IBM Sistemi - iSeries

# Sigurnost
# Upravitelj digitalnih certifikata

*Verzija 5 Izdanje 4*

IBM Sistemi - iSeries

# Sigurnost
# Upravitelj digitalnih certifikata

*Verzija 5 Izdanje 4*

**Napomena**

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene”, na stranici 79.

**Deveto izdanje (veljača, 2006)**

Ovo izdanje se primjenjuje na verziju 5, izdanje 4, modifikaciju 0 od IBM i5/OS (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


## Upravitelj digitalnih certifikata . . . . . 1

Što je novo kod V5R4 . . . . . 1
Ispisivi PDF-ovi . . . . . 2
DCM koncepti . . . . . 2
Proširenja certifikata . . . . . 3
Obnavljanje certifikata . . . . . 3
Razlikovno ime . . . . . 3
Digitalni potpisi . . . . . 4
Javni-privatni par ključeva . . . . . 5
Izdavač certifikata (CA) . . . . . 5
Lokacije Liste opoziva certifikata (CRL) . . . . . 6
Spremišta certifikata . . . . . 7
Kriptografija . . . . . 8
IBM kriptografički koprocesor za iSeries . . . . . 9
Sloj sigurnih utičnica (SSL) . . . . . 9
Definicije aplikacija . . . . . 9
Provjera valjanosti . . . . . 10
DCM scenariji . . . . . 11
Scenarij: Upotreba certifikata za eksternu provjeru autentičnosti . . . . . 11
Scenarij: Upotreba certifikata za internu provjeru autentičnosti . . . . . 17
Plan za DCM . . . . . 25
Zahtjevi za postavljanje DCM-a . . . . . 25
Razmatranja sigurnosnog kopiranja i obnavljanja za DCM podatke . . . . . 26
Tipovi digitalnih certifikata . . . . . 26
Javni certifikati naspram privatnih certifikata . . . . 28
Digitalni certifikati za SSL zaštićene komunikacije . . 30
Digitalni certifikati za provjeru korisnika . . . . . 30
Digitalni certifikati i Mapiranje identiteta u poduzeću (EIM) . . . . . 32
Digitalni certifikati za VPN veze . . . . . 33
Digitalni certifikati za potpisivanje objekata . . . . 34
Digitalni certifikati za provjeru potpisa objekata . . . 35
Konfiguriranje DCM-a . . . . . 35
Pokretanje Upravitelja digitalnih certifikata . . . . 36
Postavljanje certifikata prvi put . . . . . 36
Obnavljanje postojećeg certifikata . . . . . 50
Importiranje certifikata . . . . . 51
Upravljanje DCM-om . . . . . 52
Upotreba Lokalnog CA za izdavanje certifikata drugim iSeries sistemima . . . . . 52
Upravljanje aplikacijama u DCM-u . . . . . 60
Upravljanje certifikatima pomoću isteka . . . . . 62
Provjera valjanosti certifikata i aplikacija . . . . . 63
Dodjela certifikata aplikacijama . . . . . 64
Upravljanje CRL lokacijama . . . . . 64
Ključevi spremišta certifikata na IBM kriptografičkom koprocesoru . . . . . 65
Upravljanje lokacijom zahtjeva za PKIX CA . . . . 67
Upravljanje LDAP lokacijom za certifikate korisnika 67
Potpisivanje objekata . . . . . 68
Provjera valjanosti potpisa objekata . . . . . 70
Rješavanje problema DCM-a . . . . . 71
Rješavanje problema lozinki i općenitih problema . . 71
Rješavanje problema spremišta certifikata i baze podataka ključeva . . . . . 73
Rješavanje problema pretražitelja . . . . . 75
Rješavanje problema s HTTP poslužiteljem za iSeries 76
Rješavanje problema dodjele korisničkog certifikata. . 77
Povezane informacije za DCM . . . . . 78

## Dodatak. Napomene . . . . . 79

Zaštitni znaci . . . . . 80
Termini i uvjeti . . . . . 81

# 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 iSeries usluge i aplikacije, kao što je FTP, Telnet, HTTP poslužitelj osiguravaju SSL podršku za privatnost podataka.

iSeries osigurava opsežnu podršku digitalnih certifikata koja vam omogućuje korištenje digitalnih certifikata kao vjerodajnica u mnogim 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.

Kapitaliziranje u iSeries podršci za certifikate je lako kada koristite Upravitelja digitalnih certifikata (DCM), besplatnu značajku 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 kod V5R4

Ove informacije opisuju što je novo ili značajno promijenjeno u ovom izdanju.

### Nove informacije za Obnavljanje certifikata

Ove nove informacije objašnjavaju obradu korak po korak za obnavljanje postojećih certifikata s Lokalnim CA ili s Internet CA.

- “Obnavljanje postojećeg certifikata” na stranici 50

### Nove informacije za Importiranje certifikata

Ove nove informacije objašnjavaju obradu korak po korak za importiranje certifikata koji su smješteni u datotekama na poslužitelju ili datotekama s drugog poslužitelja.

- “Importiranje certifikata” na stranici 51

### Informacije o poboljšanjima za Listu opoziva certifikata (CRL) i Lightweight Directory Access Protocol (LDAP)

Ove informacije su ažurirane s informacijama o tome kako se anonimno vezati s LDAP poslužiteljem za CRL obradu.

- “Upravljanje CRL lokacijama” na stranici 64
- “Upravljanje LDAP lokacijom za certifikate korisnika” na stranici 67
- “Lokacije Liste opoziva certifikata (CRL)” na stranici 6

### Kako vidjeti 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.

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

---

## Ispisivi PDF-ovi

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

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 spustiti kopiju s Adobe Web stranice (www.adobe.com/products/acrobat/readstep.html) .

---

## DCM koncepti

Pogledajte ove informacije da bi bolje razumjeli što su digitalni certifikati i kako rade. Naučite o različitim tipovima certifikata i kako ih možete koristiti kao dio vaše politike sigurnosti.

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

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 da bi proširili razlikovno ime 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 identificiranje krajnje točke veze iSeries Virtualne privatne mreže (VPN), morate osigurati informacije za njihova proširenja.

**Srodni koncepti**

"Razlikovno ime"
Koristite ove informacije da naučite o karakteristikama identifikacije digitalnih certifikata.

## 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 certifikat.

## Razlikovno ime

Koristite ove informacije da naučite o karakteristikama identifikacije digitalnih certifikata.

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 privatnih certifikata, možete koristiti proširenja certifikata da biste osigurali dodatne DN informacije za certifikat, uključujući:

- Verzija 4 IP adresa
- Potpuno kvalificirano ime domene
- Adresa e-pošte

**Srodni koncepti**

"Proširenja certifikata" na stranici 3
Proširenja certifikata su polja za informacije koja daju dodatne informacije o certifikatu.

## Digitalni potpisi

Digitalni potpis u elektroničkom dokumentu ili drugom objektu je kreiran pomoću obrasca kriptografije 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 pristupate objektu koji sadrži digitalni potpis, možete provjeriti potpis na objektu da bi provjerili valjanost izvora objekta (na primjer, da aplikacija koju spuštate dolazi od ovlaštenog izvora kao što je 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 kreirao je i5/OS aplikaciju koju želi distribuirati preko Interneta kao prikladno i jeftino sredstvo za svoje kupce. 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 što su 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.

**Srodni koncepti**

"Izdavač certifikata (CA)"
Izdavač certifikata (CA) je pouzdani centralni administrativan entitet koji može izdati digitalne certifikate korisnicima i poslužiteljima.

"Kriptografija" na stranici 8
Koristite ove informacije da biste naučili što je kriptografija i kako digitalni certifikati koriste kriptografičke funkcije za osiguravanje sigurnosti.

"Javni-privatni par ključeva"
Svaki digitalni certifikat ima par pridruženih kriptografičkih ključeva koji se sastoje od privatnog i javnog ključa.

## Javni-privatni par ključeva

Svaki digitalni certifikat ima par pridruženih kriptografičkih ključeva koji se sastoje od privatnog i javnog ključa.

**Bilješka:** Certifikati provjere potpisa su iznimka ovog pravila 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 koju daju 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. Primatelj potpisanog objekta može tada koristiti javni ključ sadržan u certifikatu potpisnika za dešifriranje potpisa. Takvi digitalni potpisi osiguravaju pouzdanost porijekla objekta i osiguravaju sredstva provjere integriteta objekta.

**Srodni koncepti**

"Digitalni potpisi" na stranici 4
Digitalni potpis u elektroničkom dokumentu ili drugom objektu je kreiran pomoću obrasca kriptografije i ekvivalentan je osobnom potpisu na pisanom dokumentu.

"Izdavač certifikata (CA)"
Izdavač certifikata (CA) je pouzdani centralni administrativan entitet koji može izdati digitalne certifikate korisnicima i poslužiteljima.

## 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 svoj privatni ključ za kreiranje digitalnog potpisa na certifikatima koje izdaje radi provjere 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. Kada lokalni CA izda certifikat korisniku, DCM automatski pridružuje certifikat s korisničkim iSeries sistemskim korisničkim profilom drugog korisnika ili drugog korisničkog identiteta. 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.

**Srodni koncepti**

“Digitalni potpisi” na stranici 4
Digitalni potpis u elektroničkom dokumentu ili drugom objektu je kreiran pomoću obrasca kriptografije i ekvivalentan je osobnom potpisu na pisanom dokumentu.

“Javni-privatni par ključeva” na stranici 5
Svaki digitalni certifikat ima par pridruženih kriptografičkih ključeva koji se sastoje od privatnog i javnog ključa.

## Lokacije Liste opoziva certifikata (CRL)

Lista opoziva certifikata (CRL) je datoteka koja popisuje sve nevažeće i opozvane certifikate za određenog Izdavača certifikata (CA).

CA-i povremeno ažuriraju svoje CRL-ve i čine ih dostupnim da bi drugi izdavali u direktorijima Lightweight Directory Access Protocol (LDAP). 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) dozvoljava definiranje i upravljanje lokacijskim informacijama CRL-a da bi se osigurala stroža provjera autentičnosti certifikata koje koristite lili prihvaćate od drugih. Definicija CRL lokacije opisuje lokaciju od i informacije o pristupu za poslužitelja Lightweight Directory Access Protocol-a (LDAP), koji pohranjuje CRL.

| Prilikom povezivanja s LDAP poslužiteljem morate dobaviti DN i lozinku da biste izbjegli anonimno vezivanje s
| LDAP poslužiteljem. Anonimno vezivanje s poslužiteljem ne osigurava potrebnu razinu ovlaštenja za pristup
| ″kritičnom″ atributu kao što je CRL. U tom slučaju DCM može provjeriti valjanost certifikata s opozvanim statusom jer
| DCM ne može dobiti ispravan status od CRL-a. Ako želite anonimno pristupiti LDAP poslužitelju, morate koristiti Alat
| za Web administraciju poslužitelja direktorija i izabrati zadatak ″Upravljanje shemom″ da biste promijenili sigurnosnu
| klasu (koja se također naziva ″klasa pristupa″) atributa **certificateRevocationList** i **authorityRevocationList** iz
| ″critical″ u ″normal″.

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 .

**Srodni koncepti**

"Provjera valjanosti certifikata i aplikacija" na stranici 63
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.

**Srodni zadaci**

"Upravljanje CRL lokacijama" na stranici 64
Upravitelj digitalnih certifikata (DCM) dozvoljava vam definiranje i upravljanje informacijama Popisom opoziva certifikata (CRL) za određeno Ovlaštenje certifikata (CA) kao dio obrade provjere valjanosti certifikata.

## Spremišta certifikata

Spremište certifikata je posebna datoteka baze podataka ključa koju Upravitelj digitalnih certifikata (DCM) koristi za pohranjivanje digitalnih certifikata.

Spremište certifikata sadrži privatni ključ certifikata osim ako niste izabrali da umjesto njega ključ pohranjuje IBM kriptografički koprocesor. 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 daje sljedeća preddefinirana 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 certifikate za provjeru porijekla certifikata, koje moraju provjeriti kao dio SSL pregovora za dodjelu autorizacije resursima.

***SYSTEM**
DCM osigurava ovo spremište certifikata za upravljanje poslužiteljevim ili klijentovim certifikatima koje koriste aplikacije za sudjelovanje u komunikacijskim sesijama Sloja sigurnih utičnica (SSL). IBM iSeries 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 osigurava 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 daje 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.

**Druga sistemska spremišta certifikata**

Ovo spremište certifikata daje 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 sistemu, možete izabrati druge opcije za spremište privatnog ključa vaših certifikata (s izuzetkom certifikata potpisivanja objekta). 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.

**Srodni koncepti**

“Tipovi digitalnih certifikata” na stranici 26
Koristite ove informacije da biste naučili o različitim tipovima digitalnih certifikata i kako se koriste u Upravitelju digitalnih certifikata (DCM).

# Kriptografija

Koristite ove informacije da biste naučili što je kriptografija i kako digitalni certifikati koriste kriptografičke funkcije za osiguravanje sigurnosti.

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, poslužitelj ili korisnik može koristiti privatni ključ za ″prijavu″ objekta, a primatelj može koristiti odgovarajući javni ključ za dešifriranje digitalnog potpisa u svrhu provjere izvora i integriteta objekta.

**Srodni koncepti**

“Digitalni potpisi” na stranici 4
Digitalni potpis u elektroničkom dokumentu ili drugom objektu je kreiran pomoću obrasca kriptografije i ekvivalentan je osobnom potpisu na pisanom dokumentu.

“Sloj sigurnih utičnica (SSL)” na stranici 9
Sloj sigurnih utičnica (SSL), koji je izvorno proizveo Netscape, je industrijski standard za šifriranje sesija između klijenata i poslužitelja.

## IBM kriptografički koprocesor za iSeries

Kriptografički koprocesor omogućuje dokazane kriptografičke usluge, osiguravajući privatnost i integritet, za razvijanje sigurnih e-business aplikacija.

Korištenje IBM kriptografičkog koprocesora za iSeries dodaje sistemu mogućnost kriptografičkog obrađivanja s visokom razinom sigurnosti. 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 za pohranjivanje privatnog ključa certifikata poslužitelja ili klijenta i za certifikat lokalnog 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.

**Srodni koncepti**

“Ključevi spremišta certifikata na IBM kriptografičkom koprocesoru” na stranici 65
Pregledajte ove informacije da biste naučili kako koristiti instalirani koprocesor da biste osigurali sigurno spremište privatnih ključeva certifikata.

## 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 asimetričan ili javni ključ kriptografije za šifriranje sesija između klijenta i poslužitelja. 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.

**Srodni koncepti**

“Kriptografija” na stranici 8
Koristite ove informacije da biste naučili što je kriptografija i kako digitalni certifikati koriste kriptografičke funkcije za osiguravanje sigurnosti.

