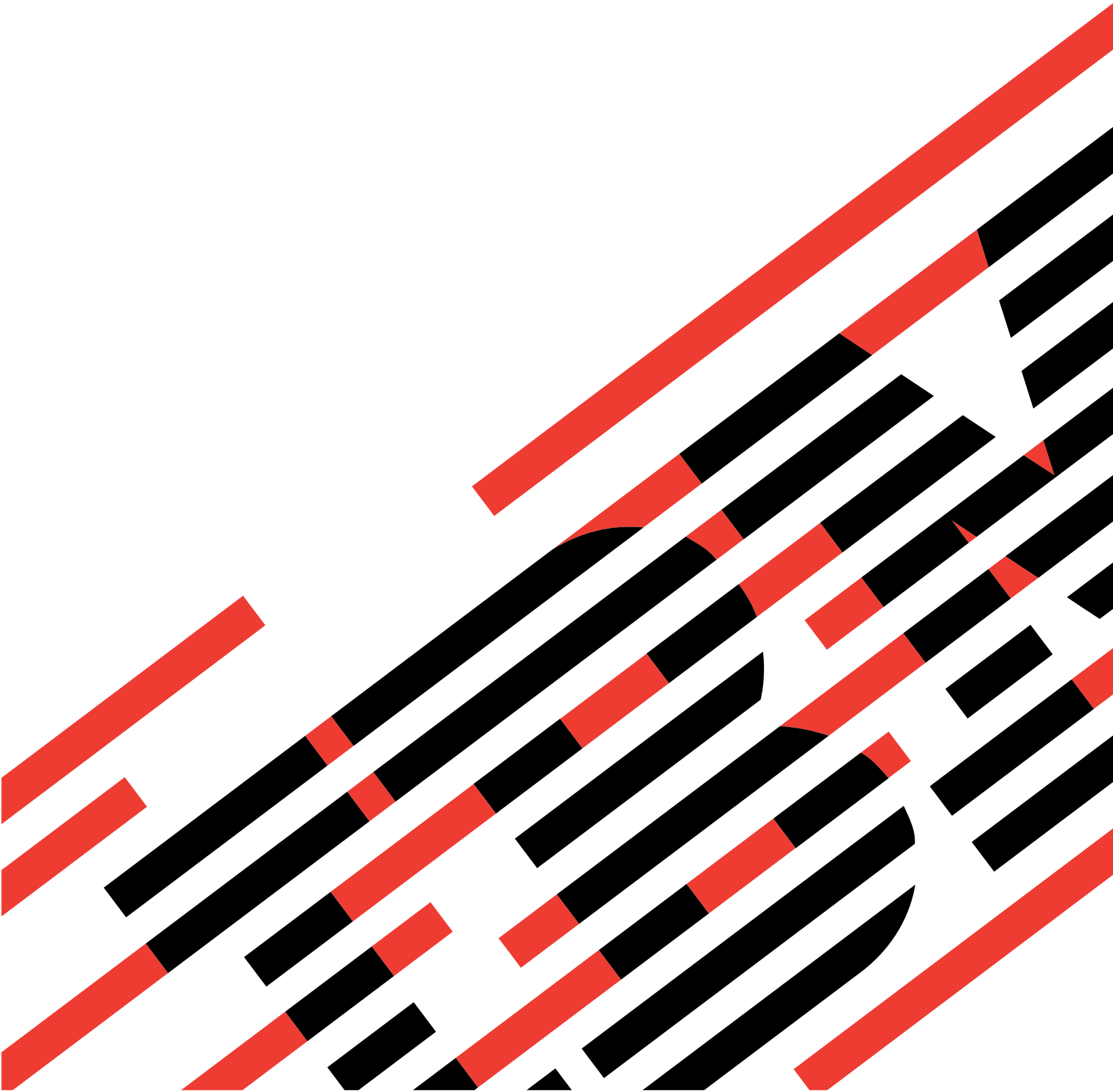
IBM

eserver

iSeries

Upravljalnik digitalnih potrdil



IBM

@server

iSeries

Upravljalnik digitalnih potrdil

Kazalo

Del 1. Digital Certificate Manager

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 iSeries, kot so FTP, Telnet, strežnik HTTP za iSeries in številne druge, nudijo podpodo SSL, ki zagotavlja zasebnost podatkov.

iSeries nudi obsežno podporo za digitalna potrdila, ki omogoča uporabo digitalnih potrdil kot priporočil v številnih zaščitnih 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, ki jo nudi iSeries za potrdila, je preprosto, če uporabljate Upravljalnik digitalnih potrdil (DCM) - brezplačno funkcijo iSeries, 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 pooblstila, s katero boste izdajali zasebna potrdila aplikcijam in uporabnikom v vaši organizaciji.

Za učinkovito izkoriščanje zaščite, ki jo nudijo potrdila, je potrebno pravilno načrtovanje in ocena. V teh temah se boste naučili, kako delujejo potrdila in kako lahko uporabite DCM za njihovo upravljanje in upravljanje aplikacij, ki potrdila uporabljajo.

Novosti za V5R2
S pomočjo teh informacij boste spoznali spremembe v komponenti Upravljalnika digitalnih potrdil ter spremembe v informativni temi za to izdajo.

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

Selitev v DCM iz zgodnješe izdaje
S pomočjo teh informacij boste spoznali, katere naloge boste morali izvesti, ter katere druge dejavnike morate upoštevati, če izvajate selitev iz zgodnejše različice DCM v tretnutno različico.

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 iSeries. 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 tiše potrdil ter možnosti njihove uporabe kot del začel o zaščiti.

Načrt za DCM
Te informacije vam bodo pomagale pri odločanju, kako in kdaj uporabiti digitalna potrdila, tako da bodo ustrezala vašim ciljem za zaščito. 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.

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

Poglavje 1. Novosti za V5R2

Izboljšave v Upravljalnik digitalnih potrdil (DCM) in zmožnostih digitalnih potrdil iSeries so naslednje:

- **Funkcija dodeljevanja potrdila**
  Ta nova naloga upravljalnika digitalnih potrdil omogoča, da hitreje in preprosteje dodelite potrdilo eni ali več aplikacijam. Do te naloge lahko dostopate s seznama nalog za **upravljalnje potrdil** ali s strani hitrih poti **Delo s strežnikom in potrdili** ter **Delo s potrdili za podpisovanje objektov**. Ta funkcija je na voljo le za prostore za potrdila *SYSTEM in *OBJECTSIGNING.
- **Objekti za podpisovanje ukazov (*CMD)**
  Upravljalnik digitalnih potrdil lahko zdaj uporabite za izdelavo digitalnih podpisov na objektih ukazov (*CMD), ki predstavljajo način za preverjanje njihove neokrnjenosti. Izberete lahko tudi področje podpisov za objekte *CMD; podpišete lahko celotni objekt *CMD ali pa podpišete le komponente jedra objekta. Če upravljalnik digitalnih potrdil uporabljate za prikaz podpisa na objektih *CMD, nudi DCM informacije o območju podpisa.
- **API-ji za izdelavo uporabniških potrdil, ki jih podpiše lokalna služba za pooblastila brez uporabe upravljalnika digitalnih potrdil**
  Na voljo sta dva nova API-ja, ki jih lahko uporabite za programsko izdajanje potrdil, ki jih lokalna služba za potrdila podpiše ne-iSeries uporabnikom. Ta API-ja omogočata izdajanje potrdil uporabnikom brez profilov uporabnikov iSeries ter brez zahteve, da bi morali uporabniki uporabiti upravljalnik digitalnih potrdil za pridobivanje potrdila za overjanje odjemalca.

Nove ali izboljšane informacije za to temo zajemajo:

- Dva nova scenarija, ki jih lahko uporabite za pomoč pri določanju, kako nabolje zaposliti potrdila za izpolnjevanje ciljev zaščite.
- Reorganizirane informacije, ki omogočajo hitrejše iskanje informacij, ki jih potrebujete za uporabo upravljalnika digitalnih potrdil.

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

Poglavje 2. Natisni to temo

Če si želite ogledati ali shraniti različico PDF, izberite Upravljalnik digitalnih potrdil  (velikost datoteke je približno 468 KB ali približno 110 strani).

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

1. V pregledovalniku odprite različico PDF (kliknite zgornjo povezavo).
2. Na meniju pregledovalnika kliknite **Datoteka**.
3. Kliknite **Shrani kot...**
4. Poiščite imenik, v katerega želite shraniti datoteko PDF.
5. Kliknite **Shrani**.

Če za pregledovanje ali tiskanje PDF-jev potrebujete program Adobe Acrobat Reader, lahko kopijo prenesete s spletne strani podjetja Adobe

(www.adobe.com/prodindex/acrobat/readstep.html)  .

Poglavje 3. Selitev iz zgodnješe različice DCM

Če selite Upravljalnik digitalnih potrdil (DCM) od različice V4R3 naprej v različico V5R2, Upravljalnik digitalnih potrdil samodejno nadgradi datoteke obstoječe lokalne službe za potrdila (CA) in sistemske datoteke obrača ključev potrdil. Te datoteke, ki se imenujejo default.kyr, nadgradi v ustrezne datoteke za shranjevanje ključev z imenom default.kdb. Upravljalnik digitalnih potrdil preseli tudi vsa veljavna potrdila v datotekah obroča ključev, povezana s strežniki HTTP (Hypertext Transfer Protocol) in LDAP (Lightweight Directory Access Protocol). Vsa veljavna potrdila preseli v prostor za potrdila *SYSTEM (default.kdb).

Opomba: Če izvajate selitev iz različice Upravljalnika digitalnih potrdil V4R4, V4R5 ali V5R1, ni potrebno opraviti nobenih selitvenih nalog, ker so datoteke potrdil iz teh različic združljive z različico Upravljalnika digitalnih potrdil V5R2.

Selitev iz obroča ključev v prostor za potrdila – selitev V4R3

Med namestitvijo DCM V5R2 preseli sistem naslednje datoteke obroča ključev:
- Privzete datoteke obroča ključev Upravljalnika digitalnih potrdil
- Obroče ključev, ki jih uporabljajo konfiguracijske datoteke strežnika HTTP
- Obroče ključev, ki jih uporabljajo konfiguracijske datoteke strežnika LDAP.

Če uporabljate datoteko .kyr, ki je Upravljalnik digitalnih potrdil ni nadgradil samodejno, jo ta pretvori v datoteko kyr.kdb, ko jo prvič uporabite v Upravljalniku digitalnih potrdil. Ko na primer prvič podate datoteko secure.kyr v uporabniškem vmesniku Upravljalnika digitalnih potrdil, Upravljalnik digitalnih potrdil pretvori datoteko v nov prostor za potrdila z imenom datoteke secure.kyr.kdb.

Opomba: Obroči ključev se razlikujejo od prostorov za potrdila, zato morate pretvoriti datoteke obroča ključev, ki jih Upravljalnik digitalnih potrdil ni nadgradil samodejno, tako da delate z njimi prek uporabniškega vmesnika DCM. Če spremenite pripone imen datotek v .kdb ročno, to pri kasnejšem delu s temi datotekami prek uporabniškega vmesnika DCM povzroči napako.

Če pri uporabi Upravljalnika digitalnih potrdil poskusite zbrisati datoteko secure.kyr, jo Upravljalnik digitalnih potrdil arhivira in zbriše datoteko secure.kyr.kdb.

Privzeto geslo prostora za potrdila

Če datoteka /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR obstaja, sistem preseli to datoteko obroča ključev in vse druge ustrezne datoteke obroča ključev v prostor za potrdila *SYSTEM. Izvorno geslo, povezano z datoteko /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR, je uporabljeno kot geslo prostora za potrdila *SYSTEM.

Če datoteka /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR ne obstaja, za selitev pa obstajajo druge ustrezne datoteke obroča ključev (na primer datoteke obroča ključev, ki jih uporabljajo konfiguracijske datoteke strežnika HTTP), sistem izdela prostor za potrdila *SYSTEM z geslom DEFAULT (same velike črke) in dokonča selitev.

Za informacije o napakah, do katerih lahko pride med postopkom selitve datotek in o možnih rešitvah preberite temo Napake pri selitvi in rešitve za obnovitev.

Poglavje 4. Scenariji DCM

Upravljalnik digitalnih potrdil ter podpora za digitalna potrdila, ki jo nudi vaš iSeries, omogočata, da s pomočjo potrdil izboljšate načela zaščite na številne različne načine. Izbira načina uporabe potrdil je odvisna od poslovnih ciljev ter potrebi 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). Za povezavo potrdila uporabnika z njegovim profilom uporabnika iSeries lahko uporabite tudi DCM. Potrdilo bo imelo enaka pooblastila in pravice kot z njim povezan profil.

Izbira načina uporabe potrdil je lahko zelo zapletena in je odvisna od številnih faktorjev. Scenariji v tej temi opisujejo nekatere od splošnejših ciljev zaščite z digitalnimi potrdili v tipičnem poslovnem okolju. Vsi scenariji opisujejo tudi vse potrebne sistemske in programske predpogoje ter vse konfiguracijske naloge, ki jih morate izvesti za izvedbo scenarija. 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 zaščito dostopa do javnih aplikacij ter sredstev
Ta scenarij opisuje, kdaj in kako uporabiti potrdila za zaščito in omejitev dostopa javnim uporabnikom do javnih ali ekstranetnih virov in aplikacij.

