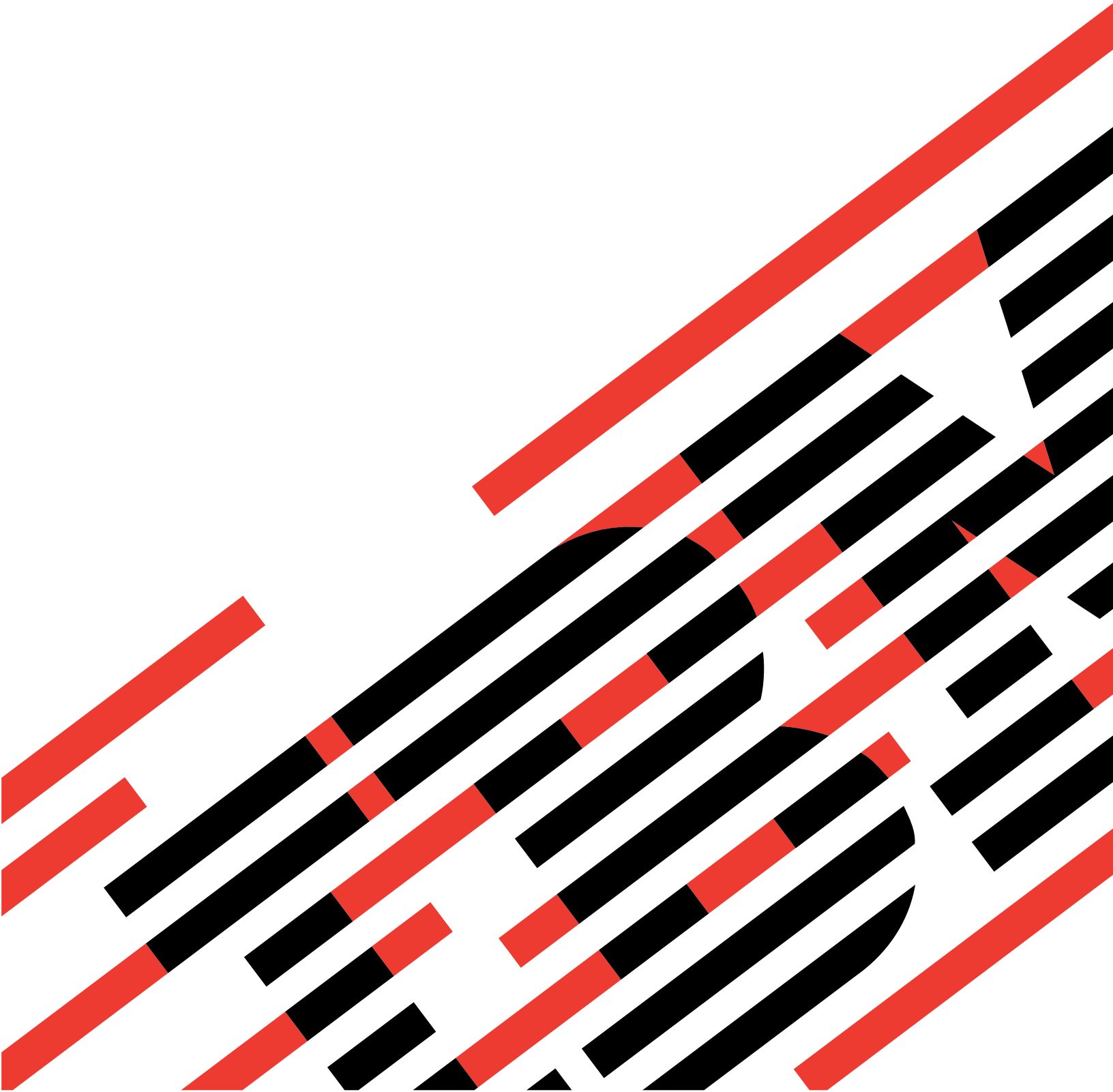
IBM

eserver

iSeries

Potpisivanje objekata i provjera potpisa

Verzija 5 Izdanje 3



IBM

@server

iSeries

Potpisivanje objekata i provjera potpisa

Verzija 5 Izdanje 3

Napomena

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene”, na stranici 43.