“Tipovi digitalnih certifikata” na stranici 26
Koristite ove informacije da biste naučili o različitim tipovima digitalnih certifikata i kako se koriste u Upravitelju digitalnih certifikata (DCM).

## Definicije aplikacija

Koristite ove informacije da biste naučili što su DCM aplikacijske definicije i kako s njima raditi za SSL konfiguraciju i potpisivanje objekta.

Postoje dva tipa aplikacijskih definicija s 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 iSeries 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.

**Srodni koncepti**

“Upravljanje aplikacijama u DCM-u” na stranici 60
Ova poglavlja sadrže 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.

**Srodni zadaci**

“Kreiranje definicije aplikacije” na stranici 60
Pregledajte ovo poglavlje da biste naučili o različitim tipovima aplikacija koje možete definirati za rad.

# Provjera valjanosti

Upravitelj digitalnih certifikata (DCM) osigurava zadatke koji dozvoljavaju provjeru valjanosti certifikata ili za provjeru valjanosti aplikacije radi provjere različitih svojstava koje moraju 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.

Ako konfigurirate mapiranje Lightweight Directory Access Protocol (LDAP) za korištenje CRL-a, DCM provjerava CRL prilikom provjere valjanosti certifikata radi osiguranja da certifikat nije ispisan u CRL-u. Međutim, da bi obrada provjere valjanosti precizno provjerila CRL, poslužitelj direktorija (LDAP poslužitelj) konfiguriran za LDAP mapiranje mora sadržavati prikladan CRL. Inače se certifikatu neće uspješno provjeriti valjanost. Morate osigurati vezanje DN-a i lozinke da biste izbjegli provjeru valjanosti certifikata s opozvanim statusom. Također, ako ne specificirate DN i lozinku prilikom konfiguriranja LDAP mapiranja, bit ćete anonimno vezani s LDAP poslužiteljem. Anonimno vezanje s LDAP poslužiteljem ne osigurava razinu ovlaštenja potrebnu za pristup atributima ″critical″, a CRL je atribut ″critical″. U tom slučaju DCM može provjeriti valjanost certifikata s opozvanim statusom jer DCM ne može dobiti ispravan status od CRL-a. Ako želite anonimno pristupiti LDAP poslužitelju, morate koristiti Alat za Web administraciju poslužitelja direktorija i izabrati zadatak ″Upravljanje shemom″ da biste promijenili sigurnosnu klasu (koja se također naziva ″klasa pristupa″) atributa **certificateRevocationList** i **authorityRevocationList** iz ″critical″ u ″normal″.

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.

**Srodni koncepti**

"Provjera valjanosti certifikata i aplikacija" na stranici 63
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.

## DCM scenariji

Koristite ove informacije za pregled dva scenarija koji ilustriraju tipične sheme implementacije certifikata koje će vam pomoći u planiranju vlastite implementacije certifikata kao dijela iSeries sigurnosne politike. Svaki scenarij također daje sve potrebne zadatke konfiguracije koje morate izvesti da upotrijebite scenarij kako je opisano.

Upravitelj digitalnih certifikata i podrška iSeries sistemskog digitalnog certifikata dozvoljava korištenje certifikata radi poboljšanja sigurnosne politike na velik broj 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 dozvoljavaju korištenje Sloja sigurnih utičnica (SSL) za siguran 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 ovisno o tome kako konfigurirate DCM, možete koristiti DCM da biste pridružili korisnički certifikat s njegovim ili njenim iSeries korisničkim profilom ili identifikatorom 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 potrebne sistemske i softverske preduvjete i sve konfiguracijske zadatke koje morate izvesti da biste iznijeli scenarij.

**Srodne informacije**

Scenariji potpisivanja objekata

## Scenarij: Upotreba certifikata za eksternu provjeru autentičnosti

U ovom scenariju ćete naučiti kada i kako koristiti certifikate kao mehanizam provjere autentičnosti da biste zaštitili i ograničili pristup javnim korisnicima na javne ili extranet resurse i aplikacije.

## 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 su informacije koje ova aplikacija daje donekle osjetljive, želite osigurati da ju koriste samo registrirani agenti. Nadalje, želite s vremenom osigurati 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.

## Ciljevi

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.

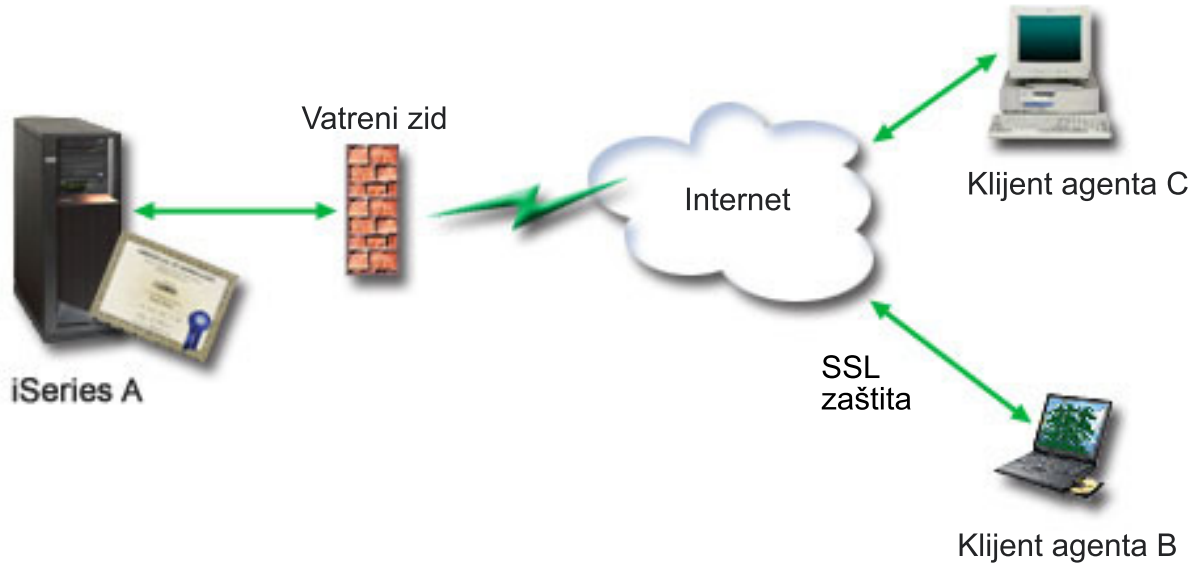
Ciljevi ovog scenarija su sljedeći:

- 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 unijeti valjano korisničko ime i lozinku za pristup aplikaciji u SSL načinu. S vremenom, ovlašteni korisnici moraju moći 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 – iSeries A**

- iSeries A je poslužitelj koji uslužuje aplikaciju za izračun tečajeva.
- iSeries A izvodi i5/OS verzija 5 izdanje 4 (V5R4).
- iSeries A ima Upravitelja digitalnih certifikata (i5/OS opcija 34) i IBM HTTP poslužitelj za i5/OS (5722–DG1) instalirane i konfigurirane.
- iSeries A izvodi aplikaciju za izračun tečajeva, koja je konfigurirana tako da:
  - 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.
- iSeries A predstavlja certifikat za pokretanje SSL sesije kada klijenti B i C pristupe aplikaciji za izračun tečajeva.
- Nakon inicijaliziranja SSL sesije, iSeries A zahtijeva da klijenti B i C osiguraju važeće korisničko ime i lozinku prije dozvole pristupa aplikaciji za izračun tečajeva.

**Sistemi klijenta agenta – Klijent B i klijent C**

- Klijenti B i C su nezavisni agenti koji pristupaju aplikaciji za izračunavanje tečajeva.
- 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 iSeries A, koja predstavlja certifikat za njihov klijentski softver radi provjere autentičnosti identiteta i pokretanje SSL sesije.
- Klijentski softver na klijentima B i C je konfiguriran tako da prihvaća certifikat od iSeries A u svrhu pokretanja SSL sesije.
- Kada započne SSL sesija, klijenti B i C moraju osigurati važeće korisničko ime i lozinku prije nego iSeries A dozvoli pristup aplikaciji.

## Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:

- Aplikacija za izračun tečajeva na iSeries A je generička aplikacija koja se može konfigurirati za korištenje SSL-a. Većina aplikacija, zajedno s mnogim iSeries aplikacijama, osiguravaju SSL podršku. SSL koraci konfiguracije razlikuju se prilično među aplikacijama. Zbog toga, ovaj scenarij ne sadrži specifične upute za konfiguriranje aplikacije za izračun tečajeva za upotrebu SSL-a. Ovaj scenarij sadrži upute za konfiguriranje i upravljanje certifikatima koji su potrebni da bi bilo koja aplikacija koristila SSL.
- Aplikacija za izračun tečajeva može osigurati sposobnost zahtijevanja certifikata za provjeru autentičnosti klijenta. Ovaj scenarij sadrži upute za upotrebu Upravitelja 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 sadrži specifične upute za konfiguriranje provjere autentičnosti certifikata klijenata za aplikaciju izračuna tečajeva.
- iSeries A ispunjava zahtjeve za instaliranje i korištenje Upravitelja digitalnih certifikata (DCM)
- Nitko prije toga nije konfigurirao ili koristio DCM na iSeries A.
- Svatko tko koristi DCM za izvođenje zadataka u ovom scenariju mora imati *SECADM i *ALLOBJ posebna ovlaštenja za svoj korisnički profil.
- iSeries A nema instaliran IBM kriptografički koprocesor.

## Konfiguracijski zadaci

**Srodni zadaci**

"Pokretanje Upravitelja digitalnih certifikata" na stranici 36
Koristite ove informacije da biste naučili kako pristupiti značajki Upravitelja digitalnih certifikata (DCM) na sistemu.

## Dovršetak radne tablice za planiranje

Sljedeće radne tablice za planiranje pokazuju informacije koje trebate skupiti i odluke koje trebate napraviti da pripremite implementaciju digitalnog certifikata koju ovaj scenarij opisuje. Da osigurate uspješnu implementaciju, trebate moći odgovoriti s Da na sve stavke preduvjeta i trebate skupiti 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 |
|---|---|
| Je li vaš i5/OS V5R42 (5722-SS1)? | Da |
| Je li opcija 34 i5/OS instalirana na sistemu? | Da |
| Je li IBM HTTP poslužitelj za i5/OS (5722–DG1) instaliran na sistemu i pokrenuta je instanca Administrativnog poslužitelja? | Da |
| Da li je TCP konfiguriran za vaš sistem tako da možete koristiti Web pretražitelj i instancu Administrativni poslužitelj HTTP Poslužitelja za pristup DCM-u? | Da |
| 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 2. Planiranje radne tablice za konfiguraciju implementacije certifikata*

| Planiranje radne tablice za iSeries 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 |
| Uslužuje li iSeries A aplikacije koje želite omogućiti za SSL? | Da |

*Tablica 2. Planiranje radne tablice za konfiguraciju implementacije certifikata (nastavak)*

| Planiranje radne tablice za iSeries A | Odgovori |
|---|---|
| Koje razlikovno ime ćete koristiti za zahtjev za potpisivanjem certifikata (CSR) za čije kreiranje koristite DCM?<br>• **Veličina ključa**: određuje snagu kriptografičkih ključeva za certifikat.<br>• **Oznaka certifikata**: identificira certifikat s jedinstvenim nizom znakova.<br>• **Uobičajeno ime**: identificira vlasnika certifikata, kao što je osoba, entitet ili aplikacija; dio DN Subjekta za certifikat.<br>• **Jedinica organizacije**: identificira organizacijsku sekciju ili područje za aplikaciju koja će koristiti certifikat.<br>• **Ime organizacije**: identificira vaše poduzeće ili odjelni dio za aplikaciju koja će koristiti certifikat.<br>• **Lokacija ili grad**: identificira vaš grad ili označavanje lokacija za vašu organizaciju.<br>• **Država ili pokrajina**: identificira državu ili pokrajinu u kojoj ćete koristiti ovaj certifikat.<br>• **Zemlja ili regija**: identificira, s dvoslovnom oznakom, zemlju ili regiju u kojoj ćete koristiti ovaj certifikat. | **Veličina ključa**: 1024**Naziv certifikata**: Myco_public_cert**Uobičajeno ime**: myco_rate_server@myco.com**Organizacijska jedinica**: Rate dept**Ime organizacije**: myco**Lokacija ili grad**: Any_city**Država**: Any**Zemlja**: 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 |

## Kreiranje zahtjeva za certikatom klijenta ili poslužitelja

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 koje vaše aplikacije mogu 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.
6. Dovršite obrazac i kliknite **Nastavak** da prikažete stranicu za potvrdu. 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.

   **Bilješka:** Kad napustite ovu stranicu, podaci se gube i ne možete ih obnoviti.
8. Kad napustite ovu stranicu, podaci se gube i ne možete ih obnoviti.
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.

## Konfiguriranje aplikacije za korištenje 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 aplikacijski ID i registriraju ID s Upraviteljem digitalnih certifikata (DCM) kada konfigurirate aplikaciju za korištenje SSL-a. 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 upute koje sadrži vaša dokumentacija za aplikaciju. Također, možete naučiti više o konfiguriranju mnogih uobičajenih IBM aplikacija korištenje SSL-a pregledavanjem Sloja sigurnih utičnica (SSL) u iSeries Informacijski Centar.

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

## Importiranje i dodjela potpisanih javnih certifikata

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.

## Pokretanje aplikacija u SSL načinu

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.

### (Opcijski): Definiranje CA pouzdane liste za aplikaciju koja je zahtijeva

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. Ovo osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA 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

U ovom scenariju ćete naučiti kako koristiti certifikate kao mehanizam provjere autentičnosti da biste zaštitili i ograničili resurse i aplikacije kojima interni korisnici mogu pristupiti na internim poslužiteljima.

## 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. Odgovorni ste za administriranje ove interne Web stranice, koja se izvodi na IBM HTTP poslužitelj za i5/OS (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 se odlučujete postaviti privatnog Lokalnog izdavača certifikata (CA) i izdajete certifikate svim zaposlenicima koje pridružujete certifikatima s njihovim iSeries 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.
  - Korisnici već imaju iSeries korisničke profile za kontroliranje pristupa aplikacijama i podacima.
  - Želite raditi s vlastitim izdavačem certifikata (CA).
- Korištenje privatnih certifikata za provjeru autentičnosti klijenta dozvoljava jednostavnije pridruživanje certifikata s ovlaštenim iSeries korisničkim profilom. Ovo pridruživanje certifikata s profilom 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.

## Ciljevi

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.

