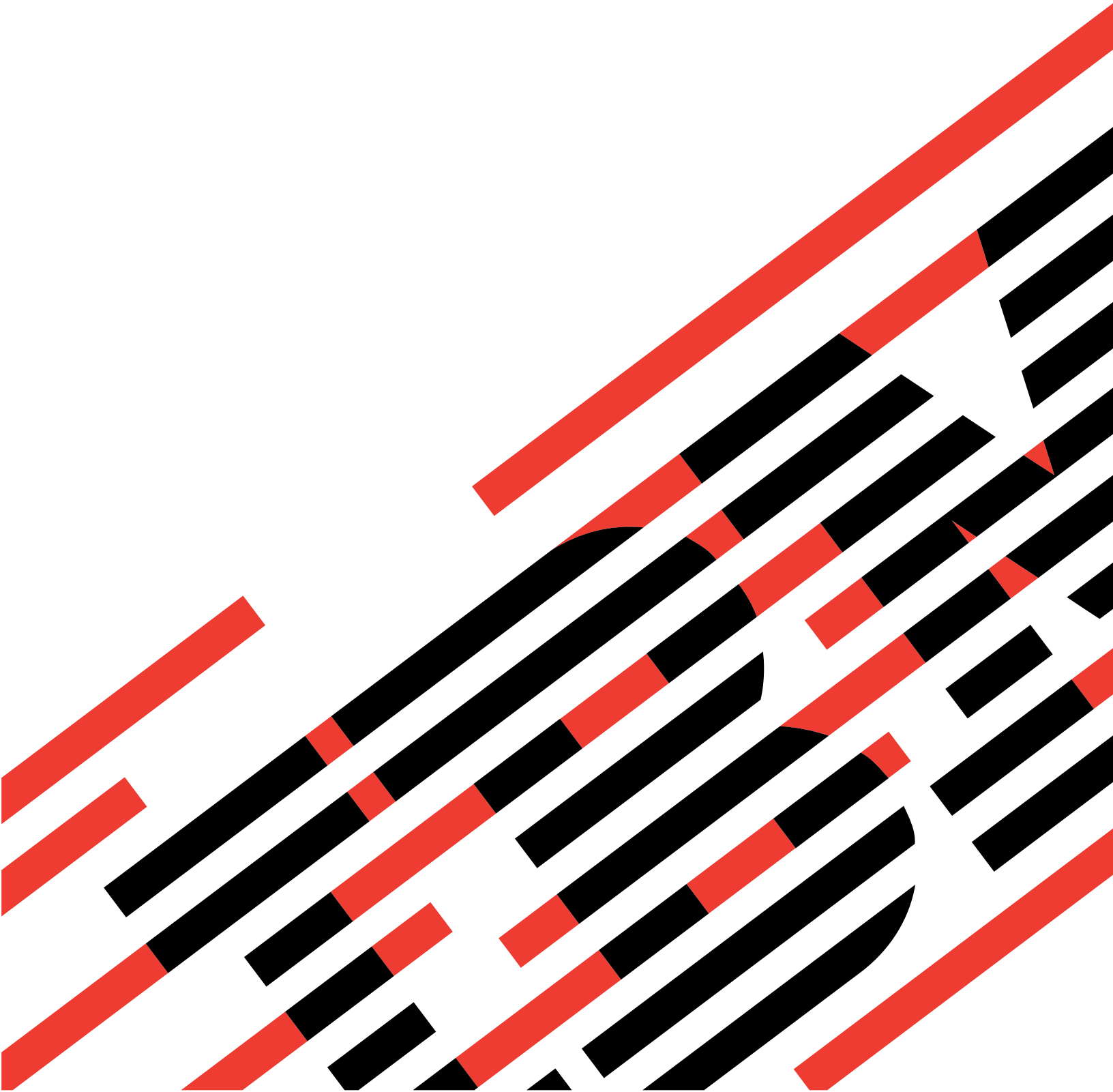
IBM

eserver

iSeries

Podpisovanje objektov in preverjanje podpisov



IBM

@server

iSeries

Podpisovanje objektov in preverjanje podpisov

Kazalo

Podpisovanje objektov in preverjanje podpisov

Podpisovanje objektov in preverjanje podpisov sta funkciji zaščite, ki ju lahko uporabite za preverjanje integritete številnih objektov iSeries. S pomočjo zasebnega ključa digitalnega potrdila podpišete objekt, s potrdilom (ki vsebuje ustrezen javni ključ) pa preverite digitalni podpis. Digitalni podpis zagotavlja časovno in vsebinsko integriteto objekta, ki ga podpisujete. Podpis je neizpodbiten dokaz pristnosti in pooblastila. Uporablja se lahko za dokaz izvora in odkrivanje vdorov. S podpisovanjem objektov določite njihov izvor in omogočite sredstva za odkrivanje sprememb v objektih. Pri preverjanju podpisa objekta lahko določite, ali je bila v vsebini objekta od njegova podpisa opravljena kakšna sprememba. Preverite lahko tudi izvor podpisa in zagotovite zanesljivost izvora objekta.

Podpisovanje objektov in preverjanje podpisov iSeries lahko izvajate s pomočjo:

- API-jev za programsko podpisovanje objektov in preverjanje podpisov v objektih.
- Upravljalnika digitalnih potrdil za podpisovanje objektov in prikaz ali preverjanje podpisov objektov.
- Osrednjega upravljanja Navigatorja iSeries za podpisovanje objektov kot del porazdelitve paketov v druge sisteme.
- Ukazov CL, kot je CHKOBJITG (Preveri integriteto objekta), za preverjanje podpisov.

Če želite podrobneje spoznati te načine podpisovanja objektov in se naučiti, kako lahko s podpisovanjem objektov izboljšate trenutno načelo zaščite, preglejte naslednje teme:

Kaj je novega v V5R2
Te informacije vas bodo poučile o novih funkcijah podpisovanja objektov in preverjanja podpisov iSeries, kot tudi o spremembah v dokumentaciji za to izdajo.

Natisni to temo
S pomočjo teh informacij natisnite celotno temo kot datoteko PDF.

Scenariji podpisovanja objektov
Te informacije kažejo scenarije, ki ilustrirajo nekaj značilnih situacij uporabe funkcij podpisovanja objektov in preverjanja podpisov iSeries. Vsi scenariji vključujejo tudi konfiguracijske naloge, ki jih morate opraviti, če želite izvesti scenarij tako kot je opisan.

Koncepti podpisovanja objektov
S pomočjo teh konceptnih in referenčnih informacij se boste naučili več o digitalnih podpisih in o delovanju postopkov podpisovanja objektov in preverjanja podpisov.

Predpogoji za podpisovanje objektov in preverjanje podpisov
Te informacije kažejo konfiguracijske predpogoje, kot tudi drugo problematiko načrtovanja za podpisovanje objektov in preverjanje podpisov.

Upravljanje podpisanih objektov
Te informacije razlagajo ukaze in sistemske vrednosti iSeries, ki jih lahko uporabite za delo s podpisanimi objekti, in opisujejo, kako vplivajo podpisani objekti na postopka varnostnega kopiranja in obnavljanja.

Odpravljanje težav v podpisovanju objektov in preverjanju podpisov
Te informacije razlagajo, kako rešiti težave in napake, na katere lahko naletite pri podpisovanju objektov in preverjanju podpisov.

Povezane informacije za podpisovanje objektov in preverjanje podpisov
S pomočjo teh informacij poiščite povezave na druge izvore, v katerih se boste lahko naučili več o podpisovanju objektov in preverjanju podpisov objektov.

Kaj je novega v V5R2

Funkciji podpisovanja objektov in preverjanja podpisov za iSeries sta bili prvič vpeljani v V5R1. Toda v V5R2 je na voljo nekaj novih funkcij in izboljšav.

Nove ali izboljšane funkcije podpisovanja objektov in preverjanja podpisov vključujejo naslednje:

- Funkcijo podpisovanja objektov Osrednjega upravljanja Navigatorja **iSeries**
  Zdaj lahko s pomočjo čarovnika za definicijo izdelka Osrednjega upravljanja podpišete objekte, ki jih pripravite za pošiljanje v sisteme zaključnih točk iSeries.
- **Podpisovanje ukaznih objektov (*CMD)**
  Zdaj lahko podpišete ukazne objekte(*CMD). Izberete lahko podpis celotnega objekta *CMD ali samo osnovnih komponent objekta *CMD.
- **Novi API-ji za podpisovanje in preverjanje**
  S pomočjo treh novih API-jev lahko programsko izkoriščate izboljšave v funkcijah podpisovanja in preverjanja OS/400:
  - API za podpis vmesnega pomnilnika (QYDOSGNB, QydoSignBuffer)
    Ta API omogoča, da lokalni sistem digitalno podpiše vmesni pomnilnik in potrdi, da je zanesljiv. Ko sistem podpiše vmesni pomnilnik, vrne digitalni podpis klicatelju API-ja. S pomočjo tega API-ja lahko na primer podpišete del datoteke XML in shranite podpis v drug del datoteke XML ali pa odčitate zapise datoteke baze podatkov v vmesni pomnilnik in jih podpišete z API-jem.
  - API za reverjanje vmesnega pomnilnika (QYDOVFYB, QydoVerifyBuffer)
    Ta API omogoča, da lokalni sistem preveri digitalni podpis v predhodno podpisanem vmesnem pomnilniku.
  - API za dodajanje verifikatorja (QYDOADDV, QydoAddVerifier)
    Ta API doda potrdilo v sistemski prostor za potrdila *SIGNATUREVERIFICATION. Sistem lahko nato s pomočjo dodanega potrdila preveri podpise v objektih, ki jih je izdelalo potrdilo. S preverjanjem podpisov lahko sistem preveri integriteto podpisanih objektov in zagotovi, da od podpisa niso bili spremenjeni. Če prostor za potrdila ne obstaja, ga ta API izdela in doda potrdilo.

    Opomba: Zaradi varnostnih razlogov ta API ne dopušča, da v prostor za potrdila *SIGNATUREVERIFICATION dodate potrdilo službe za pooblastila (CA). Če dodate v prostor za potrdila potrdilo službe za pooblastila, sistem meni, da je CA overjen izvor potrdil. Posledično obravnava sistema potrdila, ki jih izda CA, kot potrdila iz overjenega izvora. Zato s pomočjo API-ja ne morete izdelati namestitvenega izhodnega programa za vstavljanje potrdila CA v prostor za potrdila. Potrdilo CA morate dodati v prostor za potrdila s pomočjo Upravljalnika digitalnih potrdil, in s tem zagotoviti, da mora nekdo izrecno in ročno nadzorovati, katerim službam za pooblastila zaupa sistem. S tem preprečite možnost, da bi sistem uvozil potrdila iz izvorov, ki jih skrbnik ni izrecno podal kot overjene.

    Če želite preprečiti, da bi kdorkoli uporabil ta API za dodajanje potrdila za preverjanje v prostor za potrdila *SIGNATUREVERIFICATION brez vaše vednosti, lahko onemogočite ta API v sistemu. To lahko naredite s pomočjo sistemskih storitvenih orodij (SST), ki onemogočijo spreminjanje sistemskih vrednosti, povezanih z zaščito.

Predhodno so bile funkcije podpisovanja objektov in preverjanja podpisov iSeries na voljo kot del teme Informacijski center upravljanja digitalnih potrdil. Zdaj obstajajo dodatni načini, ki jih lahko uporabite za podpisovanje objektov in preverjanje podpisov. Posledično je na voljo tudi nova tema Informacijskega centra, ki poenostavlja uporabo podpisovanja objektov in preverjanja podpisov, saj nudi informacije na enem mestu. Tema vsebuje izboljšane in popolnejše informacije kot so na primer scenariji, ki vam bodo pomagale določiti, kdaj in kako uporabiti ti funkciji za zaščito.

Nove ali izboljšane informacije za to temo vključujejo naslednje:

- Scenarije, ki vam bodo pomagali določiti, kako najbolje uporabiti funkciji podpisovanja objektov in preverjanja podpisov za izvedbo zaščite.

- Nove razdelke, ki opisujejo ukaze in sistemske vrednosti, ki jih lahko uporabite za upravljanje podpisanih objektov v sistemu.
- Nove razdelke, ki opisujejo načrtovanje in druge konceptne informacije za podpisovanje objektov in preverjanje podpisov.

Če želite najti še druge informacije o tem, kaj je novega ali spremenjenega v tej izdaji, preberite Opomnik za uporabnike .

Natisni to temo

Če si želite ogledati ali presneti različico PDF, izberite Podpisovanje objektov in preverjanje podpisov (velikost datoteke je 350 kb ali okrog 44 strani).

Takole shranite PDF na delovni postaji za ogled ali natis:

1. Odprite PDF v brskalniku (kliknite zgornjo povezavo).
2. Na meniju brskalnika kliknite **Datoteka**.
3. Kliknite **Shrani kot...**
4. Izberite imenik, v katerega želite shraniti PDF.
5. Kliknite **Shrani**.

Če potrebujete za ogled ali natis datoteke PDF program Adobe Acrobat Reader, ga lahko naložite na spletni strani Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Scenariji podpisovanja objektov

Strežnik iSeries nudi številne različne načine podpisovanja objektov in preverjanja podpisov objektov. Kako izberete podpise objektov in kako delate s podpisanimi objekti se spreminja glede na poslovne in zaščitne potrebe in cilje. Včasih bo zadoščalo, če boste v sistemu preverili samo podpise objektov in zagotovili, da je njihova integriteta nedotaknjena. V drugih primerih boste izbrali podpisovanje objektov, ki jih pošljete drugim uporabnikom. S podpisom objektov omogočite, da drugi uporabniki določijo izvor objektov in preverijo njihovo integriteto.

Kateri način boste izbrali, je odvisno od več faktorjev. Scenariji v tej temi opisujejo najpogostejše cilje podpisovanja objektov in preverjanja podpisov znotraj značilnega poslovnega konteksta. Vsi scenariji opisujejo tudi predpogoje in naloge, ki jih morate opraviti, če želite izvesti scenarij tako kot je opisano. Preglejte te scenarije, ki vam bodo pomagali določiti, kako uporabljati funkcije podpisovanja objektov iSeries, tako da bodo čim bolj ustrezale vašim poslovnim in zaščitnim potrebam:

Scenarij: Uporaba Upravljalnika digitalnih potrdil za podpisovanje objektov in preverjanje podpisov
Ta scenarij opisuje podjetje, ki želi podpisati nezaščitene aplikacijske objekte na javnem spletnem strežniku. Želijo, da bi lahko na preprost način določili, ali je bila v teh objektih opravljena kakšna nepooblaščena sprememba. Na osnovi poslovnih potreb in ciljev zaščite tega podjetja opisuje ta scenarij, kako uporabiti Upravljalnik digitalnih potrdil (DCM) kot osnovni način za podpisovanje objektov in preverjanje podpisov objektov.

Scenarij: Uporaba API-jev za podpisovanje objektov in preverjanje podpisov
Ta scenarij opisuje podjetje za razvijanje aplikacij, ki želi programsko podpisati aplikacije, ki jih prodaja. Svojim strankam želijo zajamčiti, da izvirajo aplikacijo iz njihovega podjetja in jim ponuditi sredstva za odkrivanje nepooblaščenih sprememb v aplikacijah pri namestitvi. Na osnovi poslovnih potreb in ciljev zaščite tega podjetja opisuje ta scenarij, kako uporabiti API Podpisovanje objektov in API Dodajanje verifikatorja za podpisovanje objektov in omogočanje preverjanja podpisov.

Scenarij: Uporaba Osrednjega upravljanja za podpisovanje objektov
Ta scenarij opisuje podjetje, ki želi podpisati objekte, ki jih pošlje na več strežnikov iSeries. Na osnovi poslovnih potreb in ciljev zaščite tega podjetja opisuje ta scenarij, kako uporabiti funkcijo Osrednjega upravljanja Navigatorja iSeries za pošiljanje in podpisovanje objektov, ki so namenjeni drugim strežnikom iSeries.

Scenarij: Uporaba DCM za podpisovanje objektov in preverjanje podpisov

Stanje

Kot skrbnik iSeries za MyCo., Inc. ste odgovorni za upravljanje dveh strežnikov iSeries v vašem podjetju. Eden od teh strežnikov iSeries nudi javno spletno stran za vaše podjetje. Za razvitje vsebine za to javno spletno stran in za prenos datotek in programskih objektov na javni spletni strežnik po njihovem preizkusu uporabite notranji produkcijski strežnik iSeries podjetja.

Javni spletni strežnik podjetja nudi spletno stran s splošnimi informacijami o podjetju. Prav tako nudi različne obrazce, ki jih izpolnijo stranke, če želijo registrirati izdelke ali če zahtevajo informacije o izdelku, obvestila o popravkih izdelkov, mesta distribuiranja izdelkov itd. Skrbi vas odprtost programov cgi-bin, ki nudijo te obrazce, saj veste, da jih je mogoče spremeniti. Zato želite preverjati integreteto teh programskih objektov in odkriti, če so bile v njih opravljene nepooblaščene spremembe. Posledično ste se odločili, da boste za dosego tega cilja zaščite digitalno podpisali te objekte.

Raziskali ste funkcije podpisovanja objektov OS/400 in se naučili, da obstaja več načinov, ki jih lahko uporabite za podpisovanje objektov in preverjanje podpisov. Ker ste odgovorni za upravljanje majhnega števila strežnikov iSeries in menite, da objektov ne bo potrebno pogosto podpisovati, ste se za izvajanje teh nalog odločili za uporabo Upravljalnika digitalnih potrdil (DCM). Odločili ste se tudi, da boste izdelali lokalno službo za pooblastila (CA) in uporabili zasebno potrdilo za podpisovanje objektov. Z uporabo zasebnega potrdila, ki ga izda lokalni CA za podpisovanje objektov, zmanjšate strošek uporabe te tehnologije za zaščito, ker vam ni potrebno kupiti potrdila pri znani javni službi za pooblastila.

Ta zgled služi kot koristen uvod v korake, vključene v nastavitev in uporabo podpisovanja objektov, če želite podpisati objekte na manjšem številu strežnikov iSeries.

Prednosti scenarija

S tem scenarijem so povezane naslednje prednosti:

- Če podpišete objekte, lahko preverite integreteto nezaščitenih objektov in preprosteje določite, ali so bili objekti od podpisa spremenjeni. S tem boste zmanjšali tudi del odpravljanja težav, ki bi ga bilo potrebno opraviti v bodoče, da bi ugotovili aplikacijske in druge sistemske težave.
- Uporaba grafičnega uporabniškega vmesnika (GUI) DCM za podpisovanje objektov in preverjanje podpisov omogoča vam in drugim uporabnikom v podjetju preprosto in hitro izvajanje teh nalog.
- Uporaba DCM za podpisovanje objektov in preverjanje podpisov zmanjša čas, potreben za razumevanje in uporabo podpisovanja objektov kot dela zaščitne strategije.
- Uporaba potrdila, ki ga izda lokalna služba za pooblastila (CA) za podpisovanje objektov, zmanjša stroške podpisovanja objektov.

Cilji

V tem scenariju želite digitalno podpisati nezaščitene objekte kot so programi cgi-bin, ki ustvarjajo obrazce na javnem strežniku podjetja iSeries. Kot skrbnik sistema v podjetju MyCo, Inc. želite s pomočjo Upravljalnika digitalnih potrdil (DCM) podpisati te objekte in preveriti njihove podpise.

