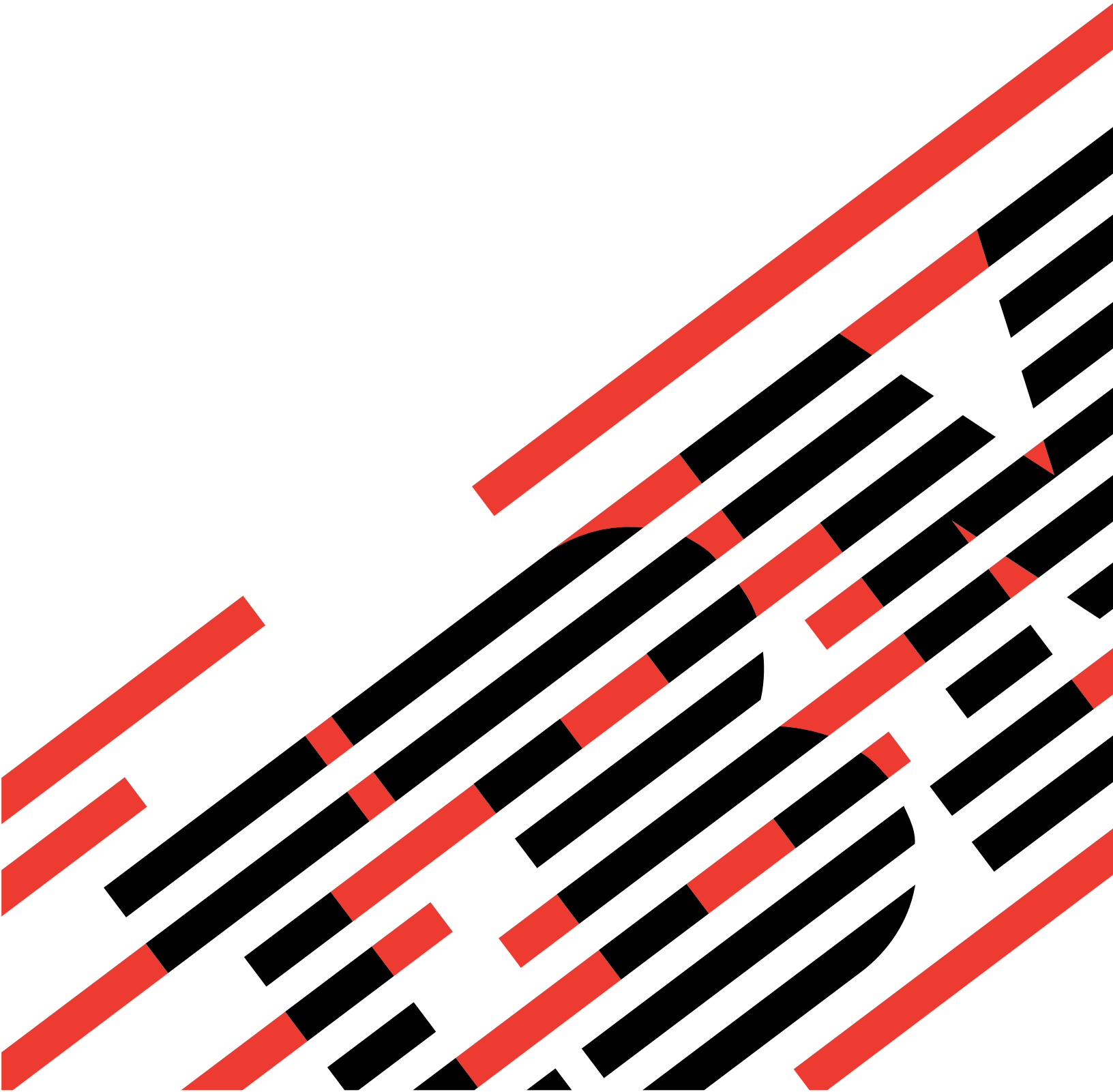
IBM

eserver

iSeries

Upravitelj digitalnih certifikata

Verzija 5 Izdanje 3



IBM

@server

iSeries

Upravitelj digitalnih certifikata

Verzija 5 Izdanje 3

Napomena

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene”, na stranici 93.

Osmo izdanje (kolovoz, 2005)

Ovo izdanje se primjenjuje na verziju 5, izdanje 3, modifikaciju 0 za IBM Operating System/400 (broj proizvoda 5722–SS1) i na sva sljedeća izdanja i modifikacije dok se drukčije ne označi u novim izdanjima. Ova verzija ne radi na svim modelima računala smanjenog seta instrukcija (RISC) niti ne radi na CISC modelima.

Sadržaj

Poglavlje 1. Upravitelj digitalnih certifikata 1

Poglavlje 2. Što je novo za V5R3 3

Poglavlje 3. Ispis ovog poglavlja 5

Poglavlje 4. DCM scenariji 7

| Scenarij: Upotreba certifikata za eksternu provjeru autentičnosti 7
Detalji konfiguracije 10
| Scenarij: Upotreba certifikata za internu provjeru autentičnosti 14
Detalji konfiguracije 17

Poglavlje 5. Koncepti digitalnog certifikata 23

| Proširenja certifikata 24
| Obnavljanje certifikata 24
Razlikovno ime 24
Digitalni potpisi 25
Javni-privatni par ključeva 25
Izdavač certifikata (CA) 26
Lokacije Liste opoziva certifikata (CRL) 26
Spremišta certifikata 27
Kriptografija 28
| IBM Kriptografički koprocesori za iSeries 28
Sloj sigurnih utičnica (SSL) 29
| Definicije aplikacija 29
| Provjera valjanosti. 29

Poglavlje 6. Plan za DCM 31

Zahtjevi za DCM postav 31
| Razmatranja o kopiranju i obnavljanju za DCM podatke 32
Tipovi digitalnih certifikata 32
Javni certifikati naspram privatnih certifikata 33
Digitalni certifikati za SSL sigurne komunikacije . . . 35
Digitalni certifikati za provjeru korisnika 35
| Digitalni certifikati i Mapiranje identiteta u poduzeću (EIM) 36
Digitalni certifikati za VPN veze 37
Digitalni certifikati za potpisivanje objekata 38
Digitalni certifikati za provjeru potpisa objekata 38

Poglavlje 7. Konfiguriranje DCM-a . . . 41

Pokretanje Upravitelja digitalnih certifikata 41
Postavljanje certifikata prvi put 42
Kreiranje i rad s Lokalnim CA 43
Upravljanje certifikatima korisnika 44
Kreiranje certifikata korisnika 45
Dodjela certifikata korisnika. 45
| Upravljanje korisničkim certifikatima pomoću isteka 46
Upotreba API-ja za programsko izdavanje certifikata ne-iSeries korisnicima 47
Dobivanje kopije privatnog CA certifikata . . . 48
Upravljanje certifikatima od javnog Internet CA . . . 48
Upravljanje javnim Internet certifikatima za SSL komunikacijske sesije. 49
Upravljanje javnim Internet certifikatima za potpisivanje objekata 50
Upravljanje certifikatima za provjeru potpisa objekata 52

Poglavlje 8. Upravljanje DCM-om . . . 55

Upotreba lokalnog CA za izdavanje certifikata za druge iSeries sisteme 55
| Upotreba privatnog certifikata za SSL sesije na V5R3 ili V5R2 ciljnom sistemu 58
Upotreba privatnog certifikata za SSL sesije na V5R1 ciljnom sistemu 62
| Upotreba privatnog certifikata za potpisivanje objekata na V5R3, V5R2 ili V5R1 ciljnom sistemu. 65
| Upotreba privatnog certifikata za SSL sesije na V4R5 ciljnom sistemu 68
Upravljanje aplikacijama u DCM-u. 72
Kreiranje definicije aplikacije 72
Upravljanje dodjelom certifikata za aplikaciju . . . 73
Definiranje CA popisa povjerenja za aplikaciju . . . 73
| Upravljanje certifikatima pomoću isteka 74
Provjera valjanosti certifikata i aplikacija 75
Dodjela certifikata aplikacijama. 75
Upravljanje CRL lokacijama. 76
Spremanje ključeva certifikata u IBM Kriptografički koprocesor 77
Spremanje privatnog ključa certifikata izravno u koprocesor 77
Upotreba glavnog ključa koprocesora za šifriranje privatnog ključa 77
Upravljanje lokacijom zahtjeva za PKIX CA 78
| Upravljanje LDAP lokacijom za korisničke certifikate . . 78
Potpisivanje objekata 79
Provjera potpisa objekata. 81

Poglavlje 9. Rješavanje problema DCM-a 83

Rješavanje problema lozinki i općenitih problema . . . 83
Rješavanje problema spremišta certifikata i baze podataka ključeva. 84
Rješavanje problema pretražitelja 86
Rješavanje problema HTTP poslužitelja za iSeries problems 87
Rješavanje problema dodjele korisničkog certifikata. . . 88

Poglavlje 10. Povezane informacije za DCM. 91

Dodatak. Napomene 93
Zaštitni znaci 94
Termini i uvjeti za spuštanje i ispis publikacija 94

Poglavlje 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 radi osiguranja boljih mjera 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 usluge i aplikacije, kao što su FTP, Telnet, HTTP poslužitelj za iSeries i mnoge druge, osiguravaju SSL podršku za osiguranje privatnosti podataka.

IBM osigurava opsežnu podršku s digitalnim certifikatima koja vam omogućuje da koristite digitalne certifikate kao vjerodajnice 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 potpisivanje objekata. Potpisivanje objekata vam dozvoljava da otkrijete promjene ili moguće zlonamjerne promjene sadržaja objekta provjeravanjem potpisa na objektima radi osiguranja njihove cjelovitosti.

Upotreba podrške za certifikate je jednostavna pomoću Upravitelja digitalnih certifikata (DCM), besplatnog dodatka za središnje upravljanje certifikatima za vaše aplikacije. DCM vam dopušta da upravljate certifikatima koje dobivate od svakog Izdavača certifikata (CA). Možete koristiti DCM i za kreiranje i rad s vašim vlastitom Lokalnim CA za izdavanje privatnih certifikata aplikacijama i korisnicima u vašoj organizaciji.

Ispravno planiranje i procjena su ključevi učinkovitog korištenja certifikata za njihove dodatne sigurnosne prednosti. Možete pregledati ova poglavlja da naučite više o tome kako rade certifikati i kako možete koristiti DCM za upravljanje njima i aplikacijama koje ih koriste:

Što je novo za V5R3
Koristite ove informacije da naučite više o poboljšanjima Upravitelja digitalnim certifikatima i promjenama poglavlja informacija za ovo izdanje.

Ispis ovog poglavlja
Koristite ovu stranicu da saznate kako ispisati cijelo poglavlje kao PDF datoteku.

DCM scenariji
Koristite ove informacije i pregledajte dva scenarija koji ilustriraju tipične primjene shema certifikata, za pomoć u planiranju vaše vlastite primjene certifikata kao dijela vaših sigurnosnih politika. Svaki scenarij također daje sve potrebne zadatke konfiguracije koje morate izvesti da upotrijebite scenarij kako je opisano.

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

Plan za DCM
Koristite ove informacije kao pomoć kod odluke kako i kada možete koristiti digitalne certifikate da ispunite vaše ciljeve sigurnosti. Koristite ove informacije da naučite o preduvjetima koje trebate instalirati kao i ostalim zahtjevima koje morate uzeti u obzir prije korištenja DCM-a.

Konfiguriranje DCM-a
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 s vašim vlastitim Izdavačima certifikata.

Rješavanje problema DCM-a
Upotrijebite ove informacije 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 informacijama.

Poglavlje 2. Što je novo za V5R3

Poboljšanja za V5R3 Upravitelja digitalnih certifikata i sposobnosti digitalnih certifikata uključuju:

- **Upravljanje LDAP lokacijom**
  Novi zadatak Upravljanje LDAP lokacijom u DCM zadatku dozvoljava vam da pohranite korisničke certifikate koje Lokalni izdavač certifikata izdaje na Lightweight Directory Access Protocol (LDAP) lokaciji. Kada konfigurirate DCM za upotrebu ove opcije, možete koristiti korisničke certifikate koji su pohranjeni na ovoj LDAP lokaciji s Mapiranjem identiteta u poduzeću (EIM). Pristupate ovom zadatku iz glavnog DCM navigacijskog izbornika.
- **Poboljšanja zadatka Dodjela korisničkog certifikata za EIM**
  Kada konfigurirate DCM za rad s Mapiranjem identiteta u poduzeću (EIM), zadatak Dodjela korisničkog certifikata pohranjuje dodijeljene certifikate na lokaciju Lightweight Directory Access Protocol (LDAP), a ne s korisničkim profilom. Kako DCM rukuje dodjelom certifikata ovisi o tome da li ste konfigurirali DCM za upotrebu Lightweight Directory Access Protocol (LDAP) lokacije za pohranu certifikata zajedno s upotrebom Mapiranja identiteta u poduzeću (EIM).
- **Provjera isteka certifikata**
  Ova nova funkcija dozvoljava vam da brzo i jednostavno pogledate i upravljate certifikatima na osnovu datuma isteka certifikata. Možete provjeriti istek certifikata za certifikate poslužitelja ili klijenta i certifikate za potpisivanje objekta na lokalnom sistemu. Također, možete provjeriti istek korisničkog certifikata. Možete provjeriti istek korisničkog certifikata ili za specifični korisnički profil, za sve korisničke certifikate na sistemu, ili za sve korisničke certifikate u poduzeću kada je EIM konfiguriran na sistemu.

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

Kako pogledati što je novo ili promijenjeno

Za pomoć da vidite gdje su napravljene tehničke promjene, ove informacije koriste:

- Sliku  da označi gdje započinju nove ili promijenjene informacije.
- Sliku da označi gdje završavaju nove ili promijenjene informacije.

Poglavlje 3. Ispis ovog poglavlja

Za pregled ili učitavanje PDF verzije ovog poglavlja, izaberite Upravitelj digitalnih certifikata  (veličina datoteke je oko 600 KB ili oko 116 stranica).

Spremanje PDF datoteka:

Da spremite PDF na vašu radnu stanicu za pregled ili ispis:

1. Desno kliknite na PDF u vašem pretražitelju (desni klik na vezu iznad).
2. Kliknite **Save Target As...** ako koristite Internet Explorer. Kliknite **Save Link As...** ako koristite Netscape Communicator.
3. Izaberite direktorij u koji želite spremiti PDF.
4. Kliknite **Save**.

Spuštanje Adobe Acrobat Readera

Trebate Adobe Acrobat Reader za pregled i ispis ovih PDF-ova. Možete učitati kopiju s Adobe Web stranice (www.adobe.com/products/acrobat/readstep.html)  .

Poglavlje 4. DCM scenariji

Upravitelj digitalnih certifikata i sistemska podrška digitalnim certifikatima vam omogućuju da koristite certifikate za poboljšanje vaše sigurnosne politike na puno različitih načina. Da li ćete izabrati upotrebu certifikata zavisi o vašim poslovnim ciljevima i vašim sigurnosnim potrebama.

Upotreba 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, zavisno o tome kako konfigurirate DCM, možete koristiti DCM za pridruživanje korisničkog certifikata s odgovarajućim korisničkim profilom ili za identifikator Mapiranja identiteta u poduzeću (EIM). Certifikat tada ima iste autorizacije i dozvole kao i pridruženi korisnički profil.

Kao posljedica, način na koji koristite certifikate može biti kompliciran i ovisi o raznim faktorima. Dobavljeni scenariji u ovom poglavlju opisuju neke od češćih objektiva sigurnosti digitalnih certifikata za sigurne komunikacije unutar tipičnog poslovnog konteksta. Svaki scenarij također opisuje sve potrebne sistemske i softverske preduvjete i sve zadatke konfiguracije koje morate izvoditi da bi implementirali scenarij. **Opaska:** Pogledajte Scenariji potpisivanja objekta u iSeries Informacijskom centru za detaljne primjere kako koristiti digitalne certifikate za potpisivanje objekata zbog zaštite njihovog integriteta.

Pregledajte te scenarije da vam pomognu odrediti kako korištenje certifikata za povećanu sigurnost može najbolje odgovarati vašim potrebama:

Scenarij: Upotreba certifikata za eksternu provjeru autentičnosti
Ovaj scenarij opisuje kada i kako koristiti certifikate kao mehanizam provjere autentičnosti da zaštitite i ograničite pristup od strane javnih korisnika do javnih ili extranet izvora i aplikacija.

Scenarij: Upotreba certifikata za internu provjeru autentičnosti
Ovaj scenarij opisuje kada i kako koristiti certifikate kao mehanizam provjere autentičnosti da zaštitite i ograničite kojim resursima i aplikacijama interni korisnici mogu pristupati na vašim internim poslužiteljima.

Scenarij: Upotreba certifikata za eksternu provjeru autentičnosti

Situacija

Vi radite za MyCo, Inc osiguravajuće poduzeće i odgovorni ste za održavanje različitih aplikacija na intranet i extranet 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 s vremenom dobaviti sigurniju metodu provjere autentičnosti korisnika za aplikaciju od vaše trenutne metode korisničkog imena i lozinke. Dodatno vas brine da neovlašteni korisnici mogu dohvatiti ove informacije kada se prenose preko mreže koja nije povjerljiva. Također vas zabrinjava da različiti agenti mogu dijeliti ove informacije jedni s drugima, bez ovlaštenja za to.

Nakon istraživanja, odlučili ste da upotreba digitalnih certifikata može omogućiti sigurnost koju trebate da zaštitite osjetljive informacije unešene u i dohvaćene iz ove aplikacije. Upotreba certifikata dozvoljava vam da koristite Sloj sigurnih utičnica (SSL) da zaštitite prijenos podataka rate. 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. Kao dodatak upotrebi provjere autentičnosti klijenta certifikatom, planirate nastaviti trenutnu upotrebu provjere autentičnosti korisničkim imenom i lozinkom jer SSL štiti privatnost ovih osjetljivih podataka u prijenosu.

Na osnovu tipa aplikacije i njegovih korisnika i vaših budućih ciljeva za provjeru autentičnosti certifikata za sve korisnike, vi odlučujete koristiti javni certifikat od dobro poznatog Izdavača certifikata (CA) da konfigurirate SSL za vašu aplikaciju.

Prednosti scenarija

Ovaj scenarij ima sljedeće prednosti:
- Korištenje digitalnih certifikata za konfiguriranje SSL pristupa na vašu aplikaciju izračuna omjera, osigurava da su informacije koje se prenose između poslužitelja i klijenta zaštićene i privatne.
- Korištenje digitalnih certifikata kad god je moguće za provjeru ovlaštenja klijenta pruža sigurniji način identificiranja ovlaštenih korisnika. Čak i tamo gdje upotreba digitalnih certifikata nije moguća, provjera autentičnosti provjerom korisničkog imena i lozinke zaštićena je i zadržana u tajnosti od strane SSL sesije, čineći razmjenu tako osjetljivih podataka sigurnom.
- Upotreba *javnih* digitalnih certifikata za ovlaštenje korisnika za vaše aplikacije i podatke na način na koji ovaj scenarij prikazuje praktičan je izbor pod ovim i sličnim uvjetima:
  - Podaci i aplikacije iziskuju različite stupnjeve zaštite.
  - Stopa prometa među pouzdanim korisnicima je vrlo velika.
  - Omogućujete javni pristup aplikacijama i podacima, kao što je Internet Web stranica, ili extranet aplikacija.
  - Ne želite raditi s vašim Izdavačem certifikata (CA) zbog administrativnih razloga, kao što je velik broj vanjskih korisnika koji pristupaju vašim aplikacijama i izvorima.
- Upotreba javnih certifikata za konfiguriranje aplikacije za izračun omjera za koji SSL u ovom scenariju smanjuje broj konfiguracija koje korisnici moraju obaviti za siguran pristup aplikaciji. Većina softvera klijenta sadrži CA certifikate za većinu poznatih CA.

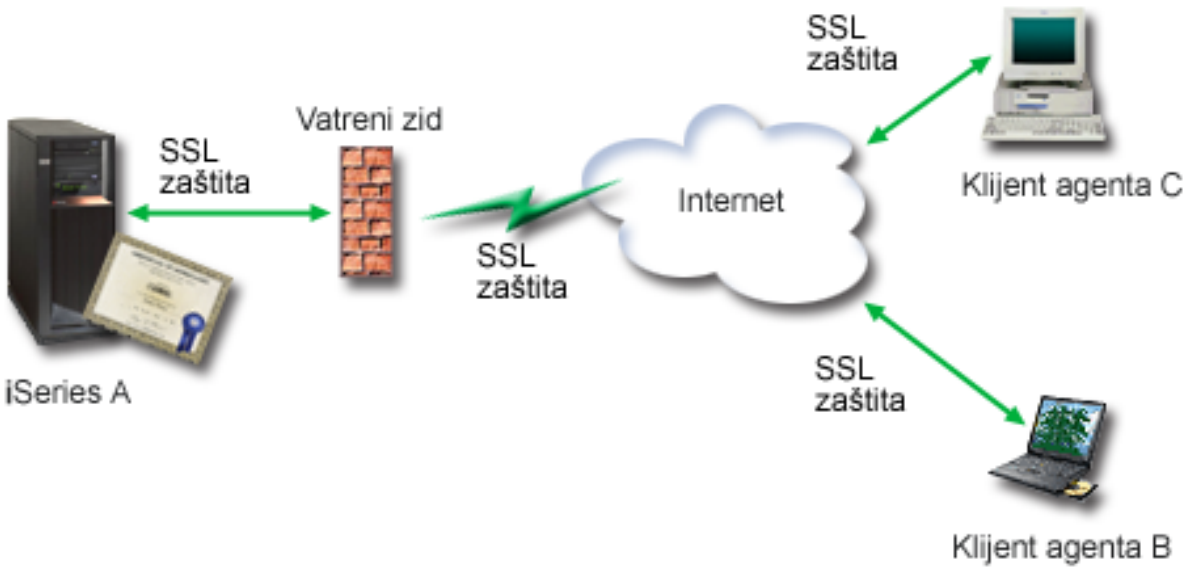
Objektivi

U ovom scenariju, MyCo, Inc. želi koristiti digitalne certifikate da zaštiti informacije o izračunu omjera koje njihova aplikacija omogućuje ovlaštenim javnim korisnicima. Poduzeće također želi sigurniju metodu provjere autentičnosti onih korisnika kojima je dozvoljen pristup ovoj aplikaciji kada je to moguće.

Ciljevi ovog scenarija su sljedeći:
- Aplikacija za izračun javne rate poduzeća mora koristiti SSL da zaštiti privatnost podataka koje dobavlja korisnicima i prima od korisnika.
- 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 predstaviti ili javni digitalni certifikat od dobro poznatog Izdavača certifikata (CA), ili važeće korisničko ime i lozinku ako certifikat nije dostupan.

Detalji

Sljedeća slika objašnjava mrežnu konfiguraciju u ovom scenariju:



Slika prikazuje sljedeće informacije o situaciji za ovaj scenarij:

Javni poslužitelj poduzeća – A
- Poslužitelj A je poslužitelj koji je host za aplikaciju izračuna tečajeva poduzeća.
- Poslužitelj A se izvodi na OS/400 Verziji 5 Izdanje 2 (V5R2) ili višu verziju.
- Poslužitelj A ima instaliranog dobavljača kriptografičkog pristupa (5722–AC3).
- Poslužitelj A ima instalirane i konfigurirane Upravitelja digitalnih certifikata(OS/400 opcija 34) i IBM HTTP poslužitelj za iSeries (5722–DG1).
- Poslužitelj A izvodi aplikaciju za izračun tečajeva, koja je konfigurirana na sljedeći način:
  - Zahtijeva SSL način.
  - Koristi javni certifikat od dobro poznatog Izdavača certifikata (CA) za vlastito ovlaštenje za inicijalizaciju SSL sesije.
  - Zahtijeva provjeru autentičnosti korisnika pomoću korisničkog imena i lozinke.
- Poslužitelj A predstavlja svoj certifikat za pokretanje SSL sesije kad Klijenti B i C pristupaju aplikaciji za izračun tečajeva.
- Nakon inicijaliziranja SSL sesije, Poslužitelj A zahtijeva da Klijenti B i C predoče važeće ime i lozinku korisnika prije nego što dozvoli pristup do aplikacije.

Sistemi klijenta agenta – Klijent B i Klijent C
- Klijenti B i C su nezavisni agenti koji pristupaju aplikaciji za izračunavanje rata.
- Klijentski softver klijenata B i C ima instaliranu kopiju dobro poznatih CA certifikata koji su izdali certifikat aplikacije.
- Klijenti B i C pristupaju aplikaciji za izračun tečajeva na Poslužitelju A, koji predstavlja svoj certifikat njihovom klijentskom softveru radi provjere autentičnosti njegovog identiteta i početka SSL sesije.
- Klijentski softver na Klijentima B i C je konfiguriran za prihvat certifikata od Poslužitelja A radi inicijaliziranja SSL sesije.
- Nakon što SSL sesija počne, Klijenti B i C moraju dati važeće korisničko ime i lozinku prije nego što Poslužitelj A dozvoli pristup do aplikacije.

Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:
1. Aplikacija izračuna tečajeva na Poslužitelju A je generička aplikacija koja se može konfigurirati za upotrebu SSL-a. Većina aplikacija, uključujući mnoge poslužiteljske aplikacije osigurava SSL podršku. SSL koraci konfiguracije razlikuju se prilično među aplikacijama. Zbog toga, ovaj scenarij ne omogućuje specifične instrukcije

za konfiguriranje aplikacije za izračun omjera za upotrebu SSL-a. Ovaj scenarij 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 scenarij omogućuje instrukcije kako koristiti Upravitelj digitalnih certifikata (DCM) za konfiguriranje povjerenja za one aplikacije koje omogućuju ovu podršku. Zato što se koraci konfiguracije poprilično razlikuju među aplikacijama, ovaj scenarij ne pruža specifične instrukcije za konfiguriranje provjere autentičnosti certifikata klijenata za aplikaciju izračuna omjera.
3. Poslužitelj A zadovoljava zahtjeve za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).
4. Nitko prije nije konfigurirao niti koristio DCM na Poslužitelju A.
5. Svatko tko koristi DCM za izvođenje zadataka u ovom scenariju mora imati *SECADM i *ALLOBJ posebna ovlaštenja za svoj korisnički profil.
6. Poslužitelj A nema instaliran IBM kriptografički koprocesor.

Koraci konfiguracije

Za primjenu ovog scenarija morate izvesti ove zadatke na Poslužitelju A.

1. Dovršite planiranje radnih tablica
2. Izvedite sve preduvjetne korake za instalaciju i konfiguriranje svih potrebnih proizvoda
3. Koristite Upravitelja digitalnih certifikata (DCM) da kreirate zahtjev za certifikatom poslužitelja
4. Konfigurirajte aplikaciju za upotrebu Sloja sigurnih utičnica (SSL)
5. Koristite DCM da importirate i dodijelite potpisani certifikat poslužitelja ili klijenta ID-u aplikacije za vašu aplikaciju
6. Pokrenite aplikaciju u SSL modu, ako je potrebno
7. **Opcijski**. Koristite DCM da definirate CA listu povjerenja da omogućite provjeru autentičnosti klijenta na osnovu certifikata za aplikacije koje omogućuju ovu podršku

Bilješka: Situacija koju ovaj scenarij opisuje ne zahtijeva da aplikacija za izračun rate 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 scenarij opisuje.

Korak 1: Dovršite planiranje radnih tablica

Sljedeće radne tablice za planiranje pokazuju informacije koje trebate sakupiti i odluke koje trebate učiniti da pripremite implemenataciju digitalnog certifikata koje ovaj scenarij opisuje. Da osigurate uspješnu implementaciju, trebate biti u mogućnosti odgovoriti Yes na sve stavke preduvjeta i trebate sakupiti sve zahtijevane informacije prije nego izvedete bilo koji od zadataka konfiguracije.

Tablica 1. Planiranje radne tablice za preduvjete implementacije certifikata

Radna tablica za preduvjete	Odgovori
Da li je vaš OS/400 V5R2 (5722-SS1), ili kasnija verzija?	Yes
Da li je dobavljač kriptografičkog pristupa (5722-AC3) instaliran na vašem sistemu?	Da
Da li je opcija 34 OS/400 instalirana na vašem sistemu?	Yes

Tablica 1. Planiranje radne tablice za preduvjete implementacije certifikata (nastavak)

Radna tablica za preduvjete	Odgovori
Da li je IBM HTTP Poslužitelj za iSeries (5722–DG1) instaliran na vašem sistemu i pokrenuta instanca Administrativnog poslužitelja?	Yes
Da li je TCP konfiguriran za vaš sistem tako da možete koristiti Web pretražitelj i instancu Administrativni poslužitelj HTTP Poslužitelja za pristup DCM-u?	Yes
Da li imate *SECADM i *ALLOBJ posebna ovlaštenja?	Yes

Trebate sakupiti sljedeće informacije o implementaciji vašeg digitalnog certifikata da izvedete sljedeće zadatke konfiguracije da dovršite implementaciju:

Tablica 2. Planiranje radne tablice za konfiguraciju implementacije certifikata

Radna tablica planiranja za Poslužitelj A	Odgovori
Da li ćete djelovati vašim vlastitim Lokalnim CA, ili ćete dobiti certifikate za vašu aplikaciju od javnog CA?	Postizanje certifikata s javnog CA
Da li je Poslužitelj A host za aplikacije koje želite omogućiti za SSL?	Da
Koje razlikovno ime ćete koristiti za zahtjev za potpisivanjem certifikata (CSR) za čije kreiranje koristite DCM? • **Veličina ključa**: određuje snagu kriptografičkih ključeva za certifikat. • **Oznaka certifikata**: identificira certifikat s jedinstvenim nizom znakova. • **Uobičajeno ime**: identificira vlasnika certifikata, kao što je osoba, entitet, ili aplikacija; dio DN Subjekta za certifikat. • **Jedinica organizacije**: identificira organizacijsku sekciju ili područje za aplikaciju koja će koristiti certifikat. • **Ime organizacije**: identificira vaše poduzeće ili odjelni dio za aplikaciju koja će koristiti certifikat. • **Lokacija ili grad**: identificira vaš grad, ili označavanje lokacija za vašu organizaciju. • **Država ili pokrajina**: identificira državu ili pokrajinu u kojoj ćete koristiti ovaj certifikat. • **Zemlja ili regija**: identificira, s dvoslovnom oznakom, zemlju ili regiju u kojoj ćete koristiti ovaj certifikat.	**Veličina ključa**: 1024 **Oznaka certifikata**: Myco_public_cert **Uobičajeno ime**: myco_rate_server@myco.com **Jedinica organizacije**: Rate dept **Ime organizacije**: myco **Lokacija ili grad**: Any_city **Država ili pokrajina**: Any **Zemlja ili regija**: ZZ
Što je ID aplikacije DCM-a za aplikaciju koju želite konfigurirati za upotrebu SSL-a?	myco_agent_rate_app
Da li ćete konfigurirati SSL-omogućenu aplikaciju za upotrebu certifikata za provjeru autentičnosti klijenta? Ako da, koje CA-ove želite dodati CA listi povjerenja aplikacije?	No

Korak 2: Izvedite preduvjetne zadatke za instalaciju svih potrebnih proizvoda

Morate izvesti sve preduvjetne zadatke za instalaciju i konfiguriranje svih potrebnih proizvoda prije nego što možete izvesti bilo koje specifične konfiguracijske zadatke za primjenu ovog scenarija.

