prenijeli sa Lokalnog CA host sistema. Unesite lozinku koju ste koristili kada ste kreirali datoteke na *host* sistemu. Sada možete promijeniti lozinku za memoriju certifikata.
4. U navigacijskom okviru izaberite **Promijeni lozinku** sa popisa sistemskih zadataka certifikata. Popunite obrazac da promijenite lozinku za memoriju certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za memoriju certifikata. Korištenjem ove opcije osigurava se da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM

certifikatima u novoj memoriji.

Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima. Zatim možete odrediti da se certifikat u toj memoriji može koristiti kao defaultni certifikat.

5. U navigacijskom okviru izaberite **Rad sa certifikatima** da se prikaže stranica koja vam dopušta obavljanje nekoliko zadataka upravljanja certifikatima.
6. Sa popisa certifikata izaberite certifikat, koji želite koristiti kao defaultni certifikat za trenutnu memoriju i kliknite **Postavi default** .

Sada kada ste kreirali i konfigurirali drugu sistemsku memoriju certifikata, svaka aplikacija koja koristi SSL_Init API može upotrijebiti certifikat u njoj za postavljanje SSL sesije.

***SYSTEM memorija certifikata postoji — importiranje datoteka u postojeću *SYSTEM memoriju certifikata**

Prije nego možete importirati certifikate u *SYSTEM na V4R5 ili V4R4 ciljni sistem, prvo morate eksportirati certifikate iz memorije certifikata koju ste kreirali u drugi format datoteke. Zatim možete importirati certifikate u memoriju *SYSTEM certifikata od novih datoteka. Prenesene datoteke memorije certifikata sadrže dva certifikata: certifikate poslužitelja ili klijenta koje ste kreirali i privatni Lokalni CA certifikat koji ste koristili za potpisivanje. Morate importirati oboje, poslužiteljski i klijentski certifikat, koje ste kreirali, i certifikat privatnog CA u memoriju *SYSTEM certifikata.

Bilješka: Funkcije eksporta dostupne u DCM za V4R5 i V4R4 nisu jednako dobro razvijene kao one za V5R2 i možete naići na probleme ako koristite ciljni sistem za eksportiranje privatnog lokalnog CA certifikata. Kao posljedicu, trebate koristiti V5R2 host sistem za eksport *dodatne* kopije Lokalnog CA certifikata u odvojenu datoteku radije nego korištenje V4R4 ili V4R5 ciljnog sistema za eksport. Nakon što eksportirate Lokalni CA certifikat na V5R2 host sistem, možete ručno prenijeti datoteku eksporta Lokalnog CA certifikata na V4R4 ili V4R5 ciljni sistem i slijedite dalje zadane korake u ovoj proceduri za importiranje Lokalnog CA certifikata u *SYSTEM memoriju certifikata. Morate importirati certifikat lokalnog CA *prije* nego importirate privatni certifikat, kojeg ste sa njim kreirali. Ako importirate prvo privatni certifikat, možete naići na grešku jer Lokalni CA certifikat ne postoji u memoriji certifikata.

Da eksportirate certifikat od datoteka memorije certifikata, dovršite ove korake na V4R4 ili V4R5 ciljnom sistemu:

1. Pokrenite DCM.
2. U navigacijskom okviru, osigurajte da je OTHER prikazano kao memorija certifikata u padajućoj kućici s popisom i izaberite **Certifikati sistema** za prikazivanje liste dostupnih zadataka. **Memorija certifikata i lozinka** prozorski prikazi.
3. Specificirajte puno kvalificirano ime staze i datoteke prenesenih datoteka memorije certifikata, pribavite lozinku koju ste koristili kada ste ih kreirali na *host* sistemu i kliknite **OK**. Sada možete promijeniti lozinku za memoriju certifikata.
4. U navigacijskom okviru izaberite **Promijeni lozinku** sa popisa sistemskih zadataka certifikata. Popunite obrazac da promijenite lozinku za memoriju certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za memoriju certifikata. Korištenjem ove opcije osigurava se da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novoj memoriji. Ako ne promijenite lozinku i izaberete opciju Automatska prijava, možete naići na pogreške kod eksportiranja certifikata iz ove memorije.

   Nakon što ste promijenili lozinku, morate ponovo otvoriti memoriju certifikata prije nego što možete u njoj raditi sa certifikatima.

5. U navigacijskom okviru izaberite **Rad sa certifikatima** da se prikaže popis certifikata.
6. Izaberite privatni certifikat sa popisa i kliknite **Eksportiraj** da se prikaže stranica za eksportiranje certifikata.
7. Dovršite obrazac Eksport certifikata.

   Bilješka: Provjerite da li ste dali datoteci jedinstveno ime i ekstenziju. Na primjer, mogli ste datoteku imenovati myfile.exp. Kad imenujete datoteku, nemojte za datoteku upotrijebiti nijednu od ovih ekstenzija:.TXT, .KDB, .RDB, ili .KYR jer korištenje jedne od tih ekstenzija može uzrokovati grešku kada importirate certifikate iz datoteke. Izaberite prikladnu razinu izdanja za ciljni sistem koji će koristiti taj certifikat. Razina izdanja koju izaberete utječe na format eksportiranog certifikata.
8. Kliknite **OK**. Na vrhu stranice će se prikazati poruka da je DCM eksportirao certifikat u datoteku, koju ste naveli.

U ovom trenutku, trebali ste koristiti DCM na originalnom V5R2 host sistemu za eksportiranje dodatne kopije Lokalnog CA certifikata i ručno prenijeti na V4R4 ili V5R5 ciljni sistem. Trebali ste također koristiti DCM na ovom ciljnom sistemu za eksportiranje privatnog certifikata poslužitelja ili klijenta u datoteku. Sada ste spremni za import ovih certifikata u memoriju *SYSTEM certifikata. Morate importirati certifikat lokalnog CA *prije* nego importirate privatni certifikat, kojeg ste sa njim kreirali. Ako importirate prvo privatni certifikat, možete naići na grešku jer Lokalni CA certifikat ne postoji u memoriji certifikata.

Da eksportirate certifikate od tih eksportnih datoteka i odredite da ih SSL omogućene aplikacije koriste, dovršite ove korake na V4R4 ili V4R5 ciljnom sistemu:

1. Pokrenite DCM.
2. U navigacijskom okviru, osigurajte da je *SYSTEM prikazano kao memorija certifikata u padajućoj kućici s popisom i izaberite **Certifikati sistema** za prikazivanje liste dostupnih zadataka. **Memorija certifikata i lozinka** prozorski prikazi.
3. Odredite *SYSTEM kao memoriju certifikata za otvaranje, unesite lozinku i kliknite **Nastavi**.
4. Sada morate importirati Lokalni CA certifikat iz datoteke eksporta koju ste kreirali na V5R2 host sistemu. U navigacijskom okviru izaberite **Primi CA certifikat** da se prikaže obrazac.
5. Dovršite obrazac i kliknite **OK** za prikaz stranice Uspješni prijem certifikata. Kad radite u memoriji *SYSTEM certifikata, ova stranica prikazuje popis aplikacija koje možete postaviti tako da imaju povjerenja u importirani CA certifikat.

   Bilješka: Neke SSL omogućene aplikacije podržavaju provjeru autentičnosti klijenta osnovanu na certifikatima. Koristeći certifikate za provjeru autentičnosti klijenta osigurava se da aplikacija primi važeći certifikat prije nego što se dopusti pristup resursima koje aplikacija kontrolira. Aplikacija sa tom podrškom mora biti postavljena tako da ima povjerenje u CA prije nego što se aplikacija osposobi za provjeru autentičnosti certifikata, koje izdaje određeni CA. Time se osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA-ova, koje ste naveli kao pouzdane. Ako korisnici ili klijentova aplikacija predoči certifikat od CA, koji nije naveden kao pouzdan, ta aplikacija ga neće prihvatiti kao temelj za važeću provjeru autentičnosti.
6. Izaberite aplikacije koje trebaju imati povjerenje u CA certifikat i kliknite **OK**. Prikaže se stranica Status zaštićenih aplikacija na kojoj potvrđujete da su izabrane aplikacije određene da vjeruju novoj potvrdi.
7. Sada možete importirati certifikat poslužitelja. U navigacijskom okviru izaberite **Rad sa certifikatima** da se prikaže popis certifikata.
8. Kliknite **Importiraj** da se prikaže stranica za import certifikata.
9. Dovršite obrazac Import certifikata i kliknite **OK** za povratak na stranicu Radi sa certifikatima. Osigurajte da ste dobavili ime datoteke koja sadrži eksportirani certifikat

poslužitelja ili klijenta i da ste specificirali ciljno izdanje koje se podudara sa onima koje ste specificirali kod prethodnog eksportiranja certifikata. Na vrhu stranice će se prikazati poruka da je DCM dodao certifikat u trenutnu memoriju certifikata. Potvrda koju ste importirali bi se trebala pojaviti i na listi potvrda.

10. Sada morate odrediti koje aplikacije trebaju koristiti importirane privatne certifikate za SSL. U navigacijskom okviru, odaberite **Rad sa sigurnim aplikacijama** za prikaz stranice koja vam dopušta upravljanje certifikatima pridružene specifičnim aplikacijama.
11. Izaberite neku aplikaciju sa popisa i kliknite **Rad sa sistemskim certifikatima** za prikaz popisa certifikata koje možete specificirati da odabrana aplikacija koristi za uspostavljanje SSL sesija.
12. Izaberite certifikat sa popisa i kliknite **Dodijeli novi certifikat** da dodijelite izabrani certifikat navedenoj aplikaciji. Na vrhu stranice se pojavi poruka potvrde za izbor certifikata.

Sa ovim dovršenim zadacima, aplikacije na V4R4 ili V4R5 ciljnom sistemu mogu koristiti certifikat koji je izdao Lokalni CA na drugom iSeries-u. Međutim, prije nego što počnete koristiti SSL za ove aplikacije, morate konfigurirati aplikacije za korištenje SSL-a.

Prije nego korisnik može pristupiti izabranim aplikacijama kroz SSL vezu, korisnik mora koristiti DCM da dobije kopiju Lokalnog CA certifikata od host sistema. CA potvrda se mora kopirati u datoteku na korisnikovom PC računalu ili učitati u korisnikov pretražitelj, ovisno o zahtjevima aplikacije koja radi sa SSL.

