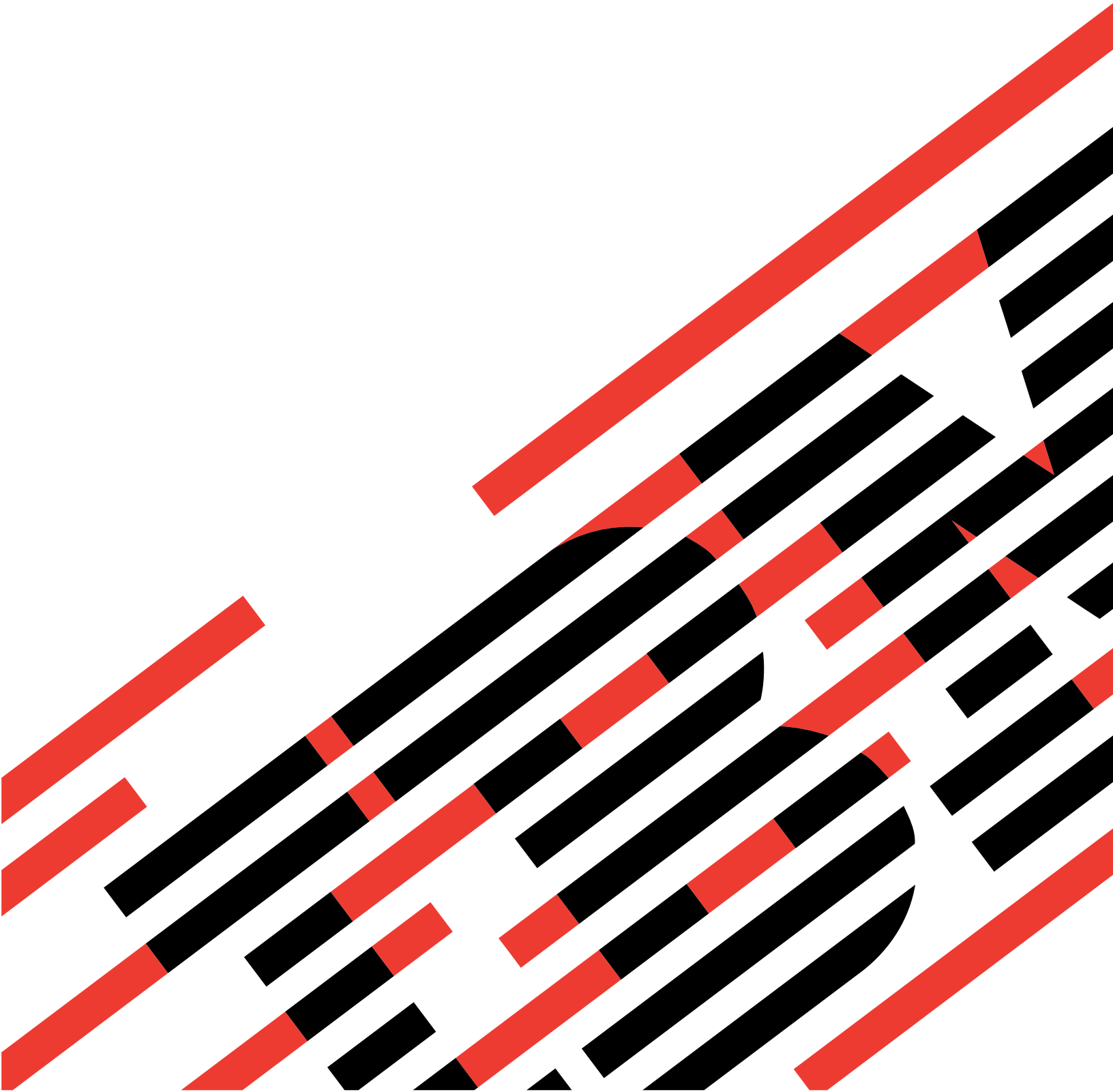
IBM

eserver

iSeries

Upravljalnik digitalnih potrdil

Različica 5 izdaja 3



IBM

@server

iSeries

Upravljalnik digitalnih potrdil

Različica 5 izdaja 3

Opomba:
Pred uporabo teh informacij in izdelka, ki ga opisujejo, preberite “Opombe”, na strani 93.

Osma izdaja (Avgust 2005)

Ta izdaja se nanaša na različico 5, izdajo 3 in popravke 0 izdelka IBM Operating System/400 (številka izdelka 5722–SS1) ter na vse nadaljnje izdaje in popravke, dokler v novih izdajah ne bomo določili drugače. Ta različica ne deluje na vseh modelih RISC (računalnik z zoženim naborom ukazov), niti ne deluje na modelih CISC.

Kazalo

Poglavje 1. Upravljalnik digitalnih potrdil

Digitalno potrdilo je elektronsko priporočilo, ki ga lahko uporabite za dokaz identitete v elektronski transakciji. Na voljo je vedno več možnosti za uporabo digitalnih potrdil, ki nudijo izboljšane načine za omrežno zaščito. Tako so na primer digitalna potrdila bistvenega pomena za konfiguriranje in uporabo plasti zaščitenih vtičnic (SSL) . Če uporabljate SSL, lahko izdelate zaščitene povezave med uporabniki in aplikacijami strežnika v neoverjenem omrežju kot je internet. SSL nudi eno izmed najboljših rešitev za zaščito zasebnosti pomembnih podatkov kot so imena uporabnikov in gesla, ki jih uporabljate na internetu. Številne storitve in aplikacije , denimo FTP, Telnet, Strežnik HTTP za iSeries (HTTP Server for iSeries) in druge nudijo podporo SSL, s pomočjo katere zagotavljajo zasebnost podatkov.

IBM nudi obširno podporo digitalnim potrdilom, ki vam omogoča, da digitalna potrdila uporabite kot priporočila v mnogih varnostnih aplikacijah. Poleg tega, da uporabite potrdila za konfiguriranje SSL, jih lahko uporabite tudi kot priporočila za overjanje odjemalca v transakcijah SSL in v transakcijah navideznega zasebnega omrežja (VPN). Digitalna potrdila ter z njimi povezane zaščitne ključe lahko uporabite za podpisovanje objektov. Podpisani objekti omogočajo, da odkrijete spremembe ali mogoče vdore v vsebino objekta, tako da preverite podpise na objektih in s tem zagotovite njihovo neokrnjenost.

Izkoriščanje podpore za potrdila je preprosto, če uporabljate Upravljalnik digitalnih potrdil (DCM) - brezplačno funkcijo, ki omogoča osrednje upravljanje potrdil za vaše aplikacije. DCM omogoča upravljanje potrdil, ki jih dobite pri katerikoli službi za potrdila (CA). Poleg tega lahko DCM uporabite tudi za izdelavo in delovanje vaše lastne lokalne službe za pooblastila, s katero boste izdajali zasebna potrdila aplikacijam in uporabnikom v vaši organizaciji.

Za učinkovito izkoriščanje zaščite, ki jo nudijo potrdila, je potrebno pravilno načrtovanje in ocena. Preglejte te teme in se naučite, kako potrdila delujejo in kako lahko z upravljalnikom digitalnih potrdil upravljate potrdila in aplikacije, ki jih uporabljajo:

Kaj je novega za V5R3
S pomočjo teh informacij se seznanite z izboljšavami upravljalnika digitalnih potrdil in spremembah tem z informacijami za to izdajo.

Tiskanje tega poglavja
Na tej strani boste spoznali, kako celotno temo natisniti kot datoteko PDF.

Scenariji DCM
S pomočjo teh informacij spoznajte dva scenarija, ki kažeta tipične sheme izvedbe potrdil, ki vam bodo v pomoč pri načrtovanju vaše lastne izvedbe potrdil kot del načel o zaščiti. Vsak scenarij nudi tudi vse potrebne konfiguracijske naloge, ki jih morate izvesti za pravilno uporabo scenarija.

Koncepti digitalnih potrdil
Te konceptne in referenčne informacije vam bodo pomagale bolje razumeti, kaj so digitalna potrdila in kako delujejo. Spoznajte različne tipe potrdil ter možnosti njihove uporabe kot del začel o zaščiti.

Načrt za DCM
Te informacije vam bodo v pomoč pri odločitvi, kako in kdaj lahko uporabite digitalna potrdila za izpolnitev vaših varnostnih ciljev. S pomočjo teh informacij spoznajte predpogoje, ki jih morate namestiti, ter tudi druge zahteve, ki jih morate upoštevati pred uporabo DCM.

Konfiguriranje DCM
S pomočjo teh informacij spoznajte, kako konfigurirati vse kar je potrebno za zagotovitev, da lahko DCM uporabite za upravljanje potrdil ter njihovih ključev.

Upravljajte DCM
Te informacije vam bodo pomagale razumeti, kako se uporablja DCM za upravljanje potrdil in aplikacij, ki potrdila uporabljajo. Naučili se boste tudi, kako digitalno podpisati objekte ter kako izdelati in voditi lastno službo za potrdila.

Odpravljanje težav v DCM
Te informacije vam bodo pomagale pri reševanju nekaterih pogostih napak, na katere lahko naletite pri uporabi DCM.

Z DCM povezane informacije
Na tej strani lahko najdete povezave do drugih virov, kjer se lahko poučite o digitalnih potrdilih, sestavi javnega ključa, upravljalniku digitalnih potrdil in o drugih s tem povezanih informacijah.

Poglavje 2. Kaj je novega za V5R3

Izboljšave za upravljalnik digitalnih potrdil (DCM) V5R3 in funkcije digitalnih potrdil vključujejo:

- **Delo z mestom LDAP**
  Nova naloga Delo z mestom LDAP v nalogah upravljalnika digitalnih potrdil vam omogoča shranjevanje uporabniških potrdil, ki jih lokalna služba za potrdila izda v mestu LDAP (poenostavljenem protokolu imeniškega dostopa). Če upravljalnik digitalnih potrdil konfigurirate za uporabo te možnosti, lahko uporabljate uporabniška potrdila, shranjena na le-tem mestu LDAP s pomočjo preslikave istovetnosti podjetij (EIM). Do te naloge dostopate prek glavnega usmerjalnega menija upravljalnika digitalnih potrdil.
- **Izboljšave naloge za dodeljevanje uporabniških potrdil za EIM**
  Če konfigurirate upravljalnik digitalnih potrdil za delo z EIM, naloga Dodeljevanje uporabniškega potrdila dodeljeno potrdilo shrani na mesto LDAP in ne skupaj z uporabniškim profilom. Način, na katerega upravljalnik digitalnih potrdil obravnava dodeljevanje potrdil, je odvisen od tega, ali ste ga konfigurirali tako, da za shranjevanje potrdil uporablja mesto LDAP skupaj s preslikavo istovetnosti podjetja (EIM).
- **Preverjanje datuma zapadlosti potrdila**
  S to novo funkcije lahko hitro in preprosto pregledujete in upravljate potrdila glede na datum njihove zapadlosti. Datum zapadlosti potrdila lahko preverite za potrdila strežnika ali odjemalca ter za potrdila za podpisovanje objektov v lokalnem sistemu. Prav tako lahko preverite datum zapadlosti za uporabniška potrdila. Datum zapadlosti za uporabniška potrdila lahko preverite bodisi za določen uporabniški profil, za vsa uporabniška potrdila sistema, ali za vsa uporabniška potrdila podjetja, če je v sistemu konfiguriran EIM.

Če želite najti druge informacije o novostih in spremembah v tej izdaji, preglejte Opombe za uporabnike .

Nasveti za pregledovanje novosti in sprememb

Te informacije za nudenje pomoči pri iskanju tehničnih sprememb uporabljajo:

- sliko , s pomočjo katere označijo, kje se pričnejo nove ali spremenjene informacije;
- sliko , s pomočjo katere označijo, kje se nove ali spremenjene informacije končajo.

Poglavje 3. Natis teme

Če si želite ogledati ali sneti različico PDF te teme, izberite Upravljalnik digitalnih potrdil  (velikost datoteke je približno 600 KB ali 116 strani).

Shranjevanje datotek PDF:

Če želite shraniti datoteko PDF na delovno postajo za prikaz ali tiskanje, naredite naslednje:

1. V pregledovalniku z desno tipko miške kliknite PDF (z desno tipko miške kliknite zgornjo povezavo).
2. Če uporabljate Internet Explorer, kliknite **Shrani cilj kot...**. Če uporabljate Netscape Communicator, kliknite **Shrani povezavo kot...**.
3. Poiščite imenik, v katerega želite shraniti datoteko PDF.
4. Kliknite **Shrani**.

Snemanje programa Adobe Acrobat Reader

Če želite pregledovati ali tiskati PDF-je, potrebujete program Adobe Acrobat Reader. Snamete ga lahko s spletne strani Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Poglavje 4. Scenariji DCM

Upravljalnik digitalnih potrdil in podpora digitalnim potrdilom sistema vam omogoča, da z uporabo potrdil izboljšate varnostna načela na več različnih načinov. Izbira načina uporabe potrdil je odvisna od poslovnih ciljev ter potrebe po zaščiti.

Z uporabo digitalnih potrdil boste izboljšali zaščito na številne načine. Digitalna potrdila omogočajo uporabo plasti zaščitenih vtičnic (SSL) za zaščiten dostop do internetnih mest in drugih internetnih storitev. Digitalna potrdila lahko uporabite za konfiguriranje povezav navideznega zasebnega omrežja (VPN). S ključem potrdila lahko digitalno podpišete objekte ali preverite veljavnost digitalnih podpisov in zagotovite pristnost objektov. Takšni digitalni podpisi zagotavljajo zanesljivost izvora objektov in ščitijo njihovo integriteto.

Zaščito sistema lahko dodatno povečate, če za overjanje in pooblaščanje v sejah med strežnikom in uporabniki uporabljate digitalna potrdila (namesto imen uporabnikov in gesel). Odvisno od tega, kako konfigurirate DCM, ga lahko uporabite za združitev uporabnikovega potrdila z njegovim uporabniškim profilom ali identifikatorjem za preslikavo istovetnosti podjetja (EIM). Takšno potrdilo ima ista pooblastila in dovoljenja kot z njim povezani profil uporabnika.

Izbira načina uporabe potrdil je lahko zelo zapletena in je odvisna od številnih faktorjev. Scenariji v tej temi opisujejo nekatere izmed splošnejših ciljev zaščite digitalnih potrdil za zaščiteno komunikacijo v okviru tipičnega poslovnega okolja. Vsi scenariji opisujejo tudi vse potrebne sistemske in programske predpogoje ter vse konfiguracijske naloge, ki jih morate izvesti za izvedbo scenarija. **Opomba:** V temi Scenariji podpisovanja objektov v informacijskem centru iSeries so vam na voljo podrobni primeri o uporabi digitalnih potrdil za podpisovanje objektov za zaščito njihove celovitosti.

Preglejte vsebino scenarijev, ki vam bo v pomoč pri določanju, kako najbolje uporabiti potrdila za povečanje varnosti, da bi zadostili vašim potrebam:

Scenarij: Uporaba potrdil za zunanje overjanje
V tem scenariju je opisano, kdaj in kako velja uporabljati digitalna potrdila kot mehanizem za overjanje, s katerim varujemo in omejimo dostop javnih uporabnikov do sredstev in aplikacij ekstraneta.

Scenarij: Uporaba potrdil za notranje overjanje
V tem scenariju je opisano, kdaj in kako velja uporabljati digitalna potrdila kot mehanizem za overjanje, s katerim varujemo in omejimo izbor sredstev in aplikacij na notranjih strežnikih, do katerih lahko dostopajo notranji uporabniki.

Scenarij: Uporaba potrdil za zunanje overjanje

Situacija

Zaposleni ste pri zavarovalnici MojePod, pri kateri ste zadolženi za vzdrževanje različnih aplikacij na straneh intraneta in ekstraneta vašega podjetja. Ena od aplikacij, za katero ste odgovorni, je aplikacija za izračunavanje obrokov, ki stotinam neodvisnih zastopnikov omogoča, da izračunavajo obroke za svoje stranke. Ker so informacije, ki jih nudi ta aplikacija, zaupne, želite zagotoviti, da jo bodo uporabljali samo registrirani zastopniki. Vpeljati pa želite tudi varnejši način overjanja uporabnikov za aplikacijo od trenutnega načina z uporabniškim imenom in geslom. Prav tako vas skrbi, da utegnejo nepooblaščeni uporabniki prestreči informacije, ko se te prenašajo prek neoverjenega omrežja. Pomisleke imate tudi ob dejstvu, da utegnejo zastopniki te informacije deliti med seboj, ne da bi bili za to pooblaščeni.

Po krajšem razmisleku se odločite, da vam uporaba digitalnih potrdil lahko nudi varnost, ki jo potrebujete za zaščito zaupnih informacij, vnesenih v to aplikacijo in priklicanih iz nje. Uporaba potrdil vam omogoča, da z uporabo plasti zaščitenih vtičnic (SSL) zaščitite prenašanje podatkov o obrokih. Čeprav želite, da bi vsi posredniki uporabljali potrdila za dostop do aplikacije, veste, da bodo vaše podjetje in posredniki potrebovali nekaj časa, preden boste lahko dosegli ta

cilj. Poleg uporabe overjanja odjemalcev s potrdili načrtujete tudi, da boste ohranili trenutni način overjanja z uporabniškim imenom in geslom, saj SSL pri prenosu varuje zasebnost zaupnih podatkov.

Na osnovi tipa aplikacije in njenih uporabnikov ter vašega cilja v prihodnosti, ki je overjanje potrdil za vse uporabnike, se odločite, da boste za konfiguriranje SSL-a za vašo aplikacijo uporabili javno potrdilo znane službe za potrdila.

Prednosti scenarija

Ta scenarij ima naslednje prednosti:
- Uporaba digitalnih potrdil za konfiguriranje dostopa SSL do aplikacije za izračun stopenj zagotavlja, da so informacije, prenesene med strežnikom in odjemalcem, zaščitene in zasebne.
- Uporaba digitalnih potrdil, kadar je mogoča, za overjanje odjemalcev nudi varnejšo metodo preverjanja pristnosti uporabnikov. Tudi če uporaba digitalnih potrdil ni mogoča, seja SSL ščiti in ohranja zasebnost pri overjanju odjemalcev z imeni uporabnikov in gesli, tako da je izmenjava zaupnih podatkov varnejša.
- Uporaba *javnih* digitalnih potrdil za overjanje uporabnikov za aplikacije in podatke na način, opisan v tem scenariju, je dobra izbira v naslednjih okoliščinah:
  - Vaši podatki in aplikacije zahtevajo spremenljive stopnje zaščite.
  - Med overjenimi uporabniki je zelo gost promet.
  - Nudite javni dostop do aplikacij in podatkov, kot je na primer internetna spletna stran ali aplikacija ekstraneta.
  - Zaradi administrativnih razlogov, kot je veliko število zunanjih uporabnikov, ki dostopajo do vaših sredstev in aplikacij, ne želite voditi lastne službe za potrdila.
- Uporaba javnega potrdila pri konfiguriranju aplikacije za izračunavanje obrokov za SSL v tem scenariju zmanjša količino konfiguriranja, ki ga morajo opraviti uporabniki, da lahko do aplikacije dostopajo na zaščiten način. Večina odjemalske programske opreme vsebuje potrdila CA za večino dobro znanih služb za potrdila.

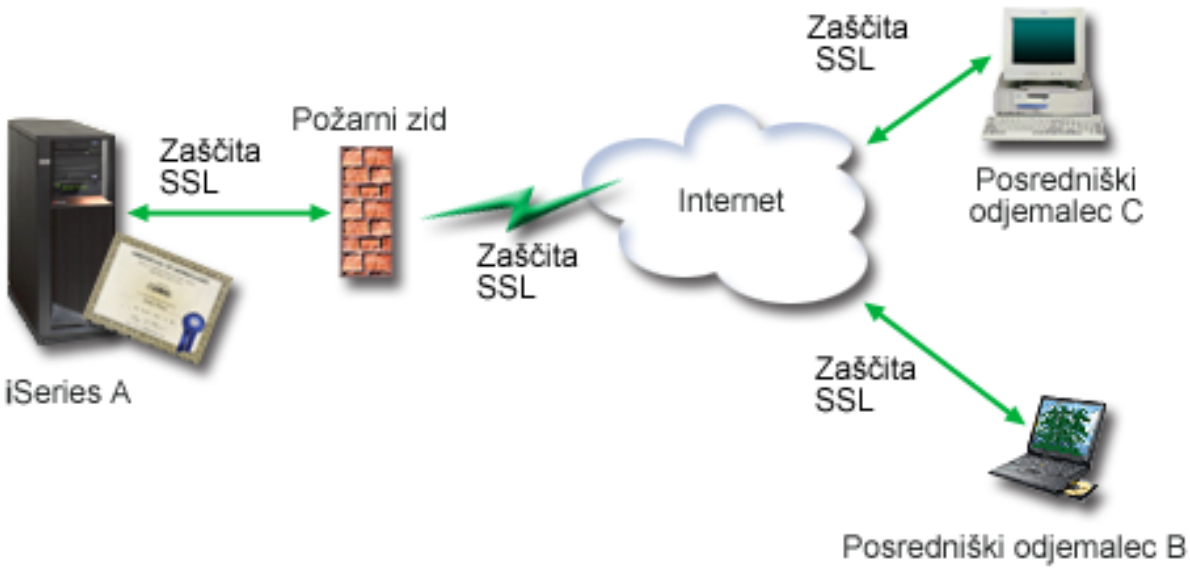
Cilji

V tem scenariju želi podjetje MojePod uporabiti digitalna potrdila za zaščito informacij o izračunavanju obrokov, ki jih njihova aplikacija posreduje overjenim uporabnikom. Podjetje prav tako želi uvesti varnejšo metodo overjanja uporabnikov, ki jim je dovoljen dostop do te aplikacije, ko je to mogoče.

Cilji tega scenarija so naslednji:
- Javna aplikacija podjetja za izračun obrokov mora uporabljati SSL, da zagotovi zasebnost podatkov, ki jih posreduje uporabnikom ter podatkov, ki jih od njih sprejema.
- Konfiguracija SSL mora biti dosežena z javnimi potrdili zelo znane javne internetne službe za potrdila (CA).
- Pooblaščeni uporabniki morajo za dostop do aplikacije v načinu SSL vnesti veljavno ime uporabnika in geslo. Dejansko mora biti pooblaščenim uporabnikom omogočena uporaba ena od dveh metod zaščitenega overjanja za dostop do aplikacije. Zastopniki morajo predložiti bodisi digitalno potrdilo znane službe za potrdila ali veljavno uporabniško ime in geslo, če potrdilo ni dosegljivo.

Podrobnosti

Naslednji zgled prikazuje konfiguracijo omrežja za ta scenarij:



Slika kaže naslednje informacije o situaciji za ta scenarij:

Javni strežnik podjetja – A
- Strežnik A je strežnik, ki gosti aplikacijo za izračun obrokov.
- Na strežniku A se izvaja OS/400 različice 5, izdaje 2 (V5R2) ali novejša.
- Na strežniku A je nameščen ponudnik šifriranega dostopa (5722–AC3).
- Strežnik A ima prav tako nameščena in konfigurirana Upravljalnik digitalnih potrdil(OS/400 možnost 34) ter IBM-ov Strežnik HTTP za iSeries (5722–DG1).
- Na strežniku A se izvaja aplikacija za izračunavanje obrokov, ki je konfigurirana tako, da:
  - Zahteva način SSL.
  - Pri overjanju samega sebe za inicializacijo seje SSL uporablja javno potrdilo znane službe za potrdila.
  - Zahteva overjanje uporabnika z imenom uporabnika ter geslom.
- Strežnik A predloži potrdilo zato, da inicializira sejo SSL, ko odjemalca B in C dostopata do aplikacije za izračunavanje obrokov.
- Po inicializaciji seje SSL strežnik A zahteva, da se odjemalca B in C izkažeta z veljavnim uporabniškim imenom in geslom, šele nato jima dovoli dostop do aplikacije za izračunavanje obrokov.

Odjemalski sistemi zastopnikov – Odjemalec B in odjemalec C
- Odjemalca B in C sta neodvisna zastopnika, ki dostopata do aplikacije za izračun obrokov.
- V programski opremi odjemalcev B in C je nameščena kopija potrdila znane službe za potrdila, ki je izdala potrdilo za aplikacijo.
- Odjemalca B in C dostopata do aplikacije za izračunavanje obrokov prek strežnika A, ki programski opremi njunega odjemalca predloži potrdilo, s katerim overi svojo istovetnost in inicializira sejo SSL.
- Programska oprema odjemalcev B in C je konfigurirana tako, da sprejema potrdila strežnika A v namen inicializiranja seje SSL.
- Po začetku seje SSL morata odjemalca B in C predložiti veljavni uporabniški imeni ter gesli, šele zatem jima strežnik A dodeli dostop do aplikacije.

Predpogoji in predpostavke.

Ta scenarij je odvisen od naslednjih predpogojev ter predpostavk:
1. Aplikacija za izračunavanje obrokov na strežniku A je generična aplikacija, ki jo je mogoče konfigurirati za uporabo SSL. Večina aplikacij, med njimi tudi veliko strežniških aplikacij, podpira SSL. Koraki konfiguriranja SSL se od aplikacije do aplikacije zelo razlikujejo. Zaradi tega ta scenarij ne podaja specifičnih navodil za konfiguriranje aplikacije za izračunavanje obrokov, da bo uporabljala SSL. Ta scenarij podaja navodila za konfiguriranje in upravljanje potrdil, ki je potrebno za vse aplikacije, da lahko uporabljajo SSL.

2. *Izbirno* lahko aplikacija izračuna obrokov nudi možnosti zahtevanja potrdil za overjanje odjemalcev. Scenarij podaja navodila o načinih uporabe Upravljalnika digitalnih potrdil (DCM) pri konfiguriranju zaupanja potrdilom za aplikacije, ki nudijo to podporo. Ker so konfiguracijski koraki za overjanje odjemalca zelo različni med aplikacijami, ta scenarij ne nudi specifičnih navodil za konfiguriranje overjanja odjemalca potrdila za aplikacijo izračuna obrokov.
3. Strežnik A ustreza zahtevam za namestitev in uporabo Upravljalnika digitalnih potrdil (DCM).
4. DCM na strežniku A še ni bil konfiguriran ali uporabljen.
5. Kdorkoli uporablja upravljalnik digitalnih potrdil za izvajanje nalog v tem scenariju, mora imeti posebna pooblastila *SECADM in *ALLOBJ za njihov profil uporabnika.
6. Na strežnik A ni nameščen IBM-ov Cryptographic Coprocessor.

Koraki konfiguriranja

Za izvršitev tega scenarija morate na strežniku A izvesti naslednje naloge:

1. Izpolnite obrazce za načrtovanje
2. Dokončajte vse predhodno zahtevane korake za namestitev in konfiguriranje potrebnih izdelkov
3. S pomočjo Upravljalnika digitalnih potrdil (DCM) izdelajte zahtevo po potrdilu za strežnik
4. Konfigurirajte aplikacijo, tako da bo uporabljala plast zaščitenih vtičnic (SSL)
5. Z uporabo Upravljalnika digitalnih potrdil uvozite in dodelite podpisana potrdila za strežnike ali odjemalce ID-ju vaše aplikacije
6. Če je potrebno, poženite aplikacijo v načinu SSL
7. **Izbirno**. S pomočjo DCM definirajte seznam zaupanja vrednih služb za potrdila, s čimer omogočite overjanje odjemalcev na osnovi potrdil za aplikacije, ki nudijo to podporo.

Opomba: Situacija, ki jo opisuje ta scenarij, ne zahteva, da aplikacija za izračunavanje obrokov odjemalce overja s pomočjo potrdil. Številne aplikacije nudijo podporo za overjanje odjemalcev s potrdili, način konfiguriranja te podpore pa se med aplikacijami zelo razlikuje. Ta neobvezna naloga je navedena, da bi bolje razumeli, kako uporabiti upravljalnik digitalnih potrdil za omogočanje zaupanja potrdil za overjanje odjemalcev kot osnove za konfiguriranje podpore overjanja potrdil odjemalca, ki jo nudi vaša aplikacija.

Podrobnosti konfiguriranja

Izpolnite naslednje korake za uporabo potrdil za konfiguriranje zaščitenega javnega dostopa do aplikacij in virov, kot jih opisuje ta scenarij.

1. korak: Izpolnite obrazce za načrtovanje

Naslednji obrazci za načrtovanje prikazujejo informacije, ki jih morate zbrati, ter odločitve, ki jih morate sprejeti za pripravo izvedbe digitalnih potrdil, ki jih opisuje ta scenarij. Če želite zagotoviti uspešno izvedbo, morate na vse predhodno zahtevane postavke odgovoriti z Da, preden pa pričnete z izvajanjem konfiguracijskih nalog, morate zbrati tudi vse potrebne informacije.

Tabela 1. Obrazec za načrtovanje predpogojev za izvedbo potrdil

Obrazec s predpogoji	Odgovori
Je vaš OS/400 V5R2 (5722-SS1) ali novejši?	Da
Je v vašem sistemu nameščen ponudnik šifriranega dostopa (5722-AC3)?	Da
Je v vašem sistemu nameščena možnost 34 OS/400?	Da
Je v sistemu nameščenIBM-ov strežnik HTTP za iSeries (5722–DG1) in zagnan primerek upravnega strežnika?	Da

Tabela 1. Obrazec za načrtovanje predpogojev za izvedbo potrdil (nadaljevanje)

Obrazec s predpogoji	Odgovori
Je TCP konfiguriran tako, da lahko do upravljalnika digitalnih potrdil dostopate s pomočjo spletnega pregledovalnika in primerka upravnega strežnika za strežnik HTTP?	Da
Imate posebna pooblastila *SECADM in *ALLOBJ?	Da

Če želite izvesti potrebne konfiguracijske naloge, morate o izvedbi vašega digitalnega potrdila zbrati naslednje informacije:

Tabela 2. Obrazec za načrtovanje konfiguriranja izvedbe potrdila

Obrazec za konfiguriranje za strežnika A	Odgovori
Boste vodili lastno službo za potrdila ali boste potrdila za aplikacijo pridobili pri javni službi za potrdila?	Pridobivanje potrdil pri javni službi za potrdila
Ali je strežnik A gostitelj aplikacij, ki jih želite omogočiti za SSL?	Da
Katero razločevalno ime želite uporabiti za zahtevo po podpisovanju potrdil (CSR), ki jo izdelujete s pomočjo Upravljalnika digitalnih potrdil? • **Velikost ključa**: označuje moč šifriranih ključev za potrdilo. • **Oznaka potrdila**: z unikatnim znakovnim nizom označuje potrdilo. • **Splošno ime**: označuje lastnika potrdila, pri čemer lahko gre za osebo, objekt ali aplikacijo; del razločevalnega imena predmeta za potrdilo. • **Enota organizacije**: označuje organizacijski oddelek ali področje za aplikacijo, ki bo uporabljala to potrdilo. • **Ime organizacije**: označuje vaše podjetje ali oddelek za aplikacijo, ki bo uporabljala to potrdilo. • **Kraj ali mesto**: označuje mesto ali oznako kraja za vašo organizacijo. • **Dežela ali provinca**: označuje deželo ali provinco, v kateri boste uporabljali to potrdilo. • **Država ali regija**: z dvema črkama označuje državo ali regijo, v kateri boste uporabljali to potrdilo.	**Velikost ključa**: 1024 **Oznaka potrdila**: MojePod_public_cert **Splošno ime**: mojepod_rate_server@mojepod.com **Enota organizacije**: Rate dept **Ime organizacije**: mojepod **Kraj ali mesto**: Any_city **Dežela ali provinca**: Any **Država ali regija**: ZZ
Kakšen je ID aplikacije Upravljalnika digitalnih potrdil za aplikacijo, ki jo želite konfigurirati za uporabo SSL?	mcyo_agent_rate_app
Želite konfigurirati aplikacijo, ki je omogočena za uporabo SSL, da bo za overjanje odjemalcev uporabljala potrdila? Če želite, katere službe za potrdila želite dodati v seznam zaupanja vrednih služb za potrdila te aplikacije?	Ne

2. korak: Dokončanje vseh predhodno zahtevanih nalog za namestitev potrebnih izdelkov

Dokončati morate vse predhodno zahtevane naloge za namestitev in konfiguriranje potrebnih izdelkov, šele nato lahko pričnete izvajati specifične naloge konfiguriranja za izvršitev tega scenarija.

3. korak: Izdelava strežnika ali zahteve po potrdilu odjemalca

Če želite začeti postopek uporabe plasti zaščitenih vtičnic (SSL) za zaščito podatkovne komunikacije aplikacije, kot jo opisuje ta scenarij, morate najprej pridobiti digitalno potrdilo od javne službe za potrdila (CA). Uporabite Upravljalnik digitalnih potrdil (DCM) za izdelavo informacij, ki jih za izdajo potrdila zahteva javna služba za potrdila.

Če želite začeti postopek pridobivanja potrdila, naredite naslednje:
1. Zaženite DCM.
2. V oknu za usmerjanje Upravljalnika digitalnih potrdil izberite **Izdelaj nov prostor za potrdila**, s čimer boste zagnali vodeno nalogo, v kateri boste izpolnili niz obrazcev. Ti obrazci vas bodo vodili skozi postopek izdelave prostora za potrdila in potrdila, ki ga bodo lahko uporabile vaše aplikacije za seje SSL.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
3. Kot prostor za potrdila izberite ***SYSTEM** in kliknite **Nadaljuj**.
4. Za izdelavo potrdila kot dela izdelave prostora za potrdila *SYSTEM izberite **Da** in kliknite **Nadaljuj**.
5. Kot podpisnika novega potrdila izberite **VeriSign ali drugo internetno službo za potrdila (CA)** in kliknite **Nadaljuj**. Prikazali boste obrazec, na katerem lahko podate določilne informacije za novo potrdilo.
6. Izpolnite obrazec in kliknite **Nadaljuj**. Prikazala se bo potrditvena stran z zahtevanimi podatki potrdila, ki jih morate posredovati javni službi za potrdila (CA), ki bo izdala vaše potrdilo. Podatki CSR (zahteva po podpisovanju potrdila) so sestavljeni iz javnega ključa, razločevalnega imena ter drugih informacij, ki ste jih podali za novo potrdilo.
7. Previdno prekopirajte podatke CSR in jih prilepite v obrazec za potrdilo ali v ločeno datoteko, ki jo potrebuje javna služba za potrdila, če zahtevate potrdilo. Uporabiti morate vse podatke CSR, vključno z vrsticama Begin in End New Certificate Request. **Opomba:** Ko zapustite to stran, so podatki izgubljeni in jih ni mogoče obnoviti.
8. Obrazec ali datoteko pošljite službi za potrdila, ki ste jo izbrali za izdajanje in podpišite potrdilo.
9. Preden nadaljujete z naslednjim korakom v scenariju, počakajte, da služba za potrdila vrne podpisano, dokončano potrdilo.

Ko služba za potrdila vrne podpisano dokončano potrdilo, lahko konfigurirate aplikacijo za uporabo SSL, uvozite potrdilo v prostor za potrdila *SYSTEM in ga dodelite vaši aplikaciji za uporabo s SSL.

4 korak: Konfiguriranje aplikacije za uporabo SSL

Ko prejmete podpisano potrdilo od javne službe za potrdila (CA), lahko nadaljujete s postopkom omogočanja komunikacij SSL (plast zaščitenih vtičnic) za vašo javno aplikacijo. Pred delom s podpisanim potrdilom morate aplikacijo konfigurirati za uporabo SSL. Nekatere aplikacije, kot je na primer Strežnik HTTP za iSeries ustvarijo unikaten ID aplikacije, ki ga pri konfiguriranju aplikacije za uporabo SSL registrirajo z Upravljalnikom digitalnih potrdil (DCM). ID aplikacije morate poznati, preden lahko DCM uporabite za dodelitev podpisanega potrdila aplikaciji in dokončati postopek konfiguriranja SSL.

Način konfiguriranja aplikacije za uporabo SSL se med aplikacijami razlikuje. Ta scenarij za aplikacijo za izračunavanje obrokov ne predvideva specifičnega vira, saj lahko MojePod aplikacijo posreduje svojim zastopnikom na mnogo načinov.

| Če želite aplikacijo konfigurirati za uporabo SSL, sledite navodilom, ki jih nudi dokumentacija vaše aplikacije. Prav
| tako se lahko naučite več o konfiguriranju splošnih IBM-ovih aplikacij za uporabo SSL, tako da pregledate poglavje
| Plast zaščitenih vtičnic (SSL) v Informacijskem centru iSeries.

| Ko dokončate konfiguriranje SSL za vašo aplikacijo, lahko zanjo konfigurirate še podpisano javno potrdilo, da bo
| aplikacija lahko inicializirala seje SSL.

5. korak: Uvažanje in dodeljevanje podpisanih javnih potrdil

Ko konfigurirate aplikacijo za uporabo SSL, lahko uporabite upravljalnik digitalnih potrdil za uvoz vašega podpisanega potrdila in njegovo dodelitev aplikaciji.

Če želite uvoziti potrdilo in ga dodeliti vaši aplikaciji, da dokončate postopek konfiguriranja SSL, naredite naslednje:
1. Zaženite DCM.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***SYSTEM**.

3. Ko se prikaže stran **Prostor za potrdila in geslo**, vnesite geslo, ki ste ga za prostor za potrdila podali pri njegovi izdelavi in kliknite **Nadaljuj**.
4. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
5. S seznama nalog izberite **Uvozi potrdilo**, da boste začeli postopek uvažanja podpisanega potrdila v prostor za potrdila *SYSTEM.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
6. Nato s seznama nalog za **upravljanje potrdil** izberite možnost **Dodeli potrdilo**, da prikažete seznam potrdil za trenutni prostor za potrdila.
7. S seznama izberite vaše potrdilo in kliknite **Dodeli k aplikacijam**, da prikažete seznam definicij aplikacij za trenutni prostor za potrdila.
8. S seznama izberite vašo aplikacijo in kliknite **Nadaljuj**. Prikaže se stran s potrditvenim sporočilom za izbiro dodelitve ali pa sporočilo o napaki, če pride do napake.

Ko končate te naloge, lahko zaženete aplikacijo v načinu SSL ter začnete ščititi zasebnost podatkov, ki jo nudi.

Korak 6: Zagon aplikacije v načinu SSL

Ko dokončate postopek uvoza in dodeljevanja potrdila vaši aplikaciji, boste morda morali končati in znova zagnati aplikacijo v načinu SSL. To je potrebno v nekaterih primerih, ker aplikacija morda ne more določiti, da obstaja dodelitev potrdila, medtem ko se aplikacija izvaja. Preglejte dokumentacijo vaše aplikacije, da ugotovite, ali morate na novo zagnati aplikacijo, ali pa najdete druge specifične informacije o zagonu aplikacije v načinu SSL.

| Če želite potrdila uporabljati za overjanje odjemalcev, lahko za aplikacijo definirate seznam zaupanja vrednih služb za
| potrdila.

7. korak: (izbiren): Definiranje seznama zaupanja vrednih služb za potrdila za aplikacijo, ki zahteva potrdila za overjanje odjemalcev

Aplikacije, ki podpirajo uporabo potrdil za overjanje odjemalca med sejo plasti zaščitenih vtičnic (SSL), morajo določiti, ali bodo sprejele potrdilo kot veljaven dokaz identitete. Eden od kriterijev, ki ga uporablja aplikacija za overjanje potrdila, je, ali aplikacija zaupa službi za potrdila (CA), ki je izdala potrdilo.

| Situacija, ki jo opisuje ta scenarij, ne zahteva, da aplikacija za izračunavanje obrokov za overjanje odjemalcev
| uporablja potrdila, temveč da je aplikacija za overjanje sposobna sprejeti potrdila, če so ta na voljo. Številne aplikacije
| nudijo podporo potrdilom za overjanje odjemalcev, način konfiguriranja te podpore pa se od aplikacije do aplikacije
| zelo razlikuje. Ta neobvezna naloga je navedena, da bi bolje razumeli, kako uporabiti upravljalnik digitalnih potrdil za
| omogočanje zaupanja potrdil za overjanje odjemalcev kot osnove za konfiguriranje aplikacij za uporabo potrdil za
| overjanje odjemalcev.

Preden lahko za aplikacijo definirate seznam overjenih služb za potrdila, mora biti izpolnjenih več pogojev:
- Aplikacija mora podpirati uporabo potrdil za overjanje odjemalca.
- Definicija upravljalnika digitalnih potrdil za aplikacijo mora podajati, da aplikacija uporablja seznam overjenih služb za potrdila.

Če definicija aplikacije podaja, da aplikacija uporablja seznam overjenih služb za potrdila, morate definirati seznam, preden lahko aplikacija uspešno overi potrdilo odjemalca. S tem zagotovite, da bo aplikacija preverjala veljavnost samo tistih potrdil služb za potrdila, ki ste jih podali kot overjene. Če uporabniki ali aplikacija odjemalca predložijo potrdilo službe za potrdila, ki na seznamu overjenih služb za potrdila ni podana kot overjena, je aplikacija ne bo sprejela kot osnovo za overjanje.

Če želite DCM uporabiti za definiranje seznama overjenih služb za potrdila za aplikacijo, naredite naslednje:
1. Zaženite DCM.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***SYSTEM**.

3. Ko se prikaže stran **Prostor za potrdila in geslo**, vnesite geslo, ki ste ga za prostor za potrdila podali pri njegovi izdelavi in kliknite **Nadaljuj**.
4. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
5. S seznama nalog izberite **Nastavi status CA**, da prikažete seznam potrdil služb za potrdila.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
6. S seznama izberite eno ali več potrdil službe za potrdila, ki jim aplikacija zaupa in kliknite **Omogoči**, da prikažete seznam aplikacij, ki uporabljajo seznam zaupanja vrednih služb za potrdila.
7. S seznama izberite aplikacijo, ki mora v svoj seznam zaupanja vrednih služb za potrdila dodati izbrano službo za potrdila in kliknite **Potrdi**. Na vrhu strani se prikaže sporočilo, ki kaže, da bodo izbrane aplikacije zaupale službi za potrdila ter potrdilom, ki jih izda.

Zdaj lahko konfigurirate vašo aplikacijo, da za overjanje odjemalca zahteva potrdila. Sledite navodilom, ki so na voljo v dokumentaciji vaše aplikacije.

Scenarij: Uporaba potrdil za notranje overjanje

Situacija

Ste skrbnik omrežja za podjetje (MojePod), katerega kadrovska služba se ukvarja z vprašanji, kot so pravne zadeve in zasebnost listin. Zaposleni v podjetju so zahtevali, da želijo neposredno dostopati do svojih informacij o osebnih ugodnostih ter zdravstvenem zavarovanju. Podjetje se je na to zahtevo odzvalo tako, da je izdelalo notranjo spletno stran, na kateri so te informacije na razpolago uslužbencem. Odgovorni ste za upravljanje notranje spletne strani, ki se izvaja na IBM-ovem strežniku HTTP za iSeries (poganja ga Apache).

Ker so zaposleni locirani na dveh geografsko ločenih pisarnah in nekateri zaposleni zelo pogosto potujejo, vas skrbi ohranjanje zasebnosti teh informacij, medtem ko potujejo prek interneta. Ker želite omejiti dostop do podatkov podjetja, uporabnike ponavadi overjate z uporabniškimi imeni in gesli. Zaradi zaupne in zasebne narave teh podatkov ste prišli do spoznanja, da omejevanje dostopa do njih z uporabo overjanja z geslom morda ni zadostno. Lahko se namreč zgodi, da uporabniki gesla souporabljajo, pozabijo ali celo ukradejo.

Po krajšem razmisleku se odločite, da vam uporaba digitalnih potrdil lahko nudi zaščito, ki jo potrebujete. S pomočjo potrdil lahko uporabite plast zaščitenih vtičnic (SSL) za zaščito prenosa podatkov. Dodatno lahko z uporabo potrdil namesto gesel varneje overite uporabnike ter omejite informacije kadrovske službe, do katerih lahko dostopajo.

Zato se odločite, da boste vzpostavili lastno lokalno službo za potrdila ter izdali potrdila vsem zaposlenim in jih pripravili, da svoja potrdila povežejo s svojimi uporabniškimi profili. Ta vrsta izvedbe zasebnih potrdil omogoča strožji nadzor nad dostopom do občutljivih podatkov, kot tudi nadzorovanje zasebnosti podatkov s pomočjo SSL. Tako ste z lastnoročnim izdajanjem potrdil povečali možnost, da bodo podatki ostali zaščiteni in dostopni le za posameznike.

Prednosti scenarija

Ta scenarij ima naslednje prednosti:
- Z uporabo digitalnih potrdil za konfiguriranje dostopa SSL do vašega spletnega strežnika za vse zaposlene je zagotovljeno, da so informacije, ki se prenašajo med strežnikom in odjemalcem,zaščitene in zasebne.
- Uporaba digitalnih potrdil za overjanje odjemalcev nudi varnejšo metodo preverjanja pristnosti uporabnikov.
- Uporaba *zasebnih* digitalnih potrdil za overjanje uporabnikov za aplikacije in podatke je dobra izbira v naslednjih okoliščinah:
  - Potrebujete visoko stopnjo zaščite, še posebej glede overjanja uporabnikov.
  - Posameznikom, ki jim izdate potrdila, zaupate.
  - Vaši uporabniki že imajo uporabniške profile, s katerimi nadzorujejo svoj dostop do aplikacij in podatkov.
  - Želite voditi svojo lastno službo za potrdila (CA).
- Uporaba zasebnih potrdil za overjanje odjemalcev vam omogoča preprostejšo povezavo potrdila z uporabniškim profilom pooblaščenega uporabnika. Ta povezava potrdila s profilom uporabnika omogoča strežniku HTTP, da med

overjanjem določi profil uporabnika lastnika potrdila. Strežnik HTTP lahko nato preklopi nanj in se izvaja pod tem uporabniškim profilom ali na osnovi informacij v uporabniškem profilu izvaja dejanja za tega uporabnika.