Korak 3: Kreirajte zahtjev za certifikatom poslužitelja ili klijenta

Da započnete proces korištenja Sloja sigurnih utičnica (SSL) za zaštitu komunikacije podataka aplikacije kako scenarij 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. Pokrenite DCM.
2. U navigacijskom okviru DCM-a izaberite **Kreiranje novog spremišta certifikata** da dovršite vođeni zadatak i popunite seriju obrazaca. Ovi obrasci vas vode kroz postupak kreiranja spremišta 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 spremište certifikata za kreiranje i kliknite **Nastavak**.
4. Izaberite **Da** za kreiranje certifikata kao dijela kreiranja *SYSTEM spremišta certifikata i klikniteNastavak.
5. Izaberite **VeriSign ili drugog Internet izdavača certifikata (CA)** kao potpisnika novog certifikata i klikniteNastavak za prikaz obrasca koji vam omogućuje da popunite informacije o identifikaciji za novi certifikat.
6. Popunite obrazac i kliknite **Nastavak** za prikaz stranice certifikata. Stranica potvrde prikazuje podatke zahtjeva certifikata koje morate dostaviti javnom Izdavaču certifikata (CA) koji će izdati vaš certifikat. Podaci Zahtjeva za potpisivanjem certifikata (CSR) sastoje se od javnog ključa, razlikovnog imena i drugih informacija koje ste specificirali 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. **Opaska:** Kada izađete s ove stranice, podaci su izgubljeni i ne možete ih obnoviti.
8. Pošaljite obrazac molbe ili datoteku CA-u kojeg ste izabrali da izdaje i potpisuje vaše certifikate.
9. Čekajte da CA vrati potpisan, dovršen certifikat prije nego nastavite na sljedeći korak zadatka za ovaj scenarij.

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

Korak 4: Kofigurirajte aplikaciju za upotrebu SSL-a

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. Morate konfigurirate vašu aplikaciju za upotrebu SSL-a prije rada s vašim potpisanim certifikatom. Neke aplikacije, kao što je HTTP Poslužitelj za iSeries generiraju jedinstveni ID aplikacije i registriraju ID s 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 scenarij ne pretpostavlja specifični izvor za aplikaciju za izračunavanje rate koju opisuje jer postoji niz načina na koji MyCo, Inc. može omogućiti ovu aplikaciju njegovim klijentima.

| Da konfigurirate vašu aplikaciju da koristi SSL, slijedite instrukcije koje vaša dokumentacija za aplikaciju pruža.
| Također, možete više naučiti o konfiguriranju mnogih uobičajenih IBM aplikacija da koriste SSL pregledom Sloja
| sigurnih utičnica (SSL) u iSeries Informacijskom centru.

| Kada dovršite SSL konfiguraciju za vašu aplikaciju, možete konfigurirati potpisani javni certifikat za aplikaciju tako da
| može započinjati SSL sesije.

Korak 5: Importirajte i dodjelite potpisani javni certifikat

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

Da importirate vaš certifikat i dodijelite ga vašoj aplikaciji da dovrši proces konfiguriranja SSL-a izvedite ove korake:
1. Pokrenite DCM.

2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***SYSTEM** da se otvori spremište certifikata.
3. Kada se prikaže stranica **Spremište certifikata i Lozinka**, unesite lozinku koju ste specificirali za spremište certifikata kada ste ga kreirali i kliknite **Nastavak**.
4. Nakon osvježenja navigacijskog okvira izaberite**Upravljanje certifikatima** za prikaz popisa zadataka.
5. Iz popisa zadataka izaberite **Import certifikata** da započnete postupak importiranja potpisanog certifikata u *SYSTEM spremište certifikata.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
6. Iz popisa zadataka izaberite **Dodjela certifikata** iz liste zadataka **Upravljanja certifikatima** da prikažete listu certifikata u trenutnom spremištu certifikata.
7. Izaberite vaš certifikat s liste i kliknite **Dodjela aplikaciji** da prikažete listu definicija aplikacija za trenutno spremište certifikata.
8. Izaberite vašu aplikaciju s popisa i kliknite **Nastavak**. Prikazuje se stranica ili s porukom potvrde za vaš izbor dodjela ili s porukom 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 6: Pokrenite aplikaciju u SSL modu

Nakon što dovršite proces importiranja i dodjele certifikata vašoj aplikaciji, možda ćete trebati zaustaviti 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 izvodi. Pregledajte dokumentaciju za vašu aplikaciju da odredite trebate li ponovno pokrenuti aplikaciju ili zbog drugih specifičnih informacija o pokretanju aplikacije u SSL načinu.

Ako želite koristiti certifikate za provjeru autentičnosti klijenta, sada možete definirati CA listu povjerenja za aplikacije.

Korak 7 (Opcijski): Definirajte CA listu povjerenja za aplikaciju koja zahtijeva certifikate za provjeru autentičnosti klijenta

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

Situacija koju ovaj scenarij opisuje ne zahtijeva da aplikacija za izračun rate koristi certifikate za provjeru autentičnosti klijenta, ali da aplikacije budu u mogućnosti prihvatiti certifikate za provjeru autentičnosti kada su dostupni. Mnoge aplikacije omogućuju podršku certifikatu za provjeru autentičnosti klijenta; kako konfigurirate ovu podršku mijenja se u širokom rasponu među aplikacijama. 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. Pokrenite DCM.

2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***SYSTEM** da se otvori spremište certifikata.
3. Kada se prikaže stranica **Spremište certifikata i Lozinka**, unesite lozinku koju ste specificirali za spremište certifikata kada ste ga kreirali i kliknite **Nastavak**.
4. Nakon osvježenja navigacijskog okvira izaberite**Upravljanje certifikatima** za prikaz popisa zadataka.
5. Iz 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 jedan ili više CA certifikata s liste kojem će vaša aplikacija vjerovati i kliknite **Omogući** za prikaz liste aplikacija koje koriste CA listu povjerenja.
7. Izaberite aplikaciju s liste koja treba dodati izabrani CA njegovoj listi 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.

Scenarij: Upotreba certifikata za internu provjeru autentičnosti

Situacija

Vi ste mrežni administrator za poduzeće (MyCo, Inc.) čiji odjel za ljudske resurse 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 ovaj zahtjev kreiranjem interne Web stranice da omogući ove informacije zaposlenicima. Vi ste odgovorni za administriranje ove interne Web stranice koja radi na IBM HTTP poslužitelju za iSeries (upravljan s Apache-om).

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, vi tradicionalno radite provjeru autentičnosti korisnika pomoću korisničkog imena i lozinke za ograničenje pristupa podacima poduzeća. Zbog osjetljive i privatne prirode ovih podataka, shvatili ste da ograničenje pristupa njima koje se bazira na provjeri autentičnosti lozinke možda neće biti dovoljno. 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 resursa kojima mogu pristupiti.

Zbog toga ste odlučili da ćete postaviti privatnog Lokalnog Izdavača certifikata (CA) i izdavati certifikate svim zaposlenicima i pridruživati certifikate zaposlenika s njihovim korisničkim profilima. 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 dostupni samo određenim osobama.

Prednosti scenarija

Ovaj scenarij ima sljedeće prednosti:
- Upotrebom digitalnih certifikata za konfiguriranje SSL pristupa vašim ljudskim resursima Web poslužitelj osigurava da su informacije prenesene između poslužitelja i klijenta zaštićene i privatne.
- Korištenje digitalnih certifikata za provjeru ovlaštenja klijenta pruža sigurniji način identificiranja ovlaštenih korisnika.
- Upotreba *privatnih* digitalnih certifikata za ovlaštenje korisnika za vaše aplikacije i podatke praktičan je izbor pod ovim i sličnim uvjetima:
  - Zahtijevate visoki stupanj sigurnosti, posebno u odnosu na provjeru autentičnosti korisnika.
  - Vjerujete pojedincima kojima izdajete certifikate.
  - Vaši korisnici već imaju korisničke profile za kontrolu njihovog pristupa do aplikacija i podataka.

  - Želite raditi s vlastitim izdavačem certifikata (CA).
- Upotreba privatnih certifikata za provjeru autentičnosti klijenata vam omogućuje da lakše pridružite certifikate s ovlaštenim korisničkim profilima. Ovo pridruživanje certifikata profilu korisnika omogućava HTTP poslužitelju da odredi profil korisnika vlasnika certifikata za vrijeme provjere autentičnosti. HTTP Poslužitelj ih zatim može zamijeniti i izvoditi pod tim korisničkim profilom, ili izvesti akcije za tog korisnika bazirane na informacijama u korisničkom profilu.

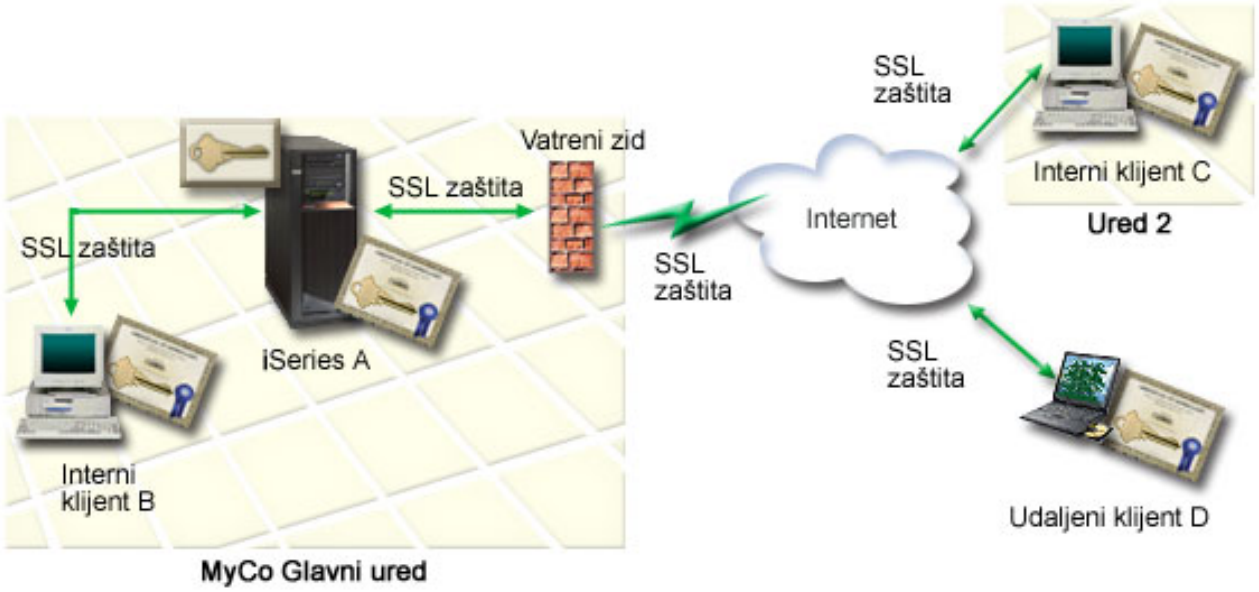
Objektivi

U ovom scenariju, MyCo, Inc. želi koristiti digitalne certifikate da zaštiti osjetljive osobne informacije koje dobavlja njihova interna Web stranica ljudskih resursa zaposlenicima poduzeća. Poduzeće također želi sigurniju metodu provjere autentičnosti onih korisnika kojima je dozvoljen pristup ovoj Web stranici.

Ciljevi ovog scenarija su sljedeći:
- Web stranica internih ljudskih resursa poduzeća mora koristiti SSL da zaštiti privatnost podataka koje omogućuje korisnicima.
- SSL konfiguracija mora biti popunjena s privatnim certifikatima od internog Lokalnog izdavača certifikata (CA).
- Ovlašteni korisnici moraju dobaviti važeći certifikat za pristup Web stranici ljudskih resursa u SSL modu.

Detalji

Sljedeća slika objašnjava mrežnu konfiguraciju za ovaj scenarij:



Slika prikazuje sljedeće informacije o situaciji za ovaj scenarij:

Web poslužitelj ljudskih resursa poduzeća – Poslužitelj A
- Poslužitelj A je poslužitelj koji je host za Web-baziranu aplikaciju ljudskih resursa poduzeća.
- Poslužitelj A se izvodi na OS/400 Verziji 5 Izdanje 2 (V5R2) ili kasnijoj verziji.
- Poslužitelj A ima instaliranog dobavljača kriptografičkog pristupa (5722–AC3).
- Poslužitelj A ima instalirane i konfigurirane Upravitelja digitalnih certifikata(OS/400 opcija 34) i IBM HTTP poslužitelj za iSeries (5722–DG1).
- Poslužitelj A izvodi aplikaciju ljudskih resursa, koja je konfigurirana na sljedeći način:
  - Zahtijeva SSL način.
  - Koristi privatni certifikat od Lokalnog Izdavača certifikata (CA) za SSL konfiguraciju.
  - Zahtijeva certifikate za provjeru autentičnosti klijenta.
- Poslužitelj A predstavlja svoj certifikat za pokretanje SSL sesije kad Klijenti B, C i D pristupaju aplikaciji.

- Nakon inicijaliziranja SSL sesije, Poslužitelj A zahtijeva da Klijenti B, C i D predoče važeće ime i lozinku korisnika prije nego što dozvoli pristup do aplikacije. 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 poduzeća gdje se nalazi i Poslužitelj 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 u poduzeću i mora biti u mogućnosti sigurno pristupiti Web stranici ljudskih resursa bez obzira na fizičku lokaciju.
- Klijenti B, C i D su zaposlenici poduzeća koji pristupaju aplikaciji ljudskih resursa.
- 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 resursa na Poslužitelju A, koji predstavlja svoj certifikat njihovom klijentskom softveru radi provjere autentičnosti njegovog identiteta i početka SSL sesije.
- Klijentski softver na Klijentima B, C i D je konfiguriran za prihvat certifikata od Poslužitelja A radi inicijaliziranja SSL sesije.
- Nakon što SSL sesija počne, Klijenti B, C i D moraju dati važeće korisničko ime i lozinku prije nego što Poslužitelj A dozvoli pristup do aplikacije.

Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:
1. IBM HTTP poslužitelj za iSeries (upravljan s Apache-om) izvodi aplikaciju ljudskih resursa na Poslužitelju A. Ovaj scenarij ne sadrži *specifične* upute za konfiguriranje HTTP poslužitelja za upotrebu SSL-a. Ovaj scenarij 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 scenarij omogućuje instrukcije kako koristiti Upravitelj digitalnih certifikata (DCM) za konfiguriranje zahtjeva za upravljanje certifikatom za ovaj scenarij. Ipak, ovaj scenarij ne pruža *specifične* korake konfiguracije za konfiguriranje provjere autentičnosti certifikata klijenta za HTTP poslužitelj.
3. HTTP poslužitelj ljudskih resursa na Poslužitelju A već koristi provjeru autentičnosti lozinke.
4. Poslužitelj A zadovoljava zahtjeve za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).
5. Nitko prije nije konfigurirao niti koristio DCM na Poslužitelju A.
6. Svatko tko koristi DCM za izvođenje zadataka u ovom scenariju mora imati *SECADM i *ALLOBJ posebna ovlaštenja za svoj korisnički profil.
7. Poslužitelj A nema instaliran IBM kriptografički koprocesor.

Koraci konfiguracije

Postoje dva skupa zadataka koje morate izvesti za primjenu ovog scenarija: Jedan skup zadataka vam omogućuje da postavite aplikaciju ljudskih resursa na Poslužitelju A za upotrebu SSL-a i za zahtijevanje certifikata za provjeru autentičnosti korisnika. Drugi skup zadataka dozvoljava vašim korisnicima na Klijentima B, C i D da sudjeluju u SSL sesijama s aplikacijom ljudskih resursa i dobivaju certifikate za provjeru autentičnosti korisnika.

Koraci zadatka za aplikaciju Web poslužitelja za ljudske resurse

Za primjenu ovog scenarija morate izvesti ove zadatke na Poslužitelju A.
1. Dovršite radne tablice za planiranje scenarija
2. Izvedite sve preduvjetne korake za instalaciju i konfiguriranje svih potrebnih proizvoda
3. Konfigurirajte HTTP Poslužitelj ljudskih resursa za upotrebu SSL-a i učinite zapis ID-a aplikacije za instancu poslužitelja
4. Koristite Upravitelja digitalnih certifikata (DCM) za kreiranje i rad s Lokalnim CA
5. Konfigurirajte provjeru autentičnosti klijenta za Web poslužitelj ljudskih resursa.
6. Pokrenite HTTP poslužitelj ljudskih resursa u SSL-u načinu .

Koraci zadatka konfiguracije klijenta

Za primjenu ovog scenarija svaki korisnik (Klijenti B, C i D) koji će pristupati Web poslužitelju ljudskih resursa na Poslužitelju A mora izvesti ove zadatke:

7. Instalirajte kopiju Lokalnog CA certifikata u softver njihovog pretražitelja
8. Zahtijevajte certifikat od Lokalnog CA

Detalji konfiguracije

Dovršite korake sljedećeg zadatka za upotrebu certifikata za konfiguraciju zaštićenog SSL pristupa internim aplikacijama i resursima i za provjeru autentičnosti korisnika kako opisuje ovaj scenarij.

Korak 1: Dovršite planiranje radnih tablica

Sljedeće radne tablice za planiranje pokazuju informacije koje trebate sakupiti i odluke koje trebate učiniti da pripremite implemenataciju digitalnog certifikata koje ovaj scenarij opisuje. Da osigurate uspješnu implementaciju, trebate biti u mogućnosti odgovoriti Yes na sve stavke preduvjeta i trebate sakupiti sve zahtijevane informacije prije nego izvedete bilo koji od zadataka konfiguracije.

Tablica 3. Planiranje radne tablice za preduvjete implementacije certifikata

Radna tablica za preduvjete	**Odgovori**
Da li je vaš OS/400 V5R2 (5722-SS1), ili kasnija verzija?	Yes
Da li je dobavljač kriptografičkog pristupa (5722-AC3) instaliran na vašem sistemu?	Da
Da li je opcija 34 OS/400 instalirana na vašem sistemu?	Yes
Da li je IBM HTTP Poslužitelj za iSeries (5722–DG1) instaliran na vašem sistemu i pokrenuta instanca Administrativnog poslužitelja?	Yes
Da li je TCP konfiguriran za vaš sistem tako da možete koristiti Web pretražitelj i instancu Administrativni poslužitelj HTTP Poslužitelja za pristup DCM-u?	Yes
Da li imate *SECADM i *ALLOBJ posebna ovlaštenja?	Da

Trebate sakupiti sljedeće informacije o implementaciji vašeg digitalnog certifikata da izvedete sljedeće zadatke konfiguracije da dovršite implementaciju:

Tablica 4. Planiranje radne tablice za konfiguraciju implementacije certifikata

Radna tablica planiranja za Poslužitelj A	**Odgovori**
Da li ćete djelovati vašim vlastitim Lokalnim CA, ili ćete dobiti certifikate za vašu aplikaciju od javnog CA?	Kreirajte Lokalni CA za izdavanje certifikata
Da li je Poslužitelj A host za aplikacije koje želite omogućiti za SSL?	Da

Tablica 4. Planiranje radne tablice za konfiguraciju implementacije certifikata (nastavak)

Radna tablica planiranja za Poslužitelj A	Odgovori
Koje razlikovno ime ćete koristiti za Lokalni CA? • **Veličina ključa**: određuje snagu kriptografičkih ključeva za certifikat. • **Ime Izdavača certifikata (CA)**: identificira CA i postaje uobičajeno ime za CA certifikat i DN Izdavatelja za certifikate koje CA izdaje. • **Jedinica organizacije**: identificira organizacijsku sekciju ili područje za aplikaciju koja će koristiti certifikat. • **Ime organizacije**: identificira vaše poduzeće ili odjelni dio za aplikaciju koja će koristiti certifikat. • **Lokacija ili grad**: identificira vaš grad, ili označavanje lokacija za vašu organizaciju. • **Država ili pokrajina**: identificira državu ili pokrajinu u kojoj ćete koristiti ovaj certifikat. • **Zemlja ili regija**: identificira, s dvoslovnom oznakom, zemlju ili regiju u kojoj ćete koristiti ovaj certifikat. • **Period valjanosti za Izdavača certifikata**: specificira broj dana za koji je certifikat Izdavača certifikata važeći	**Veličina ključa**: 1024 **Ime Izdavača certifikata (CA)**: Myco_CA@myco.com **Jedinica organizacije**: Rate dept **Ime organizacije**: myco **Lokacija ili grad**: Any_city **Država ili pokrajina**: Any **Zemlja ili regija**: ZZ **Period valjanosti Izdavača certifikata**: 1095
Želite li postaviti podatke politike za Lokalni CA da mu dozvolite da izda korisničke certifikate za provjeru autentičnosti klijenta?	Yes
Koje informacije za razlikovno ime ćete koristiti za certifikat poslužitelja koji izdaje Lokalni CA? • **Veličina ključa**: određuje snagu kriptografičkih ključeva za certifikat. • **Oznaka certifikata**: identificira certifikat s jedinstvenim nizom znakova. • **Uobičajeno ime**: identificira vlasnika certifikata, kao što je osoba, entitet, ili aplikacija; dio DN Subjekta za certifikat. • **Jedinica organizacije**: identificira organizacijsku sekciju ili područje za aplikaciju koja će koristiti certifikat. • **Ime organizacije**: identificira vaše poduzeće ili odjelni dio za aplikaciju koja će koristiti certifikat. • **Lokacija ili grad**: identificira vaš grad, ili označavanje lokacija za vašu organizaciju. • **Država ili pokrajina**: identificira državu ili pokrajinu u kojoj ćete koristiti ovaj certifikat. • **Zemlja ili regija**: identificira, s dvoslovnom oznakom, zemlju ili regiju u kojoj ćete koristiti ovaj certifikat.	**Veličina ključa**: 1024 **Oznaka certifikata**: Myco_public_cert **Uobičajeno ime**: myco_rate_server@myco.com **Jedinica organizacije**: Rate dept **Ime organizacije**: myco **Lokacija ili grad**: Any_city **Država ili pokrajina**: Any **Zemlja ili regija**: ZZ
Što je ID aplikacije DCM-a za aplikaciju koju želite konfigurirati za upotrebu SSL-a?	myco_agent_rate_app
Da li ćete konfigurirati SSL-omogućenu aplikaciju za upotrebu certifikata za provjeru autentičnosti klijenta? Ako da, koje CA-ove želite dodati CA listi povjerenja aplikacije?	Yes Myco_CA@myco.com

Korak 2: Izvedite preduvjetne zadatke za instalaciju svih potrebnih proizvoda

Morate izvesti sve preduvjetne zadatke za instalaciju i konfiguriranje svih potrebnih proizvoda prije nego što možete izvesti bilo koje specifične konfiguracijske zadatke za primjenu ovog scenarija.

Korak 3: Konfigurirajte HTTP Poslužitelj ljudskih resursa za upotrebu SSL-a

| Konfiguracija Sloja sigurnih utičnica (SSL) za HTTP poslužitelj ljudskih resursa (upravljan s Apache-om) na
| Poslužitelju A uključuje mnoštvo zadataka koji variraju zavisno o tome kako je trenutno konfiguriran vaš poslužitelj.

| Da konfigurirate poslužitelj za upotrebu SSL-a, izvedite ove korake:
| 1. Pokrenite sučelje Administracija HTTP Poslužitelja.
| 2. Za rad sa specifičnim HTTP poslužiteljem, izaberite kartice stranica **Upravljaj —> Svim poslužiteljima—> Svim HTTP Poslužiteljima** da pogledate listu svih konfiguriranih HTTP poslužitelja.
| 3. Izaberite odgovarajući poslužitelj s liste i kliknite **Upravljanje detaljima**.
| 4. U navigacijskom okviru izaberite **Sigurnost**.
| 5. Izaberite karticu **SSL s provjerom autentičnosti certifikata** na obrascu.
| 6. U **SSL** polju izaberite Omogućeno.
| 7. U polju **Ime aplikacije za certifikat poslužitelja**, specificirajte ID aplikacije po kojem je poznata ova instanca poslužitelja. Ili, možete izabrati jedan s popisa. Ovaj ID aplikacije je u obliku QIBM_HTTP_SERVER_[server_name], na primjer, QIBM_HTTP_SERVER_MYCOTEST. **Opaska:** Zapamtite ovaj ID aplikacije. Trebat ćete ga ponovno izabrati u DCM-u.

| Možete naučiti više o ukupno potrebnoj konfiguraciji za vaš HTTP Poslužitelj kod upotrebe SSL-a u poglavlju
| Informacija HTTP Poslužitelj za iSeries, posebno u primjeru zvanom Scenarij: JKL omogućuje zaštitu Sloja sigurnih
| utičnica (SSL) na njihovom HTTP Poslužitelju (pokretano Apache-om). Ovaj scenarij dobavlja sve korake zadatka za
| kreiranje virtualnog hosta i njegovo konfiguriranje da koristi SSL, uključujući sljedeće zadatke:
| 1. Postav virtualnog hosta baziranog na imenu.
| 2. Postav direktive Slušanja za virtualni host.
| 3. Postav direktorija virtualnog hosta.
| 4. Postav zaštite lozinke preko osnovne provjere autentičnosti.
| 5. Omogućavanje SSL-a za virtualni host

Za dodatne informacije o konfiguriranju oboje, trenutne i budućih verzija HTTP Poslužitelja za iSeries, pogledajte poglavlje HTTP Poslužitelj za iSeries.

| Kada dovršite konfiguraciju za HTTP Poslužitelj za upotrebu SSL-a, možete koristiti DCM da konfigurirate podršku
| certifikata koju trebate za provjeru autentičnosti SSL-a i klijenta.

Korak 4: Kreirajte i upravljajte Lokalnim CA

Nakon što konfigurirate HTTP poslužitelj ljudskih resursa da koristi sloj sigurnih utičnica (SSL), morate konfigurirati certifikat da bi ga poslužitelj koristio da inicira SSL. Na osnovi ciljeva za ovaj scenarij, izabrali ste kreiranje i rad s Lokalnim izdavačem certifikata (CA) za izdavanje certifikata poslužitelju.

Kada koristite Upravitelja 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. Ovo uključuje dodjelu certifikata koje Lokalni CA izdaje vašoj aplikaciji Web poslužitelja. Također, vi dodajete Lokalni CA listi povjerenja za aplikacije Web poslužitelja. 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 resursa, dovršite ove korake:
1. Pokrenite DCM.
2. U navigacijskom okviru DCM-a izaberite **Kreiranje 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. U upotrebi ovih obrazaca za izvođenje svih zadataka koje trebate za postav radnog Lokalnog Izdavača certifikata (CA), izvodite sljedeće korake:
   a. Dajete informacije 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. Birate 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. Birate aplikacije koje mogu koristiti poslužiteljski ili klijentski certifikat za SSL veze.

      Bilješka: Budite sigurni da ste izabrali ID aplikacije za vaš HTTP poslužitelj ljudskih resursa.
   f. Koristite novi Lokalni CA da izdate certifikat potpisivanja objekata koje vaše aplikacije mogu koristiti za digitalno potpisivanje objekata. Ovaj podzadatak kreira *OBJECTSIGNING spremište certifikata; to je spremište certifikata koje koristite za upravljanje certifikatima za potpisivanje objekata.

      Bilješka: Iako ovaj scenarij ne koristi certifikate potpisivanja objekata, obavezno dovršite ovaj korak. Ako izvedete opoziv u ovom trenutku zadatka, zadatak završava i vi morate izvesti zasebne zadatke da dovršite vašu konfiguraciju SSL certifikata.
   g. Birate aplikacije koje će vjerovati Lokalnom CA.

      Bilješka: Uvjerite se da ste izabrali ID aplikacije za vaš HTTP Poslužitelj ljudskih resursa, na primjer, QIBM_HTTP_SERVER_MYCOTEST, kao jedna od aplikacija koja daje povjerenje Lokalnom CA.

Kada dovršite konfiguraciju certifikata koju zahtijeva aplikacija vašeg Web poslužitelja za upotrebu SSL-a, možete konfigurirati Web poslužitelj da zahtijeva certifikate za provjeru autentičnosti korisnika.

Korak 5: Konfigurirajte provjeru autentičnosti klijenta za Web poslužitelj ljudskih resursa

Morate konfigurirati općenite postavke provjere autentičnosti za HTTP Poslužitelj kada specificirate da HTTP Poslužitelj zahtijeva certifikate za provjeru autentičnosti. Konfigurirate ove postavke u istom obliku sigurnosti koji ste koristili za konfiguriranje poslužitelja za upotrebu Sloja sigurnih utičnica (SSL).