Scenarij: Uporaba potrdil za zaščito dostopa do internih aplikacij ter sredstev
Ta scenarij opisuje, kdaj in kako uporabiti potrdila za zaščito in omejitev dostopa notranjim uporabnikom do virov in aplikacij na notranjih strežnikih.

Scenarij: Uporaba potrdil za zaščito dostopa do javnih aplikacij ter sredstev

Situacija

Delate za zavarovalnico (MojaZav, d.o.o.) in ste odgovorni za vzdrževanje različnih aplikacij na intranetnih in ekstranetnih spletnih straneh vašega podjetja. Ena od aplikacij, za katero ste odgovorni, je aplikacija za izračunavanje obrokov, ki stotinam neodvisnim agentom omogoča, da izračunavajo obroke za svoje stranke. Ker so informacije, ki jih nudi ta aplikacija, občutljive, želite zagotoviti, da jo uporabljajo samo registrirani agenti. Ponuditi želite varnejšo metodo dostopa uporabnikov do aplikacij, kot je vaša trenutna metoda z imenom uporabnika ter geslom. Skrbi vas, da bi lahko nepooblaščeni uporabniki zajeli te informacije, ko se prenašajo prek neoverjenega omrežja. Prav tako bi različni posredniki lahko souporabljali te informacije, čeprav za to ne bi bili pooblaščeni.

Po kratki raziskavi ste odločite, da lahko uporaba digitalnih potrdil zagotovi potrebno zaščito. S pomočjo potrdil lahko uporabite plast zaščitenih vtičnic (SSL) za zaščito prenosa 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. V tem trenutku nameravate nadaljevati z uporabo metode overjanja z imenom uporabnika ter geslom, ker SSL ščiti zasebnost teh občutljivih podatkov med prenosom.

Na osnovi vrste aplikacije in njenih uporabnikov ter prihodnjega cilja overjanja potrdil za uporabnike, se odločite uporabiti javna potrdila zelo poznane službe za potrdila (CA), s katerimi boste konfigurirali SSL za vašo aplikacijo.

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 preverjanje pristnosti uporabnikov. Tudi kadar ni mogoče, je overjanje odjemalca na način z imenom uporabnika ter geslom zaščiteno in zasebno v seji SSL, s tem pa je izmenjava občutljivih podatkov bolj varna.
- Uporaba *javnih* digitalnih potrdil za omejitev ali dopustitev dostopa do aplikacij in podatkov je praktična odločitev v naslednjih ali podobnih pogojih:
  - Vaši podatki in aplikacije zahtevajo spremenljive stopnje zaščite.
  - Med overjenimi uporabniki je zelo gost promet.
  - Do aplikacij in podatkov ste omogočili javen dostop, kot na primer prek internetnega spletnega mesta ali ekstranetne aplikacije.
  - Ne želite voditi svoje lastne službe za potrdila (CA) zaradi velikega števila uporabnikov, ki dostopajo do aplikacij in sredstev, ali zaradi drugih upravnih razlogov.
- Uporaba javnega potrdila za konfiguriranje aplikacije izračuna obrokov za SSL v tem scenariju zmanjšuje količino konfiguracije, ki jo morajo uporabniki izvesti za dostop do aplikacije. Večina odjemalske programske opreme vsebuje potrdila CA za večino dobro znanih služb za potrdila.

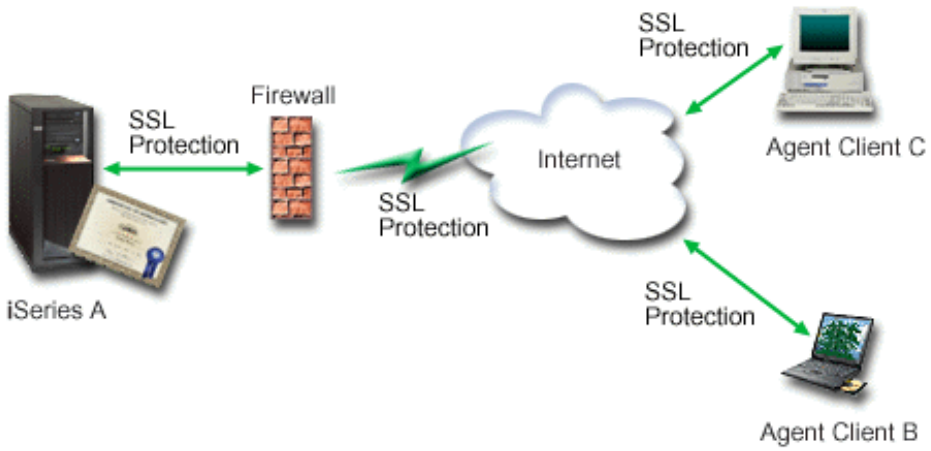
Cilji

V tem scenariju želi MojaZav, d.o.o., uporabiti digitalna potrdila za zaščito informacij o izračunu obrokov, ki jih njihvoa aplikacija nudi pooblaščenim javnim uporabnikom. Podjetje želite duti varnejšo metodo overjanja uporabnikov, ki jim je dovoljen dostop do te aplikacije.

Cilji tega scenarija so naslednji:
- Javna aplikacija podjetja za izračun obrokov mora uporabiti SSL za zaščito zasebnosti podatkov, ki jih nudi uporabnikom.
- 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. Posrednikom mora biti podano javno digitalno potrdilo zelo znane službe za potrdila (CA) ali pa veljavno ime uporabnika in geslo.

Podrobnosti

Naslednja slika kaže situacijo konfiguracijo omrežja za ta scenarij:



Slika zaže naslednje informacije o situaciji za ta scenarij:

Javni strežnik podjetja – iSeries A
- iSeries A je strežnik, ki gosti aplikacij podjetja za izračun obrokov.
- Na strežniku iSeries A teče OS/400 različica 5 izdaja 2 (V5R2).
- iSeries A ima nameščenega ponudnika šifriranega dostopa (5722–AC3).
- iSeries A ima nameščen in konfiguriran Upravljalnik digitalnih potrdil (OS/400 možnost 34) ter strežnik IBM HTTP Server za iSeries (5722–DG1).
- Na strežniku iSeries A se izvaja aplikacija za izračun obrokov, ki je konfigurirana, tako da:
  - Zahteva način SSL.
  - Uporablja javno potrdilo zelo znane službe za potrdila (CA) za konfiguracijo SSL.
  - Zahteva overjanje uporabnika z imenom uporabnika ter geslom.
- iSeries A predstavi svoje potrdilo za začetek seje SSL, ko odjemalca B in C dostopata do aplikacije.
- Po začetku seje SSL iSeries A zahteva, da odjemalca B in C podata veljavno ime uporabnika ter geslo, preden dovoli dostop do aplikacije za izračun obrokov.

Odjemalski sistemi posrednikov – Odjemalec B in odjemalec C
- Odjemalca B in C sta neodvisna posrednika, ki dostopata do aplikacije za izračun obrokov.
- Odjemalca B in C imata kopijo potrdil zelo znane službe za potrdila, ki je izdala potrdilo aplikacije, ki je nameščena v njihovi odjemalski programski opremi.
- Odjemalca B in C dostopata do aplikacije za izračun obrokov na strežniku iSeries A, ki predstavi svoje potrdilo njihovi odjemalski programski opremi, da preveri njihovo istovetnost ter začne sejo SSL.
- Odjemalska programska oprema na odjemalcih B in C je konfigurirana za sprejem potrdila iz strežnika iSeries A in seja SSL se začne.
- Po začetku seje SSL morata odjemalca B in C vnesti veljavno ime uporabnika ter geslo, preden iSeries A dodeli dostop do aplikacije.

Predpogoji in predpostavke

Ta scenarij je odvisen od naslednjih predpogojev ter predpostavk:
1. Aplikacija za izračun obrokov na iSeries A je generična aplikacija, ki jo je mogoče konfigurirati za uporabo SSL. Večina aplikacij, vključno z mnogo aplikacijami iSeries, nudi podporo SSL. Koraki konfiguracije SSL so zelo različni med aplikacijami, zato ta scenarij ne podaja podrobnih navodil za konfiguriranje aplikacije izračuna obrokov za uporabo 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. Ta scenarij nudi navodila, kako uporabiti upravljalnik digitalnih potrdil (DCM) za konfiguriranje overjanja potrdil za tiste aplikacije, ki nudijo to podporo. Ker so koraki konfiguracije za overjanje odjemalca zelo različni med aplikacijami, ta scenarij ne nudi specifičnih navodil za konfiguriranje overjanja odjemalca potrdila za aplikacijo izračuna obrokov.
3. iSeries A ustreza zahtevam za namestitev ter uporabo Upravljalnika digitalnih potrdil (DCM).
4. Na strežniku iSeries A ni predhodno nihče konfiguriral ali uporabljal DCM.
5. Kdorkoli uporablja upravljalnik digitalnih potrdil za izvajanje nalog v tem scenariju, mora imeti posebna pooblastila *SECADM in *ALLOBJ za njihov profil uporabnika.
6. iSeries A nima nameščenega šifrirnega koprocesorja IBM 4758-023 PCI.

Postopek opravila

Če želite izvesti ta scenarij, morate na strežniku iSeries A izvesti naslednje naloge:

1. Izpolniti vse predpogoje za namestitev in konfiguriranje vseh potrebnih izdelkov iSeries.
2. Uporabiti Upravljalnik digitalnih potrdil (DCM) za izdelavo zahteve potrdilo strežnika.
3. Konfigurirati vašo aplikacijo za uporabo plasti zaščitenih vtičnic (SSL).
4. Uporabiti DCM za uvoz in dodelitev podpisanega potrdila strežnika ali odjemalca ID-ju aplikacije za vašo aplikacijo.
5. Če je potrebno, zaženite aplikacijo v načinu SSL.
6. *Neobvezna naloga*: S pomočjo upravljalnika digitalnih potrdil definirajte seznam overjenih služb za potrdila, da omogočite overjanje odjemalcev na osnovi potrdil za aplikacije, ki nudijo to podporo.

   Opomba: Situacija, ki jo opisuje ta scenarij, ne zahteva, da aplikacija izračuna obrokov uporablja potrdila za overjanje odjemalcev. Številne aplikacije nudijo podporo za overjanje potrdil odjemalcev, način konfiguriranja te podpore pa se mnogo razlikuje med aplikacijami. Ta neobvezna naloga je navedena, da bo 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 konfigracije

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

Korak 1: Izpolnite predpogoje za namestitev vseh potrebnih izdelkov iSeries

Izpolniti morate vse naloge predpogojev za namestitev ter konfiguriranje vseh potrebnih izdelkov iSeries, preden lahko izvedete specifične konfiguracijske naloge za izvedbo tega scenarija.

Korak 2: Ustvarite zahtevo za potrdilo strežnika ali odjemalca

Če želite začeti postopek uporabe plasti zaščitenih vtičnih (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 boste dostopili 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 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.
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.

Korak 3: Konfigurirajte aplikacijo 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. Preden začnete delati z vašim podpisanim potrdilom, morate aplikacijo konfigurirati za uporabo SSL. Nekatere aplikacije, kot je strežnik HTTP za iSeries, generirajo unikatni ID aplikacije in ga registrirajo z upravljalnikom digitalnih potrdil, ko konfigurirate aplikacijo za uporabo SSL. 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 ne privzema specifičnega sredstva za aplikacijo izračuna obrokov, ki ga opisuje, ker lahko MojaZav, d.o.o., svojo aplikacijo ponudi posrednikom na številne načine.

Če želite aplikacijo konfigurirati za uporabo SSL, sledite navodilom, ki jih nudi dokumentacija vaše aplikacije. Prav tako lahko zveste več o konfiguriranju številnih splošnih IBM-ovih aplikacij za uporabo SSL, tako da pregledate temo Informacijskega centra, Varne aplikacije s SSL.

Korak 4: Uvozite in dodelite podpisano javno potrdilo

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 podali pri izdelavi 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 **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 boste dostopili 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 potrdilo in kliknite **Dodeli 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 5: Zaženite aplikacijo 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.

Neobvezni korak 6: Definirajte seznam overjenih služb za potrdila za aplikacijo, ki za overjanje odjemalca zahteva potrdila

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 izračuna obrokov uporablja potrdila za overjanje odjemalcev. Številne aplikacije nudijo podporo za overjanje potrdil odjemalcev, način konfiguriranja te podpore pa se mnogo razlikuje med aplikacijami. Ta neobvezna naloga je navedena, da bo 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 zadovoljenih nekaj 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 podali pri izdelavi 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 **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 boste dostopili do zaslonske pomoči.
6. S seznma izberite potrdilo službe za potrdila, ki naj mu zaupa vaša aplikacija, in kliknite **Omogoči**, da prikažete seznam aplikacij, ki uporabljajo seznam overjenih služb za potrdila.
7. S seznma izberite aplikacijo, ki ji na njen seznam želite dodati izbrano službo za potrdilo, 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 zaščito dostopa do internih aplikacij ter sredstev

Situacija

V podjetju (MojePod, d.o.o.) ste zaposlen kot skrbnik omrežja, 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 koristih ter zdravstvenem zavarovanju. Podjetje se je na to zahtevo odzvalo z izdelavo interne spletne strani, preko katere bo te informacije ponudilo zaposlenim. Vi ste odgovorni za upravljanje te interne spletne strani.