Cilji tega scenarija so naslednji:

- Aplikacije podjetja in drugi nezaščiteni objekti na javnem spletnem strežniku (iSeries B) morajo biti podpisani s potrdilom lokalnega CA, da se omejijo stroški podpisovanja aplikacij.
- Skrbniki sistema in drugi določeni uporabniki morajo imeti zmožnost preprostega preverjanja digitalnih podpisov na strežnikih iSeries, da preverijo izvor in pristnost podpisanih objektov podjetja. Za dosego tega mora imeti vsak strežnik iSeries kopijo potrdila za preverjanje podpisa podjetja in potrdilo lokalne službe za pooblastila (CA) v prostoru za potrdila *SIGNATUREVERIFICATION vsakega strežnika.
- S preverjanjem podpisov v aplikacijah podjetja in drugih objektih iSeries lahko skrbniki in drugi uporabniki odkrijejo, ali je bila vsebina objektov spremenjena, odkar so bili podpisani.
- Skrbnik sistema mora uporabiti DCM za podpisovanje objektov; skrbnik sistema in drugi uporabniki morajo imeti zmožnost za uporabo DCM za preverjanje podpisov objektov.

Podrobnosti

Naslednja slika ilustrira postopek podpisovanja objekta in preverjanja podpisa za izvedbo tega scenarija:

Slika ilustrira naslednje točke, pomembne za ta scenarij:

iSeries A

- Na iSeries A se izvaja OS/400 različice 5 izdaje 2 (V5R2).
- iSeries A je notranji produkcijski strežnik podjetja in razvijalska platforma za javni spletni strežnik iSeries (iSeries B).
- Na iSeries A je nameščen 128-bitni ponudnik šifriranega dostopa za iSeries (5722–AC3).
- Na iSeries A je nameščen in konfiguriran Upravljalnik digitalnih potrdil (OS/400 možnost 34) in strežnik IBM HTTP (5722–DG1).
- iSeries A deluje kot lokalna služba za pooblastila (CA) in potrdilo za podpisovanje objektov je v tem sistemu.
- iSeries A uporablja DCM za podpisovanje objektov in je primarni sistem za podpisovanje objektov za javne aplikacije in druge objekte podjetja.
- iSeries A je konfiguriran tako, da omogoča preverjanje podpisov.

iSeries B

- Na iSeries B se izvaja OS/400 različice 5 izdaje 1 (V5R1).
- iSeries B je zunanji javni spletni strežnik podjetja izven požarnega zidu podjetja.
- Na iSeries B je nameščen 128-bitni ponudnik šifriranega dostopa (5722–AC3).
- Na iSeries B je nameščen in konfiguriran Upravljalnik digitalnih potrdil (OS/400 možnost 34) in strežnik IBM HTTP (5722–DG1).
- iSeries B ne deluje kot lokalni CA, niti ne podpisuje objektov.
- iSeries B je konfiguriran tako, da omogoča preverjanje podpisov s pomočjo DCM z izdelavo prostora za potrdila *SIGNATUREVERIFICATION in uvoza potrebnega potrdila za preverjanje in potrdila lokalnega CA.
- DCM se uporablja za preverjanje podpisov v objektih.

Predpogoji in predpostavke

Ta scenarij je odvisen od naslednjih predpogojev in predpostavk:

1. Vsi strežniki iSeries ustrezajo zahtevam za namestitev in uporabo Upravljalnika digitalnih potrdil (DCM).
2. Nihče ni predhodno konfiguriral ali uporabil DCM na nobenem strežniku iSeries.

3. Na vseh strežnikih iSeries je nameščen licenčni program 128-bitnega ponudnika šifriranega dostopa (5722-AC3) najvišje ravni.
4. Privzeta nastavitev za preverjanje podpisov objektov med sistemsko vrednostjo za obnovitev (QVFYOBJRST) na vseh strežnikih scenarijev iSeries je 3 in ni bila spremenjena. Privzeta nastavitev zagotavlja, da lahko strežnik preveri podpise objektov pri obnovitvi podpisanih objektov.
5. Skrbnik sistema za iSeries A mora imeti posebno pooblastilo *ALLOBJ za podpisovanje objektov ali pa mora biti profil uporabnika pooblaščen za aplikacijo podpisovanja objektov.
6. Skrbnik sistema ali katerikoli drugi uporabnik, ki izdela prostor za potrdila v DCM, mora imeti posebni pooblastili *SECADM in *ALLOBJ.
7. Skrbnik sistema ali drugi uporabniki na vseh drugih strežnikih iSeries morajo imeti posebno pooblastilo *AUDIT za preverjanje podpisov objektov.

Koraki naloge

Za izvedbo tega scenarija obstajata dva niza nalog, ki jih morate izvesti: en niz nalog omogoča, da konfigurirate iSeries A kot lokalno službo za pooblastila (CA) ter podpišete objekte in preverite njihove podpise. Drug niz nalog omogoča, da konfigurirate iSeries B za preverjanje podpisov objektov, ki jih izdela iSeries A.

Koraki za nalogo **iSeries A**

Za izdelavo zasebnega lokalnega CA in za podpisovanje objektov in preverjanje njihovih podpisov kot opisuje scenarij, morate končati vse od naslednjih nalog na iSeries A:

1. Opravite vse predpogojne korake za namestitev in konfigurirajte vse potrebne izdelke iSeries.
2. S pomočjo Upravljalnika digitalnih potrdil (DCM) izdelajte lokalno službo za pooblastila (CA), ki bo izdala potrdilo za podpis objekta.
3. S pomočjo DCM izdelajte definicijo aplikacije.
4. S pomočjo DCM dodelite potrdilo definiciji aplikacije za podpisovanje objektov.
5. S pomočjo DCM podpišite programske objekte cgi-bin.
6. S pomočjo DCM izvozite potrdila, ki jih morajo uporabiti drugi sistemi za preverjanje podpisov objektov. V datoteko morate izvoziti kopijo potrdila lokalnega CA in kopijo potrdila za podpisovanje objektov.
7. Prenesite datoteke potrdil na javni strežnik iSeries podjetja (iSeries B), tako da boste lahko vi in drugi uporabniki preverjali podpise, ki jih izdela iSeries A.

Koraki za nalogo **iSeries B**

Če nameravate obnoviti podpisane objekte, ki jih v tem scenariju prenesete na javni spletni strežnik (iSeries B), opravite te konfiguracijske naloge za preverjanje podpisov na iSeries B, preden prenesete podpisane objekte. Konfiguracija preverjanja podpisov mora biti končana, preden lahko uspešno preverite podpise pri obnovitvi podpisanih objektov na javnem spletnem strežniku.

Na iSeries B morate opraviti naslednje naloge za preverjanje podpisov objektov kot opisuje ta scenarij:

8. S pomočjo Upravljalnika digitalnih potrdil Manager (DCM) izdelajte prostor za potrdila *SIGNATUREVERIFICATION.
9. S pomočjo DCM uvozite potrdilo lokalnega CA in potrdilo za preverjanje podpisa.
10. S pomočjo DCM preverite podpise v prenesenih objektih.

Podrobnosti konfiguracije

Dokončajte naslednje korake naloge, da boste konfigurirali in uporabili Upravljalnik digitalnih potrdil za podpisovanje objektov kot opisuje ta scenarij.

1. korak: Opravite vse predpogojne korake

Preden lahko opravite določene konfiguracijske naloge za izvedbo tega scenarija, morate opraviti vse predpogojne naloge za namestitev in konfiguracijo vseh potrebnih izdelkov iSeries.

2. korak: Izdelajte lokalno službo za pooblastila, ki bo izdala zasebno potrdilo za podpis objekta

Če uporabite za izdelavo lokalne službe za pooblastila (CA) Upravljalnik digitalnih potrdil (DCM), postopek zahteva, da izpolnite niz obrazcev. Ti obrazci vas vodijo skozi postopek izdelave službe za pooblastila in dokončanje drugih nalog, potrebnih za začetek uporabe potrdil za plast zaščitenih vtičnic (SSL), podpisovanje objektov in preverjanje podpisov. Čeprav v tem scenariju ni potrebno konfigurirati potrdil za SSL, morate izpolniti vse obrazce v nalogi konfiguriranja sistema za podpisovanje objektov.

Takole s pomočjo DCM izdelate in vodite lokalno službo za pooblastila:

1. Zaženite DCM.
2. V oknu za usmerjanje DCM izberite **Izdelaj službo za pooblastila (CA)**, da boste prikazali niz obrazcev.

   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. Izpolnite vse obrazce za to vodeno nalogo. Pri izvedbi te naloge morate narediti naslednje:
   a. Podati določevalne informacije za lokalni CA.
   b. Namestiti potrdilo lokalnega CA v brskalnik, da lahko programska oprema prepozna lokalni CA in preveri veljavnost potrdil, ki jih izda lokalni CA.
   c. Podati podatke načel za lokalni CA.
   d. Uporabiti nov lokalni CA za izdajo potrdila strežnika ali odjemalca, ki ga lahko uporabijo vaše aplikacije za povezave SSL.

      Opomba: Čeprav v tem scenariju to potrdilo ni uporabljeno, ga morate izdelati, preden lahko uporabite lokalni CA za izdajanje potrebnega potrdila za podpisovanje objektov. Če prekinete nalogo, ne da bi izdelali to potrdilo, morate izdelati potrdilo za podpisovanje objektov in prostor za potrdila *OBJECTSIGNING, v katerem je ločeno shranjen.
   e. Izbrati aplikacije, ki lahko uporabljajo potrdilo strežnika ali odjemalca za povezave SSL.

      Opomba: Za namen tega scenarija ne izberite nobene aplikacije in kliknite **Nadaljuj**, da boste prikazali naslednji obrazec.
   f. Uporabiti nov lokalni CA za izdajo potrdila za podpisovanje objektov, ki ga lahko uporabijo 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.
   g. Izbrati aplikacije, ki bodo zaupale lokalnemu CA.

      Opomba: Za namen tega scenarija ne izberite nobene aplikacije in kliknite **Nadaljuj**, da boste končali nalogo.

Zdaj ko ste izdelali lokalni CA in potrdilo za podpisovanje objektov, morate definirati aplikacijo za podpisovanje objektov, ki bo uporabila potrdilo, preden lahko podpišete objekte.

3. korak: Izdelava definicije aplikacije za podpisovanje objektov

Ko izdelate potrdilo za podpisovanje objektov, morate s pomočjo Upravljalnika digitalnih potrdil (DCM) definirati aplikacijo za podpisovanje objektov, ki jo lahko uporabite za podpisovanje objektov. Za definicijo aplikacije ni nujno, da se nanaša na dejansko aplikacijo; definicija aplikacije, ki jo izdelate, mora opisovati tip ali skupino objektov, ki jih nameravate podpisati. Definicijo potrebujete, da lahko povežete ID aplikacije s potrdilom in omogočite postopek podpisovanja.

Takole s pomočjo DCM izdelajte definicijo aplikacije za podpisovanje objektov:

1. V okvirju za usmerjanje kliknite **Izberi prostor za potrdila** in izberite ***OBJECTSIGNING** kot prostor za potrdila, ki ga želite odpreti.
2. Ko se prikaže stran Prostor za potrdila in geslo, podajte geslo, ki ste ga podali za prostor za potrdila pri njegovi izdelavi in kliknite **Nadaljuj**.
3. V okvirju za usmerjanje izberite **Upravljanje aplikacij**, da boste prikazali seznam nalog.
4. S seznama nalog izberite **Dodaj aplikacijo**, da boste prikazali obrazec za definiranje aplikacije.
5. Izpolnite obrazec in kliknite **Dodaj**.

Zdaj morate dodeliti potrdilo za podpisovanje objektov aplikaciji, ki ste jo izdelali.

4. korak: Dodelitev potrdila definiciji aplikacije za podpisovanje objektov

Takole dodelite potrdilo aplikaciji za podpisovanje objektov:

1. V okvirju za usmerjanje DCM izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
2. S seznama nalog izberite **Dodeli potrdilo**, da boste prikazali seznam potrdil za trenutni prostor za potrdila.
3. S seznama izberite potrdilo in kliknite **Dodeli aplikacijam**, da boste prikazali seznam definicij aplikacij za trenutni prostor za potrdila.
4. S seznama izberite eno ali več aplikacij in kliknite **Nadaljuj**. Prikaže se sporočilna stran, na kateri potrdite dodelitev potrdila, ali poda informacije o napaki, če je prišlo do kakšne težave.

Ko končate to nalogo, lahko začnete uporabljati DCM za podpisovanje programskih objektov, ki jih bo uporabljal javni spletni strežnik (iSeries B) podjetja.

5. korak: Podpisovanje programskih objektov

Takole uporabite DCM za podpisovanje programskih objektov, ki bodo uporabljeni na javnem spletnem strežniku (iSeries B) podjetja:

1. V okvirju za usmerjanje kliknite **Izberi prostor za potrdila** in izberite ***OBJECTSIGNING** kot prostor za potrdila, ki ga želite odpreti.
2. Vnesite geslo prostora za potrdila *OBJECTSIGNING in kliknite **Nadaljuj**.
3. Ko se okno za usmerjanje osveži, izberite **Upravljanje objektov, ki jih je mogoče podpisati**, da boste prikazali seznam nalog.
4. S seznama nalog izberite **Podpiši objekt**, da boste prikazali seznam definicij aplikacij, ki jih lahko uporabite za podpisovanje objektov.
5. Izberite aplikacijo, ki ste jo definirali v prejšnjem koraku in kliknite **Podpiši objekt**. Prikaže se obrazec, na katerem lahko podate mesto objektov, ki jih želite podpisati.
6. V prikazano polje vnesite celotno pot in ime datoteke objekta ali imenika objektov, ki jih želite podpisati, in kliknite **Nadaljuj**. Vnesete lahko tudi mesto imenika in kliknete **Preglej**, da boste prikazali vsebino imenika in izbrali objekte za podpisovanje.

   Opomba: Na začetku imena objekta mora biti poševnica, sicer bo prišlo do napake. Za opis dela imenika, ki ga želite podpisati, lahko uporabite tudi univerzalna znaka. 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. Univerzalna znaka lahko uporabite samo v zadnjem delu poti; če na primer vpišete /mydirectory*/filename, bo prišlo do napake. Če želite za prikaz seznama vsebine knjižnic ali imenikov uporabiti funkcijo Preglej, vnesite univerzalni znak kot del imena poti preden kliknete **Preglej**.

7. 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, se prikaže datoteka z rezultati neposredno v brskalniku. Rezultati za trenutno opravilo so pripeti na konec datoteke rezultatov. Posledično lahko vsebuje datoteka poleg rezultatov trenutnega opravila tudi rezultate iz prejšnjih opravil. S pomočjo datumskega polja v datoteki lahko določite, katere vrstice v datoteki se nanašajo na trenutno opravilo. Datumsko polje ima format LLLLMMDD. Prvo polje v datoteki je lahko ID sporočila (če je prišlo med obdelavo objekta do napake) ali datumsko polje (ki kaže datum obdelave opravila).
8. Podajte celotno pot in ime datoteke, ki bo uporabljena za shranitev rezultatov opravila operacije podpisovanja objekta in kliknite **Nadaljuj**. Vnesete lahko tudi mesto imenika in kliknete **Preglej**, da boste prikazali vsebino imenika in izbrali datoteko za shranitev rezultatov opravila. Prikaže se sporočilo, ki kaže, da je bilo predloženo opravilo za podpis objektov. Če si želite ogledati rezultate opravila, poiščite v dnevniku opravil opravilo **QOBJSGNBAT**.

Če želite zagotoviti, da boste lahko preverjali podpise, morate izvoziti potrebna potrdila v datoteko in prenesti datoteko potrdil na iSeries B. Dokončati morate tudi vse konfiguracijske naloge za preverjanje podpisov na iSeries B, preden prenesete podpisane programske objekte na iSeries B. Konfiguracija preverjanja podpisov mora biti končana, preden lahko uspešno preverite podpise pri obnovitvi podpisanih objektov iSeries B.

6. korak: Izvoz potrdil za omogočanje preverjanja podpisov na iSeries B

Podpisovanje objektov za zaščito integritete vsebine zahteva, da imati vi in drugi uporabniki na voljo sredstva za preverjanje pristnosti podpisa. Če želite preveriti podpise v istem sistemu, ki podpiše objekte (iSeries A), morate s pomočjo DCM izdelati prostor za potrdila *SIGNATUREVERIFICATION. Ta prostor za potrdila mora vsebovati kopijo potrdila za podpisovanje objektov in kopijo potrdila službe za pooblastila, ki je izdala potrdilo.

Če želite drugim uporabnikom omogočiti preverjanje podpisov, jim morate posredovati kopijo potrdila, ki je podpisalo objekt. Če izdate potrdilo s pomočjo lokalne službe za pooblastila (CA), jim morate posredovati tudi kopijo potrdila lokalne službe za pooblastila.

Naslednji koraki kažejo, kako uporabiti DCM za preverjanje podpisov v istem sistemu, ki podpiše objekte (v tem scenariju je to iSeries A):

1. V okvirju za usmerjanje izberite **Izdelaj nov prostor za potrdila** in izberite ***SIGNATUREVERIFICATION** kot prostor za potrdila, ki ga želite izdelati.
2. Izberite **Da**, da boste prekopirali obstoječa potrdila za podpisovanje objektov v nov prostor za potrdila kot potrdila za preverjanje podpisov.
3. Podajte geslo novega prostora za potrdila in kliknite **Nadaljuj**, da boste izdelali prostor za potrdila. Zdaj lahko s pomočjo DCM preverite podpise objektov v istem sistemu, ki ga uporabite za podpisovanje objektov.

Naslednji koraki kažejo, kako s pomočjo DCM izvoziti kopijo potrdila lokalne službe za pooblastila in kopijo potrdila za podpisovanje objektov kot potrdila za preverjanje podpisov, tako da lahko preverite podpise objektov v drugih sistem (iSeries B):

1. V okvirju za usmerjanje izberite **Upravljanje potrdil**, nato pa izberite nalogo **Izvozi potrdilo**.
2. Izberite **Služba za pooblastila (CA)** in kliknite **Nadaljuj**, da boste prikazali seznam potrdil CA, ki jih lahko izvozite.
3. S seznama izberite predhodno izdelano potrdilo lokalne službe za pooblastila in kliknite **Izvozi**.
4. Za cilj izvoza podajte **Datoteka** in kliknite **Nadaljuj**.

5. Podajte celotno pot in ime datoteke za izvoženo potrdilo lokalne službe za pooblastila in kliknite **Nadaljuj**, da boste izvozili potrdilo.
6. Za izhod s potrditeveni strani za izvoz kliknite **Potrdi**. Zdaj lahko izvozite kopijo potrdila za podpisovanje objektov.
7. Znova izberite nalogo **Izvozi potrdilo**.
8. Izberite **Podpisovanje objektov**, da boste prikazali seznam potrdil za podpisovanje objektov, ki jih lahko izvozite.
9. S seznama izberite ustrezno potrdilo za podpisovanje objektov in kliknite **Izvozi**.
10. Za cilj izberite **Datoteka, kot potrdilo za preverjanje podpisov** in kliknite **Nadaljuj**.
11. Podajte celotno pot in ime datoteke izvoženega potrdila za preverjanje podpisov in kliknite **Nadaljuj**, da boste izvozili potrdilo.

Zdaj lahko prenesete te datoteke v sisteme zaključnih točk iSeries, v katerih nameravate preveriti podpise, ki ste jih izdelali s potrdilom.

