System i

Sigurnost
Upravitelj digitalnih certifikata

Verzija 6 Izdanje 1

System i

Sigurnost
Upravitelj digitalnih certifikata

Verzija 6 Izdanje 1

Napomena

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene”, na stranici 85.

Ovo izdanje se primjenjuje na verziju 6, izdanje 1, modifikaciju 0 za IBM i5/OS (broj proizvoda 5761-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

Upravitelj digitalnih certifikata (DCM) omogućuje upravljanje digitalnim certifikatima na vašoj mreži i korištenje sloja sigurnih utičnica (SSL) za omogućivanje sigurnih komunikacija za mnoge aplikacije.

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. Digitalni su certifikati, na primjer, od ključne važnosti za konfiguriranje i korištenje SSL-a. 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 System i platforme i aplikacije, npr. FTP, Telnet, HTTP poslužitelj, nude podršku za SSL da bi osigurali privatnost podataka.

System i 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. Digitalne certifikate i njima pridružene sigurnosne ključeve možete koristiti i za potpisivanje objekata. Potpisivanje objekata vam dozvoljava da otkrijete promjene ili moguće zlonamjerne promjene sadržaja objekta provjeravanjem potpisa na objektima radi osiguranja njihove cjelovitosti.

Lako je iskoristi System i podršku za certifikate kada koristite Upravitelj digitalnih certifikata, besplatnu funkciju, za središnje upravljanje certifikatima za aplikacije. DCM vam dopušta da upravljate certifikatima koje dobivate od svakog Izdavača certifikata (CA). Također, možete koristiti DCM za kreiranje i upravljanje vlastitim 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:

Srodne informacije

Sloj sigurnih utičnica (SSL)

Potpisivanje objekata i provjera potpisa

Što je novo u verziji V6R1

Pročitajte nove ili znatnije izmijenjene informacije o Upravitelju digitalnih certifikata (DCM) za i5/OS.

Nove informacije o upravljanju certifikatima putem isteka

Te nove informacije objašnjavaju kako upravljati poslužiteljskim i klijentskim certifikatima, certifikatima za potpisivanje objekata, certifikatima izdavača certifikata i korisničkim certifikatima prema datumu isteka na lokalnom sistemu.

- “Upravljanje certifikatima putem isteka” na stranici 67

Nove informacije o pokretanju DCM-a

Te nove informacije detaljno objašnjavaju pokretanje DCM-a na vašem sistemu. Novi proces obuhvaća korištenje novog sučelja Web konzole na portu 2001, zvanog IBM Systems Director Navigator za i5/OS .

- “Pokretanje Upravitelja digitalnih certifikata” na stranici 40

Kako vidjeti što je novo ili promijenjeno

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

- Sliku  da označi gdje nova ili promijenjena informacija počinje.
- Sliku  da označi gdje nova ili promijenjena informacija završava.

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

PDF datoteka za DCM

Možete pogledati i ispisati ove informacije u PDF obliku.

Da biste pogledali i spustili PDF verziju ove teme, izaberite Upravitelj digitalnih certifikata  (otprilike 1100 kB).

Spremanje PDF datoteka

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

1. Desno kliknite vezu na PDF u pretražitelju.
2. Kliknite opciju koja sprema lokalno PDF.
3. Pretražite do direktorija u koji želite spremiti PDF.
4. Kliknite **Save**.

Učitavanje Adobe Acrobat Readera

Trebate Adobe Acrobat Reader za pregled i ispis tih PDF-ova. Kopiju možete spustiti s Web stranica Adobe (www.adobe.com/products/acrobat/readstep.html)  .

DCM koncepti

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 kriptografskim 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.

Lokalni CA koji osigurava Upravitelj digitalnih certifikata (DCM), na primjer, omogućuje samo korištenje proširenja certifikata Subject Alternative Name (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 System i Virtualne privatne mreže (VPN), morate osigurati informacije za njihova proširenja.

Srodni koncepti

"Razlikovno ime"
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.

Obnavljanje certifikata

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

Ako upotrijebite lokalni CA za potpisivanje obnovljenog certifikata, DCM će upotrijebiti unesene informacije za kreiranje novog certifikata u trenutnom spremištu certifikata i zadržat će 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

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.

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.

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:

- IP adresa verzije 4 ili 6
- Potpuno kvalificirano ime domene
- Adresa e-pošte

Srodni koncepti

"Proširenja certifikata" na stranici 2
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" na stranici 5
Izdavač certifikata (CA) je pouzdani centralni administrativan entitet koji može izdati digitalne certifikate korisnicima i poslužiteljima.

"Kriptografija" na stranici 8
Dijeljeni i javni ključevi dva su tipa kriptografskih funkcija pomoću kojih digitalni certifikati pružaju sigurnost.

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

Izdavač certifikata

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 upravljanje vlastitim lokalnim CA za izdavanje privatnih certifikata sistemima i korisnicima. Kada lokalni CA izda korisnički certifikat, DCM automatski pridružuje certifikat korisnikovom System i korisničkom profilu ili nekom drugom korisničkom identitetu. 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 pomoću Upravitelja digitalnih certifikata (DCM) kreirate lokalni Izdavač certifikata (CA), možete specificirati podatke o politici za lokalni CA. Podaci o politici lokalnog CA opisuju njegove povlastice za potpisivanje. Podaci o politici određuju:

- Može li lokalni CA izdavati i potpisivati korisničke certifikate.
- Koliko dugo važe certifikati koje izda lokalni CA.

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

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

CA-ovi povremeno ažuriraju svoje CRL-ove i čine ih dostupnim 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 Identifiera (URI).

Upravitelj digitalnih certifikata (DCM) dozvoljava definiranje i upravljanje lokacijskim informacijama CRL-a radi osiguranja strože provjere autentičnosti certifikata koje koristite ili prihvaćate od drugih. Definicija CRL lokacije opisuje lokaciju od i informacije o pristupu za poslužitelj Lightweight Directory Access Protocola (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 procesa koji bi za potrebe provjere autentičnosti certifikata mogli obavljati CRL: Virtual Private Networking (VPN) veze, Internet Key Exchange (IKE) poslužitelj, aplikacije s podrškom za Sloj sigurnih utičnica (SSL)i proces za potpisivanje 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 68
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 69
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 kriptografski 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 to spremište certifikata za pohranu certifikata lokalnog CA i njegova privatnog ključa ako ste kreirali lokalni CA. Certifikate iz tog spremišta certifikata možete koristiti za potpisivanje certifikata koje izdajete pomoću lokalnog CA. Kada lokalni CA izda certifikat, DCM smješta kopiju certifikata CA (bez privatnog ključa) u odgovarajuće spremište certifikata (npr. *SYSTEM) za potrebe 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). System i aplikacije (i mnoge druge aplikacije za razvijače softvera) napisane su samo za korištenje certifikata u spremištu certifikata *SYSTEM. Kada pomoću DCM-a kreirate lokalni CA, DCM za vrijeme tog procesa kreira to spremište certifikata. 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 pomoću DCM-a kreirate lokalni CA, DCM za vrijeme tog procesa kreira to spremište certifikata. 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 kriptografski 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), spremišta certifikata *SYSTEM, *OBJECTSIGNING i *SIGNATUREVERIFICATION moraju se nalaziti na određenim stazama u integriranom sistemu datoteka. Other System spremišta certifikata mogu se nalaziti bilo gdje u integriranom sistemu datoteka.

Srodni koncepti

“Tipovi digitalnih certifikata” na stranici 31
Kada koristite Upravitelj digitalnih certifikata (DCM) za upravljanje certifikatima, DCM organizira i pohranjuje te certifikate i pripadajuće privatne ključeve u spremište certifikata utemeljeno na tipu certifikata.

Kriptografija

Dijeljeni i javni ključevi dva su tipa kriptografskih funkcija pomoću kojih digitalni certifikati pružaju sigurnost.

Kriptografija je znanost o čuvanju podataka na sigurnom. Kriptografija vam omogućuje pohranu informacija i komunikaciju s drugima uz istodobno onemogućivanje razumijevanja pohranjenih informacija ili pak komunikacije neželjenim osobama. 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” na stranici 9
  Sloj sigurnih utičnica standard je za šifriranje sesija između klijenata i poslužitelja.

IBM kriptografski koprocesor za System i

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

IBM kriptografski koprocesor za platformu System i vašem sistemu dodaje sposobnost iznimno sigurne kriptografske obrade. Ako imate instaliran kriptografski koprocesor u stanju Varied on za vaš sistem, možete koristiti kriptografski koprocesor da omogućite sigurniju pohranu ključeva za vaše privatne ključeve za certifikat.

Možete koristiti kriptografski koprocesor za pohranjivanje privatnog ključa certifikata poslužitelja ili klijenta i za certifikat lokalnog Izdavača certifikata (CA). Ipak, ne možete koristiti kriptografski 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 kriptografski koprocesor ili možete koristiti glavni ključ kriptografskog 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 kriptografskog 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

"Pohrana ključeva certifikata na IBM kriptografskom koprocesoru" na stranici 70
Ako ste na sistem instalirali IBM kriptografski koprocesor, možete se poslužiti njime za sigurniju pohranu privatnog ključa certifikata. Koprocesor možete koristiti za pohranjivanje privatnog ključa za poslužiteljski certifikat, klijentski certifikat ili certifikat lokalnog izdavača certifikata (CA).

Sloj sigurnih utičnica

Sloj sigurnih utičnica standard je 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
Dijeljeni i javni ključevi dva su tipa kriptografskih funkcija pomoću kojih digitalni certifikati pružaju sigurnost.

"Tipovi digitalnih certifikata" na stranici 31
Kada koristite Upravitelj digitalnih certifikata (DCM) za upravljanje certifikatima, DCM organizira i pohranjuje te certifikate i pripadajuće privatne ključeve u spremište certifikata utemeljeno na tipu certifikata.

Definicije aplikacija

Upravitelj digitalnih certifikata (DCM) omogućuje upravljanje aplikacijskim definicijama koje će biti kompatibilne sa SSL konfiguracijama i potpisivanjem objekata.

Putem DCM-a možete upravljati dvama tipovima aplikacijskim definicija:

- 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 System i 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 64
Upravitelj digitalnih certifikata (DCM) omogućuje kreiranje aplikacijske definicije i upravljanje dodjelom certifikata određene aplikacije. Možete definirati i popis pouzdanih CA-ova koje će aplikacije koristiti kao temelj za prihvaćanje certifikata za provjeru autentičnosti klijenata.

Srodni zadaci

“Kreiranje definicije aplikacije” na stranici 64
U Upravitelju digitalnih certifikata možete kreirati sljedeća dva tipa definicija aplikacija i raditi s njima: poslužiteljske ili klijentske aplikacije koje koriste SSL i definicije aplikacija koje služe za potpisivanje objekata.

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 68
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.

Scenariji: DCM

Ovi scenariji ilustriraju tipične sheme implementacije certifikata koje će vam pomoći pri planiranju vlastite implementacije certifikata koja je dio vaše politike sigurnosti System i. Svaki scenarij ujedno sadržava i sve potrebne konfiguracijske zadatke koje morate obaviti da biste implementirali scenarij.

Upravitelj digitalnih certifikata (DCM) omogućuje korištenje certifikata radi poboljšanja politike sigurnosti na više 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 System i 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: korištenje certifikata za vanjsku 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 unesene 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

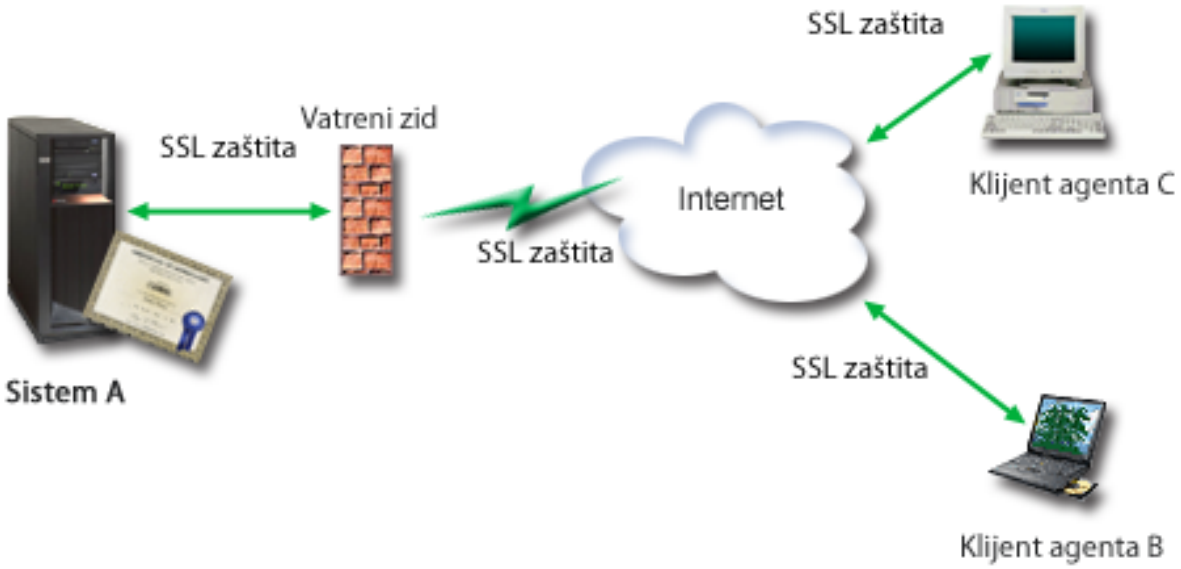
U ovom scenariju, MyCo, Inc. želi koristiti digitalne certifikate da zaštiti informacije o izračunu omjera koje njihova aplikacija omogućuje ovlaštenim javnim korisnicima. Poduzeće također želi sigurniju metodu provjere autentičnosti onih korisnika kojima je dozvoljen pristup ovoj aplikaciji kada je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

- System A je poslužitelj koji služi kao glavno računalo tvrtkine aplikacije za izračun stopa.
- System A koristi i5/OS verzije 5 izdanje 4 (V5R4) ili noviji.
- System A ima instaliran i konfiguriran Upravitelj digitalnih certifikata i IBM HTTP poslužitelj za i5/OS.
- System A pokreće aplikaciju za izračun stopa koja je konfigurirana na sljedeći način:
  - Zahtijeva SSL način.
  - Koristi javni certifikat od dobro poznatog Izdavača certifikata (CA) za vlastito ovlaštenje za inicijalizaciju SSL sesije.
  - Zahtijeva provjeru autentičnosti korisnika pomoću korisničkog imena i lozinke.
- System A predstavlja svoj certifikat da bi započeo SSL sesiju kada klijenti B i C pristupe aplikaciji za izračun stopa.
- Nakon inicijalizacije SSL sesije System A od klijenata B i C zahtijeva unos važećeg korisničkog imena i lozinke prije nego im dopusti pristup aplikaciji za izračun stopa.