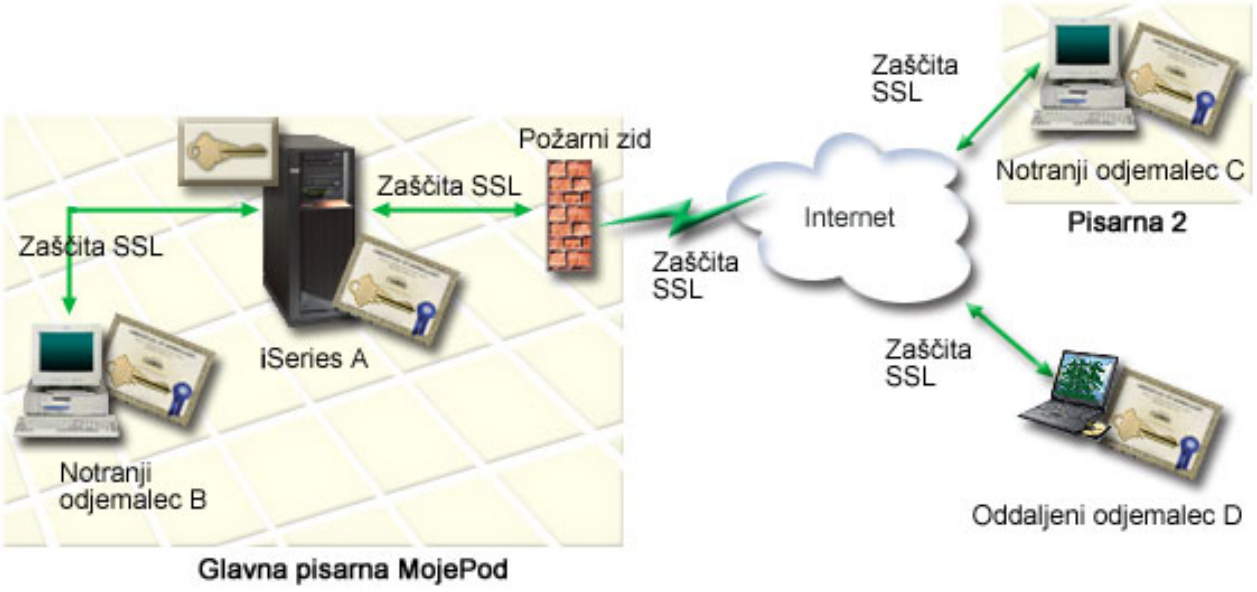
Cilji

V tem scenariju želi podjetje MojePod uporabiti digitalna potrdilo za zaščito zaupnih osebnih informacij, ki jih njihova notranja spletna stran za vse zaposlene nudi zaposlenim v podjetju. Podjetje prav tako želi vpeljati varnejšo metodo overjanja uporabnikov, ki jim je dovoljen dostop do te spletne strani.

Cilji tega scenarija so naslednji:
- Interna spletna stran podjetja za vse zaposlene mora za zaščito podatkov, ki jih nudi uporabnikom, uporabljati SSL.
- Konfiguracija SSL mora biti dosežena z zasebnimi potrdili interne lokalne službe za potrdila (CA).
- Pooblaščeni uporabniki morajo za dostop do spletne strani za zaposlene v načinu SSL predložiti veljavno potrdilo.

Podrobnosti

Naslednji zgled prikazuje konfiguracijo omrežja za ta scenarij:



Slika kaže naslednje informacije o situaciji za ta scenarij:

Spletni strežnik za zaposlene podjetja – Strežnik A
- Strežnik A je strežnik, ki gosti spletno aplikacijo podjetja za zaposlene.
- Na strežniku A se izvaja OS/400 različica 5 izdaja 2 (V5R2) ali novejši.
- Na strežniku A je nameščen ponudnik šifriranega dostopa (5722–AC3).
- Strežnik A ima prav tako nameščena in konfigurirana Upravljalnik digitalnih potrdil(OS/400 možnost 34) ter IBM-ov Strežnik HTTP za iSeries (5722–DG1).
- Na strežniku A se izvaja aplikacija za zaposlene, ki je konfigurirana tako, da:
  - Zahteva način SSL.
  - Uporablja zasebno potrdilo lokalne službe za potrdila (CA) za konfiguriranje SSL.
  - Zahteva potrdila za overjanje odjemalca.
- Strežnik A predloži potrdilo zato, da inicializira sejo SSL, ko odjemalci B, C in D dostopajo do aplikacije.
- Po inicializaciji seje SSL strežnik A zahteva, da odjemalci B, C in D predložijo veljavno potrdilo, šele nato jim dodeli dostop do aplikacije za zaposlene podjetja. Ta izmenjava potrdil je transparentna uporabnikom odjemalcev B, C in D.

Odjemalski sistemi zaposlenih – odjemalec B, odjemalec C in odjemalec D
- Odjemalec B je uslužbenec, ki dela v glavni pisarni podjetja MojePod, v kateri se nahaja strežnik A.

- Odjemalec C je zaposleni, ki dela v sekundarni pisarni MojePod, ki je geografsko ločena od glavne pisarne.
- Odjemalec D je uslužbenec, ki dela na daljavo in je pogosto na službenih potovanjih, zato mora imeti možnost zaščitenega dostopa do spletne strani za zaposlene, ne glede na to kje se nahaja.
- Odjemalci B, C in D so zaposleni podjetja, ki dostopajo do aplikacije kadrovske službe.
- Odjemalci B, C in D imajo kopijo potrdil lokalne službe za potrdila, ki je izdala potrdilo aplikacije, ki je nameščena v njihovi odjemalski programski opremi.
- Odjemalci B, C in D do aplikacije za zaposlene dostopajo prek strežnika A, ki programski opremi njihovega odjemalca predloži potrdilo, s katerim overi svojo istovetnost in inicializira sejo SSL.
- Programska oprema odjemalcev B, C in D je konfigurirana tako, da sprejema potrdila s strežnika A in seja SSL se začne.
- Po začetku seje SSL morajo odjemalci B, C in D predložiti veljavno potrdilo, šele nato jim strežnik A dodeli dostop do aplikacije in pripadajočih sredstev.

Predpogoji in predpostavke.

Ta scenarij je odvisen od naslednjih predpogojev ter predpostavk:

1. IBM-ov strežnik HTTP za iSeries (poganja ga Apache) zažene aplikacijo za vse zaposlene na strežniku A. Ta scenarij ne podaja *specifičnih* navodil za konfiguriranje Strežnika HTTP za uporabo SSL. Ta scenarij podaja navodila za konfiguriranje in upravljanje potrdil, ki je potrebno za vse aplikacije, da lahko uporabljajo SSL.
2. Strežnik HTTP nudi možnosti za zahtevanje potrdil za overjanje odjemalcev. Ta scenarij podaja navodila, s pomočjo katerih je mogoče z uporabo Upravljalnika digitalnih potrdil (DCM) konfigurirati zahteve upravljanja potrdil za ta scenarij. vendar ne nudi *podrobnih* konfiguracijskih korakov za konfiguriranje overjanja odjemalcev za strežnik HTTP.
3. Strežnik HTTP za vse zaposlene na strežniku A že uporablja overjanje z geslom.
4. Strežnik A ustreza zahtevam za namestitev in uporabo Upravljalnika digitalnih potrdil (DCM).
5. DCM na strežniku A še ni bil konfiguriran ali uporabljen.
6. Kdorkoli uporablja upravljalnik digitalnih potrdil za izvajanje nalog v tem scenariju, mora imeti posebna pooblastila *SECADM in *ALLOBJ za njihov profil uporabnika.
7. Na strežnik A IBM-ov Cryptographic Coprocessor ni nameščen.

Koraki konfiguriranja

Za izvedbo tega scenarija morate dokončati dve skupini nalog: Ena od njiju vam omogoča, da nastavite aplikacijo za vse zaposlene na strežniku A tako, da bo uporabljala SSL in za overjanje uporabnikov zahtevala potrdila. Druga skupina nalog omogoča uporabnikom na odjemalcih B, C in D, da sodelujejo v sejah SSL z aplikacijo za vse zaposlene in pridobijo potrdila za overjanje uporabnika.

Koraki nalog za aplikacijo spletnega strežnika za vse zaposlene

Za izvršitev tega scenarija morate na strežniku A izvesti naslednje naloge:

1. Izpolnite obrazce za načrtovanje scenarija
2. Dokončajte vse predhodno zahtevane korake za namestitev in konfiguriranje potrebnih izdelkov
3. Konfigurirajte strežnik HTTP za vse zaposlene, da bo uporabljal SSL, in si zabeležite ID aplikacije za primerek strežnika
4. Z uporabo Upravljalnika digitalnih potrdil izdelajte in vodite lokalno službo za potrdila
5. Konfigurirajte overjanje odjemalcev za spletni strežnik za vse zaposlene.
6. Zaženite strežnik HTTP za zaposlene v načinu SSL .

Koraki nalog za konfiguriranje odjemalca

Če želite izvršiti ta scenarij, mora vsak uporabnik (odjemalci B, C in D), ki dostopa do spletnega strežnika za zaposlene na strežniku A opraviti naslednje naloge:

7. Namestiti kopijo potrdila lokalne službe za potrdila v pregledovalnik
8. Od lokalne službe za potrdila zahtevati potrdilo

Podrobnosti konfiguriranja

Če želite uporabljati potrdila za konfiguriranje zaščitenega dostopa SSL do notranjih aplikacij in sredstev ter overjati uporabnike na način, opisan v tem scenariju, opravite naslednje naloge.

1. korak: Izpolnitev obrazcev za načrtovanje

Naslednji obrazci za načrtovanje prikazujejo informacije, ki jih morate zbrati, ter odločitve, ki jih morate sprejeti za pripravo izvedbe digitalnih potrdil, ki jih opisuje ta scenarij. Če želite zagotoviti uspešno izvedbo, morate na vse predhodno zahtevane postavke odgovoriti z Da, preden pa pričnete z izvajanjem konfiguracijskih nalog, morate zbrati tudi vse potrebne informacije.

Tabela 3. Obrazec za načrtovanje predpogojev za izvedbo potrdil

Obrazec s predpogoji	**Odgovori**
Je vaš OS/400 V5R2 (5722-SS1) ali novejši?	Da
Je v vašem sistemu nameščen ponudnik šifriranega dostopa (5722-AC3)?	Da
Je v vašem sistemu nameščena možnost 34 OS/400?	Da
Je v sistemu nameščenIBM-ov strežnik HTTP za iSeries (5722–DG1) in zagnan primerek upravnega strežnika?	Da
Je TCP konfiguriran tako, da lahko do upravljalnika digitalnih potrdil dostopate s pomočjo spletnega pregledovalnika in primerka upravnega strežnika za strežnik HTTP?	Da
Imate posebna pooblastila *SECADM in *ALLOBJ?	Da

Če želite izvesti potrebne konfiguracijske naloge, morate o izvedbi vašega digitalnega potrdila zbrati naslednje informacije:

Tabela 4. Obrazec za načrtovanje konfiguriranja izvedbe potrdila

Obrazec za konfiguriranje za strežnika A	**Odgovori**
Boste vodili lastno službo za potrdila ali boste potrdila za aplikacijo pridobili pri javni službi za potrdila?	Izdelava lokalne službe za potrdila za izdajanje potrdil
Ali je strežnik A gostitelj aplikacij, ki jih želite omogočiti za SSL?	Da
Katero razločevalno ime želite uporabiti za lokalno službo za potrdila? • **Velikost ključa**: označuje moč šifriranih ključev za potrdilo. • **Ime službe za potrdila (CA)**: označuje službo za potrdila in postane splošno ime za potrdila te službe in DN izdajatelja za potrdila, ki jih izda služba za potrdila. • **Enota organizacije**: označuje organizacijski oddelek ali področje za aplikacijo, ki bo uporabljala to potrdilo. • **Ime organizacije**: označuje vaše podjetje ali oddelek za aplikacijo, ki bo uporabljala to potrdilo. • **Kraj ali mesto**: označuje mesto ali oznako kraja za vašo organizacijo. • **Dežela ali provinca**: označuje deželo ali provinco, v kateri boste uporabljali to potrdilo. • **Država ali regija**: z dvema črkama označuje državo ali regijo, v kateri boste uporabljali to potrdilo. • **Obdobje veljavnosti službe za potrdila**: podaja število dni, ko je služba za potrdila veljavna	**Velikost ključa**: 1024 **Ime službe za potrdila (CA)**: Mojepod_CA@mojepod.com **Enota organizacije**: Rate dept **Ime organizacije**: mojepod **Kraj ali mesto**: Any_city **Dežela ali provinca**: Any **Država ali regija**: ZZ **Obdobje veljavnosti službe za potrdila**: 1095

Tabela 4. Obrazec za načrtovanje konfiguriranja izvedbe potrdila (nadaljevanje)

Obrazec za konfiguriranje za strežnika A	Odgovori
Želite nastaviti podatke načel lokalne službe za potrdila tako, da ji dopustite izdajanje uporabniških potrdil za overjanje odjemalcev?	Da
Katero razločevalno ime želite uporabiti za potrdilo strežnika, ki ga izda lokalna služba za potrdila? • **Velikost ključa**: označuje moč šifriranih ključev za potrdilo. • **Oznaka potrdila**: z unikatnim znakovnim nizom določa potrdilo. • **Splošno ime**: označuje lastnika potrdila, pri čemer lahko gre za osebo, objekt ali aplikacijo; del razločevalnega imena predmeta za potrdilo. • **Enota organizacije**: označuje organizacijski oddelek ali področje za aplikacijo, ki bo uporabljala to potrdilo. • **Ime organizacije**: označuje vaše podjetje ali oddelek za aplikacijo, ki bo uporabljala to potrdilo. • **Kraj ali mesto**: označuje mesto ali oznako kraja za vašo organizacijo. • **Dežela ali provinca**: označuje deželo ali provinco, v kateri boste uporabljali to potrdilo. • **Država ali regija**: z dvema črkama označuje državo ali regijo, v kateri boste uporabljali to potrdilo.	**Velikost ključa**: 1024 **Oznaka potrdila**: Mojepod_public_cert **Splošno ime**: mojepod_rate_server@mojepod.com **Enota organizacije**: Rate dept **Ime organizacije**: mojepod **Kraj ali mesto**: Any_city **Dežela ali provinca**: Any **Država ali regija**: ZZ
Kakšen je ID aplikacije Upravljalnika digitalnih potrdil za aplikacijo, ki jo želite konfigurirati za uporabo SSL?	mcyo_agent_rate_app
Želite konfigurirati aplikacijo, ki je omogočena za uporabo SSL, da bo za overjanje odjemalcev uporabljala potrdila? Če želite, katere službe za potrdila želite dodati v seznam zaupanja vrednih služb za potrdila te aplikacije?	Da Mojepod_CA@mojepod.com

2. korak: Dokončanje vseh predhodno zahtevanih nalog za namestitev potrebnih izdelkov

Dokončati morate vse predhodno zahtevane naloge za namestitev in konfiguriranje potrebnih izdelkov, šele nato lahko pričnete izvajati specifične naloge konfiguriranja za izvršitev tega scenarija.

3. korak: Konfiguriranje strežnika HTTP za zaposlene, da uporablja SSL

Konfiguriranje plasti zaščitenih vtičnic (SSL) za strežnik HTTP za zaposlene (poganja ga Apache) na strežniku A vključuje različne naloge, ki so odvisne od trenutne konfiguracije strežnika.

Če želite konfigurirati strežnik za uporabo SSL, upoštevajte naslednje korake:

1. Zaženite vmesnik za upravljanje strežnika HTTP.
2. Če želite delati z določenim strežnikom HTTP, izberite jezičke **Upravljanje —> Vsi strežniki —> Vsi strežniki HTTP**, da prikažete seznam vseh konfiguriranih strežnikov HTTP.
3. Izberite želen strežnik s seznama in kliknite **Podrobnosti upravljanja**.
4. V oknu za usmerjanje izberite **Zaščita**.
5. V obrazcu izberite jeziček **SSL z overjanjem potrdil**.
6. V polju **SSL** izberite Omogočeno.
7. V polju **Ime aplikacije potrdila strežnika** podajte ID aplikacije, pod katerim je znan ta primerek strežnika, ali pa ga izberite s seznama. ID aplikacije ima obliko QIBM_HTTP_SERVER_[ime_strežnika], na primer, QIBM_HTTP_SERVER_MOJEPODTEST. **Opomba:** Zapomnite si ID aplikacije, saj ga boste morali znova izbrati v Upravljalniku digitalnih potrdil.

Več informacij o splošni konfiguraciji, potrebni za strežnik HTTP pri uporabi SSL najdete v temi Strežnik HTTP za iSeries, še posebej v scenariju: JKL na strežniku HTTP (poganja ga Apache) omogoča zaščito s plastjo zaščitenih vtičnic (SSL). Ta scenarij navaja vse korake, potrebne za izdelavo navideznega gostitelja ter za njegovo konfiguriranje za uporabo SSL, pri tem pa zajema naslednje naloge:

1. Nastavitev navideznega gostitelja, ki temelji na imenu.
2. Nastavitev spremljanja za navideznega gostitelja
3. Nastavitev imenikov navideznega gostitelja.
4. Nastavitev zaščite z geslom prek osnovnega overjanja.
5. Omogočitev SSL za navideznega gostitelja

Dodatne informacije o konfiguriranju trenutnih in prihodnjih različic strežnika HTTP za iSeries so vam na voljo v temi Strežnik HTTP zaiSeries.

Ko strežnik HTTP konfigurirate, da uporablja SSL, lahko z uporabo Upravljalnika digitalnih potrdil konfigurirate še podporo potrdilom, ki jo potrebujete za SSL in overjanje odjemalcev.

4. korak: Izdelava in vodenje lokalne službe za potrdila

Ko konfigurirate strežnik HTTP kadrovske službe za uporabo plasti zaščitenih vtičnic (SSL), morate konfigurirati potrdilo za strežnik, ki bo uporabljeno za začetek SSL. Na osnovi ciljev za ta scenarij ste se odločili za osnovanje in vodenje lokalne službe za pooblastila (CA) za izdajanje potrdil strežniku.

Če Upravljalnik digitalnih potrdil uporabljate za izdelavo lokalne službe za potrdila, boste vodeni skozi postopek, ki zagotavlja, da konfigurirate vse kar potrebujete za omogočanje SSL vaši aplikaciji. V to je zajeto tudi dodeljevanje potrdila, ki ga je izdala lokalna služba za potrdila, vaši aplikaciji spletnega strežnika. Lokalno službo za potrdila dodate v seznam zaupanja vrednih služb za potrdila te aplikacije. Ker je lokalna služba za potrdila na seznamu aplikacije, je zagotovljeno, da lahko aplikacija prepozna in overi uporabnike, ki predložijo potrdila, ki jih izda lokalna služba za potrdila.

Če želite upravljalnik digitalnih potrdil uporabiti za izdelavo in delovanje lokalne službe za potrdila in izdajanje potrdil aplikaciji strežnika kadrovske službe, naredite naslednje:

1. Zaženite DCM.
2. V oknu za usmerjanje Upravljalnika digitalnih potrdil izberite **Izdelaj službo za potrdila (CA)**, da boste prikazali niz obrazcev. Ti obrazci vas bodo vodili skozi postopek izdelave lokalne službe za potrdila in dokončanje drugih nalog, ki jih morate opraviti za začetek uporabe digitalnih potrdil za SSL, podpisovanje objektov in preverjanje podpisov.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
3. Izpolnite obrazce vodenega opravila. Pri uporabi teh obrazcev za izvedbo nalog, potrebnih za vzpostavitev delujoče lokalne službe za potrdila, morate izvesti naslednje korake:
   a. Podati identifikacijske informacije za lokalno službo za potrdila.
   b. Namestiti potrdilo lokalne službe za potrdila na PC ali v pregledovalnik, da bo lahko vaša programska oprema prepoznala lokalno službo za potrdila in preverjala veljavnost potrdil, ki jih izda lokalna služba za potrdila.
   c. Izbrati podatke načel za lokalno službo za potrdila.

      Opomba: Izberite, da lokalna služba za potrdila lahko izdaja uporabniška potrdila.
   d. Uporabiti novo lokalno službo za potrdila za izdajanje potrdil strežnika ali odjemalca, ki jih lahko uporabljajo vaše aplikacije za povezave SSL.
   e. Izbrati aplikacije, ki lahko uporabljajo potrdilo strežnika ali odjemalca za povezave SSL.

      Opomba: Zagotovite, da izberete ID aplikacije za strežnik HTTP vaše kadrovske službe.
   f. Uporabiti novo lokalno službo za potrdila za izdajanje potrdil za podpisovanje objektov, ki jih lahko uporabijo vaše aplikacije za digitalno podpisovanje objektov. Ta podnaloga izdela prostor za potrdila *OBJECTSIGNING; to je prostor za potrdila, ki se uporablja za upravljanje potrdil za podpisovanje objektov.

Opomba: Čeprav ta scenarij ne uporablja potrdil za podpisovanje objektov, morate dokončati ta korak. Če nalogo prekinete v tem trenutku, se opravilo konča, vi pa morate, če želite dokončati konfiguriranje potrdil SSL, naloge izvajati ločeno.

g. Izberite aplikacije, ki bodo zaupale lokalni službi za potrdila.

Opomba: Prepričajte ste, da ste kot eno izmed aplikacij, ki zaupajo lokalni službi za potrdila, izbrali ID aplikacije strežnika HTTP za vse zaposlene, na primer, QIBM_HTTP_SERVER_MOJEPODTEST.

Ko dokončate konfiguriranje potrdil, ki jih za uporabo SSL zahteva aplikacija spletnega strežnika, lahko konfigurirate spletni strežnik tako, da za overjanje uporabnikov zahteva potrdila.

5. korak: Konfiguriranje overjanja odjemalcev za spletni strežnik za vse zaposlene

Če podate, naj strežnik HTTP za overjanje zahteva potrdila, morate konfigurirati nastavitve splošnega overjanja za strežnik HTTP. Te nastavitve konfigurirate v obrazcu za zaščito, v katerem ste konfigurirali strežnik za uporabo plasti zaščitenih vtičnic (SSL).

Če želite konfigurirati strežnik, tako da bo za overjanje odjemalcev zahteval potrdila, upoštevajte naslednje korake:

1. Zaženite vmesnik za upravljanje strežnika HTTP.
2. Če želite delati z določenim strežnikom HTTP, izberite jezičke **Upravljanje —> Vsi strežniki —> Vsi strežniki HTTP**, da prikažete seznam vseh konfiguriranih strežnikov HTTP.
3. Izberite želen strežnik s seznama in kliknite **Podrobnosti upravljanja**.
4. V oknu za usmerjanje izberite **Zaščita**.
5. V obrazcu izberite jeziček **Overjanje**.
6. Izberite možnost **Uporaba profila odjemalca OS/400.** .
7. V polju **Ime overjanja za področje** podajte ime za področje overjanja.
8. Izberite Omogočeno za polje **Zahteve po obdelavi prek pooblastil odjemalca** in kliknite **Uveljavi**.
9. V obrazcu izberite jeziček **Nadzor dostopa**.
10. Izberite **Vsi overjeni uporabniki (veljavno ime uporabnika in geslo)** in kliknite **Uveljavi**.
11. V obrazcu izberite jeziček **SSL z overjanjem potrdil**.
12. Zagotovite, da je izbrana vrednost v polju **SSL** Omogočeno.
13. Prepričajte se, da je v polju **Ime aplikacije potrdila strežnika** podana pravilna vrednost, na primer, QIBM_HTTP_SERVER_MOJEPODTEST.
14. Izberite **Pred vzpostavitvijo povezave sprejmi potrdilo odjemalca, če je na voljo**. Kliknite Potrdi.

Več informacij o splošni konfiguraciji, potrebni za strežnik HTTP pri uporabi SSL najdete v temi Strežnik HTTP za iSeries, še posebej v scenariju: JKL na strežniku HTTP (poganja ga Apache) omogoča zaščito s plastjo zaščitenih vtičnic (SSL). Za scenarij nudi vse korake nalog za izdelavo navideznega gostitelja in njegovo konfiguriranje za uporabo SSL.

Ko dokončate konfiguriranje overjanja odjemalcev, lahko znova zaženete strežnik HTTP v načinu SSL in pričnete varovati zasebnost podatkov aplikacije za vse zaposlene.

6. Korak: Zagon spletnega strežnika za vse zaposlene v načinu SSL

Morda boste morali zaustaviti in ponovno zagnati strežnik HTTP, da boste zagotovili, da strežnik lahko določi, da obstaja dodelitev potrdila in da jo lahko uporabi za začetek sej SSL.

Če želite zaustaviti in zagnati strežnik HTTP (poganja ga Apache), upoštevajte naslednje korake:

1. V **Navigatorju iSeries** razširite ikono strežnik.
2. Razširite **Omrežje > Strežniki > TCP/IP > Upravljanje HTTP**.
3. Kliknite **Poženi**, da poženete vmesnik za upravljanje strežnika HTTP.
4. Kliknite jeziček **Upravljanje**, da prikažete seznam vseh konfiguriranih strežnikov HTTP.
5. S seznama izberite želen strežnik in kliknite **Zaustavi**, če se strežnik izvaja.

6. Kliknite **Zaženi**, da znova zaženete strežnik. Podrobnejše informacije o parametrih zagona so vam na voljo v zaslonski pomoči.

Dodatne informacije o upravljanju trenutnih in prihodnjih različic strežnika HTTP za iSeries (izviren ali pa ga poganja Apache) najdete v temi Strežnik HTTP za iSeries.

Preden lahko uporabniki dostopajo do spletne aplikacije za vse zaposlene, morajo v pregledovalnik namestiti kopijo potrdila lokalne službe za potrdila.

7. korak: Uporabniki naj v pregledovalniku namestijo kopijo potrdila lokalne službe za potrdila

Ko uporabniki dostopijo do strežnika, ki nudi povezavo plasti zaščitenih vtičnic (SSL), strežnik predstavi potrdilo odjemalski programski opremi kot dokazilo svoje istovetnosti. Preden lahko strežnik vzpostavi sejo, mora programska oprema odjemalca preveriti veljavnost potrdila strežnika. Za preverjanje veljavnosti potrdila strežnika mora imeti programska oprema odjemalca dostop do lokalno shranjene kopije potrdila službe za potrdila (CA), ki je izdala potrdilo strežnika. Če strežnik predloži potrdilo javne službe za potrdila, mora pregledovalnik uporabnika ali druga programska oprema odjemalca že imeti kopijo potrdila službe za potrdila. Če pa, kot v tem scenariju, strežnik predloži potrdilo zasebne lokalne službe za potrdila, mora vsak uporabnik namestiti kopijo potrdila lokalne CA dobiti s pomočjo Upravljalnika digitalnih potrdil.

Vsi uporabniki (odjemalci B, C in D) morajo dokončati naslednje korake za pridobitev kopije potrdila lokalne službe za potrdila:
1. Zaženite DCM.
2. V oknu za usmerjanje izberite **Namesti lokalno potrdilo CA na PC**, da boste prikazali stran, na kateri lahko naložite potrdilo lokalne CA v pregledovalnik ali ga shranite v datoteko v sistemu.
3. Izberite možnost za namestitev potrdila. S to možnostjo prenesete potrdilo lokalne službe za potrdila kot overjenega skrbnika v vašem pregledovalniku. S tem je zagotovljeno, da lahko vaš pregledovalnik vzpostavi seje zaščitene komunikacije s spletnimi strežniki, ki uporabljajo potrdilo te službe za potrdila. Pregledovalnik bo prikazal niz oken, ki vam bodo pomagala dokončati namestitev.
4. Za vrnitev na domačo stran Upravljalnika digitalnih potrdil kliknite **Potrdi**.

Zdaj, ko lahko uporabniki do spletnega strežnika za vse zaposlene dostopajo v načinu SSL, morajo biti pripravljeni, da strežniku predložijo ustrezno potrdilo za overjanje. Zato si morajo od lokalne službe za potrdila pridobiti uporabniško potrdilo.

8. korak: Vsak uporabnik naj od lokalne službe za potrdila zahteva potrdilo

V prejšnjih korakih ste konfigurirali spletni strežnik za zaposlene tako, da za overjanje uporabnikov zahteva potrdila. Odslej pa morajo uporabniki za dostop do spletnega strežnika predložiti veljavno potrdilo lokalne službe za potrdila. Vsi uporabniki morajo uporabiti Upravljalnik digitalnih potrdil za pridobitev potrdila, tako da izvedejo nalogo za **izdelavo potrdila**. Za pridobivanje potrdila lokalne službe za potrdila morajo načela lokalne službe za potrdila omogočati izdajanje uporabniških potrdil.

Vsi uporabniki (odjemalci B, C in D) morajo dokončati naslednje korake za pridobitev potrdila:
1. Zaženite DCM.
2. V oknu za usmerjanje izberite **Izdelaj potrdilo**.
3. Kot tip potrdila za izdelavo izberite **Uporabniško potrdilo**. Prikaže se obrazec, na katerem lahko podate določilne informacije za potrdilo.
4. Izpolnite obrazec in kliknite **Nadaljuj**.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
5. Na tej točki začne DCM sodelovati s pregledovalnikom za izdelavo zasebnega in javnega ključa za potrdilo. Pregledovalnik bo morda prikazal okna, prek katerih vas bo vodil skozi ta postopek. Za te naloge sledite navodilom pregledovalnika. Ko pregledovalnik ustvari ključa, se prikaže potrditvena stran, ki kaže, da je DCM izdelal potrdilo.

6. Namestite novo potrdilo v vašem pregledovalniku. Pregledovalnik bo morda prikazal okna, prek katerih vas bo vodil skozi ta postopek. Sledite navodilom, ki jih pregledovalnik poda za zaključitev te naloge.
7. Kliknite **Potrdi** in s tem dokončajte nalogo.

Upravljalnik digitalnih potrdil med obdelavo samodejno poveže potrdilo s vašim profilom uporabnika.

Če so te naloge dokončane, lahko do podatkov spletnega strežnika za vse zaposlene dostopajo samo overjeni uporabniki z veljavnim potrdilom, podatki pa so med prenosom z SSL zaščiteni.

Poglavje 5. Koncepti digitalnih potrdil

Preden boste z uporabo digitalnih potrdil začeli izboljševati sistemsko in omrežno varnostno politiko, se morate najprej seznaniti z varnostnimi izboljšavami, ki jih ponujajo.

Digitalno potrdilo je digitalno priporočilo, ki preveri veljavnost identitete lastnika potrdila, podobno kot to naredi potni list. Informacije identifikacije, ki jih nudi digitalno potrdilo so znane tudi kot razločevalno ime predmeta. Zaupanja vredna stran, služba za potrdila, izdaja digitalna potrdila uporabnikom in organizacijam. Overjeno potrdilo je potrdilo CA-ja, ki mu je mogoče zaupati.

Digitalno potrdilo vsebuje tudi javni ključ, ki je del para, sestavljenega iz javnega in zasebnega ključa. Številne varnostne funkcije temeljijo na uporabi digitalnih potrdil in z njimi povezanih parih ključev. S pomočjo digitalnih potrdil lahko konfigurirate seje plasti zaščitenih vtičnic (SSL), s katerimi zagotovite zasebne in zaščitene komunikacijske seje med uporabniki in aplikacijami strežnika. Zaščito lahko izboljšate tako, da konfigurirate več aplikacij z omogočenim SSL, ki bodo namesto uporabniških imen in gesel zahtevale potrdila ter pripomogle k varnejšemu overjanju uporabnikov.

Če želite zvedeti več o pojmih digitalnih potrdil, preglejte naslednje teme:

Razširitve potrdil
S pomočjo teh informacij boste izvedeli, kaj so polja razširitve potrdil in kako jih je mogoče uporabiti.

Obnavljanje potrdil
S pomočjo teh informacij se boste seznanili s postopkom, ki ga uporablja Upravljalnik digitalnih potrdil za obnavljanje potrdil strežnikov in odjemalcev ter potrdil za podpisovanje objektov.

Razločevalno ime
S pomočjo teh informacij se boste seznanili z značilnostmi identifikacije digitalnih potrdil.

Digitalni podpisi
s pomočjo teh informacij boste spoznali, kaj so elektronskih podpisi ter kako delujejo, da zagotovijo neokrnjenost objekta.

Par zasebnega in javnega ključa
S pomočjo teh informacij se boste seznanili s ključi zaščite, povezanimi z digitalnimi potrdili.

Služba za pooblastila (CA)
S pomočjo teh informacij boste spoznali službe za potrdila, enote, ki izdajajo digitalna potrdila.

Mesta seznama za preklic potrdil (CRL)
V tej temi se boste naučili, kaj je seznam za preklic potrdil (CRL) in kako se uporablja v postopku preverjanja veljavnosti potrdil in njihovega overjanja.

Prostori za potrdila
V tej temi se boste naučili, kaj so prostori za potrdila in kako uporabiti Upravljalnik digitalnih potrdil (DCM) za delo z njimi in s potrdili, ki jih vsebujejo.

Šifriranje
V tej temi se boste naučili, kaj je šifriranje in kako uporabljajo digitalna potrdila šifriranje funkcije za nudenje zaščite.

IBM-ovi Šifrirni koprocesorji za iSeries
V teh informacijah je opisano, kako lahko s pomočjo Upravljalnika digitalnih potrdil in IBM-ovih Šifrirnih koprocesorjev zagotovite varnejšo hrambo ključev.

Secure Sockets Layer (SSL)
Ta tema vsebuje kratek opis plasti zaščitenih vtičnic.

Definicije aplikacij
S pomočjo teh informacij boste izvedeli, kaj so definicije aplikacij Upravljalnika digitalnih potrdil in kako jih lahko uporabite za konfiguriranje SSL in podpisovanje objektov.

Preverjanje
S pomočjo teh informacij boste izvedeli, kako v Upravljalniku digitalnih potrdil deluje proces preverjanja aplikacij in potrdil.

Razširitve potrdil

Razširitve potrdil so polja, ki nudijo dodatne informacije o potrdilu. Razširitve potrdil omogočajo način razširitve izvirnih informacijskih standardov za potrdila X.509. Medtem ko informacije za nekatere razširitve omogočajo razširitev identifikacijskih informacij za potrdilo, druge nudijo informacije o šifrirnih zmogljivostih potrdila.

Razširitvenih polj za razširitve razločevalnega imena in drugih informacij ne uporabljajo vsa potrdila. Število in tip razširitvenih polj, ki jih uporablja potrdilo, se med enotami služb za potrdila, ki izdajajo potrdila, razlikuje.

Lokalna služba za potrdila, ki jo nudi Upravljalnik digitalnih potrdil, vam omogoča uporabo samo razširitve potrdila Alternativno ime predmeta. Te razširitve vam omogočajo, da povežete potrdilo z določenim naslovom IP, popolnim imenom domene ali naslovom elektronske pošte. Če nameravate potrdilo uporabljati za določanje končne točke povezave navideznega zasebnega omrežja (VPN), morate za te razširitve podati razširitve.

Obnavljanje potrdil

Postopek obnavljanja potrdil, ki ga uporablja Upravljalnik digitalnih potrdil varira glede na tip službe za potrdila, ki je izdala potrdilo.

Če obnovljena potrdila podpisujete s pomočjo lokalne službe za potrdila, DCM uporabi dobljene informacije za izdelavo novega potrdila v trenutnem prostoru za potrdila, prejšnje potrdilo pa zadrži.

Če za izdajanje potrdil uporabljate znano internetno službo za potrdila, lahko potrdila obnavljate na enega od naslednjih načinov: Obnovljeno potrdilo lahko uvozite iz datoteke, ki jo prejmete od podpisujoče službe za potrdila ali s pomočjo Upravljalnika digitalnih potrdil izdelate nov javno-zasebni par ključev za potrdilo. DCM nudi prvo možnost, če morda želite potrdilo obnoviti neposredno pri službi za potrdila, ki ga je izdala.

Če izberete izdelavo novega para ključev, se DCM obnovitve loti na isti način, kot se je lotil izdelave potrdila. DCM za obnovljeno potrdilo izdela nov par, sestavljen iz javnega in zasebnega ključa, in ustvari zahtevo po podpisu potrdila (CSR), sestavljeno iz javnega ključa in drugih informacij, ki jih podate za novo potrdilo. S pomočjo CSR-a lahko od VeriSign-a ali katere druge javne službe za potrdila zahtevate novo potrdilo. Ko od službe za potrdila prejmete podpisano potrdilo, ga lahko z DCM-om uvozite v ustrezen prostor za potrdila. Prostor za potrdila nato vsebuje obe kopiji potrdila, izvirno in na novo izdano obnovljeno potrdilo.

Če z DCM ne želite izdelati novega para ključev, vas DCM vodi skozi postopek uvoza obnovljenega in podpisanega potrdila iz obstoječe datoteke, ki ste jo prejeli od službe za potrdila, v prostor za potrdila. Uvoženo obnovljeno potrdilo nato zamenja predhodno potrdilo.

Razločevalno ime

Vsaka služba za potrdila ima svoja načela za določanje, katere določilne informacije zahteva za izdajo potrdila. Nekatere javne internetne službe za potrdila zahtevajo zelo malo informacij, kot sta na primer ime in naslov elektronske pošte. Druge javne službe za potrdila pa lahko pred izdajo potrdila zahtevajo več informacij in strožji dokaz določilnih informacij. Tako lahko na primer službe za potrdila, ki podpirajo standarde PKIX (Public Key Infrastructure Exchange), pred izdajo potrdila zahtevajo, da zahtevnik preveri informacije o identiteti prek registracijske službe (RA). Če torej nameravate sprejeti in uporabiti potrdila kot priporočila, morate pregledati identifikacijske zahteve za službo za potrdila, da določite, ali te ustrezajo vašim varnostnim potrebam.

Razločevalno ime je izraz, ki opisuje označujoče informacije v potrdilu in je del potrdila samega. Potrdilo vsebuje informacije razločevalnega imena za lastnika ali zahtevnika potrdila (imenovano tudi razločevalno ime predmeta) in za službo za potrdila, ki izda potrdilo (imenovano razločevalno ime izdajatelja). Glede na identifikacijska načela službe za

| potrdila, ki izda potrdilo, lahko razločevalno ime vsebuje različne informacije. S pomočjo Upravljalnika digitalnih
| potrdil (DCM) lahko vodite zasebno službo za potrdila in izdajate zasebna potrdila, uporabite pa ga lahko tudi za
| izdelavo informacij razločevalnega imena in para ključev za potrdila, ki jih izda javna internetna služba za potrdila za
| vaše podjetje. Informacije razločevalnega imena, ki jih lahko podate za katerokoli vrsto potrdila, vključujejo naslednje:
| • splošno ime lastnika potrdila
| • podjetje
| • organizacijska enota
| • kraj ali mesto
| • zvezna država ali provinca
| • država ali regija

| Če z DCM izdajate zasebna potrdila, lahko z uporabo razširitev potrdil omogočite dodatne informacije DN za potrdilo,
| vključujoč:
| • naslov IP različice 4
| • celotno ime domene
| • naslov elektronske pošte

| Te dodatne informacije vam bodo v pomoč, če nameravate potrdilo uporabiti za konfiguriranje povezave navideznega
| zasebnega omrežja..

Digitalni podpisi

Digitalni podpis na elektronskem dokumentu ali drugem objektu izdelate z obliko šifriranja in je enakovreden osebnemu podpisu na napisanem dokumentu. Digitalni podpis nudi dokaz o izvoru in pomene za preverjanje neokrnjenosti objekta. Lastnik digitalnega potrdila ″podpiše″ objekt s pomočjo zasebnega ključa potrdila. Prejemnik objekta dešifrira podpis z ustreznim javnim ključem potrdila, ki preveri integriteto podpisanega objekta in izvor pošiljatelja.

Služba za potrdila (CA) podpiše potrdila, ki jih izda. Ta podpis vsebuje podatkovni niz, ki je šifriran z zasebnim ključem službe za potrdila. Vsak uporabnik lahko preveri podpis na potrdilu s pomočjo javnega ključa službe za potrdila in ga dešifrira.

Digitalni podpis je elektronski podpis, ki ga vi ali aplikacija izdela na objektu z uporabo zasebnega ključa digitalnega potrdila. Digitalni podpis na objektu nudi unikatno elektronsko vez istovetnosti podpisnika (lastnika ključa za podpisovanje) z izvorom objekta. Če dostopate do objekta, ki vsebuje digitalni podpis, lahko preverite podpis na objektu, da preverite veljavnost izvora objekta (na primer, da aplikacija, ki jo prenašate z oddaljenega mesta, dejansko pride iz pooblaščenega izvora, kot je na primer IBM). S tem postopkom preverjanja lahko tudi določite, ali je bila od podpisa objekta na njem izvedena kakšna nepooblaščena sprememba.

Zgled delovanja elektronskega podpisa

Razvijalec programske opreme je izdelal aplikacijo za i5/OS, ki jo želi razpošiljati prek interneta, kar je za njegove stranke udoben in ugoden način. Razvijalec ve, da stranke upravičeno skrbi prenos programov prek interneta, predvsem zaradi naraščajočih težav z objekti, ki se maskirajo kot legalni programi, v resnici pa so škodljivi programi, kot so na primer virusi.

Zato se odloči, da bo digitalno podpisal aplikacijo, tako da bodo stranke lahko preverile, ali je njegovo podjetje pravi izvor aplikacije. Uporablja zasebni ključ digitalnega potrdila, ki ga je pridobil pri dobro znani javni službi za pooblastila, s katerim podpiše aplikacijo. Nato lahko aplikacijo njegove stranke prenesejo. Kot del prenosa paketa vključi tudi kopijo digitalnega potrdila, ki ga je uporabil za podpisovanje objekta. Kot stranka prenaša aplikativni paket, lahko uporabi javni ključ potrdila, s katerim preveri podpis na aplikaciji. S tem postopkom lahko stranka določi in preveri aplikacijo, kot tudi zagotovi, da vsebina objekta ni bila spremenjena od podpisa.

Par zasebnega in javnega ključa

Vsako digitalno potrdilo ima par povezanih šifrirnih ključev. Ta par je sestavljen iz zasebnega in javnega ključa. (Potrdila za preverjanje podpisov so izjema in imajo samo z njimi povezan javni ključ.)

Javni ključ je del digitalnega potrdila lastnika in je na voljo vsem. Zasebni ključ pa je zaščiten in je na voljo samo lastniku ključa. Ta omejeni dostop zagotavlja, da so komunikacije, ki uporabljajo ključe, zaščitene.

Lastnik potrdila lahko uporabi ta ključa za izkoriščanje zaščitnih funkcij, ki jih nudijo ključi. Lastnik potrdila lahko na primer uporablja zasebni ključ potrdila za ″podpisovanje″ in šifriranje podatkov, poslanih med uporabniki ter strežniki, kot so sporočila, dokumenti in objekti kode. Prejemnik podpisanega objekta lahko nato uporabi javni ključ, ki je vsebovan v potrdilu lastnika, in dešifrira podpis. Takšni digitalni podpisi zagotavljajo zanesljivost izvora objektov in nudijo način za preverjanje neokrnjenosti objekta.

Služba za pooblastila (CA)

Služba za potrdila (CA) je overjena osrednja upravna enota, ki lahko izdaja digitalna potrdila za uporabnike in strežnike. Overjeno potrdilo je potrdilo CA-ja, ki mu je mogoče zaupati. CA uporabi svoj zasebni ključ za izdelavo digitalnega podpisa na potrdilu, ki ga izda za preverjanje izvora potrdila. Drugi uporabniki lahko z javnim ključem potrdila CA preverijo pristnost potrdil, ki jih izda in podpiše CA.

CA je lahko javna komercialna enota, kot je VeriSign ali pa zasebna enota, ki jo vodi podjetje za notranje namene. Kar nekaj podjetij nudi komercialne storitve potrdil za uporabnike interneta. Upravljalnik digitalnih potrdil (DCM) vam omogoča, da potrdila upravljate tako prek javnih kot tudi prek zasebnih služb za potrdila.

Upravljalnik digitalnih potrdil lahko uporabite tudi za vodenje lastne lokalne službe za potrdila, s pomočjo katere izdajate zasebna potrdila sistemom in uporabnikom. Ko lokalna služba za potrdila izda uporabniško potrdilo, ga upravljalnik digitalnih potrdil samodejno poveže z uporabniškim potrdilom ali drugo uporabniško istovetnostjo. Ali upravljalnik digitalnih potrdil potrdilo poveže z uporabniškim potrdilom ali pa z drugo uporabniško identiteto uporabnika, je odvisno od tega, ali je upravljalnik digitalnih potrdil konfiguriran za delo s preslikavo istovetnosti podjetja (EIM). To zagotovi, da so pravice dostopa in pooblastil za potrdilo enake kot za uporabniški profil lastnika.

Status overjenega potrdila

Izraz overjeno potrdilo se nanaša na posebno označbo, ki je dana potrdilu službe za potrdila. Ta označba omogoča pregledovalniku ali drugi aplikaciji overjanje in sprejem potrdil, ki jih izda služba za potrdila (CA).

Ko naložite potrdilo službe za potrdila v pregledovalnik, le-ta omogoči, da ga označite kot overjenega. Preden lahko aplikacija overi in zaupa potrdilom, ki jih izda določen CA, morajo biti tudi druge aplikacije, ki podpirajo uporabo potrdil, konfigurirane tako, da zaupajo CA.

S pomočjo upravljalnika digitalnih potrdil lahko omogočite ali onemogočite status zaupanja za določeno potrdilo službe za potrdila. Če omogočite potrdilo CA, lahko podate, da ga aplikacije lahko uporabljajo za overjanje in sprejem potrdil, ki jih izda CA. Če onemogočite potrdilo CA, ne morete podati, naj ga aplikacije uporabljajo za overjanje in sprejem potrdil, ki jih izda CA.