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. Za omejitev dostopa do podatkov podjetja uporabljate overjanje z imenom uporabnika ter geslom. Zaradi občutljive in zasebne narave podatkov ste spoznali, da omejevanje dostopa na osnovi gesel morda ni dovolj. Lahko se namreč zgodi, da uporabniki gesla souporabljajo, pozabijo ali celo ukradejo.

After some research, you decide that using digital certificates can provide you with the security that you need. 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 ste se odločili osnovati zasebno službo za potrdila (CA) in izdajati potrdila vsem uslužbencem ter povezati potrdila z njihovimi uporabniškimi profili iSeries. 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:
- Uporaba digitalnih potrdil za konfiguriranje dostopa SSL do spletnega strežnika kadrovske službe zagotavlja, da so informacije, prenesene med strežnikom in odjemalcem, zaščitene in zasebne.
- Uporaba digitalnih potrdil za overjanje odjemalcev nudi varnejšo metodo preverjanje pristnosti uporabnikov.
- Uporaba *zasebnih* digitalnih potrdil za omejitev ali dopustitev dostopa do aplikacij in podatkov je praktična odločitev v naslednjih ali podobnih pogojih:
  - Potrebujete visoko stopnjo zaščite, še posebej glede overjanja uporabnikov.
  - Posameznikom, ki jim izdate potrdila, zaupate.
  - Vaši uporabniki že imajo uporabniške profile iSeries za nadzorovanje dostopa do aplikacij in podatkov.
  - Želite voditi svojo lastno službo za potrdila (CA).
- Z uporabo zasebnih potrdil za overjanje odjemalec lahko preprosteje povežete potrdilo s profilom pooblaščenega uporabnika iSeries. Ta povezava potrdila s profilom uporabnika omogoča strežniku HTTP, da med overjanjem določi profil uporabnika lastnika potrdila. Strežnik HTTP ga lahko nato izmenja in se izvaja pod tem profilom uporabnika ali izvede dejanja za tega uporabnika na osnovi informacij v profilu uporabnika.

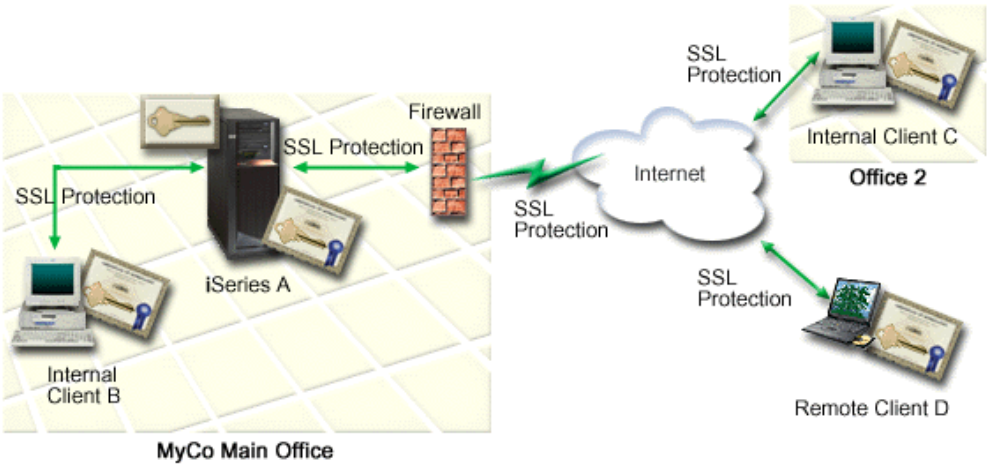
Cilji

V tem scenariju želi MojePod, d.o.o., uporabiti digitalna potrdila za zaščito občutljivih osebnih informacij, ki jih njihov interna spletna stran kadrovske službe nudi zaposlenim v podjetju. Podjetje želite duti varnejšo metodo overjanja uporabnikov, ki jim je dovoljen dostop do te spletne strani.

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

Podrobnosti

Naslednja slika kaže situacijo konfiguracijo omrežja za ta scenarij:



Slika zaže naslednje informacije o situaciji za ta scenarij:

Spletni strežnik kadrovske službe podjetja – iSeries A
- iSeries A je strežnik, ki gosti aplikacijo kadrovske službe podjetja, ki temelji na spletu
- Na strežniku iSeries A teče OS/400 različica 5 izdaja 2 (V5R2).
- iSeries A ima nameščenega ponudnika šifriranega dostopa (5722–AC3).
- iSeries A ima nameščen in konfiguriran Upravljalnik digitalnih potrdil (OS/400 možnost 34) ter strežnik IBM HTTP Server za iSeries (5722–DG1).
- Na strežniku iSeries A se izvaja aplikacija kadrovske službe, ki je konfigurirana, tako da:
  - Zahteva način SSL.
  - Uporablja zasebno potrdilo lokalne službe za potrdila (CA) za konfiguracijo SSL.
  - Zahteva potrdila za overjanje odjemalca.
- iSeries A predstavi svoje potrdilo za začetek seje SSL, ko odjemalci B, C in D dostopajo do aplikacije.
- Po začetku seje SSL iSeries A zahteva, da odjemalci B, C in D podajo veljavno potrdilo, preden dovoli dostop do aplikacije kadrovske službe. Ta izmenjava potrdil je transparentna uporabnikom odjemalcem B, C in D.

Odjemalski sistemi zaposlenih – odjemalec B, odjemalec C in odjemalec D
- Odjemalec B je zaposleni, ki dela v glavni pisarni MojePod, kjer se nahaja iSeries A.
- Odjemalec C je zaposleni, ki dela v sekundarni pisarni MojePod, ki je geografsko ločena od glavne pisarne.
- Odjemalec D je zaposleni, ki dela na daljavo in pogosto potuje po poslovnih poteh in mora varno dostopati do spletne strani kadrovske službe, ne glede na fizično nahajališče.
- 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 dostopajo do aplikacije kadrovske službe za sistemu iSeries A, ki predstavi svoje potrdilo njihovi odjemalski programski opremi, da preveri njihovo istovetnost ter začne sejo SSL.
- Odjemalska programska oprema na odjemalcih B, C in D je konfigurirana za sprejem potrdila iz strežnika iSeries A in seja SSL se začne.
- Po začetku seje SSL morajo odjemalci B, C in D podati veljavno potrdilo, preden iSeries A dodeli dostop do aplikacije in njenih virov.

Predpogoji in predpostavke

Ta scenarij je odvisen od naslednjih predpogojev ter predpostavk:

1. Strežnik IBM HTTP Server za iSeries izvaja aplikacijo kadrovske službe na iSeries A. Na voljo sta dve vrsti strežnika HTTP za iSeries (izvirni ter napajan z Apache), po objavi teh informacij pa bo na voljo znatno pregledana različica strežnika HTTP, zato ta scenarij ne podaja *podrobnih* informacij 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 nudi navodila, kako uporabiti upravljalnik digitalnih potrdil (DCM) za konfiguriranje zahtev upravljanja potrdil za ta scenarij, vendar ne nudi *podrobnih* konfiguracijskih korakov za konfiguriranje overjanja odjemalcev za strežnik HTTP.
3. Strežnik HTTP kadrovske službe na iSeries A že uporablja zaščito z gesli.
4. iSeries A ustreza zahtevam za namestitev ter uporabo Upravljalnika digitalnih potrdil (DCM).
5. Na strežniku iSeries A ni predhodno nihče konfiguriral ali uporabljal DCM.
6. Kdorkoli uporablja upravljalnik digitalnih potrdil za izvajanje nalog v tem scenariju, mora imeti posebna pooblastila *SECADM in *ALLOBJ za njihov profil uporabnika.
7. iSeries A nima nameščenega šifrirnega koprocesorja IBM 4758-023 PCI.

Postopek opravila

Za izvedbo tega scenarija morate dokončati dve skupini nalog: Ena skupina omogoča nastavitev aplikacije kadrovske službe na iSeries A za uporabo SSL in zahteva potrdila za overjanje uporabnika. Druga skupina nalog omogoča uporabnikom na odjemalcih B, C in D, da sodelujejo v sejah SSL z aplikacijo kadrovske službe in pridobijo potrdila za overjanje uporabnika.

Koraki nalog aplikacije spletnega strežnika kadrovske službe

Če želite izvesti ta scenarij, morate na strežniku iSeries A izvesti naslednje naloge:
1. Izpolniti vse predpogoje za namestitev in konfiguriranje vseh potrebnih izdelkov iSeries.
2. Konfigurirati vaš strežnik HTTP kadrovske službe, da bo uporabljal SSL, in zapisati opombo o ID-ju aplikacije za primerek strežnika.
3. Uporabite Upravljalnik digitalnih potrdil, da osnujete in vodite lokalno službo za potrdila, ter jo uporabite za izdajanje potrdil za strežnik HTTP kadrovske službe. Za vodena naloga tudi zagotavlja, da dodelite potrdilo aplikaciji spletnega strežnika, in dodate službo za pooblastila na seznam tistih, ki jim aplikacija zaupa.
4. Konfigurirajte spletni strežnik kadrovske službe, da zahteva potrdila za overjanje uporabnikov.
5. Zaženite strežnik HTTP kadrovske službe v načinu SSL.

Koraki nalog konfiguracije odjemalca

Za izvedbo tega scenarija, morajo vsi uporabniki (odjemalci B, C in D), ki bodo dostopali do spletnega strežnika kadrovske službe, na iSeries izvesti naslednje naloge:
6. Namestiti kopijo potrdila lokalne službe za pooblastila v svoje pregledovalnike.
7. Zahtevati potrdilo od lokalne služne za potrdila.

Podrobnosti konfigracije

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

Korak 1: Izpolnite predpogoje za namestitev vseh potrebnih izdelkov iSeries

Izpolniti morate vse naloge predpogojev za namestitev ter konfiguriranje vseh potrebnih izdelkov iSeries, preden lahko izvedete specifične konfiguracijske naloge za izvedbo tega scenarija.

Korak 2: Konfigurirajte strežnik HTTP kadrovske službe za uporabo SSL

Postopek konfiguracije SSL (plasti zaščitenih vtičnic) za strežnik HTTP kadrovske službe za iSeries A je lahko različen glede na to, ali uporabljate izvirno različico ali različico, napajano z Apache.

Če želite podrobnejše informacije o konfiguriranju strežnika HTTP (izvirnega) za uporabo SSL, preglejte Konfiguriranje varnega strežnika na strežniku HTTP.

Če želite podrobnejše informacije o konfiguriranju strežnika HTTP (napajan z Apache) za uporabo SSL, preglejte Scenarij: JKL omogoča zaščito s plastjo zaščitenih vtičnic (SSL) na svojih strežnikih HTTP (napajan z Apacke). Za scenarij nudi vse korake nalog za izdelavo navideznega gostitelja in njegovo konfiguriranje za uporabo SSL. Če želite podrobnejše korake za konfiguriranje SSL, preglejte naslov ″Omogoči SSL za navideznega gostitelja.″

Če želite dodatne informacije o konfiguriranju tako trenutne kot tudi prihodnih različic strežnika HTTP za iSeries (izvirnega in napajanega z Apache), preglejte temo Spletna strežba.

Korak 3: Osnujte in upravljajte lokalno službo 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. To zajema dodeljevanje potrdila, ki ga lokalna služba za potrdila izda aplikaciji spletnega strežnika. Prav tako lokalno službo za potrdila dodate na overjeni seznam služb za potrdila aplikacije spletnega strežnika. Ker je lokalna služba za potrdila na overjenem seznamu aplikacije, zagotavljate, da lahko aplikacija prepozna in overi uporabnike, ki predstavijo 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 boste dostopili do zaslonske pomoči.
3. Izpolnite obrazce vodenega opravila. Pri uporabi teh obrazcev za izvedbo vseh nalog, potrebnih za nastavitev lokalne službe za potrdila (CA), morate narediti naslednje:
   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 na tej točki, se naloga konča in morali boste izvesti ločene naloge za dokončanje konfiguracije potrdila SSL.

g. Izberite aplikacije, ki naj zaupajo lokalni službi za potrdila.

Opomba: Zagotovite, da izberete ID aplikacije za strežnik HTTP vaše kadrovske službe kot enega od aplikacij, ki zaupajo lokalni službi za potrdila.

Zdaj ste dokončali konfiguracijo potrdila, ki ga vaša aplikacija spletnega strežnika zahteva za uporabo SSL, in lahko nadaljujete s konfiguriranjem aplikacije spletnega strežnika, da zahteva potrdila za overjanje uporabnikov.

Korak 4: Konfigurirajte spletni strežnik kadrovske službe, da bo zahteval potrdila za overjanje odjemalcev

Postopek konfiguracije SSL (plasti zaščitenih vtičnic) za zahtevanje potrdil za overjanje odjemalcev za strežnik HTTP kadrovske službe na iSeries A je lahko različen glede na to, ali uporabljate izvirno različico ali različico, napajano z Apache.

Če želite podrobnejše informacije o konfiguriranju strežnika HTTP (izvirni) za zahtevanje potrdil za overjanje odjemalcev, preglejte Izdelava zaščitne nastavitve na strežniku HTTP (izvirnem) .