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 stopa na Systemu A, koji predstavlja svoj certifikat njihovu klijentskom softveru da bi potvrdio svoj identitet i započeo SSL sesiju.
- Klijentski softver na klijentima B i C konfiguriran je da prihvati certifikat sa Systema A u svrhu inicijalizacije SSL sesije.
- Nakon početka SSL sesije klijenti A i B moraju unijeti važeće ime korisnika i lozinku da bi im System A dodijelio pristup aplikaciji.

Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:

- Aplikacija za izračun stopa na Systemu A generička je aplikacija koju je moguće konfigurirati za upotrebu SSL-a. Većina aplikacija, zajedno s mnogim System i 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.
- System A ispunjava “Zahtjevi za postavljanje DCM-a” na stranici 30 za instaliranje i korištenje Upravitelja digitalnih certifikata (DCM)
- Do sada nitko nije konfigurirao niti koristio DCM na Systemu A.
- Svatko tko koristi DCM za izvođenje zadataka u ovom scenariju mora imati *SECADM i *ALLOBJ posebna ovlaštenja za svoj korisnički profil.
- System A nema instaliran IBM kriptografski koprocesor.

Konfiguracijski zadaci

Srodni zadaci

“Pokretanje Upravitelja digitalnih certifikata” na stranici 40
Da biste mogli koristiti funkcije Upravitelja digitalnih certifikata (DCM), najprije ga morate pokrenuti na svom sistemu.

Popunjavanje radnih tablica 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**
Koristi li se na vašem sistemu i5/OS V5R4 ili noviji?	Da
Imate li instaliran Upravitelj digitalnih certifikata?	Da
Je li na vašem sistemu instaliran IBM HTTP poslužitelj za i5/OS i pokrenuta administrativna instanca?	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

Radna tablica planiranja za System A	**Odgovori**
Hoćete li imati vlastiti lokalni CA ili ćete certifikate nabavljati od javnog CA?	Postizanje certifikata s javnog CA

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

Radna tablica planiranja za System A	**Odgovori**
Ima li na Systemu A aplikacija koje želite omogućiti za SSL?	Da
Koje razlikovno ime ćete koristiti za zahtjev za potpisivanjem certifikata (CSR) za čije kreiranje koristite DCM? • **Veličina ključa**: određuje snagu kriptografskih ključeva za certifikat. • **Oznaka certifikata**: identificira certifikat s jedinstvenim nizom znakova. • **Uobičajeno ime**: identificira vlasnika certifikata, kao što je osoba, entitet ili aplikacija; dio DN Subjekta za certifikat. • **Jedinica organizacije**: identificira organizacijsku sekciju ili područje za aplikaciju koja će koristiti certifikat. • **Ime organizacije**: identificira vaše poduzeće ili odjelni dio za aplikaciju koja će koristiti certifikat. • **Lokacija ili grad**: identificira vaš grad ili označavanje lokacija za vašu organizaciju. • **Država ili pokrajina**: identificira državu ili pokrajinu u kojoj ćete koristiti ovaj certifikat. • **Zemlja ili regija**: identificira, s dvoslovnom oznakom, zemlju ili regiju u kojoj ćete koristiti ovaj certifikat.	**Veličina ključa**: 1024**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 poslužiteljskim ili klijentskim certifikatom

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a.
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 tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite tipku 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** da se prikaže obrazac koji omogućuje pružanje identifikacijskih informacija za novi certifikat.
6. Dovršite obrazac i kliknite **Nastavak** da se prikaže stranica potvrde. 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 napuštate ovu stranicu, podaci se gube i ne možete ih obnoviti.
8. Kad napuštate 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 aplikacija 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, npr. IBM HTTP poslužitelj za i5/OS generiraju jedinstven ID aplikacije i registriraju ga pri Upravitelju 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. Kada dovršite SSL konfiguraciju za vašu aplikaciju, možete konfigurirati potpisani javni certifikat za aplikaciju tako da može započinjati SSL sesije.

Srodne informacije

Sigurnost aplikacija sa SSL-om

Importiranje i dodjela potpisanog javnog 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. Pogledajte Pokretanje DCM-a.
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. Kad se navigacijski izbornik osvježi, izaberite **Upravljanje certifikatima** da se prikaže popis zadataka.
5. Iz popisa zadataka izaberite **Import certifikata** da započnete postupak importiranja potpisanog certifikata u *SYSTEM spremište certifikata.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite tipku 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**. Prikazat će se stranica s potvrdnom porukom ili poruka o greški ako se desio 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. Proučite dokumentaciju koju ste dobili uz aplikaciju da biste saznali trebate li ponovno pokrenuti aplikaciju i druge specifične informacije o pokretanju aplikacije u SSL načinu.

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

(Neobvezno): Definiranje popisa pouzdanih CA-ova za aplikaciju koja 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. Pogledajte Pokretanje DCM-a.
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. Kad se navigacijski izbornik osvježi, izaberite **Upravljanje certifikatima** da se prikaže popis zadataka.
5. Iz popisa zadataka izaberite **Postavi CA status** da prikažete listu CA certifikata.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite tipku 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: korištenje 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.

Stoga ste odlučili postaviti privatni, lokalni Izdavač certifikata (CA) i izdavati certifikate svim zaposlenicima koji će svoje certifikate povezati sa svojim System i 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 System i 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 System i 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.

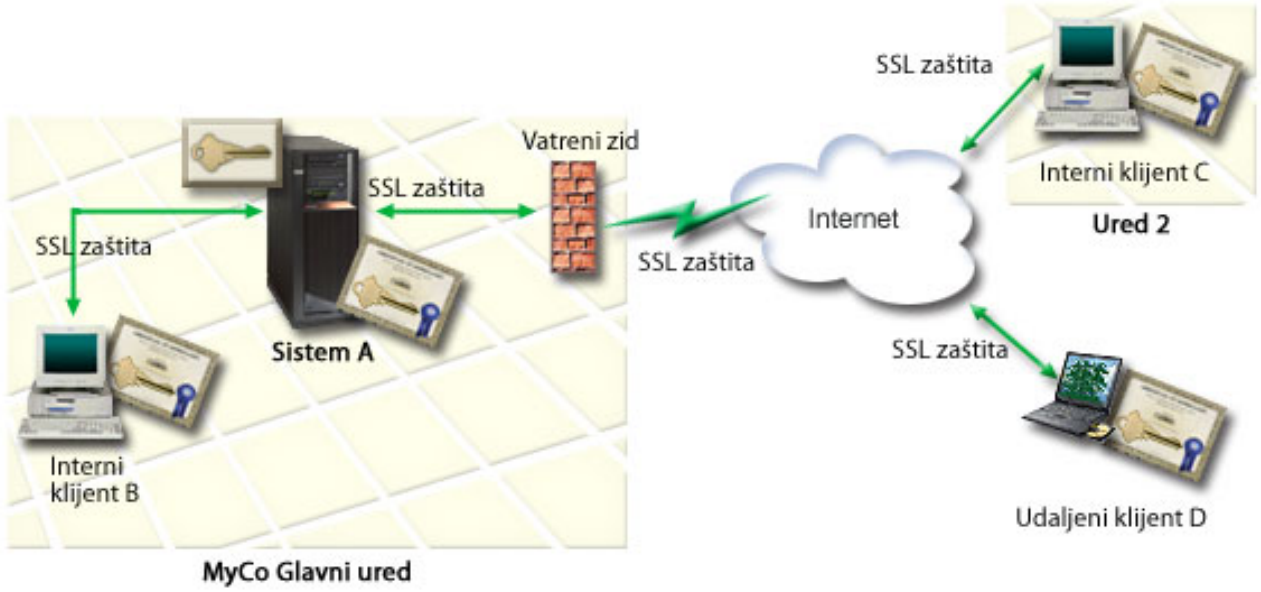
Ciljevi ovog scenarija su sljedeći:

- Web stranica internih ljudskih resursa poduzeća mora koristiti SSL da zaštiti privatnost podataka koje omogućuje korisnicima.

- SSL konfiguraciju treba obaviti pomoću privatnih certifikata 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 – System A

- System A je poslužitelj koji služi kao glavno računalo tvrtkine aplikacije za izračun stopa.
- System A koristi i5/OS verzije 5 izdanje 4 (V5R4) ili noviji.
- System A ima instaliran i konfiguriran Upravitelj digitalnih certifikata i IBM HTTP poslužitelj za i5/OS.
- System A pokreće aplikaciju za izračun stopa koja je konfigurirana na sljedeći način:
  - Zahtijeva SSL način.
  - Koristi javni certifikat od dobro poznatog Izdavača certifikata (CA) za vlastito ovlaštenje za inicijalizaciju SSL sesije.
  - Zahtijeva provjeru autentičnosti korisnika pomoću korisničkog imena i lozinke.
- System A predstavlja svoj certifikat da bi započeo SSL sesiju kada klijenti B i C pristupe aplikaciji za izračun stopa.
- Nakon inicijalizacije SSL sesije System A od klijenata B i C zahtijeva unos važećeg korisničkog imena i lozinke prije nego im dopusti pristup aplikaciji za izračun stopa.

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 stopa na Systemu A, koji predstavlja svoj certifikat njihovu klijentskom softveru da bi potvrdio svoj identitet i započeo SSL sesiju.
- Klijentski softver na klijentima B i C konfiguriran je da prihvati certifikat sa Systema A u svrhu inicijalizacije SSL sesije.

- Nakon početka SSL sesije klijenti A i B moraju unijeti važeće ime korisnika i lozinku da bi im System A dodijelio pristup aplikaciji.

Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:

- IBM HTTP poslužitelj za i5/OS (pogonjen Apacheom) koristi aplikaciju za ljudske resurse na Systemu A. Ovaj scenarij ne sadrži specifične upute za konfiguriranje aplikacije za izračun stopa za upotrebu SSL-a. 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 sadržava upute za korištenje DCM-a za konfiguriranje preduvjeta za upravljanje certifikatima za ovaj scenarij. Međutim, ovaj scenarij ne daje određene konfiguracijske korake za konfiguriranje provjere autentičnosti certifikata klijenta za HTTP poslužitelj.
- HTTP poslužitelj za ljudske resurse na Systemu A već koristi provjeru autentičnosti putem lozinke.
- System A ispunjava preduvjete za instaliranje i korištenje Upravitelja digitalnih certifikata (DCM).
- Do sada nitko nije konfigurirao niti koristio DCM na Systemu A.
- Svatko tko koristi DCM za izvođenje zadataka u ovom scenariju mora imati *SECADM i *ALLOBJ posebna ovlaštenja za svoj korisnički profil.
- System A nema instaliran IBM kriptografski koprocesor.

Konfiguracijski zadaci

Popunjavanje radnih tablica 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**
Koristi li se na vašem sistemu i5/OS V5R4 ili noviji?	Da
Imate li instaliran Upravitelj digitalnih certifikata?	Da
Je li na vašem sistemu instaliran IBM HTTP poslužitelj za i5/OS i pokrenuta administrativna poslužiteljska instanca?	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 System A	**Odgovori**
Hoćete li imati vlastiti lokalni CA ili ćete certifikate nabavljati od javnog CA?	Kreiraj lokalni CA za izdavanje certifikata
Ima li na Systemu A aplikacija koje želite omogućiti za SSL?	Da

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

Radna tablica planiranja za System A	Odgovori
Koje ćete razlikovno ime koristiti za lokalni CA? • **Veličina ključa**: određuje snagu kriptografskih ključeva za certifikat. • **Ime Izdavača certifikata (CA)**: identificira CA i postaje uobičajeno ime za CA certifikat i DN Izdavatelja za certifikate koje CA izdaje. • **Jedinica organizacije**: identificira organizacijsku sekciju ili područje za aplikaciju koja će koristiti certifikat. • **Ime organizacije**: identificira vaše poduzeće ili odjelni dio za aplikaciju koja će koristiti certifikat. • **Lokacija ili grad**: identificira vaš grad ili označavanje lokacija za vašu organizaciju. • **Država ili pokrajina**: identificira državu ili pokrajinu u kojoj ćete koristiti ovaj certifikat. • **Zemlja ili regija**: identificira, s dvoslovnom oznakom, zemlju ili regiju u kojoj ćete koristiti ovaj certifikat. • **Period valjanosti za Izdavača certifikata**: specificira broj dana za koji je certifikat Izdavača certifikata važeći	**Veličina ključa**: 1024**Ime izdavača certifikata (CA)**: Myco_CA@myco.com**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 o politici za lokalni CA tako da smije izdavati korisničke certifikate za provjeru autentičnosti klijenta?	Da
Koje ćete razlikovno ime koristiti za poslužiteljski certifikat koji izdaje lokalni CA? • **Veličina ključa**: određuje snagu kriptografskih ključeva za certifikat. • **Oznaka certifikata**: identificira certifikat s jedinstvenim nizom znakova. • **Uobičajeno ime**: identificira vlasnika certifikata, kao što je osoba, entitet ili aplikacija; dio DN Subjekta za certifikat. • **Jedinica organizacije**: identificira organizacijsku sekciju ili područje za aplikaciju koja će koristiti certifikat. • **Ime organizacije**: identificira vaše poduzeće ili odjelni dio za aplikaciju koja će koristiti certifikat. • **Lokacija ili grad**: identificira vaš grad ili označavanje lokacija za vašu organizaciju. • **Država ili pokrajina**: identificira državu ili pokrajinu u kojoj ćete koristiti ovaj certifikat. • **Zemlja ili regija**: identificira, s dvoslovnom oznakom, zemlju ili regiju u kojoj ćete koristiti ovaj certifikat.	**Veličina ključa**: 1024**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 Servera za ljudske resurse za korištenje SSL-a

SSL konfiguracija HTTP Servera za ljudske resurse (pogoni ga Apache) na Systemu A zahtijeva niz zadataka koji ovise o trenutnoj konfiguraciji vašeg poslužitelja.

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 konfigurirani 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.

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.

Srodne informacije

IBM HTTP poslužitelj za i5/OS

Kreiranje i održavanje lokalnog 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 temelju ciljeva ovog scenarija odlučili ste kreirati i održavati lokalni Izdavač certifikata (CA) za izdavanje certifikata poslužitelju.