Treće izdanje (kolovoz, 2005)

Ovo izdanje se primjenjuje na verziju 5, izdanje 3, modifikacija 0 Operating System/400 (broj proizvoda 5722) i na sva naredna izdanja i modifikacije, sve dok se drukčije ne naznači u novim izdanjima. Ova verzija ne radi na svim modelima računala smanjenog seta instrukcija (RISC) niti ne radi na CISC modelima.

Sadržaj

Potpisivanje objekata i provjera potpisa 1

| Što je novo za V5R3 2
Ispis ovog poglavlja 2
Scenariji potpisivanja objekata 2
Scenarij: Upotreba DCM-a za potpisivanje objekata i provjeru potpisa 3
Scenarij: Upotreba API-ja za potpisivanje objekata i provjeru potpisa objekata 11
Scenarij: Upotreba iSeries Navigator Središnjeg Upravljanja za potpisivanje objekata 21
Koncepti potpisivanja objekta 28
Digitalni potpisi 29
Potpisivi objekti 30
Obrada potpisivanja objekta 31
Obrada provjere potpisa 31
| Funkcija provjere integriteta provjeravatelja koda . . 32
Preduvjeti potpisivanja objekata i provjere potpisa . . . 32
Upravljanje potpisanim objektima 34
Sistemske vrijednosti i naredbe koje utječu na potpisane objekte 34
Razmatranja o spremanju i vraćanju potpisanih objekata 37
Naredbe kontrolora koda za osiguranje cjelovitosti potpisa 38
| Provjera integriteta funkcije provjere koda 39
Rješavanje problema potpisanih objekata 40
Rješavanje problema grešaka potpisivanja objekta . . 40
Rješavanje problema grešaka provjere potpisa . . . 40
Poruke grešaka provjere interpretiranja provjeritelja koda 41
Povezane informacije za potpisivanje objekta i provjeru potpisa 42
Izjava o odricanju od koda 42

Dodatak. Napomene 43

Zaštitni znaci 45
Termini i uvjeti za spuštanje i ispis publikacija 45
Informacije o odricanju od koda. 46

Potpisivanje objekata i provjera potpisa

Potpisivanje objekata i provjera potpisa su sigurnosne mogućnosti koje možete primijeniti za provjeru cjelovitosti raznolikih iSeries objekata. Koristite privatni ključ digitalnog certifikata za potpisivanje objekta i koristite certifikat (koji sadrži odgovarajući javni ključ) za provjeru digitalnog potpisa. Digitalni potpis osigurava cjelovitost vremena i sadržaja objekta kojeg potpisujete. Potpis daje dokaz autentičnosti i autorizacije. Može se upotrebljavati za dokaz porijekla i otkrivanje neovlaštenih promjena. Potpisivanjem objekta identificirate izvor objekta i pružate načine otkrivanja promjena na objektu. Kad provjeravate potpis na objektu možete odrediti da li su se desile promjene u sadržajima objekta od kad je bio potpisan. Možete također provjeriti izvor potpisa da možete jamčiti pouzdanost porijekla objekta.

Možete primijeniti iSeries potpisivanje objekta i provjeru potpisa pomoću:
- API-ja za potpisivanje objekata i programatsku provjeru potpisa na objektima.
- Upravitelja digitalnih certifikata za potpisivanje objekata i za gledanje ili provjeru potpisa objekata.
- iSeries Navigator Središnje Upravljanje za potpisivanje objekata kao dio distributivnog paketa za korištenje drugih sistema.
- CL naredbe, kao Provjera integriteta objekta (CHKOBJITG) za provjeru potpisa.

Da doznate još o ovim metodama potpisivanja objekata i kako potpisivanje objekata može poboljšati trenutnu politiku sigurnosti, pročitajte ova poglavlja:

Što je novo za V5R3
Pročitajte ove informacije da se upoznate s novim sposobnostima iSeries potpisivanja objekata i provjere potpisa kao i promjenama u dokumentaciji ovog izdanja.

Ispis ovog poglavlja
Upotrijebite ove informacije da ispišete cijelo poglavlje kao PDF datoteku.

Scenariji
Upotrijebite ove informacije da pregledate scenarije koji objašnjavaju neke tipične situacije za upotrebu sposobnosti iSeries potpisivanja objekata i provjeru potpisa. Svaki scenarij također pruža zadatke za konfiguraciju koje morate obaviti da primijenite scenarij prema opisu.