7. korak: Prenos datotek potrdil na javni strežnik podjetja iSeries B

Preden lahko konfigurirate datoteke potrdil za preverjanje objektov, ki jih podpišete, jih morate prenesti iz iSeries A na iSeries B, ki je v tem scenariju javni spletni strežnik podjetja. Za prenos datotek potrdil lahko uporabite več različnih načinov. Uporabite lahko na primer FTP (File Transfer Protocol) ali razpošiljanje paketov Osrednjega upravljanja.

8. korak: Naloge preverjanja podpisov: Izdelava prostora za potrdila *SIGNATUREVERIFICATION

Če želite preveriti podpise objektov na iSeries B (javni spletni strežnik podjetja), mora vsebovati iSeries B v prostoru za potrdila *SIGNATUREVERIFICATION ustrezno potrdilo za preverjanje podpisov. Ker ste za podpis objektov uporabili lokalno izdano potrdilo, mora ta prostor za potrdila vsebovati tudi kopijo potrdila lokalne službe za pooblastila.

Takole izdelate prostor za potrdila *SIGNATUREVERIFICATION:

1. Zaženite DCM.
2. V oknu za usmerjanje Upravljalnika digitalnih potrdil (DCM) izberite **Izdelaj nov prostor za potrdila** in za izdelavo izberite prostor za potrdila ***SIGNATUREVERIFICATION**.

   Opomba: Če imate vprašanja o izpolnitvi določenega obrazca med uporabo DCM, izberite vprašaj (**?**) na vrhu strani, da boste dostopili do zaslonske pomoči.
3. Podajte geslo novega prostora za potrdila in kliknite **Nadaljuj**, da boste izdelali prostor za potrdila. Zdaj lahko uvozite potrdila v prostor za potrdila in jih uporabite za preverjanje podpisov objektov.

9. korak: Naloge preverjanja podpisov: Uvoz potrdil

Če želite preveriti podpis objekta, mora vsebovati prostor za potrdila *SIGNATUREVERIFICATION kopijo potrdila za preverjanje podpisov. Če je potrdilo za podpisovanje zasebno, mora vsebovati ta prostor za potrdila tudi kopijo potrdila lokalne službe za pooblastila, ki je izdala potrdilo za podpisovanje. V tem scenariju smo izvozili obe potrdili v datoteko, ta datoteka pa je bila prenesena v sisteme zaključnih točk iSeries.

Takole uvozite ti potrdili v prostor za potrdila *SIGNATUREVERIFICATION:

1. V okvirju za usmerjanje DCM kliknite **Izberi prostor za potrdila** in za odpiranje izberite prostor za potrdila ***SIGNATUREVERIFICATION**.

2. Ko se prikaže stran Prostor za potrdila in geslo, podajte geslo, ki ste ga podali za prostor za potrdila pri njegovi izdelavi in kliknite **Nadaljuj**.
3. Ko se okvir za usmerjanje osveži, izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
4. S seznama nalog izberite **Uvozi potrdilo**.
5. Kot tip potrdila izberite **Služba za pooblastila (CA)** in kliknite **Nadaljuj**.

   Opomba: Potrdilo lokalne službe za pooblastila morate uvoziti preden uvozite zasebno potrdilo za preverjanje podpisov, sicer postopek uvoza potrdila za preverjanje podpisov ne bo uspel.
6. Podajte celotno pot in ime datoteke, ki vsebuje potrdilo CA, in kliknite **Nadaljuj**. Prikaže se sporočilo, ki potrdi, da se je postopek uvoza uspešno končal, ali poda informacije o napaki, če postopek ne uspe.
7. Znova izberite nalogo **Uvozi potrdilo**.
8. Kot tip potrdila izberite **Preverjanje podpisa** in kliknite **Nadaljuj**.
9. Podajte celotno pot in ime datoteke potrdila za preverjanje podpisov in kliknite **Nadaljuj**. Prikaže se sporočilo, ki potrdi, da se je postopek uvoza uspešno končal, ali poda informacije o napaki, če postopek ne uspe.

Zdaj lahko s pomočjo DCM na iSeries B preverite podpise objektov, ki ste jih izdelali z ustreznim potrdilom za podpisovanje na iSeries A.

10. korak: Naloge preverjanja podpisov: Preverjanje podpisov programskih objektov

Takole s pomočjo DCM preverite podpise v prenesenih programskih objektih:

1. V okvirju za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje izberite prostor za potrdila ***SIGNATUREVERIFICATION**.
2. Vnesite geslo prostora za potrdila *SIGNATUREVERIFICATION in kliknite **Nadaljuj**.
3. Ko se okno za usmerjanje osveži, izberite **Upravljanje objektov, ki jih je mogoče podpisati**, da boste prikazali seznam nalog.
4. S seznama nalog izberite **Preveri podpis objekta** in podajte mesto objektov, za katere želite preveriti podpise.
5. V podano polje vnesite celotno pot in ime datoteke objekta ali imenika objektov, za katere želite preveriti podpise, in kliknite **Nadaljuj**. Vnesete lahko tudi mesto imenika in kliknete **Preglej**, da boste prikazali vsebino imenika in izbrali objekte za preverjanje podpisov.

   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; če na primer vpišete /mydirectory*/filename, bo prišlo do napake. Če želite za prikaz seznama vsebine knjižnic ali imenikov uporabiti funkcijo Preglej, vnesite univerzalni znak kot del imena poti preden kliknete **Preglej**.
6. Izberite možnosti obdelave, ki jih želite uporabiti za preverjanje podpisa v izbranem objektu ali objektih, in kliknite **Nadaljuj**.

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

7. Podajte celotno pot in ime datoteke, ki bo uporabljena za shranjevanje rezultatov opravila za operacijo preverjanja podpisa in kliknite **Nadaljuj**. Vnesete lahko tudi mesto imenika in kliknete **Preglej**, da boste prikazali vsebino imenika in izbrali datoteko, v katero boste shranili rezultate opravila. Prikaže se sporočilo, ki kaže, da je bilo predloženo opravilo za preverjanje podpisov objektov. Če si želite ogledati rezultate opravila, poiščite v dnevniku opravil opravilo **QOBJSGNBAT**.

Scenarij: Uporaba API-jev za podpisovanje objektov in preverjanje njihovih podpisov

Stanje

Vaše podjetje (MyCo, Inc.) je poslovni partner iSeries, ki razvija aplikacije za uporabnike. Kot razvijalec programske opreme v podjetju ste odgovorni za pripravo teh aplikacij, tako da bodo poslane strankam. Za pakiranje aplikacije trenutno uporabljate programe. Stranke lahko naročijo zgoščenko (CD-ROM) ali obiščejo vaše spletno mesto in presnamejo aplikacijo.

Stran ohranjate ažurno z novicami, ki so še posebej namenjene zaščiti. Posledično veste, da stranke skrbi izvor in vsebina programov, ki jih prejmejo ali presnamejo. Včasih se zgodi, da stranke menijo, da so prejele ali presnele izdelek iz preverjanega izvora, za katerega pa se izkaže, da ni resničen vir izdelka. Zaradi tega se lahko zgodi, da stranke ne namestijo izdelka, ki so ga pričakovale. Ta nameščeni program je lahko zlonameren ali pa je bil spremenjen in okvari sistem.

Čeprav te težave niso pogoste pri strankah iSeries, jim želite zagotoviti, da aplikacije, ki jih prejmejo, resnično izvirajo iz vašega podjetja. Strankam želite tudi omogočiti, da preverijo integriteto teh aplikacij, da lahko pred namestitvijo določijo, ali so bile spremenjene.

Na osnovi raziskav, ki ste jih opravili, ste se odločili, da lahko za dosego ciljev zaščite uporabite funkcije podpisovanja objektov OS/400. Z digitalnim podpisovanjem aplikacij strankam omogočite, da preverijo, da je vaše podjetje zakonit izvor aplikacije, ki jo prejmejo ali presnamejo. Ker trenutno pakirate aplikacije programsko, ste se odločili, da boste s pomočjo API-jev preprosto dodali podpisovanje objektov obstoječim postopkom pakiranja. Odločili ste se tudi, da boste za podpisovanje objektov uporabili javno potrdilo, da bo postopek preverjanja podpisa transparenten za vaše stranke, ki bodo nameščale izdelek.

Kot del aplikacijskega paketa vključite kopijo digitalnega potrdila, s katerim ste podpisali objekt. Ko stranka prejme aplikacijski paket, lahko s pomočjo javnega ključa potrdila preveri podpis aplikacije. Ta postopek stranki omogoča, da določi in preveri izvor aplikacije, kot tudi zagotovi, da vsebina aplikacijskih objektov ni bila spremenjena, odkar so bili podpisani.

Ta zgled služi kot koristen uvod v korake, ki so vključeni v programsko podpisovanje objektov za aplikacije, ki jih razvijete in zapakirate za druge uporabnike.

Prednosti scenarija

S tem scenarijem so povezane naslednje prednosti:

- Uporaba API-jev za programsko pakiranje in podpisovanje objektov zmanjša čas, ki je potreben za izvedbo te vrste zaščite.
- Uporaba API-jev za podpisovanje objektov pri njihovem pakiranju zmanjša število korakov, ki jih morate opraviti za podpis objektov, ker je postopek podpisovanja del postopka pakiranja.
- S podpisom paketa objektov lahko preprosteje določite, ali so bili objekti od podpisa spremenjeni. S tem zmanjšate tudi del odpravljanja težav, ki bi ga bilo potrebno opraviti v bodoče, da bi za stranke določili, kje v aplikaciji je težava.
- Uporaba potrdila znane javne službe za pooblastila (CA) za podpisovanje objektov omogoča, da uporabite API Dodaj verifikator kot del izhodnega programa v namestitvenem programu izdelka. Ta API

omogoča, da v sistem stranke samodejno dodate javno potrdilo, ki ste ga uporabili za podpis aplikacije. S tem zagotovite, da je preverjanje podpisa transparentno za stranke.

Cilji

V tem scenariju želi podjetje MyCo, Inc. programsko podpisati aplikacije, ki jih pakira in pošlje svojim strankam. Kot razvijalec aplikacij v MyCo, Inc. trenutno pakirate aplikacije podjetja programsko in jih nato pošljete strankam. Posledično želite s pomočjo API-jev iSeries podpisati aplikacije in omogočiti, da stranke iSeries programsko preverijo podpis med namestitvijo izdelka.

Cilji tega scenarija so naslednji:

- Razvijalec podjetja lahko podpiše objekte s pomočjo API-ja Podpisovanje objektov kot dela obstoječega programskega pakiranja aplikacij.
- Aplikacije podjetja morajo biti podpisane z javnim potrdilom, da se zagotovi, da je postopek preverjanja podpisa transparenten za stranke med postopkom nameščanja aplikacije.
- Podjetje lahko s pomočjo API-jev iSeries programsko doda zahtevano potrdilo za preverjanje podpisa v prostor za potrdila *SIGNATUREVERIFICATION strežnika iSeries. Podjetje lahko programsko izdela ta prostor za potrdila na strežniku iSeries stranke kot del namestitvenega postopka izdelka, v primeru, da le-ta še ne obstaja.
- Stranke lahko preprosto preverijo digitalne podpise v aplikaciji podjetja po namestitvi izdelka. Stranke lahko preverijo podpis in določijo izvor in pristnost podpisane aplikacije, kot tudi določijo, ali je bila v aplikaciji od podpisa opravljena kakšna sprememba.

Podrobnosti

Naslednja slika ilustrira postopek podpisovanja objekta in preverjanja podpisa za izvedbo tega scenarija:

Slika ilustrira naslednje točke, pomembne za ta scenarij:

Osrednji sistem (iSeries A)

- Na iSeries A se izvaja OS/400 različice 5 izdaje 2 (V5R2).
- Na iSeries A se izvaja program za pakiranje izdelkov razvijalca aplikacij.
- Na iSeries A je nameščen 128-bitni ponudnik šifriranega dostopa za iSeries (5722–AC3).
- Na iSeries A je nameščen in konfiguriran Upravljalnik digitalnih potrdil (OS/400 možnost 34) in strežnik IBM HTTP (5722–DG1).
- iSeries A je primarni sistem podpisovanja objektov za aplikacijske izdelke podjetja. Podpisovanje objektov izdelka za razpošiljanje uporabnikom opravite na iSeries A z naslednjimi nalogami:
  1. Uporaba API-jev za podpis aplikacijskega izdelka podjetja.
  2. Uporaba DCM za izvoz potrdila za preverjanje podpisa v datoteko, da lahko stranke preverijo podpisane objekte.
  3. Sestava programa za dodajanje potrdila za preverjanje v podpisan aplikacijski izdelek.
  4. Sestava prednamestitvenega izhodnega programa za izdelek, ki uporablja API Dodaj verifikator. Ta API omogoča, da postopek namestitve izdelka programsko doda potrdilo za preverjanje v prostor za potrdila *SIGNATUREVERIFICATION na strežniku iSeries stranke (iSeries B in C).

Strežnika B in C **stranke iSeries**

- Na iSeries B se izvaja OS/400 različice 5 izdaje 2 (V5R2).
- Na iSeries C se izvaja OS/400 različice 5 izdaje 2 (V5R2).
- Na iSeries B in C je nameščen in konfiguriran Upravljalnik digitalnih potrdil (možnost 34) in strežnik IBM HTTP (5722–DG1).

- iSeries B in C kupita in presnameta aplikacijo na spletni strani podjetja za razvijanje aplikacij (ki je lastnik iSeries A).
- iSeries B in C pridobita kopijo potrdila za preverjanje podpisov podjetja MyCo, ko namestitveni postopek aplikacije MyCo izdela prostor za potrdila *SIGNATUREVERIFICATION na vsakem izmed teh strežnikov iSeries stranke.

Predpogoji in predpostavke

Ta scenarij je odvisen od naslednjih predpogojev in predpostavk:

1. Vsi strežniki iSeries ustrezajo zahtevam za namestitev in uporabo Upravljalnika digitalnih potrdil (DCM).

   Opomba: Ustrezanje predpogojem za namestitev in uporabo DCM je izbirna zahteva za stranke (v tem scenariju iSeries B in C). Čeprav API Dodajanje verifikatorja izdela prostor za potrdila *SIGNATUREVERIFICATION kot del namestitvenega postopka izdelka, ga po potrebi izdela s privzetim geslom. Stranke morajo uporabiti DCM, da spremenijo privzeto geslo in zaščitijo ta prostor za potrdila pred nepooblaščenim dostopom.
2. Nihče ni predhodno konfiguriral ali uporabil DCM na nobenem strežniku iSeries.
3. Na vseh strežnikih iSeries je nameščen licenčni program 128-bitnega ponudnika šifriranega dostopa (5722-AC3) najvišje ravni.
4. Privzeta nastavitev za preverjanje podpisov objektov med sistemsko vrednostjo za obnovitev (QVFYOBJRST) na vseh strežnikih scenarijev iSeries je 3 in ni bila spremenjena. Privzeta nastavitev zagotavlja, da lahko strežnik preveri podpise objektov pri obnovitvi podpisanih objektov.
5. Skrbnik omrežja za iSeries A mora imeti profil uporabnik s posebnim pooblastilom *ALLOBJ za podpisovanje objektov, ali pa mora imeti profil uporabnika pooblastilo za uporabo aplikacije za podpisovanje objektov.
6. Skrbnik sistema ali kdorkoli drug (vključno s programom), ki izdela prostor za potrdila v DCM, mora imeti profil uporabnika s posebnima pooblastiloma *SECADM in *ALLOBJ.
7. Skrbniki sistemov ali drugi uporabniki na vseh drugih strežnikih iSeries morajo imeti profil uporabnika s posebnim pooblastilom *AUDIT za preverjanje podpisov objektov.

Koraki naloge

Za podpisovanje objektov, tako kot opisuje ta scenarij, morate končati vse od naslednjih nalog na iSeries A:

1. Opravite vse predpogojne korake za namestitev in konfigurirajte vse potrebne izdelke iSeries.
2. S pomočjo DCM izdelajte zahtevo za potrdilo, da boste pridobili potrdilo za podpisovanje objektov pri znani javni službi za pooblastila (CA).
3. S pomočjo DCM izdelajte definicijo aplikacije za podpisovanje objektov.
4. S pomočjo DCM uvozite podpisano potrdilo za podpisovanje objektov in ga dodelite definiciji aplikacije za podpisovanje objektov.
5. S pomočjo DCM izvozite potrdilo za podpisovanje objektov kot potrdilo za preverjanje podpisov, da ga lahko uporabijo stranke za preverjanje podpisa v aplikacijskih objektih.
6. Znova napišite program za pakiranje aplikacije, tako da bo vključeval datoteko potrdila za preverjanje podpisov kot del izdelka, in uporabil API Podpisovanje izdelka za podpis aplikacije, ko jo boste pakirali za pošiljanje strankam.
7. Izdelajte prednamestitveni izhodni program, ki uporablja API Dodaj verifikator kot del postopka pakiranja aplikacije. Ta izhodni program omogoča, da izdelate prostor za potrdila *SIGNATUREVERIFICATION in dodate zahtevano potrdilo za preverjanje podpisov na strežnik iSeries stranke med namestitvijo izdelka.
8. Stranke naj s pomočjo DCM na novo nastavijo privzeto geslo prostora za potrdila *SIGNATUREVERIFICATION na svojem strežniku iSeries.

Podrobnosti konfiguracije

Dokončajte korake naslednje naloge, da boste uporabili API-je OS/400 za podpisovanje izdelkov, tako kot to opisuje ta scenarij.

1. korak: Opravite vse predpogojne korake

Preden lahko opravite določene konfiguracijske naloge za izvedbo tega scenarija, morate opraviti vse predpogojne naloge za namestitev in konfiguracijo vseh potrebnih izdelkov iSeries.

2. korak: S pomočjo DCM pridobite potrdilo pri znani javni službi za pooblastila

Ta scenarij zahteva, da niste predhodno uporabili Upravljalnika digitalnih potrdil (DCM) za izdelavo in upravljanje potrdil. Posledično morate izdelati prostor za potrdila *OBJECTSIGNING kot del postopka izdelave potrdila za podpisovanje objektov. Ko izdelate ta prostor za potrdila, nudi naloge, ki jih morate opraviti za izdelavo in upravljanje potrdil za podpisovanje objektov. Če želite pridobiti potrdilo znane javne službe za pooblastila (CA), s pomočjo DCM izdelajte določevalne informacije in par javnega in zasebnega ključa potrdila in te informacije predložite službi za pooblastila, ki vam bo izdala potrdilo.

Za izdelavo informacij zahteve za potrdilo, ki jih morate posredovati znani javni službi za pooblastila, da vam bo izdala potrdilo za podpisovanje objektov, opravite naslednje korake:

1. Zaženite DCM.
2. V okvirju za usmerjanje DCM izberite **Izdelaj nov prostor za potrdila**, da boste zagnali vodeno nalogo in izpolnili niz obrazcev. Ti obrazci vas bodo vodili skozi postopek izdelave prostora za potrdila in potrdila, ki ga lahko uporabite 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. Izberite **Da**, da boste izdelali potrdilo kot del izdelave prostora za potrdila *OBJECTSIGNING in kliknite **Nadaljuj**.
5. Kot podpisnik novega potrdila izberite **VeriSign ali drugo internetno službo za pooblastila (CA)** in kliknite **Nadaljuj**, da boste prikazali obrazec, na katerem lahko podate določevalne informacije za novo potrdilo.
6. Izpolnite obrazec in kliknite **Nadaljuj**, da boste prikazali potrditveno stran. Na tej potrditveni strani so prikazani podatki zahteve za potrdilo, ki jih morate posredovati javni službi za pooblastila (CA), ki vam bo izdala 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 na prošnjo za potrdilo ali v ločeno datoteko, ki jo zahteva javna služba za pooblastila za potrdilo. Uporabiti morate vse podatke CSR, vključno z vrsticama Begin in End New Certificate Request. Ko zaprete to stran, podatke izgubite in jih ne morete več obnoviti.
8. Prošnjo ali datoteko pošljite službi za pooblastilo, ki ste jo izbrali za podpis potrdila.
9. Preden nadaljujete z naslednjim korakom v tem scenariju, počakajte, da vam služba za pooblastila vrne podpisano, izpolnjeno potrdilo.