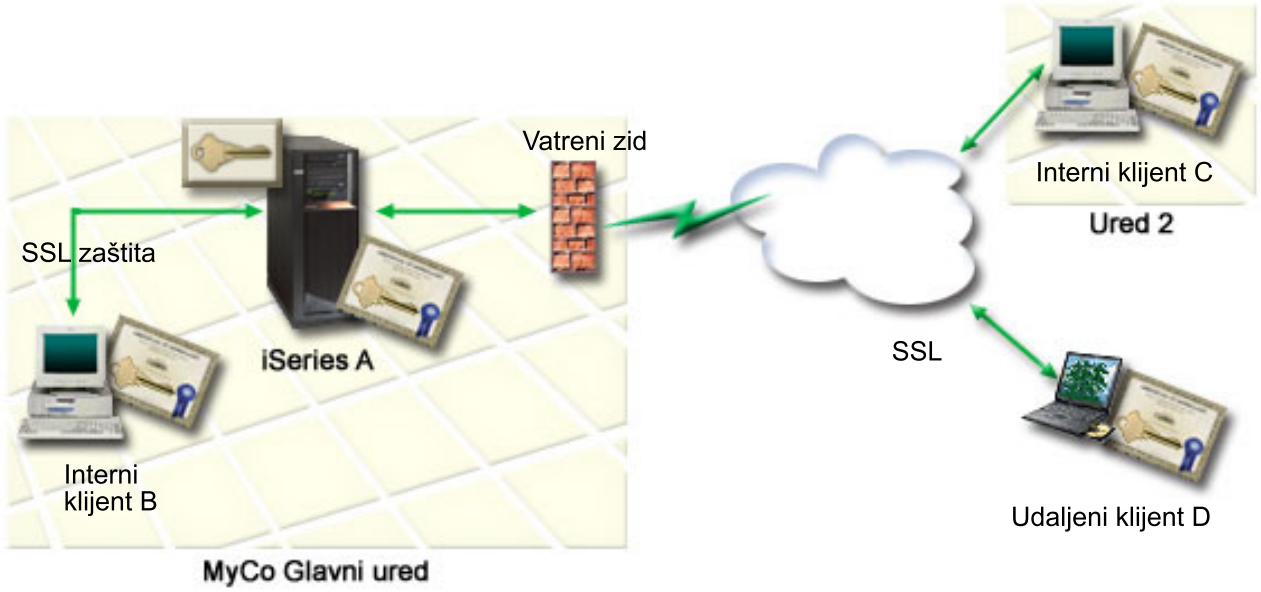
Ciljevi ovog scenarija su sljedeći:

- 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:

**Javni poslužitelj poduzeća – iSeries A**

- iSeries A je poslužitelj koji uslužuje aplikaciju za izračun tečajeva.
- iSeries A izvodi i5/OS verzija 5 izdanje 4 (V5R4).
- iSeries A ima Upravitelja digitalnih certifikata (i5/OS opcija 34) i IBM HTTP poslužitelj za i5/OS (5722–DG1) instalirane i konfigurirane.
- iSeries A izvodi aplikaciju za izračun tečajeva, koja je konfigurirana tako da:
  - 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.
- iSeries A predstavlja certifikat za pokretanje SSL sesije kada klijenti B i C pristupe aplikaciji za izračun tečajeva.
- Nakon inicijaliziranja SSL sesije, iSeries A zahtijeva da klijenti B i C osiguraju važeće korisničko ime i lozinku prije dozvole pristupa aplikaciji za izračun tečajeva.

**Sistemi klijenta agenta – Klijent B i klijent C**

- Klijenti B i C su nezavisni agenti koji pristupaju aplikaciji za izračunavanje tečajeva.
- 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 iSeries A, koja predstavlja certifikat za njihov klijentski softver radi provjere autentičnosti identiteta i pokretanje SSL sesije.
- Klijentski softver na klijentima B i C je konfiguriran tako da prihvaća certifikat od iSeries A u svrhu pokretanja SSL sesije.

- Kada započne SSL sesija, klijenti B i C moraju osigurati važeće korisničko ime i lozinku prije nego iSeries A dozvoli pristup aplikaciji.

## Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:

- IBM HTTP poslužitelj za i5/OS (upravljano s Apache) izvodi aplikaciju ljudskih resursa na iSeries A. Ovaj scenarij ne osigurava određene upute za konfiguriranje HTTP poslužitelja tako da koristi SSL. Ovaj scenarij sadrži upute za konfiguriranje i upravljanje certifikatima koji su potrebni da bi bilo koja aplikacija koristila SSL.
- HTTP poslužitelj može pružiti mogućnost zahtijevanja certifikata za provjeru autentičnosti klijenta. Ovaj scenarij sadrži upute za upotrebu Upravitelja digitalnih certifikata (DCM) za konfiguriranje zahtjeva za upravljanje certifikatom za ovaj scenarij. Međutim, ovaj scenarij ne daje određene konfiguracijske korake za konfiguriranje provjere autentičnosti certifikata klijenta za HTTP poslužitelj.
- HTTP poslužitelj ljudskih resursa na iSeries A već koristi provjeru autentičnosti lozinke.
- iSeries A ispunjava uvjete za instaliranje i korištenje Upravitelja digitalnih certifikata (DCM).
- Nitko prije toga nije konfigurirao ili koristio DCM na iSeries A.
- Svatko tko koristi DCM za izvođenje zadataka u ovom scenariju mora imati *SECADM i *ALLOBJ posebna ovlaštenja za svoj korisnički profil.
- iSeries A nema instaliran IBM kriptografički koprocesor.

## Konfiguracijski zadaci

## Dovršetak radne tablice za planiranje

Sljedeće radne tablice za planiranje pokazuju informacije koje trebate skupiti i odluke koje trebate napraviti da pripremite implementaciju digitalnog certifikata koju ovaj scenarij opisuje. Da osigurate uspješnu implementaciju, trebate moći odgovoriti s Da na sve stavke preduvjeta i trebate skupiti 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** |
|---|---|
| Je li vaš i5/OS V5R4 (5722-SS1)? | Da |
| Je li opcija 34 i5/OS instalirana na sistemu? | Da |
| Je li IBM HTTP poslužitelj za i5/OS (5722–DG1) instaliran na sistemu i pokrenuta je instanca Administrativnog poslužitelja? | Da |
| Da li je TCP konfiguriran za vaš sistem tako da možete koristiti Web pretražitelj i instancu Administrativni poslužitelj HTTP Poslužitelja za pristup DCM-u? | Da |
| 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 iSeries 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 |
| Uslužuje li iSeries A aplikacije koje želite omogućiti za SSL? | Da |

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

| **Radna tablica planiranja za iSeries A** | **Odgovori** |
|---|---|
| Koje razlikovno ime ćete koristiti za Lokalni CA?<br>• **Veličina ključa**: određuje snagu kriptografičkih ključeva za certifikat.<br>• **Ime Izdavača certifikata (CA)**: identificira CA i postaje uobičajeno ime za CA certifikat i DN Izdavatelja za certifikate koje CA izdaje.<br>• **Jedinica organizacije**: identificira organizacijsku sekciju ili područje za aplikaciju koja će koristiti certifikat.<br>• **Ime organizacije**: identificira vaše poduzeće ili odjelni dio za aplikaciju koja će koristiti certifikat.<br>• **Lokacija ili grad**: identificira vaš grad ili označavanje lokacija za vašu organizaciju.<br>• **Država ili pokrajina**: identificira državu ili pokrajinu u kojoj ćete koristiti ovaj certifikat.<br>• **Zemlja ili regija**: identificira, s dvoslovnom oznakom, zemlju ili regiju u kojoj ćete koristiti ovaj certifikat.<br>• **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**Organizacijska jedinica**: Rate dept**Ime organizacije**: myco**Lokacija ili grad**: Any_city**Država**: Any**Zemlja**: 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? | Da |
| Koje informacije za razlikovno ime ćete koristiti za certifikat poslužitelja koji izdaje Lokalni CA?<br>• **Veličina ključa**: određuje snagu kriptografičkih ključeva za certifikat.<br>• **Oznaka certifikata**: identificira certifikat s jedinstvenim nizom znakova.<br>• **Uobičajeno ime**: identificira vlasnika certifikata, kao što je osoba, entitet ili aplikacija; dio DN Subjekta za certifikat.<br>• **Jedinica organizacije**: identificira organizacijsku sekciju ili područje za aplikaciju koja će koristiti certifikat.<br>• **Ime organizacije**: identificira vaše poduzeće ili odjelni dio za aplikaciju koja će koristiti certifikat.<br>• **Lokacija ili grad**: identificira vaš grad ili označavanje lokacija za vašu organizaciju.<br>• **Država ili pokrajina**: identificira državu ili pokrajinu u kojoj ćete koristiti ovaj certifikat.<br>• **Zemlja ili regija**: identificira, s dvoslovnom oznakom, zemlju ili regiju u kojoj ćete koristiti ovaj certifikat. | **Veličina ključa**: 1024**Naziv certifikata**: Myco_public_cert**Uobičajeno ime**: myco_rate_server@myco.com**Organizacijska jedinica**: Rate dept**Ime organizacije**: myco**Lokacija ili grad**: Any_city**Država**: Any**Zemlja**: 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? | DaMyco_CA@myco.com |

## Konfiguriranje HTTP Server ljudskih resursa za korištenje SSL-a

Konfiguracija Sloja sigurnih utičnica (SSL) za HTTP Server ljudskih resursa (upravljano s Apache) na iSeries A uključuje određen broj zadataka koji mogu varirati ovisno o tome kako je trenutno konfiguriran poslužitelj.

Da konfigurirate poslužitelj za upotrebu SSL-a, izvedite ove korake:

1. Pokrenite sučelje Administracija HTTP Poslužitelja.
2. Da biste radili s određenim HTTP poslužiteljem, izaberite ove kartice stranice **Upravljanje —> Svi poslužitelji —> Svi HTTP poslužitelji** da biste pogledali listu svih konfiguriranih HTTP poslužitelja.
3. Izaberite odgovarajući poslužitelj s liste i kliknite **Upravljanje detaljima**.
4. U navigacijskom okviru izaberite **Sigurnost**.
5. U obrascu izaberite karticu **SSL s provjerom autentičnosti certifikata**.
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 cjelokupnoj konfiguraciji koja je potrebna za HTTP poslužitelj prilikom korištenja SSL-a u informacijskom poglavlju HTTP poslužitelj za iSeries, posebno u primjeru koji se naziva scenarij: JKL omogućuje zaštitu Sloja sigurnih utičnica (SSL) na HTTP poslužitelju (upravljano s Apache). 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 trenutnih 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.

## Kreiranje i rad s 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 **Kreiraj izdavača certifikata (CA)** da biste prikazali nizove 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.

## Konfiguriranje provjere 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. Pomoću pretražitelja idite na stranicu i5/OS Zadaci na sistemu http://your_system_name:2001.
3. Izaberite **IBM Web administracija za i5/OS**.
4. Da biste radili s određenim HTTP poslužiteljem, izaberite ove kartice stranice **Upravljanje → Svi poslužitelji → Svi HTTP poslužitelji** da biste pogledali listu svih konfigurirani HTTP poslužitelja.
5. Izaberite odgovarajući poslužitelj s liste i kliknite **Upravljanje detaljima**.
6. U navigacijskom okviru izaberite **Sigurnost**.
7. Izaberite karticu **Provjera autentičnosti** na obrascu.
8. Izaberite **Koristi i5/OS profil klijenta**.
9. U polju **Ime provjere autentičnosti ili područje**, specificirajte ime za područje provjere autentičnosti.
10. Izaberite Omogućeno za polje **Zahtjevi obrade upotrebom ovlaštenja klijenta** i kliknite **Primijeni**.
11. Izaberite karticu **Kontroliraj pristup** na obrascu.
12. Izaberite **Svi korisnici provjerene autentičnosti (važeće korisničko ime i lozinka)** i kliknite **Primijeni**.
13. U obrascu izaberite karticu **SSL s provjerom autentičnosti certifikata**.
14. Osigurajte da je Omogućeno izabrana vrijednost u **SSL** polju.
15. U polju **Ime aplikacije za certifikat poslužitelja**, osigurajte da je specificirana ispravna vrijednost, na primjer, QIBM_HTTP_SERVER_MYCOTEST.

16. Izaberite **Prihvati certifikat klijenta ako je dostupan prije povezivanja**. Kliknite **OK**.

Možete naučiti više o cjelokupnoj konfiguraciji koja je potrebna za HTTP poslužitelj prilikom korištenja SSL-a u informacijskom poglavlju HTTP poslužitelj za iSeries, posebno u primjeru koji se naziva scenarij: JKL omogućuje zaštitu Sloja sigurnih utičnica (SSL) na HTTP poslužitelju (upravljano s Apache). Ovaj scenarij sadrži 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.

## Pokretanje Web poslužitelja ljudskih resursa u SSL načinu

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 Navigator proširite sistem.
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.

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

**Srodne informacije**

Pregled HTTP poslužitelja u Informacijskom centru

## Neka korisnici instaliraju kopiju certifikata Lokalnog CA u svoj pretražitelj

Kad korisnici pristupaju poslužitelju koji daje 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 **Instaliraj certifikat Lokalnog CA na PC** da biste prikazali stranicu koja dozvoljava spuštanje certifikata Lokalnog CA u pretražitelj ili pohranjivanje certifikata u datoteku na 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.

### 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. Pretražitelj može prikazati prozore koji će vas voditi kroz ovu obradu. Slijedite upute pretražitelja za ove poslove. Nakon što pretražitelj generira ključeve, stranica potvrde pokazuje da je DCM kreirao certifikat.
6. Instalirajte novi certifikat u softveru pretražitelja. Pretražitelj može prikazati prozore koji će vas voditi kroz ovu obradu. 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 iSeries 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.

## 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.

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 postavljanje DCM-a

Pregledajte ovo poglavlje da biste bili sigurni imate li instalirane potrebne opcije za izvođenje Upravitelja digitalnih certifikata (DCM).

DCM je besplatna iSeries značajka koja omogućuje centralno upravljanje digitalnim certifikatima za vaše aplikacije. Da bi uspješno koristili DCM, osigurajte da ste učinili sljedeće:

- Instalirajte opciju 34 i5/OS. Ovo je DCM funkcija osnovana na pretražitelju.
- Instalirajte IBM HTTP poslužitelj za i5/OS (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 sigurnosnog kopiranja i obnavljanja za DCM podatke

Koristite ove informacije da naučite kako osigurati dodavanje važnih DCM podataka u plan sigurnosnog kopiranja i obnavljanja za vaš sistem.

Šifrirane lozinke baze podataka ključa koje koristite za pristup spremištima certifikata u Upravitelju digitalnih certifikata (DCM), pohranjene su ili *skrivene* u posebnoj sigurnosnoj datoteci na sistemu. 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 takve okolnosti je kada koristite DCM za kreiranje certifikata za drugi **iSeries** sistem i izaberete korištenje datoteka certifikata na ciljnom sistemu za kreiranje novog spremišta certifikata. U toj situaciji morate otvoriti novokreirano spremište certifikata i koristiti zadatak **Changepassword** da biste promijenili lozinku za spremište certifikata na ciljnom sistemu, koji osigurava da će DCM sakriti novu lozinku. Ako je spremište certifikata Spremište certifikata drugog sistema, trebate također specificirati da želite koristiti opciju **Auto prijava** kada mijenjate lozinku. Da biste naučili više o korištenju DCM-a za kreiranje certifikata za druge iSeries sisteme, pogledajte Korištenje Lokalnog CA za izdavanje certifikata drugim iSeries sistemima.