Kada koristite Upravitelj digitalnih certifikata (DCM) za kreiranje lokalnog CA, prolazite vođeni proces kojim se osigurava da ćete konfigurirati sve što je potrebno da omogućite SSL za svoju aplikaciju. To obuhvaća dodjelu certifikata koji je izdao vaš lokalni CA aplikaciji Web poslužitelja. Morate i dodati lokalni CA na popis pouzdanih CA-ova aplikacije za Web poslužitelj. Ako se lokalni CA nalazi na popisu pouzdanih CA-ova aplikacije, aplikacija će prepoznati i potvrditi identitet korisnika koji se predstavljaju certifikatima koje je izdao lokalni CA.

Da biste pomoću Upravitelja digitalnih certifikata (DCM) kreirali i održavali lokalni CA i izdali certifikat aplikaciji svog poslužitelja za ljudske resurse, učinite sljedeće:

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a.
2. U navigacijskom okviru DCM-a izaberite **Kreiraj izdavača certifikata (CA)** da biste prikazali nizove obrazaca. Sljedeći će vas obrasci provesti kroz proces kreiranja lokalnog CA i obavljanja drugih zadataka potrebnih za početak korištenja digitalnih certifikata za SSL, potpisivanje objekata i provjeru potpisa.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite tipku upitnik (**?**) na vrhu stranice za pristup online pomoći.
3. Dovršite obrasce za ovaj vođeni zadatak. Za vrijeme korištenja tih obrazaca za obavljanje zadataka potrebnih za postavljanje funkcionalnog lokalnog Izdavača certifikata (CA) morat ćete učiniti sljedeće:
   a. Navesti identifikacijske podatke za lokalni CA.
   b. Instalirati certifikat lokalnog CA na svoje osobno računalo ili pretražitelj, tako da softver može prepoznati lokalni CA i provjeriti valjanost certifikata koje izdaje taj CA.
   c. Izabrati podatke za politiku lokalnog CA.

      Bilješka: Svakako omogućiti izdavanje korisničkih certifikata na lokalnom CA.
   d. Upotrijebiti novi lokalni CA za izdavanje poslužiteljskog ili klijentskog certifikata koji aplikacije mogu koristiti za SSL veze.
   e. Izabrati aplikacije koje mogu koristiti poslužiteljski ili klijentski certifikat za SSL veze.

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

f. Koristite novi Lokalni CA da izdate certifikat poslužitelja ili klijenta koje aplikacija može 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 za potpisivanje objekata, 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. Izabrati aplikacije koje će smatrati lokalni CA pouzdanim.

Bilješka: Svakako izabrati ID aplikacije za svoj HTTP Server za ljudske resurse, npr. QIBM_HTTP_SERVER_MYCOTEST, kao jednu od aplikacija koje lokalni CA smatraju pouzdanim.

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 za ljudske resurse

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. Otvorite Web pretražitelj i unesite http://your_system_name:2001 da biste učitali IBM Systems Director Navigator za i5/OS pozdravnu stranicu.
3. Na pozdravnoj stranici kliknite vezu na **i5/OS stranicu sa zadacima**.
4. Izaberite **IBM Web administracija za i5/OS**.
5. 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.
6. Izaberite odgovarajući poslužitelj s liste i kliknite **Upravljanje detaljima**.
7. U navigacijskom okviru izaberite **Sigurnost**.
8. Izaberite karticu **Provjera autentičnosti** na obrascu.
9. Izaberite **Koristi i5/OS profil klijenta**.
10. U polju **Ime provjere autentičnosti ili područje**, specificirajte ime za područje provjere autentičnosti.
11. Izaberite Omogućeno za polje **Zahtjevi obrade upotrebom ovlaštenja klijenta** i kliknite **Primijeni**.
12. Izaberite karticu **Kontroliraj pristup** na obrascu.
13. Izaberite **Svi korisnici provjerene autentičnosti (važeće korisničko ime i lozinka)** i kliknite **Primijeni**.
14. U obrascu izaberite karticu **SSL s provjerom autentičnosti certifikata**.
15. Osigurajte da je Omogućeno izabrana vrijednost u **SSL** polju.
16. U polju **Ime aplikacije za certifikat poslužitelja**, osigurajte da je specificirana ispravna vrijednost, na primjer, QIBM_HTTP_SERVER_MYCOTEST.
17. Izaberite **Prihvati certifikat klijenta ako je dostupan prije povezivanja**. Kliknite **OK**.

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

Srodne informacije

IBM HTTP poslužitelj za i5/OS

Pokretanje Web poslužitelja za ljudske resurse 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 System i Navigator proširite svoj **sistem → Mreža → Poslužitelji → TCP/IP → HTTP administracija**
2. Kliknite **Pokreni** da pokrenete sučelje Administracija HTTP Poslužitelja.
3. Kliknite karticu **Upravljaj** da pogledate listu svih konfiguriranih HTTP poslužitelja.
4. Izaberite odgovarajući poslužitelj s liste i kliknite **Zaustavi** ako je poslužitelj u izvođenju.
5. Kliknite **Pokreni** da ponovno pokrenete poslužitelj. Uputite se na online pomoć za više informacija o parametrima pokretanja.

Da bi korisnici mogli pristupiti Web aplikaciji za ljudske resurse, najprije moraju instalirati kopiju certifikata lokalnog CA u svoj pretražitelj.

Srodne informacije

Pregled HTTP poslužitelja u Informacijskom centru

Instaliranje kopije certifikata lokalnog CA u 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 predstavi certifikat od privatnog lokalnog CA, svaki korisnik mora instalirati kopiju certifikata lokalnog CA putem Upravitelja digitalnih certifikata (DCM).

Svaki korisnik (klijenti B, C i D) mora učiniti sljedeće da bi dobio kopiju certifikata lokalnog CA:

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a.
2. U navigacijskom okviru izaberite **Instaliraj certifikat lokalnog CA na PC** da bi se prikazala stranica na kojoj možete spustiti certifikat lokalnog CA u pretražitelj ili ga pohraniti u datoteku na sistemu.
3. Izaberite opciju za instaliranje certifikata. Tom se opcijom certifikat lokalnog CA učitava u pretražitelj kao pouzdano ishodište. 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. To znači da moraju pribaviti korisnički certifikat od lokalnog CA.

Traženje certifikata iz lokalnog CA

U ranijim koracima konfigurirali ste Web poslužitelj za ljudske resurse da zatražite certifikate za provjeru autentičnosti korisnika. Korisnici sada moraju predstaviti važeći certifikat iz lokalnog CA prije nego im bude dopušten pristup Web poslužitelju. Svaki korisnik mora koristiti Upravitelja digitalnih certifikata (DCM) da dobije certifikat upotrebom zadatka **Kreiranje certifikata**. Da bi bilo moguće dobiti certifikat od lokalnog CA, politika lokalnog CA mora dopuštati izdavanje korisničkih certifikata.

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

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a.
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 tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite tipku 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 System i 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.

Scenarij: postavljanje izdavača certifikata uz Upravitelj digitalnih certifikata

Prije postavljanja izdavača certifikata (CA) administrator podružnice mora osigurati dovršetak nekoliko zadataka planiranja. Prije nego počnete obavljati sljedeće zadatke provjerite jesu li ispunjeni svi preduvjeti za ovaj scenarij.

Popunjavanje radnih tablica za planiranje za Upravitelj digitalnih certifikata

MyCo, Inc. popunjava radne tablice za planiranje da bi si olakšao postavljanje digitalnih certifikata koje će izdati poslovnom partneru.

Tablica 5. Radna tablica planiranja za kreiranje izdavača certifikata (CA) pomoću Upravitelja digitalnih certifikata (DCM)

Pitanja	**Odgovori**
Koju veličinu ključa planirate koristiti za generiranje javnih i privatnih ključeva za certifikat?	1024
Koja je lozinka za spremište certifikata?	tajna **Važno:** Sve lozinke koje se koriste u ovom scenariju služe samo kao primjeri. Nemojte ih koristiti u nekoj stvarnoj konfiguraciji.
Kako se zove izdavač certifikata?	mycoca
Kako se zove vaša organizacija?	myco
Koliko dana želite da traje valjanost izdavača certifikata?	1095 (3 godine)
Koji pretražitelj koristite?	Windows Internet Explorer verzije 6.0
Hoćete li izdavati certifikate korisnicima na mreži?	Ne

Tablica 6. Radna tablica planiranja za digitalni certifikat za System A

Pitanja	**Odgovori**
Koju veličinu ključa planirate koristiti za generiranje javnih i privatnih ključeva za certifikat?	1024

Tablica 6. Radna tablica planiranja za digitalni certifikat za System A (nastavak)

Pitanja	Odgovori
Koja je lozinka za spremište certifikata?	tajna **Važno:** Sve lozinke koje se koriste u ovom scenariju služe samo kao primjeri. Nemojte ih koristiti u nekoj stvarnoj konfiguraciji.
Kako se zove oznaka certifikata?	mycocert
Koje je zajedničko ime vašeg certifikata?	mycocert
Kako se zove vaša organizacija?	MyCo, Inc
Koja je IP adresa vašeg sistema?	192.168.1.2 (2001:DB8::2 za IPv6) **Važno:** IP adrese koje se koriste u ovom scenariju služe samo kao primjeri. Nisu odraz sheme IP adresiranja i ne treba ih koristiti u nekoj stvarnoj konfiguraciji. Kada budete obavljali ove zadatke, koristite vlastite IP adrese.
Koje je potpuno kvalificirano ime glavnog računala vašeg sistema?	systema.myco.min.com

Tablica 7. Radna tablica planiranja za digitalni certifikat za System B

Pitanja	Odgovori
Koju veličinu ključa planirate koristiti za generiranje javnih i privatnih ključeva za certifikat?	1024
Kako se zove oznaka certifikata?	corporatecert
Koje je zajedničko ime vašeg certifikata?	corporatecert
Koja je staza i ime datoteke spremišta certifikata?	/tmp/systemb.kdb
Koja je lozinka za spremište certifikata?	tajna2 **Važno:** Sve lozinke koje se koriste u ovom scenariju služe samo kao primjeri. Nemojte ih koristiti u nekoj stvarnoj konfiguraciji.
Koje je zajedničko ime digitalnog certifikata?	corporatecert
Koje je organizacijsko ime vlasnik ovog certifikata?	MyCo, Inc
Koja je IP adresa vašeg sistema?	172.16.1.3 (2002:DD8::3 za IPv6) **Važno:** IP adrese koje se koriste u ovom scenariju služe samo kao primjeri. Nisu odraz sheme IP adresiranja i ne treba ih koristiti u nekoj stvarnoj konfiguraciji. Kada budete obavljali ove zadatke, koristite vlastite IP adrese.
Koje je potpuno kvalificirano ime glavnog računala vašeg sistema?	systemb.myco.wis.com

Pokretanje IBM HTTP Servera za i5/OS na Systemu A

Pomoću ovog postupka pokrenite IBM HTTP poslužitelj za i5/OS na Systemu A.

Da biste pristupili sučelju Upravitelja digitalnih certifikata (DCM), morate pokrenuti administrativnu instancu HTTP Servera na sljedeći način.

1. Iz Systema A prijavite se u sučelje bazirano na znakovima.
2. U prompt za naredbe upišite strtcpsvr server(*HTTP) httpsvr(*admin). Time se pokreće administracijski sistem HTTP Servera.

Konfiguriranje Systema A kao izdavača certifikata

Pomoću ovog ćete postupka konfigurirati System A kao izdavač certifikata (CA).

1. Otvorite Web pretražitelj i unesite http://your_system_name:2001 da biste učitali IBM Systems Director Navigator za i5/OS pozdravnu stranicu.
2. Prijavite se pomoću imena za korisnički profil i lozinke za System A.
3. Na pozdravnoj stranici kliknite vezu na **i5/OSstranicu sa zadacima**.
4. Izaberite **Upravitelj digitalnih certifikata**.
5. U lijevom navigacijskom okviru izaberite **Kreiraj izdavača certifikata (CA)**.
6. Na stranici za kreiranje izdavača certifikata (CA) u sljedeća obvezna polja unesite podatke iz DCM-ove radne tablice za planiranje:
   - **Veličina ključa:** 1024
   - **Lozinka za spremište certifikata:** secret
   - **Potvrda lozinke:** tajna

     Važno: Sve lozinke koje se koriste u ovom scenariju služe samo kao primjeri. Nemojte ih koristiti u nekoj stvarnoj konfiguraciji.
   - **Ime izdavača certifikata:** mycoca
   - **Ime organizacije:** MyCo, Inc
   - **Država ili provincija:** min
   - **Zemlja ili regija:** us
   - **Razdoblje valjanosti za izdavača certifikata (2-7300):** 1095
7. Kliknite **Nastavak**.
8. Na stranici za **instalaciju lokalnog CA certifikata** kliknite **Nastavak**.
9. Na stranici s **podacima o politici za izdavača certifikata (CA)** izaberite sljedeće opcije:
   - **Dozvoli kreiranje korisničkog certifikata:** Da
   - **Razdoblje valjanosti certifikata koje izdaje ovaj Izdavač certifikata (1-2000):** 365
10. Na stranici za prihvaćanje podataka o politici pročitajte prikazane poruke i kliknite **Nastavak** za kreiranje defaultnog poslužiteljskog spremišta certifikata (*SYSTEM) i poslužiteljskog certifikata potpisanog od strane vašeg CA. Pročitajte potvrdnu poruku i kliknite **Nastavak**.
11. Na stranici za kreiranje certifikata za poslužitelj ili klijent unesite sljedeće informacije:
    - **Veličina ključa:** 1024
    - **Oznaka certifikata:** mycocert
    - **Lozinka za spremište certifikata:** tajna
    - **Potvrda lozinke:** tajna

      Važno: Sve lozinke koje se koriste u ovom scenariju služe samo kao primjeri. Nemojte ih koristiti u nekoj stvarnoj konfiguraciji.
    - **Zajedničko ime:** mycocert
    - **Ime organizacije:** myco, Inc
    - **Država ili provincija:** min
    - **Zemlja ili regija:** us
    - **Adresa IP verzije 4:** 192.168.1.2
    - **Adresa IP verzije 6:** 2001:DB8::3

Bilješka: IP adrese koje se koriste u ovom scenariju služe samo kao primjeri. Nisu odraz sheme IP adresiranja i ne treba ih koristiti u nekoj stvarnoj konfiguraciji. Kada budete obavljali ove zadatke, koristite vlastite IP adrese.

- **Potpuno kvalificirano ime domene:** systema.myco.min.com
- **Adresa e-pošte:** administrator@myco.min.com

12. Kliknite **Nastavak**.
13. Na stranici za izbor aplikacija kliknite **Nastavak**.

Savjet: Čarobnjak za novu VPN vezu automatski dodjeljuje upravo kreirani certifikat i5/OS aplikaciji za upravljanje VPN ključevima. Ako imate drugih aplikacija koje bi mogle koristiti taj certifikat, možete ih izabrati na ovoj stranici. Budući da se u ovom scenariju certifikati koriste samo za VPN veze, nema potrebe za izborom dodatnih aplikacija.