Podatki o načelih službe za potrdila

Če z upravljalnikom digitalnih potrdil izdelate lokalno službo za potrdila, lahko zanjo določite podatke o načelih. Podatki o načelih lokalne službo za potrdila opisujejo pooblastila za podpisovanje, ki jih ima lokalna služba. Podatki o načelih določajo:

- Ali lahko lokalna služba za potrdila izdaja in podpisuje uporabniška potrdila.
- Kako dolgo so potrdila, ki jih izda lokalna služba za potrdila, veljavna.

Mesta CRL (seznam za preklic potrdil)

Seznam za preklic potrdil (CRL) je datoteka, v kateri so navedena vsa neveljavna in preklicana potrdila določene službe za potrdila (CA). Službe za potrdila občasno ažurirajo svoje sezname in omogočijo, da jih uporabniki objavijo v imenikih LDAP (Directory Access Protocol). Nekatere službe za potrdila, kot je na primer SSH na Finskem, same objavijo CRL-je v imenikih LDAP, do katerih lahko dostopite neposredno. Če služba za potrdila objavi lasten CRL, to potrdilo kaže tako, da vključi pripono CRL v obliki URI-ja (Uniform Resource Identifier).

Upravljalnik digitalnih potrdil (DCM) omogoča definiranje in upravljanje mesta CRL, s čimer zagotovi strožje overjanje potrdil, ki jih uporabljate ali sprejmete od drugih. Definicija mesta CRL opisuje mesto in dostopne informacije strežnika LDAP (Lightweight Directory Access Protocol), na katerem so shranjeni CRL-ji.

Aplikacije, ki overjajo potrdila, dostopijo do mesta CRL določene službe za potrdila, da zagotovijo, da služba ni preklicala določenega potrdila. Upravljalnik digitalnih potrdil omogoča, da definirate in upravljate informacije o mestih CRL, ki jih potrebujejo aplikacije za izvajanje obdelave CRL med overjanjem potrdila. Zgledi aplikacij in postopkov, ki lahko izvajajo obdelavo CRL-jev za overjanje potrdil, so: strežnik IKE (Internet Key Exchange) navideznega zasebnega omrežja (VPN), aplikacije, omogočene za plast zaščitenih vtičnic (SSL) in postopek za podpis objektov. Če definirate mesto CRL in ga povežete s potrdilom službe za potrdila, Upravljalnik digitalnih potrdil opravi obdelavo CRL kot del preverjanja veljavnosti potrdil, ki jih izda določena služba za potrdila. .

Prostori za potrdila

Prostor za potrdila je posebna datoteka baze podatkov ključev, ki jo uporablja Upravljalnik digitalnih potrdil (DCM) za shranjevanje digitalnih potrdil. Prostor za potrdila vsebuje tudi zasebni ključ potrdila, razen če ste izbrali, da boste ključ hranili s pomočjo IBM-ovega Šifrirnega koprocesorja. Upravljalnik digitalnih potrdil omogoča izdelavo in upravljanje številnih prostorov za potrdila. DCM nadzoruje dostop do prostorov za potrdila s pomočjo gesel in nadzora dostopa do imenika integriranega datotečnega sistema ter datotek, ki sestavljajo prostor za potrdila.

Prostori za potrdila so razvrščeni glede na tipe potrdil, ki jih vsebujejo. Upravljalne naloge, ki jih lahko izvajate za vsako potrdilo, se razlikujejo glede na tip potrdila, ki ga vsebuje prostor za potrdila. Upravljalnik digitalnih potrdil nudi naslednje vnaprej definirane prostore za potrdila, ki jih lahko izdelate ter upravljate:

Lokalna služba za pooblastila (CA)
DCM ta prostor za potrdila uporablja za shranjevanje potrdila lokalne službe za potrdila in zasebnega ključa, če izdelate lokalno službo za potrdila. S potrdilom v tem prostoru za potrdila lahko podpisujete potrdila, ki jih za vas izdaja lokalna služba za potrdila. Ko lokalna služba za potrdila izda potrdilo, DCM prenese kopijo potrdila te službe (brez zasebnega ključa) v ustrezen prostor za potrdila (na primer *SYSTEM) za overjanje. Aplikacije s potrdili službe za potrdila preverjajo izvor potrdil, ki jih morajo oceniti kot del pogajanj SSL, da dodelijo pooblastilo za sredstva.

***SYSTEM**
Upravljalnik digitalnih potrdil nudi ta prostor za potrdila za upravljanje potrdil strežnika ali odjemalca, ki jih uporabljajo aplikacije za sodelovanje v komunikacijskih sejah plasti zaščitenih vtičnic (SSL). IBM-ove aplikacije (in aplikacije številnih drugih razvijalcev programske opreme) so napisane samo za uporabo potrdil v prostoru za potrdila *SYSTEM. Če za izdelavo lokalne službe za potrdila uporabljate DCM, le-ta kot del tega postopka izdela tudi prostor za potrdila. Če se odločite za pridobitev potrdil od javne službe za pooblastila, kot je VeriSign, ki ga bodo uporabljale odjemalske ali aplikacije strežnika, morate izdelati ta prostor za potrdila.

***OBJECTSIGNING**
Upravljalnik digitalnih potrdil nudi ta prostor za potrdila za upravljanje potrdil, ki jih uporabljate za digitalno podpisovanje objektov. Naloge v tem prostoru za potrdila omogočajo izdelavo digitalnih podpisov za objekte, kot tudi pregled in preverjanje podpisov na objektih. Če za izdelavo lokalne službe za potrdila uporabljate DCM, le-ta kot del tega postopka izdela tudi prostor za potrdila. Če se odločite za pridobitev potrdil od javne službe za pooblastila, kot je VeriSign, ki ga boste uporabljali za podpisovanje objektov, morate izdelati ta prostor za potrdila.

***SIGNATUREVERIFICATION**
Upravljalnik digitalnih potrdil nudi ta prostor za potrdila za upravljanje potrdil, ki jih uporabljate za preverjanje istovetnosti digitalnih podpisov na objektih. Če želite preveriti digitalni podpis, mora ta prostor za potrdila vsebovati kopijo potrdila, ki je podpisal objekt. Prostor za potrdila mora vsebovati tudi kopijo potrdila službe za pooblastila za službo za pooblastila, ki je izdala potrdilo za podpisovanje objekta. To potrdilo pridobite, tako da izvozite potrdilo za podpisovanje objekta v trenutnem sistemu v prostor, ali tako da uvozite potrdila, ki ste jih prejeli od podpisnika objekta.

Drug sistemski prostor za potrdila
Ta prostor za potrdila nudi nadomestno shranjevališče za potrdila strežnika ali odjemalca, ki jih uporabljate za seje SSL. Drugi sistemski prostori za potrdila so uporabniško definirani sekundarni prostori za potrdila SSL. Možnost Drug sistemski prostor za potrdila omogoča upravljanje potrdil za aplikacije, ki jih napišete vi ali kdo drug, in s pomočjo API-ja SSL_Init programsko dostopajo in uporabljajo potrdilo za vzpostavitev seje SSL. Ta API omogoča, da aplikacija namesto potrdila, ki ga posebej določite, uporabi privzeto potrdilo. Ta prostor za potrdila se najpogosteje uporablja pri selitvi potrdil iz prejšnje izdaje Upravljalnika digitalnih potrdil ali za izdelavo posebnega podniza potrdil za uporabo plasti zaščitenih vtičnic.

Opomba: Če je IBM-ov Šifrirni koprocesor nameščen na strežniku, lahko za vaša potrdila izberete drugo možnost shranitve zasebnega ključa (z izjemo potrdil za podpisovanje objektov). Zasebni ključ lahko shranite v sam koprocesor ali pa z njegovo pomočjo šifrirate zasebni ključ in ga namesto v prostor za potrdila shranite v posebno datoteko ključev.

Upravljalnik digitalnih potrdil nadzoruje dostop do prostorov za potrdila prek gesel. Prav tako vzdržuje nadzor dostopa do imenika integriranega datotečnega sistema in datotek, ki sestavljajo prostore za potrdila. Prostori lokalne službe za potrdila (CA), *SYSTEM, *OBJECTSIGNING in *SIGNATUREVERIFICATION morajo biti na posebnih poteh znotraj integriranega datotečnega sistema, drugi sistemski prostori za potrdila pa se lahko nahajajo kjerkoli znotraj integriranega datotečnega sistema.

Šifriranje

Šifriranje je veda o varovanju tajnosti podatkov. Šifriranje omogoča shranjevanje informacij ali komuniciranje z drugimi uporabniki, pri čemer neželenim uporabnikom preprečite, da bi razumeli shranjene informacije ali komunikacije. Šifriranje preoblikuje razumljivo besedilo v nerazumljive kose podatkov (šifrirano besedilo). Dešifriranje obnovi razumljivo besedilo iz nerazumljivih podatkov. Oba procesa vključujeta matematično formulo ali algoritem in skrivno zaporedje podatkov (ključ).

Obstajata dva tipa šifriranja:
- V šifriranju z **deljenim ali tajnim ključem (simetrično)** je en ključ deljena skrivnost med dvema strankama. Šifriranje in dešifriranje uporabljata isti ključ.
- Pri šifriranju z **javnim ključem (asimetrično)** uporabljata šifriranje in dešifriranje različne ključe. Stran ima par ključev, sestavljen iz javnega in zasebnega ključa. Javni ključ je mogoče po želji razdeljevati, običajno znotraj digitalnega potrdila, medtem ko zasebni ključ lastnik obdrži zase. Ključa sta matematično povezana, vendar je skoraj nemogoče izpeljati zasebni ključ na osnovi javnega. Objekt, kot je na primer sporočilo, ki je šifrirano z javnim ključem, je mogoče dešifrirati samo z njim povezanim zasebnim ključem. Druga možnost je, da strežnik ali uporabnik uporabita zasebni ključ, s katerim podpišeta objekt, prejemnik pa lahko z ustreznim javnim ključem dešifrira digitalni podpis in preveri izvor in integriteto objekta.

IBM-ovi Šifrirni koprocesorji za iSeries

Uporaba IBM-ovega Šifrirnega koprocesorja na vašem strežniku doda možnost varne šifrirne obdelave. Šifrirni koprocesor nudi preizkušene storitve šifriranja za razvijanje zaščitenih aplikacij e-poslovanja, pri tem pa zagotavlja zasebnost in neokrnjenost.

Če imate v sistemu nameščen in vključen šifrirni koprocesor, lahko z njegovo pomočjo omogočite varnejšo shranitev za vaše zasebne ključe potrdila.

S šifrirnim koprocesorjem lahko shranite zasebni ključ za potrdilo strežnika ali odjemalca in za potrdilo lokalne službe za potrdila. Z njim pa ne morete shraniti zasebnega ključa uporabniškega potrdila, saj mora biti ta shranjen v sistemu uporabnika. Koprocesorja zdaj tudi ne morete uporabiti za shranitev zasebnega ključa potrdila za podpisovanje objektov.

Zasebni ključ potrdila lahko bodisi neposredno shranite v šifrirni koprocesor ali pa s pomočjo glavnega ključa šifrirnega koprocesorja ključ šifrirate in ga shranite v posebno datoteko ključev. Te možnosti za shranitev ključa lahko izberete kot del postopka izdelave ali obnovitve potrdila. Če uporabite koprocesor za shranitev zasebnega ključa potrdila, lahko za ta ključ spremenite dodelitev naprave koprocesorja.

Če želite šifrirni koprocesor uporabiti za hrambo zasebnega ključa, se prepričajte, da je koprocesor vključen, šele nato lahko uporabite Upravljalnik digitalnih potrdil. V nasprotnem primeru DCM v postopku izdelave ali obnovitve potrdila ne ponuja možnosti izbire mesta za shranitev.

Plast zaščitenih vtičnic (Secure Sockets Layer (SSL))

Plast zaščitenih vtičnic (SSL), ki jo je prvotno izdelal Netscape, je industrijski standard za šifriranje sej med odjemalci in strežniki. SSL uporablja asimetrično šifriranje z javnim ključem, s katerim šifrira sejo med strežnikom in odjemalcem. Aplikacije odjemalca in strežnika se dogovorijo za ta ključ seje med izmenjavo digitalnih potrdil. Ključ samodejno poteče po 24 urah, nakar proces SSL izdela drug ključ za vsako povezavo strežnika in vsakega odjemalca. Zato tudi v primeru, če nepooblaščeni uporabniki prestrežejo in dešifrirajo ključ seje (kar je skoraj nemogoče), ga ne morejo uporabiti za prisluškovanje drugim sejam.

Definicije aplikacij

Obstajata dva tipa definicij aplikacij, ki jih lahko upravljate v Upravljalniku digitalnih potrdil:

- Definicije aplikacij odjemalca ali strežnika, ki uporabljajo komunikacijske seje plasti zaščitenih vtičnic (SSL).
- Definicije aplikacij za podpisovanje objektov, ki s podpisovanjem objektov zagotovijo njihovo neokrnjenost.

Če želite uporabljati Upravljalnik digitalnih potrdil za delo z definicijami aplikacij SSL in njihovimi potrdili, mora biti aplikacija najprej registrirana z Upravljalnikom digitalnih potrdil kot definicija aplikacije, tako da ima enkraten ID aplikacije. Razvijalci aplikacij registrirajo aplikacije, omogočene za SSL, s pomočjo API-ja (QSYRGAP, QsyRegisterAppForCertUse), ki v DCM samodejno izdela ID aplikacije. Vse IBM-ove aplikacije, omogočene za SSL, so registrirane z Upravljalnikom digitalnih potrdil, tako da ga lahko uporabite za preprosto dodelitev potrdila aplikacijam, da lahko vzpostavijo sejo SSL. Za aplikacije, ki jih izdelate ali kupite, lahko definirate tudi definicijo aplikacije in zanjo izdelate ID aplikacije znotraj DCM. Za izdelavo definicije aplikacije SSL za aplikacijo odjemalca ali strežnika morate delati v prostoru potrdil *SYSTEM.

Če želite uporabljati potrdilo za podpisovanje objektov, morate najprej definirati aplikacijo, ki jo bo uporabilo potrdilo. Aplikacija za podpisovanje objektov za razliko od definicije aplikacije SSL ne opisuje dejanske aplikacije, Namesto tega utegne izdelana definicija aplikacije opisovati tip ali skupino objektov, ki jih nameravate podpisati. Za izdelavo definicije aplikacije za podpisovanje objektov morate delati v prostoru za potrdila *OBJECTSIGNING.

Preverjanje

Upravljalnik digitalnih potrdil (DCM) nudi naloge, s pomočjo katerih lahko preverite potrdilo ali aplikacijo in različne lastnosti, ki jih morata imeti oba.

Preverjanje veljavnosti potrdila

Ko preverite potrdilo, Upravljalnik digitalnih potrdil (DCM) preveri število postavk, ki se nanašajo na potrdilo, da zagotovi verodostojnost in veljavnost potrdila. S preverjanjem veljavnosti potrdila zagotovite, da se aplikacijam, ki uporabljajo potrdilo za zaščitene komunikacije ali podpisovanje objektov, prepreči, da bi naletele na težave pri uporabi potrdila.

Kot del preverjanja veljavnosti DCM preveri, ali izbrano potrdilo ni poteklo. Prav tako preveri, da potrdilo ni navedeno na seznamu za preklic potrdil (CRL) kot preklicano, če mesto CRL obstaja za službo za potrdila, ki je izdala potrdilo. DCM preveri tudi, ali se potrdilo službe za potrdila za izdajajočo službo za potrdila nahaja v trenutnem prostoru za potrdila in ali je služba za potrdila označena kot zaupanja vredna. Če ima potrdilo zasebni ključ (na primer, potrdilo strežnika ali odjemalca ali potrdilo za podpisovanje objektov), DCM preveri tudi par javno-zasebnih ključev, da zagotovi njihovo ujemanje. Z drugimi besedami to pomeni, da DCM šifrira podatke z javnim ključem, nato pa zagotovi, da jih je mogoče dešifrirati z zasebnim ključem.

Preverjanje veljavnosti aplikacije

Ko preverjate aplikacijo, Upravljalnik digitalnih potrdil (DCM) preveri, ali za aplikacijo obstaja dodelitev potrdila, in zagotovi da je dodeljeno potrdilo veljavno. V primeru, da je aplikacija konfigurirana za uporabo seznama overjenih služb za potrdila (CA), DCM tudi preveri, ali seznam overjenih služb vsebuje vsaj eno potrdilo službe za potrdila. Nato DCM preveri, ali so potrdila službe za potrdila na seznamu overjenih služb za potrdila aplikacije veljavna. Če definicija aplikacije predvideva obdelavo seznama za preklic potrdil (CRL) in za službo za potrdila obstaja definirano mesto CRL, DCM v okviru postopka preverjanja pregleda tudi CRL.

Preverjanje aplikacije vas lahko opozori na možne težave, na katere lahko naleti aplikacija med izvajanjem funkcije, ki zahteva potrdila. Takšne težave lahko aplikaciji preprečijo, da uspešno sodeluje v seji plasti zaščitenih vtičnic (SSL) ali da uspešno podpisuje objekte.

Poglavje 6. Načrt za DCM

Če želite Upravljalnik digitalnih potrdil (DCM) uporabljati za učinkovito upravljanje digitalnih potrdil vašega podjetja, morate imeti vsestranski načrt, kako boste digitalna potrdila uporabljali kot del načel zaščite.

V naslednjih temah se lahko naučite, kako načrtovati uporabo DCM ter kako se digitalna potrdila skladajo z vašimi načeli za zaščito:

Zahteve za uporabo DCM
V tej temi se boste naučili, katero programsko opremo morate namestiti, nudi pa tudi druge informacije, ki jih potrebujete za nastavitev sistema za uporabo DCM.

Premisleki o izdelavi varnostnih kopij in obnovitvah za podatke Upravljalnika digitalnih potrdil
S temi informacijami se naučite, kako zagotoviti pomembne podatke DCM, ki jih dodate načrtu izdelave varnostnih kopij in obnovitve za vaš sistem.

Tipi digitalnih potrdil
s pomočjo teh informacij spoznajte različne vrste potrdil, ki jih lahko upravlja DCM.

Javna potrdila v primerjavi z zasebnimi potrdili
Te informacije vam bodo pomagale določiti, katera vrsta potrdila najbolj ustreza vašim poslovnim potrebam. Pred tem se morate seveda odločiti, kako želite uporabljati potrdila za izkoriščanje dodatne zaščite, ki jo nudijo. Uporabite lahko potrdila javne službe za potrdila ali osnujete in vodite zasebno službo za potrdila in potrdila izdajate sami. Kako boste pridobili potrdila, je odvisno od tega, kako jih načrtujete uporabljati.

Digitalna potrdila za komunikacije plasti zaščitenih vtičnic (SSL)
Te informacije vam bodo pomagale razumeti, kako uporabljati potrdila, tako da bodo vaše aplikacije lahko vzpostavljale zaščitene komunikacijske seje.

Digitalna potrdila za overjanje uporabnikov
Te informacije vam bodo pomagale razumeti, kako uporabljati potrdila za natančnejše overjanje uporabnikov, ki dostopajo do sredstev strežnika iSeries.

Digitalna potrdila in preslikava istovetnosti podjetja (EIM)
S pomočjo teh informacij se naučite, kako uporabiti DCM skupaj z EIM.

Digitalna potrdila za overjanje povezav navideznega zasebnega omrežja (VPN)
Te informacije vam bodo pomagale razumeti, kako uporabljati potrdila kot del konfiguriranja povezave VPN.

Digitalna potrdila za podpisovanje objektov
Te informacije vam bodo pomagale razumeti, kako s potrdili zagotoviti integriteto objekta ali preveriti digitalni podpis objekta in s tem njegovo pristnost.

Digitalna potrdila za preverjanje podpisov objekta
Te informacije vam bodo pomagale razumeti, kako s potrdili preveriti digitalni podpis objekta in s tem njegovo pristnost.

Zahteve za nastavitev upravljalnika digitalnih potrdil

Upravljalnik digitalnih potrdil (DCM) je brezplačna komponenta, ki omogoča osrednje upravljanje digitalnih potrdil za vaše aplikacije. Za uspešno uporabo Upravljalnika digitalnih potrdil naredite naslednje:

- Namestite licenčnih program ponudnika šifriranega dostopa (5722–AC3). Ta izdelek za šifriranje določa najdaljšo dolžino ključa, ki je dovoljena za šifrirne algoritme na osnovi izvoznih in uvoznih določb. Ta izdelek morate namestiti, preden lahko izdelate potrdila.
- Namestite možnost 34 v i5/OS. To je funkcija DCM, ki temelji na pregledovalniku.
- Namestite IBM-ov Strežnik HTTP za iSeries (5722–DG1) in poženite primerek strežnika za upravljanje.
- Prepričajte se, da je za vaš sistem konfiguriran TCP/IP, tako da lahko s spletnim pregledovalnikom in primerkom strežnika za upravljanje HTTP dostopate do upravljalnika digitalnih potrdil.

Opomba: Če ne boste namestili vseh zahtevanih izdelkov, ne boste mogli izdelati potrdil. Če zahtevan izdelek ni nameščen, DCM prikaže sporočilo o napaki, ki vam svetuje, da namestite manjkajočo komponento.

Premisleki o izdelavi varnostnih kopij in obnovitvah za podatke Upravljalnika digitalnih potrdil

Šifrirana gesla baze podatkov ključev, s pomočjo katerih dostopate do prostorov za potrdila v Upravljalniku digitalnih potrdil (DCM) so shranjena ali *spravljena* v posebni varnostni datoteki na strežniku. Ko z Upravljalnikom digitalnih potrdil izdelate prostor za potrdila v sistemu, Upravljalnik digitalnih potrdil samodejno spravi geslo namesto vas. Sami pa morate zagotoviti, da Upravljalnik digitalnih potrdil spravi gesla prostora za potrdila v določenih okoliščinah.

Ena takšnih okoliščin je, ko s pomočjo Upravljalnika digitalnih potrdil izdelate potrdilo za drug strežnik in izberete, da boste z datotekami potrdila v ciljnem sistemu izdelali nov prostor za potrdila. V tem primeru morate odpreti pravkar izdelan prostor za potrdila in z uporabo naloge **Spreminjanje gesla** spremeniti geslo prostora za potrdila v ciljnem sistemu, s čimer zagotovite, da bo Upravljalnik digitalnih potrdil spravil novo geslo. Če je prostor za potrdila Drugi sistemski prostor za potrdila, podajte tudi, da želite pri spreminjanju gesla uporabiti možnost **Samodejna prijava**. Podrobnejše informacije o izdelovanju potrdil za druge strežnike z Upravljalnikom digitalnih potrdil najdete v Uporaba lokalne službe za potrdila za izdajanje potrdil drugim strežnikom.

Vedno, ko spremenite ali na novo nastavite geslo za Drug sistemski prostor za potrdila, morate podati tudi možnost **Samodejne prijave**.

Če želite zagotoviti, da boste imeli celotno varnostno kopijo pomembnih podatkov DCM, naredite naslednje:

- Z ukazom (SAV) shranite vse datoteke .KDB in .RDB. Vsak prostor za potrdila DCM je sestavljen iz dveh datotek, ene s pripono .KDB in druge s pripono .RDB.
- Z ukazoma SAVSYS (shrani sistem) in SAVSECDTA (shrani varnostne podatke) shranite posebno varnostno datoteko, ki vsebuje gesla baze podatkov ključev za dostop do prostora za potrdila. Če želite obnoviti varnostno datoteko gesla DCM, izdajte ukaz RSTUSRPRF (obnovi uporabniške profile) in za možnost uporabniškega profila (USRPRF) podajte *ALL.

Druga problematika obnovitve zadeva uporabo operacije SAVSECDTA in možnosti, da trenutna gesla prostora za potrdila postanejo neusklajena z gesli v varnostni datoteki s shranjenim geslom DCM. Če geslo za prostor za potrdila spremenite zatem, ko shranite operacijo SAVSECDTA, a preden obnovite podatke te operacije, postane veljavno geslo prostora za potrdila neusklajeno z geslom v obnovljeni datoteki.

Če se želite temu izogniti, morate s pomočjo naloge **Spreminjanje gesla** (v **Upravljanje prostora za potrdila** v oknu za usmerjanje) v DCM spremeniti gesla za prostore za potrdila, potem ko obnovite podatke operacije SAVSECDTA, da zagotovite vnovično usklajenost gesel. V tem primeru ne uporabite gumba **Vnovična nastavitev gesla**, ki se prikaže, ko izbirate prostor za potrdila, ki ga želite odpreti. Če poskusite znova nastaviti geslo, DCM namreč poskusi priklicati spravljeno geslo. Če spravljeno geslo ni usklajeno s trenutnim geslom, operacija vnovične nastavitve ne bo uspela. Če gesel prostorov za potrdila ne spreminjate pogosto, morda velja razmisliti o izvedbi SAVSECDTA ob vsaki spremembi gesla, saj boste s tem imeli zmeraj shranjeno najnovejšo spravljeno različico gesla, kar vam bo v pomoč, če boste slučajno kdaj morali obnoviti te podatke.

Tipi digitalnih potrdil

Obstaja več klasifikacij digitalnih potrdil. Te klasifikacije opisujejo uporabo potrdila. Upravljalnik digitalnih potrdil lahko uporabite za upravljanje naslednjih vrst potrdil:

Potrdila službe za pooblastila
Potrdilo službe za potrdila je digitalno priporočilo, ki preveri identiteto službe za potrdila (CA), ki je lastnik potrdila. Potrdilo službe za potrdila vsebuje identifikacijske informacije o službi za potrdila, kot tudi njen javni ključ. Drugi uporabniki lahko z javnim ključem potrdila službe za potrdila preverijo pristnost potrdil, ki jih izda in podpiše služba za potrdila. Potrdilo službe za potrdila lahko podpiše druga služba za potrdila, kot je na primer VeriSign, ali pa je lastnoročno podpisano, če je neodvisna enota. Lokalna služba za potrdila, ki jo izdelate in vodite z Upravljalnikom digitalnih potrdil je neodvisna enota. Drugi uporabniki lahko z javnim ključem potrdila službe za potrdila preverijo pristnost potrdil, ki jih izda in podpiše služba za potrdila. Če želite potrdilo uporabiti za SSL, podpisovanje objektov ali preverjanje podpisov objektov, morate imeti tudi kopijo potrdila izdajajoče službe za potrdila.

Potrdila strežnika ali odjemalca.
Potrdilo strežnika ali odjemalca je digitalno priporočilo, ki določa aplikacijo strežnika ali odjemalca, ki uporablja potrdilo za zaščitene komunikacije. Potrdila strežnika ali odjemalca vsebujejo identifikacijske informacije o podjetju, ki je lastnik aplikacije, kot je na primer razločevalno ime sistema. Potrdilo vsebuje tudi javni ključ sistema. Strežnik mora imeti digitalno potrdilo, če hoče za zaščitene komunikacije uporabljati plast zaščitenih vtičnic (SSL). Aplikacije, ki podpirajo digitalna potrdila, lahko pregledajo potrdilo strežnika in preverijo identiteto strežnika, ko odjemalec dostopi do njega. Aplikacija lahko nato uporabi overjeno potrdilo kot osnovno za vzpostavitev s plastjo zaščitenih vtičnic šifrirane seje med odjemalcem in strežnikom. Te vrste potrdil lahko upravljate le iz prostora za potrdila *SYSTEM.

Potrdila za podpis objektov
Potrdilo za podpis objekta je potrdilo, ki ga uporabite za digitalno ″podpisovanje″ objekta. S podpisom objekta omogočite pomene, s katerimi lahko preverite neokrnjenost objekta ter izvor ali lastništvo objekta. S potrdili lahko podpisujete številne objekte, vključujoč večino objektov v integriranem datotečnem sistemu in objektov *CMD. Celoten seznam objektov, ki jih je mogoče podpisati, lahko najdete v temi Podpisovanje objektov ter preverjanje podpisov. Če za podpis objekta uporabite zasebni ključ potrdila za podpis objektov, mora imeti prejemnik objekta dostop do kopije ustreznega potrdila za preverjanje podpisa, s katerim lahko pravilno overi podpis objekta Te vrste potrdil lahko upravljate le iz prostora za potrdila *OBJECTSIGNING.

Potrdila za preverjanje podpisov
Potrdilo za preverjanje podpisa je kopija potrdila za podpisovanje objektov, le da ne vsebuje zasebnega ključa tega potrdila. Z javnim ključem potrdila za preverjanje podpisa lahko overite digitalni podpis, izdelan s potrdilom za podpis objekta. Preverjanje podpisa omogoča, da določite izvor objekta ter podatek o tem, ali je bil spremenjen od zadnjega podpisa. Te vrste potrdil lahko upravljate le iz prostora za potrdila *SIGNATUREVERIFICATION.

Uporabniška potrdila
Uporabniško potrdilo je digitalno priporočilo, ki preverja identiteto odjemalca ali uporabnika, ki je lastnik potrdila. Številne aplikacije zdaj nudijo podporo, ki omogoča uporabo potrdil za overjanje uporabnikov namesto imen uporabnikov in gesel. Upravljalnik digitalnih potrdil (DCM) samodejno poveže uporabniška potrdila, ki jih izda vaša zasebna služba za potrdila, s profilom uporabnika. S pomočjo Upravljalnika digitalnih potrdil lahko tudi povežete uporabniška potrdila, ki jih izda kakšna druga služba za potrdila, s profilom uporabnika.

Če potrdila upravljate z Upravljalnikom digitalnih potrdil (DCM), jih DCM razporedi in shrani skupaj s povezanimi zasebnimi ključi v prostor za potrdila glede na njihovo razvrstitev.

Opomba: Če je IBM-ov Šifrirni koprocesor nameščen na strežniku, lahko za vaša potrdila izberete drugo možnost shranitve zasebnega ključa (z izjemo potrdil za podpisovanje objektov). Shranite lahko tudi zasebni ključ samega šifrirnega koprocesorja. Ali pa s šifrirnim koprocesorjem šifrirate zasebni ključ in ga namesto v prostor za potrdila shranite v posebno datoteko ključev. Uporabniška potrdila in njihovi zasebni ključi so shranjeni v sistemu uporabnika in sicer v programski opremi pregledovalnika ali v datoteki, ki jo lahko uporabljajo drugi paketi programske opreme odjemalcev.

Javna potrdila v primerjavi z zasebnimi potrdili

Ko se odločite, da boste uporabljali potrdila, morate izbrati tip izvedbe potrdil, ki najbolj ustreza vašim varnostnim potrebam. Možnosti, ki so na voljo za pridobitev potrdil, vključujejo naslednje:
- nakup potrdila javne internetne službe za potrdila (CA)
- Vodenje lastne lokalne službe za potrdila in izdajanje zasebnih potrdil uporabnikom in aplikacijam.
- Uporaba kombinacije potrdil javnih internetnih služb za potrdila in lastne lokalne službe za potrdila.

Katero izvedbo boste uporabili, je odvisno od številnih dejavnikov, med njimi pa je najpomembnejše okolje, v katerem uporabljate potrdila. Sledi nekaj informacij, ki vam bodo pomagale določiti, katera izvedba je najprimernejša za vaše poslovne in varnostne zahteve.

Uporaba javnih potrdil

Javne internetne službe za potrdila izdajajo potrdila vsem, ki plačajo zahtevano članarino. Toda kljub temu internetna služba za potrdila pred izdajo potrdila zahteva dokazilo identitete. Ta raven dokazila se spreminja glede na identifikacijska načela službe za potrdila. Presodite, ali strogost identifikacijskih načel službe za potrdila ustreza vašim varnostnim potrebam, šele nato se odločite, ali boste prejemali in zaupali potrdilom, ki jih izdaja. Ker so se standardi

PKIX (infrastruktura javnega ključa za X.509) razvili, javne službe za potrdila nudijo precej ostrejše identifikacijske standarde za izdajanje potrdil. Čeprav je postopek pridobivanja potrdil pri takšnih službah za potrdila PKIX zahtevnejši, njihova potrdila nudijo boljše jamstvo za varen dostop do aplikacij. Upravljalnik digitalnih potrdil (DCM) omogoča, da uporabite in upravljate potrdila služb za potrdila PKIX, ki uporabljajo te nove standarde.

Razmisliti morate tudi o stroških, ki jih zaračuna javna služba za izdajanje potrdil. Če potrdila potrebujete za omejeno število aplikacij strežnikov ali odjemalcev in uporabnikov, stroški morda ne igrajo posebne vloge. Toda cena postane še kako pomembna, če imate veliko *zasebnih* uporabnikov, ki potrebujejo javna potrdila za overjanje odjemalca. V tem primeru morate razmisliti tudi o upravnih in programskih zadevah, potrebnih za konfiguriranje aplikacij strežnika, da sprejmejo samo določeno podmnožico potrdil, ki jih izda javna služba za potrdila.

Uporaba potrdil javne službe za potrdila vam lahko prihrani veliko časa in sredstev, saj je veliko strežniških, odjemalskih in uporabniških aplikacij konfiguriranih tako, da prepozna večino znanih služb za potrdila. Druga podjetja in uporabniki utegnejo bolj zaupati potrdilom, ki jih izdaja znana javna služba za potrdila, kot potrdilom, ki jih izdaja vaša zasebna lokalna služba za potrdila.

Uporaba zasebnih potrdil

Če izdelate lastno lokalno službo za potrdila, lahko izdajate potrdila sistemom in uporabnikom znotraj omejenega območja, kot je na primer podjetje ali organizacija. Izdelava in vzdrževanje lastne lokalne službe za potrdila vam omogoča, da izdajate potrdila samo uporabnikom, ki so člani vaše skupine in jim zaupate. To zagotavlja večjo zaščito, ker vedno veste, kdo ima potrdilo in lahko učinkoviteje nadzirate dostop do sredstev. Možna slabost vzdrževanja lastne lokalne službe za potrdila sta čas in sredstva, ki jih morate vložiti. Vendar pa je z Upravljalnikom digitalnih potrdil (DCM) ta postopek zelo poenostavljen.

Če uporabnikom izdajate potrdila za overjanje odjemalcev z uporabo lokalne službe za potrdila, se morate odločiti, kam želite shraniti uporabniška potrdila. Če uporabniki pridobijo potrdila lokalne službe za potrdila prek DCM, so njihova potrdila po privzetku shranjena skupaj z uporabniškim profilom. DCM lahko konfigurirate za delo s preslikavo istovetnosti podjetja (EIM) tako, da bodo potrdila namesto tega shranjena na mesto poenostavljenega protokola imeniškega dostopa (LDAP). (Več informacij o skupnem delovanju DCM in EIM najdete v Digitalna potrdila in preslikava istovetnosti podjetja (EIM).) Če uporabniških potrdil na noben način ne želite povezati ali shraniti z uporabniškim profilom , lahko z API-ji programsko izdajate potrdila uporabnikom, ki nimajo sistema iSeries.

Opomba: Ne glede na to, s katero službo za potrdila izdajate potrdila, sistemski skrbnik vedno odloča, katerim službam za potrdila bodo zaupale aplikacije v njegovem sistemu. Če je kopijo potrdila znane službe za potrdila mogoče najti v vašem pregledovalniku, lahko pregledovalnik nastavite tako, da zaupa potrdilom strežnika, ki jih je izdala ta služba za potrdila. Skrbniki nastavijo zaupanje potrdilom službe za potrdila v ustreznem prostoru za potrdila DCM, ki vsebuje kopije potrdil večine najbolj znanih javnih služb za potrdila. Če pa potrdila službe za potrdila ni v vašem prostoru za potrdila, strežnik ne more zaupati potrdilom uporabnikov ali odjemalcev, ki jih je izdala ta služba za potrdila, dokler si ne priskrbite in uvozite kopije potrdila te službe. Potrdilo službe za potrdila mora biti v pravilnem formatu datoteke, vi pa ga morate dodati v vaš prostor za potrdila DCM.

Pri odločitvi, ali so za vaše poslovne in varnostne zahteve bolj primerna javna ali zasebna potrdila, vam bo morda pomagalo, če si boste ogledali nekaj scenarijev, ki kažejo splošno uporabo potrdil.

S tem povezane naloge

Ko se boste odločili, kako želite uporabljati potrdila in katerega tipa, preglejte naslednje postopke, da se boste naučili, kako z Upravljalnikom digitalnih potrdil realizirati vaš načrt.

- Izdelava in vodenje zasebne službe za potrdila opisuje naloge, ki jih morate izvesti, če želite voditi lokalno službo za potrdila in izdajati zasebna potrdila.
- Upravljanje potrdil javne internetne službe za potrdila opisuje naloge, ki jih morate opraviti za uporabo potrdil znane javne službe za potrdila, vključno s službo za potrdila PKIX.

- Uporaba lokalne službe za potrdila v drugih strežnikih opisuje naloge, ki jih morate izvesti, če želite uporabljati potrdila zasebne službe za potrdila v več kot enem sistemu.

Digitalna potrdila za zaščitene komunikacije SSL

Digitalna potrdila lahko uporabite za konfiguriranje aplikacij za uporabo plasti zaščitenih vtičnic (SSL) za zaščitene komunikacijske seje. Za vzpostavitev seje SSL ima vaš strežnik vedno na voljo kopijo potrdila, katere veljavnost lahko preveri odjemalec, ki zahteva povezavo. Uporaba povezave SSL:

- zagotavlja pristnost odjemalca ali končnega uporabnika
- nudi šifrirano komunikacijsko sejo, ki zagotavlja zasebnost podatkov, ki potujejo prek povezave.

Aplikacije strežnika in odjemalca takole sodelujejo pri zagotavljanju zaščite podatkov:

1. Aplikacija strežnika predloži potrdilo aplikaciji odjemalca (uporabnika) kot dokaz identitete strežnika.
2. Aplikacija odjemalca preveri istovetnost strežnika glede na kopijo potrdila izdajajoče službe za potrdila. (Aplikacija odjemalca mora imeti dostop do lokalno shranjene kopije ustreznega potrdila službe za potrdila.)
3. Aplikacije strežnika in odjemalca se sporazumejo o uporabi simetričnega ključa za šifriranje in z njim šifrirajo komunikacijske seje.
4. Preden strežnik omogoči dostop do zahtevanih sredstev, lahko zahteva od odjemalca, da predloži dokaz svoje identitete. Za uporabo potrdil kot dokaza identitete morajo komunikacijske aplikacije podpirati uporabo potrdil za overjanje uporabnikov.

SSL med začetno obdelavo SSL uporablja algoritme asimetričnih ključev (javni ključi), da prejme simetrični ključ, ki ga pozneje uporabi za šifriranje in dešifriranje podatkov aplikacije za to sejo SSL. To pomeni, da uporabljata strežnik in odjemalec različne ključe za sejo, katerih veljavnost za vsako povezavo samodejno poteče po nastavljenem obdobju. V malo verjetnem primeru, da nekdo prestreže in dešifrira ključ določene seje, ga ne more uporabiti za izpeljavo nadaljnjih ključev.

Digitalna potrdila za overjanje uporabnikov

Običajno dodelita uporabnikom dostop do sredstev aplikacija ali sistem na osnovi imena uporabnika in gesla. Zaščito sistema lahko še izboljšate z uporabo digitalnih potrdil (namesto imen uporabnikov in gesel), s katerimi overite in pooblastite seje med številnimi aplikacijami strežnika in uporabniki. S pomočjo Upravljalnika digitalnih potrdil lahko povežete potrdilo uporabnika z uporabniškim profilom tega uporabnika ali istovetnostjo drugega uporabnika. Potrdilo ima nato ista pooblastila in dovoljenja kot z njim povezana istovetnost uporabnika ali njegov uporabniški profil. Prav tako lahko sežete po API-jih in programsko uporabite zasebno lokalno službo za pooblastila za izdajanje potrdil uporabnikom, ki ne uporabljajo iSeries. API-ji vam omogočajo, da izdajate zasebna potrdila uporabnikom, za katere ne želite, da imajo uporabniški profil ali drugo notranjo uporabniško istovetnost.

Digitalno potrdilo deluje kot elektronsko priporočilo, ki preveri, ali je oseba, ki ga predloži, v resnici tista, za katero se predstavlja. V tem oziru je potrdilo podobno potnemu listu. Oba dokazujeta identiteto posameznika, vsebujeta enkratno številko za identifikacijske namene in imata spoznavno službo za izdajanje, ki preveri priporočilo kot pristno. V primeru potrdila deluje služba za potrdila (CA) kot overjena tretja stranka, ki izda potrdilo in ga potrdi kot pristnega.

Potrdila uporabljajo pri overjanju javni ključ in z njim povezan zasebni ključ. Izdajna služba za potrdila poveže ta ključa skupaj z drugimi informacijami o lastniku potrdila v samo potrdilo.

Vedno več aplikacij nudi podporo za uporabo potrdil za overjanje odjemalca med sejo SSL. Trenutno te aplikacije nudijo podporo za potrdilo za overjanje odjemalca:

- strežnik Telnet
- IBM-ov Strežnik HTTP (poganja ga Apache)
- IBM-ov Imeniški strežnik
- iSeries Access za Windows (vključuje Navigatorja iSeries)
- strežnik FTP

Čez čas bodo dodatne aplikacije morda nudile podporo za overjanje potrdil odjemalce. Preglejte dokumentacijo za specifične aplikacije in ugotovite, ali nudijo to podporo.

Potrdila nudijo izboljšano overjanje uporabnikov zaradi več razlogov:
- Ker obstaja možnost, da uporabnik pozabi svoje geslo, si mora zapomniti ali zapisati ime uporabnika in geslo. Posledično si lahko nepooblaščeni uporabniki z lahkoto preskrbijo imena uporabnikov in gesla pooblaščenih uporabnikov. Ker so potrdila shranjena v datoteki ali na drugem elektronskem mestu, vodijo aplikacije odjemalca (namesto uporabnika) dostopanje do potrdila in njegovo predložitev za overjanje. Na ta način je manj verjetno, da bi uporabniki delili potrdila z nepooblaščenimi uporabniki, razen če le-ti nimajo dostopa do sistema uporabnika. Potrdila lahko namestite tudi na ″pametne kartice″ kot dodatno zaščito pred nepooblaščeno uporabo.
- Potrdilo vsebuje zasebni ključ, ki ni nikoli poslan s potrdilom za identifikacijo. Sistem uporabi ta ključ med postopkom šifriranja in dešifriranja. Drugi uporabniki lahko z ustreznim javnim ključem potrdila preverijo identiteto pošiljatelja objektov, ki so podpisani z zasebnim ključem.
- Številni sistemi zahtevajo gesla, dolga osem znakov ali manj, ki jih je zelo lahko uganiti. Šifrirni ključi potrdila so dolgi na stotine znakov. Zaradi dolžine ključev in njihove naključne sestavljenosti je šifrirne ključe mnogo težje uganiti kot gesla.
- Ključe digitalnih potrdil je mogoče uporabiti na številne načine, ki jih gesla ne nudijo, kot sta na primer integriteta podatkov in zasebnost. Potrdila in z njimi povezani ključi omogočajo naslednje:
  - Zagotovitev integritete podatkov z odkrivanjem sprememb v podatkih.
  - Dokazilo, da je bilo določeno dejanje v resnici opravljeno. To se imenuje potrditev.
  - Zagotovitev zasebnosti prenosov podatkov z uporabo plasti zaščitenih vtičnic (SSL) za šifriranje komunikacijskih sej.

Če se želite podrobneje seznaniti s konfiguriranjem aplikacij strežnika za uporabo potrdil za overjanje odjemalcev med sejo SSL, si oglejte temo Plast zaščitenih vtičnic (SSL) v Informacijskem centru iSeries.

Digitalna potrdila in preslikava istovetnosti podjetja (EIM)

Preslikava istovetnosti podjetja (EIM) je tehnologija eServerja, s pomočjo katere lahko upravljate uporabniške istovetnosti v vašem podjetju, vključujoč profile in potrdila uporabnikov. Uporabniško ime in geslo je najpogostejša oblika uporabniške istovetnosti; drugo obliko predstavljajo potrdila. Nekatere aplikacije so konfigurirane tako, da uporabnikom omogočajo overjanje z uporabniškim potrdilom in ne z uporabniškim imenom in geslo.

EIM lahko uporabite za izdelavo preslikav med istovetnostmi uporabnikov, s čimer se lahko uporabnik overi z eno uporabniško istovetnostjo in dostopa do sredstev druge uporabniške istovetnosti, ne da bi to moral predložiti. To v EIM dosežete tako, da definirate povezavo med eno in drugo uporabniško istovetnostjo. Uporabniške istovetnosti so lahko v različnih oblikah, tudi v obliki uporabniških potrdil. Izdelate lahko bodisi posamezne povezave med identifikatorjem EIM in različnimi uporabniškimi istovetnostmi, pripadajočih uporabniku, ki ga predstavlja ta identifikator EIM. Lahko pa izdelate tudi povezave načel, ki preslikajo skupino uporabniških istovetnosti v eno samo ciljno uporabniško istovetnost. Uporabniške istovetnosti so lahko v različnih oblikah, tudi v obliki uporabniških potrdil. Ko izdelate te povezave, je mogoče uporabniška potrdila preslikati v ustrezne identifikatorje EIM in tako olajšati uporabo potrdil za overjanje.

Če želite da funkcija EIM upravlja potrdila uporabnikov, morate izvesti naslednje naloge za konfiguriranje EIM, preden pričnete izvajati naloge za konfiguriranje DCM:

1. S pomočjo čarovnika za **Konfiguriranje EIM** v Navigatorju **iSeries** konfigurirajte EIM.
2. Za vsakega uporabnika, za katerega želite, da sodeluje v EIM, izdelajte identifikator EIM.
3. Izdelajte ciljno povezavo med vsakim identifikatorjem EIM in profilom uporabnika v lokalnem uporabniškem registru i5/OS, tako da je mogoče vsa uporabniška potrdila, ki jih prek DCM v DCM izdela uporabnik, mogoče preslikati v uporabniški profil. Uporabite definicijsko ime registra EIM za lokalni uporabniški register i5/OS, ki ste ga podali s čarovnikom za **Konfiguriranje EIM**. **Opomba:** Več informacij o konfiguriranju EIM vam je na voljo v temi EIM.