Če želite podrobnejše informacije o konfiguriranju strežnika HTTP (napajan z Apache) za uporabo potrdil za overjanje odjemalcev, preglejte Scenarij: JKL omogoča zaščito s plastjo zaščitenih vtičnic (SSL) na svojih strežnikih HTTP (napajan z Apacke). Za scenarij strežnika HTTP nudi vse korake nalog za izdelavo navideznega gostitelja in njegovo konfiguriranje za uporabo SSL in potrdila za overjanje odjemalcev. Če želite podrobnejše korake za konfiguriranje SSL in potrdil za overjanje odjemalcev, preglejte naslov ″Omogoči SSL za navideznega gostitelja.″

Če želite dodatne informacije o konfiguriranju tako trenutne kot tudi prihodnih različic strežnika HTTP za iSeries (izvirnega in napajanega z Apache), preglejte temo Spletna strežba.

Korak 5: Zaženite spletni strežnik kadrovske službe 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.

Za zaustavitev in zagon strežnika HTTP (izvirnega) uporabite obrazce Konfiguracija in upravljanje ter naredite naslednje:

1. Kliknite možnost **Upravljanje**.

2. Kliknite **Upravljanje strežnikov HTTP**.
3. Izberite strežnik.
4. V polje, ki je na voljo v obrazcu, vnesite izbirne parametre zagona.
5. Kliknite **Poženi**.

Opomba: Če se je med dodeljevanjem potrdila strežnik izvajal, morate strežnik zaustaviti in nato znova zagnati. S klikom na možnost **Ponovni zagon** vedno ne zagotovite, da strežnik lahko določi spremembe potrdila, ki so nastopile med izvajanjem.

Za zaustavitev in zagon strežnika HTTP (napajanega z Apache) uporabite obrazce Konfiguracija in upravljanje ter naredite naslednje:
1. Kliknite možnost **Upravljanje**.
2. Na levi strani menija kliknite **Upravljanje strežnikov** pod **Splošno upravljanje strežnika**.
3. Izberite strežnik, s katerim želite delati, nato pa kliknite **Zaženi** ali **Zaustavi**. Če želite podrobnejše informacije o zagonskih parametrih, preglejte zaslonsko pomoč.

Če želite dodatne informacije o upravljanju trenutne in prihodnjih različic strežnika HTTP za iSeries (izvirnega in napajanega z Apache), preglejte temo Spletna strežba.

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

Korak 6. Vsi uporabniki naj namestijo kopijo potrdila lokalne službe za potrdila v svojo programsko opremo pregledovalnikov.

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 internetne službe za potrdila, ima pregledovalnik ali programska oprema odjemalca že 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 boste zagotovili, da lahko pregledovalnik vzpostavi zaščitene komunikacijske seje 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**.

Korak 7: Vsi uporabniki naj zahtevajo potrdilo od lokalne službe za potrdila

V predhodnih korakih ste konfigurirali spletni strežnik kadrovske službe za zahtevanje potrdil za overjanje uporabnikov. Zdaj morajo uporabniki predstaviti veljavno potrdilo lokalne službe

za potrdila, preden jim je dovoljen dostop do spletnega strežnika. 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 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.

Poglavje 5. Pojmi digitalnih potrdil

Preden začnete uporabljati potrdila za izboljšanje zaščite sistema in omrežja, morate razumeti, kaj potrdila so in kakšne prednosti zaščite nudijo.

Digitalno potrdilo je digitalno priporočilo, ki preveri veljavnost identitete lastnika potrdila, podobno kot to naredi potni list. Pooblaščena stranka, imenovana služba za potrdila (CA), izdaja digitalna potrdila uporabnikom in aplikacijam strežnika ali odjemalca. Zaupanje v službo za potrdila predstavlja osnovo za zaupanje, da je potrdilo v resnici veljavno.

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

Razločevalno ime
V tej temi se boste naučili več o značilnostih 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
V tej temi boste zvedeli več o zaščitnih ključih, ki so povezani z digitalnimi potrdili.

Služba za pooblastila (CA)
V tej temi se boste naučili več o službah za potrdila, enotah, ki izdajajo digitalna potrdila.

Mesta 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.

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

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 nameravate sprejemati in uporabljati potrdila kot priporočila, preglejte identifikacijske zahteve službe za potrdila in se odločite, ali njihove zahteve ustrezajo vašim potrebam za zaščito.

Razločevalno ime (DN) je izraz, ki opisuje identifikacijske informacije lastnika potrdila in je del samega potrdila. 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
- mesto
- država
- področje

Če z Upravljalnikom digitalnih potrdil izdajate zasebna potrdila, lahko podate dodatne informacije razločevalnega imena za potrdilo, ki vključujejo naslednje:
- naslov IP različice 4
- celotno ime domene
- naslov elektronske pošte

Te dodatne informacije so koristne, če nameravate uporabljati potrdilo za konfiguriranje povezave navideznega zasebnega omrežja (VPN).

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 povezavo identitete 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 iSeries, ki jo želi razpošiljati prek interneta, kar je primeren in stroškovno ugoden način za njegove stranke. Razvijalec ve, da stranke upravičeno skrbi prenos programov prek interneta, predvsem zaradi naraščajočih težav z objekti, ki je 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 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 nati 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) omogoča upravljanje potrdil javnih in zasebnih CA-jev.

Poleg tega lahko uporabite DCM za vodenje zasebne službe za potrdila, ki bo izdajala zasebna potrdila za sisteme in uporabnike. Ko CA izda uporabniško potrdilo, ga DCM samodejno poveže s profilom uporabnika sistema iSeries. 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 overjeni status potrdila službe za potrdila v prostoru 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

Ko izdelate službo za potrdila (CA) z Upravljalnikom digitalnih potrdil, lahko podate podatke o načelih za CA. Podatki o načelih službe za potrdila opisujejo pravice za podpis, ki jih ima. Podatki o načelih določajo:

- ali lahko služba za potrdila izdaja in podpisuje uporabniška potrdila in
- obdobje veljavnosti potrdil, ki jih CA izda.

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 ažuriraje svoje sezname in omogočijo, da jih uporabniki objavijo v imenikih LDAP (Directory Access Protocol). Nekatere službe za pordila, 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 hrani tudi zasebni ključ potrdila, razen v primeru, da namesto tega za hrambo uporabite šifrirni koprocesor 4758. Upravljalnik digitalnih potrdil omogoča izdelavo in upravljanje številnih prostorov za potrdila. DCM krmili dostop do prostorov za potrdila prek gesel v povezavi s krmiljenjem dostopa imenika integriranega datotečnega sistema ter datotek IFS, 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)
Upravljalnik digitalnih potrdil uporablja ta prostor za potrdila za shranjevanje potrdila lokalne službe za potrdila in njegovega zasebnega ključa. Potrdilo iz tega prostora za potrdila lahko uporabite za podpisovanje potrdil, ki jih izda lokalna služba za potrdila. Če lokalna služba za potrdila izda potrdilo, shrani Upravljalnik digitalnih potrdil kopijo potrdila (brez zasebnega kljuač) v ustrezen prostor za potrdila (na primer *SYSTEM) za namene overjanja. 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). Aplikacije IBM iSeries (in aplikacije številnih drugih razvijalcev programske opreme) so napisane samo za uporabo potrdil v prostoru za potrdila *SYSTEM. Če za izdelavo lokalne službe za pooblastila uporabite DCM, DCM izdela ta prostor za potrdila kot del postopka. Če se odločite za pridobitev potrdil od javne službe za pooblstila, 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 pooblastila uporabite DCM, DCM izdela ta prostor za potrdila kot del postopka. Če se odločite za pridobitev potrdil od javne službe za pooblstila, 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 imate na strežniku iSeries nameščen šifrirani koprocesor 4758 PCI, lahko za vaša potrdila izberete tudi druge možnosti za shranitev zasebnih ključev (izjema so potrdila za podpis 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. Stranka ima par ključev, ki je sestavljen iz javnega in zasebnega ključa. Javni ključ se prosto pošilja, običajno znotraj digitalnega potrdila, zasebni ključ pa varno hrani lastnik. 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 s 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.

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.

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.

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 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 iSeries, 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 OS/400. To je funkcija DCM, ki temelji na pregledovalniku.
- Namestite strežnik IBM HTTP Server za iSeries (5722–DG1) in zaženite primerek strežnika *ADMIN.
- Zagotovite, da je za vaš sistem konfiguriran TCP, da boste lahko za dostop do Upravljalnika digitalnih potrdil uporabljali spletni pregledovalnik in primerek *ADMIN strežnika HTTP.

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.

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. Služba za potrdila, ki jo izdelate 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 objekta, morate imeti tudi kopijo potrdila službe za pooblastila za službo za pooblastila, ki je izdala potrdilo.

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. Potrdilo lahko uporabite za podpisovanje številnih objektov, vključno z večino objektov v integriranem datotečnem sistemu (IFS) ter objekti *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 iSeries. S pomočjo Upravljalnika digitalnih potrdil lahko tudi povežete uporabniška potrdila, ki jih izda kakšna druga služba za potrdila, s profilom uporabnika iSeries.

Če za upravljanje potrdil uporabite Upravljalnik digitalnih potrdil (DCM), le-ta uredi potrdila po teh klasifikacijah in jih skupaj z njimi povezanimi zasebnimi ključi shrani v prostor za potrdila.

Opomba: Če imate na strežniku iSeries nameščen šifrirni koprocesor IBM 4758 PCI, lahko za vaša potrdila izberete tudi druge možnosti za shranitev zasebnih ključev (izjema so potrdila za podpis 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. 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 za uporabo potrdil, morate izbrati izvedbo potrdil, ki se najbolj ujema z vašimi potrebami glede zaščite. Možnosti, ki so na voljo za pridobitev potrdil, vključujejo naslednje:

- nakup potrdila javne internetne službe za potrdila (CA)
- vodenje lastne službe za potrdila, ki bo izdajala zasebna potrdila za uporabnike in aplikacije
- kombinacija potrdil javnih internetnih služb za potrdila in lastne 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. Preden se odločite, da boste uporabljali potrdila določene službe za potrdila ali zaupali potrdilom, ki jih izdaja, ocenite, ali strogost njenih identifikacijskih načel ustreza vašim zahtevam za zaščito. Ker so se standardi PKIX (Public Key Infrastructure) za X.509 razvili, nekaj novejših javnih služb za potrdila nudi veliko strožje 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 boste izdali potrdila manjšemu številu strežniških ali odjemalskih aplikacij in uporabnikov, potem cena najbrž ne bo bistvenega pomena. Toda cena postane še kako pomembna, če imate veliko *zasebnih* uporabnikov, ki potrebujejo javna potrdila za overjanje odjemalca. V tem primeru razmislite o času, ki ga je potrebno vložiti za upravljanje in programiranje pri konfiguriranju aplikacij strežnika, tako da bodo sprejemale samo določen podniz 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. Tudi številna podjetja in uporabniki bodo prepoznali potrdila znane službe za potrdila in jim zaupali bolj kot tistim, ki jih izda vaša zasebna 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. Osnovanje in vzdrževanje lastne službe za potrdila omogoča, da potrdila izdate le tistim uporabnikom, ki so zaupanja vredni člani vaše skupine. 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 lokalno službo za pooblastila uporabljate za izdajanje potrdil uporabnikom za overjanje odjemalcev. se morate odločiti ali želite, da so potrdila uporabnikov povezana s profili uporabnikov iSeries. Uporabnikom lahko dovolite, da si pridobijo svoja potrdila od lokalne službe za pooblastila prek upravljalnika digitalnih potrdil, če želite, da so njihova potrdila povezana s profilom uporabnika iSeries. Začenši v V5R2 lahko uporabite API-je za programsko izdajanje potrdil uporabnikom, ki niso iSeries, tako da uporabniki nimajo profilov uporabnikov iSeries za uporabo zasebnih potrdil za overjanje odjemalca.

Opomba: Ne glede na to, katero službo za potrdila uporabite za izdajanje potrdil, skrbnik sistema nadzoruje, katerim službam naj zaupajo 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. Toda če to potrdilo službe za potrdila ni v prostoru za potrdila *SYSTEM, strežnik ne more zaupati uporabniškim ali odjemalskim potrdilom, ki jih je izdala ta služba za potrdila. Da bi zaupali uporabniškim potrdilom, ki jih je izdala služba za potrdila, morate pridobiti kopijo potrdila. Le-ta mora uporabljati pravilno datotečno obliko, vi pa morate dodati to potrdilo v prostor za potrdila Upravljalnika digitalnih potrdil.

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.

- Osnovanje in vodenje zasebne službe za potrdila opisuje naloge, ki jih morate opraviti, če se boste odločili za vodenje službe za izdajanje zasebnih potrdil.
- 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 na drugih strežnikih iSeries opisuje naloge, ki jih morate opraviti, 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 identiteto strežnika s kopijo potrdila izdajne 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 uporablja med usklajevanjem SSL algoritme asimetričnega ključa (javni ključ), s katerimi se dogovori za simetričen ključ, ki je nato uporabljen za šifriranje in dešifriranje podatkov aplikacije za določeno 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. Za povezavo potrdila uporabnika s profilom uporabnika iSeries lahko uporabite Upravljalnik digitalnih potrdil (DCM). Potrdilo bo imelo enaka pooblastila in pravice kot z njim povezan profil. Začenši v V5R2 lahko uporabite API-je za programsko uporabo vaše zasebne lokalne službe za pooblastila za izdajanje potrdil uporabnikom, ki niso iSeries. S temi API-ji lahko izdajate zasebna pooblastila uporabnikom, če ne želite, da bi ti uporabniki imeli profil uporabnika iSeries.