Da konfigurirate poslužitelj da zahtijeva certifikate za provjeru autentičnosti klijenta, izvedite ove korake:
1. Pokrenite sučelje Administracija HTTP Poslužitelja.
2. Za rad sa specifičnim HTTP poslužiteljem, izaberite kartice stranica **Upravljaj —> Svim poslužiteljima—> Svim HTTP Poslužiteljima** da pogledate listu svih konfiguriranih HTTP poslužitelja.
3. Izaberite odgovarajući poslužitelj s liste i kliknite **Upravljanje detaljima**.
4. U navigacijskom okviru izaberite **Sigurnost**.
5. Izaberite karticu **Provjera autentičnosti** na obrascu.
6. Izaberite **Koristi OS/400 profil klijenta**.
7. U polju **Ime provjere autentičnosti ili područje**, specificirajte ime za područje provjere autentičnosti.
8. Izaberite Omogućeno za polje **Zahtjevi obrade upotrebom ovlaštenja klijenta** i kliknite **Primijeni**.
9. Izaberite karticu **Kontroliraj pristup** na obrascu.
10. Izaberite **Svi korisnici provjerene autentičnosti (važeće korisničko ime i lozinka)** i kliknite **Primijeni**.
11. Izaberite karticu **SSL s Provjerom autentičnosti certifikata** na obrascu.
12. Osigurajte da je Omogućeno izabrana vrijednost u **SSL** polju.
13. U polju **Ime aplikacije za certifikat poslužitelja**, osigurajte da je specificirana ispravna vrijednost, na primjer, QIBM_HTTP_SERVER_MYCOTEST.
14. Izaberite **Prihvati certifikat klijenta ako je dostupan prije povezivanja**. Kliknite OK.

Možete naučiti više o ukupno potrebnoj konfiguraciji za vaš HTTP Poslužitelj kod upotrebe SSL-a u poglavlju Informacija HTTP Poslužitelj za iSeries, posebno u primjeru zvanom Scenarij: JKL omogućuje zaštitu Sloja sigurnih utičnica (SSL) na njihovom HTTP Poslužitelju (pokretano Apache-om). Ovaj scenarij pruža sve korake zadatka za kreiranje virtualnog hosta i konfiguriranje da koristi SSL.

Kada dovršite konfiguraciju provjere autentičnosti klijenta, možete ponovno pokrenuti HTTP Poslužitelj u SSL modu i započeti štititi privatnost podataka aplikacije za ljudske resurse.

Korak 6: Pokrenite Web poslužitelj ljudskih resursa u SSL modu

Možda ćete trebati zaustaviti i ponovno 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 (pokretan Apache-om), izvedite ove korake:
1. U **iSeries Navigatoru** proširite vaš poslužitelj.
2. Proširite **Mreža > Poslužitelji > TCP/IP > HTTP Administracija**.
3. Kliknite **Pokreni** da pokrenete sučelje Administracija HTTP Poslužitelja.
4. Kliknite karticu **Upravljaj** da pogledate listu svih konfiguriranih HTTP poslužitelja.
5. Izaberite odgovarajući poslužitelj s liste i kliknite **Zaustavi** ako je poslužitelj u izvođenju.
6. Kliknite **Pokreni** da ponovno pokrenete poslužitelj. Uputite se na online pomoć za više informacija o parametrima pokretanja.

Za dodatne informacije o upravljanju trenutnim i budućim verzijama HTTP Poslužitelja za iSeries (original ili pokretan s Apache-om), pogledajte poglavlje HTTP Poslužitelj za iSeries.

Prije nego korisnici mogu pristupiti Web aplikaciji za ljudske resurse, najprije moraju instalirati kopiju Lokalnog CA certifikata u softver njihovog pretražitelja.

Korak 7: Neka korisnici instaliraju kopiju Lokalnog CA certifikata u softver njihovog 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 predstavi certifikat od javnog Internet CA, pretražitelj korisnika ili drugi softver klijenta mora 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. 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 opciju za instaliranje certifikata. Ova opcija spušta Lokalni CA certifikat kao pouzdano ishodište u vašem pretražitelju. Ovo osigurava da vaš pretražitelj može postaviti sesiju sigurnih komunikacija s Web poslužiteljima koji koriste certifikat od ovog CA. Vaš pretražitelj će prikazati seriju prozora da vam pomogne dovršiti instalaciju.
4. Kliknite **OK** za vraćanje na početnu stranicu Upravitelj digitalnih certifikata.

Sada kada korisnici mogu pristupiti Web poslužitelju ljudskih resursa u SSL modu, ovi korisnici moraju biti u mogućnosti predstaviti odgovarajući certifikat za provjeru autentičnosti na poslužitelju. Zbog toga, oni moraju dobiti korisnički certifikat od Lokalnog CA.

Korak 8: Neka svaki korisnik zatraži certifikat od Lokalnog CA

U ranijim koracima konfigurirali ste Web poslužitelj za ljudske resurse da zatražite certifikate za provjeru autentičnosti korisnika. Sada korisnici moraju pokazati važeći certifikat od Lokalnog CA prije nego im se dozvoli pristup Web

poslužitelju. Svaki korisnik mora koristiti Upravitelja digitalnih certifikata (DCM) da dobije certifikat upotrebom zadatka **Kreiranje certifikata**. Da bi dobio certifikat od Lokalnog CA, politika Lokalnog CA mora dozvoliti da CA izda certifikate korisnika.

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

1. Pokrenite DCM.
2. U navigacijskom okviru izaberite **Kreiranje certifikata**.
3. Izaberite **Korisnički certifikat** kao tip certifikata za kreiranje. Prikazuje se obrazac tako da možete unijeti informacije o identifikaciji za certifikat.
4. Popunite obrazac i kliknite **Nastavak**.

   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 s 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.

Za vrijeme obrade, Upravitelj digitalnih certifikata automatski pridružuje certifikat s vašim korisničkim profilom.

S dovršenim ovim zadacima, samo ovlašteni korisnici s važećim certifikatom mogu pristupiti podacima s Web poslužitelja za ljudske resurse i ti su podaci zaštićeni za vrijeme prijenosa SSL-om.

Poglavlje 5. Koncepti digitalnog certifikata

Prije nego započnete upotrebu digitalnih certifikata da poboljšate politiku sigurnosti vašeg sistema i mreže, trebate razumjeti što su oni zapravo i koje prednosti sigurnosti omogućavaju.

Digitalni certifikat je digitalna vjerodajnica koja provjerava valjanost identiteta vlasnika certifikata, slično kao putovnica. Informacije o identifikaciji koje omogućuje digitalni certifikat poznate su kao razlikovno ime subjekta. Stranka od povjerenja, zvana Izdavač certifikata (CA), izdaje digitalne certifikate korisnicima ili organizacijama. Povjerenje u CA je osnova povjerenja u certifikat kao valjanu vjerodajnicu.

Digitalni certifikat također sadrži javni ključ koji je dio para javnih-privatnih ključeva. Niz funkcija sigurnosti pouzdaje se na upotrebu digitalnih certifikata i njima pridruženih parova ključeva. Možete koristiti digitalne certifikate da konfigurirate sesije Sloja sigurnih utičnica (SSL) da osigurate privatne, sigurne komunikacijske sesije između korisnika i vaših poslužiteljskih aplikacija. Možete proširiti ovu sigurnost konfiguriranjem mnogih SSL-omogućenih aplikacija da zahtijevaju certifikate umjesto korisničkih imena i lozinki za sigurniju provjeru autentičnosti korisnika.

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

Proširenja certifikata
Pročitajte ove informacije da naučite što su polja proširenja certifikata i kako se koriste.

Obnavljanje certifikata
Pročitajte ove informacije da naučite više o procesu koji DCM koristi za obnavljanje certifikata poslužitelja i klijenta i certifikata za potpisivanje objekta.

Razlikovno ime
Pročitajte ove informacije da naučite više o karakteristikama 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 naučite više o ključevima sigurnosti pridruženim digitalnim certifikatima.

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

Lokacije Liste opozvanih certifikata (CRL)
Pročitajte ove informacije da naučite što je Lista opozvanih certifikata (CRL) i kako se one koriste u postupku provjere valjanosti i provjere autentičnosti certifikata.

Spremišta certifikata
Pročitajte ove informacije da naučite što je spremište certifikata i kako treba koristiti Upravitelja digitalnih certifikata da se radi s njima i certifikatima koje ona sadrže.

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

IBM Kriptografički koprocesori za iSeries
Pročitajte ove informacije da naučite kako možete koristiti DCM i IBM Kriptografičke koprocesore za sigurniju pohranu ključeva.

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

Definicije aplikacija
Pročitajte ove informacije da naučite što su definicije DCM aplikacija i kako raditi s njima za SSL konfiguriranje i potpisivanje objekta.

Validacija
Pročitajte ove informacije da naučite kako radi proces validacije za aplikacije i certifikate u DCM-u.

Proširenja certifikata

Proširenja certifikata su polja za informacije koja daju dodatne informacije o certifikatu. Proširenja certifikata daju sredstva za proširenje originalnih informacijskih standarda X.509 certifikata. Dok su informacije za neka proširenja dobavljena za proširenje informacija o identifikaciji certifikata, druga proširenja daju informacije o kriptografičkim sposobnostima certifikata.

Ne koriste svi certifikati polja proširenja za proširenje razlikovnog imena i druge informacije. Broj i tip polja proširenja koje certifikat koristi mijenjaju se između Izdavača certifikata (CA) koji izdaju certifikate.

Na primjer, Lokalni CA koji dobavlja Upravitelj digitalnih certifikata (DCM) dozvoljava vam upotrebu samo proširenja certifikata Alternativno Ime Subjekta. Ova proširenja dozvoljavaju vam da pridružite certifikat sa specifičnom IP adresom, potpuno kvalificiranim imenom domene, ili adresom e-pošte. Ako namjeravate koristiti certifikat za identifikaciju krajnje točke veze Virtualne privatne mreže (VPN), morate navesti informacije za te ekstenzije.

Obnavljanje certifikata

Proces obnavljanja certifikata koje koristi Upravitelj digitalnih certifikata (DCM) mijenja se na osnovu tipa Izdavača certifikata (CA) koji je izdao certifikat.

Ako koristite Lokalni CA za potpisivanje obnovljenog certifikata, DCM koristi informacije koje dobavite za kreiranje novog certifikata u trenutnom spremištu certifikata i zadržava prethodni certifikat.

Ako koristite dobro poznati Internet CA za izdavanje certifikata, možete rukovati obnavljanjem certifikata na jedan od dva načina: importiranjem obnovljenog certifikata iz datoteke koju dobijete od CA koji potpisuje, ili možete prepustiti DCM-u da kreira novi javni-privatni par ključeva za certifikat. DCM omogućuje prvu opciju u slučaju da preferirate obnavljanje certifikata izravno s CA koji ga je izdao.

Ako izaberete kreiranje novog para ključeva, DCM rukuje obnavljanjem na isti način na koji je rukovao kreiranjem certifikata. DCM kreira novi par javnih-privatnih ključeva za obnovljeni certifikat i generira Zahtjev za potpisivanjem certifikata (CSR) koji se sastoji od javnog ključa i drugih informacija koje ste specificirali za novi certifikat. Možete koristiti CSR za zahtjev novog certifikata od VeriSign-a, ili bilo koji drugi javni CA. Jednom kada ste dobili potpisani certifikat od CA, koristite DCM da importirate certifikat u odgovarajuće spremište certifikata. Spremište certifikata zatim sadrži obje kopije certifikata, original i novo izdani obnovljeni certifikat.

Ako izaberete da DCM ne generira novi par ključeva, DCM vas vodi kroz proces importiranja obnovljenog, potpisanog certifikata u spremište certifikata iz postojeće datoteke koju ste dobili od CA. Importirani, obnovljeni certifikat zatim zamjenjuje prethodni ceritifikat.

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). Zbog toga, ako planirate prihvatiti upotrebu certifikata kao vjerodajnica, trebate pregledati zahtjeve za identifikacijom za CA da odredite da li njihovi zahtjevi odgovaraju vašim potrebama sigurnosti.

Razlikovno ime (DN) je termin koji opisuje identifikacijske informacije u certifikatu i dio su samog certifikata. Certifikat sadrži DN informacije za oboje, vlasnika ili zahtjevatelja certifikata (zvanog DN Subjekta) i za CA koji izdaje certifikat (zvanog DN Izdavatelj). Ovisno o politici identificiranja od CA, koji izdaje certifikat, DN može uključiti razne informacije. Možete koristiti Upravitelja digitalnih certifikata (DCM) za rad s 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
| • Lokacija ili grad
| • Država ili pokrajina
| • Zemlja ili regija

| Kada koristite DCM za izdavanje certifikata, možete koristiti proširenja certifikata da omogućite dodatne DN
| informacije za certifikat, uključujući:
| • Verzija 4 IP adresa
| • Potpuno kvalificirano ime domene
| • Adresa e-pošte

| Ove dodatne informacije korisne su vam 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 objekta omogućuje jedinstveno elektroničko vezivanje identiteta potpisivatelja (vlasnika ključa za potpis) na porijeklo 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 i5/OS aplikaciju koju želi distribuirati preko Interneta kao prikladno i jeftino sredstvo 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. Nekoliko poduzeća pruža komercijalne usluge za izdavanje certifikata korisnicima Interneta. Upravitelj digitalnih certifikata (DCM) dozvoljava vam da upravljate certifikatima od javnih CA i od privatnih CA.

Također, možete koristiti DCM za rad vašeg privatnog Lokalnog CA za izdavanje privatnih certifikata sistemima i korisnicima. Kad Lokalni CA izda korisnički certifikat, DCM automatski pridružuje certifikat korisničkom profilu na korisničkom sistemu ili drugom identitetu korisnika. Da li DCM pridružuje certifikat s korisničkim profilom ili s različitim korisničkim identitetom za korisnika ovisi o tome da li konfigurirate DCM za rad s Mapiranjem identiteta u poduzeću (EIM). 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 koristiti DCM da omogućite ili onemogućite status povjerenja za CA certifikat. 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

Kada kreirate Lokalnog Izdavača certifikata (CA) pomoću Upravitelja digitalnih certifikata, možete specificirati podatke o politici za Lokalni CA. Podaci o politici za lokalni CA opisuju privilegije potpisivanja koje ima. Podaci o politici određuju:
- Da li Lokalni CA može izdavati i potpisivati korisničke certifikate.
- Koliko dugo su važeći certifikati koje Lokalni CA izdaje.

Lokacije Liste opoziva certifikata (CRL)

Lista 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 izravno 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 informacije 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 za vrijeme 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 validacijskog postupka za certifikate, koje izdaje određeni CA .

Spremišta certifikata

Spremište certifikata je posebna datoteka baze podataka ključa koju Upravitelj digitalnih certifikata (DCM) koristi za pohranjivanje digitalnih certifikata. Spremište certifikata također sadrži privatni ključ certifikata, osim ako umjesto toga izaberete upotrebu IBM Kriptografičkog koprocesora za pohranu ključa. DCM vam omogućuje kreiranje i upravljanje s nekoliko tipova spremišta certifikata. DCM kontrolira pristup spremištima certifikata preko lozinki, zajedno s kontrolom pristupa direktoriju integriranog sistema datoteka i datoteka koje čine spremište certifikata.

Spremišta certifikata su klasificirana na temelju tipova certifikata koje sadrže. Zadaci upravljanja koje možete obaviti za svako spremište certifikata se mijenjaju ovisno o tipu certifikata kojeg sadrži spremište certifikata. DCM pruža sljedeća predefinirana spremišta certifikata koja možete kreirati i upravljati:

Lokalni Izdavač certifikata (CA)
DCM koristi ovo spremište certifikata za pohranu Lokalnog CA certifikata i njegovog privatnog ključa ako kreirate Lokalni CA. Možete koristiti certifikat u ovom spremištu certifikata da potpišete certifikate za čije izdavanje koristite Lokalni CA. Kada Lokalni CA izda certifikat, DCM stavlja kopiju CA certifikata (bez privatnog ključa) u odgovarajuće spremište certifikata (na primjer, *SYSTEM) u svrhu provjere autentičnosti. Aplikacije koriste CA certifikati za provjeru porijekla certifikata, koje moraju provjeriti kao dio SSL pregovora za dodjelu autorizacije resursima.

***SYSTEM**
DCM pribavlja ovo spremište certifikata za upravljanje poslužiteljevim ili klijentovim certifikatima koje koriste aplikacije za sudjelovanje u komunikacijskim sesijama Sloja sigurnih utičnica (SSL). IBM aplikacije (i mnoge aplikacije drugih razvijača softvera) su napisane za upotrebu certifikata samo u *SYSTEM spremištu certifikata. Kada koristite DCM za kreiranje Lokalnog CA, DCM kreira ovo spremište certifikata kao dio procesa. Kada izaberete dobivanje certifikata od javnog CA, kao VeriSign, za korištenje od vaših aplikacija poslužitelja ili klijenata, morate kreirati ovo spremište certifikata.

***OBJECTSIGNING**
DCM omogućuje ovo spremište certifikata za upravljanje certifikatima koje koristite za digitalno potpisivanje objekata. Također, zadaci u ovom spremištu 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 ovo spremište certifikata kao dio procesa. Kada izaberete dobivanje certifikata od javnog CA, kao VeriSign, za potpisivanje objekata, morate kreirati ovo spremište certifikata.

***SIGNATUREVERIFICATION**
DCM omogućuje ovo spremište 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. Spremište certifikata mora također sadržavati kopiju CA certifikata za CA koji je izdao certifikat potpisivanja objekta. Dobivate ove objekte ili eksportiranjem certifikata za potpisivanje objekata trenutnog sistema u spremište ili importiranjem certifikata koje primite od potpisnika objekta.

Spremište certifikata drugog sistema
Ovo spremište certifikata omogućuje alternativnu memorijsku lokaciju za poslužiteljeve ili klijentove certifikate koje koristite za SSL sesije. Druga sistemska spremišta certifikata su korisnički definirana sekundarna spremišta certifikata za SSL certifikate. Opcija Spremišta certifikata drugog sistema 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 spremište certifikata, a ne certifikata koji ste specifično identificirali. Najuobičajenije je da ovo spremište certifikata koristite kad premještate certifikate iz prethodnog izdanja DCM-a ili za kreiranje posebnog podskupa certifikata za SSL korištenje.

Bilješka: Ako imate instaliran IBM kriptografički koprocesor na vašem poslužitelju, možete izabrati opcije drugog spremišta privatnih ključeva za vaše certifikate (s izuzetkom certifikata za potpisivanje objekata). Možete pohraniti privatni ključ u sam koprocesor ili koprocesor upotrijebiti za šifriranje privatnog ključa i njegovo pohranjivanje u posebnu datoteku ključa umjesto u spremište certifikata.

DCM kontrolira pristup spremištima certifikata putem lozinki. DCM također održava kontrolu pristupa direktorija integriranog sistema datoteka i datoteka koje sačinjavaju spremišta certifikata. Lokalni izdavač certifikata (CA) i *SYSTEM, *OBJECTSIGNING i *SIGNATUREVERIFICATION spremišta certifikata moraju biti smješteni u posebnu stazu unutar integriranog sistema datoteka. Spremišta certifikata drugog sistema mogu biti smještena bilo gdje u integriranom sistemu datoteka.

Kriptografija

Kriptografija je znanost o čuvanju podataka na sigurnom. Kriptografija vam dopušta pohranjivanje informacija ili komunikaciju s drugim strankama sprečavajući da neovlaštene stranke razumiju pohranjene informacije ili da razumiju komunikacije. Šifriranje 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 s podijeljenim ili tajnim ključem (simetričan)** jedan ključ se tajno dijeli među dvije komunikacijske stranke. Šifriranje i dešifriranje koriste isti ključ.
- U **kriptografiji s javnim ključem (asimetrično)** šifriranje i dešifriranje koriste različite ključeve. Stranka ima par ključeva koji se sastoji od javnog i privatnog ključa. Javni ključ slobodno je distribuiran, uobičajeno unutar digitalnog certifikata, dok je privatni ključ držan u sigurnosti od strane vlasnika. 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 s 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.

IBM Kriptografički koprocesori za iSeries

Upotreba IBM kriptografičkih koprocesora dodaje izuzetno sigurne sposobnosti kriptografičkih obrada na vaš poslužitelj. Kriptografički koprocesor omogućuje dokazane kriptografičke usluge, osiguravajući privatnost i integritet, za razvijanje sigurnih e-business aplikacija.

Ako imate instaliran kriptografički koprocesor u stanju Varied on za vaš sistem, možete koristiti kriptografički koprocesor da omogućite sigurniju pohranu ključeva za vaše privatne ključeve za certifikat.

Možete koristiti kriptografički koprocesor da pohranite privatni ključ za certifikat poslužitelja ili klijenta i za lokalni certifikat Izdavača certifikata (CA). Ipak, ne možete koristiti kriptografički koprocesor za pohranu privatnog ključa za korisnički certifikat jer ovaj ključ mora biti pohranjen na sistem korisnika. Osim toga, u ovom trenutku ne možete koristiti koprocesor za pohranjivanje privatnog ključa za certifikat za potpisivanje objekta.

Možete ili pohraniti privatni ključ certifikata izravno u kriptografički koprocesor, ili možete koristiti glavni ključ kriptografičkog koprocesora da šifrirate ključ i pohranite ga u posebnoj datoteci za ključeve. Možete izabrati ove opcije pohrane ključeva kao dio procesa kreiranja ili obnavljanja certifikata. Ako koristite koprocesor za pohranjivanje certifikatovog privatnog ključa, možete promijeniti dodjelu koprocesora za taj ključ.

Za upotrebu kriptografičkog koprocesora za pohranu privatnog ključa, morate osigurati da je koprocesor u stanju Varied on prije upotrebe Upravitelja digitalnih certifikata (DCM). Inače, DCM ne omogućuje opciju za izbor memorijske lokacije kao dio kreacije certifikata, ili procesa obnavljanja.

Sloj sigurnih utičnica (SSL)

Sloj sigurnih utičnica (SSL), koji je izvorno proizveo Netscape, je industrijski standard za šifriranje 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.

Definicije aplikacija

Dva su tipa definicija aplikacija kojima možete upravljati u Upravitelju digitalnih certifikata (DCM):

- Definicije klijent ili poslužitelj aplikacija koje koriste sesije komunikacija Sloja sigurnih utičnica (SSL).
- Definicije aplikacija za potpisivanje objekta koje potpisuju objekte da osiguraju integritet objekta.

Da koristite DCM za rad s definicijama SSL aplikacija i njihovim certifikatima, aplikacija mora prvo biti registrirana s DCM-om kao definicija aplikacije tako da ima jedinstveni ID aplikacije. Razvijači aplikacija registriraju SSL-omogućene aplikacije upotrebom API-ja (QSYRGAP, QsyRegisterAppForCertUse) za automatsko kreiranje ID-a aplikacije u DCM-u. Sve IBM SSL-omogućene aplikacije se registriraju s DCM-om tako da možete lako koristiti DCM da im dodijelite certifikat i da onda one mogu uspostaviti SSL sesiju. Također, za aplikacije koje pišete ili kupite možete definirati definiciju aplikacije i kreirati ID aplikacije za nju unutar samog DCM-a. Morate raditi u *SYSTEM spremištu certifikata za kreiranje definicije SSL aplikacije za aplikaciju klijenta ili za 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 može opisivati tip ili grupu objekata koje namjeravate potpisati. Morate raditi u *OBJECTSIGNING spremištu certifikata da bi kreirali definiciju aplikacije za potpisivanje objekta.

Provjera valjanosti

Upravitelj digitalnih certifikata (DCM) omogućuje zadatke koji vam dozvoljavaju da provjerite valjanost certifikata ili aplikacije za provjeru raznih svojstava koja svaki od njih mora imati.

Provjera valjanosti certifikata

Kada provjeravate certifikat, Upravitelj digitalnih certifikata (DCM) verificira broj stavki koje pripadaju certifikatu da 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 Listi opozvanih certifikata (CRL) kao opozvan, ako postoji CRL lokacija za CA koji je izdao certifikat. DCM također provjerava da je CA certifikat za izdavajućeg CA u trenutnom spremištu certifikata i da je CA certifikat označen kao povjerljiv. Ako certifikat ima privatni ključ (na primjer, certifikati klijenta ili poslužitelja, ili za potpisivanje objekta), tada DCM također ispituje valjanost para javnih-privatnih ključeva da osigura da se par javnih-privatnih ključeva podudara. Drugim riječima, DCM šifrira podatke s javnim ključem i tada jamči da se podaci mogu dešifrirati s privatnim ključem.

Provjera valjanosti aplikacije

Kada ispitujete valjanost aplikacije, Upravitelj digitalnih certifikata (DCM) verificira da postoji dodjela certifikata za aplikaciju i osigurava 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 specificira da se pojavljuje obrada Liste opozvanih certifikata (CRL) i da postoji definirana CRL lokacija za CA, DCM provjerava CRL kao dio procesa provjere valjanosti.

Provjera valjanosti može pomoći i upozoriti vas na potencijalne probleme koje aplikacija može imati kada izvodi funkciju koja zahtijeva certifikate. Takvi problemi mogu spriječiti aplikaciju od sudjelovanja u sesiji Sloja sigurnih utičnica (SSL), ili u uspješnom potpisivanju objekata.

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.

Razmatranja o backupu i obnavljanju za DCM podatke
Pročitajte ovo da naučite kako osigurati da su važni DCM podaci dodani vašem planu backupa i obnavljanja za vaš sistem.

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 izabrati 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 i Mapiranje identiteta u poduzeću (EIM)
Koristite ove informacije da naučite više o upotrebi DCM-a zajedno s EIM-om.

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

Zahtjevi za DCM postav

Upravitelj digitalnih certifikata (DCM) je besplatni dodatak koji vam omogućuje 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 ovaj proizvod prije nego možete kreirati certifikate.
- Instalirajte opciju 34 od i5/OS. Ovo je DCM funkcija osnovana na pretražitelju.
- Instalirajte IBM HTTP Poslužitelj za iSeries (5722–DG1) i pokrenite instancu Administrativnog poslužitelja.
- Osigurajte da je TCP konfiguriran za vaš sistem tako da možete koristiti Web pretražitelj i instancu Administrativnog poslužitelja HTTP Poslužitelja za pristup DCM-u.

Bilješka: Nećete 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.

Razmatranja o kopiranju i obnavljanju za DCM podatke

Lozinke baze podataka šifriranih ključeva koje koristite za pristup spremištima certifikata u Upravitelju digitalnih certifikata (DCM) se spremaju ili *skrivaju* u posebnoj sigurnosnoj datoteci na vašem poslužitelju. Kada koristite DCM za kreiranje spremišta certifikata na vašem sistemu, DCM automatski skriva lozinku za vas. Ipak, trebate ručno osigurati da DCM skriva lozinke za spremište certifikata pod određenim okolnostima.

Primjer za jedan takav slučaj je kad koristite DCM za kreiranje certifikata za drugi poslužitelj i izaberete upotrebu datoteka certifikata na ciljnom sistemu za kreiranje novog spremišta certifikata. U ovoj situaciji, trebate otvoriti novo kreirano spremište certifikata i koristiti zadatak **Promjena lozinke** za promjenu lozinke za spremište certifikata na ciljnom sistemu, što osigurava da DCM pohranjuje novu lozinku. Ako je spremište certifikata Spremište certifikata drugog sistema, trebate također specificirati da želite koristiti opciju **Auto prijava** kada mijenjate lozinku. Da naučite više o upotrebi DCM-a za kreiranje certifikata za druge poslužitelj pogledajte Upotreba Lokalnog CA za izdavanje certifikata drugim poslužiteljima.

Dodatno, morate specificirati opciju **Auto prijava** kad god želite promijeniti ili resetirati lozinku za Spremište certifikata drugog sistema.

Da osigurate da imate potpun backup kritičnih DCM podataka, morate napraviti sljedeće:

- Koristite naredbu spremanja (SAV) da spremite sve .KDB i .RDB datoteke. Svako DCM spremište certifikata uključuje dvije datoteke, jednu s .KDB ekstenzijom i jednu s .RDB ekstenzijom.
- Koristite naredbu Spremanje sistema (SAVSYS) i naredbu Spremanje podataka sigurnosti (SAVSECDTA) da spremite datoteke posebne sigurnosti koje sadrže ključne lozinke baze podataka za pristup spremištu certifikata. Za vraćanje DCM datoteke za sigurnost lozinke, koristite naredbu vrati korisničke profile (RSTUSRPRF) i specificirajte *ALL za opciju korisničkog profila (USRPRF).

Drugo razmatranje obnavljanja tiče se upotrebe operacije SAVSECDTA i mogućnosti da trenutne lozinke za spremište certifikata postanu nesinkronizirane s lozinkama u sigurnosnoj datoteci za spremljene DCM lozinke. Ako primijenite lozinku za spremište certifikata nakon što izvedete operaciju SAVSECDTA, ali prije nego vratite podatke iz te operacije, trenutna lozinka spremišta certifikata biti će nesinkronizirana s onom u vraćenoj datoteci.

Da izbjegnete ovu situaciju, morate koristiti zadatak **Promjena lozinke** (pod **Upravljanje spremištem certifikata** u navigacijskom okviru) u DCM-u da promijenite lozinke spremišta certifikata nakon što vratite podatke iz operacije SAVSECDTA, da osigurate da ćete vratiti lozinke natrag u stanje sinkroniziranosti. Ipak, u ovoj situaciji ne koristite gumb **Resetiraj lozinku** koji se prikazuje kada izaberete otvaranje spremišta certifikata. Kada pokušate resetirati lozinku, DCM pokušava dohvatiti skrivenu lozinku. Ako skrivena lozinka nije u sinkronizirana s trenutnom lozinkom, operacija resetiranja neće uspjeti. Ako ne mijenjate često lozinke za spremište certifikata, možda ćete htjeti razmotriti izvođenje SAVSECDTA svaki put kada promijenite ove lozinke da osigurate da uvijek imate najnoviju skrivenu verziju lozinki spremljenu u slučaju da ikad zatrebate vratiti ove podatke.

Tipovi digitalnih certifikata

Postoji nekoliko klasifikacija digitalnih certifikata. Te klasifikacije opisuju kako se certifikat koristi. Upravitelja digitalnih certifikata (DCM) možete koristiti za upravljanje 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. Lokalni CA kojim kreirate i upravljate Upraviteljem digitalnih certifikata nezavisna je cjelina. Drugi mogu koristiti javni ključ CA certifikata za provjeru autentičnosti certifikata koje CA izdaje i potpisuje. Za upotrebu certifikata za SSL, potpisivanje objekata, ili provjeru potpisa objekata, morate također imati kopiju izdanih CA certifikata.