Ko dokončate potrebne naloge konfiguriranja EIM, morate z uporabo naloge **Upravljanje mesta LDAP** konfigurirati Upravljalnik digitalnih potrdil (DCM) in uporabniška potrdila ne shranite skupaj z uporabniškim profilom, temveč jih

shranite na mesto LDAP. Če konfigurirate EIM in DCM, da delujeta skupaj, naloga **Izdelava potrdila** za uporabniška potrdila in naloga **Dodelitev uporabniškega potrdila** obdelata potrdila za uporabo EIM, namesto da bi jih dodelili uporabniškemu profilu. DCM potrdilo shrani v konfiguriran imenik LDAP in s pomočjo razločevalnega imena potrdila za ustrezen identifikator EIM izdela izvorno povezavo. S tem lahko operacijski sistemi in aplikacije potrdilo uporabljajo kot vir operacije iskanja preslikav EIM za preslikovanje iz potrdila v ciljno uporabniško istovetnost, povezano z istim identifikatorjem EIM.

Če konfigurirate EIM in DCM za skupno delovanje, lahko z uporabo DCM-a preverite datum zapadlosti uporabniškega potrdila na ravni podjetja, in ne zgolj na ravni sistema.

Digitalna potrdila za povezave VPN

Digitalna potrdila lahko uporabite kot načine za vzpostavljanje povezave navideznega zasebnega omrežja (VPN). Obe strani dinamične povezave VPN morata pred aktiviranjem povezave overiti ena drugo. Overjanje zaključne točke opravi strežnik za izmenjavo internetnih ključev (IKE) na vsaki strani. Po uspešnem overjanju strežniki IKE pogodijo način šifriranja in algoritme, ki jih bodo uporabili za zaščito povezave VPN.

Ena izmed metod, ki jo lahko za medsebojno overjanje uporabijo strežniki IKE, je ključ z vnaprej določeno skupno rabo. Vendar uporaba ključa z vnaprej določeno skupno rabo ni zelo varna, saj morate ključ skrbniku druge končne točke vašega VPN posredovati ročno. Zato se lahko zgodi, da bo ključ pri posredovanju kdo prestregel.

Tej nevarnosti se lahko izognete z uporabo digitalnih potrdil, s katerimi namesto uporabe ključa z vnaprej določeno skupno rabo overite zaključne točke. Strežnik IKE lahko overi potrdilo drugega strežnika in vzpostavi povezavo ter pogodi načine šifriranja in algoritme, ki jih bodo strežniki uporabljali za zaščito povezave.

Za upravljanje potrdil, ki jih strežnik IKE uporablja za vzpostavitev dinamične povezave VPN, lahko uporabite Upravljalnik digitalnih potrdil (DCM). Najprej se morate odločiti, ali boste za strežnik IKE uporabljali javna potrdila ali boste izdajali zasebna potrdila.

Nekatere izvedbe VPN zahtevajo, da potrdilo poleg standardnih informacij o razločevalnem imenu vsebuje tudi informacije o drugem imenu predmeta, kot je na primer ime domene ali naslov elektronske pošte. Če uporabite lokalno službo za potrdila v upravljalniku digitalnih potrdil za izdajo potrdila, lahko za potrdilo podate informacije o drugem imenu predmeta. S podajanjem teh informacij zagotovite, da je povezava VPN združljiva z drugimi izvedbami VPN, ki jih lahko zahtevajo za overjanje.

Če se želite podučiti o tem, kako upravljati potrdila za povezave VNP, preglejte naslednje vire:

- Če za upravljanje potrdil niste še nikdar uporabili Upravljalnika digitalnih potrdil, vam bodo pomagale naslednje teme:
  - Osnovanje in vodenje lokalne, zasebne službe za potrdila opisuje, kako uporabljati Upravljalnik digitalnih potrdil za izdajanje zasebnih potrdil za aplikacije.
  - Upravljanje potrdil javne internetne službe za potrdila opisuje, kako uporabljati Upravljalnik digitalnih potrdil za delo s potrdili javne službe za potrdila.
- Če trenutno uporabljate Upravljalnik digitalnih potrdil za upravljanje potrdil za druge aplikacije, preglejte naslednje vire, da se boste podučili, kako podati, da aplikacija uporablja obstoječe potrdilo in katera potrdila lahko sprejme aplikacija in overi:
  - Upravljanje dodelitev potrdil za aplikacijo opisuje, kako uporabljati Upravljalnik digitalnih potrdil za dodeljevanje obstoječega potrdila aplikaciji, kot je na primer strežnik IKE.
  - Definiranje seznama overjenih služb za potrdila za aplikacijo opisuje, kako podati, katerim službam za potrdila lahko zaupa aplikacija pri sprejemanju potrdil za overjanje odjemalca (ali VPN).

Digitalna potrdila za podpisovanje objektov

i5/OS nudi podporo za uporabo potrdil za digitalno podpisovanje objektov. Z digitalnim podpisovanjem objektov zagotovite neokrnjenost vsebine objekta in njegov izvor. Podpora za podpisovanje objektov izboljšuje tradicionalna sistemska orodja za nadzorovanje tega, kdo lahko spreminja objekte. Tradicionalna orodja za nadzorovanje ne morejo zaščititi nepooblaščenega vdora pri prehodu objekta prek interneta ali drugega neoverjenega omrežja ali če je objekt shranjen v sistemu, ki ni iSeries. Tudi tradicionalni krmilni elementi ne morejo vedno določiti, ali so bile izvedene nepooblaščene spremembe ali poskusi spreminjanja objekta. Z uporabo digitalnih potrdil na objektih zagotavljate trdne načine odkrivanja sprememb v podpisanih objektih.

Digitalni podpis objekta pomeni uporabo zasebnega ključa potrdila, ki objektu doda šifriran matematičen povzetek podatkov. Podpis ščiti podatke pred nepooblaščenim spreminjanjem. Objekt in njegova vsebina nista šifrirana z digitalnim podpisom, pač pa je šifriran povzetek, ki preprečuje nepooblaščeno spreminjanje. Vsakdo, ki želi zagotoviti, da objekt pri prehodu ni bil spremenjen in da izhaja iz sprejetega, zakonitega izvora, lahko uporabi javni ključ potrdila in preveri izvorni digitalni podpis. Če se podpis ne ujema, so bili podatki morda spremenjeni. V tem primeru se lahko sprejemnik izogne uporabi objekta in namesto tega prosi podpisnika, naj pošlje drugo kopijo podpisanega objekta.

Če se odločite, da uporaba digitalnih podpisov ustreza vašim varnostnim potrebam in načelom, morate oceniti, ali je za vas primernejša uporaba javnih ali izdajanje zasebnih potrdil. . Če nameravate razdeljevati objekte javnim uporabnikom, bi morda veljalo premisliti o uporabi potrdil znane javne službe za potrdila (CA) za podpisovanje objektov. Z uporabo javnih potrdil zagotovite, da lahko drugi uporabniki preprosto in poceni preverijo podpise, ki jih dodate posredovanim objektom. Če pa nameravate objekte posredovati zgolj znotraj podjetja, lahko s pomočjo Upravljalnika digitalnih potrdil (DCM) osnujete lastno lokalno službo za potrdila in izdajate potrdila za podpisovanje objektov. Uporaba zasebnih potrdil iz lokalne službe za potrdila je cenejša kot nakup potrdil pri dobro znani javni službi za potrdila.

Podpis objekta predstavlja sistem, ki je podpisal objekt in ne določenega uporabnika v tem sistemu (čeprav mora imeti uporabnik ustrezno pooblastilo za uporabo potrdila za podpisovanje objektov). Za upravljanje potrdil, ki so vam v pomoč pri podpisovanju objektov in preverjanju podpisov objektov, lahko uporabite DCM. DCM lahko uporabite tudi za podpisovanje objektov ter preverjanje podpisov objektov.

Digitalna potrdila za preverjanje podpisov objekta

i5/OS nudi podporo za uporabo potrdil pri preverjanju digitalnih podpisov na objektih. Vsakdo, ki želi zagotoviti, da podpisani objekt pri prehodu ni bil spremenjen in da izhaja iz sprejetega, zakonitega izvora, lahko uporabi javni ključ potrdila in preveri izvorni digitalni podpis. Če se podpis ne ujema, so bili podatki morda spremenjeni. V tem primeru se lahko sprejemnik izogne uporabi objekta in namesto tega prosi podpisnika, naj pošlje drugo kopijo podpisanega objekta.

Podpis objekta predstavlja sistem, ki je podpisal objekt in ne določenega uporabnika v tem sistemu. Kot del postopka preverjanja digitalnih podpisov se morate odločiti, kateri službi za potrdila boste zaupali in katerim potrdilom boste zaupali za podpisovanje objektov. Če izberete, da boste zaupali službi za potrdila (CA), lahko izberete tudi, ali boste zaupali podpisom, izdelanih z uporabo potrdila, ki ga je izdala služba za potrdila, ki ji zaupate. Če izberete, da ne boste zaupali službi za potrdila, izberete tudi, da ne boste zaupali potrdilom, ki jih izda služba za potrdila ali podpisom, ki jih nekdo izdela z uporabo teh potrdil.

Sistemska vrednost QVFYOBJRST (Preveri obnovitev objekta)

Če se odločite, da boste preverjali veljavnost podpisov, je ena izmed prvih pomembnih odločitev, ki jih morate opraviti, določiti, kako pomembni so podpisi za objekte, ki jih obnavljate v sistemu. To lahko nadzorujete s sistemsko vrednostjo QVFYOBJRST (preveri podpise objektov med obnovitvijo). Privzeta nastavitev za to sistemsko vrednost omogoča obnavljanje nepodpisanih objektov, toda zagotavlja, da je podpisane objekte mogoče obnoviti, samo če imajo veljaven podpis. Sistem definira objekt kot podpisan, samo če ima podpis, ki mu sistem zaupa. Sistem bo zanemaril neoverjene podpise na objektih in objekte obravnaval kot nepodpisane.

Za sistemsko vrednost QVFYOBJRST lahko uporabite številne vrednosti, od tega, da zanemarite vse podpise, do tega, da zahtevate veljavne podpise za vse objekte, ki jih sistem obnovi. Ta sistemska vrednost vpliva samo na izvršilne objekte, ki so v obnovi, ne pa na shranjevalne datoteke ali integrirane datotečne sisteme. Če želite izvedeti več o tej in drugih sistemskih vrednostih, si oglejte Iskalnik sistemskih vrednosti v Informacijskem centru iSeries.

S pomočjo Upravljalnika digitalnih potrdil (DCM) lahko izvajate potrdilo in odločitve o zaupanju službe za potrdila, kot tudi upravljate potrdila, ki jih uporabljate za preverjanje podpisov objektov. DCM lahko uporabite tudi za podpisovanje objektov ter preverjanje podpisov objektov.

Poglavje 7. Konfiguriranje DCM

Upravljalnik digitalnih potrdil (DCM) je na pregledovalniku temelječ uporabniški vmesnik, ki ga lahko uporabljate za upravljanje digitalnih potrdil za aplikacije in uporabnike. Uporabniški vmesnik je razdeljen v dve glavni okni: okno za usmerjanje in okno nalog.

V oknu za usmerjanje lahko izberete naloge za upravljanje potrdil ali aplikacij, ki potrdila uporabljajo. Čeprav so posamezne naloge prikazane neposredno v glavnem oknu za usmerjanje, je večina nalog urejena v kategorije. Tako je na primer **Upravljanje potrdil** kategorija nalog, ki vsebuje številne različne vodene naloge, kot so prikaz potrdila, obnovitev potrdila, uvoz potrdila itd. Če je postavka v oknu za usmerjanje kategorija, ki vsebuje več kot eno nalogo, je na njeni levi strani prikazana puščica. Puščica kaže, da se ob izbiri povezave kategorije prikaže dodatni seznam nalog, s pomočjo katerega lahko nato izberete nalogo, ki jo želite izvesti.

Razen kategorije **Hitra pot** so vse naloge v oknu za usmerjanje vodene. Sestavljene so iz niza korakov, ki omogočajo hitro in preprosto dokončanje naloge. Kategorija Hitra pot nudi skupino funkcij za upravljanje potrdil in aplikacij, ki omogočajo izkušenim uporabnikom DCM hiter dostop do različnih s tem povezanih nalog iz osrednjega niza strani.

Katere naloge so na voljo v oknu za usmerjanje, se spreminja glede na prostor za potrdila, v katerem delate. Kategorije in število nalog, ki jih vidite v navigacijskem oknu, se spreminja glede na pooblastila, ki jih ima vaš uporabniški profil i5/OS. Vse naloge, povezane z vodenjem službe za potrdila, upravljanjem potrdil, ki jih uporabljajo aplikacije in druge naloge na sistemski ravni, so na voljo samo varnostnikom ali skrbnikom sistema. Če želita varnostnik ali skrbnik sistema prikazati te naloge in jih uporabljati, morata imeti posebni pooblastili *SECADM in *ALLOBJ. Uporabniki brez teh posebnih pooblastil lahko dostopijo samo do funkcij uporabniških potrdil.

Če želite spoznati, kako konfigurirati DCM, in ga začeti uporabljati za upravljanje vaših potrdil, preglejte naslednje teme:

Zagon DCM-a
V tej temi se boste naučili, kako dostopiti do funkcije upravljalnika digitalnih potrdil na vašem strežniku.

Prva nastavitev potrdil
V tej temi se boste naučili, kako začeti uporabljati DCM za nastavitev vsega, kar je potrebno za začetek uporabe potrdil. Spoznali boste, kako začeti upravljati potrdila javne internetne službe za potrdila (CA) ali kako osnovati in voditi zasebno lokalno službo za izdajanje potrdil.

Če želite poiskati več poučnih informacij o uporabi digitalnih potrdil v internetnem okolju in izboljšati zaščito vašega sistema in omrežja, potem je spletna stran VeriSign pravi naslov za vas. Spletno mesto VeriSign nudi obširno knjižnico iz področja digitalnih potrdil, pa tudi številne druge internetne varnostne vsebine. Njihovo knjižnico lahko obiščete prekSlužbe pomoči VeriSign .

Zagon Upravljalnika digitalnih potrdil

Preden lahko uporabite katerokoli funkcijo Upravljalnika digitalnih potrdil (DCM), ga morate zagnati. Z naslednjimi nalogami boste zagotovili uspešen zagon Upravljalnika digitalnih potrdil:

1. Namestite možnost 34 5722 SS1. To je Upravljalnik digitalnih potrdil (DCM).

   Namestite 5722 DG1. To je strežnik IBM HTTP Server za iSeries.

   Namestite 5722 AC3. To je izdelek za šifriranje, ki ga uporablja DCM za izdelavo para ključev za potrdila, sestavljenega iz javnega in zasebnega ključa, s pomočjo katerega šifrira izvožene datoteke potrdila in dešifrira uvožene datoteke potrdila.
2. Z Navigatorjem iSeries zaženite strežnik za upravljanje HTTP:
   a. Zaženite Navigator **iSeries**.
   b. V glavnem drevesnem prikazu dvokliknite vaš strežnik.

c. Razširite ikono **Omrežje > Strežniki > TCP/IP**.
d. Z desnim gumbom miške kliknite **Upravljanje HTTP**.
e. Kliknite **Poženi**.
3. Poženite spletni pregledovalnik.
4. S pomočjo pregledovalnika odprite stran Naloge na naslovu http://*ime_vašega_sistema*:2001.
5. Izberite **Upravljalnik digitalnih potrdil** s seznama izdelkov na strani z nalogami za dostop do uporabniškega vmesnika DCM.

Prva nastavitev potrdil

Levo okno Upravljalnika digitalnih potrdil (DCM) je okno za izbiro nalog. V tem oknu lahko izberete številne različne naloge za upravljanje potrdil in aplikacij, ki potrdila uporabljajo. Naloge, ki so na voljo, so odvisne od tega, s katerim prostorom za potrdila (če sploh s katerim) delate, in kakšna posebna pooblastila ima vaš uporabniški profil. Večina nalog je na voljo, samo če imate posebni pooblastili *ALLOBJ in *SECADM. Če želite z Upravljalnikom digitalnih potrdil preverjati podpise objektov, mora imeti vaš uporabniški profil tudi posebno pooblastilo *AUDIT.

Ko Upravljalnik digitalnih potrdil (DCM) uporabite prvič, še ne obstaja noben prostor za potrdila. Zaradi tega podokno za usmerjanje pri prvem dostopu do DCM prikaže samo te naloge, in še to samo, če imate potrebna posebna pooblastila:

- Upravljanje uporabniških potrdil
- Izdelava novega prostora za potrdila
- Osnovanje službe za potrdila (CA) (Opomba: Po uporabi te naloge za izdelavo zasebne lokalne službe za potrdila, se ta na seznamu ne pojavi več).
- Upravljanje mest CRL
- Upravljanje mest LDAP.
- Upravljanje mest zahtev PKIX
- Vrnitev na stran Naloge.

Tudi če v vašem sistemu že obstajajo prostori za potrdila (če na primer prehajate iz starejše različice DCM), DCM v levem oknu za usmerjanje prikaže zgolj omejeno število nalog ali kategorij nalog. Katere so naloge, ki jih DCM prikaže, je odvisno od prostora za potrdila (če obstaja), ki je odprt, in posebnih pooblastil vašega uporabniškega profila.

Preden lahko začnete delati z večino nalog za upravljanje potrdil in aplikacij, morate dostopiti do ustreznega prostora za potrdila. Če želite odpreti določen prostor za potrdila, v oknu za usmerjanje izberite **Izberi prostor za potrdila**.

Okno za usmerjanje DCM nudi tudi gumb **Zaščitena povezava**. S pomočjo tega gumba lahko prikažete okno drugega pregledovalnika, prek katerega z uporabo plasti zaščitenih vtičnic (SSL) vzpostavite zaščiteno povezavo. Za uspešno uporabo te funkcije morate najprej konfigurirati strežnik IBM HTTP Server za iSeries za uporabo SSL v zaščitenem načinu. Strežnik HTTP morate nato zagnati v zaščitenem načinu. Če strežnika HTTP ne konfigurirate in zaženete za delovanje SSL, se prikaže sporočilo o napaki, pregledovalnik pa ne zažene zaščitene seje.

Prvi koraki

Čeprav boste s pomočjo potrdil najbrž želeli doseči številne z zaščito povezane cilje, je tisto, kar boste opravili najprej, odvisno od tega, kako načrtujete pridobiti potrdila. Pri prvi uporabi DCM lahko izberete dva osnovna načina, odvisno od tega, ali nameravate uporabljati javna potrdila ali želite izdajati zasebna potrdila:

Izdelava in delovanje lokalne službe za pooblastila za izdajanje potrdil vašim aplikacijam.

Upravljanje potrdil javne internetne službe za potrdila za aplikacije, ki jih uporabljate.

Izdelava in delovanje lokalne službe za pooblastila

Po natančnem razmisleku o potrebah in načelih zaščite ste se odločili, da boste vodili lokalno službo za potrdila (CA) in izdajali zasebna potrdila za aplikacije. Za izdelavo in vodenje lastne lokalne službe za potrdila lahko uporabite

Upravljalnik digitalnih potrdil. Ta nudi nalogo, ki vas vodi skozi postopek izdelave službe za potrdila in njene uporabe za izdajanje potrdil za aplikacije. Vodena naloga zagotavlja, da imate vse, kar potrebujete za začetek uporabe digitalnih potrdil za konfiguriranje aplikacij za uporabo SSL, za podpisovanje objektov in preverjanje podpisov objektov.

Opomba: Če želite s strežnikom IBM HTTP Server za iSeries uporabljati potrdila, morate, preden pričnete delati z Upravljalnikom digitalnih potrdil, izdelati in konfigurirati spletni strežnik. Če konfigurirate spletni strežnik za uporabo SSL, je za strežnik ustvarjen ID aplikacije. ID aplikacije si morate zapisati, da lahko nato z Upravljalnikom digitalnih potrdil podate, katera potrdila bo za SSL uporabila aplikacija.

Strežnika ne zaustavite in znova zaženite, dokler mu z Upravljalnikom digitalnih potrdil ne dodelite potrdila. Če zaustavite primerek spletnega strežnika *ADMIN in ga nato znova zaženete, preden mu dodelite potrdilo, se strežnik ne bo zagnal, vi pa mu z Upravljalnikom digitalnih potrdil ne boste mogli dodeliti potrdila.

Z Upravljalnikom digitalnih potrdil izdelate in vodite lokalno službo za potrdila takole:

1. Zaženite DCM.
2. V oknu za usmerjanje Upravljalnika digitalnih potrdil izberite **Izdelaj službo za potrdila (CA)**, da boste prikazali niz obrazcev. Ti obrazci vas bodo vodili skozi postopek izdelave lokalne službe za potrdila in dokončanje drugih nalog, ki jih morate opraviti za začetek uporabe digitalnih potrdil za SSL, podpisovanje objektov in preverjanje podpisov.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
3. Izpolnite vse obrazce vodenega opravila. Pri uporabi teh obrazcev za izvedbo vseh nalog, potrebnih za nastavitev lokalne službe za potrdila (CA), morate narediti naslednje:
   a. Izbrati, kako boste shranili zasebni ključ potrdila lokalne službe za potrdila. (Ta korak je potreben le, če je v sistemu iSeries nameščen IBM-ov Šifrirni koprocesor.) Če v sistemu nimate šifrirnega koprocesorja, Upravljalnik digitalnih potrdil samodejno shrani potrdilo in njegov zasebni ključ v prostor za potrdila lokalne službe za potrdila (CA).
   b. Podati identifikacijske informacije za lokalno službo za potrdila.
   c. Namestiti potrdilo lokalne službe za potrdila na PC ali v pregledovalnik, da bo lahko vaša programska oprema prepoznala lokalno službo za potrdila in preverjala veljavnost potrdil, ki jih izda.
   d. Izbrati podatke načel za lokalno službo za potrdila.
   e. Uporabiti novo lokalno službo za potrdila za izdajanje potrdil strežnika ali odjemalca, ki jih lahko uporabljajo vaše aplikacije za povezave SSL. (Če je v vašem iSeries nameščen IBM-ov Šifrirni koprocesor, lahko s tem korakom izberete način, na katerega želite shraniti zasebni ključ za potrdilo strežnika ali odjemalca. Če v sistemu nimate koprocesorja, Upravljalnik digitalnih potrdil samodejno shrani potrdilo in njegov zasebni ključ v prostor za potrdila *SYSTEM. Upravljalnik digitalnih potrdil izdela prostor za potrdila *SYSTEM kot del te podnaloge.)
   f. Izbrati aplikacije, ki lahko uporabljajo potrdilo strežnika ali odjemalca za povezave SSL.

      Opomba: Če ste z Upravljalnikom digitalnih potrdil predhodno izdelali prostor za potrdila *SYSTEM za upravljanje potrdil za SSL iz javne internetne službe za potrdila, ne opravite tega ali prejšnjega koraka.
   g. Uporabiti novo lokalno službo za potrdila za izdajanje potrdil za podpisovanje objektov, ki jih lahko uporabijo vaše aplikacije za digitalno podpisovanje objektov. Ta podnaloga izdela prostor za potrdila *OBJECTSIGNING; to je prostor za potrdila, ki se uporablja za upravljanje potrdil za podpisovanje objektov.
   h. Izbrati aplikacije, ki lahko uporabijo potrdilo za podpisovanje objektov za dodajanje digitalnih podpisov na objekte.

      Opomba: Če ste z Upravljalnikom digitalnih potrdil predhodno izdelali prostor za potrdila *OBJECTSIGNING za upravljanje potrdil za podpisovanje objektov javne internetne službe za potrdila, ne opravite tega ali prejšnjega koraka.
   i. Izberite aplikacije, ki bodo zaupale vaši lokalni službi za potrdila.

Ko končate vodeno nalogo, imate vse, kar potrebujete za začetek konfiguriranja aplikacij za uporabo SSL za zaščitene komunikacije.

Ko konfigurirate aplikacije, morajo uporabniki, ki dostopijo do aplikacij prek povezave SSL, morate z Upravljalnikom digitalnih potrdil pridobiti kopijo potrdila lokalne službe za potrdila. Vsak uporabnik mora imeti kopijo potrdila, s pomočjo katere programska oprema uporabnikovega odjemalca overi istovetnost strežnika kot del procesa pogajanj SSL. Uporabniki lahko s pomočjo Upravljalnika digitalnih potrdil prekopirajo potrdilo lokalne službe za potrdila v datoteko ali ga naložijo v pregledovalnik. Kako uporabniki shranijo potrdilo lokalne službe za potrdila je odvisno od odjemalske programske opreme, ki jo uporabljajo za vzpostavitev povezave SSL z aplikacijo.

To lokalno službo za potrdila lahko uporabite tudi za izdajanje potrdil aplikacijam za druge sisteme iSeries v omrežju.

Če želite zvedeti več o uporabi DCM-a za upravljanje uporabniških potrdil, ter kako lahko uporabniki pridobijo kopijo potrdila lokalne službe za pooblastila za overjanje potrdil, ki jih izdaja lokalna služba za pooblastila, preglejte naslednje teme:

Upravljanje uporabniških potrdil
Spoznajte, kako lahko uporabniki uporabijo DCM za pridobivanje potrdil ali povezavo obstoječih potrdil z njihovimi uporabniškimi profili iSeries.

Uporaba API-jev za programsko izdajanje potrdil uporabnikom, ki niso uporabniki iSeries
Spoznajte, kako lahko vašo lokalno službo za pooblastila uporabite za izdajanje zasebnih potrdil uporabnikom, ne da bi potrdilo povezali s profilom uporabnika iSeries.

Pridobitev kopije potrdila zasebne službe za pooblastila
Spoznajte, kako pridobiti kopijo potrdila zasebne službe za potrdila in jo namestiti na PC, da jo boste lahko uporabljali za overjanje potrdil strežnika, ki jih izda služba za potrdila.

Upravljanje uporabniških potrdil

Upravljalnik digitalnih potrdil (DCM) lahko vi in vaši uporabniki uporabljate za upravljanje potrdil, ki jih potrebujejo uporabniki in za sodelovanje v sejah plasti zaščitenih vtičnic (SSL).

Če uporabniki dostopijo do javnih ali notranjih strežnikov prek povezave SSL, morajo imeti kopijo potrdila službe za potrdila (CA), ki je izdala potrdilo strežnika. Potrdilo je potrebno, da lahko programska oprema odjemalca preveri pristnost potrdila strežnika in vzpostavi povezavo. Če vaš strežnik uporablja potrdilo javne službe za potrdila, programska oprema vaših uporabnikov morda že ima kopijo potrdila službe za potrdila. To pomeni, da niti vam kot skrbniku DCM, niti uporabnikom, pred sodelovanjem v seji SSL ni potrebno opraviti nobenega dejanja. Če pa strežnik uporablja potrdilo zasebne lokalne službe za potrdila, morajo uporabniki pridobiti kopijo potrdila lokalne službe za potrdila, preden lahko vzpostavijo sejo SSL s strežnikom.

Če aplikacija strežnika podpira in zahteva overjanje odjemalca prek potrdil, morajo uporabniki predložiti ustrezno uporabniško potrdilo za dostop do sredstev, ki jih nudi strežnik. Od vaših potreb za zaščito je odvisno, ali bodo uporabniki predložili potrdilo javne internetne službe za potrdila ali potrdilo lokalne službe za potrdila, ki jo vodite vi. Če aplikacija strežnika nudi dostop do sredstev za notranje uporabnike, ki imajo trenutno profile uporabnikov iSeries, lahko s pomočjo DCM dodate potrdila njihovim profilom uporabnikov. Ta povezava zagotavlja, da imajo uporabniki pri predložitvi potrdil enak dostop in omejitve do sredstev, kot jih omogoča ali onemogoča njihov profil uporabnika.

Upravljalnik digitalnih potrdil (DCM) omogoča upravljanje potrdil, ki so dodeljena profilu uporabnika iSeries. Če imate profil uporabnika s posebnima pooblastiloma *SECADM in *ALLOBJ, lahko upravljate dodelitve potrdil za profile uporabnikov zase in za druge uporabnike. Če ni odprt noben prostor za potrdila ali če je odprt prostor za potrdila lokalne službe za potrdila (CA), lahko v oknu za usmerjanje za dostop do ustreznih nalog izberete **Upravljanje uporabniških potrdil**. Če je odprt kakšen drug prostor za potrdila, so naloge uporabniški potrdil združene z nalogami pod kategorijo **Upravljanje potrdil**.

Uporabniki brez pooblastil *SECADM ter *ALLOBJ lahko upravljajo samo svoje lastne dodelitve potrdil. Izberejo lahko kategorijo **Upravljanje uporabniških potrdil** in dostopijo do nalog, ki jim omogočajo prikaz potrdil, ki so povezani z njihovimi profili uporabnikov, odstranitev potrdila iz njihovih profilov uporabnikov ali dodelitev potrdila

kakšne druge službe za potrdila njihovim profilom uporabnikov. Uporabniki lahko ne glede na posebna pooblastila za njihove profile pridobijo uporabniško potrdilo od lokalne službe za pooblastila, tako da v glavnem usmerjevalnem oknu izberejo nalogo **Izdelaj potrdilo**.

Če se želite naučiti več o uporabi DCM za upravljanje in izdelavo uporabniških potrdil, preberite naslednje teme:

Izdelava uporabniškega potrdila
Te informacije vam bodo pomagale razumeti, kako lahko uporabniki uporabljajo lokalno službo za potrdila za izdajo potrdila za overjanje odjemalca.

Dodelitev uporabniškega potrdila
S pomočjo teh informacij se pozanimajte, kako dodelite potrdilo, ki je v vaši lasti, vašemu uporabniškemu profilu OS/400 ali drugi uporabniški istovetnosti. Potrdilo lahko izda zasebna lokalna služba za pooblastila na drugem sistemu ali javna dobro znana internetna služba za pooblastila. Preden lahko potrdilo dodelite uporabniški istovetnosti, mora strežnik zaupati izdajajoči službi za potrdila, potrdilo pa ne sme biti povezano z uporabniškim profilom ali drugo uporabniško istovetnostjo v sistemu.

Upravljanje uporabniških potrdil glede na datum zapadlosti
S pomočjo teh informacij se seznanite z načinom pregledovanja in upravljanja uporabniških potrdil, glede na datum njihove zapadlosti.

Izdelava uporabniškega potrdila: Če želite za overjanje uporabnikov uporabiti digitalna potrdila, morajo imeti uporabniki potrdila. Če za vodenje zasebne lokalne službe za potrdila (CA) uporabite Upravljalnik digitalnih potrdil (DCM), lahko uporabite lokalno službo za potrdila za izdajanje potrdil vsakemu uporabniku. Vsak uporabnik mora dostopiti do DCM in pridobiti potrdilo s pomočjo naloge **Izdelaj potrdilo**. Za pridobivanje potrdila lokalne službe za potrdila morajo načela službe za potrdila omogočati izdajanje uporabniških potrdil.

Potrdilo lokalne službe za potrdila pridobite takole:
1. Zaženite DCM.
2. V oknu za usmerjanje izberite **Izdelaj potrdilo**.
3. Kot tip potrdila za izdelavo izberite **Uporabniško potrdilo**. Prikaže se obrazec, na katerem lahko podate določilne informacije za potrdilo.
4. Izpolnite obrazec in kliknite **Nadaljuj**.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, s katerim boste dostopili do zaslonske pomoči.
5. Na tej točki začne DCM sodelovati s pregledovalnikom za izdelavo zasebnega in javnega ključa za potrdilo. Pregledovalnik bo morda prikazal okna, prek katerih vas bo vodil skozi ta postopek. Za te naloge sledite navodilom pregledovalnika. Ko pregledovalnik ustvari ključa, se prikaže potrditvena stran, ki kaže, da je DCM izdelal potrdilo.
6. Namestite novo potrdilo v vašem pregledovalniku. Pregledovalnik bo morda prikazal okna, prek katerih vas bo vodil skozi ta postopek. Sledite navodilom, ki jih pregledovalnik poda za zaključitev te naloge.
7. Kliknite **Potrdi** in s tem dokončajte nalogo.

Upravljalnik digitalnih potrdil med obdelavo samodejno poveže potrdilo s profilom uporabnika iSeries.

Če želite, da bo imelo potrdilo kakšne druge službe za potrdila, ki ga predloži uporabnik za overjanje odjemalca, enaka pooblastila kot njegov profil uporabnika, lahko s pomočjo DCM dodelite potrdilo profilu uporabnika.

Dodelitev uporabniškega potrdila: Nekateri uporabniki imajo morda potrdila zunanje službe za potrdila ali lokalne službe za potrdila v drugačnem sistemu iSeries, vi želite narediti, da bodo ta potrdila na voljo upravljalniku digitalnih potrdil. S tem omogočite sebi in uporabnikom, da s pomočjo upravljalnika digitalnih potrdil upravljalo ta potrdila, ki so najpogosteje v rabi za overjanje odjemalcev. Naloga **Dodelitev uporabniškega potrdila** predstavlja mehanizem, s pomočjo katerega uporabniku dovolite izdelavo dodelitve upravljalnika digitalnih potrdil za potrdilo, pridobljeno od zunanje službe za potrdila.

Ko uporabnik dodeli potrdilo, ima upravljalnik digitalnih potrdil za obravnavanje dodeljenega potrdila na voljo enega izmed naslednjih načinov:

- Lahko ga shrani lokalno v iSeries z uporabniškim profilom uporabnika.
  Če za upravljalnik digitalnih potrdil ni definirano mesto LDAP, naloga **Dodelitev uporabniškega potrdila** uporabniku omogoči, da uporabniškemu profilu OS/400 dodeli zunanje potrdilo. Dodelitev potrdila uporabniškemu profilu zagotavlja, da je potrdilo moč uporabljati z aplikacijami v sistemu, ki za overjanje odjemalcev zahtevajo potrdila.
- Shranjevanje potrdila v mestu LDAP (Lightweight Directory Access Protocol) za uporabo z EIM
  Če je definirano mesto LDAP, sistem iSeries pa je konfiguriran tako, da bo sodeloval v EIM, naloga **Dodelitev uporabniškega potrdila** uporabniku omogoča, da shrani kopijo zunanjega potrdila v podan imenik LDAP. Upravljalnik digitalnih potrdil za potrdilo izdela tudi izvorno povezavo v EIM. Takšno shranjevanje potrdil skrbniku EIM omogoča, da potrdilo prepozna kot veljavno istovetnost uporabnika, ki lahko sodeluje v EIM.

  Opomba: Uporabnik lahko dodeli potrdilo uporabniški istovetnosti v konfiguraciji EIM šele, ko je EIM primerno konfiguriran zanj. Konfiguriranje EIM zajema izdelavo identifikatorja EIM za uporabnika in izdelavo ciljne povezave med identifikatorjem EIM in uporabniškim profilom. V nasprotnem primeru upravljalnik digitalnih potrdil za potrdilo ne more izdelati ustrezne izvorne povezave z EIM. Več informacij o konfiguriranju EIM najdete v temi EIM v informacijskem centru iSeries.

Če želi uporabiti nalogo **Dodelitev uporabniškega potrdila** mora uporabnik izpolnjevati naslednje pogoje:

1. S strežnikom HTTP, prek katerega dostopate do upravljalnika digitalnih potrdil mora imeti vzpostavljeno zaščiteno sejo.

   Ali je vaša seja zaščitena, se določi s pomočjo številke vrat v URL-ju, ki ste ga uporabili za dostop do Upravljalnika digitalnih potrdil. Če ste uporabili vrata 2001, ki so privzeta vrata za dostop do Upravljalnika digitalnih potrdil, vaša seja ni zaščitena. Preden lahko preklopite v zaščiteno sejo, mora biti tudi strežnik HTTP konfiguriran za uporabo SSL.

   Če uporabnik izbere to nalogo, se pojavi novo okno pregledovalnika. Če uporabnik nima vzpostavljene zaščitene seje, upravljalnik digitalnih potrdil opozori uporabnika, naj klikne **Dodelitev uporabniškega potrdila** in jo vzpostavi. DCM nato začne pogajanja plasti zaščitenih vtičnic (SSL) s pregledovalnikom uporabnika. Med temi pogajanji lahko pregledovalnik uporabnika vpraša, ali naj zaupa službi za potrdila, ki je izdala potrdilo, s katerim je določen strežnik HTTP. Pregledovalnik prav tako lahko vpraša uporabnika, ali sploh naj sprejme potrdilo strežnika.
2. Predložiti mora potrdilo za overjanje odjemalca.

   Odvisno od konfiguracijskih nastavitev pregledovalnika je, ali bo pregledovalnik zahteval, da izberete potrdilo za overjanje. Če pregledovalnik predloži potrdilo službe za potrdila, ki jo sistem sprejme kot overjeno, bo Upravljalnik digitalnih potrdil prikazal informacije o potrdilu v ločenem oknu. Če ne predložite sprejemljivega potrdila, lahko strežnik zahteva, da pred dostopom vnesete ime uporabnika in geslo za overjanje.
3. V pregledovalniku mora imeti potrdilo, ki še ni povezano z uporabniško istovetnostjo uporabnika, ki izvaja nalogo. (Ali če je upravljalnik digitalnih potrdil konfiguriran tako, da deluje skupaj z EIM, mora imeti uporabnik v pregledovalniku potrdilo, ki še ni shranjeno v mestu LDAP za upravljalnik digitalnih potrdil).

   Ko vzpostavite zaščiteno sejo, bo upravljalnik digitalnih potrdil z vašega pregledovalnika poskušal priklicati ustrezno potrdilo, da ga lahko poveže z vašo uporabniško istovetnostjo. Če mu uspe pridobiti eno ali več potrdil, si lahko ogledate informacije o potrdilu in izberete, da boste povezali potrdilo s profilom uporabnika.

   Če upravljalnik digitalnih potrdil ne prikaže informacij s potrdila, niste predložili potrdila, ki bi ga upravljalnik digitalnih potrdil lahko povezal z vašo uporabniško istovetnostjo. Za to je lahko kriva ena od številnih težav z uporabniškimi potrdili. Potrdila v vašem pregledovalniku so na primer lahko že povezana z vašo uporabniško istovetnostjo.

Upravljanje uporabniških potrdil glede na datum zapadlosti: Upravljalnik digitalnih potrdil (DCM) nudi podporo za upravljanje datuma zapadlosti potrdil, s pomočjo katere lahko skrbniki preverjajo datum zapadlosti uporabniških potrdil v lokalnem sistemu iSeries. Podporo upravljanju datuma zapadlosti za uporabniška potrdila DCM je mogoče uporabiti skupaj s Preslikavo istovetnosti podjetja (EIM), tako da lahko skrbniki s pomočjo DCM preverijo datum zapadlosti uporabniških potrdil na ravni podjetja.

Če želite uporabljati podporo upravljanju datuma zapadlosti za uporabniška potrdila na ravni podjetja, mora biti v podjetju konfiguriran EIM ter vsebovati ustrezne informacije preslikave za uporabniška potrdila. Če želite preveriti datum zapadlosti uporabniških potrdil, ki niso povezana z vašim uporabniškim profilom, morate imeti posebna pooblastila *ALLOBJ in *SECADM.

Če z upravljalnikom digitalnih potrdil pregledujete potrdila, glede na njihov datum zapadlosti, lahko hitro in preprosto ugotovite, katera bodo kmalu potekla in jih lahko pravočasno obnovite.

Če želite pregledovati in upravljati uporabniška potrdila glede na datum njihove zapadlosti, upoštevajte naslednje korake:

1. Zaženite DCM.

   Opomba: Če imate kakšno vprašanje o izpolnitvi določenega obrazca pri uporabi DCM, izberite vprašaj (**?**) na vrhu strani, s katerim boste dostopili do zaslonske pomoči.
2. V oknu za usmerjanje, izberite **Upravljanje uporabniških potrdil**, da prikažete seznam nalog. **Opomba:** Če trenutno delate s prostorom za potrdila, izberite **Upravljanje potrdil**, da prikažete seznam nalog, nato pa izberite **Preverjanje datuma zapadlosti** in izberite **Uporabnik**.
3. Če ima vaš uporabniški profil posebna pooblastila *ALLOBJ in *SECADM, lahko izberete metodo, s katero izberete, katera uporabniška potrdila želite pregledovati in upravljati glede na njihov datum zapadlosti. (Če vaš uporabniški profil teh posebnih pooblastil nima, vas upravljalnik digitalnih potrdil opozori, naj podaste območje datuma zapadlosti, kot je opisano v naslednjem koraku.) Izberete lahko eno izmed naslednjega:
   - **Uporabniški profil**, če želite pregledovati uporabniška potrdila, dodeljena določenemu uporabniškemu potrdilu OS/400. Podajte **ime uporabniškega potrdila** in kliknite **Nadaljuj**. **Opomba:** Uporabniški profil, ki ni vaš lasten, lahko podate samo, če imate posebna pooblastila *ALLOBJ in *SECADM.
   - **Vsa uporabniška potrdila**, če želite pregledovati in upravljati uporabniška potrdila za vse uporabniške istovetnosti.
4. V polje **Območje datuma zapadlosti v dneh (1-365)** vnesite število dni, za katere želite pregledati uporabniška potrdila glede na njihov datum zapadlosti in kliknite **Nadaljuj**. Upravljalnik digitalnih potrdil prikaže vsa uporabniška potrdila za podanega uporabnika, ki potečejo med današnjim dnem in dnem, ki ustreza številu podanih dni. Upravljalnik digitalnih potrdil prav tako prikaže uporabniška potrdila z datumom zapadlosti pred današnjim dnem.
5. Izberite uporabniško potrdilo, ki ga želite upravljati. Po izbiri lahko pregledate podrobne informacije o potrdilu ali odstranite potrdilo iz z njim povezane uporabniške istovetnosti.
6. Ko zaključite delo s potrdili na seznamu, kliknite **Prekliči**, da zapustite nalogo.

Uporaba API-jev za programsko izdajanje potrdil uporabnikom, ki niso uporabniki iSeries

Začenši v V5R2 sta na voljo dva nova API-ja, ki jih lahko uporabite za programsko izdajanje potrdil ne-iSeries uporabnikom. V predhodnih izdajah je veljalo, ko ste za izdajanje potrdil uporabnikom uporabili vašo lastno lokalno službo za pooblastila (CA), so se ta potrdila samodejno povezala z uporabniškimi profili uporabnikov iSeries. Če ste želeli lokalno službo za pooblastila uporabiti za izdajanje potrdil uporabniku za overjanje odjemalca, ste morali posledično uporabniku nuditi profil uporabnika iSeries. Če so uporabniki morali pridobiti potrdilo od lokalne službe za pooblastila za overjanje odjemalca, je moral vsak uporabnik uporabiti upravljalnik digitalnih potrdil (DCM) za izdelavo potrebnega potrdila. Zato je moral vsak uporabnik imeti profil uporabnika na strežniku iSeries, ki je gostil DCM, ter veljavno prijavo na ta strežnik iSeries.

Povezovanje potrdila s profilom uporabnika ima svoje prednosti, predvsem ko gre ta interne uporabnike. Te omejitve in zahteve pa so postale manj praktične pri uporabi lokalne službe za pooblastila za izdajanje uporabniških potrdil velikemu številu uporabnikov, še posebej, kadar želite, da ti uporabniki nimajo svojega profila uporabnika iSeries. Če se želite izogniti nudenju uporabniških profilov tem uporabnikom in želite za overjanje uporabnikov za vaše aplikacije zahtevati potrdila, lahko zahtevate, da uporabniki plačajo za potrdilo znane službe za potrdila CA.

Ta dva nova API-ja nudita podporo, ki omogoča, da ponudite vmesnik za izdelavo uporabniških potrdil, ki jih podpiše potrdilo lokalne službe za pooblastila za katerokoli ime uporabnika. To potrdilo ne bo povezano s profilom uporabnika. Ni nujno, da uporabnik obstaja na strežniku iSeries, ki gosti DCM, poleg tega pa uporabniku ni potrebno uporabiti DCM-a za izdelavo potrdila.

Za vsakega od prevladujočih programov pregledovalnika obstaja po en API, ki ga lahko pokličete, ko z Net.Data izdelujete program za izdajanje potrdil uporabnikom. Aplikacija, ki jo izdelate, mora nuditi kodo grafičnega uporabniškega vmesnika, ki je potrebna za izdelavo uporabniškega potrdila ter za klic enega od ustreznih API-jev za uporabo lokalne službe za pooblastila za podpis potrdila.

Če želite podrobnejše informacije o uporabi teh API-jev, preglejte naslednji strani:
- API za izdelavo in podpisovanje zahtev za uporabniška potrdilaQYCUGSUC).
- API za podpisovanje zahtev za uporabniška potrdila (QYCUSUC).

Pridobitev kopije potrdila zasebne službe za pooblastila

Ko dostopite do strežnika, ki uporablja povezavo plasti zaščitenih vtičnic (SSL), strežnik dokaže svojo identiteto programski opremi odjemalca s potrdilom. Preden lahko strežnik vzpostavi sejo, mora programska oprema odjemalca preveriti veljavnost potrdila strežnika. Za preverjanje veljavnosti potrdila strežnika mora imeti programska oprema odjemalca dostop do lokalno shranjene kopije potrdila službe za potrdila (CA), ki je izdala potrdilo strežnika. Če strežnik predloži potrdilo javne internetne službe za potrdila, vaš pregledovalnik ali druga programska oprema odjemalca morda že ima kopijo potrdila službe za potrdila. Če pa strežnik predloži potrdilo zasebne lokalne službe za potrdila, morate kopijo potrdila lokalne CA dobiti s pomočjo Upravljalnika digitalnih potrdil.