3. korak: Izdelava definicije aplikacije za podpisovanje objektov

Ko pošljete zahtevo za potrdilo znani javni službi za pooblastila, lahko s pomočjo DCM definirate aplikacijo za podpisovanje objektov, ki jo boste uporabili za podpisovanje objektov. Za definicijo aplikacije ni nujno, da se nanaša na dejansko aplikacijo; definicija aplikacije, ki jo izdelate, mora opisovati tip ali skupino objektov, ki jih nameravate podpisati. Definicijo potrebujete, da lahko povežete ID aplikacije s potrdilom in omogočite postopek podpisovanja.

Takole s pomočjo DCM izdelajte definicijo aplikacije za podpisovanje objektov:

1. V okvirju za usmerjanje kliknite **Izberi prostor za potrdila** in izberite ***OBJECTSIGNING** kot prostor za potrdila, ki ga želite odpreti.
2. Ko se prikaže stran Prostor za potrdila in geslo, podajte geslo, ki ste ga podali za prostor za potrdila pri njegovi izdelavi in kliknite **Nadaljuj**.
3. V okvirju za usmerjanje izberite **Upravljanje aplikacij**, da boste prikazali seznam nalog.
4. S seznama nalog izberite **Dodaj aplikacijo**, da boste prikazali obrazec za definiranje aplikacije.
5. Izpolnite obrazec in kliknite **Dodaj**.

Ko vam služba za pooblastila vrne podpisano potrdilo, ga lahko dodelite aplikaciji, ki ste jo izdelali.

4. korak: Uvoz podpisanega javnega potrdila in njegova dodelitev aplikaciji za podpisovanje objektov

Takole uvozite potrdilo in ga dodelite aplikaciji, da omogočite podpisovanje objektov:

1. Zaženite DCM.
2. V okvirju za usmerjanje kliknite **Izberi prostor za potrdila** in izberite ***OBJECTSIGNING** kot prostor za potrdila, ki ga želite odpreti.
3. Ko se prikaže stran Prostor za potrdila in geslo, podajte geslo, ki ste ga podali za prostor za potrdila pri njegovi izdelavi in kliknite **Nadaljuj**.
4. Ko se okvir za usmerjanje osveži, izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
5. S seznama nalog izberite **Uvozi potrdilo**, da boste začeli postopek uvažanje podpisanega potrdila v prostor za potrdila.

   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.
6. S seznama nalog **Upravljanje potrdil** izberite **Dodeli potrdilo**, da boste prikazali seznam potrdil za trenutni prostor za potrdila.
7. S seznama izberite potrdilo in kliknite **Dodeli aplikacijam**, da boste prikazali seznam definicij aplikacij za trenutni prostor za potrdila.
8. S seznama izberite aplikacijo in kliknite **Nadaljuj**. Prikaže se stran s potrditvenim sporočilom za izbiro dodelitve ali s sporočilom o napaki, če je prišlo do težave.

Ko končate to naloge, lahko začnete podpisovati aplikacije in druge objekte s pomočjo API-jev OS/400. Toda če želite zagotoviti, da boste vi in drugi uporabniki lahko preverjali podpise, morate izvoziti potrebna potrdila v datoteko in jih prenesti na katerikoli strežnik iSeries, ki namesti vaše podpisane aplikacije. Strežniki iSeries uporabnikov morajo imeti zmožnost uporabe potrdila za preverjanje podpisa aplikacije pri njeni namestitvi. Potrebno konfiguracijo preverjanja podpisov za stranke lahko opravite s pomočjo API-ja Dodaj verifikator kot dela namestitvenega programa aplikacije. Tako lahko na primer izdelate prednamestitveni izhodni program, ki pokliče API Dodaj verifikator in konfigurira strežnik iSeries stranke.

5. korak: Izvoz potrdil za omogočanje preverjanja podpisov na drugih strežnikih iSeries

Podpisovanje objektov zahteva, da imate vi in drugi uporabniki na voljo sredstva za preverjanje pristnosti podpisa in njegove uporabe za določitev, ali je bila v podpisanih objektih opravljena kakšna sprememba. Če želite preveriti podpise v sistemu, ki podpiše objekte, morate s pomočjo DCM izdelati prostor za potrdila *SIGNATUREVERIFICATION. Ta prostor za potrdila mora vsebovati kopijo potrdila za podpisovanje objektov in kopijo potrdila službe za pooblastila, ki je izdala potrdilo.

Če želite drugim uporabnikom omogočiti preverjanje podpisov, jim morate posredovati kopijo potrdila, ki je podpisalo objekt. Če izdate potrdilo s pomočjo lokalne službe za pooblastila (CA), jim morate posredovati tudi kopijo potrdila lokalne službe za pooblastila.

Naslednji koraki kažejo, kako uporabiti DCM za preverjanje podpisov v istem sistemu, ki podpiše objekte (v tem scenariju je to iSeries A):

1. V okvirju za usmerjanje izberite **Izdelaj nov prostor za potrdila** in izberite ***SIGNATUREVERIFICATION** kot prostor za potrdila, ki ga želite izdelati.
2. Izberite **Da**, da boste prekopirali obstoječa potrdila za podpisovanje objektov v nov prostor za potrdila kot potrdila za preverjanje podpisov.
3. Podajte geslo novega prostora za potrdila in kliknite **Nadaljuj**, da boste izdelali prostor za potrdila. Zdaj lahko s pomočjo DCM preverite podpise objektov v istem sistemu, ki ga uporabite za podpisovanje objektov.

Takole s pomočjo DCM izvozite kopijo potrdila za podpisovanje objektov kot potrdilo za preverjanje podpisov, da lahko drugi uporabniki preverijo podpise objektov:

1. V okvirju za usmerjanje izberite **Upravljanje potrdil**, nato pa izberite nalogo **Izvozi potrdilo**.
2. Izberite **Podpisovanje objektov**, da boste prikazali seznam potrdil za podpisovanje objektov, ki jih lahko izvozite.
3. S seznama izberite ustrezno potrdilo za podpisovanje objektov in kliknite **Izvozi**.
4. Za cilj izberite **Datoteka, kot potrdilo za preverjanje podpisov** in kliknite **Nadaljuj**.
5. Podajte celotno pot in ime datoteke izvoženega potrdila za preverjanje podpisov in kliknite **Nadaljuj**, da boste izvozili potrdilo.

Zdaj lahko dodate to datoteko v namestitveni paket aplikacije, ki ga izdelate za vaš izdelek. S pomočjo API-ja Dodaj verifikator kot dela namestitvenega programa lahko dodate to potrdilo v prostor za potrdila *SIGNATUREVERIFICATION stranke. Če ta prostor za potrdila še ne obstaja, ga bo ta API izdelal. Namestitveni program izdelka lahko nato preveri podpis aplikacijskih objektov, ko jih obnovi na strežnikih iSeries stranke.

6. korak: Ažuriranje pakirnega programa aplikacije za uporabo API-jev iSeries za podpis vaše aplikacije

Zdaj, ko imate datoteko potrdila za preverjanje podpisov, ki jo boste dodali v aplikacijski paket, lahko s pomočjo API-ja Podpiši objekt napišete ali popravite obstoječo aplikacijo, tako da bo podpisala knjižnice izdelka, ko jih boste pakirali.

Da boste bolje razumeli, kako uporabiti API Podpiši objekt kot del pakirnega programa aplikacije, si oglejte naslednjo vzorčno kodo. Ta del vzorčne kode, napisane v jeziku C, ni popoln program za podpisovanje in pakiranje, pač pa samo zgled dela takšnega programa, ki pokliče API Podpiši objekt. Če se odločite, da boste uporabili ta vzorčni program, ga prilagodite svojim potrebam. Zaradi varnostnih razlogov IBM priporoča, da specificirate vzorčni program, namesto da bi uporabili podane privzete vrednosti.

Opomba: IBM vam daje neizključno licenco za avtorske pravice za uporabo vseh zgledov programske kode, iz katere lahko ustvarite podobne funkcije, ki jih prilagodite lastnim potrebam. IBM nudi celotno vzorčno kodo zgolj za ilustrativne namene. Ti zgledi niso bili natančno preizkušeni v vseh pogojih. IBM zato ne more zagotoviti zanesljivosti, uporabnosti ali delovanja teh programov. Vsi programi, vsebovani v tem dokumentu, so na voljo ″TAKŠNI KOT SO″ brez jamstev kakršnekoli vrste. Posredna jamstva za nekršitev, tržnost in primernost za določen namen so izrecno zavrnjena.

Prilagodite del te kode, tako da bo ustrezala vašim potrebam za uporabo API-ja Podpiši objekt kot dela pakirnega programa za vaš aplikacijski izdelek. Za ta program morate podati dva parametra: ime knjižnice za podpisovanje in ID aplikacije za podpisovanje objektov; ID aplikacije upošteva velike in male črke, ime knjižnice pa ne. Program, ki ga napišete, lahko večkrat pokliče ta del kode, če uporabite kot del izdelka, ki ga podpisujete, več knjižnic.

```
/* ------------------------------------------------------------ */
/*                                                              */
/* COPYRIGHT (C) IBM CORP. 2002                                 */
```

```
/*                                                                  */
/* Uporaba API-ja Podpiši objekt za podpis ene ali več knjižnic     */
/*                                                                  */
/* API bo digitalno podpisal vse objekte v podani knjižnici         */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* To gradivo vsebuje programsko izvorno kodo, ki jo lahko          */
/* prilagodite. Ta zgled ni bil natačno preizkušen v                */
/* vseh okoliščinah.  Zato IBM ne more zagotoviti                   */
/* zanesljivosti, uporabnosti ali delovanja                         */
/* teh programov.  Vsi programi v tem dokumentu so                  */
/* na voljo "TAKŠNI KOT SO". POSREDNA JAMSTVA ZA                    */
/* TRŽNOST IN PRIMERNOST ZA DOLOČEN NAMEN SO                        */
/* IZRECNO ZAVRNJENA.  IBM ne nudi za te programe ali               */
/* datoteke nobenih programskih storitev.                           */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Parametra sta naslednja:                                         */
/*                                                                  */
/*  char *   ime knjižnice za podpis                                */
/*  char *   ime ID-ja aplikacije                                   */
/*                                                                  */

#include <qydosgno.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int main (int argc, char *argv[])
{

    /* parametra:

       char * knjižnica, v kateri bodo podpisani objekti
       char * identifikator aplikacije, s katerim bo opravljen podpis

     */

    int         lib_length, applid_length, path_length, multiobj_length;
    Qus_EC_t    error_code;
    char        libname[11];
    char        path_name[256];

    Qydo_Multi_Objects_T * multi_objects = NULL;
    multiobj_length = 0;
    error_code.Bytes_Provided = 0;    /* za napake vrne izjemno stanje */


    /* ------------------------------------ */
    /* ime poti sestave s podanim imenom knjižnice */
    /* ------------------------------------ */
    memset(libname, '\00', 11); /* inicializacija imena knjižnice */
    for(lib_length = 0;
        ((*(argv[1] + lib_length) != ' ') &&
         (*(argv[1] + lib_length) != '\00'));
        lib_length++);
    memcpy(argv[1], libname, lib_length); /* vpišite ime knjižnice */

    /* izdelava parametra imena poti za klic API-ju */
    sprintf(path_name, "/QSYS.LIB/%s.LIB/*", libname);
    path_length = strlen(path_name);

    /* --------------------------- */
    /* iskanje dolžina ID-ja aplikacije */
    /* --------------------------- */
```

```
    for(applid_length = 0;
        ((*(argv[2] + applid_length) != ' ') &&
         (*(argv[2] + applid_length) != '\00'));
        applid_length++);

    /* -------------------------------- */
    /* podpis vseh objektov v tej knjižnici */
    /* -------------------------------- */
    QYDOSGNO  (path_name,             /* ime poti do objekta     */
               &path_length,          /* dolžina imena poti  */
               "OBJN0100",            /* ime formata             */
               argv[2],               /* identifikator (ID) aplikacije */
               &applid_length,        /* dolžina ID-ja aplikacije  */
               "1",                   /* zamenjava podvojenega podpisa */
               multi_objects,         /* kako obravnavati več
                                            objektov                */
               &multiobj_length,      /* dolžina struktur z več
                                         objekti za uporabo
                                        (0=ni strukture z več objekti)*/
               &error_code);          /* koda napake              */



       return 0;

}
```

7. korak: Izdelava prednamestitvenega izhodnega programa, ki uporablja API Dodaj verifikator

Zdaj ko ste izdelali programski postopek za podpis aplikacije, lahko s pomočjo API-ja Dodaj verifikator kot dela namestitvenega programa izdelate končni izdelek za razpošiljanje. Tako lahko na primer uporabite API Dodaj verifikator kot del prednamestitvenega izhodnega programa in zagotovite, da je potrdilo dodano v prostor za potrdila pred obnovitvijo podpisanih aplikacijski objektov. S tem zagotovite, da namestitveni program preveri podpis v aplikacijskih objektih pri njihovi obnovitvi na strežniku iSeries.

Opomba: Zaradi varnostnih razlogov ta API ne dopušča, da v prostor za potrdila *SIGNATUREVERIFICATION dodate potrdilo službe za pooblastila (CA). Če dodate v prostor za potrdila potrdilo službe za pooblastila, sistem meni, da je CA overjen izvor potrdil. Posledično obravnava sistema potrdila, ki jih izda CA, kot potrdila iz overjenega izvora. Zato s pomočjo API-ja ne morete izdelati namestitvenega izhodnega programa za vstavljanje potrdila CA v prostor za potrdila. Potrdilo CA morate dodati v prostor za potrdila s pomočjo Upravljalnika digitalnih potrdil, in s tem zagotoviti, da mora nekdo izrecno in ročno nadzorovati, katerim službam za pooblastila zaupa sistem. S tem preprečite možnost, da bi sistem uvozil potrdila iz izvorov, ki jih skrbnik ni izrecno podal kot overjene.

Če želite preprečiti, da bi kdorkoli uporabil ta API za dodajanje potrdila za preverjanje v prostor za potrdila *SIGNATUREVERIFICATION brez vaše vednosti, lahko onemogočite ta API v sistemu. To lahko naredite s pomočjo sistemskih storitvenih orodij (SST), ki onemogočijo spreminjanje sistemskih vrednosti, povezanih z zaščito .

Da boste bolje razumeli, kako uporabiti API Dodaj verifikator kot del namestitvenega programa aplikacije, si oglejte naslednji zgled kode prednamestitvenega izhodnega programa. Ta del vzorčne kode, napisane v jeziku C, ni popoln prednamestitveni izhodni program, pač pa samo zgled dela takšnega programa, ki pokliče API Dodaj verifikator. Če se odločite, da boste uporabili ta vzorčni program, ga prilagodite svojim potrebam. Zaradi varnostnih razlogov IBM priporoča, da specificirate vzorčni program, namesto da bi uporabili podane privzete vrednosti.

Opomba: IBM vam daje neizključno licenco za avtorske pravice za uporabo vseh zgledov programske kode, iz katere lahko ustvarite podobne funkcije, ki jih prilagodite lastnim potrebam. IBM nudi celotno vzorčno kodo zgolj za ilustrativne namene. Ti zgledi niso bili natančno preizkušeni v vseh

pogojih. IBM zato ne more zagotoviti zanesljivosti, uporabnosti ali delovanja teh programov. Vsi programi, vsebovani v tem dokumentu, so na voljo ″TAKŠNI KOT SO″ brez jamstev kakršnekoli vrste. Posredna jamstva za nekršitev, tržnost in primernost za določen namen so izrecno zavrnjena.

Ta del kode prilagodite tako, da bo ustrezal vašim potrebam za uporabo API-ja Dodaj verifikator kot del prednamestitvenega izhodnega programa za dodajanje zahtevanega potrdila za preverjanje podpisov na strežnik iSeries stranke pri namestitvi izdelka.