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 iSeries nudijo podporo za potrdilo za overjanje odjemalca:
- strežnik Telnet
- IBM HTTP Server (izvirnik in napajan z Apache)
- strežnik imeniških storitev (LDAP)
- Osrednje upravljanje
- Client Access Express (vključno z Navigatorjem iSeries)
- strežnik FTP

Čez čas bodo dodatne aplikacije morda nudije 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 naučiti več o konfiguriranju aplikacij strežnika iSeries za uporabo potrdil za overjanje odjemalca med sejo SSL, preberite Zaščita aplikacij s SSL.

Digitalna potrdila za povezave VPN

Digitalna potrdila lahko uporabite kot načine za vzpostavljanje povezave navideznega zasebnega omrežja (VPN) iSeries. 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.

Pred V5R1 so se strežniki IKE lahko medsebojno overjali samo s pomočjo ključev z vnaprej določeno skupno rabo. Uporaba ključa z vnaprej določeno skupno rabo je manj varna, saj morate ta ključ ročno posredovati skrbniku na drugi strani povezave VPN. 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 za izdajanje potrdil uporabite zasebno službo za potrdila pomožnega programa DCM, lahko za potrdilo podate informacije o drugem imenu predmeta. S podajanjem teh informacij zagotovite, da je povezava VPN iSeries 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 Upravljanik 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

Začenši z V5R1 nudi OS/400 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 iSeries 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 ugotovite, da uporaba digitalnih podpisov ustreza vašim potrebam in načelom zaščite, se odločite, ali boste uporabljali javna potrdila ali izdajali zasebna potrdila. Če nameravate posredovati objekte javnim uporabnikom, razmislite o uporabi potrdil znanih služb 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). S pomočjo Upravljalnika digitalnih potrdil (DCM) lahko upravljate potrdila, ki jih uporabljate za podpisovanje objektov in za preverjanje podpisov objektov. DCM lahko uporabite tudi za podpisovanje objektov ter preverjanje podpisov objektov.

Digitalna potrdila za preverjanje podpisov objekta

Začenši v V5R1 nudi sistem iSeries podporo za uporabo potrdil za preverjanje 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. Ko izberete, da boste zaupali službi za potrdila, lahko izberete, da boste zaupali podpisom, ki jih nekdo izdela, z uporabo potrdila, ki ga je izdala overjena služba za potrdila. 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 krmilite s sistemsko vrednostjo QVFYOBJRST. 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 jih obnavljate, ne pa tudi na varnostne datoteke ali datoteke IFS. Če se želite spoznati več o uporabi te in drugih sistemskih vrednosti, v Informacijskem centru poiščite temo System Value Finder.

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 usmerjenje, 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 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. Tudi kategorija in število nalog, prikazanih v oknu za usmerjanje, se spreminja glede na pooblastila, ki jih ima vaš profil uporabnika iSeries. 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 iSeries. 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 iSeries.

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 več poučnih informacij o uporabi digitalnih potrdil v internetnem okolju za izboljšanje zaščite sistema in omrežja, si oglejte spletno stran podjetja VeriSign. Tu boste našli obsežno knjižnico s temami o digitalnih potrdilih, kot tudi s številnimi drugimi temami o zaščiti na internetu. Dostopite lahko do njihove knjižnice na naslovu Službe 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 Upavljalnika 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 Upravljalnik digitalnih potrdil V5R2 uporablja za generiarnje para javnega in zasebnega ključa za potrdila, za šifriranje izvoženih datotek potrdil in za dešifriranje uvoženih datotek potrdil.

2. Z uporabo Navigatorja iSeries zaženite primerek strežnika HTTP Server *ADMIN:
   a. Zaženite Navigator **iSeries**.
   b. V glavnem drevesnem prikazu dvokliknite vaš strežnik iSeries.
   c. Dvokliknite **Omrežje**.
   d. Dvokliknite **Strežniki**.
   e. Dvokliknite **TCP/IP**.
   f. Z desnim gumbom miške kliknite **Upravljanje HTTP**.
   g. Kliknite **Poženi**.
3. Zaženite spletni pregledovalnik.
4. S pomočjo pregledovalnika odprite stran Naloge iSeries na naslovu http://*ime_vašega_sistema*:2001.
5. S seznama izdelkov na strani Naloge iSeries izberite **Upravljalnik digitalnih potrdil**, da boste dostopili do njega.

Če izvajate selitev iz starejše različica Upravljalnika digitalnih potrdil, boste na tej strani našli podrobnejše informacije za nadgraditev sistema.

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. Katere naloge so na voljo, je odvisno od tega, kateri prostor za potrdila imate odprt (če sploh katerega) in od pooblastila profila uporabnika. Večina nalog je na voljo, samo če imate posebni pooblastili *ALLOBJ in *SECADM.

Pri prvi uporabi Upravljalnika digitalnih potrdil (DCM) na obstaja noben prostor na potrdila (razen če niste opravili selitve iz prejšnje različice DCM). Če imate potrebna pooblastila, so posledično v oknu za usmerjanje prikazane samo naslednje naloge:

- Upravljanje uporabniških potrdil
- Izdelava novega prostora za potrdila
- Osnovanje službe za potrdila (CA) (Opomba: Ko to nalogo uporabite za osnovanje zasebne službe za potrdila, naloga ne bo več prikazana na seznamu.)
- Upravljanje mest CRL
- Upravljanje mest zahtev PKIX

Tudi če prostori za potrdila že obstajajo v vašem sistemu (če na primer izvajate selitev iz predhodne različice DCM), DCM v levem oknu za usmerjanje prikaže samo omejeno število nalog ali kategorij nalog. 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 odprete drugo okno pregledovalnika in s pomočjo 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 uporabljati potrdila s spletnim strežnikom IBM HTTP Server za iSeries, morate izdelati in konfigurirati spletni strežnik, preden začnete delati z Upravljalnikom digitalnih potrdil. Ko konfigurirate spletni strežnik za SSL, se izdela ID aplikacije za strežnik. Zapišite si ta ID aplikacije, da boste z Upravljalnikom digitalnih potrdil lahko podali, katero potrdilo naj ta aplikacija uporabi za SSL.

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

Takole z Upravljalnikom digitalnih potrdil izdelate in vodite lokalno službo za potrdila:

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 boste dostopili 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 vključen le, če imate v sistemu iSeries nameščen šifrirni koprocesor IBM 4758–023 PCI. 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 imate v sistemu iSeries nameščen šifrini koprocesor IBM 4758–023 PCI, ta podnaloga omogoča, da izberete, kako boste shranili zasebni ključ potrdila 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 naj zaupajo vaši lokalni službi za pooblastila.

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, da ga lahko njegova odjemalska programska oprema uporabi za overjanje identitete strežnika kot del postopka 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 strežnik uporablja potrdilo javne službe za potrdila, programska oprema uporabnikov že vsebuje 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
Te informacije vam bodo pomagale razumeti, kako povezati potrdilo, katerega lastnik ste, z vašim profilom uporabnika. Potrdilo lahko izda zasebna lokalna služba za pooblastila na drugem sistemu ali javna dobro znana internetna služba za pooblastila. Preden lahko profilu uporabnika dodelite potrdilo, mora strežnik zaupati službi za potrdila, potrdilo pa še ne sme biti povezano s profilom uporabnika v sistemu.

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.

Takole pridobite potrdilo lokalne službe za 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, 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: Če želite za overjanje uporabnikov uporabiti digitalna potrdila, morajo imeti uporabniki potrdila. Če morajo vaši uporabniki predložiti potrdila javne internetne službe za potrdila (CA), lahko s pomočjo Upravljalnika digitalnih potrdil (DCM) dodelijo potrdila svojim profilom uporabnikov. To vam in vašim uporabnikom omogoča uporabo DCM za upravljanje potrdil.

Za uporabo naloge **Dodeli uporabniško potrdilo** morate imeti zaščiteno sejo s strežnikom HTTP, prek katere boste dostopili do Upravljalnika digitalnih potrdil (DCM). 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.

Ko izberete to nalogo, se prikaže novo okno pregledovalnika. Če vaša seja ni zaščitena, vas Upravljalnik digitalnih potrdil pozove, da kliknete možnost **Dodeli uporabiško potrdilo** in jo s tem zaženete. Upravljalnik digitalnih potrdil nato začne pogajanja plasti zaščitenih vtičnic (SSL) s pregledovalnikom.

Kot del teh pogajanj vas lahko pregledovalnik vpraša, ali naj zaupa službi za potrdila (CA), ki je izdala potrdilo, ki določa strežnik HTTP. Tudi pregledovalnik vas lahko vpraša, ali naj sprejme potrdilo strežnika.

Ko omogočite pregledovalniku, da zaupa službi za potrdila in sprejmete potrdilo strežnika, lahko strežnik zahteva, da predložite 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.

Ko vzpostavite zaščiteno sejo, Upravljalnik digitalnih potrdil poskusi pridobiti ustrezno potrdilo iz pregledovalnika, da ga lahko poveže z vašim profilom uporabnika. Če mu uspe pridobiti enega 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 iz potrdila, niste predložili potrdila, ki bi ga Upravljalnik digitalnih potrdil lahko dodelil profilu uporabnika. Za to je lahko kriva ena od številnih težav z uporabniškimi potrdili. Tako so lahko na primer potrdila, ki jih vsebuje pregledovalnik, že povezana z vašim profilom uporabnika.

Če želite za izdajanje potrdil uporabnikom uporabljati lokalno službo za potrdila, morajo uporabniki izdelati uporabniško potrdilo.

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 predhodnjih 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 upravljalnika 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 za velikemu številu uporabnikov, še posebej, kadar želite, da ti uporabniki nimajo svojega profila uporabnika iSeries. Da bi se izognili nudenju uporabniških profilov tem uporabnikom, bi morali zahtevati, da uporabniki plačajo za potrdilo pri dobro znani službi za pooblastilo, če bi želeli zahtevati potrdila za overjanje uporabnikov v vaših aplikacijah.

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.

Na voljo sta dva API-ja, za vsakega od prevladujočih spletnih pregledovalnikov po eden, ki jih lahko pokličete, če uporabljate Net.Data za izdelavo programa, ki izdaja potrdila 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 generiranje in podpisovanje zahteva 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 proogramska 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, ima vaš pregledovalnik ali programska oprema odjemalca že 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 dokažete svojo pristnost s predložitvijo potrdila lokalne službe za potrdila, prenesite potrdilo lokalne službe za potrdila v pregledovalnik, preden zahtevate uporabniško potrdilo lokalne službe za potrdila.

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. Denimo, da upravljate javno spletno mesto in želite uporabiti plast zaščitenih vtičnic (SSL) za zaščitene komunikacijske seje, s katerimi boste zagotovili zasebnost pri transakcijah določenih informacij. Ker je spletno mesto javno razpoložljivo, želite uporabljati potrdila, ki jih večina spletnih pregledovalnikov prepozna brez težav.

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 ptodril 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 Upravljalnika 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 boste dostopili 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 imate v sistemu iSeries nameščen IBM-ov 4758–023 šifrirni koprocesor PCI, Upravljalnik digitalnih potrdil omogoči, da izberete, kako boste shranili zasebni ključ 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: Za uporabo potrdil s strežnikom HTTP za iSeries izdelajte in konfigurirajte spletni strežnik, preden začnete z Upravljalnikom digitalnih potrdil delati s podpisanim in dokončanim potrdilom. Ko konfigurirate spletni strežnik za SSL, se izdela ID aplikacije za strežnik. Zapišite si ta ID aplikacije, da boste z DCM lahko podali, katero potrdilo naj ta aplikacija uporabi za SSL.

   Strežnika ne zaustavite in znova zaženite, dokler z Upravljalnikom digitalnih potrdil ne dodelite podpisanega in dokončanega potrdila strežniku. Če zaustavite in znova zaženete primerek *ADMIN spletnega strežnika, preden mu dodelite potrdilo, se strežnik ne bo zagnal, vi pa ne boste mogli uporabiti Upravljalnika digitalnih potrdil za dodelitev potrdila strežniku.
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 uvozite potrdilo, lahko podate aplikacije, ki ga bodo uporabljale 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 morajo uporabniki pridobiti potrdilo službe za potrdila, naj dostopijo do spletnega mesta službe za potrdila in sledijo navodilom na strani.

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 Upravljalnika 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, dokončajte naslednje naloge:

1. Zaženite DCM.
2. V levem oknu 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 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 boste dostopili 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 **Izberi prostor za potrdila**, nato pa za odpiranje izberite prostor za potrdila ***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 se levo okno za usmerjanje osveži, izberite **Upravljanje aplikacij**, da boste prikazali 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 dokončate 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 poslati kot del paketa podpisanih objektov.

Prejemnik mora imeti tudi kopijo potrdila službe, ki je izdala potrdilo, uporabljeno za podpis objekta. Če ste podpisali objekte s potrdilom znane internetne službe za potrdila, bo prejemnikova različica Upravljalnika digitalnih potrdil najbrž že vsebovala kopijo potrebnega potrdila. Če menite, da prejemnik nima kopije, jo pošljite skupaj s podpisanimi objekti. Kopijo potrdila lokalne službe za pooblastila morate na primer poslati, če ste podpisali objekte s potrdilom zasebne lokalne službe za potrdila. Zaradi varnostnih razlogov pošljite potrdilo v ločenem paketu ali poskrbite, da bo javno na voljo za tiste, ki ga potrebujejo.