Upravljanje aplikacijama u DCM-u

Možete koristiti Upravitelja digitalnih certifikata (DCM) za izvođenje raznih zadataka upravljanja za SSL omogućene aplikacije i aplikacije za potpisivanje objekata. Na primjer, možete nadgledati koje certifikate koriste vaše aplikacije za komunikacijske sesije Sloja sigurnih utičnica (SSL). Zadaci upravljanja aplikacijom koje možete obaviti se mijenjaju ovisno o tipu aplikacije i memorije certifikata u kojoj radite. Možete upravljati aplikacijama samo od memorije *SYSTEM ili *OBJECTSIGNING certifikata.

Dok se većina zadataka upravljanja aplikacijama koje DCM pribavlja mogu lako razumjeti, neki od ovih zadataka možda vam neće biti poznati. Za više informacija o ovim zadacima, pogledajte ova poglavlja:

Kreiranje definicije aplikacije opisuje tipove aplikacija koje možete definirati i s kojima možete raditi.

Upravljanje dodjelama certifikata opisuje kako dodijeliti ili promijeniti certifikat koji aplikacija koristi za uspostavljanje SSL sesije ili za potpisivanje objekata.

Definiranje CA popisa povjerenja opisuje kada možete i trebate definirati kojim Izdavačima certifikata aplikacija može vjerovati za provjeru valjanosti i prihvaćanje certifikata.

Možete naći informacije o drugim DCM zadacima u online pomoći.

Kreiranje definicije aplikacije

Postoje dva tipa definicija aplikacija sa kojima možete raditi u DCM-u: definicije aplikacija za aplikacije poslužitelja ili klijenata koji koriste SSL i definicije aplikacija koje koristite za potpisivanje objekata.

Da koristite DCM za rad sa definicijama SSL aplikacija i njihovim certifikatima, aplikacija mora prvo biti registrirana sa DCM-om kao definicija aplikacije tako da ima jedinstveni ID aplikacije. Razvijači aplikacija registriraju SSL omogućene aplikacije koristeći API (QSYRGAP, QsyRegisterAppForCertUse) za automatsko kreiranje ID aplikacije u DCM-u.

Sve IBM iSeries SSL-omogućene aplikacije su registrirane sa DCM-om tako da možete jednostavno koristiti DCM za dodjeljivanje certifikata tako da mogu uspostaviti SSL sesiju. Također možete odrediti definiciju aplikacije i za nju kreirati ID aplikacije unutar samog DCM-a za aplikacije koje pišete ili kupujete. Morate raditi u memoriji *SYSTEM certifikata za kreiranje definicije SSL aplikacije za bilo aplikaciju klijenta ili aplikaciju poslužitelja.

Da koristite certifikat za potpisivanje objekata morate prvo definirati aplikaciju koju će koristiti certifikat. Za razliku od definicije SSL aplikacije, aplikacija za potpisivanje objekta ne opisuje stvarnu aplikaciju. Umjesto toga definicija aplikacije koju kreirate treba opisati tip ili grupu objekata koje namjeravate potpisati. Morate raditi u memoriji *OBJECTSIGNING certifikata za kreiranje definicije aplikacije za potpisivanje objekta.

Da kreirate definiciju aplikacije, slijedite ove korake:
1. Pokrenite DCM.
2. Kliknite **Izaberi memoriju certifikata** i izaberite odgovarajuću memoriju certifikata. (To je bilo memorija *SYSTEM certifikata ili memorija *OBJECTSIGNING certifikata ovisno o tipu definicije aplikacije koju kreirate.)

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup on-line pomoći.
3. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za memoriju certifikata kad ste je kreirali i kliknite **Nastavi**.
4. U navigacijskom okviru izaberite **Upravljaj aplikacijama** za prikaz popisa zadataka.
5. Izaberite **Dodaj aplikaciju** sa popisa zadataka da se prikaže obrazac za definiranje aplikacije.

   Bilješka: Ako radite u *SYSTEM memoriji certifikata, DCM će vas tražiti da izaberete dodavanje definicije aplikacije poslužitelja ili definicije aplikacije klijenta.
6. Popunite obrazac i kliknite **Dodaj**. Informacije koje možete specificirati za definiciju aplikacije se mogu mijenjati ovisno o tipu aplikacije koju definirate. Ako definirate aplikaciju poslužitelja, možete također specificirati da li aplikacija može koristiti certifikate za provjeru autentičnosti klijenta i treba zahtijevati provjeru autentičnosti klijenta. Možete također specificirati da aplikacija može koristiti popis pouzdanih CA za provjeru autentičnosti certifikata.

Upravljanje dodjelom certifikata za aplikaciju

Morate koristiti Upravitelja digitalnih certifikata (DCM) za dodjelu certifikata aplikaciji prije nego što aplikacija izvede sigurnu funkciju kao što je postavljanje sesije Sloja sigurnih utičnica (SSL) ili potpisivanje objekta. Da dodijelite certifikat aplikaciji ili da promijenite dodjelu certifikata aplikaciji, slijedite ove korake:
1. Pokrenite DCM.
2. Kliknite **Izaberi memoriju certifikata** i izaberite odgovarajuću memoriju certifikata. (To je bilo memorija *SYSTEM certifikata ili memorija *OBJECTSIGNING certifikata ovisno o tipu aplikacije kojoj dodjeljujete certifikat.)

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup on-line pomoći.
3. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za memoriju certifikata kad ste je kreirali i kliknite **Nastavi**.
4. U navigacijskom okviru izaberite **Upravljaj aplikacijama** za prikaz popisa zadataka.
5. Ako ste su *SYSTEM memoriji certifikata, izaberite tip aplikacije za upravljanje. (Izaberite ili **Poslužitelj** ili **Klijent** aplikaciju, kako je prikladno.)
6. Sa popisa zadataka izaberite **Ažuriraj dodjelu certifikata** za prikaz popisa aplikacija kojima možete dodijelili certifikat.

7. Izaberite neku aplikaciju sa popisa i kliknite **Ažuriraj dodjelu certifikata** za prikaz popisa certifikata koje možete dodijeliti aplikaciji.
8. Izaberite certifikat sa popisa i kliknite **Dodijeli novi certifikat**. DCM prikazuje poruku da potvrđuje vaš izbor certifikata za tu aplikaciju.

   Bilješka: Ako dodjeljujete certifikat SSL omogućenoj aplikaciji koja podržava korištenje certifikata za provjeru autentičnosti klijenta, morate definirati popis pouzdanih CA za aplikaciju. Time se osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA-ova koje ste naveli kao pouzdane. Ako korisnici ili klijentova aplikacija predoči certifikat od CA koji nije naveden kao pouzdan na popisu pouzdanih CA-ova, ta aplikacija ga neće prihvatiti kao temelj za važeću provjeru autentičnosti.

Kad mijenjate ili uklanjate certifikat za neku aplikaciju, aplikacija može ali ne mora prepoznati promjenu ako se aplikacija izvodi u vrijeme kad mijenjate dodjelu certifikata. Na primjer, Client Access Express poslužitelji će automatski primijeniti svaku promjenu certifikata koju napravite. Ipak, možete trebati zaustaviti i pokrenuti Telnet poslužitelje, IBM HTTP poslužitelj za iSeries ili druge aplikacije prije nego ove aplikacije mogu primijeniti promjene certifikata.

Počevši sa V5R2, možete koristiti zadatak Dodijeli certifikat kada želite dodijeliti certifikat za nekoliko aplikacija odjednom.

Definiranje CA popisa povjerenja za aplikaciju

Aplikacije koje podržavaju korištenje certifikata za provjeru autentičnosti klijenta tijekom sesije Sloja sigurnih utičnica (SSL) moraju odrediti da li prihvaćaju certifikat kao važeći dokaz identiteta. Jedan od kriterija kojeg aplikacija koristi za provjeru autentičnosti certifikata je da li aplikacija ima povjerenja u Izdavača certifikata (CA) koji je izdao certifikat.

Možete koristiti Upravitelja digitalnih certifikata (DCM) za definiranje za koje CA neka aplikacija može imati povjerenje kad izvodi provjeru autentičnosti klijenta za certifikate. Provjeravate one CA-ove, u koje aplikacija ima povjerenja, putem popisa pouzdanih CA-ova.

Prije nego što možete definirati popis pouzdanih CA, moraju se ispuniti nekoliko uvjeta:
- Aplikacija mora podržavati korištenje certifikata za provjeru autentičnosti klijenta.
- Definicija za aplikaciju mora navesti da aplikacija koristi popis pouzdanih CA.

Ako definicija za aplikaciju navede da aplikacija koristi popis pouzdanih CA morate definirati taj popis prije da aplikacija može uspješno izvesti provjeru autentičnosti klijenta certifikata. Time se osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA-ova koje ste naveli kao pouzdane. Ako korisnici ili klijentova aplikacija predoči certifikat od CA, koji nije naveden kao pouzdan na popisu pouzdanih CA-ova, ta aplikacija ga neće prihvatiti kao temelj za važeću provjeru autentičnosti.

Kad dodate CA popisu pouzdanih CA-ova, morate isto tako biti sigurni da je CA omogućen.

Da definirate popis pouzdanih CA-ova za neku aplikaciju, slijedite ove korake:
1. Pokrenite DCM.
2. Kliknite **Izaberi memoriju certifikata** i izaberi *SYSTEM da se otvori memorija certifikata.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup on-line pomoći.
3. Kad se prikaže stranica Memorija certifikata i lozinki, pribavite lozinku koju ste specificirali za memoriju certifikata kad ste je kreirali i kliknite **Nastavi**.

4. U navigacijskom okviru izaberite **Upravljaj aplikacijama** za prikaz popisa zadataka.
5. Sa popisa zadataka izaberite **Definiraj popis pouzdanih CA-ova**.
6. Izaberite tip aplikacije (poslužitelj ili klijent) za koju želite definirati popis i kliknite **Nastavi**.
7. Izaberite neku aplikaciju sa popisa i kliknite **Nastavi** za prikaz popisa CA certifikata koje koristite za definiranje pouzdanog popisa.
8. Izaberite CA-ove koje aplikacija smatra pouzdanim i kliknite**OK**. DCM prikazuje poruku da potvrđuje vaše izbore pouzdanih popisa.