S pomočjo Upravljalnika digitalnih potrdil lahko prenesete potrdilo lokalne CA neposredno v pregledovalnik ali pa ga prekopirate v datoteko, da lahko do njega dostopi in ga uporablja tudi druga programska oprema odjemalca. Če za zaščitene komunikacije uporabljate pregledovalnik in druge aplikacije, boste za namestitev potrdila lokalne CA morda morali uporabiti oba načina. Če uporabite oba načina, namestite potrdilo v pregledovalnik, preden ga prekopirate in prilepite v datoteko.

Če aplikacija strežnika zahteva, da se overite tako, da predložite potrdilo lokalne službe za potrdila, morate posneti potrdilo lokalne službe za potrdila v vaš pregledovalnik, šele nato lahko od lokalne službe za potrdila zahtevate uporabniško potrdilo.

Naslednji koraki kažejo, kako s pomočjo DCM pridobite kopijo potrdila lokalne službe za potrdila:
1. Zaženite DCM.
2. V oknu za usmerjanje izberite **Namesti lokalno potrdilo CA na PC**, da boste prikazali stran, na kateri lahko naložite potrdilo lokalne CA v pregledovalnik ali ga shranite v datoteko v sistemu.
3. Izberite način za pridobitev potrdila lokalne CA.
   a. Izberite **Namesti potrdilo**, da boste naložili potrdilo lokalne CA kot overjeno potrdilo v vaš pregledovalnik. S tem boste zagotovili, da lahko pregledovalnik vzpostavi zaščitene komunikacijske seje s strežniki, ki uporabljajo potrdilo te službe za potrdila. Pregledovalnik bo prikazal niz oken, ki vam bodo pomagala dokončati namestitev.
   b. Izberite **Prekopiraj in prilepi potrdilo**, da boste prikazali stran, ki vsebuje posebej kodirano kopijo potrdila lokalne službe za potrdila. Besedilni objekt, prikazan na strani, prekopirajte v odložišče. Te informacije morate nato prilepiti v datoteko. To datoteko uporabi pomožni program PC-ja (kot je na primer MKKF ali IKEYMAN) za shranjevanje potrdil, ki jih bodo uporabljali odjemalski programi na PC-ju. Preden lahko aplikacije odjemalca prepoznajo in uporabijo potrdilo lokalne CA za overjanje, jih morate konfigurirati, tako da prepoznajo potrdilo kot overjeno. Sledite navodilom, ki jih nudijo te aplikacije za uporabo datoteke.
4. Za vrnitev na domačo stran Upravljalnika digitalnih potrdil kliknite **Potrdi**.

Upravljanje potrdil javne internetne službe za potrdila

Po natančnem razmisleku o potrebah in načelih zaščite ste se odločili, da boste uporabljali potrdila javne internetne službe za potrdila (CA), kot je VeriSign. Odgovorni ste za javno spletno mesto in za zaščitene komunikacijske seje želite uporabiti plast zaščitenih vtičnic (SSL), da zagotovite tajnost določenih prenosov informacij. Ker je spletna stran dostopna širši javnosti, želite uporabiti potrdila, ki jih večina spletnih pregledovalnikov brez težav prepozna.

Morda pa razvijate aplikacije za zunanje uporabnike in želite uporabljati javno potrdilo za digitalno podpisovanje paketov aplikacij. Če podpišete paket aplikacij, so lahko vaši uporabniki popolnoma prepričani, da paket izvira iz vašega podjetja in da nepooblaščene stranke pri prehodu niso spremenile kode. Z uporabo javnega potrdila omogočite vašim uporabnikom preprosto in poceni preverjanje digitalnega podpisa na paketu. S tem potrdilom lahko tudi preverite podpis, preden pošljete paket svojim strankam.

Vodene naloge v Upravljalniku digitalnih potrdil (DCM) lahko uporabite za osrednje upravljanje javnih potrdil in aplikacij, ki jih uporabljajo za vzpostavljanje povezav SSL, podpisovanje objektov ali preverjanje pristnosti digitalnih podpisov na objektih.

Upravljanje javnih potrdil

Če uporabite za upravljanje potrdil javne internetne službe Upravljalnik digitalnih potrdil, morate najprej izdelati prostor za potrdila. Prostor za potrdila je posebna datoteka baze podatkov ključev, ki jo uporablja Upravljalnik digitalnih potrdil za shranjevanje digitalnih potrdil in z njimi povezanih zasebnih ključev. Upravljalnik digitalnih potrdil omogoča izdelavo in upravljanje številnih tipov prostorov za potrdila, ki temeljijo na tipih potrdil, ki jih vsebujejo.

Tip prostora za potrdila, ki ga izdelate, in nadaljnje naloge, ki jih morate izvesti za upravljanje potrdil in aplikacij, ki potrdila uporabljajo, je odvisen od tega, kako nameravate uporabljati potrdila. Če se želite naučiti, kako uporabljati Upravljalnik digitalnih potrdil za izdelavo ustreznega prostora za potrdila in upravljanje javnih internetnih potrdil za aplikacije, preberite naslednje teme:

- Upravljanje javnih internetnih potrdil za komunikacijske seje SSL.
- Upravljanje javnih internetnih potrdil za podpisovanje objektov.
- Upravljanje internetnih potrdil za preverjanje podpisov objektov.

Upravljalnik digitalnih potrdil tudi omogoča, da upravljate potrdila, ki jih pridobite od službe za potrdila javne infrastrukture ključev za X.509 (PKIX).

Upravljanje javnih internetnih potrdil za komunikacijske seje SSL

S pomočjo Upravljalnika digitalnih potrdil (DCM) lahko upravljate javna internetna potrdila za aplikacije, ki jih bodo uporabljale za vzpostavljanje zaščitenih komunikacijskih sej s plastjo zaščitenih vtičnic (SSL). Če za vodenje lokalne službe za potrdila (CA) ne uporabite Upravljalnik digitalnih potrdil, morate najprej izdelati ustrezen prostor za potrdila za upravljanje javnih potrdil, ki jih uporabljate za SSL. To je prostor za potrdila *SYSTEM. Ko izdelate prostor za potrdila, vas Upravljalnik digitalnih potrdil vodi skozi postopek izdelave informacij o potrdilu, ki jih morate posredovati javni službi za potrdila, če želite pridobiti potrdilo.

Takole uporabite Upravljalnik digitalnih potrdil za upravljanje in uporabo javnih internetnih potrdil, da bodo aplikacije lahko vzpostavile komunikacijske seje SSL:

1. Zaženite DCM.
2. V oknu za usmerjanje Upravljalnika digitalnih potrdil izberite **Izdelaj nov prostor za potrdila**, s čimer boste zagnali vodeno nalogo, v kateri boste izpolnili niz obrazcev. Ti obrazci vas bodo vodili skozi postopek izdelave prostora za potrdila in potrdila, ki ga bodo lahko uporabile vaše aplikacije za seje SSL.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
3. Kot prostor za potrdila izberite ***SYSTEM** in kliknite **Nadaljuj**.
4. Za izdelavo potrdila kot dela izdelave prostora za potrdila *SYSTEM izberite **Da** in kliknite **Nadaljuj**.
5. Kot podpisnika novega potrdila izberite **VeriSign ali drugo internetno službo za potrdila (CA)** in kliknite **Nadaljuj**. Prikazali boste obrazec, na katerem lahko podate določilne informacije za novo potrdilo.

   Opomba: Če je na vašem strežniku nameščen IBM-ov Šifrirni koprocesor, vam Upravljalnik digitalnih potrdil kot naslednjo nalogo omogoča, da izberete način hrambe zasebnega ključa za potrdilo. Če v sistemu

nimate koprocesorja, Upravljalnik digitalnih potrdil samodejno shrani zasebni ključ v prostor za potrdila *SYSTEM. Če potrebujete pomoč pri izbiri načina za shranitev zasebnega ključa, uporabite zaslonsko pomoč Upravljalnika digitalnih potrdil.

6. Izpolnite obrazec in kliknite **Nadaljuj**. Prikazala se bo potrditvena stran z zahtevanimi podatki potrdila, ki jih morate posredovati javni službi za potrdila (CA), ki bo izdala vaše potrdilo. Podatki zahteve za podpis potrdila (CSR) so sestavljeni iz javnega ključa in drugih informacij, ki ste jih podali za novo potrdilo.
7. Previdno prekopirajte podatke CSR in jih prilepite v obrazec za potrdilo ali v ločeno datoteko, ki jo potrebuje javna služba za potrdila, če zahtevate potrdilo. Uporabiti morate vse podatke CSR, vključno z vrsticama Begin in End New Certificate Request. Ko zaprete to stran, izgubite podatke in ni jih več mogoče obnoviti. Obrazec ali datoteko pošljite službi za potrdila, ki ste jo izbrali za izdajanje in podpišite potrdilo.

   Opomba: Preden lahko končate ta postopek, morate počakati, da vam služba za potrdila vrne podpisano in dokončano potrdilo.

   Opomba: Če želite s strežnikom HTTP za iSeries uporabljati potrdila, morate, preden pričnete delati z Upravljalnikom digitalnih potrdil, izdelati spletni strežnik in ga konfigurirati za delo s podpisanimi potrdili. Če konfigurirate spletni strežnik za uporabo SSL, je za strežnik ustvarjen ID aplikacije. ID aplikacije si morate zapisati, da lahko nato z Upravljalnikom digitalnih potrdil podate, katera potrdila mora za SSL uporabiti aplikacija.

   Strežnika ne zaustavite in znova zaženite, dokler z Upravljalnikom digitalnih potrdil ne dodelite podpisanega in dokončanega potrdila strežniku. Če zaustavite primerek spletnega strežnika *ADMIN in ga nato znova zaženete, preden mu dodelite potrdilo, se strežnik ne bo zagnal, vi pa mu z Upravljalnikom digitalnih potrdil ne boste mogli dodeliti potrdila.
8. Ko vam služba za potrdila vrne podpisano potrdilo, zaženite Upravljalnik digitalnih potrdil.
9. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***SYSTEM**.
10. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo, ki ste ga podali pri izdelavi prostora za potrdila in kliknite **Nadaljuj**.
11. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
12. S seznama nalog izberite **Uvozi potrdilo**, da boste začeli postopek uvažanja podpisanega potrdila v prostor za potrdila *SYSTEM. Ko končate z uvozom potrdila, lahko podate aplikacije, ki ga morajo uporabljati za komunikacije SSL.
13. V oknu za usmerjanje izberite **Upravljanje aplikacij**, da boste prikazali seznam nalog.
14. S seznama nalog izberite **Ažuriraj dodelitev potrdila**, da boste prikazali seznam aplikacij, omogočenih za SSL, ki jim lahko dodelite potrdilo.
15. S seznama izberite aplikacijo in kliknite **Ažuriraj dodelitev potrdila**.
16. Izberite potrdilo, ki ste ga uvozili in kliknite **Dodeli novo potrdilo**. Upravljalnik digitalnih potrdil prikaže sporočilo, ki zahteva, da potrdite izbiro potrdila za aplikacijo.

    Opomba: Nekatere aplikacije, ki so omogočene za SSL, podpirajo overjanje odjemalca na osnovi potrdil. Če želite, da bo aplikacija s to podporo lahko overjala potrdila, preden bo omogočila dostop do sredstev, morate zanjo definirati seznam overjenih služb za potrdila. S tem zagotovite, da bo aplikacija preverjala veljavnost samo tistih potrdil služb za potrdila, ki ste jih določili kot overjene. Če uporabnik ali aplikacija odjemalca predložita potrdilo službe za potrdila, ki na seznamu overjenih služb za potrdila ni podana kot overjena, je aplikacija ne bo sprejela kot osnovo za overjanje.

Ko končate vodeno nalogo, imate vse, kar potrebujete za začetek konfiguriranja aplikacij za uporabo SSL za zaščitene komunikacije. Preden lahko uporabniki dostopijo do teh aplikacij prek seje SSL, morajo imeti kopijo potrdila službe za potrdila, ki je izdala potrdilo strežnika. Če so uporabniki pridobili potrdilo pri znani internetni službi za potrdila, bo programska oprema odjemalcev najbrž že vsebovala kopijo potrebnega potrdila. Če si morajo uporabniki priskrbeti potrdilo službe za potrdila, morajo obiskati spletno stran službe za potrdila in slediti tamkajšnjim navodilom.

Upravljanje javnih internetnih potrdil za podpisovanje objektov

S pomočjo Upravljalnika digitalnih potrdil (DCM) lahko upravljate javna internetna potrdila za digitalno podpisovanje objektov. Če za vodenje lokalne službe za potrdila (CA) ne uporabite Upravljalnik digitalnih potrdil, morate najprej izdelati ustrezen prostor za potrdila za upravljanje javnih potrdil, ki jih uporabljate za podpisovanje objektov. To je prostor za potrdila *OBJECTSIGNING. Ko izdelate prostor za potrdila, vas Upravljalnik digitalnih potrdil vodi skozi postopek izdelave informacij zahteve o potrdilu, ki jih morate posredovati javni internetni službi za potrdila, če želite pridobiti potrdilo.

Če želite uporabljati potrdilo za podpisovanje objektov, morate definirati ID aplikacije. Ta ID aplikacije nadzoruje, kakšna pooblastila potrebuje nekdo za podpis objektov z določenim potrdilom in nudi raven nadzorovanja dostopa, ki ni na voljo v Upravljalniku digitalnih potrdil. Po privzetku zahteva definicija aplikacije, da mora imeti uporabnik, ki želi uporabljati aplikacijo za podpisovanje objektov, posebno pooblastilo *ALLOBJ. (S pomočjo Navigatorja iSeries lahko spremenite pooblastilo, ki ga zahteva ID aplikacije.)

Če želite uporabljati Upravljalnik digitalnih potrdil za upravljanje in uporabo javnih internetnih potrdil za podpisovanje objektov, opravite naslednje naloge:

1. Zaženite DCM.
2. V levem oknu za usmerjanje upravljalnika digitalnih potrdil izberite **Izdelava novega prostora za potrdila**, da poženete vodeno nalogo in izpolnite vrsto obrazcev. Ti obrazci vas bodo vodili skozi postopek izdelave prostora za potrdila in potrdila, ki ga boste uporabljali za podpisovanje objektov.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite gumb z vprašajem (**?**) na vrhu strani, da pridete do zaslonske pomoči.
3. Za izdelavo izberite prostor za potrdila ***OBJECTSIGNING** in kliknite **Nadaljuj**.
4. Za izdelavo potrdila kot dela izdelave prostora za potrdila izberite **Da** in kliknite **Nadaljuj**.
5. Kot podpisnika novega potrdila izberite **VeriSign ali drugo internetno službo za potrdila (CA)** in kliknite **Nadaljuj**. Prikazal se bo obrazec, na katerem lahko vnesete določilne informacije za novo potrdilo.
6. Izpolnite obrazec in kliknite **Nadaljuj**. Prikazala se bo potrditvena stran z zahtevanimi podatki potrdila, ki jih morate posredovati javni službi za potrdila (CA), ki bo izdala vaše potrdilo. Podatki zahteve za podpis potrdila (CSR) so sestavljeni iz javnega ključa in drugih informacij, ki ste jih podali za novo potrdilo.
7. Previdno prekopirajte podatke CSR in jih prilepite v obrazec za potrdilo ali v ločeno datoteko, ki jo potrebuje javna služba za potrdila, če zahtevate potrdilo. Uporabiti morate vse podatke CSR, vključno z vrsticama Begin in End New Certificate Request. Ko zaprete to stran, izgubite podatke in ni jih več mogoče obnoviti. Obrazec ali datoteko pošljite službi za potrdila, ki ste jo izbrali za izdajanje in podpišite potrdilo.

   Opomba: Preden lahko končate ta postopek, morate počakati, da vam služba za potrdila vrne podpisano in dokončano potrdilo.
8. Ko vam služba za potrdila vrne podpisano potrdilo, zaženite Upravljalnik digitalnih potrdil.
9. V levem oknu za usmerjanje kliknite **Izbira prostora za potrdila** in kot prostor za potrdila, ki naj se odpre, izberite ***OBJECTSIGNING**.
10. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo, ki ste ga podali pri izdelavi prostora za potrdila in kliknite **Nadaljuj**.
11. V oknu za usmerjanje izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
12. S seznama nalog izberite **Uvozi potrdilo**, da boste začeli postopek uvažanja podpisanega potrdila v prostor za potrdila *OBJECTSIGNING. Ko uvozite potrdilo, lahko izdelate definicijo aplikacije za uporabo potrdila za podpisovanje objektov.
13. Ko je levo okno za usmerjanje osveženo, izberite **Upravljanje aplikacij**, da prikažete seznam nalog.
14. S seznama nalog izberite **Dodaj aplikacijo**, da boste začeli postopek izdelave definicije aplikacije za podpisovanje objektov, tako da bo za podpisovanje objektov uporabljala potrdila.
15. Izpolnite obrazec in definirajte aplikacijo za podpisovanje objektov, nato pa kliknite **Dodaj**. Ta definicija aplikacije ne opisuje dejanske aplikacije, pač pa tip objektov, ki jih nameravate podpisovati z določenim potrdilom. Pri izpolnjevanju obrazca si pomagajte z zaslonsko pomočjo.

16. Za potrditev sporočila o definiciji aplikacije kliknite **Potrdi** in prikažite seznam nalog Upravljanje aplikacij.
17. S seznama nalog izberite **Ažuriraj dodelitev potrdila** in kliknite **Nadaljuj**, da boste prikazali seznam ID-jev aplikacij za podpisovanje objektov, za katere lahko dodelite potrdilo.
18. S seznama izberite ID aplikacije in kliknite **Ažuriraj dodelitev potrdila**.
19. Izberite potrdilo, ki ste ga uvozili in kliknite **Dodeli novo potrdilo**.

Ko končate te naloge, imate vse, kar potrebujete za začetek podpisovanja objektov, s čimer boste zagotovili njihovo integriteto.

Če pošljete podpisane objekte, morajo prejemniki uporabiti različico Upravljalnika digitalnih potrdil V5R1 ali novejšo, s katero bodo preverili veljavnost podpisa in zagotovili, da so podatki nespremenjeni in preverili identiteto pošiljatelja. Za preverjanje veljavnosti podpisa mora imeti prejemnik kopijo potrdila. Kopijo tega potrdila morate posredovati kot del paketa podpisanih objektov.

Prejemnik mora imeti tudi kopijo potrdila službe, ki je izdala potrdilo, uporabljeno za podpis objekta. Če ste objekte podpisali s potrdilom znane internetne službe za potrdila, sprejemnikova različica Upravljalnika digitalnih potrdil morda že ima kopijo potrebnega potrdila službe za potrdila. Morda boste vseeno želeli posredovati kopijo potrdila službe za potrdila skupaj s podpisanimi objekti, saj je morda sprejemnik še nima. Če ste objekte denimo podpisali s potrdilom zasebne lokalne službe za potrdila, morate sprejemniku posredovati kopijo potrdila lokalne službe za potrdila. Iz varnostnih razlogov morate potrdilo službe za potrdila posredovati v ločenem paketu ali pa ga na zahtevo tistih, ki ga potrebujejo, dati na razpolago vsem.

Upravljanje potrdil za preverjanje podpisov objektov

S pomočjo Upravljalnika digitalnih potrdil (DCM) lahko upravljate potrdila za pregledovanje podpisov, ki jih uporabljate za preverjanje veljavnosti digitalnih podpisov na objektih. Za podpis objekta uporabljate zasebni ključ potrdila, s katerim izdelate podpis. Če pošljete podpisan objekt drugim uporabnikom, morate vključiti kopijo potrdila, ki je bilo uporabljeno za podpis objekta. To naredite tako, da s pomočjo Upravljalnika digitalnih potrdil izvozite potrdilo, ki je podpisalo objekt (brez zasebnega ključa potrdila) kot potrdilo za preverjanje podpisa. Potrdilo za preverjanje podpisa lahko izvozite v datoteko, ki jo pošljete drugim uporabnikom. Če želite preveriti podpise, ki jih izdelate, lahko izvozite potrdilo za preverjanje podpisa v prostor za potrdila *SIGNATUREVERIFICATION.

Če želite preveriti veljavnost podpisa objekta, morate imeti kopijo potrdila, ki je podpisalo objekt. Z javnim ključem potrdila, ki ga vsebuje potrdilo, pregledate in preverite veljavnost podpisa, ki je bil izdelan z ustreznim zasebnim ključem. Preden torej lahko preverite veljavnost podpisa objekta, morate od uporabnika, ki vam je poslal podpisane objekte, pridobiti kopijo potrdila, uporabljenega za podpis.

Imeti morate tudi kopijo potrdila službe za potrdila (CA), ki je izdala potrdilo, uporabljeno za podpis objekta. S potrdilom CA preverite pristnost potrdila, ki je podpisalo objekt. Upravljalnik digitalnih potrdil nudi potrdila znanih služb za potrdila. Če pa je bil objekt podpisan s potrdilom druge javne službe za potrdila ali zasebne lokalne službe za potrdila, morate pridobiti njegovo kopijo, preden lahko preverite veljavnost podpisa objekta.

Če želite z Upravljalnikom digitalnih potrdil preverjati podpise objektov, morate najprej izdelati ustrezen prostor za potrdila za upravljanje potrebnih potrdil za preverjanje podpisov - to je prostor za potrdila *SIGNATUREVERIFICATION. Ko izdelate ta prostor za potrdila, ga Upravljalnik digitalnih potrdil samodejno izpolni s kopijami potrdil znanih javnih služb za potrdila.

Opomba: Če želite preveriti podpise, ki jih izdelate, z lastnimi potrdili za podpis objektov, morate izdelati prostor za potrdila *SIGNATUREVERIFICATION in vanj prekopirati potrdila iz prostora za potrdila *OBJECTSIGNING. To velja celo, če nameravate izvajati preverjanje podpisov znotraj prostora za potrdila *OBJECTSIGNING.

Za uporabo Upravljalnika digitalnih potrdil za upravljanje potrdil za preverjanje podpisov opravite naslednje naloge:

1. Zaženite DCM.
2. V levem usmerjalnem oknu upravljalnika digitalnih potrdil izberite **Izdelava novega prostora za potrdila**, da poženete vodeno nalogo in izpolnite vrsto obrazcev.

Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.

3. Za izdelavo izberite prostor za potrdila ***SIGNATUREVERIFICATION** in kliknite **Nadaljuj**.

   Opomba: Če prostor za potrdila *OBJECTSIGNING obstaja, vas bo Upravljalnik digitalnih potrdil na tej točki pozval, da podate, ali želite prekopirati potrdila za podpisovanje objektov v nov prostor za potrdila kot potrdila za preverjanje podpisov. Če želite za overjanje podpisov uporabljati obstoječa potrdila za podpisovanje objektov, izberite **Da** in kliknite **Nadaljuj**. Če želite iz prostora za potrdila *OBJECTSIGNING kopirati potrdila, morate poznati njegovo geslo.

4. Podajte geslo novega prostora za potrdila in kliknite **Nadaljuj**, da boste izdelali prostor za potrdila. Prikaže se potrditvena stran, ki kaže, da je bil prostor za potrdila izdelan uspešno. Zdaj lahko uporabite prostor za upravljanje in uporabo potrdil za preverjanje podpisov objektov.

   Opomba: Če ste ta prostor izdelali tako, da lahko preverjate potrdila na podpisanih objektih, lahko nehate. Ko izdelate nova potrdila za podpisovanje objektov, jih morate izvoziti iz prostora za potrdila *OBJECTSIGNING v ta prostor za potrdila. Če jih ne izvozite, ne boste mogli preveriti veljavnosti podpisov, ki jih izdelate z njimi.

   Opomba: Če ste ta prostor za potrdila izdelali zato, da lahko preverjate podpise objektov, ki jih prejmete od drugih virov, morate nadaljevati s tem postopkom, da lahko uvozite potrebna potrdila v prostor za potrdila.

5. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***SIGNATUREVERIFICATION**.
6. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo, ki ste ga podali pri izdelavi prostora za potrdila in kliknite **Nadaljuj**.
7. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
8. S seznama nalog izberite **Uvozi potrdilo**. Ta vodena naloga vas vodi skozi postopek uvažanja potrebnih potrdil v prostor za potrdila, tako da lahko preverite prejeti podpis objektov.
9. Izberite tip potrdila, ki ga želite uvoziti. Izberite **Preverjanje podpisa**, da boste uvozili potrdilo, ki ste ga prejeli s podpisanim objektom in dokončali nalogo uvažanja.

   Opomba: Če prostor za potrdila še ne vsebuje kopije potrdila službe za potrdila, ki je izdala potrdilo za preverjanje veljavnosti podpisa, morate tega uvoziti *najprej*. Ko uvažate potrdilo za overjanje podpisov, lahko prejmete sporočilo o napaki, če pred uvozom potrdila za preverjanje podpisov ne uvozite potrdila službe za potrdila.

Zdaj lahko s temi potrdili preverite veljavnost podpisov objektov.

Poglavje 8. Upravljanje DCM

Po konfiguriranju upravljalnika digitalnih potrdil (DCM), boste morali čez čas izvesti številne naloge upravljanja potrdil. Če želite spoznati, kako uporabiti DCM za upravljanje vaših digitalnih potrdil, preglejte naslednje teme:

Za izdajanje potrdil za druge sisteme iSeries uporabite lokalno službo za potrdila.
Spoznajte, kako uporabiti zasebno lokalno službo za potrdila na enem sistemu za izdajanje potrdil za uporabo v drugih sistemih.

Upravljanje aplikacij v upravljalniku digitalnih potrdil
Spoznajte, kako uporabljati DCM za delo z definicijami aplikacij za aplikacije, ki so omogočene za SSL, ali aplikacije za podpisovanje objektov. Ta tema nudi informacije o izdelavi definicij aplikacij in o tem, kako upravljati dodelitev potrdil aplikacijam. Naučili se boste definirati sezname overjenih služb za potrdila, ki jih uporabljajo aplikacije kot osnovo za sprejemanje potrdil za overjanje odjemalcev.

Upravljanje potrdil glede na datum zapadlosti
Seznanite se z uporabo Upravljalnika digitalnih potrdil za pregledovanje in upravljanje potrdil glede na datum njihove zapadlosti.

Preverjanje veljavnosti potrdil in aplikacij
Spoznajte, kako lahko preverite pristnost določenega potrdila, preden ga aplikacija uporabi ali sprejme.

Dodelitev potrdila
Spoznajte, kako lahko hitro dodelite potrdilo eni ali več aplikacijam za uporabo za zaščitene funkcije.

Upravljanje mest CRL
Spoznajte, kako definirati in uporabljati mesta seznama za preklic potrdil (CRL), ki jih lahko uporabljajo aplikacije za preverjanje veljavnosti potrdil, ki jih sprejmejo.

Hramba ključev potrdila v IBM-ovem Šifrirnem koprocesorju
Spoznajte, kako z nameščenim koprocesorjem za omogočite varnejšo hrambo za zasebne ključe potrdil.

Upravljanje mest zahteva za službo za potrdila PKIX
Spoznajte, kako lahko uporabite DCM za upravljanje potrdil, ki jih dobite pri javni internetni službi za potrdila, ki izdaja potrdila v skladu s standardi PKIX (Public Key Infrastructure X.509).

Upravljanje mesta LDAP za uporabniška potrdila
Naučite se konfigurirati DCM za shranjevanje uporabniških potrdil v mestu imenika strežnika LDAP (poenostavljeni protokol imeniškega dostopa), da razširite preslikavo istovetnosti podjetja (EIM), tako da bo delovala z uporabniškimi potrdili.

Podpisovanje objektov
Spoznajte, kako uporabiti DCM za upravljanje potrdil, ki jih uporabljate za digitalno podpisovanje objektov, da zagotovite njihovo integriteto.

Preverjanje podpisov objektov
Spoznajte, kako uporabiti DCM za preverjanje pristnosti digitalnih podpisov na objektih.

Uporaba lokalne službe za potrdila za izdajanje potrdil za druge sisteme iSeries

Morda na strežniku v omrežju že uporabljate zasebno lokalno službo za potrdila (CA), zdaj pa želite razširiti njeno uporabo tudi na druge strežnike v omrežju. Želite na primer, da trenutna lokalna služba za potrdila izda potrdilo strežnika ali odjemalca za aplikacijo na drugem strežniku, ki bo uporabljeno za komunikacijske seje SSL. Ali pa želite uporabiti potrdila lokalne službe za potrdila v enem sistemu za podpisovanje objektov, ki jih hranite na drugem strežniku.

To nalogo lahko opravite z Upravljalnikom digitalnih potrdil. Nekatere naloge opravite na strežniku, na katerem vodite lokalno službo za potrdila, druge pa na sekundarnem strežniku, ki gosti aplikacije, za katere želite izdajati potrdila. Ta sekundarni sistem se imenuje ciljni sistem. Naloge, ki jih morate opraviti v ciljnem sistemu, so odvisne od ravni izdaje tega sistema.

Opomba: Če strežnik, s katerega vodite lokalno službo za potrdila, uporablja izdelek ponudnika šifriranega dostopa, ki nudi močnejše šifriranje kot ciljni sistem, lahko naletite na težave. Za V5R2 in novejše različice OS/400 ali i5/OS, je edini razpoložljivi ponudnik šifriranega dostopa 5722–AC3, ki je najmočnejši razpoložljivi izdelek. V prejšnjih izdajah ste lahko namestili drug, šibkejši izdelek ponudnika šifriranega dostopa (5722–AC1 ali 5722–AC2), ki je nudil nižje ravni funkcij šifriranja. Ko izvozite potrdilo (skupaj z zasebnim ključem), sistem šifrira datoteko, da zaščiti njeno vsebino. Če sistem uporablja boljši izdelek za šifriranje kot ciljni sistem, ciljni sistem ne more dešifrirati datoteke med postopkom uvažanja. Posledično se lahko zgodi, da uvažanje ne uspe ali pa potrdila ni mogoče uporabiti za vzpostavitev sej SSL. To velja tudi, če za novo potrdilo uporabite velikost ključa, ki ustreza uporabi šifrirnega izdelka v ciljnem sistemu.

Z lokalno službo za potrdila lahko izdajate potrdila za druge sisteme, ki jih lahko nato uporabite za podpisovanje objektov ali pa jih uporabijo aplikacije za vzpostavitev sej SSL. Če z lokalno službo za potrdila izdelate potrdilo za uporabo na drugem strežniku, datoteke, ki jih izdela Upravljalnik digitalnih potrdil, vsebujejo kopijo potrdila lokalne službe za potrdila, kot tudi kopije potrdil za številne javne internetne službe za potrdila.

Naloge, ki jih morate opraviti v Upravljalniku digitalnih potrdil, se nekoliko spreminjajo glede na tip potrdila, ki ga izda lokalna služba za potrdila ter glede na raven izdaje in pogojev v ciljnem sistemu.

Izdajanje zasebnih potrdil za uporabo v drugem sistemu različice V5R3, V5R2 ali V5R3

Če želite uporabiti vašo lokalno službo za potrdila za izdajanje potrdil za uporabo v drugem sistemu različice V5R3, V5R2 ali V5R1, v sistemu V5R3, ki gosti lokalno službo za potrdila, izvedite naslednje korake:

1. Zaženite DCM.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
2. V oknu za usmerjanje izberite **Izdelaj potrdilo**, da boste prikazali seznam tipov potrdil, ki jih lahko izdelate z uporabo lokalne službe za potrdila.

   Če želite dokončati to nalogo, vam ni treba odpreti prostora za potrdila. V teh navodilih predpostavljamo, da ne delate znotraj določenega prostora za potrdila ali da delate znotraj prostora za potrdila lokalne službe za potrdila (CA). Preden lahko opravite te naloge, mora v sistemu obstajati lokalna služba za potrdila.
3. Izberite tip potrdila, ki naj ga izda lokalna služba za potrdila in kliknite **Nadaljuj**, da boste zagnali vodeno nalogo in izpolnili niz obrazcev. Izberite izdelavo **potrdila strežnika ali odjemalca za drug sistem** (za seje SSL) ali **potrdilo za podpisovanje objektov za drug sistem**.

   Opomba: Če izdelujete potrdilo za podpisovanje objektov, ki bo uporabljeno v drugem sistemu, se mora v tem sistemu izvajati različica OS/400 V5R1 ali novejša ali i5/OS. Ker mora biti ciljni sistem različice V5R1 ali novejši, vas Upravljalnik digitalnih potrdil v lokalnem sistemu gostitelja ne pozove, naj za novo potrdilo za podpisovanje objektov izberete format ciljne izdaje OS.
4. Če izdelujete potrdilo strežnika ali odjemalca, izberite raven izdaje strežnika, za katero izdelujete potrdilo. Kliknite **Nadaljuj**, da boste prikazali obrazec, na katerem lahko podate identifikacijske informacije za novo potrdilo.

   Opomba: Raven izdaje, ki jo izberete, določa obliko, ki jo uporablja Upravljalnik digitalnih potrdil za izdelavo novega potrdila. Količina in tip identifikacijskih informacij na obrazcu se spreminjata glede na izbrano raven izdaje. To zagotavlja, da so datoteke potrdil združljive s strežnikom, ki bo potrdila uporabljal.
5. Izpolnite obrazec in kliknite **Nadaljuj**. Prikazala se bo potrditvena stran

   Opomba: Če v ciljnem sistemu že obstaja prostor za potrdila *OBJECTSIGNING ali *SYSTEM, morate za potrdilo podati enkratno oznako in ime datoteke. S podajanjem enkratne oznake in imena datoteke zagotovite preprosto uvažanje potrdil v obstoječ prostor za potrdila v ciljnem sistemu.

z imeni datotek, ki jih je izdelal Upravljalnik digitalnih potrdil za prenos v ciljni sistem. Upravljalnik digitalnih potrdil izdela te datoteke na osnovi ravni izdaje ciljnega sistema, ki ste ga podali. V te datoteke samodejno shrani kopijo potrdila lokalne službe za potrdila.

Opomba: DCM izdela novo potrdilo in v lastnem prostoru za potrdila in ustvari dve datoteki za prenos: datoteko prostora za potrdila (s pripono .KDB in datoteko zahtev (s pripono .RDB).

6. Za prenos datotek v ciljni sistem uporabite dvojiški FTP (File Transfer Protocol) ali kakšen drug način.

Izdajanje zasebnih potrdil za uporabo na strežniku V4R5

Če želite uporabiti vašo lokalno službo za potrdila za izdajanje potrdil, ki bodo uporabljena na strežniku V4R5, v sistemu V5R3, ki gosti lokalno službo za potrdila, izvedite naslednje korake:

1. Zaženite DCM.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.

2. V oknu za usmerjanje izberite **Izdelaj potrdilo**, da boste prikazali seznam tipov potrdil, ki jih lahko izdelate z uporabo lokalne službe za potrdila.

   Če želite dokončati to nalogo, vam ni treba odpreti prostora za potrdila. V teh navodilih predpostavljamo, da ne delate znotraj določenega prostora za potrdila ali da delate znotraj prostora za potrdila lokalne službe za potrdila (CA). Preden lahko opravite te naloge, mora v sistemu obstajati lokalna služba za potrdila.

3. Izberite **Potrdilo strežnika ali odjemalca za drug strežnik** za tip potrdila, ki ga naj izda lokalna služba za potrdila, in kliknite **Nadaljuj**, da poženete vodeno nalogo in pričnete izpolnjevati obrazce.

   Opomba: Ker bo izdelano potrdilo uporabljeno na strežniku V4R5, morate izbrati **potrdilo strežnika ali odjemalca za drug iSeries**. Ciljni sistemi z izdajo OS, starejšo od V5R1, ne morejo uporabljati potrdil za podpisovanje objektov.

4. Izberite raven izdaje strežnika, za katerega izdelujete to potrdilo. Kliknite **Nadaljuj**, da boste prikazali obrazec, na katerem lahko podate identifikacijske informacije za novo potrdilo.

   Opomba: Raven izdaje, ki jo izberete, določa obliko, ki jo uporablja Upravljalnik digitalnih potrdil za izdelavo novega potrdila. Količina in tip identifikacijskih informacij na obrazcu se spreminjata glede na izbrano raven izdaje. To zagotavlja, da so datoteke potrdil združljive s strežnikom, ki bo potrdila uporabljal.

5. Izpolnite obrazec in kliknite **Nadaljuj**. Prikazala se bo potrditvena stran

   Opomba: Če v ciljnem sistemu že obstaja prostor za potrdila *SYSTEM, morate za potrdilo podati enolično oznako in ime datoteke. S podajanjem enkratne oznake in imena datoteke zagotovite preprosto uvažanje potrdil v obstoječ prostor za potrdila v ciljnem sistemu.

   z imeni datotek, ki jih je izdelal Upravljalnik digitalnih potrdil za prenos v ciljni sistem. Upravljalnik digitalnih potrdil izdela te datoteke na osnovi ravni izdaje ciljnega sistema, ki ste ga podali. V te datoteke samodejno shrani kopijo potrdila lokalne službe za potrdila.

   Opomba: DCM izdela novo potrdilo in v lastnem prostoru za potrdila in ustvari dve datoteki za prenos: datoteko prostora za potrdila (s pripono .KDB in datoteko zahtev (s pripono .RDB).

   Opomba: Če nameravate potrdila v teh datotekah uporabiti v obstoječem prostoru za potrdila *SYSTEM v ciljnem sistemu V4R5, potrdila lokalne službe za potrdila ne morete uvoziti neposredno iz datotek .KDB in .RDB. Razlog za to je, da potrdilo službe za potrdila ne uporablja oblike, ki jo lahko prepozna in uporabi funkcija uvažanja Upravljalnika digitalnih potrdil. Namesto tega morate s pomočjo gostiteljskega sistema izvoziti kopijo potrdila lokalne službe za potrdila v ločeno datoteko. S tem zagotovite, da uporablja potrdilo službe za potrdila obliko, ki bo delovala s funkcijo uvažanja starejših izdaj.

6. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***SYSTEM**.
7. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo, ki ste ga podali pri izdelavi prostora za potrdila pri izdelavi na gostiteljskem sistemu, in kliknite **Nadaljuj**.

8. V oknu za usmerjanje izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
9. S seznama nalog izberite **Izvozi potrdilo**.
10. Kot tip potrdila za izvoz izberite **Služba za potrdila (CA)** in kliknite **Nadaljuj**, da boste prikazali seznam potrdil službe za potrdila.
11. S seznama potrdil izberite potrdilo lokalne službe za potrdila (na primer LOCAL_CERTIFICATE_AUTHORITY). Kliknite **Izvozi**, da boste prikazali obrazec, na katerem lahko izberete cilj potrdila službe za potrdila.
12. Izberite **Datoteka** in kliknite **Nadaljuj**.
13. Podajte celotno pot in ime izvozne datoteke in kliknite **Nadaljuj**. Prikaže se potrditvena stran, ki kaže, da je Upravljalnik digitalnih potrdil uspešno izvozil datoteko.

    Opomba: Datoteki ne pozabite dati enkratnega imena in pripone. Datoteko lahko denimo poimenujete mycafile.exp. Pri poimenovanju ne smete uporabiti naslednjih datotečnih pripon: .TXT, .KDB, .RDB ali .KYR. Uporaba ene od teh vrst pripon lahko povzroči težavo, če datoteko uvažate v ciljni sistem.
14. S pomočjo dvojiškega protokola prenosa datotek (FTP) ali druge metode prenesite izdelane datoteke prostora za potrdila (.KDB in .RDB) v ciljni sistem V4R5. Za prenos datoteke, ki vsebuje izvoženo potrdilo lokalne službe za potrdila uporabite način FTP ASCII.

Uporaba prenesenih datotek v ciljnem sistemu

Ko prenesete datoteke, v ciljnem sistemu uporabite Upravljalnik digitalnih potrdil za delo s prenesenimi datotekami potrdil. Naloge Upravljalnika digitalnih potrdil, ki jih morate opraviti, se razlikujejo glede na raven izdaje ciljnega sistema in glede na to, kateri prostori za potrdila obstajajo v ciljnem sistemu. Na naloge, ki jih morate opraviti v ciljnem sistemu, pa vpliva tudi tip potrdila, ki ste ga izdelali v gostiteljskem sistemu. Če se želite naučiti, kako uporabiti Upravljalnik digitalnih potrdil v ciljnem sistemu za delo s prenesenimi datotekami potrdil, preberite naslednje teme:

- Uporaba zasebnega potrdila za seje SSL v ciljnem sistemu V5R3 ali V5R2
- Uporaba zasebnega potrdila za seje SSL v ciljnem sistemu V5R1
- Uporaba zasebnega potrdila za podpisovanje objektov v ciljnem sistemu V5R3, V5R2 ali V5R1
- Uporaba zasebnega potrdila za seje SSL v ciljnem sistemu V4R5

Uporaba zasebnega potrdila za seje SSL v ciljnem sistemu V5R3 ali V5R2

Potrdila, ki jih uporabljajo vaše aplikacije za seje SSL, upravljate v prostoru za potrdila *SYSTEM Upravljalnika digitalnih potrdil (DCM). Če z upravljalnikom digitalnih potrdil v ciljnem sistemu V5R3 ali V5R2 še niste upravljali potrdil za SSL, ta prostor za potrdila v ciljnem sistemu ne bo obstajal. Naloge, ki jih morate opraviti za uporabo prenesenih datotek prostora za potrdila, izdelanih v gostiteljskem sistemu lokalne službe za potrdila (CA), se spreminjajo glede na to, ali prostor za potrdila *SYSTEM obstaja. Če prostor za potrdila *SYSTEM ne obstaja, lahko uporabite prenesene datoteke potrdil kot način za izdelavo prostora za potrdila *SYSTEM. Če prostor za potrdila *SYSTEM obstaja v ciljnem sistemu V5R3 ali V5R2, lahko prenesene datoteke potrdil uporabite na enega izmed naslednjih načinov:

- Uporaba prenesenih datotek kot drug sistemski prostor za potrdila.
- Uvoz prenesenih datotek v obstoječi prostor za potrdila *SYSTEM .

Prostor za potrdila *SYSTEM ne obstaja

Če prostor za potrdila *SYSTEM v sistemu V5R3 ali V5R2, v katerem želite uporabiti prenesene datoteke prostora za potrdila, ne obstaja, lahko prenesene datoteke potrdil uporabite kot prostor za potrdila *SYSTEM. Če želite izdelati prostor za potrdila *SYSTEM datoteke potrdila uporabiti v ciljnem sistemu V5R3 ali V5R2, upoštevajte naslednje korake:

1. Zagotovite, da so datoteke prostora za potrdila (ena s pripono .KDB, druga pa .RDB), ki ste jih izdelali v sistemu, ki gosti lokalno službo za potrdila, v imeniku /QIBM/USERDATA/ICSS/CERT/SERVER .
2. Ko so prenesene datoteke potrdil v imeniku /QIBM/USERDATA/ICSS/CERT/SERVER , jih preimenujte v DEFAULT.KDB ter DEFAULT.RDB. S preimenovanjem teh datotek v ustreznem imeniku izdelate komponente, ki tvorijo prostor za potrdila *SYSTEM za ciljni sistem. Datoteke prostora za potrdila že vsebujejo kopije

številnih javnih internetnih služb za potrdila. Upravljalnik digitalnih potrdil jih je skupaj s kopijo potrdila lokalne službe za potrdila dodal v datoteke prostora za potrdila, ko ste jih izdelali.

Opozorilo: Če v ciljnem sistemu že obstajata datoteki DEFAULT.KDB in DEFAULT.RDB v imeniku /QIBM/USERDATA/ICSS/CERT/SERVER , potem prostor za potrdila *SYSTEM trenutno obstaja v tem ciljnem sistemu. Zato prenesenih datotek ne smete preimenovati. Če prepišete privzete datoteke, boste imeli težave pri uporabi Upravljalnika digitalnih potrdil, prenesenega prostora za potrdila in njegove vsebine. Namesto tega morate zagotoviti, da imajo unikatna imena, in prenesen prostor za potrdila uporabiti kot **Drug sistemski prostor za potrdila**. Če datoteke uporabite kot Drug sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije bodo uporabljale potrdilo.

3. Zaženite DCM. Zdaj morate spremeniti geslo prostora za potrdila *SYSTEM, ki ste ga izdelali s preimenovanjem prenesenih datotek. S spremembo gesla omogočite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil.
4. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***SYSTEM**.
5. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo, ki ste ga za prostor za potrdila podali v sistemu *gostitelja*, ko ste izdelali potrdilo za ciljni sistem V5R3 ali V5R2, in kliknite **Nadaljuj**.
6. V oknu za usmerjanje izberite **Upravljanje prostora za potrdila**, nato pa s seznama nalog izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila. Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem. Zatem lahko podate, katere aplikacije bodo uporabljale potrdila za seje SSL.
7. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***SYSTEM**.
8. Ko se prikaže stran **Prostor za potrdila in geslo**, vnesite novo geslo in kliknite **Nadaljuj**.
9. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**, da prikažete seznam nalog.
10. S seznama nalog izberite **Dodeli potrdilo**, da prikažete seznam potrdil v trenutnem prostoru za potrdila.
11. Izberite potrdilo, ki ste ga izdelali na *gostiteljskem* sistemu in kliknite **Dodeli aplikacijam**, da prikažete seznam aplikacij, ki so omogočena za SSL, katerim lahko dodelite potrdilo.
12. Izberite aplikacijo, ki bo uporabljala potrdilo za seje SSL, in kliknite **Nadaljuj**. Upravljalnik digitalnih potrdil prikaže sporočilo, ki zahteva, da potrdite izbiro potrdila za aplikacije.

Opomba: Nekatere aplikacije, ki so omogočene za SSL, podpirajo overjanje odjemalca na osnovi potrdil. Aplikacija s to podporo mora overiti potrdila preden omogoči dostop do sredstev. Posledično morate za aplikacijo definirati seznam overjenih služb za potrdila. S tem zagotovite, da bo aplikacija preverjala veljavnost samo tistih potrdil služb za potrdila, ki ste jih podali kot overjene. Če uporabniki ali aplikacija odjemalca predložijo potrdilo službe za potrdila, ki na seznamu overjenih služb za potrdila ni podana kot overjena, je aplikacija ne bo sprejela kot osnovo za overjanje.