Upravljanje potrdil za preverjenje 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 prostosra 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 oknu Upravljalnika digitalnih potrdil izberite **Izdelaj nov prostor za potrdila**, s čimer boste zagnali vodeno nalogo, v kateri boste izpolnili niz obrazcev.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca v tej vodeni nalogi, izberite vprašaj (**?**) na vrhu strani, da boste dostopili 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 uporabljati obstoječa potrdila za podpisovanje objektov za preverjanje podpisov, 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 v ta prostor za potrdila izvozite iz prostora za potrdila *OBJECTSIGNING. Če jih ne izvozite, ne boste mogli preveriti veljavnosti podpisov, ki jih izdelate z njimi.

   Opomba: Če ste ta prostor za potrdila izdelali tako, da lahko preverjate podpise na objektih, ki jih prejmete iz drugih izvorov, nadaljujte s tem postopkom, da boste lahko uvozili 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*. Če potrdila službe za potrdila ne uvozite preden uvozite potrdilo za preverjanje podpisa, lahko pride do napake.

Zdaj lahko s temi potrdili preverite veljavnost podpisov objektov.

Poglavje 8. Upravljanje DCM

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

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

Upravljalnje aplikacij v upravljalniku digitalnih potrdil
Spoznajte, kako uporabljaati 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.

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.

Shranjevanje ključev potrdil v šifrirni koprocesor IBM 4758
Spoznajte, kako uporabljati nameščeni koprocesor za nudenje varnejše hrambe 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).

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 v sistemu iSeries v omrežju že uporabljate zasebno lokalno službo za potrdila (CA), zdaj pa želite razširiti njeno uporabo tudi na druge sisteme iSeries v omrežju. Želite na primer, da trenutna lokalna služba za potrdila izda potrdilo strežnika ali odjemalca za aplikacijo v drugem sistemu iSeries, 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 v drugem strežniku iSeries.

To nalogo lahko opravite z Upravljalnikom digitalnih potrdil. Nekatere naloge opravite v sistemu iSeries, v katerem vodite lokalno službo za potrdila, druge pa v sekundarnem sistemu iSeries, 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 sistem iSeries, v katerem vodite lokalno službo za potrdila, uporablja ponudnika šifriranega dostopa, ki nudi boljše šifriranje kot ciljni sistem, pride do težave. (Za V5R2 je edini razpoložljivi ponudnik šifriranega dostopa 5722–AC3, ki je trenutno najmočnejši izdelek, ki je na voljo. V predhodnih izdajah ste lahko namestili druge, šibkejše izdelke ponudnikov šifriranega dostopa (5722–AC1 ali 5722–AC2), ki sta nudila nižje ravni šifrirnih funkcij.) Ko izvozite potrdilo (z njegovim 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 v drugem sistemu iSeries, 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 zasebnega potrdila za uporabo v drugem sistemu iSeries V5R1 ali V5R2

Za uporabo lokalne službe za potrdila za izdajanje potrdil, ki bodo uporabljena v drugem sistemu iSeries V5R2 ali V5R1, opravite v sistemu, ki gosti lokalno službo za potrdila, naslednje naloge:

1. Zaženite DCM.

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

   Za dokončanje te naloge 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 iSeries** (za seje SSL) ali **potrdilo za podpisovanje objektov za drug iSeries** (za uporabo v drugem sistemu).

   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. Ker mora uporabljati ciljni sistem različico V5R1 ali novejšo, vas Upravljalnik digitalnih potrdil v gostiteljskem sistemu ne pozove, da izberete obliko ciljne izdaje za novo potrdilo za podpisovanje objektov.
4. Če izdelujete potrdilo strežnika ali odjemalca, izberite raven izdaje iSeries, 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 sistemom iSeries, 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 v sistemu V4R4 ali V4R5 iSeries

Če želite lokalno službo za potrdila uporabiti za izdajanje potrdil v sistemu iSeries V4R4 ali V4R5, izvedite naslednje korake na sistemu, ki gosti lokalno službo za potrdila V5R2:

1. Zaženite DCM.

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

   Za dokončanje te naloge 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.

   Opomba: Ker izdelujete to potrdilo za uporabo v sistemu iSeries V4R4 ali V4R5, morate izbrati **potrdilo strežnika ali odjemalca za drug iSeries**. Ciljni sistemi z ravnijo izdaje pred V5R1 ne morejo uporabljati potrdil za podpisovanje objektov.

4. Izberite raven izdaje sistema iSeries, 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 sistemom iSeries, 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 uporabljati potrdila v teh datotekah v obstoječem prostoru za potrdila *SYSTEM v ciljnem sistemu V4R4 ali V4R5, ne morete uvoziti potrdil lokalne službe za potrdila 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 na primer poimenujete mojadat.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. Za prenos izdelanih datotek prostorov za potrdila (.KDB in .RDB) v ciljni sistem V4R4 ali V4R5 uporabite dvojiški FTP (File Transfer Protocol) ali kakšen drug način. Za prenos datoteke, ki vsebuje izvoženo potrdilo lokalne službe za potrdila uporabite način FTP ASCII.

Uporaba prenesenih datotek na 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 V5R2.
- Uporaba zasebnega potrdila za seje SSL v ciljnem sistemu V5R1.
- Uporaba zasebnega potrdila za podpisovanje objektov na ciljnem sistemu V5R2 ali V5R1.
- Uporaba zasebnega potrdila za seje SSL v ciljnem sistemu V4R5 ali V4R4 .

Uporaba zasebnega potrdila za seje SSL v ciljnem sistemu V5R2

Potrdila, ki jih uporabljajo vaše aplikacije za seje SSL, upravljate v prostoru za potrdila *SYSTEM Upravljalnika digitalnih potrdil (DCM). Če Upravljalnika digitalnih potrdil niste nikoli uporabili v ciljnem sistemu V5R2 za upravljanje potrdil za SSL, potem ta prostor za potrdila ne obstaja v ciljnem sistemu. 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 portdila *SYSTEM obstaja v ciljnem sistemu V5R2, 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 V5R2, v katerem želite uporabiti prenesene datoteke prostora za potrdila, lahko uporabite prenesene datoteke potrdil kot prostor za potrdila *SYSTEM. Če želite izdelati prostor za potrdila *SYSTEM in uporabiti datoteke potrdil na ciljnem sistemu V5R2, storite 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. V tem primeru prenesenih datotek ne preimenujte. Če prepišete privzete datoteke, boste imeli težave pri uporabi Upravljalnika digitalnih potrdil, prenesenega prostora za potrdila in njegove vsebine. Namesto tega zagotovite, da imajo enkratna imena in uporabite prenesen prostor za potrdila kot **Drug sistemski prostor za potrdila**. Če uporabite datoteke kot Drug sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije lahko uporabljajo 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 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. Zdaj lahko podate, katere aplikacije naj uporabljajo 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 aplikacije, ki bi morale uporabljati 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 omoogoči 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.

Prostor za potrdila *SYSTEM obstaja — datoteke bodo uporabljene kot Drug sistemski prostor za potrdila

Če v ciljnem sistemu V5R2 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-ja 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 se odločite, da boste uporabljali prenesene datoteke kot Drug sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije naj uporabljajo 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 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 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 — uporabljena bodo potrdila v obstoječem prostoru za potrdila *SYSTEM

Potrdila iz prenesenih datotek prostora za potrdila lahko uporabite v obstoječem prostoru za potrdila *SYSTEM v sistemu V5R2. 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 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: Potrdilo lokalne službe za potrdila izvozite v prostor za potrdila preden vanj izvozite potrdilo strežnika ali odjemalca. 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 **Izvoz potrdila**.
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 bi morale uporabljati 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 omoogoči 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 Upravljalnika digitalnih potrdil niste nikoli uporabili v ciljnem sistemu V5R1 za upravljanje potrdil za SSL, potem ta prostor za potrdila ne obstaja v ciljnem sistemu. 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 portdila *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. V tem primeru prenesenih datotek ne preimenujte. Če prepišete privzete datoteke, boste imeli težave pri uporabi Upravljalnika digitalnih potrdil, prenesenega prostora za potrdila in njegove vsebine. Namesto tega zagotovite, da imajo enkratna imena in uporabite prenesen prostor za potrdila kot **Drug sistemski prostor za potrdila**. Če uporabite datoteke kot Drug sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije lahko uporabljajo 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. Zdaj lahko podate, katere aplikacije naj uporabljajo 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 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 omoogoči 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 obstaja — datoteke bodo uporabljene 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-ja 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 se odločite, da boste uporabljali prenesene datoteke kot Drug sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije naj uporabljajo 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 — uporabljena bodo potrdila 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: Potrdilo lokalne službe za potrdila izvozite v prostor za potrdila preden vanj izvozite potrdilo strežnika ali odjemalca. 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 **Izvoz potrdila**.
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 omoogoči 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.

Uporaba zasebnega potrdila za podpisovanje objektov v ciljnem sistemu V5R1 ali V5R2

Potrdila, ki jih uporabljate za podpisovanje objektov, upravljate v prostoru za potrdila *OBJECTSIGNING Upravljalnika digitalnih potrdil (DCM). Če Upravljalnika digitalnih potrdil niste nikoli uporabili v ciljnem sistemu za upravljanje potrdil za podpisovanje objektov, potem ta prostor za potrdila ne obstaja v ciljnem sistemu. 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 ne obstaja v ciljnem sistemu V5R2 ali V5R1 s prenesenimi datotekami prostora za potrdila, opravite 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. V tem primeru prenesenih datotek ne preimenujte. Če prepišete privzete datoteke za podpisovanje objektov, boste imeli težave pri uporabi Upravljalnika digitalnih potrdil, prenesenega prostora za potrdila in njegove vsebine. Potrdila iz teh datotek lahko pridobite v prostor za potrdila *OBJECTSIGNING na dva načina. Potrdila lahko izvozite iz te datoteke v niz običajnih datotek, iz katerih lahko uvozite potrdila v obstoječ prostor za potrdila *OBJECTSIGNING ali pa odprete prenesene datoteke kot Drug sistemski prostor za potrdila in izvozite potrdila neposredno v prostor za potrdila *OBJECTSIGNING, kot bomo opisali kasneje. V obeh primerih pa morate pridobiti potrdila v prostor za potrdila *OBJECTSIGNING, če želite upravljati aplikacije, ki potrdila uporabljajo, kot je opisano v tem postopku.

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 pošljete podpisane objekte, morajo njihovi prejemniki uporabiti različico Upravljalnika digitalnih potrdil V5R2 ali V5R1, s katero bodo preverili podpis objektov in preverili identiteto pošiljatelja. Za preverjanje veljavnosti podpisa mora imeti prejemnik kopijo potrdila. Kopijo tega potrdila morate poslati kot del paketa podpisanih objektov.

Prejemnik mora imeti tudi kopijo potrdila službe, ki je izdala potrdilo, uporabljeno za podpis objekta. Če ste podpisali objekte s potrdilom znane internetne službe za potrdila, bo prejemnikova različica Upravljalnika digitalnih potrdil najbrž že vsebovala kopijo potrebnega potrdila. Toda če je potrebno, poleg podpisanih objektov v ločenem paketu pošljite tudi kopijo

potrdila službe za potrdila. Kopijo potrdila lokalne službe za pooblastila morate na primer poslati, če ste podpisali objekte s potrdilom lokalne službe za potrdila. Zaradi varnostnih razlogov pošljite potrdilo v ločenem paketu ali poskrbite, da bo javno na voljo za tiste, ki ga potrebujejo.

Prostor za potrdila *OBJECTSIGNING obstaja

Potrdila iz prenesenih datotek prostora za potrdila lahko uporabite v obstoječem prostoru za potrdila *OBJECTSIGNING sistema V5R2 ali V5R1. 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 v ciljnem sistemu V5R2 ali V5R1 kot Drug sitemski prostor za potrdila. 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.

Za izvoz potrdil iz datotek prostora za potrdila neposredno v prostor za potrdila *OBJECTSIGNING opravite naslednje korake v ciljnem sistemu V5R2 ali 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 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: Izrazoslovlje 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: Potrdilo lokalne službe za potrdila izvozite v prostor za potrdila preden vanj izvozite potrdilo za podpisovanje objektov. 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, vnesite geslo prostora za potrdila in kliknite **Nadaljuj**.
12. Zdaj lahko izvozite potrdilo za podpisovanje objektov v prostor za potrdila *OBJECTSIGNING. Znova izberite nalogo **Izvoz potrdila**.
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, vnesite geslo prostora 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 ali V4R4

Potrdila, ki jih uporabljajo vaše aplikacije za seje SSL, upravljate v prostoru za potrdila *SYSTEM Upravljalnika digitalnih potrdil (DCM). Če Upravljalnika digitalnih potrdil niste nikoli uporabili v ciljnem sistemu V4R5 ali V4R4 za upravljanje potrdil za SSL, potem ta prostor za potrdila ne obstaja v ciljnem sistemu. 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 portdila *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 ne obstaja v ciljnem sistemu V4R5 ali V4R4, v katerem želite uporabiti prenesene datoteke prostora za potrdila, sledite naslednjim korakom:

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. V tem primeru prenesenih datotek ne preimenujte. Če prepišete privzete datoteke, boste imeli težave pri uporabi Upravljalnika digitalnih potrdil, prenesenega prostora za potrdila in njegove vsebine. Namesto tega zagotovite, da imajo enkratna imena in uporabite prenesene datoteke prostora za potrdila kot **Drug** prostor za potrdila. Če uporabite datoteke kot Drug sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije lahko uporabljajo 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 naj uporabi 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.