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 digitalni certifikat 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 spremišta 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 Sistemu integriranih datoteka i *CMD objekata. 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 spremišta 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 s certifikatom potpisivanja objekta. Provjera potpisa će vam dozvoliti da odredite porijeklo objekta i je li mijenjan od kada je potpisan. Možete upravljati ovim tipovima certifikata samo iz *SIGNATUREVERIFICATION spremišta 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 korisničke certifikate koje izdaje vaš privatni CA s korisničkim profilom. DCM možete također koristiti za pridruživanje korisničkih certifikata koje izdaje drugi Izdavač certifikata, s korisničkim profilom.

Kada koristite Upravitelja digitalnih certifikata (DCM) za upravljanje vašim certifikatima, DCM ih organizira i pohranjuje zajedno s njihovim privatnim ključevima u spremište certifikata na osnovu ovih klasifikacija.

Bilješka: Ako imate instaliran IBM kriptografički koprocesor na vašem poslužitelju, možete izabrati opcije drugog spremišta privatnih ključeva za vaše certifikate (s izuzetkom certifikata za potpisivanje objekata). Možete izabrati pohranu privatnog ključa na samom kriptografičkom koprocesoru. Ili, možete koristiti kriptografički koprocesor za šifriranje privatnog ključa i njegovu pohranu u posebnoj datoteci za ključeve umjesto u spremište 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 naspram privatnih certifikata

Jednom kada odlučite koristiti certifikate, trebate izabrati tip primjene certifikata koji najbolje odgovara vašim potrebama za sigurnošću. Izbori koje imate za dobivanje vaših certifikata uključuju:
- Kupnja vaših certifikata od javnog Internet izdavača certifikata (CA).
- Rad s vašim vlastitim Lokalnim CA za izdavanje certifikata za vaše korisnike i aplikacije.
- Upotreba kombinacije certifikata od javnih Internet CA-ova i vašeg osobnog Lokalnog CA.

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.

Upotreba javnih certifikata

Javni Internet CA-ovi izdaju certifikate svakom tko plati potrebnu pristojbu. Međutim, Internet CA zahtijeva još neki dokaz identiteta prije nego što izda certifikat. Ova razina dokaza se ipak mijenja, ovisno o politici identifikacije od CA. Trebate procijeniti da li strogost politike identifikacije CA odgovara vašim potrebama sigurnosti prije nego odlučite

dobiti certifikate od CA, ili dati povjerenje certifikatima koje on izdaje. Kako standardi Infrastrukture Javnog Ključa za X.509 (PKIX) napreduju, neki javni CA-ovi sada omogućuju standarde identifikacije veće strogosti 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 certifikate za ograničeni broj apliakcija i korisnika poslužitelja ili klijenta, trošak ne mora biti važan faktor za vas. Međutim, cijena može biti naročito važna ako imate veliki broj *privatnih* korisnika koji trebaju javne certifikate za provjeru autentičnosti klijenata. U ovom slučaju, trebate također razmotriti administrativno i programersko nastojanje potrebno za konfiguriranje poslužiteljskih aplikacija za prihvat samo specifičnog podskupa certifikata koje javni CA izdaje.

Upotreba 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, druga poduzeća i korisnici mogu prepoznavati i dati povjerenje certifikatima koje dobro poznati javni CA izdaje, više nego onima koje izdaje vaš privatni Lokalni CA.

Upotreba 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 vašeg vlastitog Lokalnog CA dozvoljava vam da izdate certifikate samo onim korisnicima koji su članovi od povjerenja u vašoj grupi. 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 cetifikata korisnicima za provjeru autentičnosti klijenta, trebate odlučiti gdje želite korisničke certifikate. Kada korisnici dobiju njihove certifikate od Lokalnog CA preko DCM-a, njihovi certifikati su po defaultu pohranjeni s korisničkim profilom. Ipak, možete konfigurirati DCM za rad s Mapiranjem korisničkog identiteta (EIM) tako da su njihovi certifikati pohranjeni u lokaciji Lightweight Directory Access Protocol (LDAP) umjesto u korisničkom profilu. (Pogledajte Digitalni certifikati i Mapiranje identiteta u poduzeću (EIM) za više informacija kako DCM i EIM rade zajedno.) Ako dajete prednost varijanti da korisnički certifikati nisu udruženi ili pohranjeni s korisničkim profilom na bilo koji način, možete koristiti API-je za programatsko izdavanje certifikata ne-iSeries korisnicima.

Bilješka: Bez obzira koji CA koristili za izdavanje vaših certifikata, sistemski administrator kontrolira kojim će CA-ovima biti dano povjerenje aplikacija na njegovom sistemu. Ako se u vašem pretražitelju nalazi kopija certifikata poznatoga CA, pretražitelj možete podesiti da vjeruje poslužiteljskim certifikatima koje je izdao taj CA. Administratori postavljaju povjerenje za CA certifikate u odgovarajućem DCM spremištu certifikata, koje sadrži kopije većine dobro poznatih javnih CA certifikata. Ipak, ako CA certifikat nije u vašem spremištu certifikata, vaš poslužitelj ne može vjerovati certifikatima korisnika ili klijenta koji su izdani od tog CA, sve dok ne dobijete i importirate kopiju CA certifikata. CA certifikat mora biti u ispravnom formatu datoteke i vi morate dodati taj certifikat vašem DCM spremištu certifikata.

Možda ćete ustanoviti da je korisno da pregledate neke uobičajene scenarije upotrebe certifikata kao pomoć u odluci da li vam korištenje javnih ili privatnih certifikata najbolje odgovara za vaš posao i sigurnost.

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 s privatnim CA opisuje zadatke koje morate izvesti ako odlučite raditi s Lokalnim CA za izdavanje privatnih certifikata.
- Upravljanje certifikatima od javnog Internet CA opisuje zadatke koje morate izvesti za korištenje certifikata od dobro poznatih javnih CA-ova, uključujući PKIX CA.

- Upotreba Lokalnog CA na drugim poslužiteljima opisuje zadatke koje morate izvesti ako želite koristiti certifikate od privatnog, lokalnog 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. Upotreba 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 identitet poslužitelja s kopijom izdanom od Izdavača certifikata (CA). (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 (javnog ključa) za vrijeme početne obrade SSL-a za pregovaranje simetričnog ključa koji se koristi za šifriranje i dešifriranje podataka aplikacije za tu određenu 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. Upravitelja digitalnih certifikata (DCM) možete također koristiti za pridruživanje korisničkog certifikata s tim profilom korisnika ili drugim korisničkim identitetom. Certifikat tada ima iste autorizacije i dozvole kao i pridruženi korisnički identitet ili korisnički profil. Alternativno, možete koristiti API-je za programatsko korištenje vašeg privatnog Lokalnog Izdavača certifikata za izdavanje certifikata ne-iSeries korisnicima. Ti API-ji osiguravaju mogućnost izdavanja privatnih certifikata korisnicima, kad ne želite da ti korisnici imaju korisnički profil ili drugi interni korisnički identitet.

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 s 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 u toku SSL sesije. Trenutno ove aplikacije osiguravaju podršku certifikata za provjeru autentičnosti klijenta:

- Telnet poslužitelj
- IBM HTTP Poslužitelj (pokretan s Apache-om)
- IBM Poslužitelj direktorija
- iSeries Access za Windows (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 (a ne korisnik) rukuju pristupom i predstavljanjem certifikata za provjeru autentičnosti. Na taj način je manje vjerojatno da korisnici dijele certifikate s 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 u toku obrade šifriranja i dešifriranja. Drugi mogu koristiti odgovarajući javni certifikatov ključ za provjeru identiteta odašiljatelja objekata, koji su potpisani s 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 s 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 poslužiteljskih aplikacija za upotrebu certifikata za provjeru autentičnosti klijenta za vrijeme neke SSL sesije pogledajte poglavlje Sloj sigurnih utičnica (SSL) u iSeries Informacijskom Centru.

Digitalni certifikati i Mapiranje identiteta u poduzeću (EIM)

Mapiranje identiteta u poduzeću (EIM) je eServer tehnologija koja dozvoljava da upravljate korisničkim identitetima u vašem poduzeću, uključujući korisničke profile i korisničke certifikate. Korisničko ime i lozinka najčešći su oblik korisničkog identiteta; certifikati su drugi oblik korisničkog identiteta. Neke aplikacije su konfigurirane tako da dozvoljavaju da se korisnicima provjerava autentičnost pomoću korisničkog certifikata, a ne pomoću korisničkog imena i lozinke.

Možete koristiti EIM za kreiranje mapiranja između korisničkih identiteta, što dozvoljava korisniku da izvede provjeru valjanosti s jednim korisničkim identitetom i pristupa resursima s drugim korisničkim identitetom bez dobavljanja potrebnog korisničkog identiteta od strane korisnika. Ovo postižete u EIM-u definiranjem udruženja između jednog korisničkog identiteta i drugog korisničkog identiteta. Korisnički identiteti mogu biti u različitim oblicima, uključujući korisničke certifikate. Možete kreirati pojedinačna udruženja između EIM identifikatora i različitih korisničkih identiteta koji pripadaju korisniku predstavljenom tim EIM identifikatorom. Ili, možete kreirati udruženja politika, koja mapiraju grupu korisničkih identiteta na pojedinačni ciljni korisnički identitet. Korisnički identiteti mogu biti u različitim oblicima, uključujući korisničke certifikate. Kada kreirate ova udruženja korisnički certifikati mogu biti mapirani na odgovarajuće EIM identifikatore, time čineći lakšim korištenje certifikata za upotrebu za provjeru valjanosti.

Da iskoristite ovo EIM svojstvo za upravljanje korisničkim certifikatima, trebate izvesti ove zadatke EIM konfiguracije prije izvođenja bilo kojeg zadatka DCM konfiguracije:

1. Koristite čarobnjaka **EIM Konfiguracije** u **iSeries Navigatoru** da konfigurirate EIM.
2. Kreirajte EIM identifikator za svakog korisnika za kojeg želite da sudjeluje u EIM-u.
3. Kreirajte ciljnu asocijaciju između svakog EIM identifikatora i tog korisničkog profila u lokalnom i5/OS korisničkom registru, tako da se svi certifikati koje korisnik dodijeli kroz DCM ili kreira u DCM-u mogu mapirati na korisnički profil. Koristite ime definicije EIM registra za za lokalni i5/OS korisnički registar koji ste naveli u čarobnjaku **EIM konfiguracije**. **Opaska:** Za više informacija o konfiguriranju EIM-a, pogledajte poglavlje EIM.

Nakon što dovršite potrebne zadatke EIM konfiguracije, morate koristiti zadatak **Upravljanje LDAP lokacijom** da konfigurirate Upravitelja digitalnih certifikata (DCM) za pohranu korisničkih certifikata u lokaciju Lightweight Directory Access Protocol (LDAP) umjesto s korisničkim profilom. Kada konfigurirate EIM i DCM za zajednički rad, zadatak **Kreiranje certifikata** za korisničke certifikate i zadatak **Dodjela korisničkog certifikata** obrađuju certifikate za EIM upotrebu, a ne za dodjelu certifikata korisničkom profilu. DCM pohranjuje certifikat u konfigurirani LDAP direktorij i koristi informacije o razlikovnom imenu certifikata (DN) za kreiranje izvornog pridruživanja za odgovarajući EIM identifikator. Ovo dozvoljava operacijskim sistemima i aplikacijama upotrebu certifikata kao izvora operacije pregledavanja EIM mapiranja za mapiranje s certifikata na ciljni korisnički identitet udružen s istim EIM identifikatorom.

Dodatno, kada konfigurirate EIM i DCM za zajednički rad, možete koristiti DCM za provjeru isteka korisničkog certifikata na poduzetničkoj razini umjesto samo na sistemskoj razini.

Digitalni certifikati za VPN veze

Digitalne certifikate možete koristiti za uspostavljanje veze virtualne privatne mreže (VPN). Obje krajnje točke dinamičke VPN veze moraju biti sposobne za međusobnu provjeru autentičnost prije aktiviranja veze. Provjera krajnjih točaka se radi 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.

Jedna metoda koju IKE poslužitelji mogu koristiti za međusobnu provjeru valjanosti je pred-dijeljeni ključ. Ipak, upotreba pred-dijeljenog ključa manje je sigurna jer morate komunicirati ovim ključem ručno s administratorom drugog kraja za vaš VPN. Prema tome, postoji mogućnost da ključ bude izložen drugim korisnicima za vrijeme procesa komunikacije s 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. Kada koristite Lokalni CA u DCM-u za izdavanje certifikata, možete specificirati informacije za alternativno ime subjekta za certifikat. Specificiranje ovih informacija osigurava da je vaša VPN veza kompatibilna s drugim VPN implementacijama koje mogu zahtijevati 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

i5/OS osigurava podršku za upotrebu certifikata za digitalno ″potpisivanje″ objekata. Digitalno potpisivanje objekata pruža način provjere cjelovitosti sadržaja objekta i izvora porijekla. Podrška potpisivanja objekata poboljšava tradicionalne sistemske alate za kontrolu toga 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. Upotreba digitalnih potpisa na objektima daje 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 s 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, primalac može izbjeći korištenje objekta i umjesto toga kontaktirati potpisnika da dobije drugu kopiju potpisanog objekta.

Ako odlučite da upotreba digitalnih potpisa odgovara vašim potrebama sigurnosti i politici, trebate procijeniti da li trebate koristiti javne certifikate, ili izdavati privatne certifikate. Ako namjeravate distribuirati objekte korisnicima u općenitoj publici, možda ćete razmotriti upotrebu certifikata s dobro poznatog Izdavača certifikata (CA) za potpisivanje objekata. Upotreba javnih certifikata osigurava da drugi mogu lako i jeftino provjeriti potpise koje stavljate na objekte koje im distribuirate. Međutim, ako 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 od 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 DCM za upravljanje certifikatima koje koristite za potpisivanje objekata i za provjeru potpisa objekata. Možete također koristiti DCM za potpisivanje objekata i provjeru potpisa objekata.

Digitalni certifikati za provjeru potpisa objekata

i5/OS osigurava podršku za upotrebu 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, primalac 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 provjere digitalnih potpisa, morate odlučiti kojem Izdavaču certifikata vjerujete i kojim certifikatima za potpisivanje objekata vjerujete. Kada date povjerenje Izdavaču certifikata (CA), možete izabrati da li dati povjerenje potpisima koje netko kreira upotrebom certifikata koje je izdao CA od povjerenja. 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 sa sistemskom vrijednosti nazvanom Provjera potpisa objekata za vrijeme vraćanja (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 izvedbene objekte koji se vraćaju, na nespremljene datoteke, ili na datoteke integriranog sistema datoteka. Da naučite više o upotrebi ove i drugih sistemskih vrijednosti, pogledajte Pronalaženje sistemske vrijednosti u iSeries 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. Konfiguriranje DCM-a

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 izravno u glavnom navigacijskom okviru, većina zadataka u navigacijskom okviru se organiziraju u kategorije. Na primjer, **Upravljanje certifikatima** je kategorija zadatka koja sadrži raznolikost individualno vođenih zadataka, kao što je Pogled na certifikat, Obnavljanje certifikata, Import certifikata i tako dalje. Ako je neka stavka u navigacijskom okviru kategorija, koja sadrži više od jednog zadatka, s njene lijeve strane se pojavljuje strelica. Ta strelica označava da kad izaberete vezu na tu kategoriju, pojavit će se proširena lista tako da možete birati zadatak koji ćete izvoditi.

S izuzetkom kategorije **Brze staze**, svaki zadatak u navigacijskom okviru je vođeni zadatak koji vas brzo i lako vodi kroz slijed koraka do završetka zadatka. Kategorija Brza staza omogućuje skupinu funkcija za upravljanje certifikatima i aplikacijama koji dopušta iskusnom DCM korisniku brzi pristup različitim srodnim zadacima iz centralnog skupa stranica.

Zadaci koji su dostupni u navigacijskom okviru se mijenjaju i ovise o spremištu certifikata u kojem radite. Kategorija i broj zadataka koje vidite u navigacijskom okviru također zavisi o ovlaštenjima koja ima vaš i5/OS korisnički profil. Svi zadaci za rad sa CA, upravljanje certifikatima koje koriste aplikacije i ostali zadaci na sistemskoj razini su dostupni samo 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:

Pokretanje DCM-a
Pročitajte ovo da naučite kako se pristupa dodatku Upravitelj digitalnih certifikata na vašem poslužitelju.

Postavljanje certifikata 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 s upravljanjem certifikatima od javnog Internet Izdavača certifikata (CA) ili kako da kreirate i koristite privatni Lokalni CA da izdaje certifikate.

Ako želite više poučnih informacija o upotrebi digitalnih certifikata u Internet okolini za poboljšanje sigurnosti vašeg sistema i mreže, VeriSign Web stranica odličan je resurs. VeriSign Web stranica dobavlja opsežnu knjižnicu poglavlja vezanih uz digitalne certifikate, kao i broj drugih subjekata vezanih uz Internet sigurnost. Možete pristupiti njihovoj knjižnici na VeriSign Help Desk  .

Pokretanje Upravitelja 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 kriptografički proizvod koji DCM koristi za generiranje javnog-privatnog para ključeva za certifikate, za šifriranje eksportiranih datoteka i dešifriranje importiranih datoteka certifikata.
2. Koristite iSeries Navigator za pokretanje Administrativnog poslužitelja HTTP poslužitelja:
   a. Pokrenite **iSeries Navigator**.
   b. Dva puta kliknite na vaš poslužitelj u glavnom pogledu stabla.

c. Proširite **Mreža > Poslužitelji > TCP/IP**.
d. Desno kliknite na **HTTP Administraciju**.
e. Kliknite **Pokreni**.
3. Pokrenite vaš Web pretražitelj.
4. Pomoću vašeg pretražitelja otiđite na okvir Zadaci na vašem sistemu na http://*your_system_name*:2001.
5. Izaberite **Upravitelj digitalnih certifikata** iz liste proizvoda na okviru Zadaci da bi pristupili do DCM korisničkog sučelja.

Postavljanje certifikata prvi put

Lijevi okvir Upravitelja digitalnih certifikata (DCM) je navigacijski okvir zadatka. Ovaj okvir možete koristiti za izbor vrlo različitih zadataka za upravljanje certifikatima i aplikacijama koje ih koriste. Koji zadaci su dostupni ovisi o tome s kojom pohranom certifikata radite (ako s ijednom) i o posebnim ovlaštenjima za vaš korisnički profil. Većina zadataka su dostupni samo ako imate *ALLOBJ i *SECADM posebna ovlaštenja. Za upotrebu DCM-a za provjeru potpisa objekata, vaš korisnički profil mora također imati *AUDIT posebno ovlaštenje.

Kada prvi put koristite Upravitelja digitalnih certifikata (DCM), ne postoje spremišta certifikata. Zbog toga, kada inicijalno pristupite DCM-u, navigacijsko okno prikazuje samo ove zadatke i samo ako imate potrebna posebna ovlaštenja:

- Upravljanje korisničkim certifikatima.
- Kreiranje novog spremišta certifikata.
- Kreiranje Izdavača certifikata(CA). (Opaska: Nakon što iskoristite ovaj zadatak za kreiranje privatnog Lokalnog CA, ovaj zadatak se više ne pojavljuje na listi.)
- Upravljanje CRL lokacijama.
- Upravljanje LDAP lokacijom.
- Upravljanje PKIX lokacijama za zahtjeve.
- Vratite se na okvir Zadaci.

Čak i ako spremišta certifikata već postoje na vašem sistemu (na primjer, migrirate iz ranije verzije DCM-a), DCM prikazuje samo ograničeni broj zadataka ili kategorija zadataka u lijevom navigacijskom oknu. Koje zadatke ili kategorije DCM prikazuje ovisi o spremištu certifikata (ako postoji) koje je otvoreno i o posebnim ovlaštenjima za vaš profil korisnika.

Morate najprije pristupiti odgovarajućem spremištu certifikata prije nego što počnete raditi s većinom zadataka upravljanja aplikacijama i certifikatima. Da otvorite određeno spremište certifikata, kliknite **Izbor spremišta certifikata** u navigacijskom okviru.

Navigacijski okvir DCM-a omogućuje također gumb **Sigurna veza** . Možete koristiti ovaj gumb za prikaz drugog prozora za pretraživanje upotrebom 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. Tada morate pokrenuti HTTP poslužitelj u sigurnom načinu. Ako niste konfigurirali i pokrenuli HTTP poslužitelj za SSL izvođenje, vidjet ćete poruku o greški 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 rad s Lokalnim CA za izdavanje certifikata vašim aplikacijama.

Upravljanje certifikatima od javnog Internet CA da koriste vaše aplikacije.

Kreiranje i rad s Lokalnim 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 rad s vašim vlastitim Lokalnim CA. DCM vam pribavlja stazu vođenog zadatka koji vas vodi kroz postupak kreiranja CA i njegovog korištenja za izdavanje certifikata za vaše aplikacije. Staza vođenog zadatka vam osigurava sve što trebate za početak korištenja digitalnih certifikata za konfiguriranje aplikacije za korištenje SSL-a i potpisivanje objekata i provjeru potpisa objekata.

Bilješka: Za upotrebu certifikata pomoću IBM HTTP Poslužitelja za iSeries, morate kreirati i konfigurirati vaš Web poslužitelj prije rada s DCM-om. Kada konfigurirate Web poslužitelj za upotrebu SSL-a, ID aplikacije generiran je za poslužitelj. Morate učiniti zapis ovog ID-a aplikacije tako da možete koristiti DCM za specificiranje koji će certifikat ova aplikacija koristiti za SSL.

Ne zaustavljajte i ponovno pokrećite poslužitelj dok ne koristite DCM za dodjelu certifikata poslužitelju. Ako završite i ponovno pokrenete *ADMIN instancu Web poslužitelja prije nego mu dodijelite certifikat, poslužitelj neće biti pokrenut i vi nećete biti u mogućnosti koristiti DCM za dodjelu certifikata poslužitelju.

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

1. Pokrenite DCM.
2. U navigacijskom okviru DCM-a izaberite **Kreiranje 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. Popunite sve obrasce u ovom vođenom zadatku. Kod korištenja ovih obrazaca za izvođenje svih zadataka koji su potrebni za postavljanje Lokalnog Izdavača certifikata (CA), vi:
   a. Birate kako ćete spremati privatni ključ za Lokalni CA certifikat. (Ovaj korak je osiguran samo ako imate instaliran IBM Kriptografički koprocesor na vašem iSeriesu. Ako vaš sistem nema kriptografički koprocesor, DCM automatski pohranjuje certifikat i njegov privatni ključ u spremište certifikata lokalnog izdavača certifikata (CA).)
   b. Dajete informacije 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. Birate 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 Kriptografički koprocesor, ovaj korak vam dozvoljava da izaberete kako pohraniti privatni ključ za certifikat poslužitelja ili klijenta. Ako vaš sistem nema koprocesor, DCM automatski postavlja certifikat i njegov privatni ključ u *SYSTEM spremište certifikata. DCM kreira *SYSTEM spremište certifikata kao dio ovog podzadatka.)
   f. Birate aplikacije koje mogu koristiti poslužiteljski ili klijentski certifikat za SSL veze.

      Bilješka: Ako ste ranije koristili DCM za kreiranje *SYSTEM spremišta 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 *OBJECTSIGNING spremište certifikata; to je spremište certifikata koje koristite za upravljanje certifikatima za potpisivanje objekata.
   h. Birate aplikacije koje mogu koristiti certifikat za potpisivanje objekata za stavljanje digitalnih potpisa na objekte.

      Bilješka: Ako ste ranije koristili DCM za kreiranje *OBJECTSIGNING spremišta certifikata da upravljate certifikatima za potpisivanje objekata od javnog Internet CA, nemojte izvoditi ovaj niti prethodni korak.
   i. Birate aplikacije koje će vjerovati vašem Lokalnom CA.

Kad završite vođeni zadatak tada imate sve što je potrebno za početak konfiguriranja vaše aplikacije za upotrebu SSL-a za sigurne komunikacije.

Nakon što konfigurirate vaše aplikacije, korisnici koji pristupaju aplikacijama kroz SSL vezu moraju koristiti DCM za dobivanje kopije Lokalnog CA certifikata. Svaki korisnik mora imati kopiju certifikata tako da ga softver klijenta korisnika može koristiti za provjeru valjanosti identiteta poslužitelja kao dio procesa SSL pregovora. 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 Lokalni 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, pročitajte ova poglavlja:

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

Upotreba API-ja 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 možda već posjeduje 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 s 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 prilikom predstavljanja certifikata imaju isti pristup i ograničenja za resurse kakve i njihov korisnički profil dodjeljuje ili odbija.

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 dodjelom certifikata korisničkih profila za vas ili za druge korisnike. Kad nije otvoreno nijedno spremište certifikata ili kad je otvoreno spremište certifikata Lokalnog izdavača certifikata (CA) tada možete izabrati **Upravljanje korisničkim certifikatima** u navigacijskom okviru za pristup odgovarajućim zadacima. Ako je otvoreno drukčije spremište certifikata, zadaci korisnika certifikata se integriraju u zadatke pod **Upravljanje 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 izborom zadatka **Kreiranje 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 ove informacije da naučite kako korisnici mogu koristiti Lokalni CA za izdavanje certifikata za provjeru autentičnosti klijenta.

Dodjela certifikata korisnika
Koristite ove informacije da naučite kako dodijeliti certifikat koji posjedujete vašem OS/400 korisničkom profilu ili drugom korisničkom identitetu. Certifikat može biti od privatnog Lokalnog CA na drugom sistemu ili od poznatog Internet CA. Prije nego dodijelite certifikat identitetu korisnika, u CA koji izdaje certifikat, poslužitelj mora imati povjerenje i certifikat ne smije već biti pridružen profilu korisnika ili drugom identitetu korisnika na sistemu.

| **Upravljanje korisničkim certifikatima pomoću isteka**
Koristite ove informacije da naučite kako upravljati korisničkim certifikatima na osnovu njihovih datuma isteka.

Kreiranje certifikata korisnika: Ako želite koristiti digitalne certifikate za provjeru identiteta korisnika, korisnici moraju imati certifikate. Ako koristite Upravitelja digitalnih certifikata (DCM) za rad s 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, izvedite ove korake:
1. Pokrenite DCM.
2. U navigacijskom okviru izaberite **Kreiranje certifikata**.
3. Izaberite **Korisnički certifikat** kao tip certifikata za kreiranje. Prikazuje se obrazac tako da možete unijeti informacije o identifikaciji za certifikat.
4. Popunite obrazac i kliknite **Nastavak**.

   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 s 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 softver pretražitelja. Pretražitelj 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.

Za vrijeme 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:** Neki korisnici možda imaju certifikate od vanjskog Izdavača certifikata (CA) ili
| Lokalnog CA na različitom iSeries sistemu koji im vi, kao administrator, želite učiniti dostupnim za Upravitelja
| digitalnih certifikata (DCM). Ovo dozvoljava vama i korisniku da koristite DCM za upravljanje ovim certifikatima,
| koji su najčešće korišteni za provjeru autentičnosti klijenta. Zadatak **Dodjela korisničkog certifikata** daje mehanizam
| za dozvolu korisniku da kreira DCM dodjelu za certifikat dobavljen od vanjskog CA.

| Kada korisnik dodijeli certifikat, DCM ima jedan ili dva načina za rukovanje dodijeljenim certifikatom:

| • Pohrana certifikata lokalno na iSeries s korisničkim profilom korisnika.
| Kada LDAP lokacija nije definirana za DCM, zadatak **Dodjela korisničkog certifikata** dozvoljava korisniku da
| dodijeli vanjski certifikat OS/400 korisničkom profilu. Dodjela certifikata korisničkom profilu osigurava da
| certifikat može biti korišten s aplikacijama na sistemu koje zahtijevaju certifikate za provjeru autentičnosti klijenta.

- Pohrana certifikata u lokaciju Lightweight Directory Access Protocol (LDAP) za upotrebu pomoću Mapiranja identiteta u poduzeću (EIM).
  Kada postoji definirana LDAP lokacija i iSeries sistem je konfiguriran za sudjelovanje u EIM-u, tada zadatak **Dodijeli korisnički certifikat** dozvoljava korisniku da pohrani kopiju izvan certifikata u specificirani LDAP direktorij. DCM također kreira udruženje izvora u EIM-u za certifikat. Pohrana certifikata na ovaj način dozvoljava EIM administratoru da prepozna certifikat kao važeći korisnički identitet koji može sudjelovati u EIM-u.

  Bilješka: Prije nego što korisnik može dodijeliti certifikat korisničkom identitetu u EIM konfiguraciji, EIM mora biti odgovarajuće konfiguriran za korisnika. Ova EIM konfiguracija uključuje kreiranje EIM identifikatora za korisnika i kreiranje ciljnog udruženja između tog EIM identifikatora i korisničkog profila. Inače, DCM ne može kreirati odgovarajuće izvorno udruženje pomoću EIM identifikatora za certifikat. Za više informacija o konfiguriranju EIM-a, pogledajte EIM poglavlje u iSeries Informacijskom Centru.

Za upotrebu zadatka **Dodjela korisničkog certifikata** korisnik mora ispuniti sljedeće zahtjeve:

1. Morate imati sigurnu sesiju s HTTP Poslužiteljem preko koje pristupate DCM-u.

   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 korisnik izabere ovaj zadatak, prikazuje se novi prozor pretražitelja. Ako korisnik nema sigurnu sesiju, DCM traži od korisnika da klikne na **Dodjela korisničkog certifikata** da jednu pokrene. DCM zatim započinje pregovore Sloja sigurnih utičnica (SSL) s pretražiteljem korisnika. Kao dio ovih pregovora, pretražitelj može zatražiti odgovor od korisnika da li da vjeruje Izdavaču certifikata (CA) koji je izdao certifikat koji identificira HTTP Poslužitelj. Također, pretražitelj može pitati korisnika da li prihvatiti sam certifikat poslužitelja.
2. Predstavite certifikat za provjeru autentičnosti klijenta.

   Ovisno o postavljanjima konfiguracija za vaš pretražitelj, on vas može promptirati da izaberete certifikat i da ga predočite za provjeru autentičnosti. Ako vaš pretražitelj predoči certifikat od nekog CA kojeg sistem prihvaća s 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.
3. Morate imati certifikat u pretražitelju koji još nije pridružen korisničkom identitetu za korisnika koji izvodi zadatak. (Ili, ako je DCM konfiguriran za rad zajedno s EIM-om, korisnik mora imati certifikat u pretražitelju koji još nije pohranjen na LDAP lokaciju za DCM.)