Bilješka: Možete bilo izabrati pojedinačne CA-ove sa popisa ili možete navesti da aplikacija treba imati pouzdanja u sve ili nijedan CA u popisu. Također možete pogledati ili provjeriti valjanost CA certifikata prije nego ga dodate na pouzdani popis.

Provjera valjanosti certifikata i aplikacija

Možete koristiti Upravitelja digitalnih certifikata (DCM) za provjeru valjanosti pojedinačnih certifikata ili aplikacija koje ih koriste. Popis stvari koje DCM provjerava razlikuje se malo, ovisno o tome da li provjeravate valjanost certifikata ili aplikacije.

Provjera valjanosti aplikacije

Korištenje DCM-a za provjeru valjanosti definicije aplikacije pomaže u sprječavanju problema certifikata za aplikacije, kad ona izvodi funkciju koja zahtjeva certifikate. Takvi problemi mogu spriječiti aplikaciju bilo da uspješno sudjeluje u sesiji Sloja sigurnih utičnica (SSL) ili da uspješno potpisuje objekte.

Kad provjeravate valjanost aplikacije, DCM provjerava da li postoji dodjela certifikata za aplikaciju i jamči da je dodijeljeni certifikat važeći. Osim toga, DCM jamči da, ako je aplikacija konfigurirana za korištenje popisa pouzdanih Izdavača certifikata (CA), pouzdana lista sadrži najmanje jedan CA certifikat. DCM zatim provjerava da li su CA certifikati u aplikacijskom popisu pouzdanih CA važeći. Također ako definicija aplikacije navede da se obrada popisa opozvanih certifikata (CRL) vrši i da postoji definirana CRL lokacija za CA, DCM provjerava CRL kao dio postupka provjere valjanosti.

Provjera valjanosti certifikata

Kad provjeravate valjanost certifikata, DCM provjerava broj stavki koje pripadaju certifikatu da se osigura autentičnost i valjanost certifikata. Provjera valjanosti certifikata jamči da je malo vjerojatno da aplikacije, koje koriste certifikat za sigurne komunikacije ili za potpisivanje objekata, naiđu na probleme kad koriste certifikat.

Kao dio postupka za provjeru valjanosti, DCM provjerava da izabrani certifikat nije istekao. DCM također provjerava da certifikat nije na popisu opozvanih certifikata (CRL) kao opozvan, ako postoji CRL lokacija za CA koji je izdao certifikat. Osim toga, DCM provjerava da li je CA certifikat za izdavajući CA u trenutnoj memoriji certifikata i da li je CA certifikat omogućen i prema tome pouzdan. Ako certifikat ima privatni ključ (na primjer poslužiteljski, klijentski i certifikati za potpisivanje objekata), tada DCM također provjerava valjanost javno privatnog para ključeva da jamči da je javno privatni par ključeva usklađen. Drugim riječima, DCM šifrira podatke sa javnim ključem i tada jamči da se podaci mogu dešifrirati sa privatnim ključem.

Dodjela certifikata aplikacijama

Počevši sa V5R2, nove poboljšanja Upravitelja digitalnih certifikata (DCM) vam omogućavanju dodjeljivanje certifikata brzo i jednostavno za više aplikacija. Možete dodijeliti certifikat za više aplikacija u *SYSTEM ili *OBJECTSIGNING memoriji certifikata.

Da napravite dodjeljivanje certifikata za jednu ili više aplikacija, slijedite ove korake:
1. Pokrenite DCM.

   Bilješka: Ako imate pitanja o tome kako popuniti specifičan obrazac koristeći DCM, odaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
2. U navigacijskom okviru kliknite**Izaberi memoriju certifikata** i odaberite ili ***OBJECTSIGNING** ili ***SYSTEM** da se otvori memorija certifikata.
3. Unesite lozinku za memoriju certifikata i kliknite **Nastavi**.
4. Nakon osvježenja navigacijskog okvira izaberite **Upravljaj certifikatima** za prikaz popisa zadataka.
5. Sa popisa zadataka izaberite **Pridruži certifikat** da prikažete listu certifikata za trenutnu memoriju certifikata.
6. Izaberite certifikat sa popisa i kliknite **Dodijeli aplikacijama** da prikažete listu definicija aplikacija za trenutnu memoriju certifikata.
7. Izaberite jednu ili više aplikacija sa popisa i kliknite **Nastavi**. Prikazuje se stranica sa ili porukom potvrde za vaš izbor dodjela ili poruka o grešci ako se dogodio problem.

Upravljanje CRL lokacijama

Upravitelj digitalnih certifikata (DCM) vam omogućava da definirate informaciju o lokaciji Popisa uskraćivanja certifikata (CRL) za korištenje određenom Izdavaču certifikata (CA) kao dio procesa provjere valjanosti certifikata. DCM ili aplikacija koja zahtjeva CRL obradu, može koristiti CRL da odredi da CA, koji je izdao određeni certifikat, nije opozvao certifikat. Kada definirate CRL lokaciju za određeni CA, aplikacije koje podržavaju korištenje certifikata za provjeru autentičnosti mogu pristupiti CRL-u.

Aplikacije koje podržavaju korištenje certifikata za provjeru autentičnosti klijenta mogu izvoditi CRL obradu da osiguraju bolju provjeru autentičnosti za certifikate koje primaju kao važeći dokaz identiteta. Prije nego aplikacija može upotrijebiti CRL, kao dio postupka validacije certifikata, DCM aplikacijska definicija mora zahtijevati da aplikacija izvrši CRL obradu.

Kako radi CRL obrada

Kad koristite DCM za validaciju certifikata ili aplikacije, DCM izvodi CRL obradu po defaultu kao dio validacijskog postupka. Ako ne postoji CRL lokacija definirana za CA, koji izdaje certifikat kojem provjeravate valjanost, DCM ne može izvesti provjeravanje CRL-a. Ipak, DCM može pokušati provjeriti valjanost drugih važnih informacija o certifikatu, kao da je CA potpis na specifičnom certifikatu važeći i da je CA koji ga je izdao pouzdan.

Definiranje CRL lokacije

Da definirate CRL lokaciju za određeni CA, slijedite ove korake:
1. Pokrenite DCM.
2. U navigacijskom okviru izaberite **Upravljaj lokacijama** za prikaz popisa zadataka.
3. Izaberite **Dodaj CRL lokaciju** sa popisa zadataka da se prikaže obrazac kojeg možete upotrijebiti za opis CRL lokacije i kako treba DCM ili aplikacija pristupiti lokaciji.
4. Dovršite obrazac i kliknite **OK**. Morate dati CRL lokaciji jedinstveno ime, identificirati LDAP poslužitelj koji poslužuje CRL i pružiti informacije o vezi koje opisuju kako pristupiti LDAP poslužitelju.

Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku, izaberite upitnik **?**) na vrhu stranice za pristup online pomoći.

Sada trebate pridružiti CRL definiciju lokacije specifičnom CA.

5. U navigacijskom okviru izaberite **Upravljaj certifikata** za prikaz popisa zadataka.
6. Izaberite **Promijeni CRL dodjelu alokacije** sa liste zadataka da prikažete listu CA certifikata.
7. Izaberite CA certifikat iz liste kojoj želite dodijeliti CRL definiciju lokacije koju ste kreirali i kliknite **Promijeni CRL dodjelu lokacije**. Prikazuje se lista CRL lokacija.
8. Izaberite CRL lokaciju sa popisa koji želite pridružiti CA-u i kliknite **Promijeni dodjelu**. Prikazuje se poruka na vrhu stranice koja pokazuje da je CRL lokacija dodijeljena certifikatu Izdavača certifikata (CA).

Kad imate definiranu lokaciju za CRL za specifični CA, DCM ili druge aplikacije je mogu koristiti tijekom izvođenja CRL obrade. Međutim, prije nego se CRL obrada može izvoditi, Usluge Direktorija moraju sadržavati prikladni CRL. Morate i konfigurirati oboje, poslužitelja Usluga Direktorija i klijentske aplikacije za korištenje SSL-a i dodijeliti certifikat aplikacijama u DCM-u.

Da naučite više o konfiguriranju i korištenju iSeries poslužitelja Usluga Direktorija (LDAP), pregledajte ova poglavlja Informacijskog Centar:

- Usluge Direktorija (LDAP)
  Ovo poglavlje vam kaže sve što trebate znati o konfiguriranju i korištenju iSeries poslužitelj Usluge Direktorija (LDAP).
- Korištenje sigurnosti Sloja sigurnih utičnica (SSL) sa LDAP direktorijskim poslužiteljem
  Ovo poglavlje objašnjava što trebate učiniti da konfigurirate vašeg LDAP poslužitelja za upotrebu SSL sigurnih komunikacija.

Pohranite ključeve certifikata na IBM 4758 kriptografičkom koprocesoru

Ako ste instalirali IBM 4758–023 PCI kriptografički koprocesor na vaš iSeries, možete koristiti koprocesor za pružanje sigurnije memorije za privatne ključeve certifikata. Koprocesor možete koristiti za pohranjivanje privatnog ključa za poslužiteljski certifikat, klijentski certifikat ili certifikat lokalnog izdavača certifikata (CA). Međutim, ne možete koristiti koprocesor za pohranjivanje privatnog ključa certifikata jer taj ključ mora biti pohranjen na korisnikovom sistemu. Osim toga, u ovom trenutku ne možete koristiti koprocesor za pohranjivanje privatnog ključa za certifikat za potpisivanje objekta.

Koprocesor možete koristiti za pohranjivanje privatnog ključa certifikata, na jedan od dva načina:

- Pohranjivanje privatnog ključa certifikata neposredno u koprocesoru.
- Korištenje glavnog ključa koprocesora za šifriranje privatnog ključa za pohranjivanje u posebnu datoteku ključa.

Možete izabrati ovu opciju pohranjivanja ključa kao dijela postupka kreiranja ili produljenja certifikata. Ako koristite koprocesor za pohranjivanje certifikatovog privatnog ključa, možete promijeniti dodjelu koprocesora za taj ključ.