14. Na stranici sa statusom aplikacija pročitajte prikazane poruke i kliknite **Opoziv**. Time se prihvaćaju kreirane promjene.

Bilješka: Ako želite kreirati spremište certifikata koje će sadržavati certifikate koji se koriste za potpisivanje objekata, izaberite **Nastavak**.

15. Nakon osvježavanja DCM sučelja izaberite **Izbor spremišta certifikata**.
16. Na stranici za izbor spremišta certifikata izaberite ***SYSTEM**. Kliknite **Nastavak**.
17. Na stranici sa spremištem certifikata i lozinkom izaberite tajna. Kliknite **Nastavak**.
18. U lijevom navigacijskom okviru izaberite **Upravljanje aplikacijama**.
19. Na stranici za upravljanje aplikacijama izaberite **Definiranje liste pouzdanih CA-ova**. Kliknite **Nastavak**.
20. Na stranici za definiranje liste pouzdanih CA-ova izaberite **Poslužitelj**. Kliknite **Nastavak**.
21. Izaberite **i5/OS VPN upravitelj ključeva**. Kliknite **Definiranje liste pouzdanih CA-ova**.
22. Na stranici za definiranje liste pouzdanih CA-ova izaberite **LOCAL_CERTIFICATE_AUTHORITY**. Kliknite **OK**.

Kreiranje digitalnih certifikata za System B

Pomoću ovog postupka kreirajte digitalni certifikat za System B.

1. U lijevom navigacijskom okviru kliknite **Kreiraj certifikat** i izaberite **Poslužiteljski i klijentski certifikat za neki drugi System i**.
2. Kliknite **Nastavak**.
3. Na stranici za kreiranje poslužiteljskog ili klijentskog certifikata za neki drugi System i izaberite **V5R3**. Ovo je razina izdanja za System B. Kliknite **Nastavak**.
4. Na stranici za kreiranje poslužiteljskog ili klijentskog certifikata unesite sljedeće informacije:
   - **Veličina ključa:** 1024
   - **Oznaka certifikata:** corporatecert
   - **Staza i ime datoteke spremišta certifikata:** /tmp/systemb.kdb
   - **Lozinka za spremište certifikata:** tajna2
   - **Potvrda lozinke:** tajna2

     Bilješka: Sve lozinke koje se koriste u ovom scenariju služe samo kao primjeri. Nemojte ih koristiti u nekoj stvarnoj konfiguraciji.
   - **Zajedničko ime:** corporatecert
   - **Ime organizacije:** MyCo, Inc
   - **Država ili provincija:** wis
   - **Zemlja ili regija:** us
   - **Adresa IP verzije 4:** 172.16.1.3
   - **Adresa IP verzije 6:** 2002:DD8::3

Važno: IP adrese koje se koriste u ovom scenariju služe samo kao primjeri. Nisu odraz sheme IP adresiranja i ne treba ih koristiti u nekoj stvarnoj konfiguraciji. Kada budete obavljali ove zadatke, koristite vlastite IP adrese.

- **Potpuno kvalificirano ime hosta:** systemb.myco.wis.com
- **Adresa e-pošte:** administrator@myco.wis.com

5. Kliknite **Nastavak**. Primit ćete potvrdnu poruku kojom se potvrđuje da je poslužiteljski certifikat kreiran na Systemu A za System B. Kao administrator mreže u prodajnoj podružnici te datoteke ćete poslati administratoru u korporativnom uredu putem šifrirane poruke e-pošte. Administrator u korporativnom uredu morat će premjestiti i preimenovati datoteku spremišta certifikata (.KDB) i datoteku zahtjeva (.RDB) na System B. Administrator u korporativnom uredu mora premjestiti te datoteke u direktorij /QIBM/USERDATA/ICSS/CERT/SERVER u integriranom sistemu datoteka pomoću binarnog FTP-a. Nakon dovršetka tog postupka administrator mora preimenovati te datoteke u odgovarajućem direktoriju.

Preimenovanje .KDB i .RDB datoteka na Systemu B

Sljedećim postupkom preimenujte .KDB i .RDB datoteke na Systemu B.

Budući da spremište certifikata *SYSTEM ne postoji na Systemu B, administrator korporativne mreže mora preimenovati datoteke systemb.kdb i systemb.RDB u DEFAULT.KDB i DEFAULT.RDB i te prenesene datoteke upotrijebiti kao spremište certifikata *SYSTEM na Systemu B.

1. U System i Navigator proširite **System B → Sistemi datoteka → Integrirani sistem datoteka → Qibm → KorisničkiPodaci → ICSS → Cert → Server**, i provjerite jesu li datoteke systemb.kdb i systemb.RDB navedene u tom direktoriju.
2. U red za naredbe upišite wrklnk ('/qibm/userdata/icss/cert/server').
3. Na stranici za rad s povezanim objektima izaberite 7 (Preimenuj) za preimenovanje datoteke systemb.kdb. Pritisnite Enter.
4. Na stranici za preimenovanje objekta unesite DEFAULT.KDB u polje **Novi objekt**. Pritisnite Enter.
5. Ponovite 3. i 4. korak da biste datoteku systemb.RDB preimenovali u DEFAULT.RDB.
6. Provjerite jesu li datoteke promijenjene tako da osvježite System i Navigator i proširite ***System B*** **→ Sistemi datoteka → Integrirani sistemi datoteka → Qibm → KorisničkiPodaci → ICSS → Cert → Poslužitelj**. Datoteke DEFAULT.KDB i DEFAULT.RDB moraju biti navedene u tom direktoriju.

Promjena lozinke za spremište certifikata na Systemu B

Pomoću ovog postupka možete promijeniti lozinku za spremište certifikata na Systemu B

Sada mrežni administrator korporativnog ureda mora promijeniti lozinku za novo spremište certifikata *SYSTEM kreirano pri kreiranju datoteka DEFAULT.KDB i DEFAULT.RDB.

Bilješka: Morate promijeniti lozinku za spremište certifikata *SYSTEM. Kada promijenite lozinku, ona je skrivena tako da je aplikacija može automatski obnoviti i otvoriti spremište certifikata radi pristupa certifikatima.

1. Otvorite Web pretražitelj i unesite http://your_system_name:2001 da biste učitali IBM Systems Director Navigator za i5/OS pozdravnu stranicu.
2. Na pozdravnoj stranici kliknite vezu na **i5/OSstranicu sa zadacima**.
3. Izaberite **Upravitelj digitalnih certifikata**.
4. U lijevom navigacijskom okviru kliknite **Izbor spremišta certifikata**.
5. Izaberite ***SYSTEM spremište certifikata** i unesite tajna2 kao lozinku. To je lozinka koju je naveo administrator podružnice prodaje pri kreiranju poslužiteljskog certifikata za System B. Kliknite **Nastavak**.
6. U lijevom navigacijskom okviru izaberite **Upravljanje spremištem certifikata**, zatim izaberite **Promjena lozinke** i kliknite **Nastavak**.
7. Na stranici za promjenu lozinke za spremište certifikata unesite corporatepwd u polja **Nova lozinka** i **Potvrda lozinke**.
8. Izaberite **Lozinka ne ističe** za politiku isteka. Kliknite **Nastavak**. Učitat će se stranica za potvrdu. Kliknite **OK**.
9. Na stranici za potvrdu promjene lozinke za spremište certifikata pročitajte poruku i kliknite **OK**.

10. Na stranici sa spremištem certifikata i lozinkom koja će se ponovo učitati unesite coporatepwd u polje **Lozinka za spremište certifikata**. Kliknite **Nastavak**.

Definiranje liste pouzdanih CA-ova za i5/OS upravitelja VPN ključeva na Systemu B

Pomoću ovog postupka definirat ćete listu pouzdanih CA-ova za upravitelja VPN ključeva na Systemu B.

1. U lijevom navigacijskom okviru izaberite **Upravljanje aplikacijama**.
2. Na stranici za upravljanje aplikacijama izaberite **Definiranje liste pouzdanih CA-ova**. Kliknite **Nastavak**.
3. Na stranici za definiranje liste pouzdanih CA-ova izaberite **Poslužitelj**. Kliknite **Nastavak**.
4. Izaberite **i5/OS VPN upravitelj ključeva**. Kliknite **Definiranje liste pouzdanih CA-ova**.
5. Na stranici za definiranje liste pouzdanih CA-ova izaberite **LOCAL_CERTIFICATE_AUTHORITY**. Kliknite **OK**.

Administratori u podružnicama i u sjedištu poduzeća sada mogu započeti konfiguraciju VPN-a.

Planiranje za DCM

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

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

Zahtjevi za postavljanje DCM-a

Da bi Upravitelj digitalnih certifikata ispravno funkcionirao, morate instalirati određene proizvode i konfigurirati aplikaciju.

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

- Instalirajte Upravitelj digitalnih certifikata.Ovo je DCM funkcija osnovana na pretražitelju.
- Instalirajte IBM HTTP poslužitelj za i5/OS 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

Lozinke za šifriranu bazu podataka s ključevima koje koristite za pristup spremištima certifikata u Upravitelju digitalnih certifikata (DCM) pohranjuju se (sakrivaju) u posebnu sigurnosnu datoteku na vašem 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.

Jedan primjer takvih okolnosti je korištenje DCM-a za kreiranje certifikata za neki drugi model System i pri čemu se za kreiranje novog spremišta certifikata izabiru datoteke na ciljnom sistemu. 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.

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 bit 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

"Korištenje lokalnog CA za izdavanje certifikata za druge System i modele" na stranici 56
Pomoću Upravitelja digitalnih certifikata (DCM) možete konfigurirati privatni lokalni CA na jednom sistemu radi izdavanja certifikata koji će se koristiti na drugim System i platformama.

Tipovi digitalnih certifikata

Kada koristite Upravitelj digitalnih certifikata (DCM) za upravljanje certifikatima, DCM organizira i pohranjuje te certifikate i pripadajuće privatne ključeve u spremište certifikata utemeljeno na tipu certifikata.

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 koji kreirate i održavate pomoću Upravitelja digitalnih certifikata nezavisan je entitet. 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 System i korisničkim profilom. Možete koristiti DCM za pridruživanje korisničkih certifikata koje izdaje drugi Izdavač certifikata s System i korisničkim profilom.

Bilješka: Ako imate instaliran IBM kriptografski 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 kriptografskom koprocesoru. Ili, možete koristiti kriptografski 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” na stranici 9
Sloj sigurnih utičnica standard je 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

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).
- Održavanje vlastitog lokalnog CA radi izdavanja privatnih certifikata korisnicima i aplikacijama.
- Korištenje kombinacije certifikata javnih Internet CA-ova i vlastitog 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. Osim toga, druga poduzeća i korisnici možda će spremnije priznavati i više vjerovati certifikatima koje izdaje dobro poznati javni CA nego onima koje izdaje vaš privatni lokalni CA.

Upotreba privatnih certifikata

Ako kreirate vlastiti lokalni CA, možete izdavati certifikate sistemima i korisnicima u ograničenijem djelokrugu, npr. unutar vlastitog poduzeća ili organizacije. Kreiranje i održavanje vlastitog lokalnog CA omogućuje vam da certifikate izdajete samo onim korisnicima koji su pouzdani članovi vaše grupe. Time je osigurana bolja zaštita, jer možete strože i bolje kontrolirati tko ima certifikat i na taj način i tko ima pristup vašim resursima. Mogući nedostatak održavanja vlastitog lokalnog CA je količina vremena i resursa koje morate uložiti. Međutim, Upravitelj digitalnih certifikata (DCM) čini za vas taj postupak lakšim.

Kada koristite lokalni CA za izdavanje certifikata korisnicima za provjeru autentičnosti klijenta, morate odlučiti gdje ćete pohranjivati korisničke certifikate. Kada korisnici dobiju certifikate od lokalnog CA putem DCM-a, ti se certifikati po defaultu pohranjuju uz korisnički profil. 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 biste radije da se korisnički certifikati ne pridružuju niti na bilo koji način pohranjuju s korisničkim profilima, možete se poslužiti API-jima za programsko izdavanje certifikata korisnicima koji nisu System i korisnici.

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 održavanje privatnog CA opisuje zadatke koje morate obaviti ako odlučite imati lokalni 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 System i modelima opisuje zadatke koje morate obaviti ako želite koristiti certifikate privatnog lokalnog CA na više sistema.

Srodni koncepti

"Upravljanje certifikatima iz javnog Internet CA" na stranici 49
Kada koristite Upravitelj digitalnih certifikata (DCM) za upravljanje certifikatima javnog Internet CA, najprije morate kreirati spremište certifikata. Spremište certifikata je posebna datoteka baze podataka ključeva koju DCM koristi za pohranjivanje digitalnih certifikata i njihovih pridruženih privatnih ključeva.

"Javni certifikati naspram privatnih certifikata" na stranici 32
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.

"Prvo postavljanje certifikata" na stranici 41
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.

"Digitalni certifikati za potpisivanje objekata" na stranici 38
i5/OS osigurava podršku za korištenje certifikata u svrhu digitalnog ″potpisa″ objekata. Digitalno potpisivanje objekata pruža način provjere cjelovitosti sadržaja objekta i izvora porijekla.

Srodni zadaci

"Digitalni certifikat i mapiranje identiteta u poduzeću (EIM)" na stranici 36
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 korisničkog certifikata" na stranici 44
Ako želite koristiti digitalne certifikate za provjeru identiteta korisnika, korisnici moraju imati certifikate. Ako koristite Upravitelj digitalnih certifikata (DCM) za rad s privatnim lokalnim Izdavačem certifikata (CA), možete pomoću lokalnog CA izdavati certifikate korisnicima.

"Kreiranje i održavanje lokalnog CA" na stranici 41
Pomoću Upravitelja digitalnih certifikata (DCM) možete kreirati i održavati vlastiti lokalni CA radi izdavanja privatnih certifikata svojim aplikacijama.

"Korištenje lokalnog CA za izdavanje certifikata za druge System i modele" na stranici 56
Pomoću Upravitelja digitalnih certifikata (DCM) možete konfigurirati privatni lokalni CA na jednom sistemu radi izdavanja certifikata koji će se koristiti na drugim System i platformama.

Srodne reference

"Korištenje API-ja za programsko izdavanje certifikata korisnicima koji nisu korisnici System i" na stranici 47
Vaš lokalni CA može izdavati privatne certifikate korisnicima bez pridruživanja certifikata System i korisničkom profilu.