Koncepti
Upotrijebite ovaj koncept i referentne informacije da naučite još o radu na obradama digitalnih potpisa i potpisivanju objekata i provjeri potpisa.

Potpisivanje objekta i preduvjeti provjere potpisa
Upotrijebite ove informacije da naučite još o preduvjetima konfiguracije kao i o drugim razmatranjima planiranja za potpisivanje objekata i provjeru potpisa.

Upravljanje potpisanim objektima
Upotrijebite ove informacije da naučite o iSeries naredbama i sistemskim vrijednostima koje možete upotrijebiti za rad s potpisanim objektima i kako potpisani objekti utječu na obrade sigurnosnih kopiranja i obnavljanja.

Rješavanje problema potpisivanja objekata i provjere potpisa
Koristite ove informacije da naučite kako riješiti probleme i greške koje se mogu desiti pri potpisivanju objekata i provjeri potpisa.

Povezane informacije
Koristite ove informacije da nađete veze na druge resurse i naučite više o potpisivanju objekata i provjeri potpisa objekata.

Ova izjava o odricanju od kodu pripada primjerima koji su dani u ovom poglavlju.

Što je novo za V5R3

Sposobnosti potpisivanja objekata i provjere potpisa za iSeries su prvo uvedene u V5R1. Međutim, postoje nove funkcije i poboljšanja dostupni u V5R3.

Nove ili poboljšane funkcije za potpisivanje objekta i provjeru potpisa uključuju:
- **iSeries provjera cjelovitosti sistema**
  Počevši s V5R3 možete provjeriti integritet svih IBM-otpremljenih kodova za vaš iSeries sistem.
- **Provjera funkcije provjere koda**
  Počevši s V5R3 možete provjeriti integritet svih funkcija provjere koda koje provjeravaju kod sistema i ostale potpisane objekte na vašem iSeries sistemu.

Da vidite ostale informacije o tome što je novo ili promijenjeno u ovom izdanju, pogledajte Memorandum za korisnike .

Kako vidjeti što je novo ili promijenjeno

Da bi lakše vidjeli gdje su napravljene tehničke promjene, ove informacije koriste:
- Sliku za označavanje gdje počinju nove ili promijenjene informacije.
- Sliku za označavanje gdje nove ili promijenjene informacije završavaju.

Ispis ovog poglavlja

Za pogled ili spuštanje PDF verzije dokumenta, pogledajte Potpisivanje objekta i provjera potpisa (veličina datoteke 605 KB).

Spremanje PDF datoteka:

Da spremite PDF na vašu radnu stanicu za pregled ili ispis:
1. Desno kliknite na PDF u vašem pretražitelju (desno kliknite gornju vezu).
2. Kliknite **Save Target As...** ako koristite Internet Explorer. Kliknite **Save Link As...** ako koristite Netscape Communicator.
3. Izaberite direktorij u koji želite spremiti PDF.
4. Kliknite **Save**.

Spuštanje Adobe Acrobat Readera

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

Scenariji potpisivanja objekata

iSeries poslužitelj pruža nekoliko različitih metoda za potpisivanje objekata i provjeru potpisa na objektima. Kako birate potpisivanje objekata i kako radite s potpisanim objektima zavisi o vašem poslu i potrebama i ciljevima sigurnosti. U nekim slučajevima možda trebate samo provjeriti potpise objekata na sistemu da se uvjerite da je cjelovitost objekta netaknuta. U drugim slučajevima, možete izabrati potpisivanje objekata koje distribuirate drugima. Potpisivanje objekata omogućuje drugima da identificiraju porijeklo objekata i provjere cjelovitost objekata.

Koju metodu ćete izabrati za upotrebu ovisi o različitim faktorima. Scenariji u ovom poglavlju opisuju neke od uobičajenijih ciljeva potpisivanja objekta i provjere potpisa u tipično poslovnom kontekstu. Svaki scenarij također

opisuje sve preduvjete i zadatke koje morate obaviti da primijenite scenarij prema opisu. Pregledajte ove scenarije da vam pomognu u određivanju kako možete upotrijebiti sposobnosti iSeries potpisivanja objekata na način koji najbolje odgovara vašim poslovnim i sigurnosnim potrebama:

Scenarij: Upotreba Upravitelja digitalnih certifikata za potpisivanje objekata i provjeru potpisa
Ovaj scenarij opisuje poduzeće koje želi potpisivati ranjive objekte aplikacije na svom javnom Web poslužitelju. Oni žele mogućnost lakšeg određivanja postojanja neovlaštenih promjena na ovim objektima. Na osnovu potreba posla poduzeća i sigurnosnih ciljeva ovaj scenarij opisuje kako upotrebljavati Upravitelja digitalnih certifikata (DCM) kao primarnu metodu za potpisivanje objekata i provjeru potpisa objekata.