Ko dokončate te naloge, lahko aplikacije v ciljnem sistemu V4R5 ali V4R4 uporabijo potrdilo, ki ga je izdala lokalna služba za potrdila V5R2 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 obstaja — datoteke bodo uporabljene kot Drug sistemski prostor za potrdila

Če v ciljnem sistemu V4R5 ali V4R4 že obstaja prostor za potrdila *SYSTEM, se morate odločiti, kako boste delali z datotekami potrdil. 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 boste uporabili prenesene datoteke kot **Drug** sistemski prostor za potrdila, z Upravljalnikom digitalnih potrdil ne morete podati, katere aplikacije naj uporabljajo 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 obstaja v sistemu V4R5 ali V4R4, v katerem želite uporabiti prenesene datoteke prostora za potrdila, sledite naslednjim korakom:

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 preneseli 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 obstaja — datoteke bodo uvožene v prostor za potrdila *SYSTEM

Preden lahko uvozite potrdila v prostor za potrdila *SYSTEM v ciljnem sistemu V4R5 ali V4R4, morate izvoziti potrdila iz prostora za potrdila, ki ste ga izdelali v drugem datotečnem formatu. 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 ali V4R4, niso tako razvite kot tiste za V5R2, zato lahko naletite na težavo, če za izvoz potrdila zasebne lokalne službe za potrdila uporabite ciljni sistem. Zato za izvoz *dodatne* kopije potrdila lokalne službe za potrdila v ločeno datoteko namesto ciljnega sistema V4R4 ali V4R5 uporabite gostiteljski sistem V5R2. Ko izvozite potrdilo lokalne službe za potrdila v gostiteljski sistem V5R2, lahko ročno prenesete izvozno datoteko potrdila lokalne službe za potrdila v ciljni sistem V4R4 ali V4R5 in sledite korakom, opisanim v tem postopku za uvažanje potrdila 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.

Za izvažanje potrdil iz datotek prostora za potrdila opravite v ciljnem sistemu V4R4 ali V4R5 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 na primer poimenujete mojadat.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.

Do zdaj ste z Upravljalnikom digitalnih potrdil v izvornem gostiteljskem sistemu V5R2 izvozili dodatno kopijo potrdila lokalne službe za potrdila in ga ročno prenesli v ciljni sistem V4R4 ali V4R5. Upravljalnik digitalnih potrdil bi morali uporabiti v ciljnem sistemu tudi za izvoz zasebnega potrdila strežnika ali odjemalca v datoteko. Zdaj lahko uvozita 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 uvoziti potrdila iz izvoženih datotek in podati, naj jih uporabijo aplikacije, omogočene za SSL, opravite v ciljnem sistemu V4R4 ali V4R5 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 izvožene datoteke, ki ste jo izdelali v gostiteljskem sistemu V5R2. 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 naj zaupajo 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 Uvoz potrdila in kliknite **Potrdi**, da se boste vrnili 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. Potrdilo, ki ste ga uvozili, se mora prikazati tudi na seznamu potrdil.
10. Zdaj morate podati, katere aplikacije naj uporabljajo 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.

Ko dokončate te naloge, lahko aplikacije v ciljnem sistemu V4R4 ali V4R5 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.

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 dodelitev potrdil opisuje, kako dodeliti ali spremeniti potrdilo, ki ga uporablja aplikacija za vzpostavitev seje SSL ali podpis objektov.

Definiranje seznama overjenih služb za potrdila opisuje, kdaj lahko in kdaj morate definirati, katerim službam za potrdila lahko zaupa aplikacija pri preverjanju in sprejemanju potrdil.

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 aplikacije IBM iSeries, 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, pač pa 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 boste dostopili 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 lahko aplikacija uporablja potrdila za overjanje odjemalca in ali naj zahteva overjanje odjemalca. 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 boste dostopili 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. Tako bodo na primer strežniki Client Access Express samodejno uveljavili vse spremembe v potrdilih, 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 zadovoljenih nekaj 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 boste dostopili 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 naj jim aplikacija zaupa in kliknite **Potrdi**. Upravljalnik digitalnih potrdil prikaže sporočilo, ki zahteva, da potrdite izbire seznama overjenih služb.

   Opomba: S seznam lahko izberete posamezne službe za potrdila ali podate, naj aplikacija zaupa vsem ali nobeni službi za potrdila s seznama. Preden dodate potrdilo službe za potrdila na seznam, si ga lahko ogledate in preverite njegovo veljavnost.

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 preprečijo aplikaciji uspešno sodelovanje v seji plasti zaščitenih vtičnic (SSL) ali uspešno podpisovanje objektov.

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 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 boste dostopili 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 **Dodaj mesto CRL**, da boste prikazali obrazec, ki ga lahko uporabite za opis mesta CRL in načina, na katerega naj Upravljalnik digitalnih potrdil ali aplikacija dostopita do mesta.
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 boste dostopili 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. Poleg tega morate tudi konfigurirati strežnik imeniških storitev in aplikacije odjemalca za uporabo SSL in dodeliti potrdilo aplikacijam v Upravljalniku digitalnih potrdil.

Če se želite naučiti več o konfiguriranju in uporabi strežnika imeniških storitev iSeries, v Informacijskem centru preberite naslednje teme:

- Imeniške storitve (LDAP)
  Ta tema vas bo naučila vse, kar morate vedeti o konfiguriranju in uporabi strežnika imeniških storitev (LDAP) iSeries.
- Uporaba zaščite plasti zaščitnih vtičnic (SSL) z imeniškim strežnikom LDAP
  Ta tema razlaga, kaj morate narediti za konfiguriranje strežnika LDAP za uporabo SSL za zaščitene komunikacije.

Shranjevanje ključev potrdil v šifrirni koprocesor IBM 4758

Če ste šifrirni koprocesor IBM 4758–023 PCI namestili v vaš sistem iSeries, ga lahko uporabite za varnejšo shrambo zasebnih ključev potrdil. 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 koporocesor.
- 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 uporabiti koprocesor za shranjevanje zasebnih ključev, morate koprocesor omogočiti, preden uporabite Upravljalnik digitalnih potrdil (DCM). 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 dodatno zaščititi dostop do zasebnega ključa potrdila in njegovo uporabo, ga lahko shranite neposredno v šifrirni koprocesor IBM 4758–023 PCI. 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 dodatno zaščititi dostop do zasebnega ključa potrdila in njegovo uporabo, lahko uporabite glavni ključ šifrirnega koprocesorja IBM 4758–023 PCI in z njim šifrirate zasebni ključ, ki ga nato shranite v posebno datoteko ključev. To možnost za shranitev ključa lahko izberete kot del postopka izdelave ali obnovitve potrdila v Upravljalniku digitalnih potrdil (DCM).

Preden lahko uspešno uporabite to možnost, morate uporabiti konfiguracijski spletni vmesnik šifrirnega koprocesorja IBM 4758–023 PCI in z njim izdelati ustrezno datoteko za shranjevanje ključev.Konfiguracijski spletni vmesnik koprocesorja morate uporabiti tudi za povezavo datoteke za shranjevanje ključev z opisom naprave koprocesorja, ki jo želite uporabiti. Do spletnega vmesnika za konfiguriranje koprocesorja lahko dostopite s strani Naloge 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. Za preverjanje, ali uporabljajo naprave isti šifrirni ključ, uporabite nalogo Preverjanje glavnega ključa v spletnem vmesniku za konfiguriranje šifrirnega koprocesorja 4758. Do spletnega vmesnika za konfiguriranje koprocesorja lahko dostopite s strani Naloge 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 (Public Key Infrastructure) za X.509 je služba, ki izdaja potrdila na osnovi najnovejših internetnih standardov x.509 za izvajanje 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 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, ki podpira PKIX, raziščite, ali potrebujete strog nadzor dostopa do sredstev, ki jih nudijo uporabnikom aplikacije, omogočene za SSL. Tako na primer nudi Lotus Domino 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**.

Podpisovanje objektov

Za podpisovanje objektov lahko uporabite tri načine. Napišete lahko program, ki pokliče API za podpisovanje objekta. Za podpisovanje lahko uporabite Upravljalnik digitalnik potrdil (DCM), ali pa začenši v V5R2, v Navigatorju iSeries uporabite možnost Osrednjega upravljanja za podpisovanje objektov kot pakete za distribucijo drugim sistemom iSeries.

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 v drugih strežnikih iSeries, 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:

- Izdelati morate prostor za potrdila *OBJECTSIGNING, kot del postopka osnovanja lokalne službe za potrdila, ali kot del postopka upravljanja potrdil za podpisovanje objektov prek 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 boste dostopili 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 na primer podpisati vse objekte v določenem imeniku, lahko vnesete /mydirectory/*; če želite podpisati vse programe v določeni knjižnici, lahko vnesete /QSYS.LIB/QGPL.LIB/*.PGM. Ta univerzalna znaka lahko uporabite samo v zadnjem delu poti; tako na primer /mydirectory*/filename povzroči prikaz sporočila o napaki. Če želite za prikaz seznama knjižnice ali vsebine imenika uporabiti funkcijo pregledovanja, preden kliknete **Preglej** vnesite univerzalni znak kot del poti.
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 boste dostopili 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 na primer podpisati vse objekte v določenem imeniku, lahko vnesete /mydirectory/*; če želite podpisati vse programe v določeni knjižnici, lahko vnesete /QSYS.LIB/QGPL.LIB/*.PGM. Ta univerzalna znaka lahko uporabite samo v zadnjem delu poti; tako na primer /mydirectory*/filename povzroči prikaz sporočila o napaki. Če želite za prikaz seznama knjižnice ali vsebine imenika uporabiti funkcijo pregledovanja, preden kliknete **Preglej** vnesite univerzalni znak kot del poti.

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

Na tej straneh lahko najdete uporabne informacije, ki vam bodo v pomoč pri odpravljanju nekaterih ali več splošnih težav, na katere lahko naletite med delom z upravljalnikom digitalnih potrdil (DCM).

Če želite informacije o težavah in mogočih rešitvah zanje, preglejte naslednje strani:

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 digitalih potrdil in kako jih lahko odpravite.

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

Napake pri selitvi in rešitve za obnovitev
V tej temi se boste naučili več o splošnih težavah, na katere lahko naletite pri selitvi Upravljalnika digitalnih potrdil iz prejšnje izdaje in kako jih lahko odpravite.

Odpravljanje težav pri dodeljevanju uporabniškega potrdila
V tej temi se boste naučili več o splošnih težavah, na katere lahko naletite pri uporabi Upravljalnika digitalnih potrdil za registriranje uporabiškega 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 spletne strani na internetu.
Ko poskusite odpreti prostor za potrdila, pride do napake NET.DATA.	Če izberete nalogo **Izberi prostor za potrdila**, izberite gumb **Nadaljuj**, namesto da bi na tipkovnici pritisnili tipko **Enter**.
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 Izberi prostor 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.

Težava	Možna rešitev
	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.
	Preverite vrednost, ki je dodeljena atributu ″Dopusti nova digitalna potrdila″, pod možnostjo Delo z zaščito sistema v Orodjih sistemskih storitev (SST). Če je ta atribut nastavljen na vrednost 2 (Ne), potem ni mogoča vnovična nastavitev gesla prostora za potrdila. Vrednost za ta atribut lahko prikažete ali spremenite z uporabo ukaza STRSST in vnosom ID-ja uporabnika in gesla storitvenih orodij. 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 iSeries.	Potrdila nekaterih služb za potrdila nisa 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.
Pri delu s strežnikom LDAP ste naleteli na težavo, kot je na primer, da se dodelitve potrdil ne prikažejo, informacije o zaščiteni aplikaciji pa se prikažejo takoj po dodelitvi potrdila. Ta težava je pogostejša, če za dostop do pregledovalnika Netscape Communicator uporabljate Navigator iSeries. Vaša nastavitev za predpomnilnik pregledovalnika je nastavljena na primerjavo dokumenta v predpomnilniku s dokumentom v omrežju ″Enkar 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 sistem iSeries 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 v sistemu iSeries. Takšne težave lahko povzroča oblikovanje nekaterih spletnih strani. Druge spletne strani so oblikovane tako, da se izognejo tej težavi. Ne pozabite primerjati videza izvornega potrdila z rezultatom, ki ga dobite po lepljenju, saj morajo biti prilepljene informacije popolnoma enake.

Težava	Možna rešitev
Selitev iz upravljalnika digitalnih potrdil izdaje V4R3 v V5R2 ne prilagodi preteklih sistemskih potrdil.	Preteklo sistemsko potrdilo ni veljavno in ga ni mogoče premakniti v prostor za potrdila *SYSTEM. Pred selitvijo iz V4R3 odstranite ali preimenujte stare datoteke obroča ključev, zanemarite indikator, ki kaže na neuspelo selitev ali pa selitev ponovite.
Ne morete najti vzorčne kode za dodajanje potrdil na seznam za preverjanje veljavnosti.	Vzorčna koda še ni na voljo.