Digitalni certifikati za SSL zaštićene komunikacije

Za postavljanje SSL sesije, vaš poslužitelj uvijek pribavlja kopiju svog certifikata da klijent, koji zahtijeva vezu, provjeri valjanost.

Korištenjem SSL veze jamčite klijentu ili krajnjem korisniku da su vaše stranice autentične, a ujedno nudite i šifriranu komunikacijsku sesiju koja jamči da će svi podaci koji se prenesu tom vezom ostati zaštićeni.

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"
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.

Digitalni certifikati za provjeru korisnika

Korisnici tradicionalno primaju pristup resursima od neke aplikacije ili sistema, na osnovi njihovog korisničkog imena i lozinke. Možete i dalje povećavati sistemsku sigurnost upotrebom digitalnih certifikata (umjesto korisničkih imena i lozinki) za provjeru autentičnosti i autorizirati sesije između mnogih aplikacija i korisnika.

Pomoću Upravitelja digitalnih certifikata (DCM) možete pridružiti korisnikov certifikat njegovu System i korisničkom profilu ili identitetu nekog drugog korisnika. Certifikat tada ima iste autorizacije i dozvole kao i pridruženi korisnički identitet ili korisnički profil. Umjesto toga možete koristiti API-je za programsko korištenje svojeg lokalnog Izdavača certifikata (CA) za izdavanje certifikata korisnicima koji nisu System i korisnici. Ti API-ji omogućuju izdavanje privatnih certifikata korisnicima kada ne želite da ti korisnici imaju System i korisnički profil ili neki drugi interni korisnički identitet.

Digitalni certifikat djeluje kao elektronička vjerodajnica i potvrđuje da je osoba koja predočava taj certifikat uistinu ona za koju 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. Ako je riječ o certifikatu, CA funkcionira kao pouzdana treća strana koja izdaje certifikat i potvrđuje da je riječ o autentičnoj vjerodajnici.

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 sljedeće System i aplikacije nude podršku za certifikate za provjeru autentičnosti klijenta:

- Telnet poslužitelj
- IBM HTTP poslužitelj za i5/OS (upravljano s Apache)
- IBM Tivoli Directory Server za i5/OS
- System i Access za Windows (uključujući System i 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.

Srodni koncepti

"Digitalni certifikati za SSL zaštićene komunikacije" na stranici 34
Za postavljanje SSL sesije, vaš poslužitelj uvijek pribavlja kopiju svog certifikata da klijent, koji zahtijeva vezu, provjeri valjanost.

Srodne reference

"Korištenje API-ja za programsko izdavanje certifikata korisnicima koji nisu korisnici System i" na stranici 47
Vaš lokalni CA može izdavati privatne certifikate korisnicima bez pridruživanja certifikata System i korisničkom profilu.

Digitalni certifikat 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 omogućuje 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 **System i Navigator** za konfiguriranje EIM-a.
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 32
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.

Srodni zadaci

"Upravljanje korisničkim certifikatima putem isteka" na stranici 46
Upravitelj digitalnih certifikata (DCM) nudi podršku za upravljanje istekom certifikata koja administratorima omogućuje provjeru datuma isteka korisničkih certifikata na lokalnom System i modelu. DCM-ovu podršku za upravljanje istekom korisničkih certifikata moguće je koristiti zajedno s Mapiranjem identiteta u poduzeću (EIM-om) tako da administratori mogu pomoću DCM-a provjeravati istek korisničkih certifikata na razini poduzeća.

"Upravljanje LDAP lokacijom za korisničke certifikate" na stranici 72
Pomoću Upravitelja digitalnih certifikata (DCM) možete pohraniti korisničke certifikate na LDAP lokaciju poslužiteljskog direktorija i tako proširiti Mapiranje identiteta u poduzeću na rad s korisničkim certifikatima.

Srodne informacije

EIM poglavlje Informacijskog centra

Digitalni certifikati za VPN veze

Možete koristiti digitalne certifikate kao sredstvo uspostavljanja System i 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 u DCM-u koristite lokalni CA za izdavanje certifikata, možete navesti alternativno ime subjekta za certifikat. Specificiranje ovih informacija osigurava da je vaša VPN veza kompatibilna s drugim VPN implementacijama koje mogu zahtijevati provjeru autentičnosti.

Srodni koncepti

"Upravljanje certifikatima iz javnog Internet CA" na stranici 49
Kada koristite Upravitelj digitalnih certifikata (DCM) za upravljanje certifikatima javnog Internet CA, najprije

morate kreirati spremište certifikata. Spremište certifikata je posebna datoteka baze podataka ključeva koju DCM koristi za pohranjivanje digitalnih certifikata i njihovih pridruženih privatnih ključeva.

Srodni zadaci

“Kreiranje i održavanje lokalnog CA” na stranici 41
Pomoću Upravitelja digitalnih certifikata (DCM) možete kreirati i održavati vlastiti lokalni CA radi izdavanja privatnih certifikata svojim aplikacijama.

“Definiranje popisa pouzdanih CA-ova za aplikaciju” na stranici 66
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.

Srodne informacije

Konfiguriranje VPN veze

Digitalni certifikati za potpisivanje objekata

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 za potpisivanje objekata pojačava klasične alate System i modela kojima se kontrolira tko može mijenjati objekte. Klasične kontrole ne mogu zaštititi objekt od neovlaštenih promjena dok je objekt u tranzitu preko Interneta ili neke druge nepouzdane mreže niti dok je pohranjen na sistemu koji nije System i platforma. 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 i osigurati se da objekt potiče 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. Ako, međutim, namjeravate distribuirati objekte isključivo unutar svoje organizacije, možda bi bilo bolje da koristite Upravitelj digitalnih certifikata (DCM) i kreirate vlastiti lokalni CA za izdavanje certifikata za potpisivanje objekata. Korištenje privatnih certifikata iz lokalnog CA za potpisivanje objekata jeftinije je od kupnje certifikata od dobro 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 32
Možete koristiti certifikate od javnih CA ili možete kreirati i raditi na privatnom CA za izdavanje certifikata. Kako ćete izabrati dobivanje vaših certifikata ovisi o tome kako ih planirate koristiti.

“Digitalni certifikati za provjeru potpisa objekata” na stranici 39
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.

Srodni zadaci

“Provjera potpisa na objektima” na stranici 74
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 51
Upravitelja digitalnih certifikata (DCM) možete koristiti za upravljanje javnim Internet certifikatima za digitalno potpisivanje objekata.

“Upravljanje certifikatima radi provjere potpisa na objektima” na stranici 53
Za potpisivanje objekta koristite privatni ključ certifikata za kreiranje potpisa. Kad šaljete potpisani objekt drugima, morate uključiti i kopiju certifikata koji je potpisao objekt.

Digitalni certifikati za provjeru potpisa objekata

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.

Postoji nekoliko vrijednosti koje možete upotrebljavati za sistemsku vrijednost QVFYOBJRST, u rasponu od zanemarivanja svih potpisa do zahtijevanja važećih potpisa za sve objekte koje vraća sistem. 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 i5/OS 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 38
i5/OS osigurava podršku za korištenje certifikata u svrhu digitalnog ″potpisa″ objekata. Digitalno potpisivanje objekata pruža način provjere cjelovitosti sadržaja objekta i izvora porijekla.

Srodne informacije

Pronalazač sistemskih vrijednosti

QVFYOBJRST sistemska vrijednost

Konfiguriranje DCM-a

Upravitelj digitalnih certifikata (DCM) nudi korisničko sučelje utemeljeno na pretražitelju putem kojega možete upravljati i konfigurirati digitalne certifikate za 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 System i korisnički profil. Svi zadaci za rukovanje s CA, upravljanje certifikatima i upotrebu aplikacija i drugi zadaci sistemske razine, dostupni su samo System i 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

Da biste mogli koristiti funkcije Upravitelja digitalnih certifikata (DCM), najprije ga morate pokrenuti na svom sistemu.

Da biste bili sigurni da ćete uspješno pokrenuti DCM, učinite sljedeće:

1. Instalirajte Upravitelj digitalnih certifikata.
2. Instalirajte IBM HTTP poslužitelj za i5/OS.
3. Koristite System i Navigator da biste pokrenuli administrativni poslužitelj HTTP poslužitelj:
   a. U System i Navigator proširite svoj **sistem → Mreža → Poslužitelji → TCP/IP**.
   b. Desno kliknite na **HTTP Administraciju**.
   c. Izaberite **Početak**.
4. Otvorite Web pretražitelj i upišite http://your_system_name:2001 da biste učitali IBM Systems Director Navigator za i5/OS web konzolu.
5. Na pozdravnoj stranici kliknite vezu na **i5/OS stranicu sa zadacima**.
6. Izaberite **Upravitelj digitalnih certifikata** iz popisa proizvoda na stranici i5/OS Zadaci da pristupite DCM korisničkom sučelju.

Srodni koncepti

"Scenarij: korištenje certifikata za vanjsku 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.

Prvo postavljanje 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). (Napomena: nakon što pomoću ovog zadatka kreirate privatni lokalni CA, taj se zadatak više ne pojavljuje na popisu.)
- Upravljanje CRL lokacijama.
- Upravljanje LDAP lokacijom.
- Upravljanje PKIX lokacijama za zahtjeve.
- Povratak na i5/OS stranicu sa zadacima.

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. Zadaci ili kategorije koje prikazuje DCM ovise o otvorenom spremištu certifikata i posebnim ovlaštenjima za vaš korisnički profil.

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 32
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.

Kreiranje i održavanje lokalnog CA

Pomoću Upravitelja digitalnih certifikata (DCM) možete kreirati i održavati vlastiti lokalni CA radi izdavanja privatnih certifikata svojim aplikacijama.

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 biste koristili DCM za kreiranje i održavanje lokalnog CA, učinite sljedeće:

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a.
2. U navigacijskom okviru DCM-a, izaberite Kreiranje izdavača certifikata (CA) da biste prikazali nizove obrazaca. Sljedeći obrasci će vas provesti kroz proces kreiranja lokalnog CA i obavljanja drugih zadataka potrebnih za početak korištenja digitalnih certifikata za SSL, potpisivanje objekata i provjeru potpisa.

   Bilješka: Ako imate pitanja u vezi 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. Za vrijeme korištenja tih obrazaca za obavljanje zadataka potrebnih za postavljanje funkcionalnog lokalnog Izdavača certifikata (CA) morat ćete učiniti sljedeće:
   a. Izabrati kako pohraniti privatni ključ za certifikat lokalnog CA. (Ovaj korak je osiguran samo ako na sistemu imate instaliran IBM kriptografski koprocesor. Ako vaš sistem nema kriptografski koprocesor, DCM automatski pohranjuje certifikat i njegov privatni ključ u spremište certifikata lokalnog Izdavača certifikata (CA).
   b. Navesti identifikacijske podatke za lokalni CA.
   c. Instalirati certifikat lokalnog CA na svoje osobno računalo ili u pretražitelj tako da softver može prepoznati lokalni CA i provjeriti valjanost certifikata koje izdaje taj CA.
   d. Izabrati podatke za politiku lokalnog CA.
   e. Upotrijebiti novi lokalni CA za izdavanje poslužiteljskog ili klijentskog certifikata koji aplikacije mogu koristiti za SSL veze. (Ako sistem ima instaliran IBM kriptografski 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 poslužitelja ili klijenta koje aplikacija može 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. Izabrati aplikacije koje će smatrati lokalni CA pouzdanim.

Kada završite vođeni zadatak, imat ćete sve što vam je potrebno za početak konfiguriranja aplikacija za korištenje SSL-a za sigurno komuniciranje.

Kada konfigurirate aplikacije, korisnici koji pristupaju aplikacijama putem SSL veze morat će putem DCM-a pribaviti kopiju certifikata lokalnog CA. 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 pomoću DCM-a mogu ili kopirati certifikat lokalnog CA u datoteku ili spustiti certifikat u svoj pretražitelj. Način na koji će korisnici pohraniti certifikat lokalnog CA ovisi o klijentskom softveru koji koriste za uspostavljanje SSL veze s aplikacijom.

Pomoću tog lokalnog CA možete i izdavati certifikate aplikacijama na drugim System i modelima u svojoj mreži.

Dodatne informacije o korištenju DCM-a za upravljanje certifikatima lokalnog CA i o načinu na koji korisnici mogu nabaviti kopiju certifikata lokalnog CA za provjeru autentičnosti certifikata koje izdaje lokalni CA potražite u sljedećim poglavljima:

Srodni koncepti

"Javni certifikati naspram privatnih certifikata" na stranici 32
Možete koristiti certifikate od javnih CA ili možete kreirati i raditi na privatnom CA za izdavanje certifikata. Kako ćete izabrati dobivanje vaših certifikata ovisi o tome kako ih planirate koristiti.

"Digitalni certifikati za VPN veze" na stranici 37
Možete koristiti digitalne certifikate kao sredstvo uspostavljanja System i VPN povezivanja. Obje krajnje točke dinamičke VPN veze moraju biti sposobne za međusobnu provjeru autentičnost prije aktiviranja veze.

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

Srodni zadaci

"Korištenje lokalnog CA za izdavanje certifikata za druge System i modele" na stranici 56
Pomoću Upravitelja digitalnih certifikata (DCM) možete konfigurirati privatni lokalni CA na jednom sistemu radi izdavanja certifikata koji će se koristiti na drugim System i platformama.

"Dobivanje kopije certifikata privatnog CA" na stranici 48
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.

"Potpisivanje objekata" na stranici 73
Postoje tri različite metode potpisivanja objekata. Možete napisati program koji će pozivati API za potpisivanje objekata, koristiti Upravitelj digitalnih certifikata (DCM) ili koristiti funkciju System i Navigator Management Central za pakete koje distribuirate drugim sistemima.

Srodne reference

"Korištenje API-ja za programsko izdavanje certifikata korisnicima koji nisu korisnici System i" na stranici 47
Vaš lokalni CA može izdavati privatne certifikate korisnicima bez pridruživanja certifikata System i korisničkom profilu.

Upravljanje korisničkim certifikatima:

Možete koristiti Upravitelja digitalnih certifikata (DCM) da biste dobili certifikate sa SSL-om ili pridružili postojeće certifikate s njihovim System i 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, međutim, vaš poslužitelj koristi certifikat od privatnog lokalnog CA, vaši korisnici moraju dobiti kopiju certifikata lokalnog CA da bi mogli uspostaviti SSL vezu 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 predstaviti certifikat od javnog Internet CA ili certifikat koji su dobili od

lokalnog CA kojim upravljate. Ako aplikacija poslužitelja osigurava pristup resursima za interne korisnike koji trenutno imaju System i 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 System i 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 nema otvorenog spremišta podataka ili je otvoreno spremište certifikata lokalnog Izdavača certifikata (CA), možete izabrati **Upravljanje korisničkim certifikatima** u navigacijskom okviru za pristup odgovarajućim zadacima. Ako je otvoreno drukčije spremište certifikata, zadaci korisnika certifikata se integriraju u zadatke pod **Upravljanje certifikatima**.