Da koristite koprocesor za pohranjivanje privatnog ključa, morate se pobrinuti da je koprocesor varied on prije upotrebe Upravitelja digitalnih certifikata (DCM). Inače DCM neće pribaviti stranicu za izbor opcije memorije kao dijela kreiranja certifikata ili postupka produljenja.

Ako kreirate ili produljujete poslužiteljev ili klijentov certifikat, izaberite opciju memorije privatnog ključa nakon izbora tipa CA koji potpisuje trenutni certifikat. Ako kreirate ili produljujete lokalni CA, kao prvi korak u tom postupku izaberite opciju memorije privatnog ključa.

Pohranjivanje privatnog ključa certifikata neposredno u koprocesoru

Da bolje zaštitite pristup i upotrebu privatnog ključa certifikata, možete izabrati da pohranite ključ direktno na IBM 4758–023 PCI kriptografički koprocesor. Možete izabrati ovu opciju pohranjivanja ključa kao dijela kreiranja ili produljenja certifikata u Upravitelju digitalnih certifikata (DCM).

Slijedite ove korake sa stranice **Izaberi lokaciju memorije ključa** da pohranite certifikatov privatni ključ neposredno na koprocesor:

1. Izaberite **Hardver** kao vašu opciju memorije.
2. Kliknite **Nastavi**. Ovim se pokazuje stranica **Izaberi opis kriptografičkog uređaja**.
3. Izaberite sa popisa uređaja onaj, kojeg želite upotrijebiti za pohranjivanje certifikatovog privatnog ključa.
4. Kliknite **Nastavi**. DCM nastavlja prikazivati stranice za zadatke koje dovršavate, kao što su identifikacijske informacije za certifikat, kojeg kreirate ili produljujete.

Korištenje glavnog ključa koprocesora za šifriranje privatnog ključa

Da bolje zaštitite pristup i upotrebu privatnog ključa certifikata, možete koristiti glavni ključ IBM 4758–023 PCI kriptografičkog koprocesora za šifriranje privatnog ključa i spremanja ključa u posebnu datoteku ključeva. Možete izabrati ovu opciju pohranjivanja ključa kao dijela kreiranja ili produljenja certifikata u Upravitelju digitalnih certifikata (DCM).

Prije nego uspješno možete koristiti ovu opciju, morate koristiti konfiguracijsko web sučelje IBM 4758–023 PCI kriptografičkog koprocesora za kreiranje odgovarajuće datoteke memorije ključa. Morate upotrijebiti i web sučelje za koprocesorsku konfiguraciju da pridružite datoteku memorije ključa opisu koprocesorskog uređaja kojeg želite koristiti. Možete pristupiti web sučelju konfiguracije koprocesora sa iSeries stranice zadataka.

Ako vaš sistem ima instalirano više od jednog koprocesorskog uređaja i varied on, možete dijeliti certifikatove privatne ključeve među više uređaja. Da bi opisi uređaja dijelili privatni ključ, svi uređaji moraju imati isti glavni ključ. Postupak distribuiranja istog glavnog ključa među više uređaja se naziva *kloniranje*. Dijeljenjem ključa među uređajima omogućuje se ravnomjerno opterećenje Sloja sigurnih utičnica (SSL), što može poboljšati izvođenje sigurnih sesija.

Slijedite ove korake sa stranice **Izaberi lokaciju memorije ključa** da upotrijebite glavni ključ koprocesora za šifriranje certifikatovog privatnog ključa i njegovo pohranjivanje u posebnu datoteku memorije ključa:

1. Izaberite **Hardverski šifrirano** kao vašu memorijsku opciju.
2. Kliknite **Nastavi**. Ovim se pokazuje stranica **Izaberi opis kriptografičkog uređaja**.
3. Izaberite sa popisa uređaja onaj, kojeg želite upotrijebiti za šifriranje certifikatovog privatnog ključa.
4. Kliknite **Nastavi**. Ako imate instalirano više od jednog koprocesora i varied on, prikaže se stranica **Izaberi dodatne opise kriptografičkog uređaja** .

   Bilješka: Ako nemate više dostupnih koprocesorskih uređaja, DCM nastavlja prikazivati stranice za zadatke koje dovršavate, kao što su identifikacijske informacije za certifikat, kojeg kreirate ili produljujete.

5. Izaberite sa popisa uređaja ime jednog ili više opisa uređaja sa kojima želite dijeliti certifikatov privatni ključ.

   Bilješka: Opisi uređaja koje izaberete moraju imati isti glavni ključ kao uređaj kojeg ste izabrali na prethodnoj stranici. Da provjerite da je na svim uređajima glavni ključ isti, upotrijebite zadatak Provjera glavnog ključa u web sučelju konfiguracije 4758 kriptografičkog koprocesora. Možete pristupiti web sučelju konfiguracije koprocesora sa iSeries stranice zadataka.
6. Kliknite **Nastavi**. DCM nastavlja prikazivati stranice za zadatke koje dovršavate, kao što su identifikacijske informacije za certifikat, kojeg kreirate ili produljujete.

Upravljanje lokacijom zahtjeva za PKIX CA

Izdavač certifikata (CA) Infrastrukture javnog ključa za X.509 (PKIX) je CA koji izdaje certifikate na osnovi najnovijih Internet x.509 standarda za implementiranje infrastrukture javnog ključa. PKIX standardi su navedeni u Request For Comments (RFC) 2560.

PKIX CA zahtjeva strožu identifikaciju prije izdavanja certifikata; obično tražeći da prijavljeni pruži dokaz o identitetu preko Izdavača registracije (RA). Nakon što molitelj dobavi dokaz o identitetu kojeg zahtjeva RA, RA potvrđuje moliteljev identitet. Ili RA ili onaj koji se prijavljuje, ovisno o uspostavljenoj proceduri CA, šalje potvrđenu aplikaciju pridruženom CA. Kako su ovi standardi sve šire prihvaćeni, PKIX podržani CA će postati sve dostupniji. Trebate istražiti, koristeći CA usklađen sa PKIX, da li vaše sigurnosne potrebe zahtijevaju striktnu kontrolu pristupa resursima, koju vaše SSL omogućene aplikacije pružaju korisnicima. Na primjer, Lotus Domino pruža PKIX CA za javnu upotrebu.

Ako želite imati certifikate izdane od PKIX CA za vaše aplikacije, možete koristiti Upravitelja digitalnih certifikata (DCM) za upravljanje tim Internet certifikatima. Koristite DCM za konfiguriranje URL-a za PKIX CA. Tako se konfigurira Upravitelja digitalnih certifikata (DCM) da se pribavi PKIX CA kao opcija za dobivanje potpisanih certifikata.

Da koristite DCM za upravljanje certifikatima od PKIX CA, morate prvo konfigurirati DCM za korištenje lokacije za CA slijedeći ove korake:
1. Pokrenite DCM.
2. U navigacijskom okviru izaberite **Upravljaj lokacijom PKIX zahtjeva** za prikaz obrasca koji vam omogućuje da odredite URL za PKIX CA ili njegov pridruženi RA.
3. Unesite potpuno kvalificirani URL za PKIX CA kojeg želite upotrijebiti za zahtjev certifikata; na primjer:http://www.thawte.com i kliknite **Dodaj**. Dodavanjem URL-a konfigurira se DCM za dodavanje PKIX CA kao opcije za dobivanje potpisanih certifikata.

Nakon što dodate PKIX CA lokaciju zahtjeva, DCM dodaje PKIX CA kao opciju za određivanje tipa CA koji ste izabrali za izdavanje certifikata od korištenja zadatka **Kreiraj certifikat**.

Potpisivanje objekata

Tri su načina koje možete koristiti za potpisivanje objekata. Možete napisati program koji poziva Potpiši API objekta. Možete koristiti Upravitelj digitalnih certifikata (DCM) za potpisivanje objekata. Ili, počevši sa V5R2, možete koristiti iSeries Navigator svojstvo Središnjeg Upravljanja za potpisivanje objekata kako ih pakirate za distribuiranje na druge iSeries sisteme.

Možete koristiti certifikate kojima upravljate u DCM-u za potpisivanje svakog objekta kojeg pohranite u integrirani sistem datoteka sistema osim objekata koji su pohranjeni u knjižnici. Možete potpisati samo ove objekte koji su pohranjeni u QSYS.LIB sistemu datoteka: *PGM,

*SRVPGM, *MODULE, *SQLPKG i *FILE (samo spremanje datoteke). Novo u V5R2, možete također potpisivati objekte naredbi (*CMD). Ne možete potpisivati objekte koji su spremljeni na drugim iSeries poslužiteljima.

Možete potpisivati objekte sa certifikatima koje kupujete od javnog Internet Izdavača certifikata (CA) ili one koje kreirate sa privatnim, Lokalnim CA u DCM-u. Postupak potpisivanja certifikata je isti bez obzira da li koristite javne ili privatne certifikate.

Preduvjeti potpisivanja objekata

Prije nego što možete koristiti DCM (ili Sign Object API) za potpisivanje objekata morate biti sigurni da su ispunjeni određeni preduvjeti:

- Morate imati kreiranu *OBJECTSIGNING memoriju certifikata, ili kao dio procesa kreiranja Lokalnog CA ili kao dio procesa upravljanja certifikatima potpisivanja objekata od javnog Internet CA.
- *OBJECTSIGNING memorija certifikata mora sadržavati barem jedan certifikat, ili onaj koji ste kreirali korištenjem Lokalnog CA ili onaj koji ste dobili od javnog Internet CA.
- Morate imati kreiranu definiciju aplikacije za potpisivanje objekata za korištenje za potpisivanje objekata.
- Morate imati dodijeljen certifikat aplikaciji potpisivanja objekta koju namjeravate koristiti za potpisivanje objekata.

Korištenje DCM-a za potpisivanje objekata

Za korištenje DCM-a za potpisivanje jednog ili više objekata, slijedite ove korake:

1. Pokrenite DCM.

   Bilješka: Ako imate pitanja o tome kako popuniti specifičan obrazac koristeći DCM, odaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
2. U navigacijskom okviru kliknite **Izaberi memoriju certifikata** i odaberite ***OBJECTSIGNING** da se otvori memorija certifikata.
3. Unesite lozinku za memoriju *OBJECTSIGNING certifikata i kliknite **Nastavak**.
4. Nakon osvježenja navigacijskog okvira, odaberite **Upravljaj potpisivim objektima** za prikaz popisa zadataka.
5. Sa popisa zadataka odaberite **Potpiši objekt** za prikaz popisa definicija aplikacija koje možete koristiti za potpisivanje objekata.
6. Odaberite neku aplikaciju i kliknite **Potpiši objekt** da vidite obrazac za određivanje lokacije objekata koje želite potpisati.