Ko dokončate te naloge, lahko aplikacije v ciljnem sistemu uporabijo potrdilo, ki ga je izdala lokalna služba za potrdila na drugem strežniku. Preden pa lahko za te aplikacije začnete uporabljati SSL, morate aplikacije konfigurirati za uporabo SSL.

Preden lahko uporabnik dostopi do izbranih aplikacij prek povezave SSL, mora s pomočjo Upravljalnika digitalnih potrdil pridobiti kopijo potrdila lokalne službe za potrdila iz gostiteljskega sistema. Potrdilo lokalne službe za potrdila morate prekopirati v datoteko na PC-ju uporabnika ali presneti v pregledovalnik uporabnika, glede na zahteve aplikacij, ki uporabljajo SSL.

Prostor za potrdila *SYSTEM že obstaja —, uporaba datotek kot Drug sistemski prostor za potrdila

Če ciljni sistem V5R3 ali V5R2 že ima prostor za potrdila *SYSTEM, se morate odločiti, kako boste ravnali z datotekami prostora za potrdila, ki ste jih prenesli v ciljni sistem. Prenesene datoteke potrdil lahko uporabite kot **Drug sistemski prostor za potrdila** ali pa uvozite zasebno potrdilo in njegovo ustrezno potrdilo službe za potrdila v obstoječ prostor za potrdila *SYSTEM.

Drugi sistemski prostori za potrdila so uporabniško definirani sekundarni prostori za potrdila SSL. Izdelate in uporabite jih lahko za nudenje potrdil za uporabniško napisane aplikacije, omogočene za SSL, ki za registriranje ID-ja aplikacije ne uporabljajo API-jev Upravljalnika digitalnih potrdil. Možnost Drug sistemski prostor za potrdila omogoča upravljanje potrdil za aplikacije, ki jih napišete vi ali kdo drug, in s pomočjo API-ja SSL_Init programsko dostopajo in uporabljajo potrdilo za vzpostavitev seje SSL. Ta API omogoča, da aplikacija namesto potrdila, ki ga posebej določite, uporabi privzeto potrdilo.

Aplikacije IBM iSeries (in aplikacije številnih drugih razvijalcev programske opreme) so napisane samo za uporabo potrdil v prostoru za potrdila *SYSTEM. Če prenesene datoteke uporabite kot Drug sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije bodo uporabljale potrdilo za seje SSL. Posledično tudi ne morete konfigurirati standardnih aplikacij, omogočenih za SSL, za uporabo tega potrdila. Če želite uporabljati potrdilo za aplikacije iSeries, ga morate uvoziti iz prenesenih datotek prostora za potrdila v prostor za potrdila *SYSTEM.

Naslednji koraki kažejo, kako dostopite do prenesenih datotek potrdil in delate z njimi kot z Drugim sistemskim prostorom za potrdila:

1. Zaženite DCM.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje izberite **Drug sistemski prostor za potrdila**.
3. Ko se prikaže stran Prostor za potrdila in geslo, vnesite celotno pot in ime datoteke prostora za potrdila (s pripono .KDB), ki ste jo prenesli iz gostiteljskega sistema. Vnesite tudi geslo, ki ste ga podali za prostor za potrdila, ko ste na *gostiteljskem* sistemu izdelovali potrdilo za ciljni sistem V5R2, in kliknite **Nadaljuj**.
4. V oknu za usmerjanje izberite **Upravljanje prostora za potrdila**, nato pa s seznama nalog izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila.

   Opomba: Pri spremembi gesla prostora za potrdila morate izbrati možnost **Samodejna prijava**. Z uporabo te možnosti zagotovite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v novem prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil.

   Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem. Zdaj lahko podate, naj bo potrdilo v tem prostoru uporabljeno kot privzeto potrdilo.
5. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje izberite **Drug sistemski prostor za potrdila**.
6. Ko se prikaže stran **Prostor za potrdila in geslo**, vnesite popolno pot in ime za datoteko prostora za shranjevanje potrdila, vnesite še novo geslo in kliknite **Nadaljuj**.
7. Ko se okno za usmerjanje osveži, izberite **Upravljanje prostora za potrdila** in nato s seznama nalog izberite **Nastavitev privzetega potrdila**.

Ko izdelate in konfigurirate Drug sistemski prostor za potrdila, lahko vse aplikacije, ki uporabljajo API SSL_Init, s potrdilom, ki ga vsebuje, vzpostavijo seje SSL.

Prostor za potrdila *SYSTEM obstaja,— uporaba potrdil v obstoječem prostoru za potrdila *SYSTEM

| Potrdila v prenesenih datotekah prostora za potrdila lahko v sistemih V5R3 ali V5R2, uporabite v obstoječem prostoru
| za potrdila *SYSTEM. V ta namen morate uvoziti potrdila iz datotek prostora za potrdila v obstoječ prostor za potrdila
| *SYSTEM. Vendar pa potrdil ne morete uvoziti neposredno iz datotek .KDB in .RDB, ker funkcija uvažanja
| Upravljalnika digitalnih potrdil ne prepozna njune oblike. Če želite uporabiti prenesena potrdila uporabiti v obstoječem
| prostoru za potrdila *SYSTEM, morate odpreti datoteke kot Drugi sistemski prostor za potrdila in jih izvoziti v prostor
| za potrdila *SYSTEM.

Za izvoz potrdil iz datotek prostora za potrdila v prostor za potrdila *SYSTEM opravite naslednje korake v ciljnem sistemu V5R2:

1. Zaženite DCM.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje podajte **Drug sistemski prostor za potrdila**.

3. Ko se prikaže stran Prostor za potrdila in geslo, vnesite celotno pot in ime datoteke prostora za potrdila (s pripono .KDB), ki ste jo prenesli iz gostiteljskega sistema. Vnesite tudi geslo, ki ste ga podali za prostor za potrdila, ko ste na *gostiteljskem* sistemu izdelovali potrdilo za ciljni sistem V5R2, in kliknite **Nadaljuj**.
4. V oknu za usmerjanje izberite **Upravljanje prostora za potrdila**, nato pa s seznama nalog izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila.

   Opomba: Pri spremembi gesla prostora za potrdila morate izbrati možnost **Samodejna prijava**. Z uporabo te možnosti zagotovite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v novem prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil. Če ne spremenite gesla in izberete možnost samodejne prijave, lahko naletite na težave pri izvažanju potrdil iz tega prostora v prostor za potrdila *SYSTEM.

   Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem.
5. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje izberite **Drug sistemski prostor za potrdila**.
6. Ko se prikaže stran **Prostor za potrdila in geslo**, vnesite popolno pot in ime za datoteko prostora za shranjevanje potrdila, vnesite še novo geslo in kliknite **Nadaljuj**.
7. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**. Prikaže se seznam nalog, s katerega izberite **Izvozi potrdilo**.
8. Kot tip potrdila za izvoz izberite **Služba za potrdila (CA)** in kliknite **Nadaljuj**.

   Opomba: Preden izvozite potrdilo strežnika ali odjemalca v prostor za potrdila, morate vanj izvoziti potrdilo lokalne službe za potrdila. Če najprej izvozite potrdilo strežnika ali odjemalca, lahko pride do napake, ker potrdilo lokalne službe za potrdila ne obstaja v prostoru za potrdila.
9. Izberite potrdilo lokalne službe za potrdila za izvoz in kliknite **Izvozi**.
10. Kot cilj za izvoženo potrdilo izberite **Prostor za potrdila** in kliknite **Nadaljuj**.
11. Kot ciljni prostor za potrdila vnesite *SYSTEM, vnesite geslo prostora za potrdila *SYSTEM in kliknite **Nadaljuj**. Prikaže se sporočilo, ki kaže, da se je potrdilo uspešno izvozilo, ali pa informacije o napaki, če postopek izvoza ne uspe.
12. Zdaj lahko izvozite potrdilo strežnika ali odjemalca v prostor za potrdila *SYSTEM. Znova izberite nalogo **Izvozi potrdilo**.
13. Kot tip potrdila za izvoz izberite **Strežnik ali odjemalec** in kliknite **Nadaljuj**.
14. Izberite ustrezno potrdilo strežnika ali odjemalca za izvoz in kliknite **Izvozi**.
15. Kot cilj za izvoženo potrdilo izberite **Prostor za potrdila** in kliknite **Nadaljuj**.
16. Kot ciljni prostor za potrdila vnesite *SYSTEM, vnesite geslo prostora za potrdila *SYSTEM in kliknite **Nadaljuj**. Prikaže se sporočilo, ki kaže, da se je potrdilo uspešno izvozilo, ali pa informacije o napaki, če postopek izvoza ne uspe.
17. Zdaj lahko potrdilo dodelite aplikacijam za uporabo s SSL. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in nato za odpiranje izberite prostor za potrdila ***SYSTEM**.
18. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo za prostor za potrdila *SYSTEM in kliknite **Nadaljuj**.
19. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
20. S seznama nalog izberite **Dodeli potrdilo**, da prikažete seznam potrdil v trenutnem prostoru za potrdila.
21. Izberite potrdilo, ki ste ga izdelali na *gostiteljskem* sistemu in kliknite **Dodeli aplikacijam**, da prikažete seznam aplikacij, ki so omogočena za SSL, katerim lahko dodelite potrdilo.
22. Izberite aplikacije, ki bodo uporabljale potrdilo za seje SSL, in kliknite **Nadaljuj**. Upravljalnik digitalnih potrdil prikaže sporočilo, ki zahteva, da potrdite izbiro potrdila za aplikacije.

    Opomba: Nekatere aplikacije, ki so omogočene za SSL, podpirajo overjanje odjemalca na osnovi potrdil. Aplikacija s to podporo mora overiti potrdila preden omogoči dostop do sredstev. Posledično morate za aplikacijo definirati seznam overjenih služb za potrdila. S tem zagotovite, da bo aplikacija preverjala veljavnost samo tistih potrdil služb za potrdila, ki ste jih podali kot overjene. Če uporabniki ali aplikacija odjemalca predložijo potrdilo službe za potrdila, ki na seznamu overjenih služb za potrdila ni podana kot overjena, je aplikacija ne bo sprejela kot osnovo za overjanje.

Ko dokončate te naloge, lahko aplikacije v ciljnem sistemu uporabijo potrdilo, ki ga je izdala lokalna služba za potrdila v drugem sistemu iSeries. Preden pa lahko za te aplikacije začnete uporabljati SSL, morate aplikacije konfigurirati za uporabo SSL.

Preden lahko uporabnik dostopi do izbranih aplikacij prek povezave SSL, mora s pomočjo Upravljalnika digitalnih potrdil pridobiti kopijo potrdila lokalne službe za potrdila iz gostiteljskega sistema. Potrdilo lokalne službe za potrdila morate prekopirati v datoteko na PC-ju uporabnika ali presneti v pregledovalnik uporabnika, glede na zahteve aplikacij, ki uporabljajo SSL.

Uporaba zasebnega potrdila za seje SSL v ciljnem sistemu V5R1

Potrdila, ki jih uporabljajo vaše aplikacije za seje SSL, upravljate v prostoru za potrdila *SYSTEM Upravljalnika digitalnih potrdil (DCM). Če z Upravljalnikom digitalnih potrdil v ciljnem sistemu V5R1 še niste upravljali potrdil za SSL, ta prostor za potrdila v ciljnem sistemu ne bo obstajal. Naloge, ki jih morate opraviti za uporabo prenesenih datotek prostora za potrdila, izdelanih v gostiteljskem sistemu lokalne službe za potrdila (CA), se spreminjajo glede na to, ali prostor za potrdila *SYSTEM obstaja. Če prostor za potrdila *SYSTEM ne obstaja, lahko uporabite prenesene datoteke potrdil kot način za izdelavo prostora za potrdila *SYSTEM. Če prostor za potrdila *SYSTEM obstaja v ciljnem sistemu V5R1, lahko uporabite prenesene datoteke potrdil na enega od dveh načinov:

- Uporaba prenesenih datotek kot drug sistemski prostor za potrdila.
- Uvoz prenesenih datotek v obstoječi prostor za potrdila *SYSTEM .

Prostor za potrdila *SYSTEM ne obstaja

Če prostor za potrdila *SYSTEM ne obstaja v sistemu V5R1, v katerem želite uporabiti prenesene datoteke prostora za potrdila, lahko uporabite prenesene datoteke potrdil kot prostor za potrdila *SYSTEM. Če želite datoteke potrdil uporabiti v ciljnem sistemu V5R1, naredite naslednje:

1. Zagotovite, da so datoteke prostora za potrdila (ena s pripono .KDB, druga pa .RDB), ki ste jih izdelali v sistemu, ki gosti lokalno službo za potrdila, v imeniku /QIBM/USERDATA/ICSS/CERT/SERVER .
2. Ko so prenesene datoteke potrdil v imeniku /QIBM/USERDATA/ICSS/CERT/SERVER , jih preimenujte v DEFAULT.KDB ter DEFAULT.RDB. S preimenovanjem teh datotek v ustreznem imeniku izdelate komponente, ki tvorijo prostor za potrdila *SYSTEM za ciljni sistem. Datoteke prostora za potrdila že vsebujejo kopije številnih javnih internetnih služb za potrdila. Upravljalnik digitalnih potrdil jih je skupaj s kopijo potrdila lokalne službe za potrdila dodal v datoteke prostora za potrdila, ko ste jih izdelali.

   Opozorilo: Če v ciljnem sistemu že obstajata datoteki DEFAULT.KDB in DEFAULT.RDB v imeniku /QIBM/USERDATA/ICSS/CERT/SERVER , potem prostor za potrdila *SYSTEM trenutno obstaja v tem ciljnem sistemu. Zato prenesenih datotek ne smete preimenovati. Če prepišete privzete datoteke, boste imeli težave pri uporabi Upravljalnika digitalnih potrdil, prenesenega prostora za potrdila in njegove vsebine. Namesto tega morate zagotoviti, da imajo unikatna imena, in prenesen prostor za potrdila uporabiti kot **Drug sistemski prostor za potrdila**. Če datoteke uporabite kot Drug sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije bodo uporabljale potrdilo.
3. Zaženite DCM. Zdaj morate spremeniti geslo prostora za potrdila *SYSTEM, ki ste ga izdelali s preimenovanjem prenesenih datotek. S spremembo gesla omogočite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil.
4. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***SYSTEM**.
5. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo, ki ste ga podali za prostor za potrdila, ko ste na *gostiteljskem* sistemu izdelovali potrdilo za ciljni sistem V5R1, in kliknite **Nadaljuj**.
6. V oknu za usmerjanje izberite **Upravljanje prostora za potrdila**, nato pa s seznama nalog izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila. Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem. Zatem lahko podate, katere aplikacije bodo uporabljale potrdilo za seje SSL.
7. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***SYSTEM**.
8. Ko se prikaže stran Prostor za potrdila in geslo, vnesite novo geslo in kliknite **Nadaljuj**.

9. Ko se okno za usmerjanje osveži, izberite **Upravljanje aplikacij**, da prikažete seznam nalog.
10. S seznama nalog izberite **Ažuriraj dodelitev potrdila**, da boste prikazali seznam aplikacij, omogočenih za SSL, ki jim lahko dodelite potrdilo.
11. S seznama izberite aplikacijo in kliknite **Ažuriraj dodelitev potrdila**.
12. Izberite potrdilo, ki ga je izdala lokalna služba za potrdila na *gostiteljskem* sistemu, in kliknite **Dodeli novo potrdilo**. Upravljalnik digitalnih potrdil prikaže sporočilo, ki zahteva, da potrdite izbiro potrdila za aplikacijo.

    Opomba: Nekatere aplikacije, ki so omogočene za SSL, podpirajo overjanje odjemalca na osnovi potrdil. Aplikacija s to podporo mora overiti potrdila preden omogoči dostop do sredstev. Posledično morate za aplikacijo definirati seznam overjenih služb za potrdila. S tem zagotovite, da bo aplikacija preverjala veljavnost samo tistih potrdil služb za potrdila, ki ste jih podali kot overjene. Če uporabniki ali aplikacija odjemalca predložijo potrdilo službe za potrdila, ki na seznamu overjenih služb za potrdila ni podana kot overjena, je aplikacija ne bo sprejela kot osnovo za overjanje.

Ko dokončate te naloge, lahko aplikacije v ciljnem sistemu uporabijo potrdilo, ki ga je izdala lokalna služba za potrdila v drugem sistemu iSeries. Preden pa lahko za te aplikacije začnete uporabljati SSL, morate aplikacije konfigurirati za uporabo SSL.

Preden lahko uporabnik dostopi do izbranih aplikacij prek povezave SSL, mora s pomočjo Upravljalnika digitalnih potrdil pridobiti kopijo potrdila lokalne službe za potrdila iz gostiteljskega sistema. Potrdilo službe za potrdila morate prekopirati v datoteko na PC-ju uporabnika ali presneti v pregledovalnik uporabnika, odvisno od zahtev aplikacij, ki uporabljajo SSL.

Prostor za potrdila *SYSTEM že obstaja —, uporaba datotek kot Drug sistemski prostor za potrdila

Če v ciljnem sistemu V5R1 že obstaja prostor za potrdila *SYSTEM, se morate odločiti, kako boste delali z datotekami potrdil. Prenesene datoteke potrdil lahko uporabite kot **Drug sistemski prostor za potrdila** ali pa uvozite zasebno potrdilo in njegovo ustrezno potrdilo službe za potrdila v obstoječ prostor za potrdila *SYSTEM.

Drugi sistemski prostori za potrdila so uporabniško definirani sekundarni prostori za potrdila SSL. Izdelate in uporabite jih lahko za nudenje potrdil za uporabniško napisane aplikacije, omogočene za SSL, ki za registriranje ID-ja aplikacije ne uporabljajo API-jev Upravljalnika digitalnih potrdil. Možnost Drug sistemski prostor za potrdila omogoča upravljanje potrdil za aplikacije, ki jih napišete vi ali kdo drug, in s pomočjo API-ja SSL_Init programsko dostopajo in uporabljajo potrdilo za vzpostavitev seje SSL. Ta API omogoča, da aplikacija namesto potrdila, ki ga posebej določite, uporabi privzeto potrdilo.

Aplikacije IBM iSeries (in aplikacije številnih drugih razvijalcev programske opreme) so napisane samo za uporabo potrdil v prostoru za potrdila *SYSTEM. Če prenesene datoteke uporabite kot Drug sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije bodo uporabljale potrdilo za seje SSL. Posledično tudi ne morete konfigurirati standardnih aplikacij iSeries, omogočenih za SSL, za uporabo tega potrdila. Če želite uporabljati potrdilo za aplikacije iSeries, ga morate uvoziti iz prenesenih datotek prostora za potrdila v prostor za potrdila *SYSTEM.

Naslednji koraki kažejo, kako dostopite do prenesenih datotek potrdil in delate z njimi kot z Drugim sistemskim prostorom za potrdila:
1. Zaženite DCM.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje izberite **Drug sistemski prostor za potrdila**.
3. Ko se prikaže stran Prostor za potrdila in geslo, vnesite celotno pot in ime datoteke prostora za potrdila (s pripono .KDB), ki ste jo prenesli iz gostiteljskega sistema. Vnesite tudi geslo, ki ste ga podali za prostor za potrdila, ko ste na *gostiteljskem* sistemu izdelovali potrdilo za ciljni sistem V5R1, in kliknite **Nadaljuj**.
4. V oknu za usmerjanje izberite **Upravljanje prostora za potrdila**, nato pa s seznama nalog izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila.

    Opomba: Pri spremembi gesla prostora za potrdila morate izbrati možnost **Samodejna prijava**. Z uporabo te možnosti zagotovite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v novem

prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil.

Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem. Zdaj lahko podate, naj bo potrdilo v tem prostoru uporabljeno kot privzeto potrdilo.

5. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje izberite **Drug sistemski prostor za potrdila**.
6. Ko se prikaže stran Prostor za potrdila in geslo, vnesite celotno pot in ime datoteke prostora za potrdila, vnesite novo geslo in kliknite **Nadaljuj**.
7. Ko se okno za usmerjanje osveži, izberite **Upravljanje prostora za potrdila** in nato s seznama nalog izberite **Nastavitev privzetega potrdila**.

Ko izdelate in konfigurirate Drug sistemski prostor za potrdila, lahko vse aplikacije, ki uporabljajo API SSL_Init, s potrdilom, ki ga vsebuje, vzpostavijo seje SSL.

Prostor za potrdila *SYSTEM obstaja,— uporaba potrdil v obstoječem prostoru za potrdila *SYSTEM

Potrdila iz prenesenih datotek prostora za potrdila lahko uporabite v obstoječem prostoru za potrdila *SYSTEM v sistemu V5R1. V ta namen morate uvoziti potrdila iz datotek prostora za potrdila v obstoječ prostor za potrdila *SYSTEM. Vendar pa potrdil ne morete uvoziti neposredno iz datotek .KDB in .RDB, ker funkcija uvažanja Upravljalnika digitalnih potrdil ne prepozna njune oblike. Če želite uporabiti prenesena potrdila uporabiti v obstoječem prostoru za potrdila *SYSTEM, morate odpreti datoteke kot Drugi sistemski prostor za potrdila in jih izvoziti v prostor za potrdila *SYSTEM.

Opomba: Ta postopek opisuje, kako uporabiti drug sistemski prostor za potrdilo na ciljnem sistemu za izvažanje potrdil iz izvornih datotek prostora za potrdila v prostor za potrdila *SYSTEM. Z uporabo te metode za dodajanje potrdil v prostor za potrdila *SYSTEM se lahko izognete mogočim težavam, če ciljni sistem uporablja šibkejši izdelek ponudnika šifriranega dostop (kot je 5722–AC2) kot gostiteljski sistem.

Za izvoz potrdil iz datotek prostora za potrdila v prostor za potrdila *SYSTEM opravite naslednje korake v ciljnem sistemu V5R1:

1. Zaženite DCM.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje podajte **Drug sistemski prostor za potrdila**.
3. Ko se prikaže stran Prostor za potrdila in geslo, vnesite celotno pot in ime datoteke prostora za potrdila (s pripono .KDB), ki ste jo prenesli iz gostiteljskega sistema. Vnesite tudi geslo, ki ste ga podali za prostor za potrdila, ko ste na *gostiteljskem* sistemu izdelovali potrdilo za ciljni sistem V5R1, in kliknite **Nadaljuj**.
4. V oknu za usmerjanje izberite **Upravljanje prostora za potrdila**, nato pa s seznama nalog izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila.

   Opomba: Pri spremembi gesla prostora za potrdila morate izbrati možnost **Samodejna prijava**. Z uporabo te možnosti zagotovite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v novem prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil. Če ne spremenite gesla in izberete možnost samodejne prijave, lahko naletite na težave pri izvažanju potrdil iz tega prostora v prostor za potrdila *SYSTEM.

   Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem.
5. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje izberite **Drug sistemski prostor za potrdila**.
6. Ko se prikaže stran Prostor za potrdila in geslo, vnesite celotno pot in ime datoteke prostora za potrdila, vnesite novo geslo in kliknite **Nadaljuj**.
7. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**. Prikaže se seznam nalog, s katerega izberite **Izvozi potrdilo**.
8. Kot tip potrdila za izvoz izberite **Služba za potrdila (CA)** in kliknite **Nadaljuj**.

   Opomba: Preden izvozite potrdilo strežnika ali odjemalca v prostor za potrdila, morate vanj izvoziti potrdilo lokalne službe za potrdila. Če najprej izvozite potrdilo strežnika ali odjemalca, lahko pride do napake, ker potrdilo lokalne službe za potrdila ne obstaja v prostoru za potrdila.

9. Izberite potrdilo lokalne službe za potrdila za izvoz in kliknite **Izvozi**.
10. Kot cilj za izvoženo potrdilo izberite **Prostor za potrdila** in kliknite **Nadaljuj**.
11. Kot ciljni prostor za potrdila vnesite *SYSTEM, vnesite geslo prostora za potrdila *SYSTEM in kliknite **Nadaljuj**.
12. Zdaj lahko izvozite potrdilo strežnika ali odjemalca v prostor za potrdila *SYSTEM. Znova izberite nalogo **Izvozi potrdilo**.
13. Kot tip potrdila za izvoz izberite **Strežnik ali odjemalec** in kliknite **Nadaljuj**.
14. Izberite ustrezno potrdilo strežnika ali odjemalca za izvoz in kliknite **Izvozi**.
15. Kot cilj za izvoženo potrdilo izberite **Prostor za potrdila** in kliknite **Nadaljuj**.
16. Kot ciljni prostor za potrdila vnesite *SYSTEM, vnesite geslo prostora za potrdila *SYSTEM in kliknite **Nadaljuj**. Prikaže se sporočilo, ki kaže, da se je potrdilo uspešno izvozilo, ali pa informacije o napaki, če postopek izvoza ne uspe.
17. Zdaj lahko potrdilo dodelite aplikacijam za uporabo s SSL. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in nato za odpiranje izberite prostor za potrdila ***SYSTEM**.
18. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo za prostor za potrdila *SYSTEM in kliknite **Nadaljuj**.
19. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
20. S seznama nalog izberite **Ažuriraj dodelitev potrdila**, da boste prikazali seznam aplikacij, omogočenih za SSL, ki jim lahko dodelite potrdilo.
21. S seznama izberite aplikacijo in kliknite **Ažuriraj dodelitev potrdila**.
22. Izberite potrdilo, ki ga je izdala lokalna služba za potrdila na *gostiteljskem* sistemu, in kliknite **Dodeli novo potrdilo**. Upravljalnik digitalnih potrdil prikaže sporočilo, ki zahteva, da potrdite izbiro potrdila za aplikacijo.

    Opomba: Nekatere aplikacije, ki so omogočene za SSL, podpirajo overjanje odjemalca na osnovi potrdil. Aplikacija s to podporo mora overiti potrdila preden omogoči dostop do sredstev. Posledično morate za aplikacijo definirati seznam overjenih služb za potrdila. S tem zagotovite, da bo aplikacija preverjala veljavnost samo tistih potrdil služb za potrdila, ki ste jih podali kot overjene. Če uporabniki ali aplikacija odjemalca predložijo potrdilo službe za potrdila, ki na seznamu overjenih služb za potrdila ni podana kot overjena, je aplikacija ne bo sprejela kot osnovo za overjanje.

Ko dokončate te naloge, lahko aplikacije v ciljnem sistemu uporabijo potrdilo, ki ga je izdala lokalna služba za potrdila v drugem sistemu iSeries. Preden pa lahko za te aplikacije začnete uporabljati SSL, morate aplikacije konfigurirati za uporabo SSL.

Preden lahko uporabnik dostopi do izbranih aplikacij prek povezave SSL, mora s pomočjo Upravljalnika digitalnih potrdil pridobiti kopijo potrdila lokalne službe za potrdila iz gostiteljskega sistema. Potrdilo službe za potrdila morate prekopirati v datoteko na PC-ju uporabnika ali presneti v pregledovalnik uporabnika, odvisno od zahtev aplikacij, ki uporabljajo SSL.

Za podpisovanje objektov v ciljnem sistemu V5R3, V5R2 ali V5R1 uporabite zasebno potrdilo.

Potrdila, ki jih uporabljate za podpisovanje objektov, upravljate v prostoru za potrdila *OBJECTSIGNING Upravljalnika digitalnih potrdil (DCM). Če z Upravljalnikom digitalnih potrdil še niste upravljali potrdil za podpisovanje objektov, ta prostor za potrdila v ciljnem sistemu ne bo obstajal. Naloge, ki jih morate opraviti za uporabo prenesenih datotek prostora za potrdila, izdelanih v gostiteljskem sistemu lokalne službe za potrdila, se spreminjajo glede na to, ali prostor za potrdila *OBJECTSIGNING obstaja. Če prostor za potrdila *OBJECTSIGNING ne obstaja, lahko uporabite prenesene datoteke potrdil kot način za izdelavo prostora za potrdila *OBJECTSIGNING. Če potrdilo *OBJECTSIGNING obstaja na ciljnem sistemu, morate vanj uvoziti prenesena potrdila.

Prostor za potrdila *OBJECTSIGNING ne obstaja

Naloge, ki jih morate opraviti za uporabo datotek prostora za potrdila, izdelanih v gostiteljskem sistemu lokalne službe za potrdila, se spreminjajo glede na to, ali ste v ciljnem sistemu kdaj upravljali potrdila za podpisovanje objektov s pomočjo Upravljalnika digitalnih potrdil.

Če prostor za potrdila *OBJECTSIGNING v ciljnem sistemu V5R3, V5R2 ali V5R1 s prenesenimi datotekami prostora za potrdila ne obstaja, upoštevajte naslednje korake:

1. Zagotovite, da so datoteke prostora za potrdila (ena s pripono .KDB, druga pa .RDB), ki ste jih izdelali v sistemu, ki gosti lokalno službo za potrdila, v imeniku /QIBM/USERDATA/ICSS/CERT/SIGNING .
2. Ko so prenesene datoteke potrdil v imeniku /QIBM/USERDATA/ICSS/CERT/SIGNING , jih preimenujte v SGNOBJ.KDB ter SGNOBJ.RDB, S preimenovanjem teh datotek izdelate komponente, ki tvorijo prostor za potrdila *OBJECTSIGNING za ciljni sistem. Datoteke prostora za potrdila že vsebujejo kopije številnih javnih internetnih služb za potrdila. Upravljalnik digitalnih potrdil jih je skupaj s kopijo potrdila lokalne službe za potrdila dodal v datoteke prostora za potrdila, ko ste jih izdelali.

   Opozorilo: Če v ciljnem sistemu že obstajata datoteki SGNOBJ.KDB in SGNOBJ.RDB v imeniku /QIBM/USERDATA/ICSS/CERT/SIGNING, potem prostor za potrdila *OBJECTSIGNING trenutno obstaja v tem ciljnem sistemu. Zato prenesenih datotek ne smete preimenovati. Če prepišete privzete datoteke za podpisovanje objektov, boste imeli težave pri uporabi Upravljalnika digitalnih potrdil, prenesenega prostora za potrdila in njegove vsebine. Če prostor za potrdila *OBJECTSIGNING že obstaja, morate potrdila v obstoječi prostor za potrdila pridobiti z drugim postopkom.
3. Zaženite DCM. Zdaj morate spremeniti geslo prostora za potrdila *OBJECTSIGNING. S spremembo gesla omogočite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil.
4. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***OBJECTSIGNING**.
5. Ko se prikaže stran gesla, vnesite geslo, ki ste ga podali pri izdelavi prostora za potrdila v gostiteljskem sistemu in kliknite **Nadaljuj**.
6. V oknu za usmerjanje izberite **Upravljanje prostora za potrdila**, nato pa s seznama nalog izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila. Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem. Nato lahko izdelate definicijo aplikacije za uporabo potrdila za podpisovanje objektov.
7. Ko znova odprete prostor za potrdila, v oknu za usmerjanje izberite **Upravljanje aplikacij**, da boste prikazali seznam nalog.
8. S seznama nalog izberite **Dodaj aplikacijo**, da boste začeli postopek izdelave definicije aplikacije za podpisovanje objektov, tako da bo za podpisovanje objektov uporabljala potrdila.
9. Izpolnite obrazec in definirajte aplikacijo za podpisovanje objektov, nato pa kliknite **Dodaj**. Ta definicija aplikacije ne opisuje dejanske aplikacije, pač pa tip objektov, ki jih nameravate podpisovati z določenim potrdilom. Pri izpolnjevanju obrazca si pomagajte z zaslonsko pomočjo.
10. Ko boste s klikom na **Potrdi** potrdili sporočilo definicije aplikacije, se bo prikazal seznam nalog **Upravljanje aplikacij**.
11. S seznama nalog izberite **Ažuriraj dodelitev potrdila**, da boste prikazali seznam ID-jev aplikacij za podpisovanje objektov, za katere lahko dodelite potrdilo.
12. S seznama izberite ID aplikacije in kliknite **Ažuriraj dodelitev potrdila**.
13. Izberite potrdilo, ki ga je izdala lokalna služba za potrdila na gostiteljskem sistemu, in kliknite **Dodeli novo potrdilo**.

Ko končate te naloge, imate vse, kar potrebujete za začetek podpisovanja objektov, s čimer boste zagotovili njihovo integriteto.

Če distribuirate podpisane objekte, morajo tisti, ki jih sprejmejo, uporabljati različico Upravljalnika digitalnih potrdil V5R3, V5R2 ali V5R1, da preverijo podpis na objektih in istovetnost pošiljatelja ter zagotovijo, da so podatki nespremenjeni. Za preverjanje veljavnosti podpisa mora imeti prejemnik kopijo potrdila. Kopijo tega potrdila morate posredovati kot del paketa podpisanih objektov.

Prejemnik mora imeti tudi kopijo potrdila službe, ki je izdala potrdilo, uporabljeno za podpis objekta. Če ste objekte podpisali s potrdilom znane internetne službe za potrdila, sprejemnikova različica Upravljalnika digitalnih potrdil že ima kopijo potrebnega potrdila službe za potrdila. Če je to potrebno, pa morate kljub temu posredovati kopijo potrdila službe za potrdila v ločenem paketu, skupaj s podpisanimi objekti. Če ste objekte denimo podpisali s potrdilom lokalne

službe za potrdila, morate sprejemniku posredovati kopijo potrdila lokalne službe za potrdila. Iz varnostnih razlogov morate potrdilo službe za potrdila posredovati v ločenem paketu ali pa ga na zahtevo tistih, ki ga potrebujejo, dati na razpolago vsem.

Prostor za potrdila *OBJECTSIGNING že obstaja

| Potrdila v prenesenih datotekah prostora za potrdila lahko v sistemih V5R3, V5R2 ali V5R1 uporabite v obstoječem
| prostoru za potrdila *OBJECTSIGNING. V ta namen morate uvoziti potrdila iz datotek prostora za potrdila v obstoječ
| prostor za potrdila *OBJECTSIGNING. Vendar pa potrdil ne morete uvoziti neposredno iz datotek .KDB in .RDB, ker
| funkcija uvažanja Upravljalnika digitalnih potrdil ne prepozna njune oblike. Potrdila lahko dodate v obstoječ prostor za
| potrdila *OBJECTSIGNING tako, da prenesene datoteke odprete kot Drug sistemski prostor za potrdila v ciljnem
| sistemu V5R3, V5R2 ali V5R1. Nato lahko izvozite potrdila neposredno v prostor za potrdila *OBJECTSIGNING. Iz
| prenesenih datotek morate izvoziti kopijo potrdila za podpisovanje objektov in potrdila lokalne službe za potrdila.

| Če želite potrdila iz datotek prostora za potrdila izvoziti neposredno v prostor za potrdila *OBJECTSIGNING, v
| ciljnem sistemu V5R3, V5R2 ali V5R1 izvedite naslednje korake:

1. Zaženite DCM.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje podajte **Drug sistemski prostor za potrdila**.
3. Ko se prikaže stran Prostor za potrdila in geslo, vnesite celotno pot in ime datotek prostora za potrdila. Vnesite tudi geslo, ki ste ga uporabili pri njihovi izdelavi na gostiteljskem sistemu, in kliknite **Nadaljuj**.
4. V oknu za usmerjanje izberite **Upravljanje prostora za potrdila**, nato pa s seznama nalog izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila.

   Opomba: Pri spremembi gesla prostora za potrdila morate izbrati možnost **Samodejna prijava**. Z uporabo te možnosti zagotovite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v novem prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil. Če ne spremenite gesla in izberete možnost samodejne prijave, lahko naletite na težave pri izvažanju potrdil iz tega prostora v prostor za potrdila *OBJECTSIGNING.

   Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem.
5. V oknu za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje izberite **Drug sistemski prostor za potrdila**.
6. Ko se prikaže stran Prostor za potrdila in geslo, vnesite celotno pot in ime datoteke prostora za potrdila, vnesite novo geslo in kliknite **Nadaljuj**.
7. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**. Prikaže se seznam nalog, s katerega izberite **Izvozi potrdilo**.
8. Kot tip potrdila za izvoz izberite **Služba za potrdila (CA)** in kliknite **Nadaljuj**.

   Opomba: Izrazoslovje v tej nalogi predpostavlja, da takrat, ko delate z Drugim sistemskim prostorom za potrdila, delate s potrdili strežnika ali odjemalca. Razlog za to je, da je ta tip prostora za potrdila oblikovan za uporabo kot sekundarni prostor za potrdila k prostoru za potrdila *SYSTEM. Vendar pa je uporaba naloge izvažanja v tem prostoru za potrdila najpreprostejši način za dodajanje potrdil iz prenesenih datotek v obstoječi prostor za potrdila *OBJECTSIGNING.
9. Izberite potrdilo lokalne službe za potrdila za izvoz in kliknite **Izvozi**.

   Opomba: Preden izvozite potrdilo za podpisovanje objektov v prostor za potrdila, morate vanj izvoziti potrdilo lokalne službe za potrdila. Če najprej izvozite potrdilo za podpisovanje objektov, lahko pride do napake, ker potrdilo lokalne službe za potrdila ne obstaja v prostoru za potrdila.
10. Kot cilj za izvoženo potrdilo izberite **Prostor za potrdila** in kliknite **Nadaljuj**.
11. Kot ciljni prostor za potrdila vnesite *OBJECTSIGNING, nato vnesite geslo za prostor za potrdila *OBJECTSIGNING in kliknite **Nadaljuj**.
12. Zdaj lahko izvozite potrdilo za podpisovanje objektov v prostor za potrdila *OBJECTSIGNING. Znova izberite nalogo **Izvozi potrdilo**.
13. Kot tip potrdila za izvoz izberite **Strežnik ali odjemalec** in kliknite **Nadaljuj**.
14. Izberite ustrezno potrdilo za izvoz in kliknite **Izvozi**.

15. Kot cilj za izvoženo potrdilo izberite **Prostor za potrdila** in kliknite **Nadaljuj**.
16. Kot ciljni prostor za potrdila vnesite *OBJECTSIGNING, nato vnesite geslo za prostor za potrdila *OBJECTSIGNING in kliknite **Nadaljuj**. Prikaže se sporočilo, ki kaže, da se je potrdilo uspešno izvozilo, ali pa informacije o napaki, če postopek izvoza ne uspe.

    Opomba: Če želite to potrdilo uporabiti za podpisovanje objektov, morate aplikaciji za podpisovanje objektov zdaj dodeliti potrdilo.

Uporaba zasebnega potrdila za seje SSL v ciljnem sistemu V4R5

Potrdila, ki jih uporabljajo vaše aplikacije za seje SSL, upravljate v prostoru za potrdila *SYSTEM Upravljalnika digitalnih potrdil (DCM). Če z Upravljalnikom digitalnih potrdil v ciljnem sistemu V4R5 še niste upravljali potrdil za SSL, ta prostor za potrdila v ciljnem sistemu ne bo obstajal. Prenesene datoteke prostora za potrdila, ki ste ga izdelali na gostiteljskem sistemu lokalne službe za potrdila, vsebujejo dve potrdili. Te datoteke so strežniško in odjemalsko potrdilo, ki ste ju izdelali, ter potrdilo lokalne službe za potrdila, ki ste ga uporabili za podpisovanje.

Naloge, ki jih morate opraviti za uporabo prenesenih datotek prostora za potrdila, se spreminjajo glede na to, ali prostor za potrdila *SYSTEM obstaja. Če prostor za potrdila *SYSTEM ne obstaja, lahko uporabite prenesene datoteke potrdil kot način za izdelavo prostora za potrdila *SYSTEM. Če prostor za potrdila *SYSTEM obstaja v ciljnem sistemu, lahko uporabite prenesene datoteke potrdil na enega od dveh načinov:

- Uporaba prenesenih datotek kot drug sistemski prostor za potrdila.
- Uvoz prenesenih datotek v obstoječi prostor za potrdila *SYSTEM .

Prostor za potrdila *SYSTEM ne obstaja

Če prostor za potrdila *SYSTEM v ciljnem sistemu V4R5, v katerem želite uporabiti prenesene datoteke prostora za potrdila, ne obstaja, upoštevajte naslednje korake:

1. Zagotovite, da so datoteke prostora za potrdila (ena s pripono .KDB, druga pa .RDB), ki ste jih izdelali v sistemu, ki gosti lokalno službo za potrdila, v imeniku /QIBM/USERDATA/ICSS/CERT/SERVER .
2. Ko so prenesene datoteke potrdil v imeniku /QIBM/USERDATA/ICSS/CERT/SERVER , jih preimenujte v DEFAULT.KDB ter DEFAULT.RDB. S preimenovanjem teh datotek v ustreznem imeniku izdelate komponente, ki tvorijo prostor za potrdila *SYSTEM za ciljni sistem. Datoteke prostora za potrdila že vsebujejo kopije številnih javnih internetnih služb za potrdila. Upravljalnik digitalnih potrdil jih je skupaj s kopijo potrdila lokalne službe za potrdila dodal v datoteke prostora za potrdila, ko ste jih izdelali.

    Opozorilo: Če v ciljnem sistemu že obstajata datoteki DEFAULT.KDB in DEFAULT.RDB v imeniku /QIBM/USERDATA/ICSS/CERT/SERVER , potem prostor za potrdila *SYSTEM trenutno obstaja v tem ciljnem sistemu. Zato prenesenih datotek ne smete preimenovati. Če prepišete privzete datoteke, boste imeli težave pri uporabi Upravljalnika digitalnih potrdil, prenesenega prostora za potrdila in njegove vsebine. Namesto tega morate zagotoviti, da imajo unikatna imena in prenesene datoteke prostora za potrdila uporabiti kot **Drug** prostor za potrdila. Če datoteke uporabite kot Drug prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere datoteke bodo uporabljale potrdilo.
3. Zaženite DCM. Zdaj morate spremeniti geslo prostora za potrdila *SYSTEM. S spremembo gesla omogočite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil.
4. V oknu za usmerjanje mora biti na spustnem seznamu prostorov za potrdila prikazan prostor *SYSTEM. Nato izberite **Sistemska potrdila**, da boste prikazali seznam razpoložljivih nalog. Prikaže se okno **Prostor za potrdila in geslo**.
5. V ustrezna polja vnesite kot ime prostora potrdil, ki ga želite odpreti, *SYSTEM, vnesite pa tudi geslo, ki ste ga uporabili, ko ste izdelali datoteke s pomočjo lokalne službe za potrdila v gostiteljskem sistemu. Zdaj lahko spremenite geslo prostora za potrdila.
6. S seznama nalog v oknu za usmerjanje izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila. Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem.

7. Ko znova odprete prostor za potrdila *SYSTEM, s seznama nalog izberite **Delo z zaščitenimi aplikacijami**, da boste prikazali stran, na kateri lahko upravljate potrdila, povezana z določenimi aplikacijami.
8. S seznama aplikacij izberite aplikacijo, ki bo uporabljala preneseno zasebno potrdilo za seje SSL.
9. Kliknite **Delo s sistemskim potrdilom** in izberite potrdilo, ki ga je izdala lokalna služba za potrdila v gostiteljskem sistemu.
10. Kliknite **Dodeli novo potrdilo**, da bo podana aplikacija začela uporabljati izbrano potrdilo.

    Opomba: Nekatere aplikacije, ki so omogočene za SSL, podpirajo overjanje odjemalca na osnovi potrdil. Z uporabo potrdil za overjanje odjemalcev zagotovite, da aplikacija prejme veljavno potrdilo, preden omogoči dostop do sredstev, ki jih nadzoruje. Preden lahko aplikacija s to podporo overja potrdila, ki jih izda določena služba za potrdila, mora biti nastavljena tako, da zaupa službi za potrdila. Na strani **Delo s službami za potrdila** lahko zagotovite, da ima potrdilo službe za potrdila status overjenega v prostoru za potrdila. Nato na strani **Delo z zaščitenimi aplikacijami** zagotovite, da aplikacije, ki uporabljajo potrdilo, zaupajo lokalni službi za potrdila, ki ga je izdala. S tem zagotovite, da bo aplikacija preverjala veljavnost samo tistih potrdil služb za potrdila, ki ste jih podali kot overjene. Če uporabniki ali aplikacije odjemalcev predložijo potrdilo službe za potrdila, ki ni podana kot overjena, ga aplikacija ne bo sprejela kot osnovo za overjanje.

| Če zaključite te naloge, lahko aplikacije ciljnega sistema V4R5 potrdilo, ki ga je izdala lokalna služba za potrdila
| V5R3, uporabljajo v drugem sistemu iSeries. Preden pa lahko za te aplikacije začnete uporabljati SSL, morate
| aplikacije konfigurirati za uporabo SSL.

Preden lahko uporabnik dostopi do izbranih aplikacij prek povezave SSL, mora s pomočjo Upravljalnika digitalnih potrdil pridobiti kopijo potrdila lokalne službe za potrdila iz gostiteljskega sistema. Potrdilo službe za potrdila morate prekopirati v datoteko na PC-ju uporabnika ali presneti v pregledovalnik uporabnika, odvisno od zahtev aplikacij, ki uporabljajo SSL.

Prostor za potrdila *SYSTEM že obstaja —, uporaba datotek kot Drug sistemski prostor za potrdila

| Če ciljni sistem V4R5 že ima prostor za potrdila *SYSTEM, se morate odločiti, kako boste ravnali z datotekami
| prostora za potrdila, ki ste jih prenesli v ciljni sistem. Prenesene datoteke prostora za potrdila vsebujejo dve potrdili:
| potrdilo strežnika ali odjemalca, ki ste ga izdelali in potrdilo zasebne lokalne službe za potrdila, ki ste jo uporabili za
| podpis potrdila. Če želite, lahko uporabite prenesene datoteke potrdil kot **Drug** sistemski prostor za potrdila ali pa
| uvozite zasebno potrdilo in njegovo ustrezno potrdilo službe za potrdila v obstoječ prostor za potrdila *SYSTEM.