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2002                                     */
/*                                                                  */
/* API Dodaj verifikator uporabite za dodajanje potrdila v podano   */
/* datoteko IFS v prostoru za potrdila *SIGNATUREVERIFICATION.      */
/*                                                                  */
/* API bo izdelal prostor za potrdila, če le-ta še ne obstaja.      */
/* Če je prostor za potrdila izdelan, mu je dodeljeno privzeto      */
/* geslo, ki ga čim prej spremenite s pomočjo DCM.                  */
/* To opozorilo posredujte lastnikom sistema, ki                    */
/* uporabljajo ta program.                                          */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* To gradivo vsebuje programsko izvorno kodo, ki jo lahko          */
/* prilagodite. Ta zgled ni bil natačno preizkušen v                */
/* vseh okoliščinah.  Zato IBM ne more zagotoviti                   */
/* zanesljivosti, uporabnosti ali delovanja                         */
/* teh programov.  Vsi programi v tem dokumentu so                  */
/* na voljo "TAKŠNI KOT SO". POSREDNA JAMSTVA ZA                    */
/* TRŽNOST IN PRIMERNOST ZA DOLOČEN NAMEN SO                        */
/* IZRECNO ZAVRNJENA.  IBM ne nudi za te programe ali               */
/* datoteke nobenih programskih storitev.                           */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Parametra sta naslednja:                                         */
/*                                                                  */
/*  char * ime poti do datoteke IFS, v kateri je shranjeno potrdilo */
/*  char * oznaka potrdila, ki bo dodeljena potrdilu                */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* ---------------------------------------------------------------- */

#include <qydoadd1.h>
#include <stdlib.h>
#include <string.h>

int main (int argc, char *argv[])
{

    int         pathname_length, cert_label_length;
    Qus_EC_t    error_code;
    char      * pathname = argv[1];
    char      * certlabel = argv[2];

    /* iskanje dolžine imena poti */
    for(pathname_length = 0;
        ((*(pathname + pathname_length) != ' ') &&
         (*(pathname + pathname_length) != '\00'));
        pathname_length++);

    /* iskanje dolžine oznake potrdila */
    for(cert_label_length = 0;
        ((*(certlabel + cert_label_length) != ' ') &&
```

```
         (*(certlabel + cert_label_length) != '\00'));
        cert_label_length++);


    error_code.Bytes_Provided = 0;    /* za napake vrne izjemno stanje */

    QydoAddVerifier (pathname,         /* ime poti do datoteke s potrdilom */
                     &pathname_length, /* dolžina imena poti           */
                     "OBJN0100",       /* ime formata                      */
                     certlabel,        /* oznaka potrdila                  */
                     &cert_label_length, /* dolžina oznake potrdila    */
                     &error_code);     /* koda napake        */