Korisnici bez *SECADM i *ALLOBJ posebnih ovlaštenja profila korisnika mogu upravljati samo svojim vlastitim dodjelama certifikata. Mogu izabrati **Upravljanje certifikatima korisnika** za pristupanje zadacima koji im dozvoljavaju da gledaju certifikate pridružene njihovom korisničkom profilu, uklone certifikat iz svog korisničkog profila ili pridruže certifikat od drugog CA svom korisničkom profilu. Bez obzira na posebna ovlaštenja svojih korisničkih profila, korisnici mogu dobiti korisnički certifikat od lokalnog CA tako da izaberu zadatak **Kreiraj 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 održavanje lokalnog CA” na stranici 41
Pomoću Upravitelja digitalnih certifikata (DCM) možete kreirati i održavati vlastiti lokalni CA radi izdavanja privatnih certifikata svojim aplikacijama.

“Dobivanje kopije certifikata privatnog CA” na stranici 48
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.

Kreiranje korisničkog certifikata:

Ako želite koristiti digitalne certifikate za provjeru identiteta korisnika, korisnici moraju imati certifikate. Ako koristite Upravitelj digitalnih certifikata (DCM) za rad s privatnim lokalnim Izdavačem certifikata (CA), možete pomoću lokalnog CA izdavati certifikate korisnicima.

Svaki korisnik mora pristupiti DCM-u da dobije certifikat koristeći zadatak **Kreiraj certifikat**. Da bi bilo moguće dobiti certifikat od lokalnog CA, politika CA mora dopuštati izdavanje korisničkih certifikata.

Da biste dobili certifikat od lokalnog CA, učinite sljedeće:

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a.
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 System i 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 32
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.

Srodni zadaci

"Dodjela korisničkog certifikata"
Možete dodijeliti korisnički certifikat koji posjedujete i5/OS korisničkom profilu ili drugom korisničkom identitetu. Certifikat može potjecati od privatnog lokalnog CA na nekom drugom sistemu ili pak od dobro 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 certifikata privatnog CA" na stranici 48
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.

Dodjela korisničkog certifikata:

Možete dodijeliti korisnički certifikat koji posjedujete i5/OS korisničkom profilu ili drugom korisničkom identitetu. Certifikat može potjecati od privatnog lokalnog CA na nekom drugom sistemu ili pak od dobro 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 nekog vanjskog Izdavača certifikata (CA) ili lokalnog CA na nekom drugom iSeries sistemu, a vi kao administrator, želite da ti certifikati budu dostupni Upravitelju 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 System i 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 je definirana LDAP lokacija, a System i model je konfiguriran za sudjelovanje u EIM-u, zadatak **Dodijeli korisnički certifikat** omogućuje korisniku pohranu kopije vanjskog certifikata u navedeni 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 korisničkog certifikata” na stranici 44
   Ako želite koristiti digitalne certifikate za provjeru identiteta korisnika, korisnici moraju imati certifikate. Ako koristite Upravitelj digitalnih certifikata (DCM) za rad s privatnim lokalnim Izdavačem certifikata (CA), možete pomoću lokalnog CA izdavati certifikate korisnicima.

   “Rješavanje problema s dodjelom korisničkih certifikata” na stranici 82
   Pomoću sljedećih koraka pokušajte riješiti probleme s dodjelom korisničkih certifikata pomoću Upravitelja digitalnih certifikata (DCM).

   Srodne informacije

   Pregled EIM-a u Informacijskom centru

Upravljanje korisničkim certifikatima putem isteka:

Upravitelj digitalnih certifikata (DCM) nudi podršku za upravljanje istekom certifikata koja administratorima omogućuje provjeru datuma isteka korisničkih certifikata na lokalnom System i modelu. DCM-ovu podršku za upravljanje istekom korisničkih certifikata moguće je koristiti zajedno s Mapiranjem identiteta u poduzeću (EIM-om) tako da administratori mogu pomoću DCM-a provjeravati istek 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. Pogledajte Pokretanje DCM-a.

   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 certifikat i mapiranje identiteta u poduzeću (EIM)" na stranici 36
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.

"Upravljanje certifikatima putem isteka" na stranici 67
Upravitelj digitalnih certifikata (DCM) nudi podršku za upravljanje istekom certifikata koja administratorima omogućuje upravljanje poslužiteljskim i klijentskim certifikatima, certifikatima za potpisivanje objekata, certifikatima izdavača certifikata i korisničkim certifikatima prema datumu isteka na lokalnom sistemu.

Srodne informacije

Pregled EIM-a u Informacijskom centru

Korištenje API-ja za programsko izdavanje certifikata korisnicima koji nisu korisnici System i:

Vaš lokalni CA može izdavati privatne certifikate korisnicima bez pridruživanja certifikata System i korisničkom profilu.

| API za generiranje i potpisivanje zahtjeva za korisničkim certifikatom (QYCUGSUC) i API za potpisivanje zahtjeva za
| korisničkim certifikatom (QYCUSUC) omogućuju programsko izdavanje certifikata korisnicima koji nisu korisnici
| System i. Pridruživanje certifikata System i korisničkom profilu ima svojih prednosti, naročito kada je riječ o internim
| korisnicima. No, ta ograničenja i preduvjeti čine korištenje lokalnog CA manje praktičnim kada je riječ o izdavanju
| korisničkih certifikata većem broju korisnika, naročito kada ne želite da ti korisnici imaju System i 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 API-ja nude podršku potrebnu za sučelje kojim se kreiraju korisnički certifikati koje za bilo koje ime korisnika potpisuje lokalni CA. Ovaj certifikat neće biti pridružen profilu korisnika. Korisnik ne mora postojati na sistemu koji služi kao host za DCM, a korisnik ne mora koristiti DCM za kreiranje certifikata.

Postoje dva API-ja, jedan za svaki od pred-dominantnih pretraživačkih programa, koje možete pozivati kod upotrebe Net.Data za kreiranje programa za izdavanje certifikata korisnicima. Aplikacija koju kreirate mora imati kod za grafičko korisničko sučelje (GUI) koji je potreban za kreiranje korisničkog certifikata i za pozivanje jednog od odgovarajućih API-ja koji će se poslužiti lokalnim CA za potpisivanje certifikata.

Srodni koncepti

"Javni certifikati naspram privatnih certifikata" na stranici 32
Možete koristiti certifikate od javnih CA ili možete kreirati i raditi na privatnom CA za izdavanje certifikata. Kako ćete izabrati dobivanje vaših certifikata ovisi o tome kako ih planirate koristiti.

"Digitalni certifikati za provjeru korisnika" na stranici 35
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.

Srodni zadaci

"Kreiranje i održavanje lokalnog CA" na stranici 41
Pomoću Upravitelja digitalnih certifikata (DCM) možete kreirati i održavati vlastiti lokalni CA radi izdavanja privatnih certifikata svojim aplikacijama.

Srodne informacije

API Generiranje i potpisivanje korisničkog zahtjeva za certifikat (QYCUGSUC)

API Potpisivanje korisničkog zahtjeva za certifikat (QYCUSUC)

Dobivanje kopije certifikata privatnog 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, međutim, poslužitelj predstavi certifikat od privatnog lokalnog CA, morate dobiti kopiju certifikata lokalnog CA putem Upravitelja digitalnih certifikata (DCM).

Pomoću DCM-a možete spustiti kopiju certifikata lokalnog CA u datoteku tako da mu može pristupiti i koristiti ga i drugi klijentski softver. Ako i pretražitelj i druge aplikacije koristite za sigurnu komunikaciju, možda ćete morati koristiti obje metode za instaliranje certifikata lokalnog CA. Ako koristite obje metode, instalirajte certifikat u vaš pretražitelj prije nego ga kopirate i preslikate u datoteku.

Ako poslužiteljska aplikacija traži da potvrdite svoj identitet predstavljanjem certifikata lokalnog CA, morate spustiti taj certifikat u pretražitelj prije nego zatražite korisnički certifikat od lokalnog CA.

Da biste pomoću DCM-a dobili kopiju certifikata lokalnog CA, učinite sljedeće:

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a.
2. U navigacijskom okviru izaberite **Instaliraj certifikat lokalnog CA na PC** da bi se prikazala stranica na kojoj možete spustiti certifikat lokalnog CA u pretražitelj ili ga pohraniti u datoteku na sistemu.
3. Izaberite metodu za dobivanje certifikata lokalnog CA.
   a. Izaberite **Instaliraj certifikat** da biste spustili certifikat lokalnog CA u pretražitelj kao pouzdano ishodište. 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** da bi se prikazala stranica na kojoj se nalazi posebno kodirana kopija certifikata lokalnog CA. 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. Da bi aplikacije klijenta mogle prepoznati i koristiti certifikat lokalnog CA, morate ih konfigurirati da ga prepoznaju 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 korisničkim certifikatima" na stranici 43
Možete koristiti Upravitelja digitalnih certifikata (DCM) da biste dobili certifikate sa SSL-om ili pridružili postojeće certifikate s njihovim System i korisničkim profilima.

Srodni zadaci

"Kreiranje i održavanje lokalnog CA" na stranici 41
Pomoću Upravitelja digitalnih certifikata (DCM) možete kreirati i održavati vlastiti lokalni CA radi izdavanja privatnih certifikata svojim aplikacijama.

"Kreiranje korisničkog certifikata" na stranici 44
Ako želite koristiti digitalne certifikate za provjeru identiteta korisnika, korisnici moraju imati certifikate. Ako koristite Upravitelj digitalnih certifikata (DCM) za rad s privatnim lokalnim Izdavačem certifikata (CA), možete pomoću lokalnog CA izdavati certifikate korisnicima.

Upravljanje certifikatima iz javnog Internet CA

Kada koristite Upravitelj digitalnih certifikata (DCM) za upravljanje certifikatima javnog Internet CA, najprije morate kreirati spremište certifikata. Spremište certifikata je posebna datoteka baze podataka ključeva koju DCM koristi za pohranjivanje digitalnih certifikata i njihovih pridruženih privatnih ključeva.

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 se poslužiti vođenim zadacima u DCM-u za središnje upravljanje tim javnim certifikatima i aplikacijama koje ih koriste za uspostavu SSL veza, potpisivanje objekata i 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 32
Možete koristiti certifikate od javnih CA ili možete kreirati i raditi na privatnom CA za izdavanje certifikata. Kako ćete izabrati dobivanje vaših certifikata ovisi o tome kako ih planirate koristiti.

"Digitalni certifikati za VPN veze" na stranici 37
Možete koristiti digitalne certifikate kao sredstvo uspostavljanja System i VPN povezivanja. Obje krajnje točke dinamičke VPN veze moraju biti sposobne za međusobnu provjeru autentičnost prije aktiviranja veze.

Srodni zadaci

"Upravljanje lokacijom zahtjeva za PKIX CA" na stranici 71
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 vlastitim lokalnim Izdavačem certifikata (CA), najprije morate 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 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. Pogledajte Pokretanje DCM-a.
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 kriptografski 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 koji 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 vođeni zadatak, imat ćete sve što vam je potrebno za početak konfiguriranja aplikacija za korištenje SSL-a za sigurno komuniciranje. 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 vlastitim lokalnim Izdavačem certifikata (CA), najprije morate 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 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 System i Navigator.)

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

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a.
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 koji ste izabrali da izdaje i potpisuje vaše certifikate.

   Bilješka: Prije nego završite ovaj postupak morate početi dok CA ne vrati potpisan i dovršen certifikat.
8. Nakon što javni CA vrati vaš potpisani certifikat, pokrenite DCM.
9. U lijevom navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** kao spremište certifikata za otvoriti.
10. Kad se prikaže stranica 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 ih primaju moraju koristiti OS/400 V5R1 ili noviju verziju DCM-a za provjeru valjanosti potpisa na objektima da bi bili sigurni da podaci nisu promijenjeni i da potvrde identitet 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. Morate, na primjer, osigurati kopiju certifikata lokalnog CA ako ste potpisali objekte certifikatom iz 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 38
i5/OS osigurava podršku za korištenje certifikata u svrhu digitalnog ″potpisa″ objekata. Digitalno potpisivanje objekata pruža način provjere cjelovitosti sadržaja objekta i izvora porijekla.

Srodni zadaci

“Provjera potpisa na objektima” na stranici 74
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.

“Potpisivanje objekata” na stranici 73
Postoje tri različite metode potpisivanja objekata. Možete napisati program koji će pozivati API za potpisivanje objekata, koristiti Upravitelj digitalnih certifikata (DCM) ili koristiti funkciju System i Navigator Management Central za pakete koje distribuirate drugim sistemima.

Upravljanje certifikatima radi provjere 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, međutim, objekt potpisan certifikatom nekog drugog javnog CA ili privatnog lokalnog CA, morate dobiti kopiju certifikata CA da biste mogli provjeriti potpis na objektu.

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. Pogledajte Pokretanje DCM-a.
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 38
i5/OS osigurava podršku za korištenje certifikata u svrhu digitalnog ″potpisa″ objekata. Digitalno potpisivanje objekata pruža način provjere cjelovitosti sadržaja objekta i izvora porijekla.

Srodni zadaci

“Provjera potpisa na objektima” na stranici 74
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.

Obnova postojećeg certifikata

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

Certifikat možete obnoviti pomoću lokalnog ili Internet CA.

Obnova certifikata iz lokalnog CA

Ako obnovljeni certifikat obnavljate pomoću lokalnog CA, DCM koristi navedene informacije za kreiranje novog certifikata u trenutnom spremištu certifikata i zadržava prethodni certifikat.

Obnova certifikata pomoću lokalnog CA:

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.

Obnova 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. Drugi način obnove certifikata jest pomoću DCM-a kreirati javno-privatni par ključeva i zahtjev za potpisivanjem certifikata (CSR) za dotični certifikat, a zatim te informacije poslati Internetskom CA i dobiti novi certifikat. 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.

Import certifikata

Pomoću Upravitelja digitalnih certifikata (DCM) možete importirati certifikate koji se nalaze u datotekama na vašem sistemu. Možete importirati certifikate s drugih poslužitelja umjesto ponovnog kreiranja certifikata na trenutnom poslužitelju.