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.

**Srodni zadaci**

“Upotreba Lokalnog CA za izdavanje certifikata drugim iSeries sistemima” na stranici 52
Pregledajte ove informacije da biste naučili kako koristiti privatnog Lokalnog CA na jednom sistemu za izdavanje certifikata na korištenje u drugim iSeries sistemima.

## Tipovi digitalnih certifikata

Koristite ove informacije da biste naučili o različitim tipovima digitalnih certifikata i kako se koriste u Upravitelju digitalnih certifikata (DCM).

Možete koristiti DCM da biste upravljali 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. Da biste koristili certifikat za SSL, potpisivanje objekata ili provjeru potpisa objekata, morate imati kopiju izdavanja certifikata od CA.

**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. Poslužitelj mora imati digitalni certifikat da bi koristio Sloj sigurnih utičnica (SSL) za sigurnu 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 objekta**

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.

**Korisnički certifikati**

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 iSeries korisničkim profilom. Možete koristiti DCM za pridruživanje korisničkih certifikata koje izdaje drugi Izdavač certifikata s iSeries korisničkim profilom.

Kada koristite Upravitelja digitalnih certifikata (DCM) za upravljanje certifikatima, DCM ih organizira i pohranjuje zajedno s njihovim privatnim ključevima u spremište certifikata baziranom na ovim klasifikacijama.

**Bilješka:** Ako imate instaliran IBM kriptografički koprocesor na sistemu, možete izabrati druge opcije za spremište privatnog ključa vaših certifikata (s izuzetkom certifikata potpisivanja objekta). 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.

**Srodni koncepti**

“Sloj sigurnih utičnica (SSL)” na stranici 9
Sloj sigurnih utičnica (SSL), koji je izvorno proizveo Netscape, je industrijski standard za šifriranje sesija između klijenata i poslužitelja.

“Spremišta certifikata” na stranici 7
Spremište certifikata je posebna datoteka baze podataka ključa koju Upravitelj digitalnih certifikata (DCM) koristi za pohranjivanje digitalnih certifikata.

## Javni certifikati naspram privatnih certifikata

Pregledajte ove informacije da biste naučili kako odrediti koji tip certifikata (javni ili privatni) najbolje odgovara vašim poslovnim potrebama.

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. Kada se odlučite za tip CA koji će se koristiti za izdavanje certifikata, morate izabrati tip implementacije certifikata koja najbolje odgovara vašim sigurnosnim potrebama. 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 aplikacija 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 svoje certifikate iz Lokalnog CA preko DCM-a, njihovi certifikati su pohranjeni s korisničkim profilom po defaultu. 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. Ako ne preferirate korisničke certifikate pridružene ili pohranjene s korisničkim profilom na bilo koji način, možete koristiti API-je za programsko 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 će vam biti korisno pregledati neke uobičajene kriterije korištenja certifikata da biste lakše odlučili hoće li javni ili privatni certifikati bolje odgovarati vašim poslovnim i sigurnosnim potrebama.

**Srodni zadaci**

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

- Kreiranje i rad s privatnim CA opisuje zadatke koje morate izvesti ako odlučite raditi s Lokalnim CA za izdavanje privatnih certifikata.
- Upravljanje certifikatima iz javnog Internet CA opisuje zadatke koji se moraju izvesti za upotrebu certifikata iz dobro poznatih javnih CA, uključujući i PKIX CA.
- Korištenje Lokalnog CA na drugim iSeries poslužiteljima opisuje zadatke koje morate izvesti ako želite koristiti certifikate od privatnih lokalnih CA na više sistema.

  **Srodni koncepti**

  “Upravljanje certifikatima od javnog Internet CA” na stranici 45
  Pregledajte ove informacije da biste naučili kako upravljati certifikatima iz javnog Internet CA kreiranjem spremišta certifikata.

  “Javni certifikati naspram privatnih certifikata” na stranici 28
  Pregledajte ove informacije da biste naučili kako odrediti koji tip certifikata (javni ili privatni) najbolje odgovara vašim poslovnim potrebama.

  “Postavljanje certifikata prvi put” na stranici 36
  Koristite ove informacije da biste naučili kako započeti s upravljanjem certifikata iz javnog Internet izdavača certifikata (CA) ili kako kreirati i raditi s privatnim Lokalnim CA za izdavanje certifikata.

  “Digitalni certifikati za potpisivanje objekata” na stranici 34
  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.

  **Srodni zadaci**

  “Digitalni certifikati i Mapiranje identiteta u poduzeću (EIM)” na stranici 32
  Korištenje Mapiranja identiteta u poduzeću (EIM) i Upravitelja digitalnim certifikatima (DCM) omogućuje primjenu certifikata kao izvora operacije pregledavanja EIM mapiranja za mapiranje s certifikata na ciljni korisnički identitet udružen s istim EIM identifikatorom.

  “Kreiranje certifikata korisnika” na stranici 40
  Pregledajte ove informacije da biste naučili kako korisnici mogu koristiti Lokalnog CA za izdavanje certifikata za provjeru autentičnosti klijenta.

  “Kreiranje i rad s Lokalnim CA” na stranici 37
  Ove informacije objašnjavaju kako kreirati i raditi s Lokalnim izdavačem certifikata (CA) da biste izdali privatne certifikate aplikacijama.

“Upotreba Lokalnog CA za izdavanje certifikata drugim iSeries sistemima” na stranici 52
Pregledajte ove informacije da biste naučili kako koristiti privatnog Lokalnog CA na jednom sistemu za izdavanje certifikata na korištenje u drugim iSeries sistemima.

**Srodne reference**

“Upotreba API-ja za programsko izdavanje certifikata ne-iSeries korisnicima” na stranici 43
Koristite ove informacije da biste naučili kako možete koristiti Lokalni CA za izdavanje privatnih certifikata korisnicima bez pridruživanja certifikata iSeries korisničkom profilu.

## Digitalni certifikati za SSL zaštićene komunikacije

Upotrijebite ove informacije da naučite kako se koriste certifikati da vaše aplikacije mogu postaviti sigurne komunikacijske sesije.

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. Da biste koristili certifikate kao dokaz identiteta, aplikacije koje komuniciraju 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.

**Srodni koncepti**

“Digitalni certifikati za provjeru korisnika”
Pregledajte ove informacije da biste naučili kako koristiti certifikate za osiguravanje sredstva bolje provjere autentičnosti korisnika koji pristupaju iSeries sistemskim resursima.

## Digitalni certifikati za provjeru korisnika

Pregledajte ove informacije da biste naučili kako koristiti certifikate za osiguravanje sredstva bolje provjere autentičnosti korisnika koji pristupaju iSeries sistemskim resursima.

Korisnici tradicionalno primaju pristup resursima od neke aplikacije ili sistema, na osnovi njihovog korisničkog imena i lozinke. Možete i dalje povećavati sistemsku sigurnost upotrebom digitalnih certifikata (umjesto korisničkih imena i lozinki) za provjeru autentičnosti i autorizirati sesije između mnogih aplikacija i korisnika. Također možete koristiti Upravitelja digitalnih certifikata (DCM) da biste pridružili korisnički certifikat s tim iSeries korisničkim profilom ili bilo kojim drugim korisničkim identitetom. Certifikat tada ima iste autorizacije i dozvole kao i pridruženi korisnički identitet ili korisnički profil. Alternativno, možete koristiti API-je za programsko korištenje Lokalnog izdavača certifikata koji će izdati certifikate ne-iSeries korisnicima. Ovi API-ji vam daju mogućnost izdavanja privatnih certifikata korisnicima kada ne želite da ovi korisnici imaju iSeries 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, iSeries aplikacije osiguravaju podršku certifikata za provjeru autentičnosti klijenta:

- Telnet poslužitelj
- IBM HTTP poslužitelj za i5/OS (upravljano s Apache)
- IBM Poslužitelj direktorija
- iSeries Access za Windows (uključujući iSeries Navigator 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, koji 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 ključ certifikata za provjeru identiteta pošiljatelja 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 dužine, zajedno s njihovom nasumičnom prirodom, teže je pogoditi kriptografske ključeve nego lozinke.
- Ključevi digitalnih certifikata omogućuju nekoliko mogućih prednosti 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 biste naučili više o konfiguriranju iSeries aplikacija tako da koriste certifikate za provjeru autentičnosti klijenta za vrijeme SSL sesije, pogledajte poglavlje Sloj sigurnih utičnica (SSL) u iSeries Informacijski Centar.

**Srodni koncepti**

“Digitalni certifikati za SSL zaštićene komunikacije” na stranici 30
Upotrijebite ove informacije da naučite kako se koriste certifikati da vaše aplikacije mogu postaviti sigurne komunikacijske sesije.

**Srodne reference**

“Upotreba API-ja za programsko izdavanje certifikata ne-iSeries korisnicima” na stranici 43
Koristite ove informacije da biste naučili kako možete koristiti Lokalni CA za izdavanje privatnih certifikata korisnicima bez pridruživanja certifikata iSeries korisničkom profilu.

# Digitalni certifikati i Mapiranje identiteta u poduzeću (EIM)

Korištenje Mapiranja identiteta u poduzeću (EIM) i Upravitelja digitalnim certifikatima (DCM) omogućuje primjenu certifikata kao izvora operacije pregledavanja EIM mapiranja za mapiranje s certifikata na ciljni korisnički identitet udružen s istim EIM identifikatorom.

EIM je tehnologija @server koja dozvoljava upravljanje korisničkim identitetima u 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 za **EIM konfiguraciju** u **iSeries Navigatoru** da biste konfigurirali EIM.
2. Kreirajte EIM identifikator za svakog korisnika za kojeg želite da sudjeluje u EIM-u.
3. Kreirajte ciljno pridruživanje između EIM identifikatora i tog korisničkog profila u lokalnom i5/OS korisničkom registru tako da se u korisnički profil može mapirati bilo koji korisnički certifikat koji korisnik dodjeljuje preko DCM-a ili ga kreira u DCM-u. Koristite ime definicije EIM registra za lokalni **i5/OS** korisnički registar koji ste specificirali u čarobnjaku za **EIM konfiguraciju**.

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 tako da rade zajedno, možete koristiti DCM da biste provjerili istek korisničkog certifikata na razini poduzeća, a ne samo na sistemskoj razini.

**Srodni koncepti**

“Javni certifikati naspram privatnih certifikata” na stranici 28
Pregledajte ove informacije da biste naučili kako odrediti koji tip certifikata (javni ili privatni) najbolje odgovara vašim poslovnim potrebama.

**Srodni zadaci**

“Upravljanje korisničkim certifikatima pomoću isteka” na stranici 42
Upravitelj digitalnih certifikata (DCM) osigurava podršku upravljanja za istek certifikata da bi omogućio administratorima upravljanje certifikatima klijenta ili poslužitelja, certifikatima potpisivanja objekta i certifikatima objekta po datumu isteka na lokalnom iSeries sistemu. Podrška upravljanja isteka DCM korisničkog certifikata može se koristiti zajedno s Mapiranjem identiteta u poduzeću (EIM) tako da administratori mogu koristiti DCM za provjeru isteka korisničkih certifikata na razini poduzeća.

"Upravljanje LDAP lokacijom za certifikate korisnika" na stranici 67
Pregledajte ove informacije da biste naučili kako konfigurirati DCM za pohranjivanje certifikata na lokaciju direktorija poslužitelja Lightweight Directory Access Protocol (LDAP) radi proširenja Mapiranja identiteta u poduzeću za rad s korisničkim certifikatima.

**Srodne informacije**

EIM poglavlje Informacijskog centra

## Digitalni certifikati za VPN veze

Pregledajte ove informacije da naučite kako koristiti certifikate kao dio konfiguriranja povezivanja Virtualne privatne mreže (VPN).

Možete koristiti digitalne certifikate kao sredstvo uspostavljanja iSeries VPN povezivanja. 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. Morate prvo odlučiti hoćete li koristiti javne certifikate ili privatne za IKE poslužitelj.

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).

**Srodne informacije**

Konfiguriranje 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.

IBM i5/OS osigurava podršku za korištenje certifikata u svrhu digitalnog ″potpisa″ objekata. Digitalno potpisivanje objekata pruža način provjere cjelovitosti sadržaja objekta i izvora porijekla. Podrška potpisivanja objekta proširuje tradicionalne iSeries sistemske alate za kontrolu nad mijenjanjem objekata. 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 korištenje digitalnih potpisa odgovara sigurnosnim potrebama i politici, morate procijeniti da li trebate koristiti javne ili 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 koristiti i DCM za potpisivanje objekata i provjeru potpisa objekata.

**Srodni koncepti**

“Javni certifikati naspram privatnih certifikata” na stranici 28
Pregledajte ove informacije da biste naučili kako odrediti koji tip certifikata (javni ili privatni) najbolje odgovara vašim poslovnim potrebama.

“Digitalni certifikati za provjeru potpisa objekata” na stranici 35
Ove informacije objašnjavaju kako koristiti certifikate za provjeru digitalnog potpisa na objektu da biste provjerili njegovu autentičnost.

**Srodni zadaci**

“Provjera valjanosti potpisa objekata” na stranici 70
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.

“Upravljanje javnim Internet certifikatima za potpisivanje objekata” na stranici 47
Upravitelja digitalnih certifikata (DCM) možete koristiti za upravljanje javnim Internet certifikatima za digitalno potpisivanje objekata.

“Upravljanje certifikatima za provjeru potpisa objekata” na stranici 48
Upravitelja digitalnih certifikata (DCM) možete koristiti za upravljanje certifikatima za provjeru potpisa koje koristite za provjeru digitalnih potpisa na objektima.

## Digitalni certifikati za provjeru potpisa objekata

Ove informacije objašnjavaju kako koristiti certifikate za provjeru digitalnog potpisa na objektu da biste provjerili njegovu autentičnost.

IBM i5/OS osigurava podršku korištenja certifikata za provjeru digitalnih potpisa na objektima. Svatko tko želi zaštititi objekt od promjena u prijenosu te da objekt proizveden od prihvaćenog 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 biste naučili više o korištenju ove i drugih sistemskih vrijednosti, pogledajte Pretraživač sistemske vrijednosti u iSeries Informacijski Centar.

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 koristiti i DCM za potpisivanje objekata i provjeru potpisa objekata.

**Srodni koncepti**

“Digitalni certifikati za potpisivanje objekata” na stranici 34
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.