    return 0;
}
```

Ko dokončate te naloge, lahko zapakirate aplikacijo in jo pošljete svojim strankam. Ko bodo namestile aplikacijo, bodo objekti podpisane aplikacije preverjeni kot del namestitvenega postopka. Kasneje lahko preverijo stranke podpis aplikacijskih objektov s pomočjo Upravljalnika digitalnih potrdil (DCM). To jim omogoča, da določijo, ali je izvor aplikacije overjen, in ali so bile od podpisa aplikacije v njej opravljene kakšne spremembe.

Opomba: Namestitveni program bo izdelal prostor za potrdila *SIGNATUREVERIFICATION s privzetim geslom stranke. Strankam svetujte, naj s pomočjo DCM čim prej na novo nastavijo geslo prostora za potrdila, da ga bodo zaščitili pred nepooblaščenim dostopom.

8. korak: Stranke naj na novo nastavijo privzeto geslo prostora za potrdila *SIGNATUREVERIFICATION

API Dodaj verifikator je morda izdelal prostor za potrdila *SIGNATUREVERIFICATION kot del namestitvenega postopka izdelka na strežniku iSeries stranke. Če je bil prostor za potrdila izdelan z API-jem, je bilo zanj uporabljeno privzeto geslo. Zato svetujte svojim strankam, naj s pomočjo DCM na novo nastavijo to geslo, da bodo preprečili nepooblaščen dostop do prostora za potrdila.

Naslednji koraki kažejo, kako naj stranke na novo nastavijo geslo prostora za potrdila *SIGNATUREVERIFICATION:

1. Zaženite DCM.
2. V okvirju za usmerjanje kliknite **Izberi prostor za potrdila** in za odpiranje izberite prostor za potrdila ***SIGNATUREVERIFICATION**.
3. Ko se prikaže stran Prostor za potrdilo in geslo, kliknite **Na novo nastavi geslo**, da boste prikazali stran Vnovična nastavitev gesla prostora za potrdila.

   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.
4. Podajte novo geslo prostora za potrdila, z vnovičnim vnosom ga potrdite, izberite načelo za potek gesla in kliknite **Nadaljuj**.

Scenarij: Uporaba Osrednjega upravljanja za podpisovanje objektov

Stanje

Vaše podjetje (MyCo, Inc.) razvija aplikacije, ki jih razpošilja več strežnikom iSeries na več mestih znotraj podjetja. Kot skrbnik omrežja morate zagotoviti, da bodo te aplikacije nameščene in ažurirane na vseh strežnikih iSeries podjetja. Za preprostejše pakiranje in razdeljevanje teh aplikacij in izvajanje drugih upravnih nalog, za katere ste odgovorni, trenutno uporabljate funkcijo Osrednje upravljanje Navigatorja iSeries. Toda zaradi nepooblaščenih sprememb v objektih porabite preveč časa za iskanje in odpravo težav v teh aplikacijah. Zato želite z digitalnim podpisom bolj zaščititi integriteto teh objektov.

Raziskali ste funkcije podpisovanja objektov OS/400 in se naučili, da omogoča Osrednje upravljanje od izdaje V5R2 naprej podpisovanje objektov pri njihovem pakiranju in razdelitvi. S pomočjo Osrednjega upravljanja lahko učinkovito in dokaj preprosto zadovoljite zaščitne potrebe vašega podjetja. Odločili ste se tudi, da boste izdelali lokalno službo za pooblastila (CA), ki jo uporabili za izdajanje potrdil za podpisovanje objektov. Z uporabo potrdila, ki ga izda lokalni CA za podpisovanje objektov, zmanjšate strošek uporabe te tehnologije za zaščito, ker vam ni potrebno kupiti potrdila pri znani javni službi za pooblastila.

Ta zgled služi kot koristen uvod v korake, vključene v konfiguriranje in uporabo pdpisovanja objektov za aplikacije, ki jih razpošljete na več srežnikov iSeries podjetja.

Prednosti scenarija

S tem scenarijem so povezane naslednje prednosti:

- Uporaba Osrednjega upravljanja za pakiranje in podpisovanje objektov zmanjša čas, ki je potreben za razpošiljanje podpisanih objektov na strežnike iSeries vašega podjetja.
- Uporaba Osrednjega upravljanja za podpisovanje objektov v paketu zmanjša število korakov, potrebnih za podpis objektov, sa je postopek podpisovanja del postopka pakiranja.
- S podpisom paketa objektov lahko preprosteje določite, ali so bili objekti od podpisa spremenjeni. S tem zmanjšate tudi del odpravljanja težav, ki bi ga bilo potrebno opraviti v bodoče, da bi določili, kje v aplikaciji je težava.
- Uporaba potrdila, ki ga izda lokalna služba za pooblastila (CA) za podpisovanje objektov, zmanjša stroške podpisovanja objektov.

Cilji

V tem scenariju želi podjetje MyCo, Inc. digitalno podpisati aplikacije, ki jih razpošlje na več strežnikov iSeries znotraj podjetja. Kot skrbnik omrežja v MyCo, Inc. že izvajate številne upravne naloge iSeries s pomočjo Osrednjega upravljanja. Zato želite razširiti trenutno uporabo Osrednjega upravljanja na podpisovanje aplikacij podjetja, ki jih razpošljete drugim strežnikom iSeries.

Cilji tega scenarija so naslednji:

- Aplikacije podjetja morajo biti podpisane s potrdilom, ki ga izda lokalna služba za pooblastila, da se omejijo stroški podpisovanja apliakcij.
- Skrbniki sistemov in drugi določeni uporabniki morajo imeti zmožnost preprostega preverjanja digitalnih podpisov na vseh strežnikih iSeries, da preverijo izvor in pristnost podjetja, ki je podpisalo objekte. Za dosego tega mora imeti vsak strežnik iSeries kopijo potrdila za preverjanje podpisa podjetja in potrdilo lokalne službe za pooblastila (CA) v prostoru za potrdila *SIGNATUREVERIFICATION vsakega strežnika.
- Verifying the signatures on company applications allows iSeries administrators and others to detect whether the content of the objects has changed since they were signed.
- Skrbniki morajo imeti zmožnost za uporabo Osrednjega upravljanja za pakiranje, podpisovanje in nato razpošiljanje svojih aplikacij na strežnike iSeries.

Podrobnosti

Naslednja slika ilustrira postopek podpisovanja objekta in preverjanja podpisa za izvedbo tega scenarija:

Slika ilustrira naslednje točke, pomembne za ta scenarij:

Osrednji sistem (iSeries A)

- Na iSeries A se izvaja OS/400 različice 5 izdaje 2 (V5R2).
- iSeries A služi kot osrednji sistem, v katerem se izvajajo funkcije Osrednjega upravljanja, vključno s pakiranjem in razpošiljanjem aplikacij podjetja.

- Na iSeries A je nameščen 128-bitni ponudnik šifriranega dostopa za iSeries (5722–AC3).
- Na iSeries A je nameščen in konfiguriran Upravljalnik digitalnih potrdil (OS/400 možnost 34) in strežnik IBM HTTP (5722–DG1).
- iSeries A deluje kot lokalna služba za pooblastila (CA) in potrdilo za podpisovanje objektov je v tem sistemu.
- iSeries A je primarni sistem podpisovanja objektov za aplikacije podjetja. Podpisovanje objektov izdelka za razpošiljanje uporabnikom opravite na iSeries A z naslednjimi nalogami:
  1. Uporaba DCM za izdelavo lokalne službe za pooblastila in uporaba lokalne službe za pooblastila za izdelavo potrdila za podpisovanje objektov.
  2. Uporaba DCM za izvoz kopije potrdila lokalne službe za pooblastila in potrdila za preverjanje podpisov v datoteko, da lahko sistemi zaključnih točk (iSeries B, C, D in E) preverijo podpisane objekte.
  3. Uporaba Osrednjega upravljanja za podpisovanje aplikacijskih objektov in njihovo pakiranje z datotekami potrdil za preverjanje.
  4. Uporaba Osrednjega upravljanja za razpošiljanje podpisanih aplikacij in datotek potrdil v sisteme zaključnih točk.

Sistemi zaključnih točk (strežniki iSeries servers B, C, D in E)

- Na iSeries B in C se izvaja OS/400 različice 5 izdaje 2 (V5R2).
- Na iSeries D in E se izvaja OS/400 različice 5 izdaje 1 (V5R1).
- Na iSeries B, C, D in E je nameščen in konfiguriran Upravljalnik digitalnih potrdil (možnost 34) in strežnik IBM HTTP (5722–DG1).
- iSeries B, C, D in E prejmejo iz osrednjega sistema (iSeries A) kopijo potrdila za preverjanje podpisov podjetja in potrdila lokalne službe za pooblastila, ko sistem prejme podpisano aplikacijo.
- DCM se uporablja za izdelavo prostora za potrdila *SIGNATUREVERIFICATION in uvoz potrdila lokalne službe za pooblastila in potrdila za preverjanje v prostor za potrdila.

Predpogoji in predpostavke

Ta scenarij je odvisen od naslednjih predpogojev in predpostavk:

1. Vsi strežniki iSeries ustrezajo zahtevam za namestitev in uporabo Upravljalnika digitalnih potrdil (DCM).
2. Nihče ni predhodno konfiguriral ali uporabil DCM na nobenem strežniku iSeries.
3. iSeries A ustreza zahtevam za namestitev in uporabo Navigatorja iSeries in Osrdnjega upravljanja.
4. V vseh sistemih zaključnih točk iSeries se mora izvajati strežnik Osrednjega upravljanja.
5. Na vseh strežnikih iSeries je nameščen licenčni program 128-bitnega ponudnika šifriranega dostopa (5722-AC3) najvišje ravni.
6. Privzeta nastavitev za preverjanje podpisov objektov med sistemsko vrednostjo za obnovitev (QVFYOBJRST) na vseh strežnikih scenarijev iSeries je 3 in ni bila spremenjena. Privzeta nastavitev zagotavlja, da lahko strežnik preveri podpise objektov pri obnovitvi podpisanih objektov.
7. Skrbnik omrežja za iSeries A mora imeti profil uporabnik s posebnim pooblastilom *ALLOBJ za podpisovanje objektov, ali pa mora imeti profil uporabnika pooblastilo za uporabo aplikacije za podpisovanje objektov.
8. Skrbnik omrežja ali kdorkoli drug, ki izdela prostor za potrdila v DCM, mora imeti profil uporabnika s posebnima pooblastiloma *SECADM in *ALLOBJ.
9. Skrbniki sistemov ali drugi uporabniki na vseh drugih strežnikih iSeries morajo imeti profil uporabnika s posebnim pooblastilom *AUDIT za preverjanje podpisov objektov.

Koraki naloge

Za izvedbo tega scenarija obstajata dva niza nalog, ki jih morate izvesti: en niz nalog omogoča, da nastavite iSeries A za uporabo Osrednjega upravljanja za podpisovanje in razpošiljanje aplikacij, drugi niz nalog pa omogoča skrbnikom sistema in drugim uporabnikom, da preverijo podpise v teh aplikacijah na vseh drugih strežnikih iSeries.

Koraki naloge podpisovanja objektov

Za podpisovanje objektov, tako kot opisuje ta scenarij, morate končati vse od naslednjih nalog na iSeries A:

1. Opravite vse predpogojne korake za namestitev in konfigurirajte vse potrebne izdelke iSeries.
2. S pomočjo Upravljalnika digitalnih potrdil (DCM) izdelajte lokalno službo za pooblastila (CA), ki bo izdajala zasebna pooblastila za podpisovanje objektov.
3. S pomočjo DCM izdelajte definicijo aplikacije.
4. S pomočjo DCM dodelite potrdilo definiciji aplikacije za podpisovanje objektov.
5. S pomočjo DCM izvozite potrdila, ki jih morajo uporabiti drugi sistemi za preverjanje podpisov objektov. V datoteko morate izvoziti kopijo potrdila lokalnega CA in kopijo potrdila za podpisovanje objektov.
6. Prenesite datoteke potrdil v vse sisteme zaključnih točk iSeries, v katerih nameravate preveriti podpise.
7. S pomočjo Osrednjega upravljanja podpišite objekte aplikacije.

Koraki naloge preverjanja podpisov

Te konfiguracijske naloge preverjanja podpisov opravite v sistemu zaključne točke iSeries, preden v njih s pomočjo Osrednjega upravljanja prenesete objekte podpisane aplikacije. Konfiguracija preverjanja podpisov mora biti končana, preden lahko uspešno preverite podpise pri obnovitvi podpisanih objektov v sistemih zaključnih točk.

V vseh sistemih zaključnih točk iSeries morate opraviti naslednje naloge, če želite preveriti podpise objektov, kot opisuje ta scenarij:

8. S pomočjo Upravljalnika digitalnih potrdil Manager (DCM) izdelajte prostor za potrdila *SIGNATUREVERIFICATION.
9. S pomočjo DCM uvozite potrdilo lokalnega CA in potrdilo za preverjanje podpisa.

Podrobnosti konfiguracije

Dokončajte naslednje korake konfiguracije Osrednjega upravljanja, če želite podpisovati objekte, kot to opisuje ta scenarij.

1. korak: Opravite vse predpogojne korake

Preden lahko opravite določene konfiguracijske naloge za izvedbo tega scenarija, morate opraviti vse predpogojne naloge za namestitev in konfiguracijo vseh potrebnih izdelkov iSeries.

2. korak: Izdelajte lokalno službo za pooblastila, ki bo izdala zasebno potrdilo za podpis objekta

Če uporabite za izdelavo lokalne službe za pooblastila (CA) Upravljalnik digitalnih potrdil (DCM), postopek zahteva, da izpolnite niz obrazcev. Ti obrazci vas vodijo skozi postopek izdelave službe za pooblastila in dokončanje drugih nalog, potrebnih za začetek uporabe potrdil za plast zaščitenih vtičnic (SSL), podpisovanje objektov in preverjanje podpisov. Čeprav v tem scenariju ni potrebno konfigurirati potrdil za SSL, morate izpolniti vse obrazce v nalogi konfiguriranja sistema za podpisovanje objektov.

Takole s pomočjo DCM izdelate in vodite lokalno službo za pooblastila:

1. Zaženite DCM.
2. V oknu za usmerjanje DCM izberite **Izdelaj službo za pooblastila (CA)**, da boste prikazali niz obrazcev.

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. Izpolnite vse obrazce za to vodeno nalogo. Pri izvedbi te naloge morate narediti naslednje:
   a. Podati določevalne informacije za lokalni CA.
   b. Namestiti potrdilo lokalnega CA v brskalnik, da lahko programska oprema prepozna lokalni CA in preveri veljavnost potrdil, ki jih izda lokalni CA.
   c. Podati podatke načel za lokalni CA.
   d. Uporabiti nov lokalni CA za izdajo potrdila strežnika ali odjemalca, ki ga lahko uporabijo vaše aplikacije za povezave SSL.

      Opomba: Čeprav v tem scenariju to potrdilo ni uporabljeno, ga morate izdelati, preden lahko uporabite lokalni CA za izdajanje potrebnega potrdila za podpisovanje objektov. Če prekinete nalogo, ne da bi izdelali to potrdilo, morate izdelati potrdilo za podpisovanje objektov in prostor za potrdila *OBJECTSIGNING, v katerem je ločeno shranjen.
   e. Izbrati aplikacije, ki lahko uporabljajo potrdilo strežnika ali odjemalca za povezave SSL.

      Opomba: Za namen tega scenarija ne izberite nobene aplikacije in kliknite **Nadaljuj**, da boste prikazali naslednji obrazec.
   f. Uporabiti nov lokalni CA za izdajo potrdila za podpisovanje objektov, ki ga lahko uporabijo 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.
   g. Izbrati aplikacije, ki bodo zaupale lokalnemu CA.

      Opomba: Za namen tega scenarija ne izberite nobene aplikacije in kliknite **Nadaljuj**, da boste končali nalogo.

Zdaj ko ste izdelali lokalni CA in potrdilo za podpisovanje objektov, morate definirati aplikacijo za podpisovanje objektov, ki bo uporabila potrdilo, preden lahko podpišete objekte.

3. korak: Izdelava definicije aplikacije za podpisovanje objektov

Ko izdelate potrdilo za podpisovanje objektov, morate s pomočjo Upravljalnika digitalnih potrdil (DCM) definirati aplikacijo za podpisovanje objektov, ki jo lahko uporabite za podpisovanje objektov. Za definicijo aplikacije ni nujno, da se nanaša na dejansko aplikacijo; definicija aplikacije, ki jo izdelate, mora opisovati tip ali skupino objektov, ki jih nameravate podpisati. Definicijo potrebujete, da lahko povežete ID aplikacije s potrdilom in omogočite postopek podpisovanja.

Takole s pomočjo DCM izdelajte definicijo aplikacije za podpisovanje objektov:

1. V okvirju za usmerjanje kliknite **Izberi prostor za potrdila** in izberite ***OBJECTSIGNING** kot prostor za potrdila, ki ga želite odpreti.
2. Ko se prikaže stran Prostor za potrdila in geslo, podajte geslo, ki ste ga podali za prostor za potrdila pri njegovi izdelavi in kliknite **Nadaljuj**.
3. V okvirju za usmerjanje izberite **Upravljanje aplikacij**, da boste prikazali seznam nalog.
4. S seznama nalog izberite **Dodaj aplikacijo**, da boste prikazali obrazec za definiranje aplikacije.
5. Izpolnite obrazec in kliknite **Dodaj**.

Zdaj morate dodeliti potrdilo za podpisovanje objektov aplikaciji, ki ste jo izdelali.

4. korak: Dodelitev potrdila definiciji aplikacije za podpisovanje objektov

Takole dodelite potrdilo aplikaciji za podpisovanje objektov:

1. V okvirju za usmerjanje DCM izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.

2. S seznama nalog izberite **Dodeli potrdilo**, da boste prikazali seznam potrdil za trenutni prostor za potrdila.
3. S seznama izberite potrdilo in kliknite **Dodeli aplikacijam**, da boste prikazali seznam definicij aplikacij za trenutni prostor za potrdila.
4. S seznama izberite eno ali več aplikacij in kliknite **Nadaljuj**. Prikaže se sporočilna stran, na kateri potrdite dodelitev potrdila, ali poda informacije o napaki, če je prišlo do kakšne težave.

Ko končate to nalogo, lahko začnete podpisovati objekte s pomočjo Osrednjega upravljanja pri njihovem pakiranju in razpošiljanju. Toda če želite zagotoviti, da boste vi ali drugi uporabniki lahko preverjali podpise, morate izvoziti potrebna potrdila v datoteko in jih prenesti v vse sisteme zaključnih točk iSeries. V vseh sistemih zaključnih točk iSeries morate dokončati tudi vse konfiguracijske naloge preverjanja podpisov, preden v njih s pomočjo Osrednjega upravljanja prenesete objekte podpisane aplikacije. Konfiguracija preverjanja podpisov mora biti končana, preden lahko uspešno preverite podpise pri obnovitvi podpisanih objektov v sistemih zaključnih točk.

5. korak: Izvoz potrdil za omogočanje preverjanja podpisov v drugih sistemih iSeries

Podpisovanje objektov za zaščito integritete vsebine zahteva, da imati vi in drugi uporabniki na voljo sredstva za preverjanje pristnosti podpisa. Če želite preveriti podpise v sistemu, ki podpiše objekte, morate s pomočjo DCM izdelati prostor za potrdila *SIGNATUREVERIFICATION. Ta prostor za potrdila mora vsebovati kopijo potrdila za podpisovanje objektov in kopijo potrdila službe za pooblastila, ki je izdala potrdilo.

Če želite drugim uporabnikom omogočiti preverjanje podpisov, jim morate posredovati kopijo potrdila, ki je podpisalo objekt. Če izdate potrdilo s pomočjo lokalne službe za pooblastila (CA), jim morate posredovati tudi kopijo potrdila lokalne službe za pooblastila.

Naslednji koraki kažejo, kako uporabiti DCM za preverjanje podpisov v istem sistemu, ki podpiše objekte (v tem scenariju je to iSeries A):

1. V okvirju za usmerjanje izberite **Izdelaj nov prostor za potrdila** in izberite ***SIGNATUREVERIFICATION** kot prostor za potrdila, ki ga želite izdelati.
2. Izberite **Da**, da boste prekopirali obstoječa potrdila za podpisovanje objektov v nov prostor za potrdila kot potrdila za preverjanje podpisov.
3. Podajte geslo novega prostora za potrdila in kliknite **Nadaljuj**, da boste izdelali prostor za potrdila. Zdaj lahko s pomočjo DCM preverite podpise objektov v istem sistemu, ki ga uporabite za podpisovanje objektov.

Naslednji koraki kažejo, kako s pomočjo DCM izvozite kopijo potrdila lokalne službe za pooblastila in kopijo potrdila za podpisovanje objektov kot potrdila za preverjanje podpisov, da lahko preverite podpise objektov v drugih sistemih:

1. V okvirju za usmerjanje izberite **Upravljanje potrdil**, nato pa izberite nalogo **Izvozi potrdilo**.
2. Izberite **Služba za pooblastila (CA)** in kliknite **Nadaljuj**, da boste prikazali seznam potrdil CA, ki jih lahko izvozite.
3. S seznama izberite predhodno izdelano potrdilo lokalne službe za pooblastila in kliknite **Izvozi**.
4. Za cilj izvoza podajte **Datoteka** in kliknite **Nadaljuj**.
5. Podajte celotno pot in ime datoteke za izvoženo potrdilo lokalne službe za pooblastila in kliknite **Nadaljuj**, da boste izvozili potrdilo.
6. Za izhod s potrditeveni strani za izvoz kliknite **Potrdi**. Zdaj lahko izvozite kopijo potrdila za podpisovanje objektov.
7. Znova izberite nalogo **Izvozi potrdilo**.
8. Izberite **Podpisovanje objektov**, da boste prikazali seznam potrdil za podpisovanje objektov, ki jih lahko izvozite.

9. S seznama izberite ustrezno potrdilo za podpisovanje objektov in kliknite **Izvozi**.
10. Za cilj izberite **Datoteka, kot potrdilo za preverjanje podpisov** in kliknite **Nadaljuj**.
11. Podajte celotno pot in ime datoteke izvoženega potrdila za preverjanje podpisov in kliknite **Nadaljuj**, da boste izvozili potrdilo.

Zdaj lahko prenesete te datoteke v sisteme zaključnih točk iSeries, v katerih nameravate preveriti podpise, ki ste jih izdelali s potrdilom.

6. korak: Prenos datotek potrdil v sisteme zaključnih točk iSeries

Datoteke potrdil, ki ste jih izdalali na iSeries A, morate v tem scenariju prenesti v sisteme zaključnih točk iSeries, preden jih lahko konfigurirate za preverjanje objektov, ki jih podpišete. Za prenos datotek potrdil lahko uporabite več različnih načinov. Uporabite lahko na primer FTP (File Transfer Protocol) ali razpošiljanje paketov Osrednjega upravljanja.

7. korak: Podpisovanje objektov s pomočjo Osrednjega upravljanja

Postopek podpisovanja objektov v Osrednjem upravljanju je del postopka razpošiljanja pakiranih objektov. V vseh sistemih zaključnih točk iSeries morate dokončati vse konfiguracijske naloge preverjanja podpisov, preden s pomočjo Osrednjega upravljanja v njih prenesete objekte podpisane aplikacije. Konfiguracija preverjanja podpisov mora biti končana, preden lahko uspešno preverite podpise pri obnovitvi podpisanih objektov v sistemih zaključnih točk.

Za podpis aplikacije, ki jo razpošljete sistemom zaključnih točk iSeries, kot to opisuje ta scenarij, opravite naslednje korake:

1. S pomočjo Osrednjega upravljanja zapakirajte in razpošljite izdelke programske opreme.
2. V oknu **Identifikacija** v čarovniku **Definicija izdelka** kliknite **Zahtevnejše**, da boste prikazali okno **Zahtevnejša identifikacija**.
3. V polje **Digitalno podpisovanje** vnesite ID predhodno izdelane aplikacije za podpisovanje objektov in kliknite **Potrdi**.
4. Dokončajte čarovnika in z Osrednjim upravljanjem nadaljujte postopek pakiranja in razpošiljanja izdelkov programske opreme.

8. korak: Naloge preverjanja podpisov: Izdelava prostora za potrdila *SIGNATUREVERIFICATION v sistemih zaključnih točk iSeries

Če želite v tem scenariju preveriti podpise objektov v sistemih zaključnih točk iSeries, mora vsak sistem v prostoru za potrdila *SIGNATUREVERIFICATION vsebovati kopijo ustreznega potrdila za preverjanje podpisov. Če ste objekte podpisali z zasebnim potrdilom, mora vsebovati ta prostor za potrdila tudi kopijo potrdila zasebne službe za pooblastila.

Takole izdelate prostor za potrdila *SIGNATUREVERIFICATION:

1. Zaženite DCM.
2. V oknu za usmerjanje Upravljalnika digitalnih potrdil (DCM) izberite **Izdelaj nov prostor za potrdila** in za izdelavo izberite prostor za potrdila ***SIGNATUREVERIFICATION**.

   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. Podajte geslo novega prostora za potrdila in kliknite **Nadaljuj**, da boste izdelali prostor za potrdila. Zdaj lahko uvozite potrdila v prostor za potrdila in jih uporabite za preverjanje podpisov objektov.

9. korak: Naloge preverjanja podpisov: Uvoz potrdil