Scenarij: Upotreba API-ja za potpisivanje objekata i provjeru potpisa
Ovaj scenarij opisuje poduzeće za razvoj aplikacija koje želi programatski potpisivati aplikacije koje prodaje. Oni žele biti sposobni uvjeriti svoje korisnike da su aplikacije došle iz njihovog poduzeća i žele im osigurati način za otkrivanje neovlaštenih promjena na aplikacijama kad ih instaliraju. Na osnovi potreba posla poduzeća i sigurnosnih ciljeva ovaj scenarij opisuje kako upotrebljavati API za Potpisivanje objekata i API za dodavanje provjeritelja za potpisivanje objekata i omogućavanje potpisa objekata.

Scenarij: Upotreba Središnjeg Upravljanja za potpisivanje objekata
Ovaj scenarij opisuje poduzeće koje želi potpisivati objekte koje pakira i distribuira višestrukim iSeries poslužiteljima. Na osnovi potreba posla poduzeća i sigurnosnih ciljeva ovaj scenarij opisuje kako upotrebljavati funkciju iSeries Navigator Središnjeg Upravljanja za pakiranje i potpisivanje objekata koje oni distribuiraju drugim iSeries poslužiteljima.

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

Situacija

Kao iSeries administrator za Myco, Inc. odgovorni ste za upravljanje s dva iSeries poslužitelja vašeg poduzeća. Jedan od tih iSeries poslužitelja pruža javnu Web stranicu za vaše poduzeće. Upotrebljavate interni proizvodni iSeries poslužitelj poduzeća za razvoj sadržaja za te javne Web stranice i prijenos objekata datoteka i programa javnom Web poslužitelju nakon njihovog testiranja.

Javni Web poslužitelj poduzeća sadrži Web stranicu s općenitim informacijama poduzeća. Web stranica također pruža raznolike obrasce koje korisnici ispunjavaju za registraciju proizvoda i traženje informacija o proizvodu, napomene o ažuriranju proizvoda, mjesta distribucije proizvoda itd. Zabrinuti ste za ranjivost cgi-bin programa koji obrađuju ove obrasce; znate da se oni mogu promijeniti. Prema tome, želite biti sposobni provjeriti cjelovitost tih objekata i otkriti kad su na njima napravljene neovlaštene promjene. Radi toga ste odlučili digitalno potpisivati ove objekte da postignete sigurnosni cilj.

Istražili ste sposobnosti OS/400 potpisivanja objekta i naučili da ima nekoliko metoda koje možete upotrebljavati za potpisivanje objekata i provjeru potpisa objekata. Budući da ste odgovorni za upravljanje malim brojem iSeries poslužitelja i ne mislite da ćete trebati često potpisivati objekte, odlučili ste koristiti Upravitelja digitalnih certifikata DCM) za izvođenje ovih zadataka. Također ste odlučili kreirati Lokalnog izdavača certifikata (CA) i upotrebljavati privatni certifikat za potpisivanje objekata. Upotreba privatnog certifikata kojeg je izdao Lokalni CA za potpisivanje objekata ograničava trošak upotrebe sigurnosne tehnologije, jer ne morate kupiti certifikat od poznatog CA.

Ovaj primjer služi kao korisni uvod za korake potrebne u postavljanju i upotrebi potpisivanja objekta kad želite potpisati objekte na malom broju iSeries poslužitelja.

Prednosti scenarija

Ovaj scenarij ima sljedeće prednosti:
- Potpisivanje objekata pruža sredstvo provjere integriteta ranjivih objekata i lakše određivanje da li su objekti promijenjeni nakon što su bili potpisani. Ovim se mogu smanjiti neka rješavanja problema koje ćete raditi u budućnosti za praćenje aplikacija i drugih sistemskih problema.