Če prenesene datoteke uporabite kot **Drug** sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije bodo uporabljale potrdilo za seje SSL. Lahko pa določite potrdilo v tem prostoru za potrdila kot privzeto potrdilo. Možnost Drug sistemski prostor za potrdila omogoča upravljanje potrdil za aplikacije, ki jih napišete vi ali kdo drug, in s pomočjo API-ja SSL_Init programsko dostopajo in uporabljajo potrdilo za vzpostavitev seje SSL. Ta API omogoča, da aplikacija namesto določenega potrdila uporabi privzeto potrdilo prostora za potrdila.

| Če prostor za potrdila *SYSTEM v ciljnem sistemu V4R5, v katerem želite uporabiti prenesene datoteke prostora za
| potrdila, že obstaja, upoštevajte naslednje korake:
1. Zaženite DCM. Zdaj morate spremeniti geslo prenesenega prostora za potrdila. S spremembo gesla omogočite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil.
2. V oknu za usmerjanje mora biti na spustnem seznamu prostorov za potrdila prikazan prostor OTHER. Nato izberite **Sistemska potrdila**, da boste prikazali seznam razpoložljivih nalog. Prikaže se okno **Prostor za potrdila in geslo**.
3. V ustrezna polja vnesite celotno pot in ime datoteke prostora za potrdila (s pripono .KDB), ki ste ga prenesli iz gostiteljskega sistema lokalne službe za potrdila. Vnesite geslo, ki ste ga uporabili pri izdelavi datotek na *gostiteljskem* sistemu. Zdaj lahko spremenite geslo prostora za potrdila.
4. S seznama nalog Sistemsko potrdilo v oknu za usmerjanje izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila.

   Opomba: Pri spremembi gesla prostora za potrdila morate izbrati možnost **Samodejna prijava**. Z uporabo te možnosti zagotovite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v novem

prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil.

Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem. Zdaj lahko podate, naj bo potrdilo v tem prostoru uporabljeno kot privzeto potrdilo.

5. V oknu za usmerjanje izberite **Delo s potrdili**, da boste prikazali stran, na kateri lahko izvedete številne naloge upravljanja potrdil.
6. S seznama potrdil izberite potrdilo, ki ga želite uporabiti kot privzetek za trenutni prostor za potrdila in kliknite **Nastavi privzetek**.

Ko izdelate in konfigurirate Drug sistemski prostor za potrdila, lahko vse aplikacije, ki uporabljajo API SSL_Init, s potrdilom, ki ga vsebuje, vzpostavijo seje SSL.

Prostor za potrdila *SYSTEM že obstaja— Uvažanje datotek v obstoječ prostor za potrdila *SYSTEM

Preden lahko uvozite potrdila v *SYSTEM v ciljnem sistemu V4R5, morate potrdila iz prostora za potrdila, ki ste ga izdelali, izvoziti v drug format datoteke. Nato lahko iz novih datotek uvozite potrdila v prostor za potrdila *SYSTEM. Prenesene datoteke prostora za potrdila vsebujejo dve potrdili: potrdilo strežnika ali odjemalca, ki ste ga izdelali in potrdilo zasebne lokalne službe za potrdila, ki ste jo uporabili za podpis potrdila. V prostor za potrdila *SYSTEM morate uvoziti izdelano potrdilo strežnika ali odjemalca in potrdilo zasebne lokalne službe za potrdila.

Opomba: Funkcije za izvoz, ki so na voljo v Upravljalniku digitalnih potrdil za V4R5, niso tako izpopolnjene kot funkcije za V5R3, zato lahko naletite na težave, če ciljni sistem uporabljate za izvoz zasebnega potrdila lokalne službe za potrdila. Zato morate *dodatno* kopijo potrdila lokalne službe za potrdila v ločeno datoteko izvoziti s sistemom gostitelja V5R3, in ne s ciljnim sistemom V4R5. Potem ko izvozite potrdilo lokalne službe za potrdila v sistem V5R3, lahko ročno prenesete izvozno datoteko potrdila lokalne službe za potrdila v ciljni sistem V4R5 in s pomočjo korakov, navedenih v tem postopku, uvozite potrdilo lokalne službe za potrdila v prostor za potrdila *SYSTEM. Potrdilo lokalne službe za potrdila morate uvoziti, *preden* uvozite zasebno potrdilo, ki ste ga izdelali z njim. Če najprej uvozite zasebno potrdilo, lahko pride do napake, ker potrdilo lokalne službe za potrdila ne obstaja v prostoru za potrdila.

Če želite izvoziti potrdila iz datotek prostora za potrdila, v ciljnem sistemu V4R5 izvedite naslednje korake:

1. Zaženite DCM.
2. V oknu za usmerjanje mora biti na spustnem seznamu prostorov za potrdila prikazan prostor OTHER. Nato izberite **Sistemska potrdila**, da boste prikazali seznam razpoložljivih nalog. Prikaže se okno **Prostor za potrdila in geslo**.
3. Podajte celotno pot in ime prenesenih datotek prostora za potrdila, podajte geslo, ki ste ga uporabili pri njihovi izdelavi v *gostiteljskem* sistemu, nato pa kliknite **Potrdi**. Zdaj lahko spremenite geslo prostora za potrdila.
4. S seznama nalog Sistemsko potrdilo v oknu za usmerjanje izberite **Spremeni geslo**. Izpolnite obrazec, da boste spremenili geslo prostora za potrdila.

   Opomba: Pri spremembi gesla prostora za potrdila morate izbrati možnost **Samodejna prijava**. Z uporabo te možnosti zagotovite, da Upravljalnik digitalnih potrdil shrani novo geslo, da boste lahko v novem prostoru za potrdila uporabljali vse upravljalne funkcije Upravljalnika digitalnih potrdil. Če ne spremenite gesla in izberete možnost samodejne prijave, lahko naletite na težave pri izvažanju potrdil iz tega prostora.

   Ko spremenite geslo, morate znova odpreti prostor za potrdila, preden lahko delate s potrdili, ki so shranjena v njem.
5. V oknu za usmerjanje izberite **Delo s potrdili**, da boste prikazali seznam potrdil.
6. S seznama izberite zasebno potrdilo in kliknite **Izvozi**, da boste prikazali stran Izvoz potrdila.
7. Izpolnite obrazec za izvažanje potrdila.

   Opomba: Datoteki ne pozabite dati enkratnega imena in pripone. Datoteko lahko denimo poimenujete myfile.exp. Pri poimenovanju ne smete uporabiti naslednjih datotečnih pripon: .TXT, .KDB, .RDB ali .KYR, ker lahko uporaba teh pripon povzroči napako pri uvažanju potrdil iz datoteke. Izberite ustrezno raven izdaje ciljnega sistema, v katerem boste uporabili to potrdilo. Izbrana raven izdaje vpliva na format za izvoženo potrdilo.
8. Kliknite **V redu**. Na vrhu strani se prikaže sporočilo, da je Upravljalnik digitalnih potrdil izvozil potrdilo v podano datoteko.

V tem trenutku ste z Upravljalnikom digitalnih potrdil v izvirnem sistemu gostitelja V5R3 že gotovo izvozili dodatno kopijo potrdila lokalne službe za potrdila in jo ročno prenesli v načinu ASCII v ciljni sistem V4R5. Prav tako ste v ciljnem sistemu z Upravljalnikom digitalnih potrdil že gotovo izvozili zasebno potrdilo strežnika ali odjemalca v datoteko. Zdaj lahko uvozite ta potrdila v prostor za potrdila *SYSTEM. Potrdilo lokalne službe za potrdila morate uvoziti, *preden* lahko uvozite zasebno potrdilo, ki ste ga izdelali z njim. Če najprej uvozite zasebno potrdilo, lahko pride do napake, ker potrdilo lokalne službe za potrdila ne obstaja v prostoru za potrdila.

Če želite ta potrdila uvoziti iz izvoznih datotek in podati, da jih lahko uporabljajo aplikacije, omogočene za SSL, v ciljnem sistemu V4R5 izvedite naslednje korake:

1. Zaženite DCM.
2. V oknu za usmerjanje mora biti na spustnem seznamu prostorov za potrdila prikazan prostor *SYSTEM. Nato izberite **Sistemska potrdila**, da boste prikazali seznam razpoložljivih nalog. Prikaže se okno **Prostor za potrdila in geslo**.
3. Za odpiranje izberite prostor za potrdila *SYSTEM, podajte geslo in kliknite **Nadaljuj**.
4. Zdaj morate uvoziti potrdilo lokalne službe za potrdila iz izvozne datoteke, ki ste jo izdelali v sistemu gostitelja V5R3. V oknu za usmerjanje izberite **Sprejmi potrdilo službe za potrdila**, da boste prikazali obrazec.
5. Izpolnite obrazec in kliknite **Potrdi**, da boste prikazali stran Uspešen sprejem potrdila. Če delate s prostorom za potrdila *SYSTEM, se na tej strani prikaže seznam aplikacij, za katere lahko določite, naj zaupajo uvoženemu potrdilu službe za potrdila.

   Opomba: Nekatere aplikacije, ki so omogočene za SSL, podpirajo overjanje odjemalca na osnovi potrdil. Z uporabo potrdil za overjanje odjemalcev zagotovite, da aplikacija prejme veljavno potrdilo, preden omogoči dostop do sredstev, ki jih nadzoruje. Preden lahko aplikacija s to podporo overja potrdila, ki jih izda določena služba za potrdila, mora biti nastavljena tako, da zaupa službi za potrdila. S tem zagotovite, da bo aplikacija preverjala veljavnost samo tistih potrdil služb za potrdila, ki ste jih podali kot overjene. Če uporabniki ali aplikacije odjemalcev predložijo potrdilo službe za potrdila, ki ni podana kot overjena, ga aplikacija ne bo sprejela kot osnovo za overjanje.
6. Izberite aplikacije, ki bodo zaupale potrdilu službe za potrdila in kliknite **Potrdi**. Prikaže se stran Status zaščitenih aplikacij, na kateri lahko potrdite, da so izbrane aplikacije nastavljene tako, da zaupajo novemu potrdilu.
7. Zdaj lahko uvozite potrdilo strežnika. V oknu za usmerjanje izberite **Delo s potrdili**, da boste prikazali seznam potrdil.
8. Kliknite **Uvozi**, da boste prikazali stran Uvoz potrdila.
9. Izpolnite obrazec za uvoz potrdila in kliknite **Potrdi**, da se vrnete na stran **Delo s potrdili**. Pazite, da boste podali ime datoteke, ki vsebuje izvoženo potrdilo strežnika ali odjemalca, ter ciljno izdajo, ki se ujema s podano, ko ste izvažali potrdilo. Na vrhu strani se prikaže sporočilo, da je Upravljalnik digitalnih potrdil dodal potrdilo v trenutni prostor za potrdila. Tudi uvoženo potrdilo se bo prikazalo na seznamu potrdil.
10. Sedaj morate podati, katere aplikacije bodo uporabljale uvoženo zasebno potrdilo za SSL. V oknu za usmerjanje izberite **Delo z zaščitenimi aplikacijami**, da boste prikazali stran, na kateri lahko upravljate potrdila, povezana s specifičnimi aplikacijami.
11. S seznama izberite aplikacijo in kliknite **Delo s sistemskim potrdilom**, da boste prikazali seznam potrdil, za katera lahko podate, naj jih uporabijo izbrane aplikacije za vzpostavljanje sej SSL.
12. S seznama izberite potrdilo in kliknite **Dodeli novo potrdilo**, da boste dodelili izbrano potrdilo podani aplikaciji. Na vrhu strani se prikaže potrditveno sporočilo, ki kaže izbiro potrdila.

Če zaključite te naloge, lahko aplikacije ciljnega sistema V4R5 potrdilo, ki ga je izdala lokalna služba za potrdila, uporabljajo na drugem strežniku. Preden pa lahko za te aplikacije začnete uporabljati SSL, morate aplikacije konfigurirati za uporabo SSL.

Preden lahko uporabnik dostopi do izbranih aplikacij prek povezave SSL, mora s pomočjo Upravljalnika digitalnih potrdil pridobiti kopijo potrdila lokalne službe za potrdila iz gostiteljskega sistema. Potrdilo službe za potrdila morate prekopirati v datoteko na PC-ju uporabnika ali presneti v pregledovalnik uporabnika, odvisno od zahtev aplikacij, ki uporabljajo SSL.

Upravljanje aplikacij v DCM

Upravljalnik digitalnih potrdil (DCM) lahko uporabite za izvajanje različnih upravljalnih nalog za aplikacije, omogočene za SSL in za aplikacije za podpisovanje objektov. Tako lahko na primer nadzirate, katera potrdila bodo uporabile aplikacije za komunikacijske sej plasti zaščitenih vtičnic (SSL). Naloge upravljanja aplikacije, ki jih lahko izvajate, se razlikujejo glede na tip aplikacije in prostor za potrdila, v katerem delate. Aplikacije lahko upravljate samo iz prostorov za potrdila *SYSTEM ali *OBJECTSIGNING.

Čeprav je večina nalog upravljanja aplikacij, ki jih nudi Upravljalnik digitalnih potrdil, preprostih, je nekaj takšnih, ki jih morda ne poznate. Za podrobnejše informacije o teh nalogah preberite naslednje teme:

Izdelava definicije aplikacije opisuje tipe aplikacij, ki jih lahko definirate in delate z njimi.

Upravljanje dodeljevanja potrdil za aplikacijo opisuje, kako lahko dodeljujete ali spreminjate potrdila, ki jih uporablja aplikacija za vzpostavitev seje SSL ali za podpisovanje objektov.

Definiranje seznama služb za potrdila, vrednih zaupanja, za aplikacijo opisuje, kdaj lahko in kdaj morate definirati, katerim službam za potrdila lahko za overjanje in sprejemanje potrdil zaupa aplikacija.

Informacije o drugih nalogah upravljalnika digitalnih potrdil lahko poiščete v zaslonski pomoči.

Izdelava definicije aplikacije

V Upravljalniku digitalnih potrdil lahko delate z dvema tipoma definicij aplikacij: definicije za aplikacije strežnika ali odjemalca, ki uporabljajo SSL in definicije za aplikacije, ki jih uporabljate za podpisovanje objektov.

Če želite uporabljati Upravljalnik digitalnih potrdil za delo z definicijami aplikacij SSL in njihovimi potrdili, mora biti aplikacija najprej registrirana z Upravljalnikom digitalnih potrdil kot definicija aplikacije, tako da ima enkraten ID aplikacije. Razvijalci aplikacij registrirajo aplikacije, omogočene za SSL, s pomočjo API-ja (QSYRGAP, QsyRegisterAppForCertUse), ki v Upravljalniku digitalnih potrdil samodejno izdela ID aplikacije. Vse IBM-ove aplikacije, omogočene za SSL, so registrirane z Upravljalnikom digitalnih potrdil, tako da ga lahko uporabite za preprosto dodelitev potrdila aplikacijam, da lahko vzpostavijo sejo SSL. Tudi za aplikacije, ki jih napišete ali kupite, lahko definirate definicijo aplikacije in zanjo izdelate ID znotraj samega Upravljalnika digitalnih potrdil. Za izdelavo definicije aplikacije SSL za aplikacijo odjemalca ali strežnika morate delati v prostoru potrdil *SYSTEM.

Če želite uporabljati potrdilo za podpisovanje objektov, morate najprej definirati aplikacijo, ki jo bo uporabilo potrdilo. Aplikacija za podpisovanje objektov za razliko od definicije aplikacije SSL ne opisuje dejanske aplikacije, Namesto tega lahko izdelana definicija aplikacije opisuje tip ali skupino objektov, ki jih nameravate podpisati. Za izdelavo definicije aplikacije za podpisovanje objektov morate delati v prostoru za potrdila *OBJECTSIGNING.

Naslednji koraki kažejo, kako izdelate definicijo aplikacije:

1. Zaženite DCM.
2. Kliknite **Izberi prostor za potrdila** in izberite ustrezen prostor za potrdila. (To je prostor za potrdila *SYSTEM ali *OBJECTSIGNING, odvisno od tipa definicije aplikacije, ki jo izdelujete.)

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
3. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo, ki ste ga podali pri izdelavi prostora za potrdila in kliknite **Nadaljuj**.
4. V oknu za usmerjanje izberite **Upravljanje aplikacij**, da boste prikazali seznam nalog.
5. S seznama nalog izberite **Dodaj aplikacijo**, da boste prikazali obrazec za definiranje aplikacije.

   Opomba: Če delate v prostoru za potrdila *SYSTEM, vas bo Upravljalnik digitalnih potrdil pozval, da izberete, ali boste dodali definicijo aplikacije strežnika ali definicijo aplikacije odjemalca.
6. Izpolnite obrazec in kliknite **Dodaj**. Informacije, ki jih lahko podate za definicijo aplikacije, se razlikujejo glede na tip aplikacije, ki jo definirate. Če definirate aplikacijo strežnika, lahko podate tudi, ali aplikacija lahko uporablja

potrdila za overjanje odjemalcev in ali mora zahtevati overjanje odjemalcev. Podate lahko tudi, da mora aplikacija za overjanje potrdil uporabljati seznam overjenih služb za potrdila.

Upravljanje dodelitve potrdila za aplikacijo

Preden lahko aplikacija izvede funkcijo zaščite, kot je na primer vzpostavitev seje plasti zaščitenih vtičnic (SSL) ali podpis objekta, morate s pomočjo Upravljalnika digitalnih potrdil (DCM) aplikacijo dodeliti potrdilo. Naslednji koraki kažejo, kako dodelite potrdilo aplikaciji ali kako spremenite dodelitev potrdila:

1. Zaženite DCM.
2. Kliknite **Izberi prostor za potrdila** in izberite ustrezen prostor za potrdila. (To je prostor za potrdila *SYSTEM ali *OBJECTSIGNING, odvisno od tipa aplikacije, ki ji želite dodeliti potrdilo.)

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
3. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo, ki ste ga podali pri izdelavi prostora za potrdila in kliknite **Nadaljuj**.
4. V oknu za usmerjanje izberite **Upravljanje aplikacij**, da boste prikazali seznam nalog.
5. Če ste v prostoru za potrdila *SYSTEM, izberite vrsto aplikacije, ki jo želite upravljati. (Ustrezno izberite aplikacijo **strežnika** ali **odjemalca**.)
6. S seznama nalog izberite **Ažuriraj dodelitev potrdila**, da boste prikazali seznam aplikacij, za katere lahko dodelite potrdilo.
7. S seznama izberite aplikacijo in kliknite **Ažuriraj dodelitev potrdila**, da boste prikazali seznam potrdil, ki jih lahko dodelite aplikaciji.
8. S seznama izberite potrdilo in kliknite **Dodeli novo potrdilo**. Upravljalnik digitalnih potrdil prikaže sporočilo, ki zahteva, da potrdite izbiro potrdila za aplikacijo.

   Opomba: Če dodeljujete potrdilo aplikaciji, omogočeni za SSL, ki podpira uporabo potrdil za overjanje odjemalca, morate za aplikacijo definirati seznam overjenih služb za potrdila. S tem zagotovite, da bo aplikacija preverjala veljavnost samo tistih potrdil služb za potrdila, ki ste jih določili kot overjene. Če uporabniki ali aplikacija odjemalca predložijo potrdilo službe za potrdila, ki na seznamu overjenih služb za potrdila ni podana kot overjena, je aplikacija ne bo sprejela kot osnovo za overjanje.

Če spremenite ali odstranite potrdilo za aplikacijo, aplikacija morda ne bo prepoznala spremembe, če se le-ta v času spreminjanja dodelitve potrdila izvaja. Strežniki iSeries Access za Windows bodo samodejno uveljavili spremembe potrdil, ki jih opravite. strežnike Telnet, strežnike IBM HTTP Server za iSeries in druge aplikacije pa boste najbrž morali zaustaviti in znova zagnati, da bodo uveljavili spremembe v potrdilu.

Začenši v V5R2 lahko uporabite nalogo Dodelite potrdila, če želite potrdilo dodeliti več aplikacijam hkrati.

Definiranje seznama overjenih služb za potrdila za aplikacijo

Aplikacije, ki podpirajo uporabo potrdil za overjanje odjemalca med sejo plasti zaščitenih vtičnic (SSL), morajo določiti, ali bodo sprejele potrdilo kot veljaven dokaz identitete. Eden od kriterijev, ki ga uporablja aplikacija za overjanje potrdila, je, ali aplikacija zaupa službi za potrdila (CA), ki je izdala potrdilo.

S pomočjo Upravljalnika digitalnih potrdil (DCM) lahko definirate, katerim službam za potrdila lahko zaupa aplikacija pri overjanju odjemalca za potrdila. Službe za potrdila, ki jim zaupa aplikacija, vodite s pomočjo seznama overjenih služb za potrdila.

Preden lahko za aplikacijo definirate seznam overjenih služb za potrdila, mora biti izpolnjenih več pogojev:

- Aplikacija mora podpirati uporabo potrdil za overjanje odjemalca.
- Definicija aplikacije mora podajati, da aplikacija uporablja seznam overjenih služb za potrdila.

Če definicija aplikacije podaja, da aplikacija uporablja seznam overjenih služb za potrdila, morate definirati seznam, preden lahko aplikacija uspešno overi potrdilo odjemalca. S tem zagotovite, da bo aplikacija preverjala veljavnost samo

tistih potrdil služb za potrdila, ki ste jih določili kot overjene. Če uporabniki ali aplikacija odjemalca predložijo potrdilo službe za potrdila, ki na seznamu overjenih služb za potrdila ni podana kot overjena, je aplikacija ne bo sprejela kot osnovo za overjanje.

Ko dodate službo za potrdila na seznam overjenih služb za aplikacijo, morate zagotoviti, da je služba za potrdila omogočena.

Naslednji koraki kažejo, kako za aplikacijo definirate seznam overjenih služb za potrdila:
1. Zaženite DCM.
2. Kliknite **Izberi prostor za potrdila** in za odpiranje izberite prostor za potrdila *SYSTEM.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
3. Ko se prikaže stran Prostor za potrdila in geslo, vnesite geslo, ki ste ga podali pri izdelavi prostora za potrdila in kliknite **Nadaljuj**.
4. V oknu za usmerjanje izberite **Upravljanje aplikacij**, da boste prikazali seznam nalog.
5. S seznama nalog izberite **Definiraj seznam overjenih služb za potrdila**.
6. Izberite tip aplikacije (strežniška ali odjemalska), za katero želite definirati seznam in kliknite **Nadaljuj**.
7. S seznama izberite aplikacijo in kliknite **Nadaljuj**, da boste prikazali seznam potrdil službe za potrdila, ki jih uporabljate za definiranje seznama overjenih služb.
8. Izberite službe za potrdila, ki jim bo zaupala aplikacija, in kliknite **Potrdi**. Upravljalnik digitalnih potrdil prikaže sporočilo, ki zahteva, da potrdite izbire seznama overjenih služb.

   Opomba: S seznama lahko izberete bodisi posamezne službe za potrdila ali pa podate, da bo aplikacija zaupala vsem ali nobeni službi za potrdila na seznamu. Preden dodate potrdilo službe za potrdila na seznam, si ga lahko ogledate in preverite njegovo veljavnost.

Upravljanje potrdil glede na datum zapadlosti

Upravljalnik digitalnih potrdil (DCM) nudi podporo za upravljanje datuma zapadlosti potrdil, s pomočjo katere lahko skrbniki upravljajo potrdila strežnika ali odjemalca, potrdila za podpisovanje objektov in uporabniška potrdila na lokalnem strežniku, glede na njihov datum zapadlosti. Če konfigurirate DCM za delo s preslikavo istovetnosti podjetja (EIM), lahko upravljate uporabniška potrdila glede na njihov datum zapadlosti po vsem podjetju.

Če z upravljalnikom digitalnih potrdil pregledujete potrdila, glede na njihov datum zapadlosti, lahko hitro in preprosto ugotovite, katera bodo kmalu potekla in jih lahko pravočasno obnovite.

Opomba: Ker lahko s pomočjo potrdila za preverjanje podpisov preverjate podpise objektov, tudi ko so potrdila že potekla, DCM ne nudi podpore za preverjanje datuma zapadlosti teh potrdil.

Če želite pregledovati in upravljati potrdila strežnika ali odjemalca ali potrdila za podpisovanje objektov glede na njihov datum zapadlosti, upoštevajte naslednje korake:
1. Zaženite DCM.

   Opomba: Če imate kakšno vprašanje o izpolnitvi določenega obrazca pri uporabi DCM, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***OBJECTSIGNING** ali ***SYSTEM**.
3. Vnesite geslo prostora za potrdila in kliknite **Nadaljuj**.
4. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**, da prikažete seznam nalog.
5. S seznama nalog izberite **Preveri datum zapadlosti**.
6. Izberite tip potrdila, ki ga želite preveriti. Če ste za v prostoru za shranjevanje potrdil *SYSTEM, izberite **Strežnik ali odjemalec**; če pa ste v prostoru za shranjevanje potrdil *OBJECTSIGNING, izberite **Podpisovanje objektov**.

7. V polje **Območje datuma zapadlosti v dneh (1-365)** vnesite število dni, za katere želite pregledati potrdila glede na njihov datum zapadlosti in kliknite **Nadaljuj**. Upravljalnik digitalnih potrdil prikaže vsa potrdila, ki potečejo med današnjim dnem in dnem, ki ustreza številu podanih dni. Upravljalnik digitalnih potrdil prav tako prikaže potrdila z datumom zapadlosti pred današnjim dnem.
8. Izberite potrdilo, ki ga želite upravljati. Po izbiri lahko pregledate podrobne informacije o potrdilu, potrdilo zbrišete, ali pa ga obnovite.
9. Ko zaključite delo s potrdili na seznamu, kliknite **Prekliči** za izhod.

Preverjanje veljavnosti potrdil in aplikacij

S pomočjo Upravljalnika digitalnih potrdil (DCM) lahko preverite veljavnost posameznih potrdil ali aplikacij, ki potrdila uporabljajo. Seznam stvari, ki jih preveri DCM, se nekoliko razlikuje glede na to, ali preverjate veljavnost potrdila ali aplikacije.

Preverjanje veljavnosti aplikacije

Z uporabo DCM za preverjanje veljavnosti definicije aplikacije pomagate preprečiti težave s potrdili za aplikacijo, če le-ta izvaja funkcijo, ki zahteva potrdila. Takšne težave lahko aplikaciji preprečijo, da uspešno sodeluje v seji plasti zaščitenih vtičnic (SSL) ali da uspešno podpisuje objekte.

Če preverjate veljavnost aplikacije, DCM preveri, ali za aplikacijo obstaja dodelitev potrdila in zagotovi, da je dodeljeno potrdilo veljavno. V primeru, da je aplikacija konfigurirana za uporabo seznama overjenih služb za potrdila (CA), DCM tudi preveri, ali seznam overjenih služb vsebuje vsaj eno potrdilo službe za potrdila. Nato DCM preveri, ali so potrdila službe za potrdila na seznamu overjenih služb za potrdila aplikacije veljavna. Če definicija aplikacije podaja obdelavo seznama za preklic potrdil (CRL) in za službo za potrdila obstaja definirano mesto CRL, DCM preveri CRL kot del postopka preverjanja veljavnosti.

Preverjanje veljavnosti potrdila

Če preverjate veljavnost potrdila, DCM preveri številne elemente, ki se nanašajo na potrdilo, da zagotovi njegovo pristnost in veljavnost. S preverjanjem veljavnosti potrdila zagotovite, da se aplikacijam, ki uporabljajo potrdilo za zaščitene komunikacije ali podpisovanje objektov, prepreči, da bi naletele na težave pri uporabi potrdila.

Kot del preverjanja veljavnosti DCM preveri, ali izbrano potrdilo ni poteklo. Prav tako preveri, da potrdilo ni navedeno na seznamu za preklic potrdil (CRL) kot preklicano, če mesto CRL obstaja za službo za potrdila, ki je izdala potrdilo. DCM tudi preveri, ali je potrdilo službe za potrdila v trenutnem prostoru za potrdila in ali je potrdilo omogočeno in s tem overjeno. Če ima potrdilo zasebni ključ (na primer potrdila strežnika, odjemalca in potrdila za podpisovanje objektov), potem DCM preveri tudi veljavnost javnega in zasebnega ključa in zagotovi, da se par ujema. Z drugimi besedami to pomeni, da DCM šifrira podatke z javnim ključem, nato pa zagotovi, da jih je mogoče dešifrirati z zasebnim ključem.

Dodelitev potrdila aplikacijam

Začenši v V5R2 omogoča nova izboljšava upravljalnika digitalnih potrdil (DCM), da potrdilo hitro in preprosto dodelite več aplikacijam. Potrdilo lahko dodelite več aplikacijam le v prostorih za potrdila *SYSTEM ali *OBJECTSIGNING.

Če želite izvesti dodelitev potrdila za eno ali več aplikacij, naredite naslednje:
1. Zaženite DCM.

   Opomba: Če imate kakšno vprašanje o izpolnitvi določenega obrazca pri uporabi DCM, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***OBJECTSIGNING** ali ***SYSTEM**.
3. Vnesite geslo prostora za potrdila in kliknite **Nadaljuj**.

4. Ko se okno za usmerjanje osveži, izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
5. S seznama nalog izberite **Dodeli potrdilo**, da prikažete seznam potrdil za trenutni prostor za potrdila.
6. S seznama izberite potrdilo in kliknite **Dodeli aplikacijam**, da prikažete seznam definicij aplikacij za trenutni prostor za potrdila.
7. S seznama izberite eno ali več aplikacij in kliknite **Nadaljuj**. Prikaže se stran s potrditvenim sporočilom za izbiro dodelitve ali pa sporočilo o napaki, če pride do napake.

Upravljanje mest CRL

Upravljalnik digitalnih potrdil (DCM) omogoča, da definirate in upravljate informacije o mestih CRL (seznam za preklic potrdil), ki jih bo uporabila določena služba za potrdila (CA) kot del postopka preverjanja veljavnosti potrdila. Upravljalnik digitalnih potrdil ali aplikacija, ki zahteva obdelavo CRL, lahko uporabita CRL, da preverita, ali služba za potrdila, ki je izdala določeno potrdilo, le-tega ni preklicala. Če za določeno službo za potrdila definirate CRL, lahko aplikacije, ki podpirajo uporabo potrdil za overjanje odjemalca, dostopijo do CRL-ja.

Aplikacije, ki podpirajo uporabo potrdil za overjanje odjemalcev, lahko z obdelavo CRL zagotovijo strožje overjanje potrdil, ki jih sprejmejo kot veljavno dokazilo identitete. Preden lahko uporabi aplikacija definirani CRL kot del postopka preverjanja veljavnosti potrdila, mora definicija aplikacije Upravljalnika digitalnih potrdil zahtevati, da aplikacija izvede obdelavo CRL.

Kako deluje obdelava CRL

Če z Upravljalnikom digitalnih potrdil preverite veljavnost potrdila ali aplikacije, Upravljalnik digitalnih potrdil izvede obdelavo CRL po privzetku kot del postopka preverjanja veljavnosti. Če za službo za potrdila, ki je izdala potrdilo, katerega veljavnost preverjate, ni definirano nobeno mesto CRL, Upravljalnik digitalnih potrdil ne more izvesti preverjanja CRL, lahko pa poskusi preveriti veljavnost drugih pomembnih informacij o potrdilu, kot veljavnost podpisa službe za potrdila na določenem potrdilu ter overjenost službe za potrdila, ki ga je izdala.

Definiranje vmesnika CRL

Naslednji koraki kažejo, kako definirate mesto CRL:
1. Zaženite DCM.
2. V oknu za usmerjanje izberite **Upravljanje mest CRL**, da boste prikazali seznam nalog.
3. S seznama nalog izberite **Dodajanje mesta CRL**, da prikažete obrazec, s katerim lahko opišete mesto CRL in način, na katerega bosta DCM ali aplikacija do tega mesta dostopala.
4. Izpolnite obrazec in kliknite **Potrdi**. Mestu CRL morate dodeliti enolično ime, določiti strežnik LDAP, ki gosti CRL in podati povezovalne informacije, ki opisujejo, kako dostopiti do strežnika LDAP.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.

   Zdaj morate definicijo mesta CRL povezati z določeno službo za pooblastila.
5. V oknu za usmerjanje izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
6. S seznama nalog izberite **Posodobi dodelitev mesta CRL**, da prikažete seznam potrdil službe za potrdila.
7. S seznama izberite potrdilo službe za potrdila, ki ga želite dodeliti definiciji mesta CRL, ki ste ga izdelali, in nato kliknite možnost **Posodobi dodelitev mesta CRL**. Prikaže se seznam mest CRL.
8. S seznama izberite mesto CRL, ki ga želite povezati s službo za potrdila, in kliknite **Posodobi dodelitev**. Na vrhu strani se prikaže sporočilo, ki kaže, da je bilo mesto CRL dodeljeno potrdilu službe za potrdila (CA).

Ko definirate mesto CRL za določeno službo za potrdila, ga lahko Upravljalnik digitalnih potrdil ali druge aplikacije uporabijo pri izvajanju obdelave CRL. Preden pa lahko obdelava CRL deluje, mora strežnik imeniških storitev vsebovati ustrezen CRL. Prav tako morate konfigurirati Imeniški strežnik (LDAP) in aplikacije odjemalca za uporabo SSL ter dodeliti potrdilo aplikacijam v DCM..

Če želite izvedeti več o konfiguriranju in uporabi Imeniškega strežnika iSeries (LDAP), preglejte naslednje teme Informacijskega centra:

- IBM Imeniški strežnik za iSeries (LDAP)
  V tej temi najdete vse potrebne informacije o konfiguriranju in uporabi Imeniškega strežnika iSeries.
- Omogočitev SSL za Imeniški strežnik
  V tej temi najdete napotke, kako konfigurirati Imeniški strežnik, da za zaščitene komunikacije uporablja SSL.

Hramba ključev potrdila v IBM-ovem Šifrirnem koprocesorju

Če ste IBM-ov Šifrirni koprocesor namestili v vaš iSeries, lahko z njegovo pomočjo ponudite varnejšo hrambo zasebnih ključev potrdila. Koprocesor lahko uporabite za shranitev zasebnega ključa potrdila strežnika, potrdila odjemalca ali potrdila lokalne službe za potrdila (CA), ne morete pa ga uporabiti za shranitev zasebnega ključa uporabniškega potrdila, ker mora biti ta shranjen v sistemu uporabnika. Koprocesorja zdaj tudi ne morete uporabiti za shranitev zasebnega ključa potrdila za podpisovanje objektov.

Koprocesor lahko uporabite za shranitev zasebnih ključev potrdil na dva načina:
- Shranitev zasebnega ključa potrdila neposredno v sam koprocesor.
- Uporaba glavnega ključa koprocesorja za šifriranje zasebnega ključa potrdila, ki ga shranite v posebni datoteki ključev.

To možnost za shranjevanje ključev lahko izberete kot del postopka izdelave ali obnovitve potrdila. Če uporabite koprocesor za shranitev zasebnega ključa potrdila, lahko za ta ključ spremenite dodelitev naprave koprocesorja.

Če želite koprocesor uporabiti za hrambo zasebnega ključa, se prepričajte, da je koprocesor vključen, šele nato lahko uporabite Upravljalnik digitalnih potrdil. V nasprotnem primeru Upravljalnik digitalnih potrdil ne bo prikazal strani za izbiro shranjevalne možnosti kot dela postopka izdelave ali obnovitve potrdila.

Če izdelujete ali obnavljate potrdilo strežnika ali odjemalca, izberete možnost za shranitev zasebnega ključa za tem, ko izberete tip službe za potrdila, ki bo podpisala trenutno potrdilo. Če izdelujete ali obnavljate lokalno službo za potrdila, izberete možnost za shranitev zasebnega ključa kot prvi korak v postopku.

Shranjevanje zasebnega ključa potrdila neposredno v koprocesor

Če želite učinkovitejšo zaščito dostopa in uporabe zasebnega ključa potrdila, ga lahko shranite neposredno v IBM-ov Šifrirni koprocesor. To možnost za shranitev ključa lahko izberete kot del postopka izdelave ali obnovitve potrdila v Upravljalniku digitalnih potrdil (DCM).

Za shranitev zasebnega ključa potrdila neposredno v koprocesor sledite korakom na strani **Izbira mesta za shranitev ključa**:
1. Kot možnost za shranitev izberite **Strojna oprema**.
2. Kliknite **Nadaljuj**. S tem boste prikazali stran **Izbira opisa šifrirne naprave**.
3. S seznama naprav izberite napravo, ki jo želite uporabiti za shranitev zasebnega ključa potrdila.
4. Kliknite **Nadaljuj**. Upravljalnik digitalnih potrdil bo prikazal nadaljnje strani za nalogo, ki jo izvajate, kot so na primer identifikacijske informacije za potrdilo, ki ga izdelujete ali obnavljate.

Uporaba glavnega ključa koprocesorja za šifriranje zasebnega ključa potrdila

Če želite učinkovitejšo zaščito dostopa in uporabe zasebnega ključa potrdila, lahko s pomočjo glavnega ključa IBM-ovega Šifrirnega koprocesorja šifrirate zasebni ključ in ga shranite v posebno datoteko ključev. To možnost za shranitev ključa lahko izberete kot del postopka izdelave ali obnovitve potrdila v Upravljalniku digitalnih potrdil (DCM).

To možnost lahko učinkovito uporabite šele, ko s spletnim vmesnikom za konfiguriranje IBM-ovega Šifrirnega koprocesorja izdelate ustrezno datoteko za shranitev ključa. S spletnim vmesnikom za konfiguriranje koprocesorja morate prav tako povezati datoteko za shranitev ključa z opisom naprave koprocesorja, ki ga želite uporabiti. Do spletnega vmesnika za konfiguriranje koprocesorja lahko dostopate prek strani z nalogami iSeries.

Če imate v sistemu nameščen in omogočen več kot en koprocesor, lahko souporabljate zasebni ključ potrdila za več naprav. Da bi lahko opisi naprav souporabljali zasebni ključ, morajo vse naprave uporabljati enak glavni ključ. Postopek porazdelitve enega glavnega ključa med več naprav se imenuje *kloniranje*. Souporaba ključa za več naprav omogoča uravnoteženje obremenitve plasti zaščitenih vtičnic (SSL), ki lahko izboljša delovanje zaščitenih sej.

Za uporabo glavnega ključa koprocesorja za šifriranje zasebnega ključa potrdila in njegovo shranitev v posebno datoteko ključev sledite korakom na strani **Izbira mesta za shranitev ključa**:

1. Kot možnost za shranitev izberite **Šifriran s strojno opremo**.
2. Kliknite **Nadaljuj**. S tem boste prikazali stran **Izbira opisa šifrirne naprave**.
3. S seznama naprav izberite tisto, ki jo želite uporabiti za šifriranje zasebnega ključa potrdila.
4. Kliknite **Nadaljuj**. Če imate nameščen in omogočen več kot en koprocesor, se prikaže stran **Izbira dodatnih opisov šifrirnih naprav**.

   Opomba: Če nimate na voljo več koprocesorjev, Upravljalnik digitalnih naprav nadaljuje s prikazom strani za nalogo, ki jo izvajate, kot so na primer identifikacijske informacije za potrdilo, ki ga izdelujete ali obnavljate.
5. S seznama naprav izberite ime enega ali več opisov naprav, s katerimi želite souporabljati zasebni ključ potrdila.

   Opomba: Opisi naprav, ki jih izberete, morajo uporabljati isti glavni ključ kot naprava, ki ste jo izbrali na prejšnji strani. Če želite preveriti, ali vse naprave uporabljajo isti glavni ključ, lahko to storite s pomočjo naloge za preverjanje glavnega ključa v spletnem vmesniku za konfiguriranje šifrirnega koprocesorja 4758. Do spletnega vmesnika za konfiguriranje koprocesorja lahko dostopate prek strani z nalogami iSeries.
6. Kliknite **Nadaljuj**. Upravljalnik digitalnih potrdil bo prikazal nadaljnje strani za nalogo, ki jo izvajate, kot so na primer identifikacijske informacije za potrdilo, ki ga izdelujete ali obnavljate.

Upravljanje mest zahteva za službo za potrdila PKIX

Služba za potrdila PKIX (Infrastruktura javnih ključev za X.509) je služba za potrdila, ki izdaja potrdila, temelječa na najnovejših internetnih standardih X.509 za izvrševanje infrastrukture javnih ključev. Standardi PKIX so očrtani v RFC-ju (Request For Comments) 2560.

Služba za potrdila PKIX zahteva pred izdajo potrdila strožjo identifikacijo, kar običajno pomeni, da mora aplikacija dokazati svojo identiteto prek registracijske službe (RA). Ko prosilec predloži dokaz o identiteti, ki ga zahteva registracijska služba, le-ta potrdi identiteto prosilca. Odvisno od veljavnih postopkov službe za potrdila bosta registracijska služba ali prosilec predložila potrjeno aplikacijo z njo povezani službi za potrdila. Ker se ti standardi uporabljajo vedno več, bodo na voljo tudi nove službe za potrdila, ki podpirajo PKIX. S pomočjo službe za potrdila, skladne s PKIX, lahko raziščete, ali vaše potrebe po zaščiti zahtevajo strog nadzor dostopa do sredstev, ki jih vaše aplikacije, omogočene za SSL, nudijo uporabnikom. Lotus Domino, na primer, nudi službo za potrdila PKIX za javno uporabo.

Če se odločite, da bo izdajala služba za potrdila PKIX potrdila za vaše aplikacije, lahko ta potrdila upravljate s pomočjo Upravljalnika digitalnih potrdil (DCM). Z njim lahko konfigurirate URL za službo za potrdila PKIX. S tem konfigurirate Upravljalnik digitalnih potrdil (DCM) tako, da nudi službo za potrdila PKIX kot možnost za pridobivanje podpisanih potrdil.

Če želite uporabljati Upravljalnik digitalnih potrdil za upravljanje potrdil službe za potrdila PKIX, morate konfigurirati Upravljalnik digitalnih potrdil tako, da uporabi mesto službe za potrdila. Kako , kažejo naslednji koraki:

1. Zaženite DCM.
2. V oknu za usmerjanje izberite **Upravljanje zahtevnega mesta PKIX**, da boste prikazali obrazec, na katerem lahko podate URL za službo za potrdila PKIX ali z njo povezano registracijsko službo.
3. Vnesite celoten URL službe za potrdila PKIX, ki jo želite uporabiti pri zahtevi za potrdilo, kot je na primer http://www.thawte.com in kliknite **Dodaj**. Z dodajanjem URL-ja konfigurirate Upravljalnik digitalnih potrdil, tako da doda službo za potrdila PKIX kot možnost za pridobivanje podpisanih potrdil.

Ko dodate zahtevno mesto službe za potrdila PKIX, Upravljalnik digitalnih potrdil doda službo za potrdila PKIX kot možnost za podajanje tipa službe za potrdila, ki jo lahko izberete za izdajanje potrdila, če izberete nalogo **Izdelaj potrdilo**.

Upravljanje mesta LDAP za uporabniška potrdila

Po privzetku Upravljalnik digitalnih potrdil (DCM) uporabniška potrdila, ki jih izda lokalna služba za potrdila (CA) shrani z uporabniškimi profili i5/OS. Vendar pa lahko konfigurirate Upravljalnik digitalnih potrdil (DCM) skupaj s preslikavo istovetnosti podjetja (EIM) tako, da bo, ko lokalna služba za potrdila izda uporabniška potrdila, javna kopija potrdila shranjena v določeno mesto imenika strežnika LDAP. Skupno konfiguriranje EIM in DCM vam omogoča, da uporabniška potrdila shranjujete na mesto imenika LDAP in tako izboljšate njihovo razpoložljivost za druge aplikacije. Takšno združeno konfiguriranje vam omogoča tudi, da z EIM upravljate uporabniška potrdila kot del uporabniške istovetnosti znotraj vašega podjetja.

Opomba: Če želite, da uporabnik shrani potrdilo druge službe za potrdila na mesto LDAP, mora dokončati nalogo **Dodeljevanje uporabniškega potrdila**.

EIM je tehnologijaeServerja, ki omogoča, da v vašem podjetju upravljate istovetnosti uporabnikov, vključujoč profile in potrdila uporabnikov i5/OS. Če želite da EIM upravlja potrdila uporabnikov, morate izvesti naslednje naloge za konfiguriranje EIM, preden pričnete izvajati naloge za konfiguriranje DCM:

1. S pomočjo čarovnika za **Konfiguriranje EIM**v Navigatorju **iSeries** konfigurirajte EIM.
2. Za vsakega uporabnika, za katerega želite, da sodeluje v EIM, izdelajte identifikator EIM.
3. Izdelajte ciljno povezavo med vsakim identifikatorjem EIM in profilom uporabnika v lokalnem uporabniškem registru i5/OS. Uporabite definicijsko ime registra EIM za lokalni uporabniški register i5/OS, ki ste ga podali s čarovnikom za **Konfiguriranje EIM**. **Opomba:** Več informacij o konfiguriranju EIM vam je na voljo v temi EIM v Informacijskem centru iSeries.

Ko končate potrebne naloge konfiguriranja EIM, morate izvesti naslednje naloge, da dokončate vsestransko konfiguriranje za skupno uporabo EIM in DCM:

1. Z nalogo Upravljalnika digitalnih opravil **Upravljanje mesta LDAP** podajte imenik LDAP, v katerega bo Upravljalnik digitalnih potrdil shranil uporabniško potrdilo, ki ga izdela lokalna služba za potrdila. Mesto LDAP ni potrebno, da je na lokalnem strežniku, niti ni potrebno, da je isti strežnik LDAP, ki ga uporablja EIM. Ko konfigurirate mesto LDAP v DCM, DCM v podani imenik LDAP shrani vsa uporabniška potrdila, ki jih izda lokalna služba za potrdila. DCM na mesto LDAP shrani tudi uporabniška potrdila, ki jih obdela naloga **Dodelitev uporabniškega potrdila**, in jih ne shrani skupaj z uporabniškim profilom.
2. Poženite ukaz **Pretvori uporabniška potrdila** (CVTUSRCERT). S tem ukazom kopirate obstoječa uporabniška potrdila v ustrezno mesto imenika LDAP. Vendar pa je z ukazom mogoče kopirati samo potrdila za uporabnika, ki je imel izdelano povezavo med identifikatorjem EIM in uporabniškim profilom. Ukaz nato izdela izvorno povezavo med vsakim potrdilom in z njim povezanim identifikatorjem EIM. Ukaz s pomočjo razločevalnega imena predmeta potrdila, razločevalnega imena izdajatelja, razpršitve teh razločevalnih imen ter javnega ključa potrdila definira ime istovetnosti uporabnika za izvorno povezavo.