**Srodne informacije**

Pronalazač sistemske vrijednosti

---

## 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.

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 slobodni u navigacijskom okviru ovise o spremištu certifikata u kojem radite. Također, kategorija i broj zadataka koje vidite u navigacijskom okviru ovise o ovlaštenjima koje ima i5/OS korisnički profil. Svi zadaci za rukovanje s CA, upravljanje certifikatima i upotrebu aplikacija te drugi zadaci sistemske razine, dostupni su samo iSeries službenicima sigurnosti ili administratorima. Službenik za zaštitu ili administrator mora imati *SECADM i *ALLOBJ posebna ovlaštenja, kako bi mogao pregledavati i koristiti ove zadatke. Korisnici bez ovih posebnih ovlaštenja imaju pristup samo funkcijama korisničkih certifikata.

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

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

Koristite ove informacije da biste naučili kako pristupiti značajki Upravitelja digitalnih certifikata (DCM) na sistemu.

Prije korištenja bilo kojih DCM funkcija, morate je pokrenuti. Dovršite ove zadatke da budete sigurni u uspješno pokretanje DCM-a.

1. Instalirajte 5722 SS1 opcija 34. Ovo je Upravitelj digitalnih certifikata (DCM).
2. Instalirajte 5722 DG1. To je IBM HTTP poslužitelj za i5/OS.
3. Koristite iSeries Navigator da biste pokrenuli administrativni poslužitelj HTTP poslužitelj:
   a. Pokrenite **iSeries Navigator** .
   b. Dva puta kliknite sistem u glavnom pogledu stabla.
   c. Proširite **Mreža > Poslužitelji > TCP/IP**.
   d. Desno kliknite na **HTTP Administraciju**.
   e. Kliknite **Pokreni**.
4. Pokrenite vaš Web pretražitelj.
5. Pomoću vašeg pretražitelja otiđite na stranicu iSeries Zadaci na vašem sistemu na http://*your_system_name*:2001.
6. Izaberite **Upravitelj digitalnih certifikata** iz popisa proizvoda na stranici iSeries Zadaci da pristupite DCM korisničkom sučelju.

   **Srodni koncepti**

   “Scenarij: Upotreba certifikata za eksternu provjeru autentičnosti” na stranici 11
   U ovom scenariju ćete naučiti kada i kako koristiti certifikate kao mehanizam provjere autentičnosti da biste zaštitili i ograničili pristup javnim korisnicima na javne ili extranet resurse i aplikacije.

## Postavljanje certifikata prvi put

Koristite ove informacije da biste naučili kako započeti s upravljanjem certifikata iz javnog Internet izdavača certifikata (CA) ili kako kreirati i raditi s privatnim Lokalnim CA za izdavanje certifikata.

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 iSeries Zadatke.

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 biste uspješno koristili ovu funkciju, morate prvo konfigurirati IBM HTTP poslužitelj za i5/OS za upotrebu SSL da bi radio 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 kada prvi put upotrijebite DCM, na temelju toga jeste li namjeravali koristiti javne certifikate ili izdavati privatne.

**Srodni koncepti**

“Javni certifikati naspram privatnih certifikata” na stranici 28
Pregledajte ove informacije da biste naučili kako odrediti koji tip certifikata (javni ili privatni) najbolje odgovara vašim poslovnim potrebama.

## Kreiranje i rad s Lokalnim CA

Ove informacije objašnjavaju kako kreirati i raditi s Lokalnim izdavačem certifikata (CA) da biste izdali privatne certifikate aplikacijama.

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:** Da biste koristili certifikate s IBM HTTP poslužitelj za i5/OS, morate kreirati i konfigurirati 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 Kreiraj izdavača certifikata (CA) da biste prikazali nizove 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 u svezi dovršavanja određenog obrasca u ovom vođenom zadatku, izaberite znak upitnika (?) 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 na sistemu imate instaliran IBM kriptografički koprocesor. 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 sistem ima instaliran IBM kriptografički koprocesor, ovaj korak vam dozvoljava izbor načina pohranjivanja privatnog ključa za certifikat. 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.

Kada završite s vođenim zadatkom, imate sve što je potrebno za početak s konfiguriranjem aplikacija za korištenje 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 ovog Lokalnog CA za izdavanje certifikata aplikacijama na drugim iSeries sistemima u 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:

**Srodni koncepti**

"Javni certifikati naspram privatnih certifikata" na stranici 28
Pregledajte ove informacije da biste naučili kako odrediti koji tip certifikata (javni ili privatni) najbolje odgovara vašim poslovnim potrebama.

"Upravljanje certifikatima korisnika"
Možete koristiti Upravitelja digitalnih certifikata (DCM) da biste dobili certifikate s SSL-om ili pridružili postojeće certifikate s njihovim iSeries korisničkim profilima.

**Srodni zadaci**

"Upotreba Lokalnog CA za izdavanje certifikata drugim iSeries sistemima" na stranici 52
Pregledajte ove informacije da biste naučili kako koristiti privatnog Lokalnog CA na jednom sistemu za izdavanje certifikata na korištenje u drugim iSeries sistemima.

"Dobivanje kopije privatnog CA certifikata" na stranici 44
Pregledajte ove informacije da naučite kako nabaviti kopiju privatnog CA certifikata i instalirali je na PC tako da možete provjeriti autentičnost certifikata poslužitelja koje izdaje CA.

**Srodne reference**

"Upotreba API-ja za programsko izdavanje certifikata ne-iSeries korisnicima" na stranici 43
Koristite ove informacije da biste naučili kako možete koristiti Lokalni CA za izdavanje privatnih certifikata korisnicima bez pridruživanja certifikata iSeries korisničkom profilu.

**Upravljanje certifikatima korisnika:**

Možete koristiti Upravitelja digitalnih certifikata (DCM) da biste dobili certifikate s SSL-om ili pridružili postojeće certifikate s njihovim iSeries korisničkim profilima.

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. Ako, ipak, poslužitelj pokazuje certifikat od privatnog Lokalnog CA, korisnici moraju nabaviti kopiju certifikata Lokalnog CA 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 aplikacija poslužitelja osigurava pristup resursima za interne korisnike koji trenutno imaju iSeries korisničke profile, možete koristiti DCM da biste dodali njihove certifikate u korisničke profile. To udruživanje osigurava korisnicima da prilikom predstavljanja certifikata imaju isti pristup i ograničenja za resurse kakve i njihov korisnički profil dodjeljuje ili odbija.

Upravitelj digitalnih certifikata (DCM) dozvoljava upravljanje certifikatima koji su dodijeljeni iSeries korisničkom profilu. Ako imate korisnički profil sa *SECADM i *ALLOBJ posebnim ovlaštenjem, možete upravljati dodjelom certifikata korisničkih profila za vas ili za druge korisnike. Kada nije otvoreno spremište certifikata ili kada je otvoreno spremište certifikata Lokalnog izdavača certifikata (CA), možete izabrati **Upravljanje certifikatima korisnika** u navigacijskom okviru da biste pristupili prikladnim 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:

**Srodni zadaci**

"Kreiranje i rad s Lokalnim CA" na stranici 37
Ove informacije objašnjavaju kako kreirati i raditi s Lokalnim izdavačem certifikata (CA) da biste izdali privatne certifikate aplikacijama.

"Dobivanje kopije privatnog CA certifikata" na stranici 44
Pregledajte ove informacije da naučite kako nabaviti kopiju privatnog CA certifikata i instalirali je na PC tako da možete provjeriti autentičnost certifikata poslužitelja koje izdaje CA.

*Kreiranje certifikata korisnika:*

Pregledajte ove informacije da biste naučili kako korisnici mogu koristiti Lokalnog CA za izdavanje certifikata za provjeru autentičnosti klijenta.

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. Pretražitelj može prikazati prozore koji će vas voditi kroz ovu obradu. Slijedite upute pretražitelja za ove poslove. Nakon što pretražitelj generira ključeve, stranica potvrde pokazuje da je DCM kreirao certifikat.
6. Instalirajte novi certifikat u softveru pretražitelja. Pretražitelj može prikazati prozore koji će vas voditi kroz ovu obradu. 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 iSeries korisničkim profilom.

Ako želite certifikat od drugog CA kojeg korisnik predstavlja da bi provjera autentičnosti klijenta imala ista ovlaštenja kao i njihov korisnički profil, možete koristiti DCM za dodjelu certifikata korisničkom profilu.

**Srodni koncepti**

"Javni certifikati naspram privatnih certifikata" na stranici 28
Pregledajte ove informacije da biste naučili kako odrediti koji tip certifikata (javni ili privatni) najbolje odgovara vašim poslovnim potrebama.

**Srodni zadaci**

"Dodjela certifikata korisnika"
Možete dodijeliti korisnički certifikat koji posjedujete i5/OS 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.

"Dobivanje kopije privatnog CA certifikata" na stranici 44
Pregledajte ove informacije da naučite kako nabaviti kopiju privatnog CA certifikata i instalirali je na PC tako da možete provjeriti autentičnost certifikata poslužitelja koje izdaje CA.

*Dodjela certifikata korisnika:*

Možete dodijeliti korisnički certifikat koji posjedujete i5/OS 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.

Neki korisnici mogu imati certifikate od vanjskog Izdavača certifikata (CA) ili Lokalnog CA na različitim iSeries sistemima koje vi, kao administrator, želite napraviti 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:

- Lokalno pohranjivanje certifikata na iSeries s korisničkim profilom. Kada LDAP lokacija nije definirana za DCM, zadatak **Dodjela korisničkog certifikata** dozvoljava korisniku dodjelu vanjskog certifikata i5/OS 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 pohranjivanje i kopiranje vanjskog 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 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 koji 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. Može biti odgovorno nekoliko problema s korisničkim certifikatom. Na primjer, certifikati koje vaš pretražitelj sadrži mogu već biti pridruženi s vašim korisničkim identitetom.

   **Srodni zadaci**

   “Kreiranje certifikata korisnika” na stranici 40
   Pregledajte ove informacije da biste naučili kako korisnici mogu koristiti Lokalnog CA za izdavanje certifikata za provjeru autentičnosti klijenta.

   “Rješavanje problema dodjele korisničkog certifikata” na stranici 77

   **Srodne informacije**

   Pregled EIM-a u Informacijskom centru

*Upravljanje korisničkim certifikatima pomoću isteka:*

Upravitelj digitalnih certifikata (DCM) osigurava podršku upravljanja za istek certifikata da bi omogućio administratorima upravljanje certifikatima klijenta ili poslužitelja, certifikatima potpisivanja objekta i certifikatima objekta po datumu isteka na lokalnom iSeries sistemu. Podrška upravljanja isteka DCM korisničkog certifikata može se koristiti zajedno s Mapiranjem identiteta u poduzeću (EIM) tako da administratori mogu koristiti DCM za provjeru isteka korisničkih 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 odgovarajuće 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.

   **Bilješka:** Ako trenutno radite sa spremištem certifikata, izaberite **Upravljanje certifikatima** da bi prikazali popis zadataka, a zatim izaberite **Provjeri istek**, 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 pregled i upravljanje korisničkim certifikatima koji su dodijeljeni određenom i5/OS korisničkom profilu. Specificirajte **Ime korisničkog profila** i kliknite **Nastavak**.

**Bilješka:** Možete navesti korisnički profil koji nije vaš vlastiti samo ako imate posebna ovlaštenja *ALLOBJ i *SECADM.

- **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.

**Srodni zadaci**

"Digitalni certifikati i Mapiranje identiteta u poduzeću (EIM)" na stranici 32
Korištenje Mapiranja identiteta u poduzeću (EIM) i Upravitelja digitalnim certifikatima (DCM) omogućuje primjenu certifikata kao izvora operacije pregledavanja EIM mapiranja za mapiranje s certifikata na ciljni korisnički identitet udružen s istim EIM identifikatorom.

**Srodne informacije**

Pregled EIM-a u Informacijskom centru

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

Koristite ove informacije da biste naučili kako možete koristiti Lokalni CA za izdavanje privatnih certifikata korisnicima bez pridruživanja certifikata iSeries korisničkom profilu.

U i5/OS V5R3 ili novijem, dostupna su dva nova API-ja koja možete koristiti za programsko izdavanje certifikata ne-iSeries korisnicima. U prethodnim izdanjima kada ste koristili Lokalnog izdavača certifikata (CA) za izdavanje certifikata korisnicima, ovi certifikati bili su automatski pridruženi iSeries korisničkim profilima. Prema tome, da biste koristili Lokalnog CA za izdavanje certifikata korisniku za provjeru autentičnosti klijenta, morali ste osigurati 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. Zbog toga svaki korisnik mora imati korisnički profil na iSeries poslužitelju koji uslužuje DCM i važeću prijavu za taj iSeries poslužitelj.

Pridruživanje certifikata korisničkom profilu ima svojih prednosti, posebno kada se radi o internim korisnicima. Međutim, ova ograničenja i zahtjevi nisu omogućila praktično korištenje Lokalnog CA za izdavanje korisničkih certifikata 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 uslužuje DCM i ne treba koristiti DCM da bi se kreirao certifikat.

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 API-ja za korištenje Lokalnog CA za potpisivanje certifikata.

Za više informacija o korištenju ovih API-ja, pogledajte ove stranice:

- Generiranje i potpisivanje zahtjeva certifikata korisnika(QYCUGSUC) API.
- Potpisivanje zahtjeva certifikata korisnika( QYCUSUC) API.

**Srodni koncepti**

"Javni certifikati naspram privatnih certifikata" na stranici 28
Pregledajte ove informacije da biste naučili kako odrediti koji tip certifikata (javni ili privatni) najbolje odgovara vašim poslovnim potrebama.

"Digitalni certifikati za provjeru korisnika" na stranici 30
Pregledajte ove informacije da biste naučili kako koristiti certifikate za osiguravanje sredstva bolje provjere autentičnosti korisnika koji pristupaju iSeries sistemskim resursima.

**Srodni zadaci**

"Kreiranje i rad s Lokalnim CA" na stranici 37
Ove informacije objašnjavaju kako kreirati i raditi s Lokalnim izdavačem certifikata (CA) da biste izdali privatne certifikate aplikacijama.

**Dobivanje kopije privatnog CA certifikata:**

Pregledajte ove informacije da naučite kako nabaviti kopiju privatnog CA certifikata i instalirali je na PC tako da možete provjeriti autentičnost certifikata poslužitelja koje izdaje CA.

Kad pristupate poslužitelju koji koristi vezu Sloja sigurnih utičnica (SSL), poslužitelj predočava certifikat vašem klijentskom softveru kao dokaz njegovog identiteta. Softver klijenta mora zatim provjeriti poslužiteljev certifikat da poslužitelj može uspostaviti sesiju. Da provjerite valjanost certifikata poslužitelja, softver klijenta 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 vašu provjeru autentičnosti predstavljanjem certifikata od Lokalnog CA, morate spustiti certifikat Lokalnog CA u 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 **Instaliraj certifikat Lokalnog CA na PC** da biste prikazali stranicu koja dozvoljava spuštanje certifikata Lokalnog CA u pretražitelj ili pohranjivanje certifikata u datoteku na 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.