   Bilješka: Ako aplikacija koju odabirete nema njoj dodijeljeni certifikat, ne možete je koristiti za potpisivanje objekta. Morate najprije upotrijebiti zadatak **Ažuriraj dodjelu certifikata** u **Upravljanje aplikacijama** za dodjelu certifikata definiciji aplikacije.
7. U dobiveno polje unesite potpuno kvalificiranu stazu i ime datoteke objekta ili direktorija objekata koje želite potpisati i kliknite **Nastavi**. Ili unesite lokaciju direktorija i kliknite **Pretraži** da vidite sadržaje direktorija i da odaberete objekte za potpisivanje.

   Bilješka: Morate pokrenuti ime objekta sa vodećom kosom crtom ili ćete dobiti grešku. Možete također koristiti određene generičke znakove za opis direktorija kojeg želite potpisati. Ovi generički znakovi su zvjezdica *****), koja specificira ″svaki broj znakova ″ i upitnik**?**), koji specificira ″svaki pojedinačni znak.″ Na primjer, za potpisivanje objekata u određenom direktoriju možete unijeti /mydirectory/*; za potpisivanje svih programa u određenoj knjižnici možete unijeti/QSYS.LIB/QGPL.LIB/*.PGM. Ove generičke znakove možete koristiti samo u zadnjem dijelu imena staze; na primjer, /mydirectory*/filename ima za posljedicu poruku greške. Ako želite koristiti funkciju pretražitelja da vidite

popis sadržaja knjižnica ili direktorija trebate unijeti generički znak kao dio imena staze prije nego što kliknete **Pretraži**.

8. Odaberite opcije obrada koje želite koristiti za potpisivanje odabranog objekta ili objekata i kliknite **Nastavi**.

   Bilješka: Ako odlučite čekati rezultate posla, prikazati će se datoteka rezultata neposredno u vašem pretražitelju. Rezultati trenutnog posla se pridodaju kraju datoteke rezultata. Prema tome, datoteka može sadržavati rezultate od svakog prethodnog posla osim onih od trenutnog posla. Možete koristiti polje podataka u datoteci za određivanje linija u datoteci koje se odnose na trenutni posao. Polje podataka je u YYYYMMDD formatu. Prvo polje u datoteci može biti bilo ID poruke (ako nastane greška tijekom obrade objekta) ili polje podataka (pokazujući podatke na kojima se obavlja posao).

9. Specifirajte potpuno kvalificiranu stazu i ime datoteke za korištenje u pohranjivanju rezultata posla za potpisivanje objekta i kliknite **Nastavi**. Ili unesite lokaciju direktorija i kliknite **Pretraži** da pogledate sadržaje direktorija te da odaberete datoteku za pohranjivanje rezultata posla. Prikazuje se poruka koja pokazuje da je posao poslan na izvođenje za potpis objekata. Da vidite rezultate posla, pogledajte posao **QOBJSGNBAT** u dnevniku posla.

Provjeravanje valjanosti potpisa objekata

Možete koristiti Upravitelja digitalnih certifikata (DCM) za provjeru autentičnosti digitalnih potpisa na objektima. Kad provjeravate potpis budite sigurni da podaci u objektu nisu promijenjeni od kad je vlasnik objekta potpisao objekt.

Preduvjeti provjere potpisa

Prije nego što koristite DCM za provjeru potpisa na objektima, morate biti sigurni da su ispunjeni određeni preduvjeti:

- Morate imati kreiranu memoriju za *SIGNATUREVERIFICATION certifikate za upravljanje vašim certifikatima za provjeru potpisa. .

  Bilješka: Možete provesti provjeru potpisa tijekom rada u memoriji za *OBJECTSIGNING certifikate za slučaj gdje provjeravate potpise za objekte koji su potpisani na istom sistemu. Koraci koje izvodite za provjeru potpisa u DCM-u su isti u obje memorije certifikata. Međutim, memorija za *SIGNATUREVERIFICATION certifikate mora postojati i mora sadržavati kopiju certifikata koji je potpisao objekt čak ako vršite provjeru potpisa tijekom rada unutar memorije za *OBJECTSIGNING certifikate.

- Memorija *SIGNATUREVERIFICATION certifikata mora sadržavati kopiju certifikata koji je potpisao objekte.
- Memorija *SIGNATUREVERIFICATION certifikata mora sadržavati kopiju certifikata CA koji je izdao certifikat koji je potpisao objekte.

Korištenje DCM-a za provjeravanje potpisa objekata

Da koristite DCM za provjeru potpisa objekata slijedite ove korake:

1. Pokrenite DCM.

   Bilješka: Ako imate pitanja o tome kako popuniti specifičan obrazac koristeći DCM, odaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.

2. U navigacijskom okviru kliknite **Odaberi memoriju certifikata** i odaberite ***SIGNATUREVERIFICATION** da se otvori memorija certifikata.

3. Unesite lozinku za memoriju *SIGNATUREVERIFICATION certifikata i kliknite **Nastavi**.
4. Nakon osvježenja navigacijskog okvira, odaberite **Upravljaj potpisivim objektima** za prikaz popisa zadataka.
5. Sa popisa zadataka odaberite **Provjeri potpis objekta** za specifikaciju lokacija objekata za koje želite provjeru potpisa.
6. U dobiveno polje unesite potpuno kvalificiranu stazu i ime datoteke objekta ili direktorija objekata za koje želite provjeriti potpise i kliknite**Nastavi**. Ili unesite lokaciju direktorija i kliknite **Pretraži** da vidite sadržaje direktorija i da odaberete objekte za provjeru potpisa.

   Bilješka: Možete također koristiti određene generičke znakove za opis direktorija kojeg želite provjeriti. Ovi generički znakovi su zvjezdica (*****), koja specificira ″svaki broj znakova,″ i upitnik **?**), koji specificira ″svaki pojedinačni znak.″ Na primjer, za potpisivanje svih objekata u određenom direktoriju možete unijeti /mydirectory/*; za potpisivanje svih programa u određenoj knjižnici možete unijeti/QSYS.LIB/QGPL.LIB/*.PGM. Ove generičke znakove možete koristiti samo u zadnjem dijelu imena staze; na primjer, /mydirectory*/filename rezultira u poruci greške. Ako želite koristiti funkciju pretražitelja da vidite popis sadržaja knjižnica ili direktorija trebate unijeti generički znak kao dio imena staze prije nego što kliknete **Pretraži**.
7. Odaberite opcije obrada koje želite koristiti za provjeru potpisa odabranog objekta ili objekata i kliknite **Nastavi**.

   Bilješka: Ako odlučite čekati rezultate posla, prikazati će se datoteka rezultata neposredno u vašem pretražitelju. Rezultati trenutnog posla se pridodaju kraju datoteke rezultata. Prema tome, datoteka može sadržavati rezultate od svakog prethodnog posla osim onih od trenutnog posla. Možete koristiti polje podataka u datoteci za određivanje linija u datoteci koje se odnose na trenutni posao. Polje podataka je u YYYYMMDD formatu. Prvo polje u datoteci može biti bilo ID poruke (ako nastane greška tijekom obrade objekta) ili polje podataka (pokazujući podatke na kojima se obavlja posao).
8. Specifirajte potpuno kvalificiranu stazu i ime datoteke za korištenje u pohranjivanju rezultata posla za provjeru potpisa objekta i kliknite**Nastavi** . Ili unesite lokaciju direktorija i kliknite **Pretraži** da pogledate sadržaje direktorija da odaberete datoteku za pohranjivanje rezultata posla. Prikazuje se poruka koja pokazuje da je posao poslan na izvođenje za provjeru potpisa objekata. Da vidite rezultate posla, pogledajte **QOBJSGNBAT** u dnevniku posla.

Možete također koristiti DCM i za pregled informacija o certifikatu koji je potpisao objekt. Time vam je dopušteno da prije nego što radite sa objektom, odredite da li je objekt od izvora kojemu vjerujete.

Poglavlje 9. Rješavanje pogrešaka u DCM

Možete koristiti ove stranice da nađete korisne informacije koje vam mogu pomoći u rješavanju češćih problema koje možete susresti za vrijeme rada sa Upraviteljem digitalnih certifikata (DCM).

Za informacije o problemima i mogućim rješenjima, pregledajte ove stranice:

Rješavanje problema lozinki i općenitih problema
Koristite ove informacije da se upoznate sa uobičajenim problemima DCM korisničkog sučelja, na koje možete naići i kako bi ih mogli ispraviti.

Rješavanje problema memorije certifikata i baze podataka
Koristite ove informacije da se upoznate sa uobičajenim problemima memorije certifikata i ključne baze podataka, na koje možete naići i kako bi ih mogli ispraviti.

Rješavanje problema pretražitelja
Koristite ove informacije da se upoznate sa uobičajenim problemima, na koje možete naići, kad koristite pretražitelja za pristup DCM-u, i kako bi ih mogli ispraviti.

Rješavanje problema HTTP poslužitelja za iSeries
Koristite ove informacije da se upoznate sa uobičajenim problemima HTTP poslužitelja, na koje možete naići i kako bi ih mogli ispraviti.

Migracijske greške i rješenja obnavljanjem
Koristite ove informacije da se upoznate sa uobičajenim problemima, na koje možete naići, kad migrirate DCM od ranijeg izdanja, i kako bi ih mogli ispraviti.

Ispravljanje pogrešaka kod dodjeljivanja korisničkog certifikata
Koristite ove informacije da se upoznate sa uobičajenim problemima, na koje možete naići, kad koristite DCM za registraciju korisničkog certifikata, i kako bi ih mogli ispraviti.

Rješavanje problema lozinki i općenitih problema

Koristite sljedeću tablicu da nađete informacije da vam pomognu u rješavanju češćih problema lozinke i ostalih koje možete susresti za vrijeme rada sa Upraviteljem digitalnih certifikata (DCM).