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.
Izdelava baze podatkov ključev ni uspela.	Preverite možnost neskladnosti imena datoteke. Do neskladnosti lahko pride v drugi datoteki in ne v tisti, ki je zahtevana.
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 idnetiteta internetnega uporabnika ustrezno preverjena, da je potrdilo mogoče dodati na seznam za preverjanje veljavnosti. Preberite temo Informacijskega centra za API QsyAddVldlCertificate. Za pomoč pri konfiguriranju primerka zaščitenega strežnika za uporabo seznama za preverjanje veljavnosti uporabite knjigo Webmaster's Guide.

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. Skrbnik sistema mora biti prepričan, da prostor za potrdila (baza podatkov ključev) še vedno zaupa službi za potrdila, ki je podpisala uporabniško in sistemsko potrdilo.
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. Preverite tudi, ali je pravilno nastavljen imenski strežnik domen.
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.
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 še vedno sporoča končnemu uporabniku, da služba za potrdila še ni overjena.	S pomočjo Upravljalnika digitalnih potrdil nastavite **status službe za potrdila** na omogočeno, da boste označili službo za potrdila kot overjeno.
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

Naslednjo tabelo lahko uporabite za iskanje informacij, ki vam bodo pomagale pri odpravljanju nekaterih pogostih težav v strežniku HTTP za iSeries, na katere lahko naletite pri delu z Upravljalnikom digitalnih potrdil.

Težava	Možna rešitev
HTTPS (Hypertext Transfer Protocol Secure) ne deluje.	Zagotovite, da je strežnik HTTP pravilno konfiguriran za uporabo SSL. V V5R1 ali novejših različicah mora imeti konfiguracijska datoteka nastavljeno možnost **SSLAppName** z uporabo grafičnega uporabniškega vmesnika (GUI) strežnika HTTP. Prav tako mora imeti konfiguracija konfiguriranega navideznega gostitelja, ki uporablja vrata SSL z **SSLEnable** v navideznem gostitelju. Tam morata biti tudi dve smernici za poslušanje, ki podajata dvoje različnih vrat, ena za SSL ter druga, ki niso za SSL. Preverite tudi, ali je primerek srežnika izdelan in potrdilo strežnika podpisano.
Postopek registriranja primerka strežnika HTTP kot zaščitene aplikacije zahteva razjasnitev.	Na vašem sistemu iSeries pojdite na spletni vmesnik strežnika HTTP in nastavite konfiguracijo za vaš strežnik HTTP. Najprej morate definirati navideznega gostitelja, da omogoča SSL. To naredite na zaslonu za upravljalnje konteksta. Navideznega gostitelja morate definirati tako, da uporablja vrata SSL, ki ste jih predhodno definirali s smernico za poslušanje. Nato morate na zaslonu Splošne nastavitve SSL vključiti SSL na predhodno konfiguriranem navideznem gostitelju. Vse spremembe morajo biti uveljavljene v konfiguracijski datoteki. Pomnite, da registrianje vašega primerka ne izbere samodejno, katera potrdila naj primerek uporablja. Z uporabo upravljalnika digitalnih potrdil morate aplikaciji dodeliti specifično potrdilo, preden poskusite zaustaviti in znova zagnati primerek strežnika.
Težave imate pri nastavljanju strežnika HTTP za sezname za preverjanje veljavnosti in izbirno overjanje odjemalcev.	Dodatne informacije o možnostih pri nastavljanju primerka poiščite v knjigi HTTP Server Webmaster's Guide. Te informacije so na voljo v Informacijskem centru pod temo Spletna strežba.
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 OS/400. Ogledate si lahko tudi naslednje sezname za preverjanje veljavnosti ali API-je povezane s potrdili: • QsyListVldlCertificates in QSYLSTVC • QsyRemoveVldlCertificate in QRMVVC • QsyCheckVldlCertificate in QSYCHKVC • QsyParseCertificate in QSYPARSC in tako dalje.
Ne morete najti datoteke zahtev, ki se izdela, ko namestite strežnik HTTP. Sistem s pomočjo te datoteke pokaže veljavne datoteke obroča ključev v smernici KEYFILE konfiguracijskih datotek.	Če želite podrobnejše informacije, preglejte Selitev v DCM iz zgodnejše izdaje. Pravilna datoteka za strežnik HTTP je /qibm/userdata/httpsvr/keyring/keymreq.crt, pravilna datoteka za LDAP pa /qibm/userdata/os400/dirsrv/qdirsrv.crt.
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.
Po namestitvi V5R2 prek izdaje V4R3 ste opazili težavo pri prostorih za potrdila, datoteka /qibm/userdata/httpsvr/keyring/keymreq.crt ali /qibm/usedata/os400/dirsrv/qdirsrv.crt pa zdaj obstaja. Sistem ni uspel končati samodejne selitve obroča ključev v bazo podatkov ključev.	Podajte stare datoteke obroča ključev kot prostor za potrdila in preden pokličete qicss/qyepmgrt za vnovičen poskus selitve poiščite in zbrišite neveljavno potrdilo ali potrdila iz datotek obroča ključev. Če je postopek selitve prenesel vsa pomembna potrdila, lahko tudi zanemarite ali zbrišete datoteko .crt.

Težava	Možna rešitev
Strežnik HTTP se ne bo zagnal uspešno z nastavljeno možnostjo **SSLEnable**, v dnevniku opravil pa se pojavi sporočilo o napaki HTP8351. Če strežnik HTTP ne uspe, dnevnik napak za strežnik *ADMIN kaže napako, da operacija inicializacije SSL ni uspela s povratno kodo napake 107.	Napaka 107 pomeni, da je potrdilo poteklo. Če gre za primerek strežnika *ADMIN, začasno nastavite **SSLDisable**, da boste na strežniku *ADMIN lahko uporabljali Upravljalnik digitalnih potrdil. Z njegovo pomočjo dodelite aplikaciji drugo potrdilo, kot je na primer QIBM_HTTP_SERVER_ADMIN, če gre za primerek strežnika *ADMIN.

Napake pri selitvi in rešitve za obnovitev

Napake in okrevanje po njih

Naslednji indikatorji opozarjajo na napake, do katerih lahko pride med selitvijo:

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
Prisotnost tega indikatorja po uspešni namestitvi možnosti 34 in 5722-DG1 pomeni, da selitev obroča ključev, ki jo je poskusil izvesti 5722-DG1, ni uspela. Morda boste morali izvesti selitev obroča ključev v prostor za potrdila *SYSTEM.

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT
Prisotnost tega indikatorja po uspešni namestitvi možnosti 34 pomeni, da selitev obroča ključev za strežnik LDAP ni uspela.

Poleg naznačenih napak lahko pride tudi do drugih napak pri selitvi, ki jih sistem morda ne naznani. Če sistem na primer najde datoteke obroča ključev, ki jih mora preseliti v prostor za potrdila *SYSTEM, se lahko zgodi, da pride do navzkrižja z obstoječimi uporabniškimi podatkovnimi datotekami integriranega datotečnega sistema. V tem primeru sistem morda ne bo uspel dokončati selitve datotek obroča ključev, čeprav je namestitev uspela.

V redkih primerih se lahko zgodi, da se selitev datoteke obroča ključev zaključi z delno dodelitvijo sistemskega potrdila, preden napaka prepreči dokončanje selitve. To lahko povzroči napake pri zagonu primerka *ADMIN strežnika IBM HTTP, če je SSLMODE nastavljen na ON. Možne razlage so:

- Preseljena datoteka obroča ključev je imela kot svoj privzetek nastavljeno neveljavno sistemsko potrdilo.
- Upravljalnik digitalnih potrdil je končal selitev, da bi ohranil uporabniške podatke, ki so obstajali v kritični datoteki.
- V kodi za selitev je prišlo do nepričakovane napake.

Strežnik IBM HTTP lahko zaženete, ne da bi bil SSLMODE nastavljen na ON. To naredite tako, da ga začasno nastavite na OFF za primerek *ADMIN, ki ga šele nato zaženete. S tem lahko preiskujete prostore za potrdila z Upravljalnikom digitalnih potrdil in razrešite težave, preden zaključite primerek *ADMIN. Ko zaključite primerek *ADMIN, lahko nastavite SSLMODE znova na ON in zaženete primerek *ADMIN in pravilno inicializirate SSL.

Po selitvi možnosti 34 lahko pride do napak med običajnimi zahtevami Upravljalnika digitalnih potrdil, ki uporabljajo prostore za potrdila. Do teh napak pride v pregledovalniku. Sledijo primeri teh napak:

```
Napaka v bazi podatkov
Napaka pri branju iz baze podatkov
Napaka pri pisanju v bazo podatkov
Okvarjena baza podatkov
Okvarjena tabela baze podatkov
```

V sistemu lahko obstaja datoteka, ki ni veljaven prostor za potrdila z imenom default.kdb v istem imeniku kot /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR ali

/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR. V tem primeru morate pred uporabo Upravljalnika digitalnih potrdil za izdelavo novih potrdil dokončati naslednjo ročno selitev:

Opomba: Če se odločite, da ne boste preselili datotek obroča ključev in namesto tega izdelate novo službo za potrdila in sistemsko potrdilo, preskočite naslednji postopek ročne selitve.

- Če nameravate namestiti strežnik HTTP Server za iSeries (5722-DG1), ga namestite zdaj, preden nadaljujete.

  Opombe:

  1. Namestitvena koda možnosti 34 5722–SS1 ne poskusi znova izvesti selitve, ko namestite možnost 34. Vnovična namestitev možnosti 34 ni rešitev.
  2. Ustrezne datoteke so v imenikih z uporabniškimi podatki, ki so bili izdelani s pooblastilom PUBLIC *EXCLUDE. Zagotovite, da imate zanje ustrezna pooblastila.

- Preverite, ali obstajata naslednji datoteki:
  - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

  Če obstajata, ju z ukazom WRKLNK preimenujte in izdelajte varnostne kopije.
- Iz profila uporabnika, ki ima pooblastilo *ALLOBJ, takole pokličite program QICSS/QYEPMGRT v ukazno vrstico:

  ```
  CALL QICSS/QYEPMGRT
  ```

  Če uspete, zagotovite, da v sistemu ne obstaja nobena od naslednjih datotek:
  - /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
  - /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

Upravljalnik digitalnih potrdil običajno hrani varnostne kopije uporabniških podatkov, ki ste jih shranili v datoteke, katerih imena so v navzkrižju s tistimi, ki jih uporablja Upravljalnik digitalnih potrdil. Če naslednji datoteki ne obstajata:

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

obstajata pa naslednji datoteki:

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

ju sistem poskusi preimenovati tako, da jima doda pripono .OLD. Če tudi ti datoteki že obstajata, sistem ne izdela nobenih varnostnih kopij, pač pa preprosto prepiše obstoječe datoteke .STH.

Razno

Če imajo poskusi izdelave službe za potrdila in sistemskega potrdila vedno znova za posledico napake zaradi navzkrižij imen datotek, ste morda naleteli na naslednje:

- **Navzkrižje zaradi različnega imena datoteke** – Upravljalnik digitalnih potrdil poskuša zaščititi uporabniške podatke v imenikih, ki jih izdela, čeprav te datoteke preprečijo Upravljalniku digitalnih potrdil uspešno izdelavo potrebnih datotek. 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. Po prenosu naslednjih datotek 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
```

- **Manjkajoča predpogojna možnost** – Preverite, ali ste pravilno namestili predpogojne licenčne programe (LPP-je).
- **Težave s kodo** – Obrnite se na predstavnika servisne službe.

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 DCM ne more prikazati potrdila, težavo lahko povzroča eno od naslednjih stanj:

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 bo prikazal poziv za izbiro potrdila.
2. Potrdilo, ki ga želite registrirati, je že registrirano z DCM.
3. Služba za potrdila, ki je izdala potrdilo, v sistemu ni označena kot overjena. 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 uporabiti nalogo **Delo s potrdili CA**, s katero bo določil službo za potrdila kot overjeno v sistemu.

4. Nimate potrdila, ki bi ga lahko registrirali. Če želite preveriti, ali to povzroča težavo, lahko v pregledovalniku preverite uporabniška potrdila.
5. 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.
6. Strežnik IBM HTTP Server za iSeries ni pravilno nastavljen za izvajanje registracije potrdil s SSL in overjanja odjemalca v primeru zaščitenega strežnika *ADMIN. 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. Povezane informacije za DCM

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 iSeries:

- **Spletna stran službe za pomoč VeriSign**
  Tu boste našli obsežno knjižnico s temami o digitalnih potrdilih, kot tudi s številnimi drugimi temami o zaščiti na internetu.
- **IBM eServer Zaščita ožičenega omrežja iSeries: OS/400 V5R1 DCM in šifrirne izboljšave 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 iSeries, 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 strežniku iSeries. Razlaga, kako nastaviti različne strežnike in odjemalce za uporabo potrdil in nudi informacije in vzoročno kodo za uporabo API-jev OS/400 za upravljanje in uporabo digitalnih potrdil v uporabniških aplikacijah.
- **Iskanje indeksov RFC**
  Ta spletna stran nudi iskalno skladišče za RFC-je (Request for Comments). RFC-ji opisujejo standarde za internetne protokole, kot so SSL, PKIX in drugi, ki so povezani z uporabo digitalnih potrdil.

Natisnjeno na Danskem