**Srodni koncepti**

"Upravljanje certifikatima korisnika" na stranici 39
Možete koristiti Upravitelja digitalnih certifikata (DCM) da biste dobili certifikate s SSL-om ili pridružili postojeće certifikate s njihovim iSeries korisničkim profilima.

**Srodni zadaci**

"Kreiranje i rad s Lokalnim CA" na stranici 37
Ove informacije objašnjavaju kako kreirati i raditi s Lokalnim izdavačem certifikata (CA) da biste izdali privatne certifikate aplikacijama.

"Kreiranje certifikata korisnika" na stranici 40
Pregledajte ove informacije da biste naučili kako korisnici mogu koristiti Lokalnog CA za izdavanje certifikata za provjeru autentičnosti klijenta.

## Upravljanje certifikatima od javnog Internet CA

Pregledajte ove informacije da biste naučili kako upravljati certifikatima iz javnog Internet CA kreiranjem spremišta certifikata.

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.

**Bilješka:** DCM također dozvoljava upravljanje certifikatima koje dobivate od Izdavača certifikata Infrastrukture javnog ključa za X.509 (PKIX).

Da naučite kako koristiti DCM za kreiranje odgovarajućeg spremišta certifikata i upravljanje javnim Internet certifikatima za vaše aplikacije, pregledajte ova poglavlja:

**Srodni koncepti**

"Javni certifikati naspram privatnih certifikata" na stranici 28
Pregledajte ove informacije da biste naučili kako odrediti koji tip certifikata (javni ili privatni) najbolje odgovara vašim poslovnim potrebama.

**Srodni zadaci**

"Upravljanje lokacijom zahtjeva za PKIX CA" na stranici 67
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.

**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 koje vaše aplikacije mogu 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 sistem ima instaliran IBM kriptografički koprocesor, DCM vam dozvoljava izbor načina pohranjivanja privatnog ključa 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. Dovršite obrazac i kliknite **Nastavak** da prikažete stranicu za potvrdu. 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 pričekati dok CA ne vrati potpisan i dovršen certifikat.

   Za upotrebu certifikata s HTTP poslužiteljem za vaš sistem, morate kreirati i konfigurirati Web poslužitelj prije rada s DCM-om da bi mogli raditi s potpisanim dovršenim certifikatima. Kada konfigurirate Web poslužitelj za upotrebu SSL-a, ID aplikacije se generira za poslužitelj. Morate zapisati ovaj ID aplikacije tako da možete koristiti DCM za specificiranje koji certifikat ova aplikacija mora koristiti za SSL.

   Ne zaustavljajte i ponovno pokrećite poslužitelj dok ne upotrijebite 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 moći 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 sa Spremištem certifikata i lozinkom, navedite lozinku koju ste specificirali za spremište certifikata kada 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 koji 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. Ovo osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA 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.

Kada završite s vođenim zadatkom, imate sve što je potrebno za početak s konfiguriranjem aplikacija za korištenje SSL-a 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. (Međutim, možete provjeriti zahtijevanje ovlaštenje aplikacijskog ID-a pomoću iSeries Navigator.)

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 koje 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 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. Ovo prikazuje obrazac koji vam dopušta da unesete informacije o identifikaciji za novi certifikat.
6. Dovršite obrazac i kliknite **Nastavak** da prikažete stranicu za potvrdu. 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.

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 sa Spremištem certifikata i lozinkom, navedite lozinku koju ste specificirali za spremište certifikata kada 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. Dovršite obrazac da biste definirali aplikaciju potpisivanja 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 koji ste importirali i kliknite **Dodjela novog certifikata**.

Kada završite s ovim zadacima, imate sve što je potrebno za potpisivanje objekata radi osiguravanja integriteta.

Kada distribuirate potpisane objekte, oni koji primaju objekte moraju koristiti OS/400 V5R1 ili noviju verziju DCM-a za provjeru valjanosti potpisa nad objektima da bi se osigurala stalnost podataka i radi provjere identiteta pošiljatelja. Da biste provjerili valjanost potpisa, primatelj mora imati kopiju certifikata provjere valjanosti potpisa. Morate dobaviti kopiju ovog certifikata kao dio paketa potpisanih objekata.

Primatelj također mora imati kopiju CA certifikata za CA koji je izdao certifikat koji 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 primatelj 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.

**Srodni koncepti**

“Digitalni certifikati za potpisivanje objekata” na stranici 34
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.

**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.

Za potpisivanje objekta 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 potpise koje 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 javni ključ certifikata 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. 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** kao spremište certifikata za otvaranje.
6. Kad se prikaže stranica sa Spremištem certifikata i lozinkom, navedite lozinku koju ste specificirali za spremište certifikata kada 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 koji želite importirati. Izaberite **Provjera potpisa** da importirate certifikat koji ste primili s potpisanim objektima i dovršite zadatak importiranja.

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

Sada možete koristiti ove certifikate za provjeru potpisa objekta.

**Srodni koncepti**

"Digitalni certifikati za potpisivanje objekata" na stranici 34
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.

**Srodni zadaci**

"Provjera valjanosti potpisa objekata" na stranici 70
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.

# Obnavljanje postojećeg certifikata

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

Možete obnoviti certifikat s Lokalnim CA ili s Internet CA.

## Obnavljanje certifikata iz Lokalnog CA

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.

Da biste obnovili certifikat s Lokalnim CA, pratite ove korake:

1. U navigacijskom okviru kliknite **Izbor spremišta certifikata**, a zatim izaberite spremište certifikata koje sadrži certifikat koji želite obnoviti.
2. U navigacijskom okviru izaberite **Upravljanje certifikatima**.
3. U navigacijskom okviru izaberite **Obnovi certifikat**.
4. Izaberite certifikat koji želite obnoviti i kliknite **Obnovi**.
5. Izaberite **Lokalni izdavač certifikata (CA)** i kliknite **Nastavak**.
6. Dovršite obrazac identifikacije certifikata. Morate promijeniti polje **Nova labela certifikata**, ali sva ostala polja mogu ostati ista.
7. Izaberite aplikacije koje želite da obnovljeni certifikat koristi i kliknite **Nastavak** da završite obnavljanje certifikata.

   **Bilješka:** Ne morate izabrati aplikaciju koja će koristiti certifikat.

## Obnavljanje certifikata iz Internet CA

Ako koristite dobro poznati Internet CA za izdavanje certifikata, možete rukovati obnavljanjem certifikata na dva načina.

Možete obnoviti certifikat izravno iz Internet CA, a zatim ga importirati iz datoteke koju ste primili potpisivanjem CA. Ili možete koristiti DCM da biste kreirali novi par javnog privatnog ključa i certifikata Zahtjeva za potpisivanje certifikata (CSR), a zatim poslali informacije Internet CA radi dobivanja novog certifikata. Kada primite taj certifikat natrag od CA, možete dovršiti obradu obnove.

**Importiranje i obnova certifikata dobivenog izravno od Internet CA:**

Da biste importirali i obnovili certifikat koji ste dobili izravno od Internet CA, pratite ove korake:

1. U navigacijskom okviru kliknite **Izbor spremišta certifikata**, a zatim izaberite spremište certifikata koje sadrži certifikat koji želite obnoviti.

   **Bilješka:** Kliknite "?" na bilo kojem panelu za odgovor na bilo koja daljnja pitanja o dovršavanju panela.
2. U navigacijskom okviru izaberite **Upravljanje certifikatima**.
3. U navigacijskom okviru kliknite **Obnovi certifikat**.
4. Izaberite certifikat koji želite obnoviti i kliknite **Obnovi**.
5. Izaberite **VeriSign** ili drugog **Internet izdavača certifikata (CA)** i kliknite **Nastavak**.
6. Izaberite **Ne - importiraj obnovljeni potpisani certifikat iz postojeće datoteke**.
7. Dovršite vođeni zadatak za import certifikata. Kada izaberete obnovu certifikata izravno s CA koji ga je izdao, taj CA vam vraća obnovljeni certifikat u datoteci. Provjerite jeste li specificirali ispravnu apsolutnu stazu za datoteku gdje je pohranjen certifikat na poslužitelju kada importirate certifikat. Datoteka koja sadrži obnovljeni certifikat može se pohraniti u bilo koji direktorij integriranog sistema datoteka (IFS).
8. Kliknite **OK** da dovršite zadatak.

**Obnavljanje certifikata kreiranje novog para javnog-privatnog ključa i CSR-a za certifikat:**

Da biste obnovili certifikat s Internet CA kreiranjem novog para javnog-privatnog ključa i CSR-a za certifikat, pratite ove korake

1. U navigacijskom okviru kliknite **Izbor spremište certifikata**, a zatim izaberite spremište certifikata koje sadrži certifikat koji želite obnoviti.

   **Bilješka:** Kliknite "?" na bilo kojem panelu za odgovor na bilo koja daljnja pitanja o dovršavanju panela.
2. U navigacijskom okviru izaberite **Upravljanje certifikatima**.
3. U navigacijskom okviru kliknite **Obnovi certifikat**
4. Izaberite certifikat koji želite obnoviti i kliknite **Obnovi**.
5. Izaberite **VeriSign** ili drugog **Internet izdavača certifikata (CA)** i kliknite **Nastavak**.
6. Kliknite **Da - kreiraj novi par za ovaj certifikat i kliknite Nastavak**.
7. Dovršite obrazac identifikacije certifikata. Morate promijeniti naslov polja Novog certifikata, ali sva druga polja mogu ostati ista. Napomena: kliknite "?" na bilo kojem panelu za odgovor na bilo koja daljnja pitanja o dovršavanju panela.
8. Kliknite **OK** da dovršite zadatak.

## Importiranje certifikata

Pregledajte ove informacije da biste naučili kako koristiti Upravitelja digitalnih certifikata (DCM) da biste importirali certifikate koji su smješteni u datotekama na poslužitelju.

Možete importirati certifikate s drugih poslužitelja umjesto ponovnog kreiranja certifikata na trenutnom poslužitelju. Na primjer, na iSeries A ste koristili Lokalnog CA za kreiranje certifikata vaše retail web aplikacije za iniciranje SSL povezivanja. Posao je nedavno procvao i instalirali ste novi iSeries poslužitelj (iSeries B) koji će usluživati više instanci ove vrlo zauzete retail aplikacije. Želite da sve instance retail aplikacije koriste identični certifikat za identificiranje i iniciranje SSL povezivanja. Prema tome, možda ćete odlučiti importirati certifikat Lokalnog CA i certifikat poslužitelja iz iSeries A u iSeries B, umjesto da koristite Lokalni CA na iSeries A za kreiranje novog, drukčijeg certifikata kojeg će iSeries B koristiti.

Pratite ove korake da bi koristili DCM za importiranje certifikata:

1. U navigacijskom okviru na lijevoj strani kliknite **Izbor spremišta certifikata** i izaberite spremište certifikata u koje želite importirati certifikat. Spremište certifikata u koje importirate certifikat mora sadržavati certifikate istog

tipa kao i certifikat koji ste eksportirali na drugi sistem. Na primjer, ako importirate certifikat poslužitelja (tip) tada ga importirajte u spremište certifikata koje sadrži certifikate poslužitelja kao što je *SYSTEM ili Spremište certifikata drugog sistema.

2. U navigacijskom okviru izaberite **Upravljanje certifikatima**.
3. U navigacijskom okviru izaberite **Importiraj certifikat**.
4. Izaberite tip certifikata koji želite importirati i kliknite **Nastavak**. Tip certifikata koji importirate mora biti istog tipa certifikata koji ste eksportirali. Na primjer, ako ste eksportirali certifikat poslužitelja, izaberite importiranje certifikata poslužitelja.

   **Bilješka:** Kada DCM eksportira certifikat u formatu pkcs12, CA koji ga je izdao uključen je u lanac eksportiranog certifikata i zbog toga se automatski importira kad je sam certifikat importiran u spremište certifikata od strane DCM-a. Međutim, ako certifikat nije eksportiran u formatu pkcs12 i nemate CA certifikat u spremištu certifikata u kojeg importirate, morate importirati certifikat CA koji ga je izdao prije nego možete importirati certifikat.
5. Dovršite vođeni zadatak da biste importirali certifikat. Kada importirate certifikat provjerite jeste li specificirali ispravnu apsolutnu stazu gdje je certifikat pohranjen na poslužitelju.

---

# 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.

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 drugim iSeries sistemima

Pregledajte ove informacije da biste naučili kako koristiti privatnog Lokalnog CA na jednom sistemu za izdavanje certifikata na korištenje u drugim iSeries sistemima.

Možda već koristite privatnog lokalnog izdavača ovlaštenja (CA) na sistemu u mreži. Sada biste htjeli proširiti upotrebu ovog Lokalnog CA na druge sisteme u mreži. Na primjer, želite da trenutni Lokalni CA izda certifikat poslužitelja ili klijenta za aplikaciju na drugom sistemu radi korištenja SSL komunikacijskih sesija. 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). Izvest ćete neke zadatke na sistemu na kojem radite s Lokalnim CA, druge ćete izvesti na sekundarnom sistemu koji uslužuje aplikacije kojima želite izdat i 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 sistem na kojem radite s Lokalnim CA koristi proizvod dobavljača kriptografičkog pristupa koji osigurava bolje šifriranje od ciljnog sistema. Za OS/400 V5R2 i OS/400 V5R3 je jedini dostupni kriptografički pristup 5722–AC3, koji je najjači dostupan proizvod. Međutim, u ranijim izdanjima ste mogli instalirati druge, slabije proizvode dobavljača kriptografičkog pristupa (5722–AC1 ili 5722–AC2) koji su osiguravali niže razine kriptografičke funkcije. Kada bi eksportirali certifikat (s privatnim ključem), sistem bi šifrirao datoteku radi zaštite njenog sadržaja. 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. Kada koristite Lokalnog CA za kreiranje certifikata radi korištenja na drugom sistemu, datoteke koje kreira DCM sadrže kopiju certifikata Lokalnog CA, kao i kopije certifikata za mnoge javne Internet CA-e.

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 radi korištenja na drugom iSeries sistemu**

Da biste koristili Lokalnog CA za izdavanje certifikata radi korištenja na drugom sistemu, izvedite ove korake na sistemu koji uslužuje Lokalnog CA:

1. Pokretanje DCM-a
2. U navigacionom okviru, izaberite **Kreiraj certifikat** da prikažete listu tipova certifikata za čije kreiranje možete koristiti vaš Lokalni CA.

   **Bilješka:** 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. Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
3. Izaberite tip certifikata koji želite da Lokalni CA izda i kliknite **Nastavak** da pokrenete vođeni zadatak i dovršite nizove obrazaca.
4. Izaberite kreiranje **certifikata poslužitelja ili klijenta za drugi iSeries** (za SSL sesije) ili **certifikat potpisivanja objekta za drugi iSeries** (za korištenje na drugom sistemu).