Podpisovanje objektov

Za podpisovanje objektov lahko uporabite tri načine. Napišete lahko program, ki pokliče API za podpisovanje objekta. Za podpisovanje lahko uporabite Upravljalnik digitalnih potrdil (DCM), Začenši z V5R2, lahko Navigatorja iSeries s funkcijo Osrednjega upravljanja uporabite za podpisovanje objektov , medtem ko jih pakirate za distribucijo na druge strežnike.

Potrdila, ki jih upravljate z DCM, lahko uporabite za podpisovanje katerihkoli objektov, ki so shranjeni v integriranem datotečnem sistemu, razen za objekte, ki so shranjeni v knjižnici. Podpišete lahko samo te objekte, ki so shranjeni v datotečnem sistemu QSYS.LIB: *PGM, *SRVPGM, *MODULE, *SQLPKG in *FILE (samo varnostna datoteka). Novost v V5R2 je, da lahko podpišete objekte ukazov (*CMD). Objektov, ki so shranjeni na drugih strežnikih, ne morete podpisati.

Objekte lahko podpišete s potrdili, ki jih kupite pri javni internetni službi za potrdila (CA) ali s potrdili, ki jih izdelate z zasebno, lokalno službo za potrdila v DCM. Postopek podpisovanja potrdil je enak, ne glede na to, ali uporabite javna ali zasebna potrdila.

Predpogoji za podpisovanje objektov

Preden lahko za podpisovanje objektov uporabite DCM (ali API za podpisovanje objektov), morate izpolniti nekaj predpogojev:
- Prostor za potrdila *OBJECTSIGNING ste morali izdelati med postopkom za izdelavo lokalne službe za potrdila ali med upravljanjem potrdil za podpisovanje objektov javne internetne službe za potrdila.
- Prostor za potrdila *OBJECTSIGNING mora vsebovati vsaj eno potrdilo. Le-to lahko izdelate z lokalno službo za potrdila ali pa ga pridobite pri javni internetni službi za potrdila.
- Izdelati morate definicijo aplikacije, ki jo boste uporabljali za podpisovanje objektov.
- Definiciji aplikacije za podpisovanje objektov, ki jo nameravate uporabljati za podpisovanje objektov, morate dodeliti potrdilo.

Uporaba upravljalnika digitalnih potrdil za podpisovanje objektov

Naslednji koraki kažejo, kako uporabiti DCM za podpisovanje enega ali več objektov:
1. Zaženite DCM.

   Opomba: Če imate kakšno vprašanje o izpolnitvi določenega obrazca pri uporabi DCM, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***OBJECTSIGNING**.
3. Vnesite geslo za prostor potrdil *OBJECTSIGNING in kliknite **Nadaljuj**.
4. Ko se okno za usmerjanje osveži, izberite **Upravljanje podpisljivih objektov**, da boste prikazali seznam nalog.
5. S seznama nalog izberite **Podpiši objekt**, da boste prikazali seznam definicij aplikacij, ki jih lahko uporabite za podpisovanje objektov.
6. Izberite aplikacijo in kliknite **Podpiši objekt**, da boste prikazali obrazec za podajanje mesta objektov, ki jih želite podpisati.

   Opomba: Če aplikaciji, ki jo izberete, ni dodeljeno potrdilo, je ne morete uporabiti za podpis objekta. Najprej morate uporabiti nalogo **Ažuriraj dodelitev potrdila** iz kategorije **Upravljanje aplikacij**, da boste definiciji aplikacije dodelili potrdilo.
7. V prikazano polje vnesite celotno pot in ime datoteke objekta ali imenika objektov, ki jih želite podpisati in kliknite **Nadaljuj**. Namesto tega lahko tudi vnesete mesto imenika in kliknete **Preglej**, si ogledate vsebino imenika in izberete objekte, ki jih želite podpisati.

   Opomba: Ime objekta morate začeti s poševnico, sicer bo prišlo do napake. Za opis dela imenika, ki ga želite podpisati, lahko uporabite tudi določene univerzalne znake. Ta univerzalna znaka sta zvezdica (*****), ki podaja ″katerokoli število znakov″ in vprašaj (**?**), ki podaja ″katerikoli samostojni znak.″ Če želite denimo podpisati vse objekte v določenem imeniku, lahko vnesete /mydirectory/*; če želite podpisati vse programe v določeni knjižnici, vnesite /QSYS.LIB/QGPL.LIB/*.PGM. Univerzalne znake lahko uporabite samo v zadnjem delu imena poti; če vnesete, na primer, /mydirectory*/filename prejmete sporočilo o napaki. Če želite za prikaz seznama z vsebino knjižnice ali imenika uporabiti funkcijo za pregledovanje, morate univerzalni znak vnesti kot del imena poti, preden kliknete **Preglej**.
8. Izberite možnosti obdelave, ki jih želite uporabiti za podpis izbranega objekta ali objektov in kliknite **Nadaljuj**.

   Opomba: Če izberete, da boste počakali na rezultate opravila, bo datoteka rezultatov prikazana neposredno v pregledovalniku. Rezultati za trenutno opravilo bodo priključeni na konec datoteke rezultatov. Posledično lahko vsebuje datoteka poleg rezultatov trenutnega opravila tudi rezultate prejšnjih opravil. S pomočjo datumskega polja v datoteki lahko določite, katere vrstice v datoteki se nanašajo na trenutno opravilo. Datumsko polje ima obliko LLLLMMDD. Prvo polje v datoteki je lahko ID sporočila (če je med obdelavo objekta prišlo do napake) ali datumsko polje (ki kaže datum obdelave opravila).

9. Podajte celotno pot in ime datoteke, ki jo boste uporabili za shranitev rezultatov opravila za operacijo podpisovanja objekta in kliknite **Nadaljuj**. Namesto tega lahko tudi vnesete mesto imenika in kliknete **Preglej**, si ogledate vsebino imenika in izberete datoteko za shranitev rezultatov opravila. Prikaže se sporočilo, ki kaže, da je bilo predloženo opravilo za podpis objektov. Za prikaz rezultatov opravila si v dnevniku opravil oglejte opravilo **QOBJSGNBAT**.

Preverjanje podpisov objektov

S pomočjo Upravljalnika digitalnih potrdil (DCM) lahko preverite pristnost digitalnih podpisov na objektih. S preverjanjem podpisa zagotovite, da podatki v objektu niso bili spremenjeni od trenutka, ko je lastnik podpisal objekt.

Predpogoji za preverjanje podpisa

Preden lahko za preverjanje podpisov objektov uporabite DCM, morate izpolniti nekaj predpogojev:

- Izdelati morate prostor za potrdila *SIGNATUREVERIFICATION za upravljanje potrdil za preverjanje podpisov.

  Opomba: Če preverjate podpise za objekte, ki so bili podpisani v istem sistemu, lahko opravite preverjanje, medtem ko delate znotraj prostora za potrdila *OBJECTSIGNING. Koraki, ki jih morate opraviti za preverjanje podpisov v DCM, so enaki ne glede na to, kateri prostor za potrdila uporabljate. Prostor za potrdila *SIGNATUREVERIFICATION pa mora obstajati in vsebovati kopijo potrdila, ki je podpisal objekt, tudi če izvajate preverjanje podpisa med delom znotraj prostora potrdil *OBJECTSIGNING.
- Prostor za potrdila *SIGNATUREVERIFICATION mora vsebovati kopijo potrdila, ki je podpisal objekt.
- Prostor za potrdila *SIGNATUREVERIFICATION mora vsebovati kopijo potrdila službe za potrdila, ki je izdala potrdilo, uporabljeno za podpis objektov.

Uporaba DCM za preverjanje podpisov objektov

Naslednji koraki kažejo, kako uporabiti DCM za preverjanje podpisov objektov:

1. Zaženite DCM.

   Opomba: Če imate kakšno vprašanje o izpolnitvi določenega obrazca pri uporabi DCM, izberite vprašaj (**?**) na vrhu strani, da pridete do zaslonske pomoči.
2. V oknu za usmerjanje kliknite **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***SIGNATUREVERIFICATION**.
3. Vnesite geslo za prostor za potrdila *SIGNATUREVERIFICATION in kliknite **Nadaljuj**.
4. Ko se okno za usmerjanje osveži, izberite **Upravljanje podpisljivih objektov**, da boste prikazali seznam nalog.
5. S seznama nalog izberite **Preveri podpis objekta** in podajte mesto objektov, za katere želite preveriti podpise.
6. V prikazano polje vnesite celo pot in ime datoteke objekta ali imenika objektov, za katere želite preveriti podpise in kliknite **Nadaljuj**. Namesto tega lahko tudi vnesete mesto imenika in kliknete **Preglej**, si ogledate vsebino imenika in izberete objekte, za katere želite preveriti podpis.

   Opomba: Za opis dela imenika, ki ga želite preveriti, lahko uporabite tudi določene univerzalne znake. Ta univerzalna znaka sta zvezdica (*****), ki podaja ″katerokoli število znakov″ in vprašaj (**?**), ki podaja ″katerikoli samostojni znak.″ Če želite denimo podpisati vse objekte v določenem imeniku, lahko vnesete /mydirectory/*; če želite podpisati vse programe v določeni knjižnici, vnesite /QSYS.LIB/QGPL.LIB/*.PGM. Univerzalne znake lahko uporabite samo v zadnjem delu imena poti; če vnesete, na primer, /mydirectory*/filename prejmete sporočilo o napaki. Če želite za prikaz seznama z vsebino knjižnice ali imenika uporabiti funkcijo za pregledovanje, morate univerzalni znak vnesti kot del imena poti, preden kliknete **Preglej**.
7. Izberite možnosti obdelave, ki jih želite uporabiti za preverjanje podpisa izbranega objekta ali objektov in kliknite **Nadaljuj**.

   Opomba: Če izberete, da boste počakali na rezultate opravila, bo datoteka rezultatov prikazana neposredno v pregledovalniku. Rezultati za trenutno opravilo bodo priključeni na konec datoteke rezultatov. Posledično lahko vsebuje datoteka poleg rezultatov trenutnega opravila tudi rezultate prejšnjih opravil.

S pomočjo datumskega polja v datoteki lahko določite, katere vrstice v datoteki se nanašajo na trenutno opravilo. Datumsko polje ima obliko LLLLMMDD. Prvo polje v datoteki je lahko ID sporočila (če je med obdelavo objekta prišlo do napake) ali datumsko polje (ki kaže datum obdelave opravila).

8. Podajte celotno pot in ime datoteke, ki jo boste uporabili za shranitev rezultatov opravila za operacijo preverjanja podpisa in kliknite **Nadaljuj**. Namesto tega lahko tudi vnesete mesto imenika in kliknete **Preglej**, si ogledate vsebino imenika in izberete datoteko za shranitev rezultatov opravila. Prikaže se sporočilo, ki kaže, da je bilo predloženo opravilo za preverjanje podpisa objekta. Za prikaz rezultatov opravila si v dnevniku opravil oglejte opravilo **QOBJSGNBAT**.

DCM lahko uporabite tudi za prikaz informacij o potrdilu, ki je podpisalo objekt. Preden začnete delati z objektom, lahko na ta način določite, ali objekt izhaja iz izvora, ki mu zaupate.

Poglavje 9. Odpravljanje težav v DCM

Pri delu z Upravljalnikom digitalnih potrdil (DCM) in potrdili, lahko naletite na napake, zaradi katerih ne morete zaključiti nalog in doseči želenih ciljev. Večina splošnih napak ali težav, na katere utegnete naleteti, sodijo v določene kategorije, na primer naslednje:

Odpravljanje težav v geslih in splošne težave
V tej temi se boste naučili več o splošnih težavah uporabniškega vmesnika DCM, na katere lahko naletite in kako jih lahko odpravite.

Odpravljanje težav v prostoru za potrdila in v bazi podatkov ključev
V tej temi se boste naučili več o splošnih težavah v prostoru za potrdila in v bazi podatkov ključev, na katere lahko naletite in kako jih lahko odpravite.

Odpravljanje težav v pregledovalniku
V tej temi se boste naučili več o splošnih težavah, na katere lahko naletite pri uporabi pregledovalnika za dostopanje do Upravljalnika digitalnih potrdil in kako jih lahko odpravite.

Odpravljanje težav v strežniku HTTP
V tej temi se boste naučili več o splošnih težavah na strežniku HTTP, na katere lahko naletite in kako jih lahko odpravite.

Odpravljanje težav z nalogo za dodelitev uporabniškega potrdila
V tej temi se boste naučili več o splošnih težavah, na katere lahko naletite pri uporabi Upravljalnika digitalnih potrdil za registriranje uporabniškega potrdila in kako jih lahko odpravite.

Odpravljanje težav v geslih in splošne težave

Naslednjo tabelo lahko uporabite za iskanje informacij, ki vam bodo pomagale pri odpravljanju nekaterih pogostih težav z gesli in drugih splošnih težav, na katere lahko naletite pri delu z Upravljalnikom digitalnih potrdil.

Težava	Možna rešitev
Ne najdete dodatne pomoči za Upravljalnik digitalnih potrdil.	V Upravljalniku digitalnih potrdil kliknite ikono pomoči ″**?**″ . Preiščete lahko tudi informacijski center in zunanje IBM-ove spletne strani na internetu.
Geslo za lokalno službo za potrdila (CA) in prostor za potrdila *SYSTEM ne deluje.	Gesla so občutljiva na velike in male črke. Pazite, da boste geslo vnesli tako, kot ste to storili pri dodelitvi.
Poskus vnovične nastavitve gesla pri uporabi naloge **Izbira prostora za potrdila** ni uspel.	Funkcija vnovične nastavitve deluje samo, če je Upravljalnik digitalnih potrdil shranil geslo. Upravljalnik digitalnih potrdil shrani geslo samodejno pri izdelavi prostora za potrdila, vendar če spremenite (ali na novo nastavite) geslo za drug sistemski prostor za potrdila, morate izbrati možnost **Samodejna prijava**, tako da DCM nadaljuje s skrivanjem gesla.
	Če prostor za potrdila premaknete iz enega sistema v drugega, morate spremeniti geslo za prostor za potrdila na novem sistemu, tako da zagotovite, da ga DCM samodejno skrije. Pri spreminjanju gesla morate podati izvirno geslo prostora za potrdila, ko ga odprete na novem sistemu. Možnosti za vnovično nastavitev gesla ne morete uporabiti, dokler prostora ne odprete z izvirnim geslom in ne spremenite gesla, tako da se skrije. Če geslo ni spremenjeno in skrito, DCM in SSL ne moreta samodejno obnoviti gesla, ko ga potrebujeta za različne funkcije. Če premikate prostor za potrdila, ki ga boste uporabili kot drug sistemski prostor za potrdila, morate izbrati možnost **Samodejne prijave**, ko spremenite geslo, s čimer zagotovite, da DCM skrije novo geslo za to vrsto prostora za potrdila.

Težava	Možna rešitev
	Preverite vrednost, dodeljeno atributu **Dopusti nova digitalna potrdila**, pod možnostjo **Delo z zaščito sistema** v sistemskih storitvenih orodjih (SST). Če je ta atribut nastavljen na vrednost 2 (Ne), potem ni mogoča vnovična nastavitev gesla prostora za potrdila. Vrednost tega atributa lahko pregledate ali spremenite tako, da uporabite ukaz STRSST in vnesete ID uporabnika in geslo za storitvena orodja. Nato izberite možnost **Delo z zaščito sistema** . ID uporabnika storitvenih orodij je verjetno ID uporabnika QSECOFR.
Ne morete najti izvora potrdila službe za potrdila, da bi ga sprejeli v sistem.	Potrdila nekaterih služb za potrdila niso pripravljena. Če ne uspete pridobiti potrdila službe za potrdila, se obrnite na svojega VAR, ker je morda sklenil poseben ali plačilni dogovor s službo za potrdila.
Ne morete najti prostora za potrdila *SYSTEM.	Mesto datoteke prostora za potrdila *SYSTEM mora biti /qibm/userdata/icss/cert/server/default.kdb. Če ta prostor za potrdila ne obstaja, ga izdelajte z Upravljalnikom digitalnih potrdil. To storite z nalogo za **izdelavo novega prostora za potrdila**.
Upravljalnik digitalnih potrdil je sporočil napako, ki se ponavlja, tudi ko jo popravite.	Počistite predpomnilnik pregledovalnika. Velikost predpomnilnika nastavite na 0 in znova zaženite pregledovalnik.
Imate težavo z imeniškim strežnikom (LDAP), ki vam ob prikazu informacij o zaščiteni aplikaciji, takoj po dodelitvi potrdila, ne prikaže tudi dodelitve potrdila. Ta težava je pogostejša, če za dostop do pregledovalnika Netscape Communicator uporabljate Navigator iSeries. Z vašo nastavitvijo za predpomnilnik pregledovalnika je dokument v predpomnilniku primerjan z dokumentom na omrežju **Enkrat na sejo**.	Spremenite privzeto nastavitev, da bo vsakič preverila predpomnilnik.
Če Upravljalnik digitalnih potrdil uporabite za uvoz potrdila, ki ga je podpisala zunanja služba za potrdila, kot je Entrust, se prikaže sporočilo o napaki, ki pravi, da obdobje veljavnosti ne vsebuje današnjega datuma ali ni znotraj obdobja veljavnosti izdajatelja.	Sistem uporablja splošni format časa za obdobje veljavnosti. Počakajte en dan in poskusite znova. Preverite tudi, ali ima strežnik pravilno vrednost za odmik UTC (dspsysval qutcoffset). Če v vaši državi upoštevate zimski/poletni čas, zamik morda ni pravilno nastavljen.
Pri poskusu uvoza potrdila službe Entrust pride do osnovne napake 64.	Sistem je prepoznal, da uporablja potrdilo določen format, kot je na primer format PEM. Če funkcija pregledovalnika za kopiranje ne deluje najbolje, ste morda prekopirali dodatno gradivo, ki ne spada k potrdilu, kot so na primer presledki pred vsako vrstico. Če je tako, potrdilo nima pravilnega formata za uporabo na strežniku. Nekatere zasnove spletnih strani lahko povzročijo te težave. Druge spletne strani so zasnovane tako, da se težavam izognejo. Ne pozabite primerjati videza izvirnega potrdila z izidom lepljenja, saj morajo prilepljene informacije izgledati popolnoma enako.

Odpravljanje težav v prostoru za potrdila in v bazi podatkov ključev

Z naslednjo tabelo si pomagajte pri iskanju informacij, ki vam bodo v pomoč pri odpravljanju nekaterih pogostih težav, na katere lahko naletite pri delu z prostorom za potrdila ter Upravljalnikom digitalnih potrdil.

Težava	Možna rešitev
Sistem ni našel baze podatkov ključev ali pa je odkril, da ni veljavna.	Preverite pravilnost vnesenega gesla in imena datoteke. Zagotovite, da je z imenom datoteke podana tudi pot, vključno z vodilno poševnico.

Težava	Možna rešitev

Izdelava baze podatkov ključev ni uspela ali pa ne uspe izdelava lokalne službe za potrdila.	Preverite možnost neskladnosti imena datoteke. Do neskladnosti lahko pride v drugi datoteki in ne v tisti, ki je zahtevana. Upravljalnik digitalnih potrdil poskuša zaščititi uporabniške podatke v imenikih, ki jih izdela, četudi ga te datoteke ovirajo pri uspešni izdelavi datotek, ki jih mora izdelati.
	
	To napako odpravite tako, da vse datoteke, ki so v navzkrižju, prekopirate v drug imenik, in če je mogoče, za brisanje datotek uporabite ustrezne funkcije Upravljalnika digitalnih potrdil. Če v ta namen ne morete uporabiti Upravljalnika digitalnih potrdil, ročno zbrišite datoteke iz izvornega imenika integriranega datotečnega sistema, v katerem povzročajo navzkrižje z Upravljalnikom digitalnih potrdil. Natančno si zapišite, katere datoteke ste prenesli in kam. Kopije teh datotek omogočajo, da jih obnovite, če jih boste potrebovali. Ko prenesete naslednje datoteke, morate izdelati novo službo za potrdila:
	`/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`
	
	Po prenosu naslednjih datotek morate izdelati nov prostor za potrdila *SYSTEM in sistemsko potrdilo:
	`/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`

	Morda vam manjka predpogojni licenčni program (LPP), katerega namestitev zahteva Upravljalnik digitalnih potrdil. Preverite seznam Predpogojev DCM in se prepričajte, da so vsi licenčni programi pravilno nameščeni.

Težava	Možna rešitev
Sistem ne sprejme besedilne datoteke službe za potrdila, ki je bila v dvojiškem načinu prenesena iz drugega sistema. Datoteko sprejme, če je prenesena v obliki ASCII (American National Standard Code for Information Interchange).	Obroči ključev in baze podatkov ključev so dvojiški in so torej različni. Za besedilne datoteke službe za potrdila morate uporabiti FTP (File Transfer Protocol) v načinu ASCII in FTP v dvojiškem načinu za dvojiške datoteke, kot so datoteke z naslednjimi priponami: .kdb, .kyr, .sth, .rdb itd.
Gesla baze podatkov ključev ni mogoče spremeniti. Potrdilo v bazi podatkov ključev ni več veljavno.	Ko se boste prepričali, da vzrok težavi ni napačno geslo, poiščite in zbrišite neveljavno potrdilo ali potrdila iz prostora za potrdila, nato pa poskusite spremeniti geslo. Če so potrdila v prostoru za potrdila potekla, niso več veljavna. Ker potrdila niso veljavna, funkcija za spremembo gesla tega prostora za potrdila morda ne bo dopustila spremembe gesla, postopek za šifriranje pa ne bo šifriral zasebnih ključev za pretekla potrdila. Na ta način se prepreči sprememba gesla, sistem pa lahko javi, da je eden od vzrokov poškodovan prostor za potrdila. Neveljavna (pretekla) potrdila morate odstraniti iz prostora za potrdila.
Uporabiti morate potrdila za internetnega uporabnika in torej tudi sezname za preverjanje veljavnosti, toda Upravljalnik digitalnih potrdil ne nudi funkcij za sezname za preverjanje veljavnosti.	Poslovni partnerji, ki razvijajo aplikacije, ki uporabljajo sezname za preverjanje veljavnosti, morajo programe izdelati tako, da se seznam za preverjanje veljavnosti poveže z njihovo aplikacijo kot je pričakovano. Razviti morajo tudi kodo, ki določa, kdaj je identiteta internetnega uporabnika ustrezno preverjena, da je potrdilo mogoče dodati na seznam za preverjanje veljavnosti. Preberite temo Informacijskega centra za API QsyAddVldlCertificate. Preglejte dokumentacijo Strežnik HTTP za iSeries, v kateri najdete pomoč za konfiguriranje zaščitenega primerka strežnika HTTP za uporabo seznama za overjanje.

Odpravljanje težav v pregledovalniku

Naslednjo tabelo lahko uporabite kot pomoč pri odpravljanju nekaterih pogostih težav, povezanih s pregledovalnikom, na katere lahko naletite pri delu z Upravljalnikom digitalnih potrdil.

Težava	Možna rešitev
Microsoft Internet Explorer ne pusti, da izberete drugo potrdilo, dokler ne zaženete nove seje pregledovalnika.	Zaženite novo sejo pregledovalnika za Internet Explorer.
Internet Explorer ne prikaže vseh potrdil odjemalcev/uporabnikov, ki so na izbiro na seznamu izbir pregledovalnika. Internet Explorer prikaže samo potrdila, ki jih je izdala overjena služba za potrdila, ki jih lahko uporabite na zaščitenem mestu.	Služba za potrdila mora biti overjena v bazi podatkov ključev in tudi z zaščiteno aplikacijo. Na PC se morate prijaviti za Internet Explorer z istim imenom uporabnika, kot ste ga uporabili pri shranitvi uporabniškega potrdila v pregledovalnik. Pridobite drugo uporabniško potrdilo iz sistema, do katerega dostopate. Sistemski skrbnik mora biti prepričan, da prostor za potrdila (ključna baza podatkov) še zmeraj zaupa službi za potrdila, ki je podpisala uporabniška in sistemska potrdila.
Internet Explorer 5 sprejme potrdilo službe za potrdila, ne more pa odpreti datoteke ali najti diska, na katerem je shranjeno potrdilo.	To je nova funkcija pregledovalnika za potrdila, ki jim pregledovalnik Internet Explorer še ne zaupa. Izberete lahko mesto na PC-ju.
Sprejeli ste opozorilo pregledovalnika, da se ime sistema in sistemsko potrdilo ne ujemata.	Nekateri pregledovalniki pri primerjanju imen upoštevajo velike in male črke. Vnesite URL natanko tako, kot je prikazan v sistemskem potrdilu (pazite na velike/male črke) ali pa za sistemsko potrdilo uporabite velikost črk, ki se ujema s tisto, ki jo uporablja večina uporabnikov. Če niste poznavalec, pustite ime strežnika ali sistema takšno, kot je bilo. Preveriti morate tudi, ali je imenski strežnik domene pravilno nastavljen.
Internet Explorer ste zagnali s HTTPS namesto s HTTP in prejeli opozorilo o mešanju zaščitenih in nezaščitenih sej.	Sprejmite to potrdilo in ga zanemarite, saj bo ta težava popravljena v naslednji izdaji Internet Explorerja.

Težava	Možna rešitev
Netscape Communicator 4.04 za Windows je pretvoril šestnajstiški vrednosti A1 in B1 v B2 in 9A v poljski kodni strani.	To je napaka pregledovalnika, ki vpliva samo na NSL (podpora za državne jezike). Uporabite drug pregledovalnik ali celo isto različico tega pregledovalnika na drugi platformi, kot je na primer Netscape Communicator 4.04 za AIX.
V profilu uporabnika je Netscape Communicator za 4.04 pravilno prikazal velike črke NLS uporabniškega potrdila, male črke pa napačno.	Nekateri znaki državnih jezikov, ki so bili pravilno vneseni, kasneje pri prikazu niso več pravilni. V različici Netscape Communicatorja 4.04 za Windows sta šestnajstiški vrednosti A1 in B1 pretvorjeni v B2 in 9A za poljsko kodno stran, kar povzroči prikaz drugih znakov NLS.
Pregledovalnik uporabnika opozarja, da služba potrdila še ni vredna zaupanja.	Z pomočjo DCM spremenite **Status službe za potrdila** v **omogočeno**, da službo za potrdilo označite kot zaupanja vredno.
Zahteve Internet Explorerja zavračajo povezavo za HTTPS.	To je težava funkcije pregledovalnika ali njegove konfiguracije. Pregledovalnik ne vzpostavi povezave z mestom, ki uporablja sistemsko potrdilo, ki je lahko lastnoročno podpisano ali neveljavno iz kakšnega razloga.
Pregledovalnik Netscape Communicator in strežniški izdelki uporabljajo osnovna potrdila podjetij kot je VeriSign, kot funkcijo, ki omogoča komunikacije SSL, še posebej overjanje. Vsa osnova potrdila občasno potečejo. Nekatera osnovna potrdila strežnika in pregledovalnika Netscape so potekla med 25. decembrom 19999 in 31. decembrom 1999. Če te težave niste popravili 14. decembra 1999 ali pred tem, se prikaže sporočilo o napaki.	Prejšnje različice pregledovalnika (Netscape Communicator 4.05 ali starejše) uporabljajo potrdila, ki potečejo. Pregledovalnik morate nadgraditi v trenutno različico Netscape Communicatorja. Informacije o osnovnih potrdilih pregledovalnika so na voljo na številnih spletnih mestih, vključno s http://home.netscape.com/security/ in http://www.verisign.com/server/cus/rootcert/webmaster.html. Brezplačne presnete datoteke za pregledovalnik lahko dobite na naslovu http://www.netcenter.com.

Odpravljanje težav v strežniku HTTP za iSeries

S pomočjo naslednje tabele najdete informacije, ki vam bodo v pomoč pri odpravljanju nekaterih običajnih težav s strežnikom HTTP, na katere utegnete naleteti pri delu z upravljalnikom digitalnih potrdil (DCM).

Težava	Možna rešitev
HTTPS (Hypertext Transfer Protocol Secure) ne deluje.	Zagotovite, da je strežnik HTTP pravilno konfiguriran za uporabo SSL. Konfiguracijska datoteka mora imeti v različici V5R1 in novejših **SSLAppName** nastavljen z uporabo vmesnika za upravljanje strežnika HTTP. Za konfiguracijsko datoteko mora biti prav tako konfiguriran navidezni gostitelj, ki uporablja vrata SSL, **SSL** pa mora biti za navideznega gostitelja nastavljen na **Omogočeno**. Izdana morata biti tudi dva napotka za **Spremljanje**, ki podajata dvoje različnih vrat, ena za SSL in druga, ki niso za SSL. Nastaviti ju je mogoče na strani **Splošne nastavitve**. Preverite tudi, ali je primerek strežnika izdelan in potrdilo strežnika podpisano.
Postopek registriranja primerka strežnika HTTP kot zaščitene aplikacije zahteva razjasnitev.	Na strežniku pojdite do vmesnika za upravljanje strežnika HTTP ter nastavite konfiguracijo za vaš strežnik HTTP. Najprej morate definirati navideznega gostitelja, da omogočite SSL. Potem, ko definirate navideznega gostitelja, morate podati, naj le-ta uporablja vrata, ki ste ju definirali poprej z napotkoma za **Spremljanje**(na strani **Splošne nastavitve**). Nato morate z uporabo strani **SSL z overjanjem potrdil**, ki jo najdete pod **Zaščito**, omogočiti SSL za predhodno konfiguriranega navideznega gostitelja. Vse spremembe morajo biti uveljavljene v konfiguracijski datoteki. Pomnite, da registracija vašega primerka ne pomeni tudi samodejne izbire potrdil, ki jih bo uporabljal primerek. Z upravljalnikom digitalnih potrdil morate vaši aplikaciji dodeliti določeno potrdilo, šele nato lahko poskusite zaustaviti in znova zagnati vaš primerek strežnika.

Težava	Možna rešitev
Težave imate pri nastavljanju strežnika HTTP za sezname za preverjanje veljavnosti in izbirno overjanje odjemalcev.	Možnosti za nastavitev primerka so vam na voljo v dokumentaciji Strežnik HTTP za iSeries.
Netscape Communicator počaka, da se konfiguracijska smernica v kodi strežnika HTTP izteče in šele nato dovoli, da izberete drugo potrdilo.	Velika vrednost za potrdila otežuje registriranje drugega potrdila, ker pregledovalnik še vedno uporablja prvega.
Pregledovalnik poskušate nastaviti tako, da bi predložil potrdilo X.509 strežniku HTTP, da bi lahko uporabili potrdilo kot vhodni podatek za API QsyAddVldlCertificate.	Uporabiti morate **SSLEnable** in **SSLClientAuth ON**, da bo strežnik HTTP naložil spremenljivko okolja HTTPS_CLIENT_CERTIFICATE. Ta API-ja lahko najdete v Informacijskem centru pod temo API-ji i5/OS. Morda si želite ogledati tudi seznam za preverjanje ali API-je, povezane s potrdili: • QsyListVldlCertificates in QSYLSTVC • QsyRemoveVldlCertificate in QRMVVC • QsyCheckVldlCertificate in QSYCHKVC • QsyParseCertificate in QSYPARSC in tako dalje.
Če zahtevate seznam potrdil s seznama za preverjanje veljavnosti, ga strežnik HTTP predolgo izdeluje ali pa se zaustavi, obstaja pa več kot 10.000 postavk.	Izdelajte paketno opravilo, ki poišče in zbriše potrdila, skladna z določenimi pogoji, na primer vsa potrdila, ki so potekla, ali vsa potrdila, ki jih je izdala določena služba za potrdila.
Če je **SSL** nastavljen na **Omogočeno** zagon strežnika HTTP ne bo uspešen, v dnevniku opravila pa bo zapisano sporočilo HTP8351. Če zagon strežnika HTTP ne uspe, dnevnik napak za strežnik HTTP prikaže sporočilo o napaki, da operacija inicializacije SSL ni uspela in napako povratne kode 107.	Napaka 107 pomeni, da je potrdilo poteklo. Z upravljalnikom digitalnih potrdil aplikaciji dodelite drugo potrdilo, na primer QIBM_HTTP_SERVER_MY_SERVER. Če je primerek strežnika, ki ga ni mogoče zagnati, strežnik *ADMIN, za nekaj časa nastavite **SSL** na **Onemogočeno**, tako da lahko na strežniku *ADMIN uporabite upravljalnik digitalnih potrdil. Z njegovo pomočjo nato aplikaciji QIBM_HTTP_SERVER_ADMIN dodelite drugo potrdilo in poskusite **SSL** nastaviti nazaj na **Omogočeno**.

Odpravljanje težav pri dodeljevanju uporabniškega potrdila

Če uporabite nalogo **Dodelitev uporabniškega potrdila**, Upravljalnik digitalnih opravil (DCM) prikaže informacije o potrdilu, ki jih morate pred registriranjem potrdila odobriti. Če upravljalnik digitalnih potrdil ne more prikazati potrdila, je težavo morda povzročila katera izmed naslednjih situacij:

1. Pregledovalnik ni zahteval, da izberete potrdilo, ki bo predstavljeno strežniku. Do tega lahko pride, če je pregledovalnik shranil predhodno potrdilo v predpomnilnik (pri dostopanju do drugega strežnika). Počistite predpomnilnik pregledovalnika in ponovite nalogo. Pregledovalnik vas bo pozval, da izberete potrdilo.
2. Do tega lahko pride tudi, če konfigurirate strežnik tako, da ne prikazuje seznama izbir, pregledovalnik pa v seznamu služb za potrdila, ki jim strežnik zaupa, vsebuje samo eno potrdilo službe za potrdila. Preverite konfiguracijske nastavitve pregledovalnika in jih, če je to potrebno, spremenite. Pregledovalnik vas bo nato pozval, da izberete potrdilo. Če ne morete predložiti potrdila službe za potrdila, ki ji strežnik zaupa, ne morete dodeliti potrdila. Obrnite se na vašega skrbnika DCM.
3. Potrdilo, ki ga želite registrirati, je že registrirano z DCM.
4. Služba za potrdila, ki je izdala potrdilo, ni označena kot služba, vredna zaupanja za sistem ali omenjeno aplikacijo. Zato predstavljeno potrdilo ni veljavno. Obrnite se na skrbnika sistema, ki vam bo pomagal določiti, ali je služba za potrdila, ki je izdala potrdilo, pravilna. Če je služba pravilna, bo moral skrbnik sistema morda **uvoziti** potrdilo CA v prostor za potrdila *SYSTEM. Ali pa bo moral administrator s pomočjo naloge **Nastavitev statusa službe za potrdila** službo spremeniti v zaupanja vredno in tako odpraviti težavo.
5. Nimate potrdila, ki bi ga lahko registrirali. Če želite preveriti, ali to povzroča težavo, lahko v pregledovalniku preverite uporabniška potrdila.
6. Potrdilo, ki ga želite registrirati, je poteklo ali pa ni popolno. Če želite odpraviti težavo, morate obnoviti potrdilo ali se obrniti na službo za potrdila, ki je potrdilo izdala.
7. IBM-ov Strežnik HTTP ni pravilno nastavljen za registracijo potrdil z uporabo SSL in overjanje odjemalcev v zaščitenem primerku strežnika za upravljanje. Če ne deluje noben od predhodno navedenih nasvetov za odpravljanje težav, se obrnite na skrbnika sistema, ki vam bo pomagal sporočiti težavo.

Za **dodelitev uporabniškega potrdila** se morate povezati z Upravljalnikom digitalnih potrdil (DCM) prek seje SSL. Če pri izbiri naloge **Dodelitev uporabniškega potrdila** ne uporabite SSL, DCM prikaže sporočilo, da morate uporabljati SSL. Sporočilo vsebuje gumb, ki omogoča povezavo z DCM prek SSL. Če je sporočilo prikazano brez gumba, to sporočite skrbniku sistema. Za zagotovitev aktiviranja konfiguracijskih navodil za uporabo SSL boste najbrž morali znova zagnati spletni strežnik.

Poglavje 10. Z DCM povezane informacije

Ker je uporaba digitalnih potrdil vedno bolj razširjena, je na voljo tudi vedno več virov informacij. Sledi kratek seznam drugih virov, ki si jih ogledate, če se želite naučiti več o digitalnih potrdilih in njihovi uporabi za izboljšanje načel zaščite:

- **Spletno mesto službe za pomoč VeriSign**
  Spletno mesto VeriSign nudi obširno knjižnico iz področja digitalnih potrdil, pa tudi številne druge internetne varnostne vsebine.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Ta IBM-ova rdeča knjiga se osredotoča na izboljšave omrežne zaščite V5R1. Rdeča knjiga pokriva številne teme, vključno s tem, kako uporabiti možnosti za podpisovanje objektov, upravljalnik digitalnih potrdil, podporo šifrirnega koprocesorja 4758 za SSL in tako naprej.
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)**
  Ta rdeča knjiga opisuje, kaj lahko naredite z digitalnimi potrdili na vašem strežniku. Razlaga, kako nastaviti različne strežnike in odjemalce za uporabo potrdil in nudi informacije in vzorčno kodo za uporabo API-jev i5/OS za upravljanje in uporabo digitalnih potrdil v uporabniških aplikacijah.
- **Iskanje indeksov RFC**
  To spletno mesto nudi odlagališče RFC-jev (zahteve po komentarjih), po katerem je mogoče iskati. RFC-ji opisujejo standarde za internetne protokole, kot so SSL, PKIX in drugi, ki so povezani z uporabo digitalnih potrdil.

Dodatek. Opombe

Te informacije smo razvili za izdelke in storitve, ki jih ponujamo v Združenih državah Amerike.

IBM drugih izdelkov, storitev ali komponent, omenjenih v tem dokumentu, morda ne bo nudil v drugih državah. Podatke o izdelkih in storitvah, ki so trenutno na voljo v vašem področju, boste dobili pri lokalnem IBM-ovem predstavniku. Nobena referenca na IBM-ov izdelek, program ali storitev ne pomeni, da lahko uporabljate samo ta IBM-ov izdelek, program ali storitev. Namesto njih lahko uporabite katerikoli funkcionalno enakovreden izdelek, program ali storitev, ki ne krši IBM-ovih pravic intelektualne lastnine, vendar pa mora uporabnik sam oceniti in preveriti delovanje vseh izdelkov, programov ali storitev, ki niso IBM-ovi.

IBM ima lahko patente aplikacije ali za patent priglašene aplikacije, ki obsegajo predmet tega dokumenta. Imetje tega dokumenta vam ne daje nobene licence za te patente. Pisna vprašanja v zvezi z licencami lahko pošljete na naslednji naslov:

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

Za licenčna vprašanja v zvezi z naborom dvobajtnih znakov (DBCS) se obrnite na IBM-ov oddelek za intelektualno lastnino v svoji državi ali pa pošljite pisna vprašanja na naslednji naslov:

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

Naslednji odstavek ne velja za Veliko Britanijo ali za druge države, kjer takšni predpisi niso skladni z lokalnim zakonom: INTERNATIONAL BUSINESS MACHINES CORPORATION NUDI TO PUBLIKACIJO " TAKŠNO KOT JE", BREZ JAMSTEV KAKRŠNEKOLI VRSTE, PA NAJ BODO IZRECNA ALI POSREDNA, KAR VKLJUČUJE, VENDAR NI OMEJENO NA POSREDNA JAMSTVA NEKRŠENJA, TRŽNOSTI ALI PRIMERNOSTI ZA DOLOČEN NAMEN. V nekaterih državah ni dovoljena zavrnitev izrecnih ali posrednih jamstev v določenih transakcijah, zato ta izjava za vas morda ne velja.

Te informacije lahko vsebujejo tehnične ali tipografske napake. Informacije v tem dokumentu občasno spremenimo; te spremembe bomo vključili v nove izdaje publikacije. IBM lahko kadarkoli in brez obvestila izboljša in/ali spremeni izdelek(ke) in/ali program(e), opisane v tej publikaciji.

Vse reference v teh informacijah na spletne strani, ki niso IBM-ove, so podane zgolj zaradi priročnosti, in na noben način ne pomenijo, da uporabo teh spletnih strani odobravamo. Vsebina teh spletnih strani ni del vsebine tega IBM-ovega izdelka, zato te spletne strani uporabljate na lastno odgovornost.

| IBM lahko informacije, ki nam jih pošljete, uporablja ali razpečuje na kakršenkoli način, ki se mu zdi primeren, pri
| čemer nima do vas nobene odgovornosti.

Imetniki licenc za ta program, ki potrebujejo informacije, da bi omogočili: (i) izmenjavo informacij med neodvisno izdelanimi programi in drugimi programi (vključno s tem) in (ii) medsebojno uporabo izmenjanih informacij, naj se obrnejo na:

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

Rochester, MN 55901
U.S.A.

Takšne informacije bodo na voljo v skladu z določenimi pogoji in določbami, ki včasih zahtevajo tudi plačilo.

Licenčni program, opisan v teh informacijah, in vse licenčno gradivo, ki je na voljo zanj, nudi IBM v skladu z pogoji IBM-ove pogodbe s strankami, IBM-ove mednarodne licenčne pogodbe ali katerekoli enakovredne pogodbe med nami.

Vsi podatki o zmogljivosti, vsebovani tukaj, so bili določeni v nadzorovanem okolju, zato se lahko rezultati, dobljeni v drugih operacijskih okoljih, zelo razlikujejo. Nekatere meritve so bile opravljene v sistemih na razvojni stopnji in zato ne dajemo nobenega jamstva, da bodo te meritve enake tudi v splošno razpoložljivih sistemih. Prav tako so bile morda nekatere meritve ocenjene z ekstrapolacijo. Dejanski rezultati se lahko razlikujejo. Uporabniki tega dokumenta naj preverijo ustrezne podatke za njihovo okolje.

Vse izjave v zvezi z IBM-ovo bodočo usmeritvijo ali namenom lahko spremenimo ali umaknemo brez vsakega opozorila, in predstavljajo samo cilje in namene.

Te informacije vsebujejo zglede podatkov in poročil, uporabljenih v vsakodnevnih poslovnih operacijah. Da bi bili zgledi čim bolj nazorni, vključujejo imena posameznikov, podjetij, znamk in izdelkov. Vsa ta imena so izmišljena; vsaka podobnost z imeni in naslovi dejanskih poslovnih podjetij je zgolj naključna.

Prodajne znamke

Naslednji izrazi so blagovne znamke International Business Machines Corporation v Združenih državah Amerike, v drugih državah ali v obojih:

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

Lotus, Freelance in WordPro so blagovne znamke International Business Machines Corporation in Lotus Development Corporation v Združenih državah Amerike, v drugih državah ali v obojih.

Microsoft, Windows, Windows NTin logotip Windows so blagovne znamke Microsoft Corporation v Združenih državah Amerike, ostalih državah ali v obojih.

Druga imena podjetij, izdelkov in storitev so lahko blagovne ali storitvene znamke njihovih ustreznih lastnikov.

Določbe in pogoji za snemanje in tiskanje publikacij

Dovoljenja za uporabo publikacij, izbranih za snemanje, so podvržene naslednjim določbam in pogojem, ki jih morate sprejeti.

Osebna raba: Publikacije lahko reproducirate za osebno in nekomercialno rabo pod pogojem, da se ohranijo vse lastniške pravice. Teh publikacij ne smete distribuirati, prikazovati ali izdelovati izvlečkov brez izrecne odobritve IBM-a.

Komercialna uporaba: te publikacije lahko kopirate, razpečujete in prikazujete samo v vašem podjetju, pod pogojem, da ohranite vse oznake lastništva. Ustvarjanje izpeljanih del iz teh publikacij ali kopiranje, razpečevanje ali prikazovanje teh publikacij ali kateregakoli njihovega dela izven vašega podjetja ni dovoljeno brez izrecnega dovoljenja IBM-a.

Razen pravice, opisane tu, vam niso dodeljene nobene druge pravice, licence ali pooblastila, pa naj bodo posredna ali izrecna, za publikacije ali katerekoli informacije, podatke, programsko opremo ali drugo intelektualno lastnino, ki jo vsebujejo.

Pri IBM-u si pridržujemo pravico kadarkoli odvzeti dovoljenja, podeljena s tem dokumentom, če menimo, da uporaba publikacij škoduje našemu interesu ali če pri IBM-u ugotovimo, da zgornjih pravil ne upoštevate.

Te informacije lahko presnamete, izvozite ali znova izvozite samo s popolnim upoštevanjem vseh ustreznih zakonov in predpisov, vključno z vsemi ameriškimi zakoni in predpisi o izvozu. IBM NE JAMČI ZA VSEBINO TEH PUBLIKACIJ. PUBLIKACIJE SO NA VOLJO ″TAKŠNE KOT SO″, BREZ JAMSTEV KAKRŠNEKOLI VRSTE, PA NAJ BODO IZRECNA ALI POSREDNA, KAR VKLJUČUJE, VENDAR NI OMEJENO NA JAMSTVA TRŽNOSTI IN PRIMERNOSTI ZA DOLOČEN NAMEN.

Lastnik avtorskih pravic za vse gradivo je IBM Corporation.

S presnetjem ali natisom publikacije s te spletne strani soglašate s temi pogoji in določbami.

Natisnjeno na Danskem