   Jednom kada postavite sigurnu sesiju, DCM pokušava dohvatiti odgovarajući certifikat s vašeg poslužitelja tako da ga može pridružiti s vašim korisničkim identitetom. 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 iz certifikata, niste bili u mogućnosti dobaviti certifikat koji DCM može dodijeliti vašem korisničkom identitetu. Jedan od nekoliko problema korisničkih certifikata može biti za to odgovoran. Na primjer, certifikati koje vaš pretražitelj sadrži mogu već biti pridruženi s vašim korisničkim identitetom.

Upravljanje korisničkim certifikatima pomoću isteka: Upravitelj digitalnih certifikata (DCM) dobavlja podršku upravljanja istekom certifikata da dozvoli administratorima provjeru datuma isteka korisničkih certifikata na lokalnom iSeries sistemu. Podrška upravljanja istekom DCM korisničkih certifikata može biti korištena zajedno s Mapiranjem identiteta u poduzeću (EIM) tako da administratori mogu koristiti DCM za provjeru isteka korisničkog certifikata na razini poduzeća.

Da iskoristi prednosti podrške upravljanja istekom za korisničke certifikate na razini poduzeća, EIM mora biti konfiguriran u poduzeću i EIM mora sadržavati prikadne informacije mapiranja za korisnike certifikata. Za provjeru isteka korisničkih certifikata različitih od onih pridruženih vašem korisničkim profilu, morate imati *ALLOBJ i *SECADM posebna ovlaštenja.

Upotreba DCM-a za gledanje certifikata na osnovu njihovog isteka dozvoljava vam da odredite brzo i jednostavno koji certifikati su blizu isteku, tako da certifikati mogu biti na vrijeme obnovljeni.

Za gledanje i upravljanje korisničkim certifikatima na osnovu datuma isteka, izvedite ove korake:

1. Pokrenite DCM.

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

2. U navigacijskom okviru izaberite **Upravljanje korisničkim certifikatima** za prikaz popisa zadataka. **Opaska:** Ako trenutno radite sa spremištem certifikata, izaberite **Upravljanje certifikatima** za prikaz popisa zadataka, zatim izaberite **Provjera isteka** i izaberite **Korisnik**.
3. Ako vaš korisnički profil ima *ALLOBJ i *SECADM posebna ovlaštenja, možete izabrati metodu za izbor korisničkih certifikata koje želite pogledati i njima upravljati na osnovu njihovih datuma isteka. (Ako vaš korisnički profil nema ova posebna ovlaštenja, DCM od vas traži da specificirate raspon za datum isteka kako je opisano u sljedećem koraku.) Možete izabrati jedno od sljedećeg:
   - **Korisnički profil** za gledanje i upravljanje korisničkim certifikatima koji su dodijeljeni specifičnom OS/400 korisničkom profilu. Specificirajte **Ime korisničkog profila** i kliknite **Nastavak**. **Opaska:** Možete specificirati korisnički profil različit od vašeg korisničkog profila samo ako imate *ALLOBJ i *SECADM posebna ovlaštenja.
   - **Certifikati svih korisnika** da pogledate i upravljate korisničkim profilima za sve korisničke identitete.
4. U polju **Raspon datuma isteka u danima (1-365)**, upišite broj dana za koje treba pogledati korisničke certifikate na osnovu njihovog datuma isteka i kliknite **Nastavak**. DCM prikazuje sve korisničke certifikate za specificirani korisnički profil koji ističu između današnjeg datuma i datuma koji odgovara broju specificiranih dana. DCM također prikazuje sve korisničke certifikate koji imaju datume isteka prije današnjeg datuma.
5. Izaberite korisnički certifikat za upravljanje. Za gledanje možete izabrati detalje informacija o certifikatu, ili ukloniti certifikat iz pridruženog korisničkog identiteta.
6. Kada završite rad s certifikatima s popisa, kliknite **Opoziv** za izlaz iz zadatka.

Upotreba API-ja za programsko izdavanje certifikata ne-iSeries korisnicima

Počevši od V5R2, postoje dva nova API-ja 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 s njihovim iSeries korisničkim profilima. Kao posljedica, da bi koristili Lokalni CA da izdaje certifikate za provjeru autentičnosti klijenta, morali ste dobaviti tog korisnika s 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 dobavljanje korisničkih profila ovim korisnicima, možda ćete zahtijevati od korisnika da plate za certifikat od dobro poznatog CA ako ste htjeli tražiti certifikate za provjeru valjanosti korisnika za vaše aplikacije.

Ta dva nova API-ja daju podršku koja dozvoljava da osigurate 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.

Postoje dva API-ja, jedan za svaki od pred-dominantnih pretraživačkih programa, koje možete pozivati kod upotrebe 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 predstavi certifikat od javnog Internet CA, vaš pretražitelj ili drugi softver klijenta možda već ima 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 zahtijeva da napravite vlastitu provjeru valjanosti prikazom certifikata od Lokalnog CA, morate učitati Lokalni CA certifikat u vaš pretražitelj prije zahtijevanja korisničkog certifikata od Lokalnog CA.

Da koristite DCM da dobijete kopiju Lokalnog CA certifikata, izvedite sljedeće korake:

1. Pokrenite DCM.
2. U navigacijskom okviru, izaberite **Instaliranje Lokalnog CA certifikata 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 **Instaliranje certifikata** da spustite Lokalni CA certifikat kao pouzdano ishodište u vašem pretražitelju. Time se osigurava da vaš pretražitelj može postaviti sesije sigurnih komunikacija s 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 (kao što je MKKF ili IKEYMAN) za spremanje certifikata koje će koristiti klijent programi na PC računalu. Prije nego što 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 s javnom Web stranicom i želite koristiti Sloj sigurnih utičnica (SSL) za sesije sigurnih komunikacija da osigurate privatnost određenih informacijskih transakcija. Stoga što je Web stranica dostupna za opću javnost, želite koristiti certifikate koje većina Web pretražitelja može brzo 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 iz vašeg poduzeća i da neovlaštene stranke nisu promijenile kod za vrijeme 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 slanja 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 spremište certifikata. Spremište certifikata je posebna datoteka baze podataka ključeva koju DCM koristi za pohranjivanje digitalnih

certifikata i njihovih pridruženih privatnih ključeva. DCM vam omogućuje kreiranje i upravljanje s nekoliko tipova spremišta certifikata ovisno o tipovima certifikata, koje ona sadrže.

Tip spremišta certifikata, koje kreirate i naredne zadatke koje morate izvesti za upravljanje vašim certifikatima i aplikacijama koje ih koriste, ovisi o tome kako planirate koristiti vaše certifikate. Da naučite kako koristiti DCM za kreiranje odgovarajućeg spremišta 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 provjeru 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

Upravitelja digitalnih certifikata (DCM) možete koristiti 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 odgovarajuće spremište certifikata za upravljanje javnim certifikatima koje koristite za SSL. To je *SYSTEM spremište certifikata. Kad kreirate spremište 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, izvedite ove korake:

1. Pokrenite DCM.
2. U navigacijskom okviru DCM-a izaberite **Kreiranje novog spremišta certifikata** da dovršite vođeni zadatak i popunite seriju obrazaca. Ovi obrasci vas vode kroz postupak kreiranja spremišta 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 spremište certifikata za kreiranje i kliknite **Nastavak**.
4. Izaberite **Da** za kreiranje certifikata kao dijela kreiranja *SYSTEM spremišta certifikata i kliknite**Nastavak**.
5. Izaberite **VeriSign ili drugog Internet izdavača certifikata (CA)** kao potpisnika novog certifikata i kliknite**Nastavak** za prikaz obrasca koji vam omogućuje da popunite informacije o identifikaciji za novi certifikat.

   Bilješka: Ako vaš poslužitelj ima instaliran IBM kriptografički koprocesor, DCM vam dozvoljava da izaberete kako ćete spremiti privatni ključ za certifikat, kao sljedeći zadatak. Ako vaš sistem nema koprocesor, DCM automatski postavlja privatni ključ u *SYSTEM spremište certifikata. Ako trebate pomoć kod izbora kako pohraniti privatni ključ, pogledajte online pomoć u DCM-u.
6. Popunite obrazac i kliknite **Nastavak** 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 izabrali da izdaje i potpisuje vaše certifikate.

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

   Bilješka: Za upotrebu certifikata pomoću HTTP Poslužitelja za iSeries, morate kreirati i konfigurirati vaš Web poslužitelj prije rada s DCM-om za rad s potpisanim dovršenim certifikatom. Kada konfigurirate Web

poslužitelj za upotrebu SSL-a, ID aplikacije generiran je za poslužitelj. Morate učiniti zapis ovog ID-a aplikacije tako da možete koristiti DCM za specificiranje koji certifikat ova aplikacija mora koristiti za SSL.

Ne zaustavljajte i ponovno pokrećite poslužitelj dok ne koristite DCM za dodjelu potpisanog dovršenog certifikata poslužitelju. Ako završite i ponovno pokrenete *ADMIN instancu Web poslužitelja prije nego mu dodijelite certifikat, poslužitelj neće biti pokrenut i vi nećete biti u mogućnosti koristiti DCM za dodjelu certifikata poslužitelju.

8. Nakon što javni CA vrati vaš potpisani certifikat, pokrenite DCM.
9. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***SYSTEM** da se otvori spremište certifikata.
10. Kad se prikaže stranica Spremište certifikata i lozinki, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
11. Nakon osvježenja navigacijskog okvira izaberite**Upravljanje certifikatima** za prikaz popisa zadataka.
12. Iz popisa zadataka izaberite **Import certifikata** da započnete postupak importiranja potpisanog certifikata u *SYSTEM spremište certifikata. Nakon što završite importiranje certifikata, možete specificirati aplikacije koje ga moraju koristiti za SSL komunikacije.
13. U navigacijskom okviru izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
14. Iz popisa zadataka izaberite **Ažuriranje dodjele certifikata** za prikaz popisa SSL omogućenih aplikacija kojima ste dodijelili certifikat.
15. Izaberite neku aplikaciju s popisa i kliknite **Ažuriranje dodjele certifikata** .
16. Izaberite certifikat kojeg ste importirali i kliknite**Dodjela novog certifikata**. 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 s 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, oni moraju pristupiti Web stranici za CA i slijediti upute koje stranica daje.

Upravljanje javnim Internet certifikatima za potpisivanje objekata

Upravitelja digitalnih certifikata (DCM) možete koristiti za upravljanje javnim Internet certifikatima za digitalno potpisivanje objekata. Ako ne koristite DCM za upravljanje vašim Lokalnim Izdavačem certifikata CA), morate prvo kreirati odgovarajuće spremište certifikata za upravljanje javnim certifikatima koje koristite za potpisivanje objekata. To je *OBJECTSIGNING spremište certifikata. Kad kreirate spremište 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 zahtijeva, 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 izaberite **Kreiranje novog spremišta certifikata** za pokretanje vođenog zadatka i dovršite niz obrazaca. Ovi obrasci vas vode kroz postupak kreiranja spremišta certifikata i certifikata kojeg možete koristiti za potpisivanje objekata.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
3. Izaberite ***OBJECTSIGNING** kao spremište certifikata za kreiranje i kliknite **Nastavak**.
4. Izaberite **Da** za kreiranje certifikata kao dijela kreiranja spremišta certifikata i klikniteNastavak.
5. Izaberite **VeriSign ili drugog Internet izdavača certifikata (CA)** kao potpisnika novog certifikata i klikniteNastavak za prikaz obrasca koji vam omogućuje da popunite 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 **Nastavak** 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 izabrali 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 **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** kao spremište certifikata za otvoriti.
10. Kad se prikaže stranica Spremište certifikata i lozinki, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
11. U navigacijskom okviru izaberite **Upravljanje certifikatima** za prikaz popisa zadataka.
12. Iz popisa zadataka izaberite **Import certifikata** da započnete postupak importiranja potpisanog certifikata u *OBJECTSIGNING spremište certifikata. Nakon što ste završili importiranje certifikata, možete kreirati definiciju aplikacije koju certifikat koristi za potpisivanje objekata.
13. Nakon osvježavanja lijevog navigacijskog okvira izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
14. Iz popisa zadataka izaberite **Dodavanje aplikacije** 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. Iz popisa zadataka izaberite **Ažuriranje dodjele certifikata** i kliknite **Nastavak** za prikaz popisa ID-ova aplikacija koje potpisuju objekte kojima ste dodijelili certifikat.
18. Izaberite ID vaše aplikacije s popisa i kliknite **Ažuriranje dodjele certifikata** .
19. Izaberite certifikat kojeg ste importirali i klikniteDodjela novog certifikata.

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. Morate dobaviti kopiju ovog certifikata kao dio 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 s certifikatom od dobro poznatog Internet CA, verzija DCM-a primatelja može već imati kopiju potrebnog CA certifikata. Ipak, možda dobavite kopiju CA certifikata zajedno s potpisanim objektima ako

mislite da primalac još nema kopiju. Na primjer, morate dobaviti kopiju Lokalnog CA certifikata ako ste potpisali objekte sa certifikatom od privatnog Lokalnog CA. Iz sigurnosnih razloga morate dobaviti CA certifikat u odijeljenim paketima, ili javno učiniti dostupnim CA certifikat na zahtjev onih koji ga trebaju.

Upravljanje certifikatima za provjeru potpisa objekata

Upravitelja digitalnih certifikata (DCM) možete koristiti 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 *SIGNATUREVERIFICATION spremište 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 s 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 odgovarajuće spremište certifikata za upravljanje potrebnim certifikatima za provjeru potpisa; to je *SIGNATUREVERIFICATION spremište certifikata. Kad kreirate to spremište certifikata, DCM ga automatski popunjava kopijama certifikata većine dobro poznatih javnih CA.

Bilješka: Ako želite provjeriti potpise koje ste kreirali s vašim vlastitim certifikatima za potpisivanje objekata, morate kreirati *SIGNATUREVERIFICATION spremište certifikata i kopirati u njega certifikate iz *OBJECTSIGNING spremišta certifikata. To je potrebno čak i onda kad planirate izvesti provjeru potpisa iz *OBJECTSIGNING spremišta certifikata.

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

1. Pokrenite DCM.
2. U lijevom navigacijskom okviru DCM-a izaberite **Kreiranje novog spremišta certifikata** za pokretanje vođenog zadatka i dovršite niz obrazaca.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
3. Izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za kreiranje i kliknite **Nastavak**.

   Bilješka: Ako postoji *OBJECTSIGNING spremište certifikata tada će vas DCM pitati da li ćete kopirati certifikate za potpisivanje objekata u novo spremište certifikata kao certifikate za provjeru potpisa. Ako želite koristiti vaše potpisane certifikate postojećeg objekta za provjeru potpisa, izaberite **Da** i kliknite **Nastavak**. Morate znati lozinku za *OBJECTSIGNING spremište certifikata da iz njega kopirate certifikate.
4. Odredite lozinku za novo spremište certifikata i kliknite **Nastavak** za kreiranje spremišta certifikata. Stranica potvrde pokazuje da je spremište certifikata uspješno kreirano. Sada možete koristiti spremište da upravljate i koristite certifikate za provjeru potpisa objekata.

   Bilješka: Ako ste kreirali ovo spremište tako da možete provjeriti potpise na objektima koje ste potpisali, tada se možete zaustaviti. Kako kreirate potpisane certifikate novog objekta, morate ih eksportirati iz *OBJECTSIGNING spremišta certifikata u ovo spremište certifikata. Ako ih ne eksportirate nećete moći provjeriti potpise koje ste s njima kreirali.

Bilješka: Ako ste kreirali ovo spremište certifikata tako da možete provjeriti potpise na objektima koje ste primili od drugih izvora, morate nastaviti s ovom procedurom tako da možete importirati certifikate koje trebate u spremište certifikata.

5. U navigacijskom okviru kliknite**Izbor spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** za otvaranje.
6. Kad se prikaže stranica Spremište certifikata i lozinki, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
7. Nakon osvježenja navigacijskog okvira izaberite**Upravljanje certifikatima** za prikaz popisa zadataka.
8. Iz popisa zadataka izaberite**Import certifikata**. Ovaj vođeni zadatak vas vodi kroz proces importiranja certifikata koje trebate u spremište 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 s potpisanim objektima i dovršite zadatak importiranja.

   Bilješka: Ako spremište certifikata još ne sadrži kopiju CA certifikata za CA koji je izdao certifikat provjere potpisa, morate importirati CA certifikat *prije*. Možda ćete dobiti grešku kod importiranja certifikata za provjeru potpisa ako ne importirate CA certifikat prije importiranja certifikata za provjeru potpisa.

Ove certifikate možete koristiti za provjeru potpisa objekata.

Poglavlje 8. Upravljanje DCM-om

Nakon što konfigurirate Upravitelja digitalnih certifikata (DCM), postoje mnogi zadaci upravljanja certifikatima koje ćete trebate obaviti tokom vremena. Da naučite kako koristiti DCM za upravljanje vašim digitalnim certifikatima, pročitajte ova poglavlja:

Upotreba lokalnog CA za izdavanje certifikata za druge iSeries sisteme
Naučite kako se koristi privatni, lokalni CA na jednom sistemu za izdavanje certifikata za upotrebu na drugim sistemima.

Upravljanje aplikacijama u DCM-u
Naučite kako koristiti DCM za rad s 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 autentičnosti klijenta.

Upravljanje certifikatima pomoću isteka
Naučite kako koristiti DCM za gledanje i upravljanje certifikatima na osnovu datuma njihovog isteka.

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 Liste opoziva certifikata koje aplikacije mogu koristiti za provjeru valjanosti certifikata.

Spremanje ključeva certifikata na IBM Kriptografički koprocesor
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 javnog Internet CA koji izdaje certifikate pod Infrastrukturom javnog ključa za X.509 (PKIX) standarde.

Upravljanje LDAP lokacijom za korisničke certifikate
Naučite kako konfigurirati DCM za pohranu korisničkih certifikata u lokaciji Lightweight Directory Access Protocol (LDAP) poslužitelja direktorija za proširenje Mapiranja identiteta u poduzeću za rad s korisničkim certifikatima.

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

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

Upotreba lokalnog CA za izdavanje certifikata za druge iSeries sisteme

Možda već koristite privatnog Lokalnog izdavača certifikata (CA) na poslužitelju u vašoj mreži. Sad želite proširiti upotrebu tog lokalnog CA na drugi poslužitelj u vašoj mreži. Na primjer, želite da vaš trenutni lokalni CA izdaje poslužiteljske ili klijent certifikate za neku aplikaciju na drugom poslužitelju za upotrebu u SSL komunikacijskim sesijama. Ili želite koristiti certifikate od vašeg lokalnog CA na jednom sistemu za potpisivanje objekata koje želite spremiti na drugi poslužitelj.

Taj cilj možete postići upotrebom Upravitelja digitalnih certifikata (DCM). Neke zadatke izvodite na poslužitelju na kojem radi Lokalni CA, a druge izvodite na sekundarnom poslužitelju koji je host za aplikacije za koje želite izdavati certifikate. Taj sekundarni sistem se naziva ciljni sistem. Zadaci koje morate izvesti na ciljnom sistemu ovise o razini izdanja tog sistema.

Bilješka: Možete naići na problem ako poslužitelj na kojem radi lokalni CA koristi proizvod dobavljača kriptografičkog pristupa koji daje jače šifriranje nego ciljni sistem. Za V5R2 i kasnije verzije OS/400 ili i5/OS, jedini dostupni dobavljač kriptografičkog pristupa je 5722–AC3, koji je trenutno najjači dostupni proizvod. Ipak, u ranijim izdanjima mogli ste instalirati druge, slabije proizvode za kriptografičko dobavljanje pristupa (5722–AC1, ili 5722–AC2) koji su omogućavali niže razine kriptografičke funkcije. Kad eksportirate certifikat (s 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 za vrijeme procesa 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 odgovarajuća za korištenje s 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. Kad koristite lokalnog CA za kreiranje certifikata za upotrebu na drugom poslužitelju, datoteke koje kreira DCM sadrže kopiju certifikata lokalnog CA, kao i kopije certifikata za mnoge javne Internet CA-ove.

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.

Izdavanje privatnih certifikata za upotrebu na drugom V5R3, V5R2 ili V5R1 sistemu

Da bi koristili vašeg lokalnog CA za izdavanje certifikata za upotrebu na drugom V5R3, V5R2 ili V5R1 sistemu izvedite ove korake na V5R3 sistemu koji je host za 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 trebate otvarati spremište certifikata da dovršite ovaj zadatak. Ove upute pretpostavljaju da ili ne radite u određenom spremištu certifikata ili da radite u spremištu 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 **Nastavak** da započnete vođeni zadatak i završite seriju obrazaca. Izaberite kreiranje **poslužiteljskog ili klijentskog certifikata za drugi sistem** (za SSL sesije) ili **certifikata za potpisivanje objekata za drugi sistem**.

   Bilješka: Ako kreirate certifikat za potpisivanje objekata za drugi sistem, taj sistem mora izvoditi V5R1 ili kasniju verziju OS/400 ili i5/OS da bi se certifikat mogao koristiti. Stoga što ciljni sistem mora biti V5R1 ili kasniji, DCM na sistemu lokalnog hosta od vas ne traži da izaberete format ciljnog izdanja za certifikat za potpis novog objekta.
4. Ako kreirate poslužiteljski ili klijentski certifikat izaberite razinu izdanja poslužitelja za koji kreirate taj certifikat. Kliknite **Nastavak** za prikaz obrasca koji vam dopušta da osigurate identifikacijske informacije za novi certifikat.

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

   Bilješka: Ako postoji *OBJECTSIGNING ili *SYSTEM spremište 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 postojeće spremište 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 vlastitom spremištu certifikata i generira dvije datoteke za prijenos: datoteku spremišta certifikata (.KDB ekstenzija) i datoteku zahtjeva (.RDB ekstenzija).

6. Koristite binarni Protokol za prijenos datoteka (FTP) ili drugi način prijenosa datoteka na ciljni sistem.

Izdavanje privatnih certifikata za upotrebu na V4R5 poslužitelju

Da bi koristili vašeg lokalnog CA za izdavanje certifikata za upotrebu na V4R5 poslužitelju izvedite ove korake na V5R3 sistemu koji je host za 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 trebate otvarati spremište certifikata da dovršite ovaj zadatak. Ove upute pretpostavljaju da ili ne radite u određenom spremištu certifikata ili da radite u spremištu certifikata lokalnog Izdavača certifikata (CA). Lokalni CA mora postojati na ovom sistemu prije nego možete izvesti ove zadatke.

3. Izaberite **Poslužiteljski ili klijentski certifikat za drugi poslužitelj** kao tip certifikata koji želite da lokalni CA izda i kliknite **Nastavak** da pokrenete vođeni zadatak i ispunite niz obrazaca.

   Bilješka: Zbog toga što kreirate ovaj certifikat za upotrebu na V4R5 poslužitelju, morate izabrati **poslužiteljski ili klijentski certifikat za drugi iSeries**. Ciljni sistemi s razinom izdanja prije V5R1 ne mogu koristiti certifikate za potpisivanje objekta.

4. Izaberite razinu izdanja poslužitelja za koji kreirate ovaj certifikat. Kliknite **Nastavak** za prikaz obrasca koji vam dopušta da osigurate identifikacijske informacije za novi certifikat.

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

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

   Bilješka: Ako postoji *SYSTEM spremište 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 postojeće spremište certifikata na ciljnom sistemu.

   Ova stranica za potvrdu 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 vlastitom spremištu certifikata i generira dvije datoteke za prijenos: datoteku spremišta certifikata (.KDB ekstenzija) i datoteku zahtjeva (.RDB ekstenzija).

   Bilješka: Ako planirate koristiti certifikate u ovim datotekama u postojećem *SYSTEM spremištu certifikata na V4R5 ciljnom sistemu, ne možete importirati Lokalni CA certifikat izravno iz .KDB i .RDB datoteka. To je zbog toga što CA certifikat nije u formatu kojeg DCM import 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 formatu koji će raditi s import funkcijom za ranija izdanja.

6. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***SYSTEM** da se otvori spremište certifikata.
7. Kad se prikaže stranica Spremište certifikata i lozinka, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali na host sistemu i kliknite **Nastavak**.
8. U navigacijskom okviru izaberite **Upravljanje certifikatima** za prikaz popisa zadataka.
9. Iz popisa zadataka izaberite **Eksport certifikata**.
10. Izaberite **Izdavača certifikata (CA)** kao tip certifikata za eksport i **Nastavak** 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 **Nastavak** .
13. Specificirajte potpuno kvalificirano ime i stazu datoteke za eksportnu datoteku i klikniteNastavak . Stranica potvrde pokazuje da je DCM uspješno eksportirao datoteku.

    Bilješka: Provjerite da li ste dali datoteci jedinstveno ime i ekstenziju. Na primjer, možete imenovati datoteku mycafile.exp. Kad imenujete datoteku, nemojte za datoteku upotrijebiti nijednu od ovih ekstenzija:.TXT, .KDB, .RDB, ili .KYR. Upotreba jednog od ovih tipova ekstenzije može kreirati problem kada importirate datoteku na ciljni sistem.
14. Koristite binarni File Transfer Protocol (FTP) ili drugu metodu za prijenos datoteka spremišta certifikata koje ste kreirali (.KDB i .RDB) na V4R5 ciljni sistem. Koristite ASCII FTP način za prijenos datoteke koja sadrži eksportirani Lokalni CA certifikat.

Upotreba prenešenih datoteka na ciljnom sistemu

Nakon što prenesete datoteke, koristite DCM na ciljnom sistemu da radite s prenesenim datotekama certifikata. DCM zadaci, koje morate obaviti, variraju ovisno o razini izdanja ciljnog sistema i o tome koja spremišta 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 s prenesenim datotekama certifikata, pogledajte ova poglavlja:

- Upotreba privatnog certifikata za SSL sesije na V5R3 ili V5R2 ciljnom sistemu
- Upotreba privatnog certifikata za SSL sesije na V5R1 ciljnom sistemu.
- Upotreba privatnog certifikata za potpisivanje objekta na V5R3, V5R2, ili V5R1 ciljnom sistemu
- Upotreba privatnog certifikata za SSL sesije na V4R5 ciljnom sistemu

Upotreba privatnog certifikata za SSL sesije na V5R3 ili V5R2 ciljnom sistemu

Certifikatima, koje koriste vaše aplikacije za SSL sesije, upravljate iz *SYSTEM spremišta certifikata u Upravitelju digitalnih certifikata. Ako nikad niste koristili DCM na V5R3 ili V5R2 ciljnom sistemu za upravljanje certifikatima za SSL, tada ovo spremište certifikata neće postojati na ciljnom sistemu. Zadaci za korištenje prenesenih datoteka spremišta certifikata koje ste kreirali na host sistemu Lokalnog Izdavača certifikata (CA) ovise o tome postoji li *SYSTEM spremište certifikata. Ako *SYSTEM spremište certifikata ne postoji, možete koristiti prenesene datoteke certifikata kao način za kreiranje *SYSTEM spremišta certifikata. Ako *SYSTEM spremište certifikata postoji na V5R3 ili V5R2 ciljnom sistemu, možete koristiti prenešene datoteke certifikata na jedan od dva načina:

- Koristite prenesene datoteke kao Spremište certifikata drugog sistema.
- Importirajte prenesene datoteke u postojeće *SYSTEM spremište certifikata.

***SYSTEM spremište certifikata ne postoji**

Ako *SYSTEM spremište certifikata ne postoji na V5R3 ili V5R2 sistemu na kojem želite koristiti prenešene datoteke spremišta certifikata, možete koristiti prenešene datoteke certifikata kao *SYSTEM spremište certifikata. Da kreirate *SYSTEM spremište certifikata i koristite datoteke certifikata na vašem V5R3 ili V5R2 ciljnom sistemu, izvedite ove korake:

1. Budite sigurni da su datoteke spremišta certifikata (dvije datoteke: jedna s .KDB ekstenzijom i jedna s .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 čine *SYSTEM spremište certifikata za ciljni sistem. Datoteke spremišta certifikata već sadrže kopije certifikata za mnoge javne Internet CA-ove. DCM ih je dodao, kao i kopiju Lokalnog CA certifikata, u datoteke spremišta 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 spremište certifikata trenutno postoji na ovom ciljnom sistemu. Zbog toga, ne smijete preimenovati prenešene datoteke kako je predloženo. Prepisivanje defaultne datoteke će uzrokovati problem kod korištenja DCM-a, prenesenog

spremišta certifikata i njegovog sadržaja. Umjesto toga morate osigurati da imaju jedinstvena imena i morate koristiti prenešeno spremište certifikata kao **Spremište certifikata drugog sistema**. Ako koristite datoteke kao Spremište certifikata drugog sistema, ne možete koristiti DCM da specificirate koje aplikacije će koristiti certifikat.

3. Pokrenite DCM. Sada morate promijeniti lozinku za *SYSTEM spremište 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 spremištu certifikata.
4. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***SYSTEM** da se otvori spremište certifikata.
5. Kada se prikaže stranica Spremište certifikata i Lozinka, unesite lozinku koju ste specificirali na *host* sistemu za spremište certifikata kada ste kreirali certifikat za V5R3 ili V5R2 ciljni sistem i kliknite **Nastavak**.
6. U navigacijskom okviru izaberite **Upravljanje spremištem certifikata** i izaberite **Promjena lozinke** iz popisa zadataka. Popunite obrazac da promijenite lozinku za spremište certifikata. Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima. Sljedeće možete specificirati koje će aplikacije koristiti certifikat za SSL sesije.
7. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***SYSTEM** da se otvori spremište certifikata.
8. Kada se prikaže stranica **Spremište certifikata i Lozinka**, unesite novu lozinku i kliknite **Nastavak**.
9. Nakon osvježenja navigacijskog okvira, izaberite **Upravljanje certifikatima** u navigacijskom okviru da se prikaže popis zadataka.
10. Iz popisa zadataka izaberite **Dodjela certifikata** da prikažete listu certifikata u trenutnom spremištu certifikata.
11. Izaberite certifikat koji ste kreirali na *host* sistemu i kliknite **Dodjela aplikacijama** da prikažete listu SSL omogućenih aplikacija kojima možete dodijeliti certifikat.
12. Izaberite aplikacije koje će koristiti certifikat za SSL sesije i kliknite **Nastavak**. DCM prikazuje poruku da potvrđuje vaš izbor certifikata za te aplikacije.