Če želite preveriti podpis objekta, mora vsebovati prostor za potrdila *SIGNATUREVERIFICATION kopijo potrdila za preverjanje podpisov. Če je potrdilo za podpisovanje zasebno, mora vsebovati ta prostor za potrdila tudi kopijo potrdila lokalne službe za pooblastila, ki je izdala potrdilo za podpisovanje. V tem scenariju smo izvozili obe potrdili v datoteko, ta datoteka pa je bila prenesena v sisteme zaključnih točk iSeries.

Takole uvozite ti potrdili v prostor za potrdila *SIGNATUREVERIFICATION:

1. V okvirju za usmerjanje DCM kliknite **Izberi prostor za potrdila** in za odpiranje izberite prostor za potrdila ***SIGNATUREVERIFICATION**.
2. Ko se prikaže stran Prostor za potrdila in geslo, podajte geslo, ki ste ga podali za prostor za potrdila pri njegovi izdelavi in kliknite **Nadaljuj**.
3. Ko se okvir za usmerjanje osveži, izberite **Upravljanje potrdil**, da boste prikazali seznam nalog.
4. S seznama nalog izberite **Uvozi potrdilo**.
5. Kot tip potrdila izberite **Služba za pooblastila (CA)** in kliknite **Nadaljuj**.

   Opomba: Potrdilo lokalne službe za pooblastila morate uvoziti preden uvozite zasebno potrdilo za preverjanje podpisov, sicer postopek uvoza potrdila za preverjanje podpisov ne bo uspel.
6. Podajte celotno pot in ime datoteke, ki vsebuje potrdilo službe za pooblastila in kliknite **Nadaljuj**. Prikaže se sporočilo, ki potrdi, da se je postopek uvoza uspešno končal, ali poda informacije o napaki, če postopek ne uspe.
7. Znova izberite nalogo **Uvozi potrdilo**.
8. Kot tip potrdila za uvoz izberite **Preverjanje podpisa** in kliknite **Nadaljuj**.
9. Podajte celotno pot in ime datoteke potrdila za preverjanje podpisov in kliknite **Nadaljuj**. Prikaže se sporočilo, ki potrdi, da se je postopek uvoza uspešno končal, ali poda informacije o napaki, če postopek ne uspe.

Vaš sistem iSeries lahko zdaj pri obnovitvi podpisanih objektov preveri podpise, ki ste jih izdelali z ustreznim potrdilom za podpisovanje.

Koncepti podpisovanja objektov

Preden začnete uporabljati funkcije iSeries za podpisovanje objektov in preverjanje podpisov, preglejte naslednje koncepte:

Digitalni podpisi
Naučite se, kaj so digitalni podpise in kakšno vrsto zaščite nudijo.

Objekti, ki jih je mogoče podpisati
Naučite se, katere objekte iSeries lahko podpišete in spoznajte možnosti podpisovanja ukaznih (*CMD) objektov.

Obdelava podpisov objektov
Spoznajte, kako deluje postopek podpisovanja objektov in katere parametre lahko nastavite zanj.

Obdelava preverjanja podpisov
Spoznajte, kako deluje postopek preverjanja podpisov in katere parametre lahko nastavite zanj.

Digitalni podpisi

OS/400 nudi podporo za uporabo digitalnih potrdil za digitalno ″podpisovanje″ objektov. Digitalni podpis objekta izdelate s pomočjo kodirane pisave, ki deluje podobno kot osebni podpis na pisanem dokumentu. Digitalni podpis nudi dokaz o izvoru objekta in sredstva za preverjanje njegove integritete. Lastnik

digitalnega potrdila ″podpiše″ objekt s pomočjo zasebnega ključa potrdila. Prejemnik objekta dešifrira podpis s pomočjo ustreznega javnega ključa potrdila, s čimer preveri integriteto podpisanega objekta in pošiljatelja.

Podpora za podpisovanje objektov dopolnjuje tradicionalna orodja strežnika iSeries za krmiljenje, kdo lahko podpiše objekte. Tradicionalen nadzor ne more ščititi objektov pred nepooblaščenimi vdori, ko je objek na poti skozi internet ali drugo neoverjeno omrežje. Ker lahko odkrijete, ali je bila vsebina objekta od njegovega podpisa spremenjena, lahko preprosteje določite, ali boste zaupali objektom, ki jih prejmete na ta način.

Digitalni podpis je šifriran matematični povzetek podatkov v objektu. Objekt in njegova vsebina nista šifrirana z digitalnim podpisam, pač pa je šifriran sam povzetek, da se prepreči njegovo nepooblaščeno spreminjanje. Vsakdo, ki želi zagotoviti, da objekt na poti ni bil spremenjen, in da izhaja iz sprejemljivega in zakonitega izvora, lahko s pomočjo javnega ključa potrdila preveri izvirni digitalni podpis. Če se podpis ne ujema več, so bili podatki morda spremenjeni. V tem primeru se lahko uporabnik izogne uporabi objekta in se namesto tega obrne na podpisnika, ki mu pošlje drugo kopijo podpisanega objekta.

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).

Če se odločite, da uporaba digitalnih podpisov zadovoljuje vaše potrebe in načela za zaščito, se morate odločiti, ali boste uporabljali javna potrdila ali izdajali zasebna. Če nameravate pošiljati objekte javnim uporabnikom, razmislite o uporabi znane javne službe za pooblastila (CA) za podpisovanje objektov. Uporaba javnih pooblastil zagotavlja, da lahko uporabniki preprosto in poceni preverijo podpise objektov, ki jim jih pošljete. Če pa boste pošiljali objekte zgolj znotraj vašega podjetja, boste morda raje uporabili Upravljalnik digitalnih potrdil (DCM), s pomočjo katerega boste vodili lokalno službo za pooblastila, ki bo izdajala potrdila za podpisovanje objektov. Uporaba zasebnih potrdil, ki jih izda zasebna služba za pooblastila, je cenejša od nakupa potrdil pri znani javni službi za pooblastila.

Vrste digitalnih podpisov

Od izdaje V5R2 naprej lahko podpisujete ukazne (*CMD) objekte; za objekte *CMD lahko izbirate tudi med dvema vrstama podpisov: osnovni podpisi objektov ali podpisi celotnih objektov.

- **Podpisi celotnih objektov**
  Ta vrsta podpisa pokrije skoraj vse razen nekaj nebistvenih bajtov objekta.
- **Osnovni podpisi objektov**
  Ta vrsta podpisa pokrije bistvene bajte objekta *CMD. Toda podpis ne pokriva tistih bajtov, ki so predmet pogostejših sprememb. Ta vrsta podpisa omogoča izvedbo nekaterih sprememb v ukazu, ne da bi se razveljavila veljavnost podpisa. Katerih bajtov ne pokriva osnovni podpis objekta, se spreminja glede na posamezne objekte *CDM, toda osnovni podpisi na primer ne pokrivajo privzetkov parametrov za objekte *CMD. Zgledi sprememb, ki ne razveljavijo veljavnosti osnovnega podpisa objekta, so:
  - Spreminjanje privzetih vrednosti ukazov
  - Dodajanje programa za preverjanje veljavnosti v ukaz, ki ga še ne vsebuje
  - Spreminjanje parametera Where allowed to run
  - Spreminjanje parametra Allow limited users

Če se želite podučiti, katere objekte iSeries lahko podpišete in katere bajtove objekta CMD* pokriva osnovni podpis objekta, preberite temo Objekti, ki jih je mogoče podpisati.

Objekti, ki jih je mogoče podpisati

Digitalno lahko podpišete veliko tipov objektov OS/400 ne glede na uporabljen način podpisovanja. Podpišete lahko katerikoli objekt (*STMF), ki ga shranite v integriranem datotečnem sistemu sistema, razen objektov, ki so shranjeni v knjižnici. Če ima objekt priključen program Java, bo podpisan tudi ta. V

datotečnem sistemu QSYS.LIB lahko podpišete samo naslednje objekte: programe (*PGM), storitvene programe (*SRVPGM), module (*MODULE), pakete SQL (*SQLPKG), *FILE (samo shranjevalne datoteke) in ukaze (*CMD).

Če želite podpisati objekt, mora le-ta biti v lokalnem sistemu. Če na primer delate s strežnikom Windows 2000 na integriranem strežniku xSeries za iSeries, je v integriranem datotečnem sistemu na voljo datotečni sistem QNTC. Imeniki tega datotečnega sistema niso lokalni, ker vsebujejo datoteke, katerih lastnik je operacijski sistem Windows 2000. Prav tako ne morete podpisati praznih objektov ali objektov, ki so prevedeni za izdajo pred V5R1.

Podpisi ukaznih (*CMD) objektov

Pri podpisovanju objektov *CMD lahko izberete med dvema vrstama podpisov. Podpišete lahko celoten objekt ali pa samo osnovni del objekta. Če podpišete celoten objekt, je podpis uveljavljen za vse bajte objekta, razen za tiste, ki niso bistveni. Podpis celotnega objekta pokriva postavke, vsebovane v osnovnem podpisu objekta.

Če izberete, da boste podpisali samo osnovni objekt, so osnovni bajti zaščiteni s podpisom, bajti, ki so predmet pogostih sprememb, pa ne. Kateri bajti niso podpisani je odvisno od objekta *CMD, toda to lahko vključuje tudi bajte, ki določajo način, v katerem je objekt veljaven ali med drugim tudi, kje se objekt lahko izvaja. Osnovni podpisi na primer ne pokrivajo privzetih vrednosti parametrov za objekte *CMD. Ta vrsta podpisa omogoča izvedbo nekaterih sprememb v ukazu, ne da bi se razveljavila veljavnost njegovega podpisa. Zgledi sprememb, ki ne razveljavijo veljavnosti teh vrst podpisov, vključujejo naslednje:

- Spreminjanje privzetih vrednosti ukazov
- Dodajanje programa za preverjanje veljavnosti v ukaz, ki ga še ne vsebuje
- Spreminjanje parametra Where allowed to run
- Spreminjanje parametra Allow limited users

Naslednja tabela natančno opisuje, kateri bajti objekta *CMD so vključeni kot del osnovnega podpisa objekta.

Sestava osnovnega podpisa objektov *CMD

Del objekta	Povezava z osnovnim podpisom objekta
Privzete vrednosti ukazov, spremenjene s CHGCMDDFT	Niso del osnovnega podpisa objekta
Programi za obdelavo ukazov in knjižnic	Vedno so vključeni kot del osnovnega podpisa objekta
Izvorna datoteka REXX in knjižnica	Vključeni sta, če sta podani za ukaz pri podpisovanju, sicer pa nista del osnovnega podpisa objekta
Izvorni član REXX	Vključen je, če je podan za ukaz pri podpisovanju, sicer pa ni del osnovnega podpisa objekta
Ukazno okolje REXX in knjižnica	Vključena sta, če sta podana za ukaz pri podpisovanju, sicer pa nista del osnovnega podpisa objekta
Ime izhodnega programa REXX, knjižnica in izhodna koda	Vključeni so, če so podani za ukaz pri podpisovanju, sicer pa niso del osnovnega podpisa objekta
Program za preverjanje veljavnosti in knjižnica	Vključena sta, če sta podana za ukaz pri podpisovanju, sicer pa nista del osnovnega podpisa objekta
Način veljavnosti	Ni del osnovnega podpisa objekta
Kje se lahko izvaja	Ni del osnovnega podpisa objekta
Omogoči omejene uporabnike	Ni del osnovnega podpisa objekta
Knjižnica polica pomoči	Vključena je, če je podana za ukaz pri podpisovanju, sicer pa ni del osnovnega podpisa objekta

Del objekta	Povezava z osnovnim podpisom objekta
Skupina oken pomoči in knjižnica	Vključena sta, če sta podana za ukaz pri podpisovanju, sicer pa nista del osnovnega podpisa objekta
Identifikator pomoči	Vključena je, če je podan za ukaz pri podpisovanju, sicer pa ni del osnovnega podpisa objekta
Stvarno kazalo pomoči in knjižnica	Vključena sta, če sta podana za ukaz pri podpisovanju, sicer pa nista del osnovnega podpisa objekta
Takoče knjižnica	Vključena je, če je podana za ukaz pri podpisovanju, sicer pa ni del osnovnega podpisa objekta
Knjižnica izdelka	Vključena je, če je podana za ukaz pri podpisovanju, sicer pa ni del osnovnega podpisa objekta
Nadomestni pozivni program in knjižnica	Vključen je, če je podan za ukaz pri podpisovanju, sicer pa ni del osnovnega podpisa objekta
Besedilo (opis)	Ni del osnovnega podpisa objekta niti celotnega podpisa objekta, ker ni shranjen v objektu
Omogoči grafični uporabniški vmesnik (GUI)	Ni del osnovnega podpisa objekta

Obdelava podpisov objektov

Pri podpisovanju objektov lahko podate za obdelavo podpisov naslednje možnosti.

- **Obdelava napak**
  Pri izdelavi podpisov za več objektov lahko podate, katero vrsto obdelave napak naj uporabi aplikacija. Podate lahko, naj aplikacija pri pojavu napake zaustavi podpisovanje objektov ali nadaljuje s podpisovanjem drugih objektov v procesu.
- **Podvojen podpis objekta**
  Podate lahko, kako naj aplikacija obravnava postopek vnovičnega podpisovanja objekta. Aplikacija lahko pusti izvirni podpis ali pa ga zamenja z novim podpisom.
- **Objekti v podimenikih**
  Podate lahko, kako naj aplikacija obravnava podpisovanje objektov v podimenikih. Aplikacija lahko posamezno podpiše vse podimenike ali pa samo objekte znotraj glavnega imenika, podimenike pa zanemari.
- **Območje podpisa objekta**
  Pri podpisovanju objektov *CMD lahko podate, ali želite podpisati celoten objekt ali pa samo njegov osnovni del.

Obdelava preverjanja podpisov

Za obdelavo preverjanja podpisov lahko podate naslednje možnosti.

- **Obdelava napak**
  Pri preverjanju podpisov za več objektov lahko podate, katero vrsto obdelave napak naj uporabi aplikacija. Podate lahko, naj aplikacija pri pojavu napake zaustavi preverjanje podpisov ali nadaljuje s preverjanjem drugih objektov v procesu.
- **Objekti v podimenikih**
  Podate lahko, kako naj aplikacija obravnava preverjanje podpisov za objekte v podimenikih. Aplikacija lahko posamezno preveri podpise za objekte v podimenikih ali pa samo podpise v objektih znotraj glavnega imenika, podimenike pa zanemari.
- **Primerjava preverjanja osnovnih podpisov in celotnih podpisov**
  Sistemska pravila določajo, kako sistem obravnava osnovne in celotne podpise objektov med postopkom preverjanja. Ta pravila so naslednja:
  – Če objekt nima nobenega podpisa, postopek preverjanja sporoči, da objekt ni podpisan in nadaljuje s preverjanjem drugih objektov v procesu.

– Če je objekt podpisal sistemsko preverjen izvor (IBM), se mora podpis ujemati, sicer postopek preverjanja ne uspe. Če se podpis ujema, se postopek preverjanja nadaljuje. Podpis je šifriran matematičen povzetek podatkov v objektu, zato se podpis ujema, če se podatki v objektu med preverjanjem ujemajo s podatki v objektu pri njegovem podpisu.
– če ima objekt celotne podpise objektov, ki so overjeni (na osnovi potrdil iz prostora za potrdila *SIGNATUREVERIFICATION), se mora ujemati vsaj eden izmed teh podpisov, sicer postopek preverjanja ne uspe. Če se ujema vsaj en celoten podpis objekta, se postopek preverjanja nadaljuje.
– Če ima objekt osnovne podpise objektov, ki so overjeni, se mora vsaj eden med njimi ujemati s potrdilom iz prostora za potrdila *SIGNATUREVERIFICATION, sicer postopek preverjanja ne uspe. Če se ujema vsaj eden izmed osnovnih podpisov objektov, se postopek preverjanja nadaljuje.

Predpogoji za podpisovanje objektov in preverjanje podpisov

Funkcije podpisovanja objektov in preverjanja podpisov OS/400 nudijo dodatna močna sredstva za nadzorovanje objektov na strežniku iSeries. Če želite uporabljati te funkcije, morate zadovoljiti predpogoje za njihovo uporabo.

Predpogoji za podpisovanje objektov

Za podpisovanje objektov lahko uporabite številne načine, ki so odvisni od vaših poslovnih in varnostnih potreb:

- Uporabite lahko Upravljalnik digitalnih potrdil (DCM).
- Napišete lahko program, ki uporablja API Podpiši objekt.
- Uporabite lahko funkcijo Osrednjega upravljanja Navigatorja iSeries in podpišete objekte, ko jih pripravite za pošiljanje v sisteme zaključnih točk iSeries.

Način, ki ga izberete za podpisovanje objektov, je odvisen od vaših poslovnih in varnostnih potreb. Ne glede na način, ki ga boste uporabili, morate zagotoviti, da so zadovljeni določeni predpogoji:

- Zadovoljiti morate predpogoje za namestitev in uporabo Upravljalnika digitalnih potrdil (DCM).
  – S pomočjo DCM morate izdelati prostor za potrdila *OBJECTSIGNING. Ta prostor za potrdila izdelate kot del postopka izdelave lokalne službe za pooblastila (CA) ali kot del postopka upravljanja potrdil za podpisovanje objektov prej javne internetne službe za pooblastila.
  – Prostor za potrdila *OBJECTSIGNING mora vsebovati vsaj eno potrdilo; to je lahko potrdilo, ki ste ga izdelali s pomočjo lokalne službe za pooblastila ali potrdilo, ki ste ga pridobili pri javni internetni službi za pooblastila.
  – S pomočjo DCM morate izdelati vsaj eno definicijo aplikacije za podpisovanje objektov, ki jo boste uporabili za podpisovanje objektov.
  – S pomočjo DCM morate dodeliti določeno potrdilo definiciji aplikacije za podpisovanje objektov.
- Profil uporabnika iSeries, ki podpisuje objekte, mora imeti posebno pooblastilo *ALLOBJ. Profil uporabnika iSeries, ki izdela prostor za potrdila *SIGNATUREVERIFICATION, mora imeti posebni pooblastili *SECADM in *ALLOBJ.

Predpogoji za preverjanje podpisov

Za preverjanje podpisov objektov lahko uporabite številne načine:

- Uporabite lahko Upravljalnik digitalnih potrdil (DCM).
- Napišete lahko program, ki uporablja API Preveri objekt (QYDOVFYO).
- Uporabite lahko enega izmed številnih ukazov, kot je na primer CHKOBJITG (Preveri integriteto objekta).

Način, ki ga izberete za preverjanje podpisov, je odvisen od vaših poslovnih in varnostnih potreb. Ne glede na način, ki ga boste uporabili, morate zagotoviti, da so zadovljeni določeni predpogoji:

- Zadovoljiti morate predpogoje za namestitev in uporabo Upravljalnika digitalnih potrdil (DCM).
- Izdelati morate prostor za potrdila *SIGNATUREVERIFICATION. Ta prostor za potrdila lahko izdelate na dva načina. Način, ki ga izberete, je odvisen od vaših potreb. Izdelate ga lahko s pomočjo Upravljalnika digitalnih potrdil (DCM), ki upravlja potrdila za preverjanje podpisov, ali v primeru uporabe javnih potrdil tako, da napišete program, ki uporablja API Dodaj verifikator (QYDOADDV).

  Opomba: API Dodaj verifikator izdela prostor za potrdila s privzetim geslom. S pomočjo DCM morate na novo nastaviti to privzeto geslo, da preprečite nepooblaščen dostop do prostora za potrdila.
- Prostor za potrdila *SIGNATUREVERIFICATION mora vsebovati kopijo potrdila, ki je podpisalo objekte. To potrdilo lahko dodate v prostor za potrdila na dva načina. S pomočjo DCM v podpisnem sistemu lahko izvozite potrdilo v datoteko in nato z DCM v ciljnem preverjalnem sistemu uvozite potrdilo v prostor za potrdila *SIGNATUREVERIFICATION. Če uporabljate za podpisovanje objektov javno potrdilo, lahko dodate potrdilo v prostor za potrdila ciljnega preverjalnega sistema tako, da napišete program, ki uporablja API Dodaj verifikator.
- Prostor za potrdila *SIGNATUREVERIFICATION mora vsebovati kopijo potrdila službe za pooblastila, ki je izdala potrdilo za podpisovanje objektov. Če uporabljate za podpisovanje objektov javno potrdilo, mora prostor za potrdila v ciljnem preverjalnem sistemu že vsebovati kopijo zahtevanega potrdila službe za pooblastila. Če uporabljate potrdilo, ki ga je za podpisovanje objektov izdala lokalna služba za pooblastila, morate s pomočjo DCM dodati kopijo potrdila lokalne službe za pooblastila v prostor za potrdila v ciljnem preverjalnem sistemu.

  Opomba: Zaradi varnostnih razlogov API Dodaj verifikator ne dopušča vstavljanje potrdila službe za pooblastila (CA) v prostor za potrdila *SIGNATUREVERIFICATION. Če dodate potrdilo službe za pooblastila v prostor za potrdila, sistem meni, da je služba za pooblastila overjen izvor potrdil. Posledično obravnava sistema potrdila, ki jih izda služba za pooblastila, kot potrdila iz overjenega izvora. Zato s pomočjo API-ja ne morete izdelati namestitvenega izhodnega programa za vstavljanje potrdila služba za pooblastila v prostor za potrdila. Potrdilo službe za pooblastila morate dodati v prostor za potrdila s pomočjo Upravljalnika digitalnih potrdil, in s tem zagotoviti, da mora nekdo izrecno in ročno nadzorovati, katerim službam za pooblastila zaupa sistem. S tem preprečite možnost, da bi sistem uvozil potrdila iz izvorov, ki jih skrbnik ni izrecno podal kot overjene.

  Če uporabljate potrdilo, ki ga je za podpisovanje objektov izdala lokalna služba za pooblastila, morate s pomočjo DCM na lokalnem gostiteljskem strežniku CA iSeries izvoziti kopijo potrdila lokalne službe za pooblastila v datoteko. Nato lahko s pomočjo DCM na ciljnem preverjalnem strežniku iSeries uvozite potrdilo lokalne službe za pooblastila v prostor za potrdila *SIGNATUREVERIFICATION. Da bi preprečili možno napako, morate uvoziti potrdilo lokalne službe za pooblastila v ta prostor za potrdila preden z API-jem Dodaj verifikator dodate potrdilo za preverjanje podpisov. Če uporabljate potrdilo, ki ga je izdala lokalna služba za pooblastila, vam bo morda preprosteje s pomočjo DCM uvoziti v prostor za potrdila potrdilo službe za pooblastila in potrdilo za preverjanje.

  Če želite preprečiti, da bi kdorkoli uporabil ta API za dodajanje potrdila za preverjanje v prostor za potrdila *SIGNATUREVERIFICATION brez vaše vednosti, lahko onemogočite ta API v sistemu. To lahko naredite s pomočjo sistemskih storitvenih orodij (SST), ki onemogočijo spreminjanje sistemskih vrednosti, povezanih z zaščito .
- Profil uporabnika iSeries, ki preverja podpise, mora imeti posebno pooblastilo *AUDIT. Profil uporabnika iSeries, ki izdela prostor za potrdila *SIGNATUREVERIFICATION ali spremeni njegovo geslo, mora imeti posebni pooblastili *SECADM in *ALLOBJ.

Upravljanje podpisanih objektov

Od izdaje V5R1 naprej je začel IBM s podpisovanjem licenčnih programov OS/400 in PTF-jev, da je uradno označil, da je izvor operacijskega sistema IBM, in omogočil sredstva za odkrivanje nepooblaščenih sprememb v sistemskih objektih. Tudi poslovni partnerji in drugi prodajalci lahko podpišejo aplikacije, ki jih kupite. Tudi če objektov ne podpišete sami, morate razumeti, kako delati s podpisanimi objekti in kako vplivajo podpisani objekti na običajne naloge za upravljanje sistema.

Podpisani objekti vplivajo predvsem na naloge varnostnega kopiranja in obnavljanja, in še posebej na to, kako shranite in obnovite objekte v sistemu.

Sistemske vrednosti in ukazi, ki vplivajo na podpisane objekte
Naučite se o sistemskih vrednostih in ukazih, ki jih lahko uporabite za upravljanje podpisanih objektov, ali ki vplivajo na podpisane objekte pri njihovem izvajanju.

Problematika shranitve in obnovitve podpisanih objektov
Naučite se, kako vplivajo podpisani objekti na izvajanje nalog shranjevanja in obnavljanja v sistemu.

Ukazi nadzornika kode, ki zagotavljajo integriteto podpisov
Spoznajte podrobnosti o uporabi ukazov za preverjanje podpisov objektov za določitev njihove integritete.

Sistemske vrednosti in ukazi, ki vplivajo na podpisane objekte

Za učinkovito upravljanje podpisanih objektov morate razumeti, kako vplivajo sistemske vrednosti in ukazi na podpisane objekte. Sistemska vrednost QVFYOBJRST (**Preveri podpise objektov med obnovitvijo**) določa, kako vplivajo določeni obnovitveni ukazi na podpisane objekte in kako sistem obravnava podpisane objekte med operacijami obnavljanja. Za delo s podpisanimi objekti v sistemu iSeries niso izrecno oblikovani nobeni ukazi CL. Vendar pa obstaja veliko splošnih ukazov CL, ki jih lahko uporabite za upravljanje podpisanih objektov (ali za upravljanje infrastrukturnih objektov, ki omogočajo podpisovanje objektov). Drugi ukazi lahko negativno vplivajo na podpisane objekte v sistemu, saj odstranijo njihove podpise in s tem tudi zaščito, ki jih nudijo.

Sistemske vrednosti, ki vplivajo na podpisane objekte