- Upotrebom DCM-ovog grafičkog korisničkog sučelja za potpisivanje objekata i provjeru potpisa objekata dozvoljava se vama i drugima u poduzeću da lagano i brzo obavljate zadatke.
- Upotreba DCM-a za potpisivanje objekata i provjeru potpisa objekata smanjuje vrijeme koje morate utrošiti za učenje i upotrebu potpisivanja objekta kao dijela sigurnosne strategije.
- Upotreba certifikata kojeg je izdao Lokalni izdavač certifikata (CA) za potpisivanje objekata pojeftinjuje primjenu potpisivanja objekata.

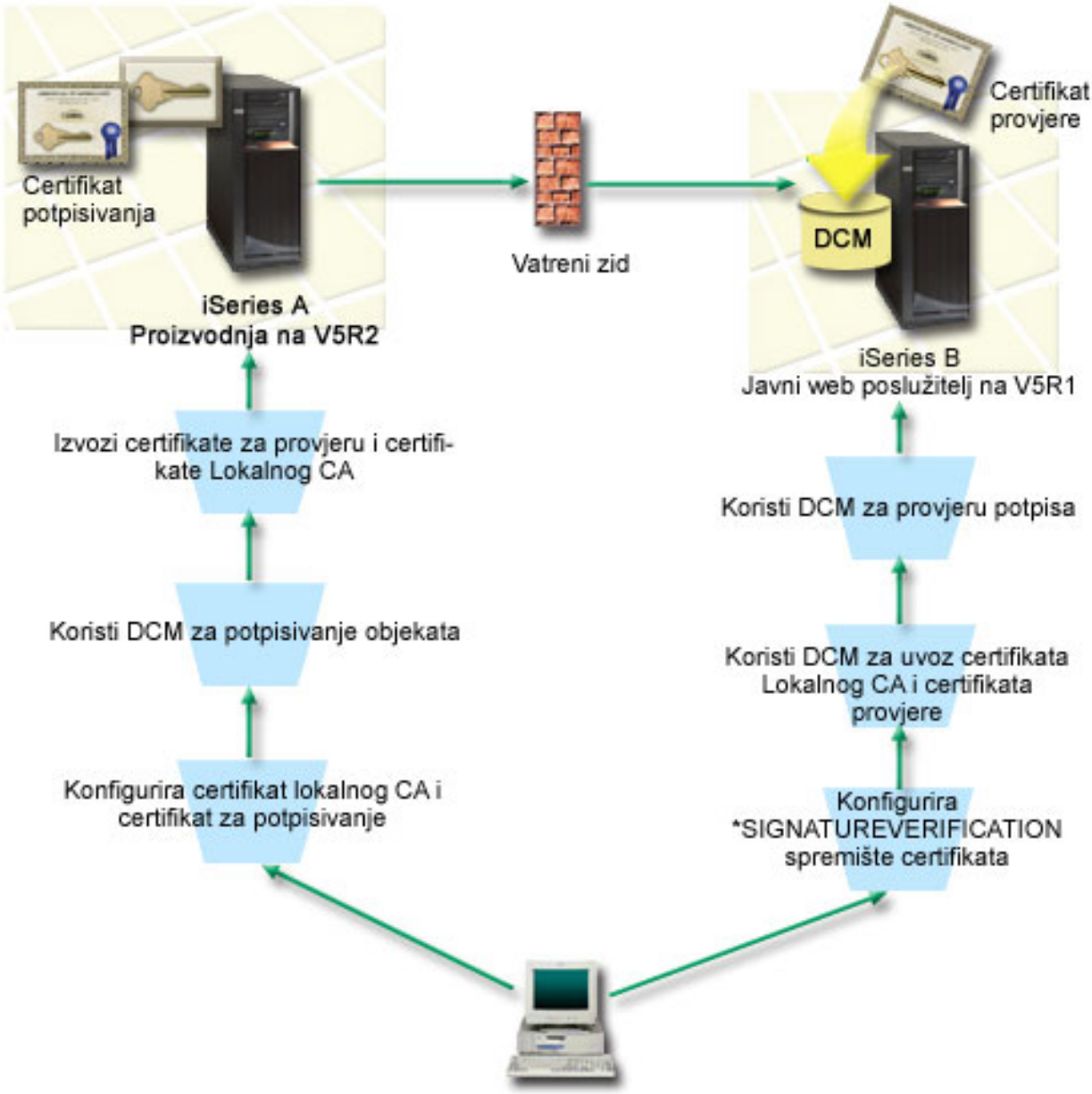
Ciljevi

U ovom scenariju želite digitalno potpisivati ranjive objekte, kao cgi-bin programe koji generiraju obrasce, na javnom iSeries poslužitelju poduzeća. Kao sistemski administrator pri MyCo, Inc, želite koristiti Upravitelja digitalnog certifikata (DCM) za potpisivanje ovih objekata i provjeru potpisa na objektima.