    Bilješka: Neke SSL omogućene aplikacije podržavaju provjeru autentičnosti klijenta osnovanu na certifikatima. Aplikacija s 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 završenim ovim zadacima, aplikacije na ciljnom sistemu mogu koristiti certifikat izdan od lokalnog CA na drugom poslužitelju. 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 spremište certifikata postoji — upotreba datoteka kao Spremište certifikata drugog sistema**

Ako V5R3 ili V5R2 ciljni sistem već ima *SYSTEM spremište certifikata, morate odlučiti kako raditi s datotekama certifikata koje ste prenijeli na ciljni sistem. Možete odlučiti da radite s prenesenim datotekama certifikata kao **Spremištem certifikata drugog sistema** . Ili, možete izabrati importiranje privatnog certifikata i njemu odgovarajućeg Lokalnog CA certifikata u postojeće *SYSTEM spremište certifikata.

Druga sistemska spremišta certifikata su korisnički definirana sekundarna spremišta 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 s DCM svojstvom. Opcija Spremišta certifikata drugog sistema 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 spremište certifikata, a ne certifikata koji ste specifično identificirali.

IBM iSeries aplikacije (i mnoge druge aplikacije razvijatelja softvera) su pisane za korištenje certifikata samo u *SYSTEM spremištu certifikata. Ako odlučite koristiti prenešene datoteke kao Spremište certifikata drugog sistema, ne možete koristiti DCM da specificirate koje aplikacije će koristiti certifikat za SSL sesije. Isto tako ne možete konfigurirati standardne SSL-omogućene aplikacije za upotrebu ovog certifikata. Ako želite koristiti certifikat za iSeries aplikacije, morate importirati certifikat iz vaših prenesenih datoteka spremišta certifikata u *SYSTEM spremište certifikata.

Da pristupite i radite s prenesenim datotekama certifikata kao sa Spremištem certifikata drugog sistema, izvedite ove korake:
1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite **Spremište certifikata drugog sistema** da se otvori spremište certifikata.
3. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite puno kvalificirano ime staze i datoteke za datoteku spremišta certifikata (ona s .KDB ekstenzijom) koju ste prenijeli s host sistema. Također unesite lozinku koju ste specificirali na *host* sistemu za spremište certifikata kada ste kreirali certifikat za V5R2 ciljni sistem i kliknite **Nastavak**.
4. U navigacijskom okviru izaberite **Upravljanje spremištem certifikata** i izaberite **Promjena lozinke** iz popisa zadataka. Popunite obrazac da promijenite lozinku za spremište certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za spremište certifikata. Upotreba ove opcije osigurava da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novom spremištu.

   Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima. Zatim možete odrediti da se certifikat u tom spremištu može koristiti kao defaultni certifikat.
5. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite **Spremište certifikata drugog sistema** da se otvori spremište certifikata.
6. Kada se prikaže stranica **Spremište certifikata i Lozinka**, unesite potpuno kvalificirano ime i stazu datoteke za datoteku spremišta certifikata, unesite novu lozinku i kliknite **Nastavak**.
7. Nakon osvježavanja navigacijskog okvira, izaberite **Upravljanje spremištem certifikata** i izaberite **Postav default certifikat** iz popisa zadataka.

Sada kada ste kreirali i konfigurirali Spremište certifikata drugog sistema, svaka aplikacija koja koristi SSL_Init API može upotrijebiti certifikat u njemu za postavljanje SSL sesije.

***SYSTEM spremište certifikata postoji — upotreba certifikata u postojećem *SYSTEM spremištu certifikata**

| Možete koristiti certifikate u prenešenim datotekama spremišta certifikata u postojećem *SYSTEM spremištu
| certifikata na V5R3 ili V5R2 sistemu. Da to napravite, morate importirati certifikate iz datoteka spremišta certifikata u
| postojeće *SYSTEM spremište certifikata. Ipak, ne možete importirati certifikate izravno iz .KDB i .RDB datoteka, jer
| nisu u formatu koji DCM funkcija importa može prepoznati i koristiti. Za korištenje prenesenih certifikata u
| postojećem *SYSTEM spremištu certifikata morate otvoriti datoteke kao Spremište certifikata drugog sistema i
| eksportirati ih u *SYSTEM spremište certifikata.

Za eksportiranje certifikata iz datoteka spremišta certifikata u *SYSTEM spremište certifikata, dovršite ove korake na V5R2 ciljnom sistemu:
1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i specificirajte **Spremište certifikata drugog sistema** da se otvori spremište certifikata.
3. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite puno kvalificirano ime staze i datoteke za datoteku spremišta certifikata (ona s .KDB ekstenzijom) koju ste prenijeli s host sistema. Također unesite lozinku koju ste specificirali na *host* sistemu za spremište certifikata kada ste kreirali certifikat za V5R2 ciljni sistem i kliknite **Nastavak**.
4. U navigacijskom okviru izaberite **Upravljanje spremištem certifikata** i izaberite **Promjena lozinke** iz popisa zadataka. Popunite obrazac da promijenite lozinku za spremište certifikata.

Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za spremište certifikata. Upotreba ove opcije osigurava da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novom spremištu. Ako ne promijenite lozinku i izaberete opciju Automatska prijava, možete naići na pogreške kod eksportiranja certifikata iz ovog spremišta u *SYSTEM spremište certifikata.

Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima.

5. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite **Spremište certifikata drugog sistema** da se otvori spremište certifikata.
6. Kada se prikaže stranica **Spremište certifikata i Lozinka**, unesite potpuno kvalificirano ime i stazu datoteke za datoteku spremišta certifikata, unesite novu lozinku i kliknite **Nastavak**.
7. Nakon osvježenja navigacijskog okvira, izaberite **Upravljanje 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 **Nastavak**.

   Bilješka: Morate eksportirati Lokalni CA certifikat u spremište certifikata prije nego eksportirate certifikat poslužitelja ili klijenta u spremište certifikata. Ako eksportirate prvo certifikat poslužitelja ili klijenta, možete naići na grešku, jer Lokalni CA certifikat ne postoji u spremištu certifikata.
9. Izaberite certifikat lokalnog CA za eksport i kliknite **Eksport**.
10. Izaberite **Spremište certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavak**.
11. Unesite *SYSTEM kao ciljno spremište certifikata, unesite lozinku za *SYSTEM spremište certifikata i kliknite **Nastavak**. Prikazuje se poruka da pokaže da je certifikat uspješno eksportiran ili da pokaže informacije o grešci ako proces eksporta nije uspio.
12. Sada možete eksportirati certifikat poslužitelja ili klijenta u *SYSTEM spremište certifikata. Ponovno izaberite zadatak **Eksport certifikata**.
13. Izaberite **Poslužitelj ili klijent** kao tip certifikata za eksport i kliknite **Nastavak**.
14. Izaberite odgovarajući certifikat poslužitelja ili klijenta za eksport i kliknite **Eksportiraj**.
15. Izaberite **Spremište certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavak**.
16. Unesite *SYSTEM kao ciljno spremište certifikata, unesite lozinku za *SYSTEM spremište certifikata i kliknite **Nastavak**. Prikazuje se poruka da pokaže da je certifikat uspješno eksportiran ili da pokaže informacije o grešci ako proces eksporta nije uspio.
17. Sada možete pridružiti certifikat aplikacijama za korištenje za SSL. Kliknite **Izbor spremišta certifikata** u navigacijskom okviru i izaberite ***SYSTEM** kao spremište certifikata koje treba otvoriti.
18. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite lozinku za *SYSTEM spremište certifikata i kliknite **Nastavak**.
19. Nakon osvježenja navigacijskog okvira izaberite**Upravljanje certifikatima** za prikaz popisa zadataka.
20. Iz popisa zadataka izaberite **Dodjela certifikata** da prikažete listu certifikata u trenutnom spremištu certifikata.
21. Izaberite certifikat koji ste kreirali na *host* sistemu i kliknite **Dodjela aplikacijama** da prikažete listu SSL omogućenih aplikacija kojima možete dodijeliti certifikat.
22. Izaberite aplikacije koje će koristiti certifikat za SSL sesije i kliknite **Nastavak**. DCM prikazuje poruku da potvrđuje vaš izbor certifikata za te aplikacije.

    Bilješka: Neke SSL omogućene aplikacije podržavaju provjeru autentičnosti klijenta osnovanu na certifikatima. Aplikacija s 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.

S ovim dovršenim zadacima, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao Lokalni CA na drugom iSeriesu. 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.

Upotreba privatnog certifikata za SSL sesije na V5R1 ciljnom sistemu

Certifikatima, koje koriste vaše aplikacije za SSL sesije, upravljate iz *SYSTEM spremišta certifikata u Upravitelju digitalnih certifikata. Ako nikada niste koristili DCM na V5R1 ciljnom sistemu za upravljanje certifikatima za SSL, tada ovaj certifikat neće postojati na ciljnom sistemu. Zadaci za korištenje prenesenih datoteka spremišta certifikata koje ste kreirali na host sistemu Lokalnog Izdavača certifikata (CA) ovise o tome postoji li *SYSTEM spremište certifikata. Ako *SYSTEM spremište certifikata ne postoji, možete koristiti prenesene datoteke certifikata kao način za kreiranje *SYSTEM spremišta certifikata. Ako *SYSTEM spremište certifikata postoji na V5R1 ciljnom sistemu, možete koristiti prenesene datoteke certifikata na jedan od dva načina:

- Koristite prenesene datoteke kao Spremište certifikata drugog sistema.
- Importirajte prenesene datoteke u postojeće *SYSTEM spremište certifikata.

***SYSTEM spremište certifikata ne postoji**

Ako *SYSTEM spremište certifikata ne postoji na V5R1 sistemu na kojem želite koristiti prenesene datoteke spremišta certifikata, možete koristiti prenesene datoteke certifikata kao *SYSTEM spremište certifikata. Za korištenje datoteka certifikata na vašem V5R1 ciljnom sistemu izvedite ove korake:

1. Budite sigurni da su datoteke spremišta certifikata (dvije datoteke: jedna s .KDB ekstenzijom i jedna s .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 čine *SYSTEM spremište certifikata za ciljni sistem. Datoteke spremišta certifikata već sadrže kopije certifikata za mnoge javne Internet CA-ove. DCM ih je dodao, kao i kopiju Lokalnog CA certifikata, u datoteke spremišta 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 spremište certifikata trenutno postoji na ovom ciljnom sistemu. Zbog toga, ne smijete preimenovati prenešene datoteke kako je predloženo. Prepisivanje defaultne datoteke će uzrokovati problem kod korištenja DCM-a, prenesenog spremišta certifikata i njegovog sadržaja. Umjesto toga morate osigurati da imaju jedinstvena imena i morate koristiti prenešeno spremište certifikata kao **Spremište certifikata drugog sistema**. Ako koristite datoteke kao Spremište certifikata drugog sistema, ne možete koristiti DCM da specificirate koje aplikacije će koristiti certifikat.
3. Pokrenite DCM. Sada morate promijeniti lozinku za *SYSTEM spremište 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 spremištu certifikata.
4. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***SYSTEM** da se otvori spremište certifikata.
5. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite lozinku koju ste specificirali za *host* sistem za spremište certifikata kad ste kreirali certifikat za V5R1 ciljni sistem i kliknite **Nastavak**.
6. U navigacijskom okviru izaberite **Upravljanje spremištem certifikata** i izaberite **Promjena lozinke** iz popisa zadataka. Popunite obrazac da promijenite lozinku za spremište certifikata. Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima. Sljedeće možete specificirati koje će aplikacije koristiti certifikat za SSL sesije.
7. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***SYSTEM** da se otvori spremište certifikata.
8. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite novu lozinku i kliknite **Nastavak**.
9. Nakon osvježenja navigacijskog okvira, izaberite **Upravljanje aplikacijama** u navigacijskom okviru da se prikaže popis zadataka.
10. Iz popisa zadataka izaberite **Ažuriranje dodjele certifikata** za prikaz popisa SSL omogućenih aplikacija kojima ste dodijelili certifikat.
11. Izaberite neku aplikaciju s popisa i kliknite **Ažuriranje dodjele 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 s 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.

S ovim dovršenim zadacima, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao Lokalni CA na drugom iSeriesu. 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 certifikat se mora kopirati u datoteku na korisnikovom PC računalu ili učitati u korisnikov pretražitelj, ovisno o zahtjevima aplikacije koja radi sa SSL.

***SYSTEM spremište certifikata postoji — upotreba datoteka kao Spremište certifikata drugog sistema**

Ako V5R1 ciljni sistem već ima *SYSTEM spremište certifikata, morate odlučiti kako raditi s datotekama certifikata. Možete odlučiti da radite s prenesenim datotekama certifikata kao **Spremištem certifikata drugog sistema** . Ili, možete izabrati importiranje privatnog certifikata i njemu odgovarajućeg Lokalnog CA certifikata u postojeće *SYSTEM spremište certifikata.

Druga sistemska spremišta certifikata su korisnički definirana sekundarna spremišta 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 s DCM pomoćnim programom. Opcija Spremišta certifikata drugog sistema 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 spremište certifikata, a ne certifikata koji ste specifično identificirali.

IBM iSeries aplikacije (i mnoge druge aplikacije razvijatelja softvera) su pisane za korištenje certifikata samo u *SYSTEM spremištu certifikata. Ako odlučite koristiti prenešene datoteke kao Spremište certifikata drugog sistema, ne možete koristiti DCM da specificirate koje aplikacije će koristiti certifikat za SSL sesije. 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 spremišta certifikata u *SYSTEM spremište certifikata.

Da pristupite i radite s prenesenim datotekama certifikata kao sa Spremištem certifikata drugog sistema, izvedite ove korake:

1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite **Spremište certifikata drugog sistema** da se otvori spremište certifikata.
3. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite puno kvalificirano ime staze i datoteke za datoteku spremišta certifikata (ona s .KDB ekstenzijom) koju ste prenijeli s host sistema. Također unesite lozinku koju ste specificirali na *host* sistemu za spremište certifikata kada ste kreirali certifikat za V5R1 ciljni sistem i kliknite **Nastavak**.
4. U navigacijskom okviru izaberite **Upravljanje spremištem certifikata** i izaberite **Promjena lozinke** iz popisa zadataka. Popunite obrazac da promijenite lozinku za spremište certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za spremište certifikata. Upotreba ove opcije osigurava da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novom spremištu.

   Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima. Zatim možete odrediti da se certifikat u tom spremištu može koristiti kao defaultni certifikat.
5. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite **Spremište certifikata drugog sistema** da se otvori spremište certifikata.

6. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite puno kvalificirano ime staze i datoteke za datoteku spremišta certifikata, unesite novu lozinku i kliknite **Nastavak**.
7. Nakon osvježavanja navigacijskog okvira, izaberite **Upravljanje spremištem certifikata** i izaberite **Postav default certifikat** iz popisa zadataka.

Sada kada ste kreirali i konfigurirali Spremište certifikata drugog sistema, svaka aplikacija koja koristi SSL_Init API može upotrijebiti certifikat u njemu za postavljanje SSL sesije.

***SYSTEM spremište certifikata postoji — upotreba certifikata u postojećem *SYSTEM spremištu certifikata**

Možete koristiti certifikate u prenesenim datotekama spremišta certifikata u postojećem *SYSTEM spremištu certifikata na V5R1 sistemu. Da to napravite, morate importirati certifikate iz datoteka spremišta certifikata u postojeće *SYSTEM spremište certifikata. Ipak, ne možete importirati certifikate izravno iz .KDB i .RDB datoteka, jer nisu u formatu koji DCM funkcija importa može prepoznati i koristiti. Za korištenje prenesenih certifikata u postojećem *SYSTEM spremištu certifikata morate otvoriti datoteke kao Spremište certifikata drugog sistema i eksportirati ih u *SYSTEM spremište certifikata.

Bilješka: Ova procedura opisuje kako koristiti Spremište certifikata drugog sistema na ciljnom sistemu za eksportiranje certifikata iz originalnih datoteka spremišta certifikata u *SYSTEM spremište certifikata. Upotreba ove metode dodavanja certifikata *SYSTEM spremištu certifikata vam pomaže da izbjegnete moguće probleme kada sistem koristi slabije proizvode dobavljača kriptografičkih usluga (kao 5722–AC2) od host sistema.

Za eksportiranje certifikata iz datoteka spremišta certifikata u *SYSTEM spremište certifikata, dovršite ove korake na V5R1 ciljnom sistemu:
1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i specificirajte **Spremište certifikata drugog sistema** da se otvori spremište certifikata.
3. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite puno kvalificirano ime staze i datoteke za datoteku spremišta certifikata (ona s .KDB ekstenzijom) koju ste prenijeli s host sistema. Također unesite lozinku koju ste specificirali na *host* sistemu za spremište certifikata kada ste kreirali certifikat za V5R1 ciljni sistem i kliknite **Nastavak**.
4. U navigacijskom okviru izaberite **Upravljanje spremištem certifikata** i izaberite **Promjena lozinke** iz popisa zadataka. Popunite obrazac da promijenite lozinku za spremište certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za spremište certifikata. Upotreba ove opcije osigurava da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novom spremištu. Ako ne promijenite lozinku i izaberete opciju Automatska prijava, možete naići na pogreške kod eksportiranja certifikata iz ovog spremišta u *SYSTEM spremište certifikata.

   Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima.
5. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite **Spremište certifikata drugog sistema** da se otvori spremište certifikata.
6. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite puno kvalificirano ime staze i datoteke za datoteku spremišta certifikata, unesite novu lozinku i kliknite **Nastavak**.
7. Nakon osvježenja navigacijskog okvira, izaberite **Upravljanje 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 **Nastavak**.

   Bilješka: Morate eksportirati Lokalni CA certifikat u spremište certifikata prije nego eksportirate certifikat poslužitelja ili klijenta u spremište certifikata. Ako eksportirate prvo certifikat poslužitelja ili klijenta, možete naići na grešku, jer Lokalni CA certifikat ne postoji u spremištu certifikata.
9. Izaberite certifikat lokalnog CA za eksport i kliknite **Eksport**.
10. Izaberite **Spremište certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavak**.

11. Unesite *SYSTEM kao ciljno spremište certifikata, unesite lozinku za *SYSTEM spremište certifikata i kliknite **Nastavak**.
12. Sada možete eksportirati certifikat poslužitelja ili klijenta u *SYSTEM spremište certifikata. Ponovno izaberite zadatak **Eksport certifikata**.
13. Izaberite **Poslužitelj ili klijent** kao tip certifikata za eksport i kliknite **Nastavak**.
14. Izaberite odgovarajući certifikat poslužitelja ili klijenta za eksport i kliknite **Eksportiraj**.
15. Izaberite **Spremište certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavak**.
16. Unesite *SYSTEM kao ciljno spremište certifikata, unesite lozinku za *SYSTEM spremište certifikata i kliknite **Nastavak**. Prikazuje se poruka da pokaže da je certifikat uspješno eksportiran ili da pokaže informacije o grešci ako proces eksporta nije uspio.
17. Sada možete pridružiti certifikat aplikacijama za korištenje za SSL. Kliknite **Izbor spremišta certifikata** u navigacijskom okviru i izaberite ***SYSTEM** kao spremište certifikata koje treba otvoriti.
18. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite lozinku za *SYSTEM spremište certifikata i kliknite **Nastavak**.
19. Nakon osvježenja navigacijskog okvira izaberite**Upravljanje certifikatima** za prikaz popisa zadataka.
20. Iz popisa zadataka izaberite **Ažuriranje dodjele certifikata** za prikaz popisa SSL omogućenih aplikacija kojima ste dodijelili certifikat.
21. Izaberite neku aplikaciju s popisa i kliknite **Ažuriranje dodjele certifikata** .
22. Izaberite certifikat koji je Lokalni CA na *host* sistemu izdao i kliknite **Dodjela novog certifikata**. DCM prikazuje poruku da potvrđuje vaš izbor certifikata za tu aplikaciju.

    Bilješka: Neke SSL omogućene aplikacije podržavaju provjeru autentičnosti klijenta osnovanu na certifikatima. Aplikacija s 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.

S ovim dovršenim zadacima, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao Lokalni CA na drugom iSeriesu. 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 certifikat se mora kopirati u datoteku na korisnikovom PC računalu ili učitati u korisnikov pretražitelj, ovisno o zahtjevima aplikacije koja radi sa SSL.

Upotreba privatnog certifikata za potpisivanje objekata na V5R3, V5R2 ili V5R1 ciljnom sistemu

Certifikatima koje koristite za potpisivanje objekata upravljate iz *OBJECTSIGNING spremišta certifikata u Upravitelju digitalnih certifikata. Ako nikada niste koristili DCM na ciljnom sistemu za upravljanje certifikatima za potpisivanje objekata, tada ovo spremište certifikata neće postojati na ciljnom sistemu. Zadaci koje morate obaviti za korištenje prenesenih datoteka spremišta certifikata koje ste kreirali na host sistemu Lokalnog CA ovise o tome postoji li *OBJECTSIGNING spremište certifikata. Ako *OBJECTSIGNING spremište certifikata ne postoji, možete koristiti prenesene datoteke certifikata kao način kreiranja *OBJECTSIGNING spremišta certifikata. Ako *OBJECTSIGNING certifikat postoji na ciljnom sistemu, morate na njega importirati prenesene certifikate.

***OBJECTSIGNING spremište certifikata ne postoji**

Zadaci koje obavljate za korištenje datoteka spremišta 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 spremište certifikata ne postoji na V5R3, V5R2, ili V5R1 ciljnom sistemu s prenešenim datotekama spremišta certifikata, izvedite ove korake:

1. Budite sigurni da su datoteke spremišta certifikata (dvije datoteke: jedna s .KDB ekstenzijom i jedna s .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 čine *OBJECTSIGNING spremište certifikata za ciljni sistem. Datoteke spremišta certifikata već sadrže kopije certifikata za mnoge javne Internet CA-ove. DCM ih je dodao, kao i kopiju Lokalnog CA certifikata, u datoteke spremišta 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 spremište certifikata trenutno postoji na ovom ciljnom sistemu. Zbog toga, ne smijete preimenovati prenešene datoteke kako je predloženo. Prepisivanje defaultnih datoteka za potpisivanje objekata će uzrokovati problem kod korištenja DCM-a, prenesenog spremišta certifikata i njegovog sadržaja. Kada *OBJECTSIGNING spremište certifikata već postoji, morate koristiti različitu obradu da stavite certifikate u postojeće spremište certifikata.
3. Pokrenite DCM. Sada morate promijeniti lozinku za *OBJECTSIGNING spremište certifikata. Promjenom lozinke se dopušta da DCM pohrani novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u spremištu certifikata.
4. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** da se otvori spremište certifikata.
5. Kad se prikaže stranica s lozinkom, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali na host sistemu i kliknite **Nastavak**.
6. U navigacijskom okviru izaberite **Upravljanje spremištem certifikata** i izaberite **Promjena lozinke** iz popisa zadataka. Popunite obrazac da promijenite lozinku za spremište certifikata. Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima. Zatim možete kreirati definiciju aplikacije koju certifikat koristi za potpisivanje objekata.
7. Nakon ponovnog otvaranja spremišta certifikata izaberite **Upravljanje aplikacijama** u navigacijskom okviru da se prikaže popis zadataka.
8. Iz popisa zadataka izaberite **Dodavanje aplikacije** da započnete postupak kreiranja definicije aplikacije za potpis objekata da koristite certifikat za potpis 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 **Upravljanje aplikacijama**.
11. Iz popisa zadataka izaberite **Ažuriranje dodjele certifikata** za prikaz popisa ID-ova aplikacija koje potpisuju objekte kojima ste dodijelili certifikat.
12. Izaberite ID vaše aplikacije s popisa i kliknite **Ažuriranje dodjele certifikata** .
13. Izaberite certifikat koji je Lokalni CA na host sistemu kreirao i kliknite **Dodjela novog certifikata**.

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

Kada distribuirate potpisane objekte, oni koji dobiju objekte moraju koristiti V5R3, V5R2, ili V5R1 verziju DCM-a da provjere potpis na objektima da osiguraju da su podaci nepromijenjeni i da provjere identitet odašiljača. Da provjeri potpis, primatelj mora imati kopiju certifikata za provjeru potpisa. Morate dobaviti kopiju ovog certifikata kao dio 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 s certifikatom od dobro poznatog Internet CA, verzija DCM-a primatelja već će imati kopiju potrebnog CA certifikata. Ipak, morate dobaviti kopiju CA certifikata, u odijeljenim paketima, zajedno s potpisanim objektima ako je potrebno. Na primjer, morate dobaviti kopiju Lokalnog CA certifikata ako ste potpisali objekte sa certifikatom od Lokalnog CA. Iz sigurnosnih razloga morate dobaviti CA certifikat u odijeljenim paketima, ili javno učiniti dostupnim CA certifikat na zahtjev onih koji ga trebaju.

***OBJECTSIGNING spremište certifikata postoji**

| Možete koristiti certifikate u prenešenim datotekama spremišta certifikata u postojećem *OBJECTSIGNING spremištu
| certifikata na V5R3, V5R2, ili V5R1 sistemu. Da to učinite, morate importirati certifikate iz datoteka spremišta
| certifikata u postojeće *OBJECTSIGNING spremište certifikata. Ipak, ne možete importirati certifikate izravno iz
| .KDB i .RDB datoteka, jer nisu u formatu koji DCM funkcija importa može prepoznati i koristiti. Možete dodati
| certifikate u postojeće *OBJECTSIGNING spremište certifikata otvaranjem prenešenih datoteka kao Spremišta
| certifikata drugog sistema na V5R3, V5R2, ili V5R1 ciljnom sistemu. Možete eksportirati certifikate izravno u
| *OBJECTSIGNING spremište certifikata. Morate eksportirati kopiju certifikata potpisivanja objekta i Lokalnog CA
| certifikata iz prenesenih datoteka.

| Da eksportirate certifikate iz datoteka spremišta certifikata izravno u *OBJECTSIGNING spremište certifikata,
| dovršite ove korake na V5R3, V5R2, ili V5R1 ciljnom sistemu:

1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i specificirajte **Spremište certifikata drugog sistema** da se otvori spremište certifikata.
3. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite potpuno kvalificirano ime staze i datoteke za datoteke spremišta certifikata. Također unesite lozinku koju ste koristili kada ste ih kreirali na host sistemu i kliknite **Nastavak**.
4. U navigacijskom okviru izaberite **Upravljanje spremištem certifikata** i izaberite **Promjena lozinke** iz popisa zadataka. Popunite obrazac da promijenite lozinku za spremište certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za spremište certifikata. Korištenje ove opcije osigurava da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novom spremištu. Ako ne promijenite lozinku i izaberete opciju Automatska prijava, možete naići na pogreške kod eksportiranja certifikata iz ovog spremišta u *OBJECTSIGNING spremište certifikata.

   Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima.
5. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite **Spremište certifikata drugog sistema** da se otvori spremište certifikata.
6. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite puno kvalificirano ime staze i datoteke za datoteku spremišta certifikata, unesite novu lozinku i kliknite **Nastavak**.
7. Nakon osvježenja navigacijskog okvira, izaberite **Upravljanje 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 **Nastavak**.

   Bilješka: Formulacija ovog zadatka podrazumijeva da kad radite sa Spremištem certifikata drugog sistema da radite s poslužiteljskim ili klijentskim certifikatima. To je zato što je ovaj tip spremišta certifikata oblikovan za upotrebu kao sekundarno spremište certifikata u *SYSTEM spremištu certifikata. Ipak, korištenje zadatka eksportiranja u ovom spremištu certifikata je najlakši način dodavanja certifikata iz prenesenih datoteka u postojeće *OBJECTSIGNING spremište certifikata.
9. Izaberite certifikat lokalnog CA za eksport i kliknite **Eksport**.

   Bilješka: Morate eksportirati Lokalni CA certifikat u spremište certifikata prije nego eksportirate certifikat potpisivanja objekata u spremište certifikata. Ako eksportirate prvo certifikat potpisivanja objekta, možete naići na grešku, jer Lokalni CA certifikat ne postoji u spremištu certifikata.
10. Izaberite **Spremište certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavak**.
11. Upišite *OBJECTSIGNING kao ciljno spremište certifikata, upišite lozinku za *OBJECTSIGNING spremište certifikata i kliknite **Nastavak**.
12. Sada možete eksportirati certifikat za potpisivanje objekta u *OBJECTSIGNING spremište certifikata. Ponovno izaberite zadatak **Eksport certifikata**.
13. Izaberite **Poslužitelj ili klijent** kao tip certifikata za eksport i kliknite **Nastavak**.
14. Izaberite odgovarajući certifikat za eksportiranje i kliknite **Eksportiraj**.
15. Izaberite **Spremište certifikata** kao odredište za eksportirani certifikat i kliknite **Nastavak**.
16. Upišite *OBJECTSIGNING kao ciljno spremište certifikata, upišite lozinku za *OBJECTSIGNING spremište certifikata i kliknite **Nastavak**. Prikazuje se poruka da pokaže da je certifikat uspješno eksportiran ili da pokaže informacije o grešci ako proces eksporta nije uspio.

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

Upotreba privatnog certifikata za SSL sesije na V4R5 ciljnom sistemu

Certifikatima, koje koriste vaše aplikacije za SSL sesije, upravljate iz *SYSTEM spremišta certifikata u Upravitelju digitalnih certifikata. Ako nikada niste koristili DCM na V4R5 ciljnom sistemu za upravljanje certifikatima za SSL, tada ovaj certifikat neće postojati na ciljnom sistemu. Prenesene datoteke spremišta 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 spremišta certifikata ovise o tome postoji li *SYSTEM spremište certifikata. Ako *SYSTEM spremište certifikata ne postoji, možete koristiti prenesene datoteke certifikata kao način za kreiranje *SYSTEM spremišta certifikata. Ako *SYSTEM certifikat postoji na ciljnom sistemu, možete koristiti prenesene datoteke certifikata na jedan od dva načina:

- Koristite prenesene datoteke kao Spremište certifikata drugog sistema.
- Importirajte prenesene datoteke u postojeće *SYSTEM spremište certifikata.