Sistemska vrednost QVFYOBJRST (**Preveri podpise objektov med obnovitvijo**), član sistemskih vrednosti obnovitvene kategorije OS/400, določa, kako vplivajo ukazi na podpisane objekte v sistemu. Ta sistemska vrednost, ki je na voljo prek Navigatorja iSeries, nadzoruje, kako sistem obravnava preverjanje podpisov med operacijami obnovitve. Nastavitev, ki jo uporabite za to sistemsko vrednost, skupaj z dvema drugima nastavitvama sistemskih vrednosti vpliva na operacije obnavljanja v sistemu. Glede na nastavitev, ki jo izberete za to vrednost, lahko omogoči ali onemogoči obnavljanje objektov na osnovih njihovega statusa podpisa. (Na primer ali objekt ni podpisan, ima neveljaven podpis, podpisal ga je preverjen izvor itd.) Privzeta nastavitev za to sistemsko vrednost omogoča obnovitev nepodpisanih objektov in zagotavlja obnovitev podpisanih objektov samo, če imajo veljaven podpis. Sistem definira, da je objekt podpisan, samo če ima podpis, ki mu vaš sistem zaupa; druge ″neoverjene″ podpise v objektih zanemari in objekte obravnava kot nepodpisane.

Za sistemsko vrednost QVFYOBJRST lahko uporabite veliko vrednosti, vključno z zanemaritvijo vseh podpisov in zahtevo veljavnih podpisov za vse objekte, ki jih sistem obnovi. Ta sistemska vrednost vpliva samo na izvršilne objekte, ki jih obnovite, kot so programi (*PGM), ukazi (*CMD), storitveni programi (*SRVPGM), paketi SQL (*SQLPKG) in moduli (*MODULE). Velja tudi za objekte tokovne datoteke (*STMF), ki imajo povezane programe Java, izdelane z ukazom CRTJVAPGM (Izdelaj program Java). Ne velja pa za shranitvene datoteke (*SAV) ali datoteke IFS.

Če se želite naučiti več o uporabi te in drugih sistemskih vrednosti, preberite temo Informacijskega centra Iskalnik sistemskih vrednosti.

Ukazi CL, ki vplivajo na podpisane objekte

Na voljo je veliko ukazov CL, ki omogočajo delo s podpisanimi objekti ali ki vplivajo na podpisane objekte na strežniku iSeries. Z različnimi ukazi si lahko ogledate informacije o podpisih objektov, preverite podpise objektov ter shranite in obnovite varnostne objekte, zahtevane za preverjanje podpisov. Poleg tega obstaja tudi skupina ukazov, ki lahko pri izvajanju odstranijo podpis objektov in razveljavijo zaščito, ki jo nudijo podpisi.

Ukazi za prikaz informacij o podpisu objekta

- Ukaz DSPOBJD (Prikaži opis objekta).
  Ta ukaz prikaže ime in lastnosti podanih objektov v podani knjižnici ali v knjižnicah s seznama knjižnic niti. S pomočjo tega ukaza lahko določite, ali je objekt podpisan, in prikažete informacije o podpisu.
- Ukaza integriranega datotečnega sistema DSPLNK (Prikaži povezave objekta) in WRKLNK (Delo s povezavami objekta).
  S tema ukazoma lahko prikažete informacije o podpisu objekta v integriranem datotečnem sistemu.

Ukazi za preverjanje podpisov objektov

- Ukaz CHKOBJITG (Preveri integriteto objekta).
  Ta ukaz omogoča, da določite, ali objekti v sistemu kršijo integriteto. S pomočjo tega ukaza lahko preverite podpise podobno kot z nadzornikom virusov, ki določi, ali je virus okvaril datoteke ali druge objekte v sistemu. Če se želite naučiti več o uporabi tega ukaza s podpisanimi objekti in z objekti, ki jih je mogoče podpisati, preberite temo Ukazi nadzornika kode za zagotavljanje integritete podpisov.
- Ukaz CHKPRDOPT (Preveri možnost izdelka).
  Ta ukaz sporoči razlike med pravilno strukturo in dejansko strukturo izdelka programske opreme. Ukaz na primer sporoči napako, če je objekt zbrisan iz nameščenega izdelka. S pomočjo parametra CHKSIG lahko podate, kako naj ukaz obravnava in sporoči možne težave v podpisu izdelka. Če se želite naučiti več o uporabi tega ukaza s podpisanimi objekti in z objekti, ki jih je mogoče podpisati, preberite temo Ukazi nadzornika kode za zagotavljanje integritete podpisov.
- Ukaz SAVLICPGM (Shrani licenčni program).
  Ta ukaz shrani kopijo objektov, ki tvorijo licenčni program. Licenčni program shrani v takšni obliki, da ga je mogoče obnoviti z ukazom RSTLICPGM (Obnovi licenčni program). S pomočjo parametra CHKSIG lahko podate, kako naj ukaz obravnava in sporoči možne težave v podpisu izdelka. Če se želite naučiti več o uporabi tega ukaza s podpisanimi objekti in z objekti, ki jih je mogoče podpisati, preberite temo Ukazi nadzornika kode za zagotavljanje integritete podpisov.
- Ukaz RST (Obnovi).
  Ta ukaz obnovi kopijo enega ali več objektov, ki jih je mogoče uporabiti v integriranem datotečnem sistemu (IFS). Ukaz omogoča tudi obnovitev prostorov za potrdila in njihove vsebine. Vendar pa tega ukaza ne morete uporabiti za obnovitev prostora za potrdila *SIGNATUREVERIFICATION. Kako ukaz za obnovitev obravnava podpisane objekte in objekte, ki jih je mogoče podpisati, določa nastavitev za sistemsko vrednost QVFYOBJRST (Preveri podpise objektov med obnovitvijo).
- Ukaz RSTLIB (Obnovi knjižnico).
  Ta ukaz obnovi eno knjižnico ali skupino knjižnic, ki ste jih shranili z ukazom SAVLIB (Shrani knjižnico). Ukaz RSTLIB obnovi celotno knjižnico, kar vključuje opis knjižnice, opise objektov in vsebino objektov v knjižnici. Kako ta ukaz obravnava podpisane objekte in objekte, ki jih je mogoče podpisati, določa nastavitev za sistemsko vrednost QVFYOBJRST (Preveri podpise objektov med obnovitvijo).
- Ukaz RSTLICPGM (Obnovi licenčni program).
  Ta ukaz naloži ali obnovi licenčni program, in sicer za začetno namestitev ali namestitev nove izdaje. Kako ta ukaz obravnava podpisane objekte in objekte, ki jih je mogoče podpisati, določa nastavitev za sistemsko vrednost QVFYOBJRST (Preveri podpise objektov med obnovitvijo).
- Ukaz RSTOBJ (Obnovi objekt).
  Ta ukaz obnovi enega ali več objektov v eni knjižnici, ki so bili shranjeni na disketo, na trak, na optični

nosilec ali v shranitveno datoteko z uporabo enega ukaza. Kako ta ukaz obravnava podpisane objekte in objekte, ki jih je mogoče podpisati, določa nastavitev za sistemsko vrednost QVFYOBJRST (Preveri podpise objektov med obnovitvijo).

Ukazi za shranjevanje in obnavljanje prostorov za potrdila

- Ukaz SAV (Shrani).
  Ta ukaz omogoča, da shranite kopijo enega ali več objektov, ki jih je mogoče uporabiti v integriranem datotečnem sistemu, vključno s prostori za potrdila. Vendar pa tega ukaza ne morete uporabiti za shranitev prostora za potrdila *SIGNATUREVERIFICATION.
- Ukaz SAVSECDTA (Shrani varnostne podatke).
  Ta ukaz omogoča, da shranite vse varnostne informacije, ne da bi moral biti sistem zato v omejenem stanju. Uporaba tega ukaza omogoča shranitev prostora za potrdila *SIGNATUREVERIFICATION in potrdil, ki jih vsebuje. Ta ukaz ne shrani nobenega drugega prostora za potrdila.
- Ukaz SAVSYS (Shrani sistem).
  Ta ukaz omogoča, da shranite kopijo licenčne notranje kode in knjižnice QSYS v formatu, ki je združljiv z namestitvijo strežnika iSeries. Ukaz ne shranite objektov iz nobene druge knjižnice. Poleg tega pa omogoča, da shranite varnostne in konfiguracijske objekte, ki jih lahko shranite tudi z ukazoma SAVSECDTA in SAVCFG. Uporaba tega ukaza omogoča shranitev prostora za potrdila *SIGNATUREVERIFICATION in potrdil, ki jih vsebuje.
- Ukaz RST (Obnovi).
  Ta ukaz omogoča, da v sistemu obnovite prostore za potrdila in njihovo vsebino. Vendar pa tega ukaza ne morete uporabiti za obnovitev prostora za potrdila *SIGNATUREVERIFICATION.
- Ukaz RSTUSRPRF (Obnovi profile uporabnikov).
  Ta ukaz omogoča, da obnovite osnovne dela profila uporabnika ali niz profilov uporabnikov, ki ste jih shranili z ukazom SAVSYS (Shrani sistem) ali z ukazom SAVSECDTA (Shrani varnostne podatke). Ta ukaz lahko uporabite za obnovitev prostora za potrdila *SIGNATUREVERIFICATION in skritih gesel prostorov za potrdila. Prostor za potrdila *SIGNATUREVERIFICATION lahko obnovite, ne da bi obnovili informacije o profilu uporabnika, s tem da podate *DCM kot vrednost za parameter SECDTA in *NONE za parameter USRPRF. Če želite uporabiti ta ukaz za obnovitev informacij o profilu uporabnika ter prostorov za potrdila in njihovih gesel, podajte *ALL za parameter USRPRF.

Ukazi, ki lahko odstranijo podpise objektov

Če uporabite naslednje ukaze v podpisanih objektih, lahko to naredite na način, da odstranite njihove podpise. Odstranitev podpisov lahko povzroči težave v objektih. Če nič drugega, ne boste več mogli preveriti izvora objekta in podpisa objekta in v njem odkriti sprememb. Te ukaze uporabljajte samo v tistih podpisanih objektih, ki ste jih izdelelali sami (za razliko od podpisanih objektov, ki jih dobite od drugje, kot na primer pri IBM-u ali drugih proizvajalcih). Če vas skrbi, da je ukaz odstranil podpis objekta, s pomočjo ukaza DSPOBJD (Prikaži opis objekta) preverite, ali podpis še obstaja in objekt po potrebi znova podpišite.

Opomba: Če želite preveriti, ali je ukaz za shranitev odstranil podpis objekta, morate obnoviti objekt v knjižnico, ki ni tista, iz katere ste ga shranili (na primer QTEMP). Nato lahko s pomočjo ukaza DSPOBJD določite, ali je objekt na shranjevalnem nosilcu izgubil svoj podpis.

- Ukaz CHGPGM (Spremeni program).
  Ta ukaz spremeni lastnosti program, ne da bi zahteval njegovo vnovično prevajanje. Ukaz lahko uporabite tudi, če želite prisiliti vnovično izdelavo programa, tudi če so lastnosti, ki jih podate, iste kot trenutne lastnosti.
- Ukaz CHGSRVPGM (Spremeni storitveni program).
  Ta ukaz spremeni lastnosti storitvenega program, ne da bi zahteval njegovo vnovično prevajanje. Ukaz lahko uporabite tudi, če želite prisiliti vnovično izdelavo storitvenega programa, tudi če so lastnosti, ki jih podate, iste kot trenutne lastnosti.
- Ukaz CLRSAVF (Počisti shranjevalno datoteko).
  Ta ukaz počisti vsebino shranjevalne datoteke; iz shranjevalne datoteke počisti vse obstoječe zapise in zmanjša pomnilnik, ki ga uporablja datoteka.

- Ukaz SAV (Shrani).
  Ta ukaz shrani kopijo enega ali več objektov, ki jih je mogoče uporabiti v integriranem datotečnem sistemu. — Pri uporabi tega ukaza lahko izgubite podpise v ukaznih (*CMD) objektih na shranjevalnem nosilcu, če podate za parameter TGTRLS vrednost pred V5R2M0. Do izgube podpisov pride, ker ukaznih objektov v izdajah pred V5R2 ni mogoče podpisati.
- Ukaz SAVLIB (Shrani knjižnico).
  Ta ukaz omogoča, da shranite kopijo ene ali več knjižnic. Pri uporabi tega ukaza lahko izgubite podpise v ukaznih (*CMD) objektih na shranjevalnem nosilcu, če podate za parameter TGTRLS vrednost pred V5R2M0. Do izgube podpisov pride, ker ukaznih objektov v izdajah pred V5R2 ni mogoče podpisati.
- Ukaz SAVOBJ (Shrani objekt).
  Ta ukaz shrani kopijo enega objekta ali skupine objektov v isti knjižnici. Pri uporabi tega ukaza lahko izgubite podpise v ukaznih (*CMD) objektih na shranjevalnem nosilcu, če podate za parameter TGTRLS vrednost pred V5R2M0. Do izgube podpisov pride, ker ukaznih objektov v izdajah pred V5R2 ni mogoče podpisati.

Problematika shranitve in obnovitve podpisanih objektov

Obstaja precej sistemskih vrednosti, ki lahko vplivajo na operacije shranjevanja za strežnik iSeries. Toda samo ena izmed teh sistemskih vrednosti, **QVFYOBJRST (Preveri podpise objektov med obnovitvijo)**, določa, kako sistem obravnava podpisane objekte med obnovitvijo. Nastavitev, ki jo izberete za to sistemsko vrednost, določa, kako postopek obnovitve obravnava preverjanje objektov brez podpisov ali z neveljavnimi podpisi.

Nekateri ukazi za shranitev in obnovitev vplivajo na podpisane objekte ali določajo, kako bo sistem obravnaval podpisane ali nepodpisane objekte med operacijami shranitve in obnovitve. Te ukaze morate razumeti in se zavedati vpliva, ki ga imajo na podpisane objekte, da boste bolje upravljali sistem in se izognili možnim težavam.

Naslednji ukazi lahko preverijo podpise v objektih med operacijami shranitve in obnovitve:
- Ukaz SAVLICPGM (Shrani licenčni program).
- Ukaz RST (Obnovi).
- Ukaz RSTLIB (Obnovi knjižnico).
- Ukaz RSTLICPGM (Obnovi licenčni program).
- Ukaz RSTOBJ (Obnovi objekt).

Ti ukazi omogočajo shranitev in obnovitev prostorov za potrdila; prostori za potrdila so na zaščito občutljivi objekti, ki vsebujejo potrdila, ki jih uporabljate za podpisovanje objektov in preverjanje podpisov:
- Ukaz SAV (Shrani).
- Ukaz SAVSECDTA (Shrani varnostne podatke).
- Ukaz SAVSYS (Shrani sistem).
- Ukaz RST (Obnovi).
- Ukaz RSTUSRPRF (Obnovi profile uporabnikov).

Nekateri ukazi za shranitev lahko glede na vrednost parametra, ki jo uporabite, odstranijo podpis objekta na shranjevalnem nosilcu in s tem razveljavijo zaščito, ki jo nudijo podpisi. Tako na primer *katerakoli* operacija shranitve, ki se nanaša na ukazni (*CMD) objekt s ciljno izdajo pred V5R2M0, povzroči shranitev ukazov brez podpisov. Odstranitev podpisov lahko povzroči težave v objektih, na katere se nanaša. Če nič drugega, ne boste več mogli preveriti izvora objekta in podpisa objekta in v njem odkriti sprememb. Te ukaze uporabite samo v tistih podpisanih objektih, ki ste jih izdelali sami (za razliko od podpisanih objektov, ki jih prejmete od drugje, kot na primer pri IBM-u ali pri drugih proizvajalcih).

Opomba: Če želite preveriti, ali je ukaz za shranitev odstranil podpis objekta, morate obnoviti objekt v knjižnico, ki ni tista, iz katere ste ga shranili (na primer QTEMP). Nato lahko s pomočjo ukaza DSPOBJD določite, ali je objekt na shranjevalnem nosilcu izgubil svoj podpis.

Te možnosti se morate zavedati pri naslednjih specifičnih shranjevalnih ukazih, kot tudi na splošno pri shranjevalnih ukazih:

- Ukaz SAV (Shrani).
- Ukaz SAVLIB (Shrani knjižnico).
- Ukaz SAVOBJ (Shrani objekt).

Podrobnejše informacije o vplivu teh ukazov na podpisane objekte in o podpisih objektov med operacijami shranitve in obnovitve lahko najdete v temi Sistemske vrednosti in ukazi, ki vplivajo na podpisane objekte.

Ukazi nadzornika kode, ki zagotavljajo integriteto podpisov

Za preverjanje podpisov v objektih lahko uporabite Upravljalnik digitalnih potrdil (DCM) ali API-je. Prav tako lahko uporabite tudi številne ukaze. S pomočjo teh ukazov lahko preverite te podpise podobno kot z nadzornikom virusov, ki določi, ali je virus okvaril datoteke ali druge objekte v sistemu. Večina podpisov je preverjena pri obnovitvi ali namestitvi objekta v sistem, na primer s pomočjo ukaza RSTLIB.

Za preverjanje podpisov v objektih, ki so že v sistemu, lahko uporabite enega izmed treh ukazov. Med temi je ukaz CHKOBJITG (Preveri integriteto objekta) posebej oblikovan za preverjanje podpisov objektov. Preverjanje podpisov za te ukaze krmili parameter CHKSIG. Ta parameter omogoča, da preverite vse tipe objektov, ki jih lahko podpišete, zanemarite vse podpise in preverite samo tiste objekte, ki so podpisani. Zadnja možnost je privzeta vrednost tega parametra.

Ukaz CHKOBJITG (Preveri integriteto objekta)

Ukaz CHKOBJITG (Preveri integriteto objekta) omogoča, da določite, ali je v katerem od objektov v sistemu prišlo do kršitve integritete. S pomočjo tega ukaza lahko preverite kršitve integritete v objektih, katerih lastnik je določen profil uporabnika, v objektih, ki se ujemajo z določeno potjo ali v vseh objektih v sistemu. Vnos v dnevnik kršitev integritete je zabeležen, če se zgodi nekaj od naslednjega:

- Lastnosti ukaza, programa, objekta modula ali knjižnice so bile spremenjene.
- Digitalni podpis objekta je določen kot neveljaven. Podpis je šifriran matematičen povzetek podatkov v objektu, zato se zapis ujema in je veljaven, če se podatki v objektu med preverjanjem ujemajo s podatki v objektu pri njegovem podpisu. Neveljaven podpis je določen na osnovi primerjave šifriranega matematičnega povzetka, ki je izdelan pri podpisu objekta, in šifriranega matematičnega povzetka, izdelanega med preverjanjem podpisa. Postopek preverjanja podpisov primerja dve vrednosti povzetka. Če vrednosti nista enaki, je bila vsebina objekta od njegovega podpisa spremenjena, zato je podpis določen kot neveljaven.
- Objekt ima neveljavno lastnost domene za tip objekta.
-

Če odkrije ukaz kršitev integritete v objektu, doda v datoteko dnevnika baze podatkov ime objekta, ime knjižnice (ali pot), tip objekta, lastnika objekta in vrsto napake. Ukaz v nekaterih drugih primerih tudi izdela vnos dnevnika, čeprav ti primeri niso kršitve integritete. Ukaz na primer izdela vnos dnevnika za objekte, ki jih je mogoče podpisati, vendar nimajo digitalnega podpisa, za objekte, ki jih ni mogoče preveriti in za objekte v formatu, ki zahtevajo spremembo, da bi jih bilo mogoče uporabiti v trenutni izvedbi sistema (pretvorba iz IMPI v RISC).

Vrednost parametra CHKSIG krmili, kako obravnava ukaz digitalne podpise v objektih. Za ta parameter lahko podate eno od treh vrednosti:

- *SIGNED – Če podate to vrednost, preveri ukaz objekte z digitalnimi podpisi. Ukaz izdela vnos dnevnika za vse objekte z neveljavnim podpisom. To je privzeta vrednost.

- *ALL – Če podate to vrednost, preveri ukaz vse objekte, ki jih je mogoče podpisati, da določi, ali imajo podpis. Ukaz izdela vnos dnevnika za vse objekte, ki jih je mogoče podpisati, vendar nimajo podpisa, in za vse objekte z neveljanim podpisom.
- *NONE – Če podate to vrednost, ukaz ne preveri digitalnih podpisov v objektih.

Ukaz CHKPRDOPT (Preveri možnost izdelka)

Ukaz CHKPRDOPT (Preveri možnost izdelka) sporoči razlike med pravilno strukturo in dejansko strukturo izdelka programske opreme. Ukaz na primer sporoči napako, če je objekt zbrisan iz nameščenega izdelka.

Vrednost parametra CHKSIG krmili, kako obravnava ukaz digitalne podpise v objektih. Za ta parameter lahko podate eno od treh vrednosti:

- *SIGNED – Če podate to vrednost, preveri ukaz objekte z digitalnimi podpisi. Ukaz preveri podpise v vseh podpisanih objektih. Če ukaz določi, da podpis v objektu ni veljaven, pošlje v dnevnik opravil sporočilo in določi, da je izdelek v napačnem stanju. To je privzeta vrednost.
- *ALL – Če podate to vrednost, preveri ukaz vse objekte, ki jih je mogoče podpisati, da določi, ali imajo podpis, ki ga tudi preveri. Ukaz pošlje v dnevnik opravil sporočilo za vse objekte, ki jih je mogoče podpisati, vendar nimajo podpisa, toda ukaz ne določi izdelka kot napačnega. Če ukaz določi, da podpis objekta ni veljaven, pošlje v dnevnik opravil sporočilo in nastavi izdelek kot napačen.
- *NONE – Če podate to vrednost, ukaz ne preveri digitalnih podpisov v objektih izdelka.

Ukaz SAVLICPGM (Shrani licenčni program)

Ukaz SAVLICPGM (Shrani licenčni program) omogoča, da shranite kopijo objektov, ki tvorijo licenčni program. Licenčni program shrani v takšni obliki, da ga je mogoče obnoviti z ukazom RSTLICPGM (Obnovi licenčni program).

Vrednost parametra CHKSIG krmili, kako obravnava ukaz digitalne podpise v objektih. Za ta parameter lahko podate eno od treh vrednosti:

- *SIGNED – Če podate to vrednost, preveri ukaz objekte z digitalnimi podpisi. Ukaz preveri podpise v vseh podpisanih objektih, ne pa tudi v nepodpisanih. Če ukaz določi, da podpis objekta ni veljaven, pošlje v dnevnik opravil sporočilo, ki določa objekt, shranitev pa ne uspe. To je privzeta vrednost.
- *ALL – Če podate to vrednost, preveri ukaz vse objekte, ki jih je mogoče podpisati, da določi, ali imajo podpis, ki ga tudi preveri. Ukaz pošlje v dnevnik opravil sporočilo za vse objekte, ki jih je mogoče podpisati, vendar nimajo podpisa, toda postopek shranitve se ne konča. Če ukaz določi, da podpis objekta ni veljaven, pošlje v dnevnik opravil sporočilo, shranitev pa ne uspe.
- *NONE – Če podate to vrednost, ukaz ne preveri digitalnih podpisov v objektih izdelka.

Odpravljanje težav v podpisanih objektih

Naslednje tabele vam bodo pomagale poiskati informacije, ki vam bodo v pomoč pri odpravljanju nekaterih najpogostejših težav, na katere lahko naletite pri delu s funkcijami podpisovanja objektov in preverjanja podpisov iSeries.

Splošne težave pri podpisovanju objektov

Težava	Možna rešitev
Če uporabite API Podpiši objekt za podpisovanje objekta v ciljni izdaji V4R5 ali starejši, postopek podpisovanja ne uspe in objekt ni podpisan (sporočilo o napaki CPFB721).	iSeries ne nudi podpore za podpisovanje objektov do izdaje V5R1. Za tiste objekte, ki vrnejo sporočilo o napaki CPFB721, morate znova izdelati te programe s ciljno izdajo V5R1 ali novejšo in jih nato podpisati.

Splošne težave pri preverjanju podpisov

Težava	Možna rešitev
Postopek obnovitve za objekte brez podpisov ne uspe.	Če vas izguba podpisa ne skrbi, preverite, ali je sistemska vrednost QVFYOBJRST nastavljena na 5. Vrednost 5 namreč podaja, da nepodpisanih objektov ni mogoče obnoviti. Vrednost spremenite v 3 in ponovite obnovitev.
Postopek obnovitve za objekte s podpisi ne uspe.	To se lahko zgodi, če ste prostor za potrdila *SIGNATUREVERIFICATION prenesli v sistem in njegovega gesla niste spremenili s pomočjo DCM. V tem primeru ni mogoče uporabiti potrdil, ki jih vsebuje prostor za potrdila, za preverjanje podpisov v objektih med postopkom obnovitve. S pomočjo DCM spremenite geslo prostora za potrdila. Če ne poznate gesla, morate prostor za potrdila zbrisati in ga nato znova izdelati s pomočjo DCM.
Pri obnovitvi ali namestitvi izdelka pride do napake, ker preverjanje podpisa ne uspe.	Če preverjanja podpisa objekta ni mogoče pravilno opraviti, lahko napaka kaže, da je bil objekt od podpisa spremenjen. Če vas skrbi integriteta objekta, ne spremenite sistemske vrednosti QVFYOBJRST in ne izvedite kakšnega drugega dejanja, ki bi lahko omogočilo obnovitev vprašljivega objekta. S tem bi namreč razveljavili zaščito, ki jo nudi preverjanje podpisa, in omogočili vstop škodljivemu objektu v sistem. Namesto tega se obrnite na podpisnika objekta, ki bo določil ustrezno dejanje za rešitev težave.

Povezane informacije za podpisovanje objektov in preverjanje podpisov

Podpisovanje objektov in preverjanje podpisov sta dokaj novi tehnologiji za zaščito. Sledi kratek seznam drugih virov, ki vam bodo koristili, če želite bolje razumeti ti tehnologiji in njuno delovanje:

- **Spletna stran VeriSign Help Desk**
  Spletna stran podjetja VeriSign nudi obsežno knjižnico s temami o digitalnih potrdilih, kot je podpisovanje objektov, kot tudi številne druge podteme o internetni zaščiti.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Ta rdeča IBM-ova knjiga je usmerjena na izboljšave v omrežni zaščiti v izdaji V5R1. Knjiga vsebuje številne teme, ki vključujejo tudi uporabo funkcij podpisovanja objektov iSeries, Upravljalnik digitalnih potrdil (DCM) in druge.

Natisnjeno na Danskem