Problem	Moguće rješenje
Ne možete naći dodatnu pomoć za DCM.	U DCM-u, kliknite **?″** ikonu pomoći. Možete i pretraživati Informativni centar i vanjske lokacije na Internetu.
Primate NET.DATA grešku kad pokušate otvoriti memoriju certifikata.	Kada **Izaberete memoriju certifikata**, izaberite mišem gumb **Nastavi** radije nego tipku **Unos** na vašoj tipkovnici.
Vaša lozinka za lokalnog izdavača certifikata (CA) i memorije *SYSTEM certifikata ne radi.	Lozinke razlikuju mala i velika slova. Pazite da veličina slova bude ista kao i kad ste lozinku dodjeljivali.
Vaš pokušaj da ponovo postavite lozinku kada ste koristili zadatak Izaberi memoriju certifikata nije uspio.	Funkcija za ponovno postavljanje radi samo ako je DCM pohranio lozinku. DCM pohranjuje lozinku automatski kada kreirate memoriju certifikata. Ipak, ako promijenite (ili ponovo postavite) lozinku na memoriji certifikata drugog sistema, tada morate izabrati opciju **Automatska prijava** tako da DCM nastavlja skrivati lozinku.

Problem	Moguće rješenje
	Također, ako premjestite memoriju certifikata sa jednog sistema na drugi, morate promijeniti lozinku za memoriju certifikata na novom sistemu da osigurate da je DCM automatski skriva. Za promjenu lozinke, morate dobaviti originalnu lozinku za memoriju certifikata kada je otvorite na novom sistemu. Ne možete koristiti opciju ponovnog postavljanja lozinke dok niste otvorili memoriju sa originalnom lozinkom i promijenili lozinku da je sakrijete. Ako lozinka nije promijenjena i skrivena, DCM i SSL ne mogu automatski obnoviti lozinku kada je potrebna za razne funkcije. Ako mijenjate memoriju certifikata koju ćete koristiti kao Memoriju certifikata drugog sistema, morate izabrati opciju **Automatska prijava** kada mijenjate lozinku da osigurate da DCM skriva novu lozinku za ovaj tip memorije certifikata.
	Provjerite vrijednost dodijeljenu atributu ″Dozvoli nove digitalne certifikate″ pod opcijom Rad sa sistemskom sigurnosti u Alati sistemskih usluga (SST). Ako je ovaj atribut postavljen na vrijednost 2 (No), tada lozinka memorije certifikata ne može biti ponovo postavljena. Možete gledati ili mijenjati vrijednost ovog atributa korištenjem naredbe STRSST i unošenjem korisničkog ID-a i lozinke za Servisne alate. Tada izaberite opciju ″Rad sa sistemskom sigurnosti″. ID korisnika za Servisne alate je vjerojatno QSECOFR ID korisnika.
ne možete naći izvor za CA certifikat za primanje u vaš iSeries sistem.	Neki CA ne nude gotove CA certifikate. Ako ne možete dobiti CA certifikat od CA, obratite se svom VAR, jer je VAR možda sklopio neki posebni sporazum sa CA ili sporazum oko načina plaćanja.
Ne možete naći memoriju *SYSTEM certifikata.	Mjesto datoteke *SYSTEM certifikata mora biti /qibm/userdata/icss/cert/server/default.kdb. Ako ta memorija certifikata ne postoji, trebate upotrijebiti DCM i kreirati memoriju certifikata. Koristite zadatak **Kreiraj novu memoriju certifikata**.
Iz DCM-a ste primili grešku, a greška se pojavljuje i dalje, nakon što ste ju ispravili.	Obrišite predmemoriju vašeg pretražitelja. Postavite veličinu predmemorije na 0 te zaustavite i ponovo pokrenite pretražitelja.
S LDAP poslužiteljem imate probleme kao što je neprikazivanje pridruženja certifikata kad se prikaže informacija o zaštićenoj aplikaciji, odmah nakon pridruživanja potvrde. Ovaj se problem dešava češće kod korištenja iSeries Navigatora za dobivanje Netscape Communications pretražitelja. Vaše preference za predmemoriju pretražitelja s postavljaju da usporede dokument u predmemoriji dokumenta na mreži ″Jednom za sesiju″.″	Promijenite default postavku da svaki puta provjerava predmemoriranje.
Kada koristite DCM za importiranje certifikata koji je potpisan od vanjskog CA kao Entrust, možete primiti poruku o grešci da period valjanosti ne sadrži današnji dan ili ne pada u unutar period valjanosti svog izdavača.	Za razdoblje valjanosti sistem koristi generalizirani format vremena. Pričekajte jedan dan i pokušajte ponovo. Također, provjerite da vaš iSeries ima ispravnu vrijednost pomaka za UTC (dspsysval qutcoffset). Ako promatrate vrijeme uštede dnevne svjetlosti, možda je vrijednost krivo postavljena.
Primili ste grešku baze 64 kada ste pokušavali importirati Entrust certifikat.	Certifikat se izlista kao da je u nekom posebnom formatu kao što je PEM format. Ako funkcija za kopiranje na vašem pretražitelju ne radi dobro, možete kopirati posebni materijal, koji ne pripada certifikatu, kao znakove za prazna mjesta na početku svakog reda. Ako je to slučaj, tada certifikat neće biti ispravnog formata kada ga pokušate koristiti na iSeries. Neke web stranice izazivaju ovaj problem svojim oblikovanjem. Kod nekih stranica je oblikovanje izvedeno tako da je ovaj problem izbjegnut. Pobrinite se da usporedite izgled originalnog certifikata sa rezultatom preslikavanja, jer preslikana informacija treba imati isti izgled.

Problem	Moguće rješenje
Kada migrirate sa V4R3 verzije DCM-a na V5R2 verziju, migracija ne prilagođava sistemske certifikate koji su istekli.	Sistemski certifikat koji je prestao važiti je sad nevaljan i ne može dospjeti u *SYSTEM memoriju certifikata. Uklonite ili preimenujte stare datoteke prstenova ključeva od V4R3 prije migracije, zanemarite pokazivač neuspjeha migracije ili pokušajte ponovo sa migracijom.
Ne možete naći uzorak kodiranja za dodavanje certifikata u validacijske liste.	Uzorak kodiranja još nije dostupan.

Rješavanje problema memorije certifikata i baze podataka

Koristite sljedeću tablicu da nađete informacije da vam pomognu u rješavanju češćih problema memorije certifikata i baze podataka ključeva koje možete susresti za vrijeme rada sa Upraviteljem digitalnih certifikata (DCM).

Problem	Moguće rješenje
Sistem nije našao bazu ključeva ili je ustanovio da je nevaljana.	Provjerite lozinku i ime datoteke da nemaju tiskarskih grešaka. Pobrinite se da staza bude uključena u ime datoteke, uključujući i vodeću kosu crtu /.
Kreiranje baze ključeva nije uspjelo.	Provjerite je li ime u sukobu. Možda je sukob u nekoj drugoj datoteci a ne u onoj koju ste zatražili.
Sistem ne prihvaća CA tekst datoteku koja je prenesena u binarnom načinu sa drugog sistema. On prihvaća tu datoteku kad se prenosi u American National Standard Code for Information Interchange (ASCII kodu).	Prstenovi ključeva i ključne baze podataka su binarne i stoga različite. Morate upotrebiti Protokol za prijenos datoteka (FTP) u ASCII načinu za CA tekstualne datoteke a FTP u binarnom načinu za binarne datoteke, kao datoteke sa ovim ekstenzijama: .kdb, .kyr, .sth, .rdb, i tako dalje.
Ne možete mijenjati lozinku baze ključeva. Certifikat u bazi ključeva više ne važi.	Nakon provjere da problem nije u neispravnoj lozinci, pronađite i obrišite nevaljane certifikate iz memorije certifikata i zatim pokušajte promijeniti lozinku. Ako u svojoj memoriji certifikata imate istekle certifikate, tada istekli certifikati nisu više važeći. Pošto certifikati više ne važe, funkcija promjene lozinke memorije certifikata ne mora dopustiti promjenu lozinke, a postupak enkripcije neće šifrirati privatni ključ certifikata kojem je važenje isteklo. Ovime se sprečava promjena lozinke a sistem može javiti da je jedan od razloga oštećenje memorije certifikat. Nevažeće (one koje su istekle) certifikate morate ukloniti iz memorije certifikata.
Trebate koristiti certifikate za Internet korisnika i stoga trebate koristiti validacijske popise. Međutim, DCM ne pruža funkcije za validacijske popise.	Poslovni partneri koji pišu aplikacije za korištenje validacijskih popisa moraju ih tako kodirati da validacijske liste pridruže aplikacijama kako se i očekuje. Moraju kodirati tako da odrede kada je identitet korisnika Interneta validiran na odgovarajući način, tako da se potvrda može dodati u validacijsku listu. Pregledajte poglavlje Informativnog centra za QsyAddVldlCertificate API. Isto tako se posavjetujte i sa Vodičem za kreatore mreže i potražite pomoć oko konfiguriranja instanci sigurnih poslužitelja za upotrebu validacijskih popisa.

Rješavanje problema pretražitelja

Koristite sljedeću tablicu da vam pomogne u rješavanju češćih problema pretražitelja koje možete susresti za vrijeme rada sa Upraviteljem digitalnih certifikata (DCM).

Problem	Moguće rješenje
Microsoft Internet Explorer vam ne dozvoljava da izaberete različit certifikat dok ne pokrenete novu sesiju pretražitelja.	Počnite sa novom pretražiteljskom sesijom na Internet Explorer-u.