***SYSTEM spremište certifikata ne postoji**

Ako *SYSTEM spremište certifikata ne postoji na V4R5 sistemu na kojem želite koristiti prenešene datoteke spremišta certifikata, izvedite ove korake:

1. Budite sigurni da su datoteke spremišta certifikata (dvije datoteke: jedna s .KDB ekstenzijom i jedna s .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 čine *SYSTEM spremište certifikata za ciljni sistem. Datoteke spremišta certifikata već sadrže kopije certifikata za mnoge javne Internet CA-ove. DCM ih je dodao, kao i kopiju Lokalnog CA certifikata, u datoteke spremišta 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 spremište certifikata trenutno postoji na ovom ciljnom sistemu. Zbog toga, ne smijete preimenovati prenešene datoteke kako je predloženo. Prepisivanje defaultne datoteke će uzrokovati problem kod korištenja DCM-a, prenesenog spremišta certifikata i njegovog sadržaja. Umjesto toga morate osigurati da imaju jedinstvena imena i koristiti prenešene datoteke spremišta certifikata kao **Drugo** spremište certifikata. Ako koristite datoteke kao Drugo spremište certifikata, ne možete koristiti DCM da specificirate koje aplikacije će koristiti certifikat.
3. Pokrenite DCM. Sada morate promijeniti lozinku za *SYSTEM spremište certifikata. Promjenom lozinke se dopušta da DCM pohrani novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u spremištu certifikata.
4. U navigacijskom okviru, osigurajte da je *SYSTEM prikazano kao spremište certifikata u padajućoj kućici s popisom i izaberite **Certifikati sistema** za prikaz liste dostupnih zadataka. Prikazuje se prozor **Spremište certifikata i lozinka** .
5. U odgovarajuća polja, unesite *SYSTEM za spremište certifikata koje ćete otvoriti i lozinku koju ste koristili kada ste kreirali datoteke korištenjem Lokalnog CA na host sistemu. Sada možete promijeniti lozinku za spremište certifikata.
6. Iz popisa zadataka u navigacijskom okviru izaberite **Promjena lozinke**. Popunite obrazac da promijenite lozinku za spremište certifikata. Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima.
7. Nakon ponovnog otvaranja *SYSTEM spremišta certifikata, izaberite **Rad sa sigurnim aplikacijama** iz popisa zadataka za prikaz stranice koja vam dopušta upravljanje certifikatima pridružene specifičnim aplikacijama.
8. Iz popisa aplikacija izaberite aplikaciju koja će koristiti prenešeni privatni certifikat za SSL sesije.
9. Kliknite **Rad sa sistemskim certifikatima** i izaberite certifikat koji je izdao Lokalni CA na host sistemu.
10. Kliknite **Dodjela novog certifikata** 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 s tom podrškom mora biti postavljena tako da ima povjerenje u CA prije nego što će aplikacija moći provjeriti autentičnost certifikata, koje izdaje određeni CA. Koristite stranicu **Rad s Izdavačima certifikata** da osigurate da CA certifikat ima pouzdan status u spremištu certifikata. Tada, koristite stranicu **Rad sa sigurnim aplikacijama** da osigurate da aplikacije koje koriste certifikate imaju povjerenja u Lokalnog 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.

S ovim zadacima dovršenim, aplikacije na V4R5 ciljnom sistemu mogu koristiti certifikat izdan od strane V5R3 Lokalnog CA na drugom iSeries. 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 certifikat se mora kopirati u datoteku na korisnikovom PC računalu ili učitati u korisnikov pretražitelj, ovisno o zahtjevima aplikacije koja radi sa SSL.

***SYSTEM spremište certifikata postoji — upotreba datoteka kao Spremište certifikata drugog sistema**

Ako V4R5 ciljni sistem već ima *SYSTEM spremište certifikata, morate odlučiti kako raditi s datotekama certifikata koje ste prenijeli na ciljni sistem. Prenesene datoteke spremišta 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 **Spremište** certifikata drugog sistema. Ili, možete izabrati importiranje privatnog certifikata i njemu odgovarajućeg CA certifikata u postojeće *SYSTEM spremište certifikata.

Ako izaberete koristiti prenešene datoteke kao Spremište certifikata **drugog** sistema, ne možete koristiti DCM da specificirate koje će aplikacije koristiti certifikat za SSL sesije. Međutim, možete označiti certifikat u tom spremištu certifikata kao defaultni certifikat za spremište certifikata. Opcija Spremišta certifikata drugog sistema 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 spremište certifikata, a ne specifičnog certifikata.

Ako *SYSTEM spremište certifikata postoji na V4R5 sistemu na kojem želite koristiti prenešene datoteke spremišta certifikata, izvedite ove korake:

1. Pokrenite DCM. Sada morate promijeniti lozinku za preneseno spremište certifikata. Promjenom lozinke se dopušta da DCM pohrani novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u spremištu certifikata.
2. U navigacijskom okviru, osigurajte da je OTHER prikazano kao spremište certifikata u padajućoj kućici s popisom i izaberite **Certifikati sistema** za prikaz liste dostupnih zadataka. Prikazuje se prozor **Spremište certifikata i lozinka** .
3. U odgovarajućim poljima, unesite puno kvalificirano ime staze i datoteke za spremište certifikata (.KDB ekstenzija) koje ste prenijeli s Lokalnog CA host sistema. Unesite lozinku koju ste koristili kada ste kreirali datoteke na *host* sistemu. Sada možete promijeniti lozinku za spremište certifikata.
4. U navigacijskom okviru izaberite **Promjena lozinke** iz popisa zadataka Sistemskih certifikata. Popunite obrazac da promijenite lozinku za spremište certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za spremište certifikata. Korištenje ove opcije osigurava da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novom spremištu.

   Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima. Zatim možete odrediti da se certifikat u tom spremištu 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. Iz popisa certifikata izaberite certifikat, koji želite koristiti kao defaultni certifikat za trenutno spremište i kliknite **Postavi default** .

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

***SYSTEM spremište certifikata postoji — Importiranje datoteka u postojeće *SYSTEM spremište certifikata**

Prije nego možete importirati certifikate u *SYSTEM na V4R5 ciljnom sistemu, najprije morate eksportirati certifikate iz spremišta certifikata koje ste kreirali u različiti format datoteke. Zatim možete importirati certifikate u *SYSTEM spremište certifikata od novih datoteka. Prenesene datoteke spremišta 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 *SYSTEM spremište certifikata.

Bilješka: Funkcije eksportiranja dostupne u DCM-u za V4R5 nisu tako dobro razvijene kao one za V5R3 i možda ćete naići na probleme ako koristite ciljni sistem za eksportiranje privatnog Lokalni CA certifikata. Zbog toga, morate koristiti V5R3 host sistem da eksportirate *dodatnu* kopiju Lokalnog CA certifikata u zasebnu datoteku, a ne koristiti V4R5 ciljni sistem da ga eksportirate. Nakon što eksportirate Lokalni CA certifikat na V5R3 host sistem, možete ručno prenesti datoteku eksporta Lokalnog CA certifikata na V4R5 ciljni sistem i slijediti preostale korake u ovoj proceduri da importirate Lokalni CA certifikat u *SYSTEM spremište certifikata. Morate importirati certifikat lokalnog CA *prije* nego importirate privatni certifikat, kojeg ste s njim kreirali. Ako importirate prvo privatni certifikat, možete naići na grešku, jer Lokalni CA certifikat ne postoji u spremištu certifikata.

Da eksportirate certifikat iz datoteka spremišta certifikata, dovršite ove korake na V4R5 ciljnom sistemu:

1. Pokrenite DCM.
2. U navigacijskom okviru, osigurajte da je OTHER prikazano kao spremište certifikata u padajućoj kućici s popisom i izaberite **Certifikati sistema** za prikaz liste dostupnih zadataka. Prikazuje se prozor **Spremište certifikata i lozinka** .
3. Specificirajte puno kvalificirano ime staze i datoteke prenesenih datoteka spremišta certifikata, unesite lozinku koju ste koristili kada ste ih kreirali na *host* sistemu i kliknite **OK**. Sada možete promijeniti lozinku za spremište certifikata.
4. U navigacijskom okviru izaberite **Promjena lozinke** iz popisa zadataka Sistemskih certifikata. Popunite obrazac da promijenite lozinku za spremište certifikata.

   Bilješka: Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za spremište certifikata. Korištenje ove opcije osigurava da DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u novom spremištu. Ako ne promijenite lozinku i izaberete opciju Automatska prijava, možete naići na pogreške kod eksportiranja certifikata iz ovog spremišta.

   Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima.
5. U navigacijskom okviru izaberite **Rad sa certifikatima** da se prikaže popis certifikata.
6. Izaberite privatni certifikat s 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, možete imenovati datoteku 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 odgovarajuću 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.

Do ovog trenutka sigurno ste koristili DCM na originalnom V5R3 host sistemu za eksportiranje dodatne kopije Lokalnog CA certifikata i ručno ga prenesli u ASCII mod na V4R5 ciljni sistem. Sigurno ste koristili i DCM na ovom ciljnom sistemu da eksportirate certifikat privatnog poslužitelja ili klijenta u datoteku. Sada ste spremni za import ovih

certifikata u *SYSTEM spremište certifikata. Morate importirati certifikat lokalnog CA *prije* nego importirate privatni certifikat, kojeg ste s njim kreirali. Ako importirate prvo privatni certifikat, možete naići na grešku, jer Lokalni CA certifikat ne postoji u spremištu certifikata.

Da importirate certifikate iz ovih eksportiranih datoteka i specificirate da ih koriste SSL-omogućene aplikacije, dovršite ove korake na V4R5 ciljnom sistemu:

1. Pokrenite DCM.
2. U navigacijskom okviru, osigurajte da je *SYSTEM prikazano kao spremište certifikata u padajućoj kućici s popisom i izaberite **Certifikati sistema** za prikaz liste dostupnih zadataka. Prikazuje se prozor **Spremište certifikata i lozinka** .
3. Odredite *SYSTEM kao spremište certifikata za otvaranje, unesite lozinku i kliknite **Nastavak**.
4. Sada morate importirati Lokalni CA certifikat sa datoteke za eksport koju ste kreirali na V5R3 host sistemu. U navigacijskom okviru izaberite **Primanje CA certifikata** da se prikaže obrazac.
5. Dovršite obrazac i kliknite **OK** za prikaz stranice Uspješni prijem certifikata. Kad radite u *SYSTEM spremištu 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 s 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 će dati povjerenje CA certifikatu i kliknite **OK**. Prikazuje se stranica Status zaštićenih aplikacija na kojoj potvrđujete da su izabrane aplikacije određene da vjeruju novom certifikatu.
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 Importiraj certifikat i kliknite **OK** da se vratite na stranicu **Rad sa certifikatima**. Osigurajte da ste dobavili ime datoteke koja sadrži eksportirani certifikat poslužitelja ili klijenta i da ste specificirali ciljno izdanje koje se podudara s onima koje ste specificirali kod prethodnog eksportiranja certifikata. Na vrhu stranice će se prikazati poruka da je DCM dodao certifikat u trenutno spremište certifikata. Certifikat koji ste importirali pojavit će se također i na listi certifikata.
10. Sada morate specificirati koje će aplikacije koristiti importirani privatni certifikat za SSL. U navigacijskom okviru, izaberite **Rad sa sigurnim aplikacijama** za prikaz stranice koja vam dopušta upravljanje certifikatima pridružene specifičnim aplikacijama.
11. Izaberite neku aplikaciju s popisa i kliknite **Rad sa sistemskim certifikatima** za prikaz popisa certifikata koje možete specificirati da izabrana aplikacija koristi za uspostavljanje SSL sesija.
12. Izaberite certifikat s popisa i kliknite **Dodjela novog certifikata** da dodijelite izabrani certifikat navedenoj aplikaciji. Na vrhu stranice se pojavljuje poruka potvrde za izbor certifikata.

Sa završenim ovim zadacima, aplikacije na V4R5 ciljnom sistemu mogu koristiti certifikat izdan od lokalnog CA na drugom poslužitelju. 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 certifikat 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

Upravitelja digitalnih certifikata (DCM) možete koristiti 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 spremišta certifikata u kojem radite. Možete upravljati aplikacijama samo iz *SYSTEM ili *OBJECTSIGNING spremišta 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 dodjelom certifikata za aplikaciju opisuje kako dodijeliti ili promijeniti certifikat koji aplikacija koristi za uspostavljanje SSL sesije ili potpisivanje objekata.

Definiranje CA liste povjerenja za aplikaciju opisuje kada možete i morate 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 s 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 s definicijama SSL aplikacija i njihovim certifikatima, aplikacija mora prvo biti registrirana s 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 SSL-omogućene aplikacije se registriraju s DCM-om tako da možete lako koristiti DCM da im dodijelite certifikat i da onda one 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 *SYSTEM spremištu certifikata za kreiranje definicije SSL aplikacije za aplikaciju klijenta ili za 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 može opisivati tip ili grupu objekata koje namjeravate potpisati. Morate raditi u *OBJECTSIGNING spremištu certifikata da bi kreirali definiciju aplikacije za potpisivanje objekta.

Da kreirate definiciju aplikacije, izvedite ove korake:
1. Pokrenite DCM.
2. Kliknite **Izbor spremišta certifikata** i izaberite odgovarajuće spremište certifikata. (To je ili *SYSTEM ili *OBJECTSIGNING spremište 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 online pomoći.
3. Kad se prikaže stranica Spremište certifikata i lozinki, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
4. U navigacijskom okviru izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
5. Izaberite **Dodavanje aplikacije** iz popisa zadataka da se prikaže obrazac za definiranje aplikacije.

   Bilješka: Ako radite u *SYSTEM spremištu 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 valjanosti klijenta i morate zahtijevati provjeru valjanosti 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, izvedite ove korake:

1. Pokrenite DCM.
2. Kliknite **Izbor spremišta certifikata** i izaberite odgovarajuće spremište certifikata. (To je ili *SYSTEM ili *OBJECTSIGNING spremište 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 online pomoći.
3. Kad se prikaže stranica Spremište certifikata i lozinki, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
4. U navigacijskom okviru izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
5. Ako ste u *SYSTEM spremištu certifikata, izaberite tip aplikacije za upravljanje. (Izaberite ili **Poslužitelj** ili **Klijent** aplikaciju, kako je prikladno.)
6. Iz popisa zadataka izaberite **Ažuriranje dodjele certifikata** za prikaz popisa aplikacija kojima možete dodijelili certifikat.
7. Izaberite neku aplikaciju s popisa i kliknite **Ažuriranje dodjele certifikata** za prikaz popisa certifikata koje možete dodijeliti aplikaciji.
8. Izaberite certifikat s popisa i kliknite **Dodjela novog certifikata**. 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, poslužitelji iSeries Access za Windows će primijeniti svaku promjenu certifikata koju možete učiniti automatski. 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 od 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 u toku 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.

Upravitelja digitalnih certifikata (DCM) možete koristiti za definiranje u 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, izvedite ove korake:
1. Pokrenite DCM.
2. Kliknite **Izbor spremišta certifikata** i izaberite *SYSTEM da se otvori spremište certifikata.

   Bilješka: Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
3. Kad se prikaže stranica Spremište certifikata i lozinki, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
4. U navigacijskom okviru izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
5. Iz popisa zadataka izaberite **Definiranje liste pouzdanih CA-ova**.
6. Izaberite tip aplikacije (poslužitelj ili klijent) za koju želite definirati popis i kliknite **Nastavak**.
7. Izaberite neku aplikaciju s popisa i kliknite **Nastavak** za prikaz popisa CA certifikata koje koristite za definiranje pouzdanog popisa.
8. Izaberite CA-ove kojima će apikacija vjerovati i kliknite **OK**. DCM prikazuje poruku da potvrđuje vaše izbore pouzdanih popisa.

   Bilješka: Možete ili izabrati pojedinačne CA-ove s popisa, ili možete specificirati da će aplikacija vjerovati svima, ili niti jednom CA-u na listi. Također možete pogledati ili provjeriti valjanost CA certifikata prije nego ga dodate na pouzdani popis.

Upravljanje certifikatima pomoću isteka

Upravitelj digitalnih certifikata (DCM) osigurava podršku za upravljanje istekom certifikata i omogućuje administratorima da upravljaju poslužiteljskim ili klijentskim certifikatima, certifikatima za potpisivanje objekata i korisničkim certifikatima prema datumu isteka na lokalnom poslužitelju. Dodatno, ako konfigurirate DCM za rad s Mapiranjem identiteta u poduzeću (EIM), možete upravljati korisničkim certifikatima po datumu isteka u poduzeću.

Upotrebom DCM-a za gledanje certifikata na osnovu njihovog datuma isteka dozvoljava vam da odredite brzo i jednostavno koji certifikati su blizu isteku, tako da certifikati mogu biti na vrijeme obnovljeni.

Opaska: Zato što možete koristiti certifikat za provjeru potpisa objekata čak i kada je certifikat istekao, DCM ne omogućuje podršku za provjeru isteka ovih certifikata.

Da pogledate i upravljate certifikatima poslužitelja i klijenta, ili certifikatima za potpisivanje objekata na osnovu datuma njihovog isteka, izvedite ove korake:
1. Pokrenite DCM.

   Bilješka: Ako imate pitanja o tome kako popuniti specifičan obrazac koristeći DCM, izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ili ***OBJECTSIGNING** ili ***SYSTEM** da se otvori spremište certifikata.
3. Unesite lozinku za spremište certifikata i kliknite **Nastavak**.
4. Nakon osvježenja navigacijskog okvira izaberite**Upravljanje certifikatima** za prikaz popisa zadataka.
5. Iz popisa zadataka izaberite **Provjera isteka**.
6. Izaberite tip certifikata koji želite provjeriti. Ako ste u *SYSTEM spremištu certifikata izaberite **Poslužitelj ili klijent**; ako ste u *OBJECTSIGNING spremištu certifikata izaberite **Potpisivanje objekta**.
7. U polju **Raspon datuma isteka u danima (1-365)**, upišite broj dana za koji treba pogledati certifikate na osnovu njihovog datuma isteka i kliknite **Nastavak**. DCM prikazuje sve certifikate koji ističu između današnjeg datuma i datuma koji odgovara broju dana koji ste specificirali. DCM također prikazuje sve certifikate koji imaju datume isteka prije današnjeg datuma.
8. Izaberite certifikat kojim želite upravljati. Možete izabrati da pogledate detalje informacija o certifikatu, brisanje certifikata, ili obnavljanje certifikata.

9. Kada završite rad s certifikatima s popisa, kliknite **Opoziv** za izlaz.

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 zahtijeva certifikate. Takvi problemi mogu spriječiti aplikaciju od sudjelovanja u sesiji Sloj sigurnih utičnica (SSL), ili u uspješnom potpisivanju objekata.

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 Liste opozvanih certifikata (CRL) radi 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 Listi 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 trenutnom spremištu 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 s javnim ključem i tada jamči da se podaci mogu dešifrirati s privatnim ključem.

Dodjela certifikata aplikacijama

Počevši s V5R2, nova poboljšanja Upravitelja digitalnih certifikata (DCM) vam omogućavanju dodjelu certifikata brzo i jednostavno za više aplikacija. Možete dodijeliti certifikat za više aplikacija u *SYSTEM ili *OBJECTSIGNING spremištu certifikata.

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

   Bilješka: Ako imate pitanja o tome kako popuniti specifičan obrazac koristeći DCM, izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ili ***OBJECTSIGNING** ili ***SYSTEM** da se otvori spremište certifikata.
3. Unesite lozinku za spremište certifikata i kliknite **Nastavak**.
4. Nakon osvježenja navigacijskog okvira izaberite**Upravljanje certifikatima** za prikaz popisa zadataka.
5. Iz popisa zadataka izaberite **Dodjela certifikata** da prikažete listu certifikata za trenutno spremište certifikata.
6. Izaberite certifikat s popisa i kliknite **Dodjela aplikacijama** da prikažete listu definicija aplikacija za trenutno spremište certifikata.
7. Izaberite jednu ili više aplikacija s popisa i kliknite **Nastavak**. Prikazuje se stranica ili s porukom potvrde za vaš izbor dodjela ili s porukom o grešci ako se dogodio problem.

Upravljanje CRL lokacijama

Upravitelj digitalnih certifikata (DCM) vam omogućava da definirate informacije o lokaciji Liste opoziva certifikata (CRL) za korištenje od određenog Izdavača certifikata (CA) kao dio procesa provjere valjanosti certifikata. DCM ili aplikacija koja zahtijeva 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 izvede 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 provjeru 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, izvedite ove korake:

1. Pokrenite DCM.
2. U navigacijskom okviru izaberite **Upravljanje lokacijama** za prikaz popisa zadataka.
3. Izaberite **Dodavanje CRL lokacije** s liste zadataka za prikaz obrasca koji možete koristiti za opis CRL lokacije i kako će 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 **Upravljanje certifikatima** za prikaz popisa zadataka.
6. Izaberite **Promjena dodjele CRL lokacije** s liste zadataka da prikažete listu CA certifikata.
7. Izaberite CA certifikat iz liste kojoj želite dodijeliti CRL definiciju lokacije koju ste kreirali i kliknite **Promjena dodjele CRL lokacije**. Prikazuje se lista CRL lokacija.
8. Izaberite CRL lokaciju s 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 za vrijeme izvođenja CRL obrade. Međutim, prije nego se CRL obrada može izvoditi, Usluge Direktorija moraju sadržavati odgovarajući CRL. Također, morate konfigurirate oboje, aplikacije Poslužitelja direktorija (LDAP) i klijenta za upotrebu SSL-a i dodijeliti certifikat aplikacijama u DCM-u.

Da naučite više o konfiguriranju i upotrebi iSeries Poslužitelja direktorija (LDAP), pregledajte ova pogavlja Informacijskog Centra:

- IBM Poslužitelj direktorija za iSeries (LDAP)
  Ovo poglavlje govori vam sve što trebate znati o konfiguriranju i upotrebi iSeries Poslužitelja direktorija.
- Omogući SSL na Poslužitelju direktorija
  Ovo poglavlje objašnjava što trebate znati da konfigurirate vaš Poslužitelj direktorija za upotrebu SSL-a za sigurne komunikacije.

Spremanje ključeva certifikata u IBM Kriptografički koprocesor

Ako ste instalirali IBM Kriptografički koprocesor na vašem iSeries, možete koristiti koprocesor da omogućite sigurniju pohranu za privatni ključ 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:
- Spremanje privatnog ključa certifikata izravno u koprocesoru.
- Upotreba glavnog ključa koprocesora za šifriranje privatnog ključa za pohranjivanje u posebnu datoteku ključa.

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

Za upotrebu koprocesora za pohranu privatnog ključa, morate osigurati da je koprocesor u stanju Varied on prije upotrebe Upravitelja digitalnih certifikata (DCM). Inače DCM neće pribaviti stranicu za izbor opcije memorije kao dijela kreiranja certifikata ili postupka obnavljanja.

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

Spremanje privatnog ključa certifikata izravno u koprocesor

Za jače zaštićen pristup i upotrebu privatnog ključa certifikata, možete izabrati pohranu ključa izravno na IBM Kriptografički koprocesor. Možete izabrati ovu opciju pohranjivanja ključa kao dijela kreiranja ili obnavljanja certifikata u Upravitelju digitalnih certifikata (DCM).

Slijedite ove korake sa stranice **Izbor lokacije memorije ključa** da pohranite certifikatov privatni ključ izravno na koprocesor:
1. Izaberite **Hardver** kao vašu opciju memorije.
2. Kliknite **Nastavak**. Ovim se pokazuje stranica **Izaberi opis kriptografičkog uređaja**.
3. Izaberite s popisa uređaja onaj, kojeg želite upotrijebiti za pohranjivanje certifikatovog privatnog ključa.
4. Kliknite **Nastavak**. DCM nastavlja prikazivati stranice za zadatke koje dovršavate, kao što su identifikacijske informacije za certifikat, kojeg kreirate ili obnavljate.

Upotreba glavnog ključa koprocesora za šifriranje privatnog ključa

Za jače zaštićen pristup i upotrebu privatnog ključa certifikata, možete koristiti glavni ključ IBM Kriptografičkog koprocesora da šifrirate privatni ključ i pohranite ključ u posebnu datoteku za ključeve. Možete izabrati ovu opciju pohranjivanja ključa kao dijela kreiranja ili obnavljanja certifikata u Upravitelju digitalnih certifikata (DCM).

Prije nego možete uspješno koristiti ovu opciju, morate upotrijebiti konfiguraciju IBM Kriptografički koprocesor Web sučelja da kreirate odgovarajuću datoteku za pohranu ključeva. Također, morate koristiti koprocesorsku konfiguraciju Web sučelja za pridruživanje datoteke za pohranu ključeva opisu koprocesorskog uređaja koji želite koristiti. Možete pristupiti koprocesorskoj konfiguraciji Web sučelja sa stranice iSeries Zadaci.

Ako vaš sistem ima instaliran više od jednog koprocesorskog uređaja i u stanju varied on, možete dijeliti certifikatove privatne ključeve između 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 **Izbor lokacije 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 **Nastavak**. Ovim se pokazuje stranica **Izaberi opis kriptografičkog uređaja**.
3. Izaberite s popisa uređaja onaj, kojeg želite upotrijebiti za šifriranje certifikatovog privatnog ključa.
4. Kliknite **Nastavak**. Ako imate instaliran više od jednog koprocesora i u stanju varied on, prikazuje se stranica **Izbor dodatnih opisa kriptografičkog uređaja** .

   Bilješka: Ako nemate više dostupnih koprocesorskih uređaja, DCM nastavlja prikazivati stranice za zadatke koje dovršavate, kao što su identifikacijske informacije za certifikat koji kreirate ili obnavljate.
5. Izaberite iz popisa uređaja ime jednog ili više opisa uređaja s 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 glavni ključ jednak na uređajima, koristite zadatak Provjera Glavnog Ključa u Web sučelju 4758 Konfiguracija Kriptografičkog koprocesora. Možete pristupiti Web sučelju konfiguracije koprocesora sa stranice iSeries Zadaci.
6. Kliknite **Nastavak**. DCM nastavlja prikazivati stranice za zadatke koje dovršavate, kao što su identifikacijske informacije za certifikat, kojeg kreirate ili obnavljate.

Upravljanje lokacijom zahtjeva za PKIX CA

Infrastruktura Javnog Ključa za X.509 (PKIX) Izdavač certifikata (CA) je CA koji izdaje certifikate na osnovu najnovijih Internet X.509 standarda za implementaciju infrastrukture javnog ključa. PKIX standardi su navedeni u Request For Comments (RFC) 2560.

PKIX CA zahtijeva strožu identifikaciju prije izdavanja certifikata; obično tražeći da prijavljeni pruži dokaz o identitetu preko Izdavača registracije (RA). Nakon što zahtjevatelj dobavi dokaz o identitetu kojeg zahtijeva RA, RA potvrđuje njegov 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. Možete istražiti upotrebu PKIX mogućeg CA ako vaše potrebe sigurnosti zahtijevaju čvrstu kontrolu pristupa izvorima koje vaše SSL-omogućene aplikacije dobavljaju 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 **Upravljanje 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**.

Upravljanje LDAP lokacijom za korisničke certifikate

Po defaultu, Upravitelj digitalnih certifikata (DCM) sprema korisničke certifikate koje lokalni Izdavač certifikata (CA) izdaje s i5/OS korisničkim profilima. Ipak, možete konfigurirati Upravitelja digitalnih certifikata (DCM) zajedno s Mapiranjem identiteta u poduzeću (EIM) tako da kada Lokalni Izdavač certifikata (CA) izda korisničke certifikate, javna kopija certifikata se pohranjuje u specifičnu lokaciju Lightweight Directory Access Protocol (LDAP) poslužiteljskog direktorija. Kombinirana konfiguracija EIM-a s DCM-om dozvoljava vam da pohranite korisničke

certifikate u lokaciju LDAP direktorija da napravite certifikate spremnijim za druge aplikacije. Ova kombinirana konfiguracija također vam dozvoljava upotrebu EIM-a za upravljanje korisničkim certifikatima kao tip korisničkog identiteta unutar vašeg poduzeća.

Opaska: Ako želite da korisnik pohrani certifikat s drugog CA u LDAP lokaciji, korisnik mora dovršiti zadatak **Dodjela korisničkog certifikata**.

EIM je eServer tehnologija koja vam omogućuje upravljanje korisničkim identitetima u vašem poduzeću, uključujući i5/OS korisničke profile i korisničke certifikate. Ako želite koristiti EIM za upravljanje korisničkim certifikatima, trebate izvesti ove zadatke EIM konfiguracije prije izvođenja bilo kakvih zadataka DCM konfiguracije:

1. Koristite čarobnjaka **EIM Konfiguracije** u **iSeries Navigatoru** da konfigurirate EIM.
2. Kreirajte EIM identifikator za svakog korisnika za kojeg želite da sudjeluje u EIM-u.
3. Kreirajte ciljnu asocijaciju između svakog EIM identifikatora i korisničkog profila tog korisnika u lokalnom i5/OS korisničkom registru. Koristite ime definicije EIM registra za za lokalni i5/OS korisnički registar koji ste naveli u čarobnjaku **EIM konfiguracije**. **Opaska:** Za više informacija o konfiguriranju EIM-a, pogledajte EIM poglavlje u iSeries Informacijskom Centru.

Nakon što dovršite potrebne zadatke EIM konfiguracije, morate izvesti sljedeće zadatke da završite ukupnu konfiguraciju za upotrebu EIM-a i DCM-a zajedno:

1. U DCM-u, koristite zadatak **Upravljanje LDAP lokacijom** da specificirate LDAP direktorij koji će DCM koristiti za pohranu korisničkih certifikata koje kreira Lokalni CA. LDAP lokacija ne treba biti na lokalnom poslužitelju, niti ne treba biti na istom LDAP poslužitelju koji koristi i EIM. Kada konfigurirate LDAP lokaciju u DCM-u, DCM koristi specificirani LDAP direktorij za pohranu svih korisničkih certifikata koje Lokalni CA izdaje. DCM također koristi LDAP lokaciju za pohranu korisničkih certifikata obrađenih zadatkom **Dodjela korisničkog certifikata** umjesto pohrane certifikata s korisničkim profilom.
2. Izvedite naredbu **Konvertiranje korisničkih certifikata** (CVTUSRCERT). Ova naredba kopira postojeće korisničke certifikate u odgovarajuću lokaciju LDAP direktorija. Ipak, naredba kopira samo certifikate za korisnika koji je imao ciljno udruženje kreirano između EIM identifikatora i korisničkog profila. Naredba zatim kreira udruženje izvora između svakog certifikata i pridruženog EIM identifikatora. Naredba koristi razlikovno ime subjekta (DN) certifikata, DN izdavača i raspršenje ovih DN-ova zajedno s javnim ključem certifikata za definiranje imena korisničkog identiteta za udruženje izvora.