   **Bilješka:** Ako kreirate certifikat potpisivanja objekta za korištenje na drugom sistemu, taj sistem mora izvoditi OS/400 V5R1 ili noviji da bi koristio certifikat. Budući da ciljni sistem mora biti verzije OS/400 V5R1 ili novije, DCM na lokalnom host sistemu ne traži od vas da izaberete format ciljnog izdanja za novi certifikat potpisivanja objekta.
5. Dovršite obrazac i kliknite **Nastavak** da prikažete stranicu za potvrdu.

   **Bilješka:** Ako postoji *OBJECTSIGNING ili *SYSTEM spremište certifikata na ciljnom sistemu, svakako odredite jedinstvenu oznaku certifikata i jedinstveno ime datoteke za certifikat. Određivanje jedinstvene oznake certifikata i imena datoteke omogućuje vam lako importiranje certifikata u postojeće spremište certifikata na ciljnom sistemu. Ova stranica za potvrdu prikazuje nazive datoteka koje je DCM kreirao za vas radi prijenosa na ciljni sistem. DCM kreira ove datoteke na osnovi razine izdanja ciljnog sistema koju ste specificirali. DCM automatski stavlja kopiju Lokalnog CA certifikata u te datoteke.

   DCM kreira novi certifikat u vlastitom spremištu certifikata i generira dvije datoteke za prijenos: datoteku spremišta certifikata (.KDB proširenje) i datoteku zahtjeva (.RDB proširenje).
6. Koristite binarni Protokol za prijenos datoteka (FTP) ili drugi način prijenosa datoteka na ciljni sistem.

**Srodni koncepti**

“Razmatranja sigurnosnog kopiranja i obnavljanja za DCM podatke” na stranici 26
Koristite ove informacije da naučite kako osigurati dodavanje važnih DCM podataka u plan sigurnosnog kopiranja i obnavljanja za vaš sistem.

“Javni certifikati naspram privatnih certifikata” na stranici 28
Pregledajte ove informacije da biste naučili kako odrediti koji tip certifikata (javni ili privatni) najbolje odgovara vašim poslovnim potrebama.

**Srodni zadaci**

“Kreiranje i rad s Lokalnim CA” na stranici 37
Ove informacije objašnjavaju kako kreirati i raditi s Lokalnim izdavačem certifikata (CA) da biste izdali privatne certifikate aplikacijama.

## Upotreba privatnih certifikata za SSL

Certifikatima, koje koriste vaše aplikacije za SSL sesije, upravljate iz *SYSTEM spremišta certifikata u Upravitelju digitalnih certifikata. Ako nikada niste koristili DCM na 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 spremište certifikata *SYSTEM postoji na ciljnom sistemu, možete koristiti prenesene datoteke kao Spremište certifikata drugog sistema ili importirati prenesene datoteke u postojeće spremište certifikata *SYSTEM.

**Spremište certifikata *SYSTEM ne postoji:**

Ako spremište certifikata *SYSTEM ne postoji na sistemu na kojem želite koristiti prenesene datoteke spremišta certifikata, možete koristiti prenesene datoteke certifikata kao spremište certifikata *SYSTEM. Da biste kreirali spremište certifikata *SYSTEM i koristili datoteke certifikata na ciljnom sistemu, pratite 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.

   **Pažnja:** 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, osigurajte lozinku koju ste naveli u *host* sistemu za spremište certifikata kada ste kreirali certifikat za 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 **Dodijeli aplikacijama** da biste prikazali 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. Ovo osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA 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.

Kada dovršite ovaj zadatak, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao Lokalni CA na drugom sistemu. 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 — korištenje datoteka kao Certifikat drugog sistema:**

Ako ciljni sistem već ima spremište certifikata *SYSTEM, morate odlučiti kako će se 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 aplikacije drugih razvijača softvera) su napisane za upotrebu 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. Prema tome, ne možete konfigurirati standardne iSeries SSL-omogućene aplikacije da biste koristili ovaj certifikat. Ako želite koristiti certifikat za iSeries aplikacije, morate importirati certifikat iz prenesenih datoteka spremišta certifikata u spremište certifikata *SYSTEM.

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 bi se otvorilo 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 osigurajte lozinku koju ste specificirali na *host* sistemu za spremište certifikata kada ste kreirali certifikat za 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. Korištenjem ove opcije DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatom u novom spremištu.

   Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima. Dalje možete specificirati da se certifikat u ovom spremištu koristi 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 — korištenje certifikata u postojećem spremištu certifikata *SYSTEM:*

Možete koristiti certifikate u prenesenim datotekama spremišta certifikata u postojećem spremištu certifikata *SYSTEM na 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.

Da biste eksportirali certifikate iz datoteka spremišta certifikata u spremište certifikata *SYSTEM, dovršite ove korake na 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 osigurajte lozinku koju ste specificirali na *host* sistemu za spremište certifikata kada ste kreirali certifikat za 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. Nakon što ste promijenili lozinku, morate ponovno otvoriti spremište certifikata prije nego što možete u njemu raditi s certifikatima.

   **Bilješka:** Budite sigurni da ste izabrali opciju **Automatska prijava** kada mijenjate lozinku za spremište certifikata. Korištenjem ove opcije DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatom 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.
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 prikladan certifikat klijenta ili poslužitelja za eksport i kliknite **Eksport**.
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** da bi se otvorilo spremište certifikata.
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 **Dodijeli aplikacijama** da biste prikazali 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. Ovo osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA 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.

Kada dovršite ovaj zadatak, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao Lokalni CA na drugom sistemu. 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 potpisivanje objekata na 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 za kreiranje *OBJECTSIGNING spremišta certifikata. Ako certifikat *OBJECTSIGNING postoji na ciljnom sistemu, morate u 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 spremište certifikata *OBJECTSIGNING ne postoji na ciljnom sistemu s prenesenim datotekama spremišta certifikata, pratite 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.

   **Pažnja:** 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** za otvaranje spremišta 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. Dovršite obrazac da biste definirali aplikaciju potpisivanja 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 primaju objekte moraju koristiti DCM za provjeru valjanosti potpisa nad objektima da bi se osigurala stalnost podataka i radi provjere identiteta pošiljatelja. Da biste provjerili valjanost potpisa, primatelj mora imati kopiju certifikata provjere valjanosti potpisa. Morate dobaviti kopiju ovog certifikata kao dio paketa potpisanih objekata.

Primatelj također mora imati kopiju CA certifikata za CA koji je izdao certifikat koji 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.

**Spremište certifikata *OBJECTSIGNING postoji:**

Možete koristiti certifikate u datotekama spremišta certifikata u postojećem spremištu certifikata *OBJECTSIGNING na 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 spremište certifikata *OBJECTSIGNING otvaranjem prenesenih datoteka kao Drugo sistemsko spremište certifikata na ciljnom sistemu. Možete eksportirati certifikate izravno u *OBJECTSIGNING spremište certifikata. Morate eksportirati kopiju certifikata potpisivanja objekta i Lokalnog CA certifikata iz prenesenih datoteka.

Da biste eksportirali certifikate iz datoteka spremišta certifikata izravno u spremište certifikata *OBJECTSIGNING, dovršite ove korake na 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. Kad se prikaže stranica s lozinkom, unesite lozinku koju ste koristili kad ste ga 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. Korištenjem ove opcije DCM pohranjuje novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatom 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 eksportirane certifikate 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.

# Upravljanje aplikacijama u DCM-u

Ova poglavlja sadrže 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.

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:

**Srodni koncepti**

“Definicije aplikacija” na stranici 9
Koristite ove informacije da biste naučili što su DCM aplikacijske definicije i kako s njima raditi za SSL konfiguraciju i potpisivanje objekta.

## Kreiranje definicije aplikacije

Pregledajte ovo poglavlje da biste naučili o različitim tipovima aplikacija koje možete definirati za rad.

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 iSeries 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 sa Spremištem certifikata i lozinkom, navedite lozinku koju ste specificirali za spremište certifikata kada 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.

   **Srodni koncepti**

   "Definicije aplikacija" na stranici 9
   Koristite ove informacije da biste naučili što su DCM aplikacijske definicije i kako s njima raditi za SSL konfiguraciju i potpisivanje objekta.

## 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 sa Spremištem certifikata i lozinkom, navedite lozinku koju ste specificirali za spremište certifikata kada 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. Ovo osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA 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, iSeries Access za Windows poslužitelji će primijeniti bilo koje promjene certifikata koje automatski napravite. Međutim, možda ćete morati zaustaviti i pokrenuti Telnet poslužitelje, IBM HTTP poslužitelj za i5/OS ili druge aplikacije prije nego ove aplikacije mogu primijeniti promjene certifikata.

U OS/400 V5R2 ili novijem možete koristiti zadatak Dodjela certifikata kada odjednom želite dodijeliti certifikat za nekoliko aplikacija.

### 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 koji 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, mora 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. Ovo osigurava da aplikacija može provjeriti valjanost samo onih certifikata od CA 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** kao spremište certifikata koje treba otvoriti.

   **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 sa Spremištem certifikata i lozinkom, navedite lozinku koju ste specificirali za spremište certifikata kada 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 aplikacija 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 upravljanja za istek certifikata da bi omogućio administratorima upravljanje certifikatima klijenta ili poslužitelja, certifikatima potpisivanja objekta i certifikatima objekta po datumu isteka na lokalnom sistemu.

**Bilješka:** Ako konfigurirate DCM za rad s Mapiranjem identiteta u poduzeću (EIM), možete upravljati korisničkim certifikatima prema datumu isteka u cijelom 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.

**Bilješka:** Budući da možete koristiti certifikat provjere potpisa da biste provjerili potpise objekta čak i kada je certifikat istekao, DCM ne osigurava podršku a 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.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ili ***OBJECTSIGNING** ili ***SYSTEM** da se otvori spremište certifikata.

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

**Srodni koncepti**

"Lokacije Liste opoziva certifikata (CRL)" na stranici 6
Lista opoziva certifikata (CRL) je datoteka koja popisuje sve nevažeće i opozvane certifikate za određenog Izdavača certifikata (CA).

"Provjera valjanosti" na stranici 10
Upravitelj digitalnih certifikata (DCM) osigurava zadatke koji dozvoljavaju provjeru valjanosti certifikata ili za provjeru valjanosti aplikacije radi provjere različitih svojstava koje moraju imati.

## Dodjela certifikata aplikacijama

Upravitelj digitalnih certifikata (DCM) dozvoljava brzu i jednostavnu dodjelu certifikata višestrukim aplikacijama. 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.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ili ***OBJECTSIGNING** ili ***SYSTEM** da se otvori spremište certifikata.

   **Bilješka:** Ako imate pitanja o tome kako popuniti specifičan obrazac koristeći DCM, izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
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) dozvoljava vam definiranje i upravljanje informacijama Popisom opoziva certifikata (CRL) za određeno Ovlaštenje certifikata (CA) kao dio obrade 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.

   **Bilješka:** Ako imate pitanja o popunjavanju specifičnog obrasca u ovom vođenom zadatku izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
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 osigurati informacije o vezi koje opisuju kako pristupiti LDAP poslužitelju. Sada treba pridružiti definiciju CRL lokacije s određenim 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).

**Bilješka:** Da biste anonimno povezali LDAP poslužitelj za CRL obradu, morate koristiti Alat za Web administraciju poslužitelja direktorija i izabrati zadatak ″Upravljanje shemom″ da biste promijenili klasu sigurnosti (koja se također naziva ″klasa pristupa″) atributa certificateRevocationList i authorityRevocationList iz ″critical″ u ″normal″ i ostavili praznim polje **Prijava razlikovnog imena** i **Lozinka**.

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.

**Srodni koncepti**

“Lokacije Liste opoziva certifikata (CRL)” na stranici 6
Lista opoziva certifikata (CRL) je datoteka koja popisuje sve nevažeće i opozvane certifikate za određenog Izdavača certifikata (CA).

**Srodne informacije**

IBM Poslužitelj direktorija za iSeries (LDAP)

Omogućavanje SSL-a na Poslužitelju direktorija

## Ključevi spremišta certifikata na IBM kriptografičkom koprocesoru

Pregledajte ove informacije da biste naučili kako koristiti instalirani koprocesor da biste osigurali sigurno spremište privatnih ključeva certifikata.

Ako ste instalirali IBM kriptografički koprocesor na sistemu, možete koristiti koprocesor da biste osigurali sigurnije spremište 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:

- Pohranjivanje privatnog ključa certifikata izravno u sam koprocesor.
- Korištenje glavnog ključa koprocesora za šifriranje privatnog ključa certifikata za spremište u posebnoj datoteci 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.

**Srodni koncepti**

"IBM kriptografički koprocesor za iSeries" na stranici 9
Kriptografički koprocesor omogućuje dokazane kriptografičke usluge, osiguravajući privatnost i integritet, za razvijanje sigurnih e-business aplikacija.

## Spremanje privatnog ključa certifikata izravno u koprocesor

Za dodatnu sigurnost u zaštiti pristupa i korištenja privatnog ključa certifikata, možete izabrati pohranjivanje 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 koji želite upotrijebiti za pohranjivanje privatnog ključa certifikata.
4. Kliknite **Nastavak**. DCM nastavlja prikazivati stranice za zadatke koje dovršavate, kao što su identifikacijske informacije za certifikat, koji kreirate ili obnavljate.

## Upotreba glavnog ključa koprocesora za šifriranje privatnog ključa

Za dodatnu sigurnost zaštite pristupa i upotrebe privatnog ključa certifikata, možete koristiti glavni ključ IBM kriptografičkog koprocesora za šifriranje privatnog ključa i pohranu ključa u posebnu datoteku ključa. 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 Web sučelju konfiguracije koprocesora 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 koji želite upotrijebiti za šifriranje privatnog ključa certifikata.
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 koji 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, koji 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 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 koji zahtijeva RA, RA potvrđuje njegov identitet. Ili RA ili podnositelj, zavisno o uspostavljenoj proceduri CA, predaje potvrđenu aplikaciju pridruženom CA-u. 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 sadrži 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 koji 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**.

**Bilješka:** PKIX standardi su navedeni u Request For Comments (RFC) 2560.

**Srodni koncepti**

“Upravljanje certifikatima od javnog Internet CA” na stranici 45
Pregledajte ove informacije da biste naučili kako upravljati certifikatima iz javnog Internet CA kreiranjem spremišta certifikata.

## Upravljanje LDAP lokacijom za certifikate korisnika

Pregledajte ove informacije da biste naučili kako konfigurirati DCM za pohranjivanje certifikata na lokaciju direktorija poslužitelja Lightweight Directory Access Protocol (LDAP) radi proširenja Mapiranja identiteta u poduzeću za rad s korisničkim certifikatima.