Na Systemu A, na primjer, koristili ste lokalni CA za kreiranje certifikata za svoju maloprodajnu web-aplikaciju i upotrijebili ga za iniciranje SSL veza. Vaše se poslovanje u posljednje vrijeme proširilo i zato ste instalirali novi model System i (System B) koji će služiti kao host za dodatne instance za tu vrlo prometnu maloprodajnu aplikaciju. Želite da sve instance maloprodajne aplikacije koriste identični certifikat za identificiranje i iniciranje SSL povezivanja. Zato ćete možda odlučiti importirati i certifikat lokalnog CA i poslužiteljski certifikat sa Systema A na System B, umjesto da se poslužite lokalnim CA na Systemu A za kreiranje novog, različitog certifikata koji će koristiti System B.

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

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:

Korištenje lokalnog CA za izdavanje certifikata za druge System i modele

Pomoću Upravitelja digitalnih certifikata (DCM) možete konfigurirati privatni lokalni CA na jednom sistemu radi izdavanja certifikata koji će se koristiti na drugim System i platformama.

Možda na nekom sistemu u svojoj mreži već koristite privatni lokalni Izdavač certifikata (CA). Sada želite upotrebu tog lokalnog CA proširiti na neki drugi sistem u mreži. Želite, na primjer, da trenutni lokalni CA izda poslužiteljski ili klijentski certifikat za aplikaciju na nekom drugom sistemu da bi bilo moguće koristiti SLL komunikacijske sesije. Ili pak želite pomoću certifikata lokalnog CA na jednom sistemu potpisati objekte koje pohranjujete na nekom drugom poslužitelju.

To možete postići pomoću DCM-a. Neke zadatke obavit ćete na sistemu na kojem koristite lokalni CA, a druge na sekundarnom sistemu koji služi kao host za aplikacije za koje želite izdati certifikate. Taj sekundarni sistem se naziva ciljni sistem. Zadaci koje morate izvesti na ciljnom sistemu ovise o razini izdanja tog sistema.

Bilješka: Mogu se pojaviti problemi ako sistem na kojem koristite lokalni CA koristi neki proizvod dobavljača kriptografskog pristupa koji nudi jače šifriranje od onoga na ciljnom sistemu. Kada eksportirate certifikat (zajedno s privatnim ključem), sistem šifrira datoteku da bi zaštitio njezin sadržaj. Ako sistem upotrebljava jači kriptografski 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 kriptografskim proizvodom na ciljnom sistemu.

Pomoću lokalnog CA možete izdavati certifikate drugim sistemima i zatim ih koristiti za potpisivanje objekata ili za omogućavanje aplikacijama uspostavu SSL sesija. Kada koristite lokalni CA za kreiranje certifikata na nekom drugom sistemu, datoteke koje kreira DCM sadrže kopiju certifikata lokalnog CA i kopije certifikata mnogih javnih Internet CA-ova.

Zadaci koje morate obaviti u DCM-u neznatno se razlikuju ovisno o tipu certifikata koji izdaje vaš lokalni CA i o izdanju i uvjetima na ciljnom sistemu.

Izdavanje privatnih certifikata za korištenje na nekom drugom System i modelu

Da biste pomoću lokalnog CA izdavali certifikate koji će se koristiti na nekom drugom sistemu, učinite sljedeće na sistemu na kojem se nalazi lokalni CA:

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a.
2. U navigacijskom okviru izaberite **Kreiraj certifikat** za prikaz popisa certifikata koje možete kreirati pomoću lokalnog CA.

   Bilješka: Ne trebate otvarati spremište certifikata da dovršite ovaj zadatak. U uputama koje slijede pretpostavlja se da ne radite u nekom određenom spremištu certifikata ili pak da radite u spremištu certifikata lokalnog Izdavača certifikata (CA). Na sistemu mora postojati lokalni CA da biste mogli obaviti zadatke koji slijede. 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 izdati pomoću CA i kliknite **Nastavak** da biste započeli vođeni zadatak i popunili niz obrazaca.
4. Izaberite kreiranje **poslužiteljskog ili klijentskog certifikata za neki drugi System i** (za SSL sesije) ili **certifikat za potpisivanje objekata za neki drugi System i** (za korištenje na nekom drugom sistemu).
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 certifikata lokalnog CA 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 30
Lozinke za šifriranu bazu podataka s ključevima koje koristite za pristup spremištima certifikata u Upravitelju digitalnih certifikata (DCM) pohranjuju se (sakrivaju) u posebnu sigurnosnu datoteku na vašem 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.

“Javni certifikati naspram privatnih certifikata” na stranici 32
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.

Srodni zadaci

“Kreiranje i održavanje lokalnog CA” na stranici 41
Pomoću Upravitelja digitalnih certifikata (DCM) možete kreirati i održavati vlastiti lokalni CA radi izdavanja privatnih certifikata svojim aplikacijama.

Korištenje privatnog 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 koje morate obaviti da biste koristili prenesene datoteke spremišta certifikata koje ste kreirali na glavnom sistemu lokalnog CA razlikuju se ovisno o tome postoji li spremište certifikata *SYSTEM. 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. Provjerite nalaze li se datoteke spremišta certifikata (dvije datoteke: jedna s ekstenzijom .KDB i jedna s ekstenzijom .RDB) koje ste kreirali na sistemu koji služi kao glavno računalo za lokalni CA u direktoriju /QIBM/USERDATA/ICSS/CERT/SERVER.
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 je dodao te datoteke, kao i kopiju certifikata lokalnog CA, datotekama 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 prenesene datoteke kako je predloženo. Prepisivanje default datoteka će uzrokovati problem kod korištenja DCM-a, prenesenog spremišta certifikata i njegovog sadržaja. Umjesto toga morate osigurati da imaju jedinstvena imena i morate koristiti preneseno spremište certifikata kao **Spremište certifikata drugog sistema**. Ako koristite datoteke kao Spremište certifikata drugog sistema, ne možete koristiti DCM da specificirate koje aplikacije će koristiti certifikat.
3. Pokrenite DCM. Sada morate promijeniti lozinku za *SYSTEM spremište certifikata koju ste kreirali preimenovanjem prenesenih datoteka. Promjenom lozinke se dopušta da DCM pohrani novu lozinku tako da možete koristiti sve funkcije upravljanja DCM certifikatima u spremištu certifikata.
4. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***SYSTEM** da se otvori spremište certifikata.
5. Kad se prikaže stranica sa Spremištem certifikata i lozinkom, navedite lozinku koju ste specificirali na glavnom računalu 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 obavite navedene zadatke, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao lokalni CA na nekom drugom sistemu. Međutim, prije nego što počnete koristiti SSL za ove aplikacije, morate konfigurirati aplikacije za korištenje SSL-a.

Da bi korisnik mogao pristupiti izabranim aplikacijama putem SSL veze, mora se poslužiti DCM-om da pribavi kopiju certifikata lokalnog CA od glavnog sistema. Certifikat lokalnog CA mora se kopirati u datoteku na korisnikovu računalu ili učitati u korisnikov pretražitelj, ovisno o potrebama aplikacije koja podržava 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** . Umjesto toga možete i importirati privatni certifikat i njegov odgovarajući certifikat lokalnog CA u postojeće spremište certifikata *SYSTEM.

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 System i aplikacije (i mnoge aplikacije drugih razvijača softvera) su napisane za upotrebu certifikata samo u *SYSTEM spremištu certifikata. Ako odlučite koristiti prenesene 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 System i SSL-omogućene aplikacije da biste koristili ovaj certifikat. Ako želite koristiti certifikat za System i 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 certifikat lokalnog CA u spremište certifikata prije nego eksportirate poslužiteljski ili klijentski certifikat u spremište certifikata. Ako najprije eksportirate poslužiteljski ili klijentski certifikat, možete naići na grešku jer u spremištu certifkata ne postoji certifikat lokalnog CA.
9. Izaberite certifikat lokalnog CA koji želite eksportirati i kliknite **Eksportiraj**.
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 obavite navedene zadatke, aplikacije na ciljnom sistemu mogu koristiti certifikat koji je izdao lokalni CA na nekom drugom sistemu. Međutim, prije nego što počnete koristiti SSL za ove aplikacije, morate konfigurirati aplikacije za korištenje SSL-a.

Da bi korisnik mogao pristupiti izabranim aplikacijama putem SSL veze, mora se poslužiti DCM-om da pribavi kopiju certifikata lokalnog CA od glavnog sistema. Certifikat lokalnog CA mora se kopirati u datoteku na korisnikovu računalu ili učitati u korisnikov pretražitelj, ovisno o potrebama aplikacije koja podržava SSL.

Potpisivanje objekata na ciljnom sistemu pomoću privatnog certifikata

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 da biste koristili prenesene datoteke spremišta certifikata koje ste kreirali na glavnom sistemu lokalnog CA razlikuju se ovisno o tome postoji li spremište certifikata *OBJECTSIGNING. 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 morate obaviti da biste koristili prenesene datoteke spremišta certifikata koje ste kreirali na glavnom sistemu lokalnog CA razlikuju se ovisno o tome jeste li na ciljnom sistemu ikada koristili DCM za upravljanje certifikatima za potpisivanje objekata.

Ako spremište certifikata *OBJECTSIGNING ne postoji na ciljnom sistemu s prenesenim datotekama spremišta certifikata, pratite ove korake:

1. Provjerite nalaze li se datoteke spremišta certifikata (dvije datoteke: jedna s ekstenzijom .KDB i jedna s ekstenzijom .RDB) koje ste kreirali na sistemu koji služi kao glavno računalo za lokalni CA u direktoriju /QIBM/USERDATA/ICSS/CERT/SIGNING.
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 je dodao te datoteke, kao i kopiju certifikata lokalnog CA, datotekama 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 prenesene datoteke kako je predloženo. Prepisivanje default 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 kreirao lokalni CA na glavnom sistemu i kliknite **Dodijeli novi certifikat**.

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

Kada distribuirate potpisane objekte, 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. Morate, na primjer, osigurati kopiju certifikata lokalnog CA ako ste potpisali objekte

certifikatom iz 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 samog certifikata za potpisivanje objekata i certifikata lokalnog CA 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 koji želite eksportirati i kliknite **Eksportiraj**.

   Bilješka: Morate eksportirati certifikat lokalnog CA u spremište certifikata prije nego eksportirate certifikat za potpisivanje objekata u spremište certifikata. Ako najprije eksportirate certifikat za potpisivanje objekata, možete naići na grešku jer u spremištu certifkata ne postoji certifikat lokalnog CA.
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

Upravitelj digitalnih certifikata (DCM) omogućuje kreiranje aplikacijske definicije i upravljanje dodjelom certifikata određene aplikacije. Možete definirati i popis pouzdanih CA-ova koje će aplikacije koristiti kao temelj za prihvaćanje certifikata za provjeru autentičnosti klijenata.

Možete koristiti DCM za obavljanje raznih zadataka upravljanja za aplikacije koje podržavaju Sloj sigurnih utičnica (SSL) i aplikacije za potpisivanje objekata. Možete, na primjer, odrediti koje će certifikate aplikacije koristiti za SSL komunikacijske sesije. 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
Upravitelj digitalnih certifikata (DCM) omogućuje upravljanje aplikacijskim definicijama koje će biti kompatibilne sa SSL konfiguracijama i potpisivanjem objekata.

Kreiranje definicije aplikacije

U Upravitelju digitalnih certifikata možete kreirati sljedeća dva tipa definicija aplikacija i raditi s njima: poslužiteljske ili klijentske aplikacije koje koriste SSL i definicije aplikacija koje služe 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 upotrebom API-ja (QSYRGAP, QsyRegisterAppForCertUse) za automatsko kreiranje ID-a aplikacije u DCM-u. Sve IBM System i 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. Pogledajte Pokretanje DCM-a.
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
   Upravitelj digitalnih certifikata (DCM) omogućuje upravljanje aplikacijskim definicijama koje će biti kompatibilne sa SSL konfiguracijama i potpisivanjem objekata.

   Srodne informacije

   QSYRGAP, QsyRegisterAppForCertUse API

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. Pogledajte Pokretanje DCM-a.
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, System i 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.

Srodni zadaci

"Upravljanje CRL lokacijama" na stranici 69
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.

"Dodjela certifikata aplikacijama" na stranici 68
Upravitelj digitalnih certifikata (DCM) dozvoljava brzu i jednostavnu dodjelu certifikata višestrukim aplikacijama. Možete dodijeliti certifikat za više aplikacija u *SYSTEM ili *OBJECTSIGNING spremištu certifikata.

Definiranje popisa pouzdanih CA-ova 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. Pogledajte Pokretanje DCM-a.
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 na listi. Također možete pogledati ili provjeriti valjanost CA certifikata prije nego ga dodate na pouzdani popis.

Srodni koncepti

“Digitalni certifikati za VPN veze” na stranici 37
Možete koristiti digitalne certifikate kao sredstvo uspostavljanja System i VPN povezivanja. Obje krajnje točke dinamičke VPN veze moraju biti sposobne za međusobnu provjeru autentičnost prije aktiviranja veze.

Upravljanje certifikatima putem isteka

Upravitelj digitalnih certifikata (DCM) nudi podršku za upravljanje istekom certifikata koja administratorima omogućuje upravljanje poslužiteljskim i klijentskim certifikatima, certifikatima za potpisivanje objekata, certifikatima izdavača certifikata i korisničkim certifikatima prema datumu isteka na lokalnom sistemu.

Bilješka: Ako konfigurirate DCM za rad s Mapiranjem identiteta u poduzeću (EIM-om), možete upravljati korisničkim certifikatima prema datumu isteka na svim razinama poduzeća.

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. Pogledajte Pokretanje DCM-a ako DCM već nije pokrenut.
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.

   Bilješka: Da biste provjerili kada ističe poslužiteljski ili klijentski certifikat, morate se nalaziti u spremištu certifikata *SYSTEM ili Other System. Da biste provjerili kada ističe certifikat za potpisivanje objekata, morate se nalaziti u spremištu certifikata *OBJECTSIGNING. Datum isteka certifikata izdavača certifikata moguće je provjeriti u svim spremištima certifikata osim u spremištu certifikata lokalnog Izdavača certifikata. Datum isteka korisničkih certifikata moguće je provjeriti u bilo kojem spremištu certifikata. Morate pogledati pojedinačan certifikat lokalnog CA da bi utvrdili kada ističe.
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.

Srodni zadaci

“Upravljanje korisničkim certifikatima putem isteka” na stranici 46
Upravitelj digitalnih certifikata (DCM) nudi podršku za upravljanje istekom certifikata koja administratorima omogućuje provjeru datuma isteka korisničkih certifikata na lokalnom System i modelu. DCM-ovu podršku za upravljanje istekom korisničkih certifikata moguće je koristiti zajedno s Mapiranjem identiteta u poduzeću (EIM-om) tako da administratori mogu pomoću DCM-a provjeravati istek korisničkih certifikata na razini poduzeća.