Problem	Moguće rješenje
Internet Explorer ne pokazuje sve odabirive klijent/korisničke certifikate na popisu izbora pretražitelja. Internet Explorer prikazuje samo one certifikate, koje je izdao pouzdani CA, koje možete koristiti na sigurnoj stranici.	CA mora biti dojavljen kao pouzdan u bazi ključeva kao i u zaštićenoj aplikaciji. Pobrinite se da potpišete na PC računalu za Internet Explorer pretražitelja sa istim korisničkim imenom kao ono ime s kojim je stavljen korisnički certifikat u pretražitelja. Dohvatite drugi korisnički certifikat sa sistema kojem pristupate. Sistemski administrator treba biti siguran da memorija certifikata (ključna baza podataka) još uvijek vjeruje CA-u, koji je potpisao korisničke i sistemske certifikate.
Internet Explorer 5 prima CA certifikat, ali ne može otvoriti datoteku ili pronaći disk u kojem ste pohranili certifikat.	To je novo svojstvo pretražitelja za certifikate, koji Internet Explorer pretražitelju još nisu pouzdani. Možete izabrati lokaciju na svom PC računalu.
Primili ste upozorenje pretražitelja da se sistemsko ime i sistemski certifikat ne slažu.	Neki pretražitelji različito postupaju kod usklađivanja malih i velikih slova u sistemskim imenima. Utipkajte URL istom veličinom slova kako se vidi na sistemskom certifikatu. Ili kreirajte sistemski certifikat sa slovnikom koji se slaže sa većinom korisničkih upotreba. Ako ne znate što činite, najbolje je da sistemsko ime ili ime poslužitelja ostavite kako je bilo. Trebali biste i provjeriti je li ime vaše domene ispravno dojavljeno.
Pokrenuli ste Internet Explorer sa HTTPS umjesto HTTP i primili ste upozorenje o miješanju sigurnih i nesigurnih sesija.	Prihvatite i ignorirajte upozorenje; buduće izdanje Internet Explorer-a će riješiti taj problem.
Netscape Communicator 4.04 za Windows je pretvorio heksadecimalne vrijednosti A1 i B1 u B2 i 9A u Poljskoj kodnoj stranici.	Ovo je buba u pregledniku koja pogađa NLS. Koristite različit pretražitelj ili koristite istu verziju ovog pretražitelja na drugoj platformi, kao Netscape Communicator 4.04 za AIX.
U korisničkom profilu Netscape Communicator za 4.04 pokazao je ispravno NLS znakove velikih slova korisničkog certifikata, ali znakove malih slova nije prikazao ispravno.	Neki znakovi nacionalnih jezika, koji su ispravno unijeti kao jedan znak ali nisu kasnije prikazani kao jedan znak. Na primjer, na Windows verziji Netscape Communicator 4.04, heksadecimalne vrijednosti A1 i B1 su pretvorene u B2 i 9A za Poljsku kodnu stranicu, rezultirajući različitim NLS znakovima koji se prikazuju.
Pretražitelj i dalje javlja krajnjem korisniku da se tom CA još ne vjeruje.	Upotrijebite DCM za postavljanje **CA statusa** da se omogući pouzdanost CA.
Internet Explorer zahtjeva odbacivanje veze za HTTPS.	Ovo je problem s pretražiteljevom funkcijom ili njegovom konfiguracijom. Pretražitelj odluči da se ne spoji na stranicu koja koristi sistemski certifikat koji bi mogao biti samopotpisan ili možda nije važeći radi nekih drugih razloga.
Pretražitelj Netscape Communicator-a i poslužiteljski proizvodi upotrebljavaju korijenske certifikate od poduzeća, uključujući ali se ne ograničavajući, VeriSign, kao svojstvo omogućavanja SSL komunikacija — specifično, provjera autentičnosti. Svi korijenski certifikati povremeno ističu. Neki Netscape pretražitelji i korijenski certifikati pretražitelja ističu između 25. prosinca 1999 i 31. prosinca 1999. Ako niste taj problem riješili na ili prije 14. prosinca 1999, primiti ćete poruku o greški.	Ranije verzije pretražitelja (Netscape Communicator 4.05 ili ranije) imaju certifikate koji ističu. Ne trebate ažurirati pretražitelja na trenutnu verziju Netscape Communicator-a. Informacije o pretražiteljevim korijenskim certifikatima su dostupne na mnogim stranicama uključujući http://home.netscape.com/security/ i http://www.verisign.com/server/cus/rootcert/webmaster.html. Slobodna učitavanja pretražitelja su dostupna sa http://www.netcenter.com.

Rješavanje problema HTTP poslužitelja za iSeries problems

Koristite sljedeću tablicu da nađete informacije da vam pomognu u rješavanju češćih problema HTTP poslužitelja za iSeries koje možete susresti za vrijeme rada sa Upraviteljem digitalnih certifikata (DCM).

Problem	Moguće rješenje
Hypertext Transfer Protocol Secure (HTTPS) ne radi.	Pobrinite se da je HTTP poslužitelj ispravno konfiguriran za korištenje SSL-a. U V5R1 ili kasnijim verzijama konfiguracijska datoteka mora imati **SSLAppName** postavljeno korištenjem grafičkog korisničkog sučelja (GUI) HTTP poslužitelja. Također, konfiguracija mora imati virtualni host konfiguriran koji koristi SSL port, sa **SSLEnable** unutar virtualnog hosta. Moraju također bit dvije direktive Slušanja koje specificiraju dva različita porta, jedan za SSL i drugi koji nije za SSL. Osigurajte da je instanca poslužitelja kreirana i certifikat poslužitelja potpisan.
Postupak registriranja instance HTTP poslužitelja kao zaštićene aplikacije treba pojašnjenje.	Na vašem iSeries sistemu, idite na web sučelje HTTP poslužitelja da postavite konfiguraciju za vaš HTTP poslužitelj. Morate prvo definirati virtualan host da omogući SSL. To se radi na ekranu Upravljanje kontekstom. Virtualni host mora biti definiran da koristi SSL port definiran prethodno u Slušaj direktivu. Sljedeće, morate koristiti ekran SSL općenite postavke da uključite SSL u prethodno konfiguriranom SSL virtualnom hostu. Sve promjene moraju biti primijenjene na konfiguracijsku datoteku. Zapamtite da registriranje vaše instance ne bira automatski koje certifikate instanca treba koristiti. Morate koristiti DCM za dodjelu određenog certifikata vašoj aplikaciji prije nego pokušate zaustaviti i ponovno pokrenuti vašu instancu poslužitelja.
Imate teškoća u podešavanju HTTP poslužitelja za rad s validacijskim listama i opcionom provjerom klijenata.	Opcije o ustroju instance potražite u Vodiču za HTTP Server Webmaster. Ova informacija je također dostupna u poglavlju Web posluživanje u Informacijskom Centru.
Netscape Communicator čeka na komunikacijska upute u HTTP poslužiteljskom kodu da istekne prije nego vam dopusti izbor raznih certifikata.	Uz veliku vrijednost certifikata teško je registrirati drugi certifikat jer pretražitelj još koristi prvi certifikat.
Pokušavate dohvatiti pretražitelja da predoči certifikat HTTP poslužitelju tako da taj certifikat možete upotrijebiti kao ulaz QsyAddVldlCertificate API-u.	Morate koristiti **SSLEnable** i **SSLClientAuth ON** da bi HTTP poslužitelj učitao HTTPS_CLIENT_CERTIFICATE varijablu okoline. Možete naći ove APIje u poglavlju OS/400 APIji u Informacijskom Centru. Možete također htjeti pogledati te validacijske popise ili API-e, koji se odnose na certifikate: • QsyListVldlCertificates i QSYLSTVC • QsyRemoveVldlCertificate i QRMVVC • QsyCheckVldlCertificate i QSYCHKVC • QsyParseCertificate i QSYPARSC, itd.
Ne možete naći datoteku zahtjeva koja je kreirana kad se instalirao HTTP poslužitelj. Sistem koristi ovu datoteku da pokaže važeće datoteke prstenova ključeva pronađene na KEYFILE uputi u konfiguracijskim datotekama u njenom direktoriju.	Pogledajte Migriranje na DCM sa ranijeg izdanja za više informacija. Za HTTP poslužitelj ispravna datoteka je /qibm/userdata/httpsvr/keyring/keymreq.crt. Za LDAP ispravna datoteka je /qibm/userdata/os400/dirsrv/qdirsrv.crt.
Povratak HTTP poslužitelja predugo traje, ili istekne vrijeme ako zatražite popis certifikata u validacijskom popisu a tamo postoji više od 10.000 stavki.	Kreirajte paketni posao koji traži i briše certifikate koji odgovaraju određenim kriterijima, kao što su svi oni koji su istekli ili su od nekog određenog CA.
Uočili ste problem sa vašim memorijama certifikata nakon instaliranja V5R2 preko izdanja V4R3 i /qibm/userdata/httpsvr/keyring/keymreq.crt ili /qibm/usedata/os400/dirsrv/qdirsrv.crt datoteka sada postoji. Sistem nije mogao dovršiti migraciju automatskog prstena ključeva ili baze ključeva.	Specificirajte stare datoteke prstenova ključeva kao memorija certifikata, pronađite i izbrišite nevažeći certifikat ili certifikate od datoteka prstenova ključeva, prije nego što pozovete qicss/qyepmgrt za ponovni pokušaj migracije. Ili, zanemarite ili izbrišite datoteku .crt ako je aktivnost migracije pomaknula sve važne certifikate.

Problem	Moguće rješenje
HTTP poslužitelj nije uspješno pokrenut sa postavljenim **SSLEnable** i poruka o grešci HTP8351 se pojavila u dnevniku posla. Dnevnik grešaka za *ADMIN poslužitelj pokazuje grešku da SSL operacija inicijalizacije nije uspjela sa povratnim kodom 107 kada HTTP poslužitelj ne uspije.	Greška 107 znači da je certifikat istekao. Ako je instanca poslužitelja *ADMIN poslužitelj, tada privremeno postavite **SSLDisable** tako da možete koristiti DCM na *ADMIN poslužitelju. Koristite DCM za dodjeljivanje različitih certifikata aplikacijama; na primjer, QIBM_HTTP_SERVER_ADMIN ako je instanca poslužitelja *ADMIN poslužitelj.

Migracijske greške i rješenja obnavljanjem

Greške i ponovo dobivanje grešaka

Slijedeći pokazatelji vas upozoravaju na greške koje bi se mogle pojaviti tijekom migracije:

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
Prisustvo ovog pokazatelja, nakon što ste uspješno instalirali obje opcije, 34 i 5722-DG1, znači da migracija prstena ključeva koju je pokušala opcija 5722-DG1 32 nije uspjela. Možda ćete trebati izvesti migraciju prstena ključeva u *SYSTEM memoriju certifikata.