Po defaultu, Upravitelj digitalnih certifikata (DCM) pohranjuje korisničke certifikate koje izdaje Lokalni izdavač certifikata (CA) 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.

**Bilješka:** Ako želite da korisnik pohrani certifikat od drugog CA na LDAP lokaciju, korisnik mora dovršiti zadatak **Dodjela korisničkoga certifikata**.

EIM je @server tehnologija koja dozvoljava upravljanje korisničkim identitetima u poduzeću, uključujući i 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 za **EIM konfiguraciju** u iSeries Navigator za konfiguriranje EIM-a.
2. Kreirajte X.509 registar u EIM domeni za upotrebu za pridruživanja certifikata
3. Izaberite opciju izbornika Svojstva za Konfiguracijski folder u EIM domeni i unesite X.509 ime registra.
4. Kreirajte EIM identifikator za svakog korisnika za kojeg želite da sudjeluje u EIM-u.
5. Kreirajte ciljno pridruživanje između svakog EIM identifikatora i tog korisničkog profila u lokalnom i5/OS korisničkom registru. Koristite ime definicije EIM registra za lokalni i5/OS korisnički registar koji ste specificirali u čarobnjaku za **EIM konfiguraciju**.

   **Bilješka:** Za više informacija o konfiguriranju EIM-a pogledajte poglavlje EIM u .

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 iSeries sistemu niti ne treba biti na istom LDAP poslužitelju kojeg koristi 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.

**Bilješka:** Da biste anonimno povezali LDAP poslužitelj za CRL obradu, morate koristiti Alat za Web administraciju poslužitelja direktorija i izabrati zadatak ″Upravljanje shemom″ da biste promijenili klasu sigurnosti (koja se također naziva ″klasa pristupa″) atributa certificateRevocationList i authorityRevocationList iz ″critical″ na ″normal″ i ostavili praznim polje **Prijava razlikovnog imena** i **Lozinka**.

**Srodni zadaci**

“Digitalni certifikati i Mapiranje identiteta u poduzeću (EIM)” na stranici 32
Korištenje Mapiranja identiteta u poduzeću (EIM) i Upravitelja digitalnim certifikatima (DCM) omogućuje primjenu certifikata kao izvora operacije pregledavanja EIM mapiranja za mapiranje s certifikata na ciljni korisnički identitet udružen s istim EIM identifikatorom.

## Potpisivanje objekata

Koristite ove informacije da biste naučili kako koristiti DCM za upravljanje certifikatima koje koristite za digitalno potpisivanje objekata, radi osiguravanja njihovog integriteta.

Tri su načina koje možete koristiti za potpisivanje objekata. Možete napisati program koji poziva API Potpisivanje objekta. Možete koristiti Upravitelj digitalnih certifikata (DCM) za potpisivanje objekata. U OS/400 V5R2 ili novijem možete koristiti iSeries Navigator Management Središnju značajku za potpisivanje objekata dok ih pakirate za distribuciju na druge sisteme.

Možete koristiti certifikate kojima upravljate u DCM-u za potpisivanje svakog objekta koji 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). U OS/400 V5R2 ili novijem možete potpisati i objekte naredbe (*CMD). Ne možete potpisati objekte koji su pohranjeni na drugim sistemima.

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 API Potpisivanje objekta) 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. Pokretanje DCM-a
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** za otvaranje spremišta certifikata.

   **Bilješka:** Ako imate pitanja o tome kako popuniti specifičan obrazac koristeći DCM, izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
3. Unesite lozinku za spremište certifikata *OBJECTSIGNING 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 koji želite potpisati. Ovi zamjenski znakovi su zvjezdica (*****), koja specificira ″bilo koji 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 ID poruke (ako se desi greška za vrijeme obrađivanja objekta) ili polje datuma (koje označava datum kad se posao obradio).

9. Specificirajte 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 pregledate sadržaj direktorija za izbor datoteke za pohranjivanje rezultata posla. Prikazuje se poruka koja pokazuje da je posao poslan na izvođenje za potpis objekata. Da biste pregledali rezultate posla, pogledajte posao **QOBJSGNBAT** u dnevniku posla.

## Provjera valjanosti potpisa objekata

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

### Preduvjeti provjere potpisa

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

- Morate imati 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.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za otvaranje.

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

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 koji želite provjeriti. Ovi zamjenski znakovi su zvjezdica (*****), koja specificira ″bilo koji 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 ID poruke (ako se desi greška za vrijeme obrađivanja objekta) ili polje datuma (koje označava datum kad se posao obradio).
8. Specificirajte potpuno kvalificirano ime i stazu datoteke za korištenje u pohranjivanju rezultata posla za provjeru potpisa objekta i kliknite **Nastavak** . Ili unesite lokaciju direktorija i kliknite **Pregled** da pregledate sadržaj direktorija za izbor datoteke za pohranjivanje rezultata posla. Prikazuje se poruka koja pokazuje da je posao poslan na izvođenje za provjeru potpisa objekata. Za pregled rezultata posla, pogledajte posao **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.

**Srodni koncepti**

“Digitalni certifikati za potpisivanje objekata” na stranici 34
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.

**Srodni zadaci**

“Upravljanje certifikatima za provjeru potpisa objekata” na stranici 48
Upravitelja digitalnih certifikata (DCM) možete koristiti za upravljanje certifikatima za provjeru potpisa koje koristite za provjeru digitalnih potpisa na objektima.

## Rješavanje problema DCM-a

Pregledajte ove informacije da biste naučili kako riješiti neke uobičajene greške na koje možete naići u toku korištenja 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 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 pretražiti i Informacijski Centar i vanjske IBM Web stranice na Internetu. |

| Problem | Moguće rješenje |
| --- | --- |
| 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. |
| Primili ste poruku o greški da je lozinka istekla kada pokušate otvoriti spremište certifikata. | Morate promijeniti lozinku za spremište certifikata. Kliknite gumb **OK** da biste promijenili lozinku. |
| 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. |
| | 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 problem pojavljuje se često prilikom korištenja iSeries Navigator za dobivanje pretražitelja Netscape Communications. 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. |

| Problem | Moguće rješenje |
| --- | --- |
| 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 ima li sistem ispravne vrijednosti za UTC offset (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 ispravnog formata kada ga pokušate koristiti na sistemu. 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 podatke u direktorijima koje kreira, čak i ako te datoteke sprečavaju DCM da uspješno kreira datoteke kada to treba učiniti.<br><br>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:<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.KDB`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.RDB`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH .OLD`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POL`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.BAK`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STHBAK`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.STH`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TXT`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.BAK`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TMP`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLTMP`<br>`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLBAK`<br>`/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CACRT`<br>`/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CATMP`<br>`/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CABAK`<br>`/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CLIENT/*.USRCRT`<br><br>Trebate kreirati novo *SYSTEM spremište certifikata i sistemski certifikat nakon premještanja sljedećih datoteka:<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.BAK`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.RDB`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH.OLD`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STHBAK`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TMP`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TEMP.STH`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TMP`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.BAK`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TXT`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.SGN`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/SGN.TMP`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/SGN.BAK`<br>`/QIBM/USERDATA/ICSS/CERT/SERVER/EXPSRV.TMP`<br>`/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 daje 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 i proizvodi poslužitelja koriste korijenske certifikate iz poduzeća, uključujući, ali ne ograničavajući se na, VeriSign, kao funkciju omogućavanja SSL komunikacija — posebno, provjere 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 korijenskim certifikatima pretražitelja su dostupne na mnogim mjestima, uključujući http://home.netscape.com/security/ i http://www.verisign.com/server/cus/rootcert/webmaster.html. Besplatna spuštanja pretražitelja su dostupna s http://www.netcenter.com. |

## Rješavanje problema s HTTP poslužiteljem za iSeries

| 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. |
| Postupak registriranja instance HTTP poslužitelja kao zaštićene aplikacije treba pojašnjenje. | Na sistemu otiđite u sučelje Administracije HTTP poslužitelja da postavite konfiguraciju za 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. |

| Problem | Moguće rješenje |
| --- | --- |
| 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. Informacije o ovim API-jima možete pronaći u poglavlju API tragač u Informacijskom Centru. Možda ćete također htjeti pogledati ove validacijske liste ili API-je koji se odnose na certifikat:<br>• QsyListVldlCertificates i QSYLSTVC<br>• QsyRemoveVldlCertificate i QRMVVC<br>• QsyCheckVldlCertificate i QSYCHKVC<br>• 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 aplikaciji; na primjer, QIBM_HTTP_SERVER_MY_SERVER. Ako je instanca poslužitelja koja se ne pokreće *ADMIN poslužitelj, privremeno postavite **SSL** na onemogućeno da biste mogli 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 za i5/OS trenutno nije postavljen za registraciju certifikata pomoću SSL-a i provjere autentičnosti klijenta na instanci sigurnog Administrativnog poslužitelja. Ako nijedan od navedenih savjeta za otklanjanje problema ne radi, obratite se sistemskom administratoru i prijavite problem.

Da **Dodijelite korisnički certifikat** morate se spojiti na Upravitelja digitalnih certifikata (DCM) koristeći SSL sesiju. Ako ne koristite SSL kad 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.

**Srodni zadaci**

"Dodjela certifikata korisnika" na stranici 41
Možete dodijeliti korisnički certifikat koji posjedujete i5/OS 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.

## Povezane informacije za DCM

Pregledajte ovu stranicu da biste pronašli veze do drugih resursa gdje ćete naučiti više o digitalnim certifikatima, infrastrukturi javnog ključa, Upravitelju digitalnih certifikata i drugim srodnim informacijama.

Kako je upotreba digitalnih certifikata postala prevladavajuća, i informacijski resursi su postali dostupni. Ovdje je mali popis resursa koji možete pregledati da naučite više o digitalnim certifikatima i kako ih možete koristiti za poboljšanje sigurnosne politike sistema:

- **VeriSign Help Desk Web site** VeriSign Web stranica osigurava opsežnu knjižnicu o poglavljima digitalnih certifikata, kao i velik broj drugih tema o Internet sigurnosti.
- **IBM eServer iSeries žičana mrežna sigurnost: OS/400 V5R1 DCM i kriptografička poboljšanja SG24-6168**

  Ovaj IBM Redbook se usredotočuje na OS/400 V5R1 poboljšanja mrežne sigurnosti. Redbook pokriva mnoga poglavlja uključujući i kako koristiti iSeries sposobnosti potpisivanja objekta, Upravitelja digitalnih certifikata (DCM), podršku 4758 kriptografičkog koprocesora za SSL i tako dalje.

- **AS/400 Internet sigurnost: Razvijanje infrastrukture digitalnog certifikata (SG24-5659)** Ovaj redbook opisuje što možete napraviti s digitalnim certifikatima na iSeries poslužitelju. Objašnjava se kako postaviti različite poslužitelje i klijente za korištenje certifikata. Nadalje, osigurava informacije i primjer koda kako koristiti OS/400 API-je za upravljanje i korištenje digitalnih certifikata u korisničkim aplikacijama.

- **RFC indeks pretraživanja** Ova Web stranica sadrži spremište koje možete pretraživati za Request for Comments (RFC-ove). 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 dodatke o kojima se raspravlja u ovom dokumentu u drugim zemljama. Za informacije o proizvodima i uslugama koji su trenutno dostupni u vašem području kontaktirajte vašeg lokalnog IBM predstavnika. Bilo koje upućivanje na neki 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 molbe za patente koje su još u toku, a koje pokrivaju predmet o kojem se govori u ovom dokumentu. Posjedovanje ovog dokumenta vam ne daje nikakvo pravo na te patente. Možete poslati upit za licence, u pismenom obliku, na:

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

Za upite o licenci u vezi s dvobajtnim (DBCS) informacijama, kontaktirajte IBM odjel intelektualnog vlasništva u vašoj zemlji ili pošaljite upite, u pisanom obliku na adresu:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, 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 sve informacije koje vi dobavite, na bilo koji način za koji smatra da je prikladan i bez ikakvih 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 YBWA
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 sav licencni materijal koji je za njega dostupan IBM isporučuje pod uvjetima IBM Ugovora s korisnicima, IBM Internacionalnog ugovora o licenci za programe, IBM Ugovora o licenci za strojni kod 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.

Sve pokazane IBM cijene su IBM-ove predložene maloprodajne cijene, trenutne su i podložne promjeni bez obavijesti. Cijene kod zastupnika se mogu razlikovati.

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.

AUTORSKO PRAVO LICENCE:

Ove informacije sadrže primjere aplikacijskih programa u izvornom jeziku, koji ilustriraju tehnike programiranja na različitim operativnim platformama. Možete kopirati, modificirati i distribuirati te primjere programa u bilo kojem obliku, bez plaćanja IBM-u, za svrhe razvoja, upotrebe, marketinga ili distribucije aplikacijskih programa, u skladu sa sučeljem programiranja aplikacija za operativnu platformu za koju su primjeri programa napisani. Ti primjeri nisu bili temeljito testirani u svim uvjetima. IBM, zbog toga, ne može jamčiti ili potvrditi pouzdanost, upotrebljivost ili funkcioniranje tih programa.

Svaka kopija ili bilo koji dio tih primjera programa ili iz njih izvedenih radova, mora uključivati sljedeću napomenu o autorskom pravu:

© (ime vašeg poduzeća) (godina). Dijelovi ovog koda su izvedeni iz IBM Corp. primjera programa. © Autorsko pravo IBM Corp. _unesite godinu ili godine_. Sva prava pridržana.

Ako ove informacije gledate na nepostojanoj kopiji, fotografije i ilustracije u boji se možda neće vidjeti.

## Zaštitni znaci

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

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

| Lotus
| Net.Data
| OS/400

Microsoft, Windows 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

Dozvole za upotrebu ovih publikacija se dodjeljuju prema sljedećim terminima i uvjetima.

**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 izvedena djela iz ovih publikacija ili bilo kojeg njihovog dijela, bez izričite suglasnosti IBM-a.

**Komercijalna upotreba:** Možete reproducirati, distribuirati i prikazivati ove publikacije samo unutar vašeg poduzeća uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete raditi izvedena dijela iz ovih publikacija ili kopirati, distribuirati ili prikazivati te publikacije ili bilo koji njihov dio izvan vašeg poduzeća, bez izričite suglasnosti od strane IBM-a.

Osim kako je izričito dodijeljeno u ovoj dozvoli, nisu dane nikakve dozvole, licence ili prava, niti izričita niti posredna, na publikacije ili bilo koje podatke, softver ili bilo koje drugo intelektualno vlasništvo sadržano unutar.

IBM rezervira pravo da bilo kad, po vlastitom nahođenju, povuče ovdje dodijeljene dozvole, ako je upotreba publikacija 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, POSREDNA JAMSTVA PROĐE NA TRŽIŠTU, NEKRŠENJA I PRIKLADNOSTI ZA ODREĐENU SVRHU.

Tiskano u Hrvatskoj