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. Počevši od V5R2, možete koristiti iSeries Navigator funkciju Središnjeg upravljanja za potpisivanje objekata dok ih pakirate za distribuciju na druge poslužitelje.

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 potpisati objekte koji su spremljeni na drugim poslužiteljima.

Možete potpisivati objekte sa certifikatima koje kupujete od javnog Internet Izdavača certifikata (CA) ili one koje kreirate s 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 kreirano *OBJECTSIGNING spremište certifikata, ili kao dio procesa kreiranja Lokalnog CA ili kao dio procesa upravljanja certifikatima potpisivanja objekata od javnog Internet CA.

- *OBJECTSIGNING spremište 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.

Upotreba DCM-a za potpisivanje objekata

Za korištenje DCM-a za potpisivanje jednog ili više objekata, izvedite ove korake:
1. Pokrenite DCM.

   Bilješka: Ako imate pitanja o tome kako popuniti specifičan obrazac koristeći DCM, izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** da se otvori spremište certifikata.
3. Unesite lozinku za *OBJECTSIGNING spremište certifikata i kliknite **Nastavak**.
4. Nakon osvježenja navigacijskog okvira, izaberite **Upravljanje potpisivim objektima** za prikaz popisa zadataka.
5. Iz popisa zadataka izaberite **Potpisivanje objekta** za prikaz popisa definicija aplikacija koje možete koristiti za potpisivanje objekata.
6. Izaberite neku aplikaciju i kliknite **Potpisivanje objekta** da vidite obrazac za određivanje lokacije objekata koje želite potpisati.

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

   Bilješka: Morate pokrenuti ime objekta s 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 svih objekata u specifičnom direktoriju, možete upisati /mydirectory/*; za potpisivanje svih programa u specifičnoj knjižnici, možete upisati /QSYS.LIB/QGPL.LIB/*.PGM. Možete koristiti ove generičke znakove samo u zadnjem dijelu imena staze; na primjer, /mydirectory*/filename rezultira u poruci greške. Ako želite koristiti funkciju Pregled da pogledate popis knjižnica ili sadržaja direktorija, morate upisati generički znak kao dio imena staze prije nego kliknete na **Pregled**.
8. Izaberite opcije obrada koje želite koristiti za potpisivanje izabranog objekta ili objekata i kliknite **Nastavak**.

   Bilješka: Ako odlučite čekati rezultate posla, prikazati će se datoteka rezultata izravno 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 za vrijeme obrade objekta) ili polje podataka (pokazujući podatke na kojima se obavlja posao).
9. Specifirajte potpuno kvalificirano ime i stazu datoteke za korištenje u pohranjivanju rezultata posla za potpisivanje objekta i kliknite **Nastavak**. Ili unesite lokaciju direktorija i kliknite **Pregled** da pogledate sadržaje direktorija te da izaberete 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.

Provjera 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 kreirano *SIGNATUREVERIFICATION spremište certifikata za upravljanje vašim certifikatima za provjeru potpisa.

  Bilješka: Možete provesti provjeru potpisa za vrijeme rada u *OBJECTSIGNING spremištu certifikata u slučajevima kad provjeravate potpise za objekte koji su potpisani na istom sistemu. Koraci koje izvodite za provjeru potpisa u DCM-u su isti u oba spremišta certifikata. Međutim, *SIGNATUREVERIFICATION spremište certifikata mora postojati i mora sadržavati kopiju certifikata koji je potpisao objekt čak i ako radite provjeru potpisa za vrijeme rada unutar *OBJECTSIGNING spremišta certifikata.
- *SIGNATUREVERIFICATION spremište certifikata mora sadržavati kopiju certifikata koji je potpisao objekte.
- *SIGNATUREVERIFICATION spremište certifikata mora sadržavati kopiju certifikata CA koji je izdao certifikat koji je potpisao objekte.

Upotreba DCM-a za provjeru potpisa objekata

Da koristite DCM za provjeru potpisa objekata izvedite ove korake:

1. Pokrenite DCM.

   Bilješka: Ako imate pitanja o tome kako popuniti specifičan obrazac koristeći DCM, izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
2. U navigacijskom okviru kliknite**Izbor spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** za otvaranje.
3. Unesite lozinku za *SIGNATUREVERIFICATION spremište certifikata i kliknite **Nastavak**.
4. Nakon osvježenja navigacijskog okvira, izaberite **Upravljanje potpisivim objektima** za prikaz popisa zadataka.
5. Iz popisa zadataka izaberite **Provjera potpisa objekta** za specifikaciju lokacija objekata za koje želite provjeru potpisa.
6. U dobiveno polje unesite potpuno kvalificirano ime i stazu datoteke objekta ili direktorija objekata za koje želite provjeriti potpise i kliknite**Nastavak**. Ili unesite lokaciju direktorija i kliknite **Pregled** da vidite sadržaje direktorija i da izaberete 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 specifičnom direktoriju, možete upisati /mydirectory/*; za potpisivanje svih programa u specifičnoj knjižnici, možete upisati /QSYS.LIB/QGPL.LIB/*.PGM. Možete koristiti ove generičke znakove samo u zadnjem dijelu imena staze; na primjer, /mydirectory*/filename rezultira u poruci greške. Ako želite koristiti funkciju Pregled da pogledate popis knjižnica ili sadržaja direktorija, morate upisati generički znak kao dio imena staze prije nego kliknete na **Pregled**.
7. Izaberite opcije obrada koje želite koristiti za provjeru potpisa izabranog objekta ili objekata i kliknite **Nastavak**.

   Bilješka: Ako odlučite čekati rezultate posla, prikazati će se datoteka rezultata izravno 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 u toku obrade objekta) ili polje podataka (pokazujući podatke na kojima se obavlja posao).

8. Specifirajte potpuno kvalificirano ime i stazu datoteke za korištenje u pohranjivanju rezultata posla za provjeru potpisa objekta i klikniteNastavak . Ili unesite lokaciju direktorija i kliknite **Pregled** da pogledate sadržaje direktorija da izaberete 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 s objektom, odredite da li je objekt iz izvora kojem vjerujete.

Poglavlje 9. Rješavanje problema DCM-a

Kada radite s Upraviteljem digitalnih certifikata (DCM) i certifikatima, možete se susresti s greškama koje vas sprečavaju u postizanju vaših zadataka i ciljeva. Mnogo čestih grešaka ili problema s kojima se možete susresti spadaju u različite kategorije, kao što su sljedeće:

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

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

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

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

Rješavanje problema zadatka Dodjela korisničkog certifikata
Koristite ove informacije da se upoznate s 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 s Upraviteljem digitalnih certifikata (DCM).

Problem	Moguće rješenje
Ne možete naći dodatnu pomoć za DCM.	U DCM-u, kliknite **?**″ ikonu pomoći. Možete također pretražiti Informacijski centar i vanjske IBM Web stranice na Internetu.
Vaša lozinka za lokalnog izdavača certifikata (CA) i *SYSTEM spremište certifikata ne radi.	Lozinke razlikuju mala i velika slova. Pazite da veličina slova bude ista kao i kad ste lozinku dodijelili.
Vaš pokušaj da resetirate lozinku kada ste koristili zadatak **Izbor spremišta certifikata** nije uspio.	Funkcija za ponovno postavljanje radi samo ako je DCM pohranio lozinku. DCM pohranjuje lozinku automatski kada kreirate spremište certifikata. Ipak, ako promijenite (ili ponovno postavite) lozinku na Spremištu certifikata drugog sistema, tada morate izabrati opciju **Automatska prijava** tako da DCM nastavlja skrivati lozinku.
	Također, ako premjestite spremište certifikata s jednog sistema na drugi, morate promijeniti lozinku za spremište certifikata na novom sistemu da osigurate da je DCM automatski skriva. Za promjenu lozinke, morate dobaviti originalnu lozinku za spremište certifikata kad ga otvorite na novom sistemu. Ne možete koristiti opciju ponovnog postavljanja lozinke dok niste otvorili spremište s 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 spremište certifikata koje ćete koristiti kao Spremište certifikata drugog sistema, morate izabrati opciju **Automatska prijava** kada mijenjate lozinku da osigurate da DCM skriva novu lozinku za ovaj tip spremišta certifikata.

Problem	Moguće rješenje
	Provjerite vrijednost dodijeljenu atributu **Dozvoli nove digitalne certifikate** pod opcijom **Rad sa sistemskom sigurnosti** Sistemskih servisnih alata (SST). Ako je ovaj atribut postavljen na vrijednost 2 (Ne), tada lozinka spremišta certifikata ne može biti ponovno postavljena. Možete pogledati ili promijeniti vrijednost za ovaj atribut upotrebom naredbe STRSST i upisom ID-a korisnika i lozinke za Servisne alate. Zatim 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 na vaš sistem.	Neki CA-ovi ne nude gotove CA certifikate. Ako ne možete dobiti CA certifikat od CA, obratite se svom dobavljaču, jer je vaš dobavljač možda sklopio neki posebni sporazum ili sporazum oko načina plaćanja s CA-om.
Ne možete naći *SYSTEM spremište certifikata.	Mjesto datoteke *SYSTEM certifikata mora biti /qibm/userdata/icss/cert/server/default.kdb. Ako to spremište certifikata ne postoji, trebate upotrijebiti DCM i kreirati spremište certifikata. Koristite zadatak **Kreiranje novog spremišta 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 ponovno pokrenite pretražitelj.
Imate problem Direktorija usluga (LDAP) kao što je neprikazivanje dodjele certifikata kada su informacije o sigurnim aplikacijama prikazane odmah nakon dodjele certifikata. Ovaj se problem dešava češće kod korištenja iSeries Navigatora za dobivanje Netscape Communications pretražitelja. Vaša preferenca za predmemoriju pretražitelja postavljena je za usporedbu dokumenta u predmemoriji s dokumentom na mreži **Jednom po sesiji**.	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 ponovno. Također provjerite da li vaš poslužitelj ima ispravnu vrijednost za UTC pomak (dspsysval qutcoffset). Ako promatrate ljetno računanje vremena, 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 u pravom formatu kad ga pokušate koristiti na poslužitelju. Neka oblikovanja Web stranica uzrokuju ovaj problem. Druge Web stranice su oblikovane da izbjegnu ovaj problem. Svakako usporedite izgled originalnog certifikata s rezultatom funkcije zalijepi, jer zalijepljene informacije moraju izgledati jednako.

Rješavanje problema spremišta certifikata i baze podataka ključeva

Koristite sljedeću tablicu da nađete informacije da vam pomognu u rješavanju češćih problema spremišta certifikata i baze podataka ključeva koje možete susresti za vrijeme rada s 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 /.

Problem	Moguće rješenje

Kreiranje baze podataka ključeva nije uspjelo, ili kreiranje Lokalnog CA nije uspjelo.	Provjerite da li postoji sukob imena datoteka. Možda je sukob u nekoj drugoj datoteci, a ne u onoj koju ste zatražili. DCM pokušava zaštititi korisničke podatake u direktorijima koje kreira, čak i ako te datoteke sprečavaju DCM da uspješno kreira datoteke kada to treba učiniti.
	
	Ovo riješite tako da kopirate sve datoteke koje su u sukobu u neki drugi direktorij i, ako je moguće, upotrijebite funkciju DCM-a za brisanje odgovarajućih datoteka. Ako ne možete upotrijebiti DCM da to obavite, ručno izbrišite datoteke iz direktorija integriranog sistema datoteka, tamo gdje je postojao sukob s DCM-om. Pazite da zabilježite točno one datoteke koje premještate i kamo ih premještate. Kopije vam omogućuju da vratite datoteke ako uvidite da vam još trebaju. Trebate kreirati novi Lokalni CA nakon uklanjanja sljedećih datoteka:
	`/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 novo *SYSTEM spremište certifikata i sistemski certifikat nakon premještanja 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`

	Možda će vam nedostajati preduvjetni licencni program (LPP) za koji DCM zahtijeva da bude instaliran. Provjerite listu DCM preduvjeta i osigurajte da svi licencni programi budu ispravno instalirani.

Problem	Moguće rješenje
Sistem ne prihvaća CA tekst datoteku koja je prenesena u binarnom načinu s drugog sistema. On prihvaća tu datoteku kad se prenosi u American National Standard Code for Information Interchange (ASCII kodu).	Prstenovi ključeva i baze podataka ključeva su binarni i stoga različiti. Morate upotrijebiti Protokol za prijenos datoteka (FTP) u ASCII načinu za CA tekstualne datoteke i FTP u binarnom načinu za binarne datoteke, kao što su datoteke s 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 spremišta certifikata i zatim pokušajte promijeniti lozinku. Ako u svom spremištu certifikata imate istekle certifikate, tada istekli certifikati nisu više važeći. S obzirom na to da certifikati više ne važe, funkcija promjene lozinke spremišta certifikata ne mora dopustiti promjenu lozinke, a postupak šifriranja neće šifrirati privatni ključ certifikata kojem je važenje isteklo. Ovime se sprečava promjena lozinke, a sistem može javiti da je jedan od razloga oštećenje spremišta certifikata. Nevažeće (one koje su istekle) certifikate morate ukloniti iz spremišta certifikata.
Trebate koristiti certifikate za Internet korisnika i stoga trebate koristiti validacijske liste. Međutim, DCM ne pruža funkcije za validacijske liste.	Poslovni partneri koji pišu aplikacije za korištenje validacijskih listi moraju ih tako kodirati da validacijske liste pridruže aplikacijama kako se i očekuje. Moraju kodirati tako da odrede kada je identitet korisnika Interneta provjeren na odgovarajući način, tako da se certifikat može dodati u validacijsku listu. Pregledajte poglavlje Informacijskog Centra za QsyAddVldlCertificate API. Posavjetujte se s dokumentacijom HTTP Poslužitelja za iSeries za pomoć kod konfiguriranja sigurne instance HTTP poslužitelja za upotrebu validacijske liste.

Rješavanje problema pretražitelja

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

Problem	Moguće rješenje
Microsoft Internet Explorer vam ne dozvoljava da izaberete različit certifikat dok ne pokrenete novu sesiju pretražitelja.	Počnite s novom pretražiteljskom sesijom na Internet Explorer-u.
Internet Explorer ne pokazuje sve izborne 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 s istim korisničkim imenom kao ono ime s kojim je stavljen korisnički certifikat u pretražitelja. Dohvatite drugi korisnički certifikat sa sistema kojem pristupate. Sistem administrator mora biti siguran da spremište certifikata (baza podataka ključeva) još uvijek vjeruje CA-u koji je potpisao korisnički i sistemski certifikat.
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 s većinom korisničkih upotreba. Osim ako znate što činite, najbolje je da ime poslužitelja ili ime sistema ostavite takvim kakvo je bilo. Morate također provjeriti da je poslužitelj imena domene ispravno postavljen.

Problem	Moguće rješenje
Pokrenuli ste Internet Explorer s 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 nastavlja poručivati korisniku da CA još uvijek nije od povjerenja.	Koristite DCM da postavite **CA status** na **omogućeno** da označite CA kao povjerljiv.
Internet Explorer zahtijeva 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 s http://www.netcenter.com.

Rješavanje problema HTTP poslužitelja za iSeries problems

Koristite sljedeću tablicu da nađete informacije za pomoć u rješavanju nekih uobičajenih problema HTTP poslužitelja na koje možete naići za vrijeme rada s 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** postavljen upotrebom sučelja Administracije HTTP poslužitelja. Također, konfiguracija mora imati virtualni host konfiguriran tako da koristi SSL port, sa **SSL-om** postavljenim na **Omogućeno** za virtualni host. Također moraju postojati dvije direktive **Slušanja** koje specificiraju dva različita porta, jedna za SSL i druga koja nije za SSL. Ove su postavljene na stranici **Opće postavke**. Osigurajte da je instanca poslužitelja kreirana i certifikat poslužitelja potpisan.

Problem	Moguće rješenje
Postupak registriranja instance HTTP poslužitelja kao zaštićene aplikacije treba pojašnjenje.	Na vašem poslužitelju otiđite u sučelje administracije HTTP poslužitelja da bi postavili konfiguraciju za vaš HTTP poslužitelj. Najprije morate definirati virtualni host da omogućite SSL. Nakon što definirate virtualni host, morate specificirati da virtualni host koristi SSL port definiran prethodno na direktivi **Slušanje** na stranici **Opće postavke**. Sljedeće, morate koristiti stranicu **SSL s Provjerom autentičnosti certifikata** pod **Sigurnost** da omogućite SSL u prethodno konfiguriranom virtualnom hostu. Sve promjene moraju biti primijenjene na konfiguracijsku datoteku. Primijenite da registriranje vaše instance ne bira automatski koje će certifikate instanca koristiti. Morate koristiti DCM da dodijelite specifični certifikat vašoj aplikaciji prije nego pokušate ugasiti i zatim ponovno pokrenuti instancu vašeg poslužitelja.
Imate teškoća u podešavanju HTTP poslužitelja za rad s validacijskim listama i opcionom provjerom klijenata.	Pogledajte dokumentaciju HTTP Poslužitelj za iSeries za opcije o postavljanju instance.
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.
Tražite od pretražitelja da predoči certifikat HTTP poslužitelju, tako da taj certifikat možete upotrijebiti kao ulaz u QsyAddVldlCertificate API.	Morate koristiti **SSLEnable** i **SSLClientAuth ON** da bi postigli da HTTP poslužitelj napuni HTTPS_CLIENT_CERTIFICATE varijablu okruženja. Te API-je možete naći u poglavlju i5/OS API-ji u Informacijskom Centru. Možda ćete također htjeti pogledati ove validacijske liste ili API-je koji se odnose na certifikat: • QsyListVldlCertificates i QSYLSTVC • QsyRemoveVldlCertificate i QRMVVC • QsyCheckVldlCertificate i QSYCHKVC • QsyParseCertificate i QSYPARSC, itd.
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.
HTTP Poslužitelj neće biti uspješno pokrenut sa **SSL-om** postavljenim na **Omogućeno** i s porukom greške HTP8351 koja se pojavljuje u dnevniku posla. Dnevnik pogrešaka za HTTP Poslužitelj pokazuje grešku da operacija SSL Inicijalizacija nije uspjela s povratnim kodom greške 107 kada ne uspije HTTP Poslužitelj.	Greška 107 znači da je certifikat istekao. Koristite DCM da dodijelite različit certifikat apliakciji; na primjer, QIBM_HTTP_SERVER_MY_SERVER. Ako je instanca poslužitelja čije pokretanje ne uspijeva *ADMIN poslužitelj, tada privremeno postavite **SSL** na **Onemogućeno** tako da možete koristiti DCM na *ADMIN poslužitelju. Zatim koristite DCM da dodijelite različiti certifikat QIBM_HTTP_SERVER_ADMIN aplikaciji i pokušajte postavljanje **SSL-a** ponovno na **Omogućeno**.

Rješavanje problema dodjele korisničkog certifikata

Kada koristite zadatak **Dodjela korisničkog certifikata**, Upravitelj digitalnih certifikata (DCM) prikazuje informacije certifikata da odobrite prije registriranja certifikata. Ako DCM nije u mogućnosti prikazati certifikat, problem može biti uzrokovan jednom od sljedećih 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 ponovno izvesti posao. Pretražitelj će vas zatražiti da izaberete certifikat.
2. Ovo se može također dogoditi ako konfigurirate vaš pretražitelj tako da ne prikazuje listu izbora i da pretražitelj sadrži samo jedan certifikat od Izdavača certifikata (CA) na popisu CA-ova kojima poslužitelj vjeruje. Provjerite postavke konfiguracije vašeg pretražitelja i promijenite ih ako je potrebno. Vaš pretražitelj će vas zatim tražiti da izaberete certifikat. Ako ne možete prezentirati certifikat od CA kojem je poslužitelj postavljen da vjeruje, ne možete dodijeliti certifikat. Kontaktirajte vašeg DCM administratora.
3. Certifikat koji želite registrirati je već registriran pri DCM-u.

4. Izdavač certifikata koji je izdao certifikat nije određen kao izdavač od povjerenja za sistem ili aplikaciju o kojoj se radi. 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 će možda trebati napraviti **Import** CA certifikata u *SYSTEM spremište certifikata. Ili, administrator će možda trebati koristiti zadatak **Postavi CA status** da omogući CA kao onaj od povjerenja da ispravi problem.
5. Nemate nikakav certifikat za registraciju. Provjerite ima li korisničkih certifikata u pregledniku da vidite je li to problem.
6. 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.
7. IBM HTTP poslužitelj nije ispravno postavljen za registraciju certifikata sa SSL-om i provjeru ovlaštenja klijenta na sigurnoj instanci poslužitelja administracije. 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 izaberete 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 ponovno 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 mala lista drugih resursa koju možete pregledati da naučite više o digitalnim certifikatima i kako ih možete koristiti za poboljšanje vaše politike sigurnosti:

- **VeriSign Help Desk Web stranica**
  VeriSign Web stranica omogućuje opsežnu knjižnicu s poglavljima o digitalnim certifikatima, kao i mnoštvo drugih tema o Internet sigurnosti.
- **IBM eServer iSeries Sigurnost ožičene mreže: OS/400 V5R1 DCM i kriptografička poboljšanja SG24-6168**

  Ovaj IBM Redbook se fokusira na V5R1 poboljšanja mrežne sigurnosti. Redbook pokriva mnoga poglavlja, uključujući način upotrebe sposobnosti potpisivanja objekata, Upravitelja digitalnih certifikata, podrške za 4758 kriptografički koprocesor za SSL i tako dalje.

- **AS/400 Internet sigurnost: Razvijanje infrastrukture digitalnog certifikata (SG24-5659)**
  Ovaj redbook opisuje što možete napraviti s digitalnim certifikatima na vašem poslužitelju. Objašnjava se kako postaviti različite poslužitelje i klijente za korištenje certifikata. Osim toga on sadrži informacije i uzorke koda za upotrebu i5/OS API-ja za upravljanje i upotrebu digitalnih certifikata u korisničkim aplikacijama.

- **RFC indeksno traženje**
  Ova Web stranica omogućuje pretražljivo spremište Zahtjeva za Komentarima (RFC-ova). RFC-ovi opisuju standarde za Internet protokole, kao SSL, PKIX i druge koji se odnose na korištenje digitalnih certifikata.

Dodatak. Napomene

Ove informacije su razvijene za proizvode i usluge koji se nude u SAD.

IBM možda ne nudi proizvode, usluge ili funkcije raspravljane u ovom dokumentu u drugim zemljama. Posavjetujte se sa svojim lokalnim IBM predstavnikom za informacije o proizvodima i uslugama koji su trenutno dostupni u vašem području. Bilo koje upućivanje na IBM proizvod, program ili uslugu nema namjeru tvrditi da se samo taj IBM proizvod, program ili usluga mogu koristiti. Bilo koji funkcionalno ekvivalentan proizvod, program ili usluga koji ne narušava nijedno IBM pravo na intelektualno vlasništvo, se može koristiti kao zamjena. Međutim, na korisniku je odgovornost da procijeni i verificira operacije bilo kojeg ne-IBM proizvoda, programa ili usluge.

IBM može imati patente ili aplikacijske patente koje su još u toku, a koji pokrivaju predmet o kojem se govori u ovom dokumentu. Posjedovanje ovog dokumenta vam ne daje nikakve licence na ove patente. Možete poslati upit za licence, u pismenom obliku, na:

| IBM Director of Licensing
| IBM Corporation
| 500 Columbus Avenue
| Thornwood, NY 10594-1785
| U.S.A.

Za zahtjeve za licencu koji se odnose na dvo-bajtne (DBCS) informacije, kontaktirajte IBM Odjel za intelektualno vlasništvo u vašoj zemlji ili pošaljite pismeni zahtjev na:

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

Sljedeći odlomak se ne primjenjuje na Ujedinjeno Kraljevstvo ili bilo koju drugu zemlju gdje su takve izjave nekonzistentne s lokalnim zakonima: INTERNATIONAL BUSINESS MACHINES CORPORATION DAJE OVU PUBLIKACIJU “KAKVA JE ”, BEZ IKAKVIH JAMSTAVA, BILO IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, UKLJUČENA JAMSTVA O NE-POVREĐIVANJU, PROĐI NA TRŽIŠTU ILI SPOSOBNOSTI ZA ODREĐENU SVRHU. Neke zemlje ne dozvoljavaju odricanje od izravnih ili posrednih jamstava u određenim transakcijama, zbog toga, se ova izjava možda ne odnosi na vas.

Ove informacije mogu sadržavati tehničke netočnosti ili tipografske pogreške. Povremeno se rade promjene na ovim informacijama; te promjene bit će uključene u nova izdanja ove publikacije. IBM može raditi poboljšanja i/ili promjene u proizvodu(ima) i/ili programu/ima opisanim u ovoj publikaciji, bilo kad, bez prethodne obavijesti.

Bilo koje upućivanje u ovim informacijama na ne-IBM Web stranice, služi samo kao pomoć i ni na kakav način ne služi za promicanje tih Web stranica. Materijali na tim Web stranicama nisu dio materijala za ovaj IBM proizvod i upotreba tih Web stranica je na vaš osobni rizik.

| IBM može koristiti ili distribuirati bilo koje informacije koje dobavite na bilo koji način koji smatra prikadnim, bez bilo
| kakvih obaveza prema vama.

Vlasnici licence za ovaj program, koji žele imati informacije o njemu u svrhu omogućavanja: (i) izmjene informacija između neovisno kreiranih programa i drugih programa (uključujući i ovaj) i (ii) uzajamne upotrebe informacija koje su bile izmijenjene, trebaju kontaktirati:

| IBM Corporation
| Software Interoperability Coordinator, Department 49XA
| 3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Takve informacije mogu biti dostupne, uz odgovarajuće termine i uvjete, uključujući u nekim slučajevima i plaćanje pristojbe.

Licencni program opisan u ovim informacijama i svi licencni materijali dostupni za to, su osigurani od strane IBM-a, pod uvjetima od IBM Customer Agreement, IBM International Program License Agreement, ili bilo kojeg ekvivalentnog ugovora između nas.

Svi podaci o izvedbi koji su ovdje sadržani su utvrđeni u kontroliranoj okolini. Prema tome, rezultati dobiveni u drugim operacijskim okruženjima se mogu značajno razlikovati. Neka mjerenja su možda bila izvedena na sistemima na razvojnoj razini i ne postoji nikakvo jamstvo da će ta mjerenja biti ista na općenito dostupnim sistemima. Osim toga, neka mjerenja su možda bila procijenjena pomoću ekstrapolacije. Stvarni rezultati se mogu razlikovati. Korisnici ovog dokumenta bi trebali provjeriti primjenljive podatke za njihovo određeno okruženje.

Sve izjave u vezi budućih IBM namjera ili smjernica su podložne promjeni ili povlačenju bez prethodne obavijesti, te predstavljaju samo ciljeve i namjere.

Ove informacije sadrže primjere podataka i izvještaja koji se koriste u svakodnevnim operacijama. Radi što boljeg objašnjenja, ti primjeri uključuju imena pojedinaca, poduzeća, brandova i proizvoda. Sva ta imena su izmišljena i bilo koja sličnost s imenima i adresama koja se koriste u stvarnom poslovnom okruženju, je u potpunosti slučajna.

Zaštitni znaci

Sljedeći termini su zaštitni znaci International Business Machines Corporation u Sjedinjenim Državama, drugim zemljama ili oboje:

AIX
Application System/400
AS/400
Domino
e (logo)
eServer
i5/OS
IBM
iSeries
Net.Data
Operating System/400
OS/400
400

Lotus, Freelance i WordPro zaštitni su znaci International Business Machines Corporation i Lotus Development Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

Microsoft, Windows, Windows NT i Windows logo su zaštitni znaci Microsoft Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

Ostala imena poduzeća, proizvoda i usluga mogu biti zaštitni znaci ili servisne oznake drugih.

Termini i uvjeti za spuštanje i ispis publikacija

Dozvole za upotrebu publikacija koje ste izabrali za spuštanje se dodjeljuju prema sljedećim terminima i uvjetima i nakon vašeg prihvaćanja.

Osobna upotreba: Možete reproducirati ove Publikacije za vašu osobnu, nekomercijalnu upotrebu, uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete distribuirati, prikazivati ili raditi derivacije ovih publikacija ili njihovih dijelova, bez izričitog pristanka IBM-a.

Komercijalna upotreba: Možete reproducirati, distribuirati i prikazivati ove Publikacije samo unutar vašeg poduzeće uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete raditi derivacije ovih publikacija ili reproducirati, distribuirati ili prikazivati ove publikacije ili bilo koji njihov dio, izvan vašeg poduzeća, bez izričitog pristanka IBM-a.

Osim kako je izričito dodijeljeno u ovoj dozvoli, nisu dane nikakve dozvole, licence ili prava, niti izričita niti uključena, na Publikacije ili bilo koje informacije, podatke, softver ili bilo koju drugu intelektualnu svojinu koja je sadržana.

IBM rezervira pravo da bilo kad, po vlastitom nahođenju, povuče ovdje dodijeljenu dozvolu, ako je ona štetna za njegove interese ili je ustanovljeno od strane IBM-a, da gornje upute nisu bile ispravno slijeđene.

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune usklađenosti sa svim primjenjivim zakonima i propisima, uključujući sve zakone i propise o izvozu Sjedinjenih Država. IBM NE DAJE NIKAKVA JAMSTVA NA SADRŽAJ OVIH PUBLIKACIJA. PUBLIKACIJE SE DAJU ″KAKVE JESU″ I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, IZRAVNA JAMSTVA ZA PROĐU NA TRŽIŠTU I PRIKLADNOST ZA ODREĐENU SVRHU.

Spuštanjem i ispisom publikacija s ove stranice, naznačili ste da se slažete s ovim terminima i uvjetima.

Tiskano u Hrvatskoj