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” 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. Pogledajte Pokretanje DCM-a.
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.

Srodni zadaci

"Upravljanje dodjelom certifikata za aplikaciju" na stranici 65
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.

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. Pogledajte Pokretanje DCM-a.
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. Morate konfigurirati i Directory Server (LDAP) i klijentske aplikacije za korištenje SSL-a i dodijeliti certifikat aplikacijama u DCM-u.

Srodni koncepti

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

Srodni zadaci

"Upravljanje dodjelom certifikata za aplikaciju" na stranici 65
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.

Srodne informacije

IBM Poslužitelj direktorija za iSeries (LDAP)

Omogućavanje SSL-a na Poslužitelju direktorija

Pohrana ključeva certifikata na IBM kriptografskom koprocesoru

Ako ste na sistem instalirali IBM kriptografski koprocesor, možete se poslužiti njime za sigurniju pohranu privatnog ključa certifikata. Koprocesor možete koristiti za pohranjivanje privatnog ključa za poslužiteljski certifikat, klijentski certifikat ili certifikat lokalnog izdavača certifikata (CA).

Ne možete koristiti koprocesor za pohranu privatnog ključa korisničkog certifikata jer taj ključ mora biti pohranjen na korisnikovu 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 kriptografski koprocesor za System i" na stranici 8
kriptografski koprocesor omogućuje dokazane kriptografske usluge, osiguravajući privatnost i integritet, za razvijanje sigurnih e-business aplikacija.

Srodne informacije

Pregled kriptografije

Korištenje glavnog ključa koprocesora za šifriranje privatnog ključa certifikata

Za dodatnu sigurnost zaštite pristupa i upotrebe privatnog ključa certifikata, možete koristiti glavni ključ IBM kriptografskog 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).

Da biste mogli uspješno koristiti tu opciju, morate se poslužiti konfiguracijskim Web sučeljem IBM kriptografskog koprocesora za kreiranje odgovarajuće datoteke 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 System i 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 kriptografskog 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 kriptografskog 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 kriptografskog koprocesora. Konfiguracijskom Web sučelju koprocesora možete pristupiti putem Web konzole IBM Systems Director Navigator za i5/OS.
6. Kliknite **Nastavak**. DCM nastavlja prikazivati stranice za zadatke koje dovršavate, kao što su identifikacijske informacije za certifikat, koji kreirate ili obnavljate.

Srodne informacije

Pregled kriptografije

Rad s IBM Systems Director Navigatorom za i5/OS

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. Pogledajte Pokretanje DCM-a.

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 iz javnog Internet CA" na stranici 49
Kada koristite Upravitelj digitalnih certifikata (DCM) za upravljanje certifikatima javnog Internet CA, najprije morate kreirati spremište certifikata. Spremište certifikata je posebna datoteka baze podataka ključeva koju DCM koristi za pohranjivanje digitalnih certifikata i njihovih pridruženih privatnih ključeva.

Upravljanje LDAP lokacijom za korisničke certifikate

Pomoću Upravitelja digitalnih certifikata (DCM) možete pohraniti korisničke certifikate na LDAP lokaciju poslužiteljskog direktorija i tako proširiti Mapiranje identiteta u poduzeću na rad s korisničkim certifikatima.

DCM po defaultu pohranjuje korisničke certifikate koje izdaje lokalni Izdavač certifikata (CA) s i5/OS korisničkim profilima. Međutim, možete konfigurirati Upravitelj digitalnih certifikata (DCM) u kombinaciji s Mapiranjem identiteta u poduzeću (EIM-om) tako da se, kada lokalni Izdavač certifikata (CA) izda korisničke certifikate, javna kopija certifikata pohrani na specifičnoj LDAP lokaciji 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 eServer 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 System i 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**.

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

1. Poslužite se zadatkom **Upravljanje LDAP lokacijom** u DCM-u da biste naveli LDAP direktorij u koji će DCM pohraniti korisnički certifikat koji kreira lokalni CA. LDAP lokacija ne mora se nalaziti na lokalnom System i modelu niti na istom LDAP poslužitelju koji koristi EIM. Kada konfigurirate LDAP lokaciju u DCM-u, DCM koristi navedeni LDAP direktorij za pohranu svih korisničkih certifikata koje izda lokalni CA. DCM također koristi LDAP lokaciju za pohranu korisničkih certifikata obrađenih zadatkom **Dodjela korisničkog certifikata** umjesto pohrane certifikata s korisničkim profilom.
2. Pokrenite naredbu **Konvertiraj korisnički certifikat** (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 certifikat i mapiranje identiteta u poduzeću (EIM)” na stranici 36
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

Naredba Konvertiraj korisnički certifikat (CVTUSRCERT)

Mapiranje identiteta u poduzeću (EIM)

Potpisivanje objekata

Postoje tri različite metode potpisivanja objekata. Možete napisati program koji će pozivati API za potpisivanje objekata, koristiti Upravitelj digitalnih certifikata (DCM) ili koristiti funkciju System i Navigator Management Central za pakete koje distribuirate drugim sistemima.

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). Možete potpisivati i naredbene (*CMD) objekte. Ne možete potpisivati objekte pohranjene na drugim sistemima.

Objekte možete potpisivati certifikatima koje kupite od javnog Internet izdavača certifikata (CA) ili onima 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:

- Prije toga morate kreirati spremište certifikata *OBJECTSIGNING, kao dio procesa kreiranja lokalnog CA ili kao dio upravljanja certifikatima za potpisivanje objekata iz javnog Internet CA.
- Spremište certifikata *OBJECTSIGNING mora sadržavati barem jedan certifikat, kreiran pomoću lokalnog CA ili dobiven od javnog Internet CA.
- Morate imati kreiranu definiciju aplikacije za potpisivanje objekata za korištenje za potpisivanje objekata.
- Morate imati dodijeljen certifikat aplikaciji potpisivanja objekta koju namjeravate koristiti za potpisivanje objekata.

Upotreba DCM-a za potpisivanje objekata

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

1. Pokrenite DCM. Pogledajte 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, prikazat 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.

Srodni zadaci

“Kreiranje i održavanje lokalnog CA” na stranici 41
Pomoću Upravitelja digitalnih certifikata (DCM) možete kreirati i održavati vlastiti lokalni CA radi izdavanja privatnih certifikata svojim aplikacijama.

“Upravljanje javnim Internet certifikatima za potpisivanje objekata” na stranici 51
Upravitelja digitalnih certifikata (DCM) možete koristiti za upravljanje javnim Internet certifikatima za digitalno potpisivanje objekata.

Srodne informacije

API Potpisivanje objekta

Scenarij: Upotreba System i Navigatora Središnjeg upravljanja za potpisivanje objekata

Scenarij: Upotreba DCM-a za potpisivanje objekata i provjeru potpisa

Provjera potpisa na objektima

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 kreirati spremište certifikata *SIGNATUREVERIFICATION za upravljanje 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. Pogledajte Pokretanje DCM-a.
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, prikazat 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 38
i5/OS osigurava podršku za korištenje certifikata u svrhu digitalnog ″potpisa″ objekata. Digitalno potpisivanje objekata pruža način provjere cjelovitosti sadržaja objekta i izvora porijekla.

Srodni zadaci

"Upravljanje javnim Internet certifikatima za potpisivanje objekata" na stranici 51
Upravitelja digitalnih certifikata (DCM) možete koristiti za upravljanje javnim Internet certifikatima za digitalno potpisivanje objekata.

"Upravljanje certifikatima radi provjere potpisa na objektima" na stranici 53
Za potpisivanje objekta koristite privatni ključ certifikata za kreiranje potpisa. Kad šaljete potpisani objekt drugima, morate uključiti i kopiju certifikata koji je potpisao objekt.

Rješavanje problema s DCM-om

Pomoću sljedećih metoda rješavanja problema riješit ćete neke osnovne probleme na koje možete naići za vrijeme konfiguriranja i korištenja Upravitelja digitalnih certifikata (DCM).

Pri radu s DCM-om i certifikatima možete naići na greške koje će vam onemogućiti izvođenje zadataka i postizanje ciljeva. Mnogo čestih grešaka ili problema s kojima se možete susresti spadaju u različite kategorije, kao što su sljedeće:

Rješavanje problema s lozinkama i općenitih problema

Sljedeća tablica će vam pomoći pri rješavanju uobičajenijih problema s lozinkama i ostalih općenitih problema na koje biste mogli naići 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 i5/OS Informacijski centar i vanjske IBM web stranice na Internetu.
Vaša lozinka za lokalnog Izdavača certifikata (CA) i spremišta certifikata *SYSTEM 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.

Problem	Moguće rješenje
	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.
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 i 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 System i 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.
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 sa spremištima certifikata i bazama ključeva

Sljedeća tablica će vam pomoći pri rješavanju uobičajenijih problema sa spremištem certifikata i bazama ključeva na koje biste mogli naići 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

Neuspješno kreiranje baze ključeva ili lokalnog CA.	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.
	
	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. Morate kreirati novi lokalni CA nakon premještanja sljedećih datoteka:
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.KDB`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.RDB`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH .OLD`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POL`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.BAK`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STHBAK`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.STH`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TXT`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.BAK`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TMP`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLTMP`
	`/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLBAK`
	`/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CACRT`
	`/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CATMP`
	`/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CABAK`
	`/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CLIENT/*.USRCRT`
	
	Trebate kreirati novo *SYSTEM spremište certifikata i sistemski certifikat nakon premještanja sljedećih datoteka:
	`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.BAK`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.RDB`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH.OLD`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STHBAK`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TMP`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TEMP.STH`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TMP`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.BAK`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TXT`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.SGN`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/SGN.TMP`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/SGN.BAK`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/EXPSRV.TMP`
	`/QIBM/USERDATA/ICSS/CERT/SERVER/EXPSGN.TMP`

	Možda će vam nedostajati preduvjetni licencni program (LPP) za koji DCM zahtijeva da bude instaliran. Provjerite popis “Zahtjevi za postavljanje DCM-a” na stranici 30 i provjerite jesu li svi licencni programi 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. Dodatne informacije potražite u poglavlju i5/OS Informacijski centarQsyAddVldlCertificate API. Proučite dokumentaciju za IBM HTTP Server za i5/OS ako vam treba pomoć s konfiguriranjem instance sigurnog HTTP poslužitelja za korištenje validacijske liste.

Rješavanje problema s pretražiteljem

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.
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.

Problem	Moguće rješenje
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, primit 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 i5/OS problema s HTTP poslužiteljem

Sljedeća tablica će vam pomoći pri rješavanju problema s HTTP poslužiteljem na koje biste mogli naići za vrijeme rada s Upraviteljem digitalnih certifikata (DCM).

Problem	Moguće rješenje
Hypertext Transfer Protocol Secure (HTTPS) ne radi.	Pobrinite se da je HTTP poslužitelj ispravno konfiguriran za korištenje SSL-a. U V5R1 ili kasnijim verzijama, konfiguracijska datoteka mora imati **SSLAppName** postavljen upotrebom sučelja Administracije HTTP poslužitelja. Također, konfiguracija mora imati virtualni host konfiguriran tako da koristi SSL port, sa **SSL-om** postavljenim na **Omogućeno** za virtualni host. Također moraju postojati dvije direktive **Slušanja** koje specificiraju dva različita porta, jedna za SSL i druga koja nije za SSL. Ove su postavljene na stranici **Opće postavke**. Osigurajte da je instanca poslužitelja kreirana i certifikat poslužitelja potpisan.
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.	Proučite dokumentaciju za IBM HTTP Server za i5/OS ako trebate pomoć s opcijama za postavljanje 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 tim API-jima možete pronaći pomoću teme Pronalaženje API-ja topic u i5/OS Informacijski centar. Možda ćete također htjeti pogledati ove validacijske liste ili API-je koji se odnose na certifikat: • QsyListVldlCertificates i QSYLSTVC • QsyRemoveVldlCertificate i QRMVVC • QsyCheckVldlCertificate i QSYCHKVC • QsyParseCertificate i QSYPARSC, itd.
Povratak HTTP poslužitelja predugo traje ili istekne vrijeme ako zatražite popis certifikata u validacijskom popisu a tamo postoji više od 10.000 stavki.	Kreirajte paketni posao koji traži i briše certifikate koji odgovaraju određenim kriterijima, kao što su svi oni koji su istekli ili su od nekog određenog CA.
HTTP Poslužitelj neće biti uspješno pokrenut sa **SSL-om** postavljenim na **Omogućeno** i s porukom greške HTP8351 koja se pojavljuje u dnevniku posla. Dnevnik pogrešaka za HTTP Poslužitelj pokazuje grešku da operacija SSL Inicijalizacija nije uspjela s povratnim kodom greške 107 kada ne uspije HTTP Poslužitelj.	Greška 107 znači da je certifikat istekao. Koristite DCM da dodijelite različit certifikat 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 s dodjelom korisničkih certifikata

Pomoću sljedećih koraka pokušajte riješiti probleme s dodjelom korisničkih certifikata pomoću Upravitelja digitalnih certifikata (DCM).

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 korisničkog certifikata" na stranici 45
Možete dodijeliti korisnički certifikat koji posjedujete i5/OS korisničkom profilu ili drugom korisničkom identitetu. Certifikat može potjecati od privatnog lokalnog CA na nekom drugom sistemu ili pak od dobro 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

IBM Redbooks publikacije i Web stranice sadrže informacije koje se odnose na zbirku poglavlja Upravitelj digitalnih certifikata (DCM). Možete gledati ili ispisati bilo koju od PDF datoteka.

IBM Redbooks

- IBM eServer iSeries Sigurnost ožičene mreže: OS/400 V5R1 poboljšanja u DCM-u i kriptografiji
- AS/400 Internet sigurnost: Razvoj infrastrukture digitalnih certifikata

Web stranica

- Web stranica **VeriSign Help Desk** Ova Web stranica sadrži opsežnu knjižnicu poglavlja o digitalnim certifikatima, kao i više drugih poglavlja o Internet sigurnosti.
- **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 obveza 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 ovom dokumentu i sav licencni materijal koji je za njega dostupan IBM daje pod uvjetima IBM ugovora s kupcem, IBM međunarodnog ugovora za programske licence, 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 i 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.

Informacije o sučelju programiranja

Ova publikacija za Upravitelj digitalnih certifikata je predviđena za sučelja programiranja koja korisniku omogućuju pisanje programa za dobivanje usluga iz IBM i5/OS.

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
| Redbooks
| System i

| Adobe, Adobe logo, PostScript i PostScript logo su registrirani zaštitni znaci ili zaštitni znaci Adobe Systems
| Incorporated u Sjedinjenim Državama i drugim zemljama.

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 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