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT
Prisustvo ovog pokazatelja, nakon što ste uspješno instalirali opciju 34 znači da migracija prstena ključeva za LDAP poslužitelj nije uspjela.

Uz naznačene greške, moguće su i migracijske greške na koje sistem ne mora ukazati. Na primjer, kad sistem pronađe datoteke prstenova ključeva koje treba za migraciju u memoriju *SYSTEM certifikata, mogla bi naići i na sukobe sa postojećim datotekama podataka u integriranom sistemu datoteka. U takvom slučaju sistem možda ne bi mogao dovršiti migraciju datoteke prstena ključeva, čak iako ste uspješno dovršili instalaciju.

U rijetkom slučaju bi bilo moguće imati migraciju datoteke prstena ključeva sa djelomičnom dodjelom sistemskog certifikata, dovršenom prije nego greška spriječi dovršetak migracije. To može rezultirati pogreškama kada pokrenete IBM HTTP poslužitelj *ADMIN instancu ako je SSLMODE na ON. Moguća objašnjenja su:

- Migrirana datoteka prstena ključeva imala je loš skup sistemskih certifikata kao svoj default.
- DCM je završio migraciju kako bi sačuvao korisničke podatke koji su već postojali u kritičnoj datoteci.
- U kodiranju migracije došlo je do nepredviđene greške.

Možete pokrenuti IBM HTTP poslužitelj bez SSLMODE postavljenog na ON privremeno postavljanjem SSLMODE na OFF za *ADMIN instancu prije pokretanja *ADMIN instance. Time vam je omogućeno da istražite memorije certifikata pomoću DCM-a i riješite problem prije nego što završite s instancom *ADMIN. Nakon što završite *ADMIN instancu, možete zatim postaviti SSLMODE natrag na Uključeno i pokrenuti *ADMIN instancu za ispravnu inicijalizaciju SSL-a.

Nakon migracije opcije 34, greške se mogu desiti tijekom normalnih DCM zahtjeva koji koriste memorije certifikata. Te se greške događaju na pretražitelju. Slijede primjeri takvih grešaka:

```
Greška baze podataka
Greška u čitanju baze podataka.
Greška u pisanju baze podataka.
Oštećenje baze podataka
Tablica baze oštećena
```

Nadalje, sistem bi mogao imati datoteku, koja nije važeća memorija certifikata imenovana default.kdb u istom direktoriju kao/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR ili /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR. U tom slučaju trebate dovršiti sljedeću ručnu migraciju prije upotrebe DCM-a za kreiranje novih certifikata:

Bilješka: Ako odlučite da ne migrirate datoteke prstenova ključeva te umjesto kreiranja novog CA i sistemskog certifikata, preskočite slijedeći postupak ručne migracije.

- Ako planirate instalirati HTTP poslužitelj iSeries (5722-DG1), instalirajte ga sada prije nastavljanja.

  Bilješke:

  1. 5722–SS1 opcija 34 instalacioni kod ne pokušava ponovo migrirati nakon što ste instalirali opciju 34. Jednostavno reinstaliranje opcije 34 ne pomaže.
  2. Odgovarajuće datoteke su smještene u direktorijima korisničkih podataka koji su bili kreirani s ovlaštenjem PUBLIC *EXCLUDE. Pobrinite se da za njih budete ispravno ovlašteni.

- Provjerite da vidite postoje li sljedeće datoteke:
  - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

  Ako one postoje, upotrijebite naredbu WRKLNK da ih preimenujete i kreirate backup-ove.
- Sa korisničkog profila koji ima *ALLOBJ ovlaštenje, pozovite program QICSS/QYEPMGRT na redu za naredbe, kako slijedi:

  ```
  CALL QICSS/QYEPMGRT
  ```

  Ako je rezultat uspješan, pobrinite se da na vašem sistemu ne postoji ni jedna od slijedećih datoteka:
  - /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
  - /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

DCM obično čuva zaštitnu kopiju (rezervu) korisničkih podataka koje pohranjujete u datotekama, čija imena dolaze u sukob s onima koja koristi DCM. Ako sljedeće datoteke ne postoje:

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

Ali postoje sljedeće datoteke:

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

Onda ih sistem pokušava preimenovati sa pridodanom ekstenzijom .OLD. Ako te datoteke također već postoje, sistem ne napravi nikakvu zaštitnu kopiju. Umjesto toga on jednostavno prepiše postojeće .STH datoteke.

Razno

Ako vaši pokušaji da kreirate CA i sistemski certifikat i dalje ostaju bezuspješni zbog sukoba u imenima, možda ste naletjeli na jednu od slijedećih situacija:

- **Sukob različitih imena datoteka** – DCM pokušava zaštititi korisničke podatke u direktorijima koje kreira, čak i ako te datoteke osujećuju DCM u uspješnom kreiranju datoteka kad to treba učiniti. Ovo riješite tako da kopirate sve datoteke u sukobu u neki drugi direktorij i, ako je moguće, upotrijebite funkciju DCM-a za brisanje odgovarajućih datoteka. Ako ne možete upotrijebiti DCM za obavljanje toga, ručno izbrišite datoteke sa

direktorija integriranog sistema datoteka, gdje su se sukobljavale sa DCM-om. Pazite da zabilježite točno one datoteke koje selite i kamo ih selite. Kopije vam omogućuju da povratite datoteke ako uvidite da vam još trebaju. Novi CA trebate kreirati nakon što preselite sljedeće datoteke:

```
/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
```

Trebate kreirati novu memoriju *SYSTEM certifikata i sistemski certifikat nakon pomicanja sljedećih datoteka:

```
/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
```

- **Preduvjeti koji nedostaju** – Pobrinite se da imate ispravno instalirane preduvjetne licencne programe (LPP-ove).
- **Problem u kodiranju** – Obratite se predstavniku servisa.

Ispravljanje pogrešaka kod dodjeljivanja korisničkog certifikata

Kada koristite zadatak **Dodijeli korisnički certifikat**, Upravitelj digitalnih certifikata (DCM) prikazuje informacije certifikata da odobrite prije registriranja certifikata. Ako DCM nije u stanju prikazati certifikat, problem bi mogao biti uzrokovan jednom od slijedećih situacija:

1. Vaš pretražitelj nije zahtijevao da izaberete certifikat koji ćete predočiti poslužitelju. Ovo se može desiti ako je pretražitelj stavio prethodni certifikat u skrivenu memoriju (kod pristupa nekom drugom poslužitelju). Ispraznite predmemoriju pretražitelja i pokušajte ponovo izvesti posao. Pretražitelj bi vas trebao upitati da izaberete certifikat.
2. Certifikat koji želite registrirati je već registriran pri DCM-u.
3. Izdavač certifikata nije označen kao pouzdan na sistemu. Stoga certifikat koji predočavate nije valjan. Obratite se sistemskom administratoru da utvrdi je li izdavač koji je izdao certifikat ispravan. Ako je CA ispravan, sistemski administrator bi mogao trebati **Unijeti**

CA certifikat u memoriju *SYSTEM certifikata. Ili, administrator može trebati zadatak **Rad sa CA certifikatima** da omogući CA kao pouzdano ishodište na sistemu za ispravljanje problema.

4. Nemate nikakav certifikat za registraciju. Provjerite ima li korisničkih certifikata u pregledniku da vidite je li to problem.
5. Certifikat koji nastojite registrirati je istekao ili je nepotpun. Morate ili obnoviti certifikat ili se obratiti izdavaču koju ga je izdao da riješi ovaj problem.
6. IBM HTTP poslužitelj za iSeries nije ispravno postavljen da radi registracije certifikata korištenjem SSL-a i provjeru autentičnosti klijenta na sigurnoj instanci *ADMIN poslužitelja. Ako nijedan od navedenih savjeta za otklanjanje problema ne radi, obratite se sistemskom administratoru i prijavite problem.

Da **Dodijelite korisnički certifikat** morate se spojiti na Upravitelja digitalnih certifikata (DCM) koristeći SSL sesiju. Ako ne koristite SSL kad odaberete zadatak **Dodijeli korisnički certifikat** DCM će prikazati poruku da morate upotrijebiti SSL. Poruka sadrži gumb tako da se možete spojiti na DCM koristeći se SSL-om. Ako se poruka prikaže bez toga gumba, obavijestite sistemskog administratora o problemu. Možda će trebati ponovo pokrenuti mrežni poslužitelj da budete sigurni da su sve upute u konfiguraciji za upotrebu SSL-a aktivirane.

Poglavlje 10. Povezane informacije za DCM

Kako je upotreba digitalnih certifikata postala prevladavajuća, i informacijski resursi su postali dostupni. Ovdje je malen popis drugih resursa koje možete pregledati da naučite više o digitalnim certifikatima i kako ih možete koristiti da poboljšate vašu iSeries politiku sigurnosti:

- **VeriSign Help Desk web stranica**
  VeriSign web mjesto pruža opsežnu knjižnicu o temama digitalnih certifikata kao i određen broj drugih Internet sigurnosnih tema.
- **IBM eServer iSeries Žičana mrežna sigurnost: OS/400 V5R1 DCM i kriptografička poboljšanja SG24-6168**
  Ovaj IBM Redbook se fokusira na V5R1 poboljšanja mrežne sigurnosti. Redbook poriva mnoga poglavlja uključujući kako koristiti iSeries mogućnosti potpisivanja objekata, Upravitelj digitalnih certifikata (DCM), podršku 4758 kriptografičkog koprocesora za SSL, i tako dalje.
- **AS/400 Internet sigurnost: Razvijanje infrastrukture digitalnog certifikata (SG24-5659)**
  Ovaj redbook opisuje što možete učiniti sa digitalnim certifikatima na iSeries poslužitelju. Objašnjava se kako postaviti različite poslužitelje i klijente za korištenje certifikata. Nadalje pruža informacije i uzorak koda kako koristiti OS/400 APIje za upravljanje i korištenje digitalnih certifikata u aplikacijama korisnika.
- **RFC indeksno traženje**
  Ova web stranica pruža spremište Zahtjeva za komentarom (RFCa) koje se može pretražiti. RFC-ovi opisuju standarde za Internet protokole, kao SSL, PKIX i druge koji se odnose na korištenje digitalnih certifikata.

Tiskano u Hrvatskoj