Ciljevi ovog scenarija su sljedeći:
- Aplikacije poduzeća i drugi ranjivi objekti na javnom Web poslužitelju iSeries B) moraju se potpisati sa certifikatom Lokalnog CA da se ograniče troškovi aplikacije potpisivanja.
- Sistemski administratori i drugi ovlašteni korisnici moraju moći lako provjeriti digitalne potpise na iSeries poslužiteljima da provjere izvor i vjerodostojnost objekata koje je potpisalo poduzeće. Da se to postigne svaki iSeries poslužitelj mora imati kopiju certifikata poduzeća za provjeru potpisa i certifikat Lokalnog izdavača certifika (CA) u *SIGNATUREVERIFICATION spremištu certifikata svakog poslužitelja.
- Provjerom potpisa na aplikacijama poduzeća i drugim objektima iSeries administratori i drugi mogu otkriti da li je sadržaj objekata promijenjen od kada su bili potpisani.
- Sistemski administrator mora upotrebljavati DCM za potpisivanje objekata; sistemski administrator i drugi moraju moći upotrebljavati DCM za provjeru potpisa objekata.

Detalji

Sljedeća slika ilustrira postupak potpisivanja objekta i provjere potpisa za primjenu ovog scenarija:



Slika ilustrira sljedeće točke relevantne za ovaj scenarij:

iSeries A

- iSeries A radi s OS/400 verzijom 5, izdanje 2 (V5R2).
- iSeries A je interni proizvodni poslužitelj poduzeća i razvojna platforma za javni iSeries Web poslužitelj (iSeries B).
- iSeries ima instaliran Dobavljač kriptografičkog pristupa 128-bitni za iSeries (5722–AC3).
- iSeries A ima instaliran i konfiguriran Upravitelj digitalnih certifikata (OS/400 opcija 34) i IBM HTTP poslužitelj (5722–DG1).
- iSeries A djeluje kao Lokalni izdavač certifikata (CA) i certifikat za potpisivanje objekta se nalazi na tom sistemu.
- iSeries A upotrebljava DCM za potpisivanje objekata i predstavlja primarni sistem potpisivanja objekata za javne aplikacije poduzeća i druge objekte.
- iSeries A je konfiguriran za omogućavanje provjere potpisa.

iSeries B

- iSeries B radi s OS/400 verzijom 5, izdanje 1 (V5R1).
- iSeries B je vanjski javni Web poslužitelj poduzeća izvan vatrenog zida poduzeća.
- iSeries B ima instaliranog Dobavljača kriptografičkog pristupa, 128-bitova, (5722–AC3).
- iSeries B ima instaliranog i konfiguriranog Upravitelja digitalnih certifikata (OS/400 opcija 34) i IBM HTTP poslužitelj (5722–DG1).
- iSeries B nema Lokalnog CA, niti iSeries B potpisuje objekte.
- iSeries B je konfiguriran da omogući provjeru potpisa upotrebom DCM-a za kreiranje *SIGNATUREVERIFICATION spremišta certifikata i importiranje potrebnih certifikata provjere i certifikata Lokalnog CA.
- DCM se koristi za provjeru potpisa objekata.

Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:
1. Svi iSeries poslužitelji zadovoljavaju zahtjeve za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).
2. Nitko nije ranije konfigurirao ili upotrebljavao DCM na nijednom iSeries poslužitelju.
3. Svi iSeries poslužitelji imaju instaliranu najveću razinu licencnog programa Dobavljača kriptografičkog pristupa 128-bitni (5722-AC3).
4. Default postavka za provjeru potpisa objekata za vrijeme vraćanja (QVFYOBJRST) sistemske vrijednosti na sve iSeries poslužitelje u scenariju je 3 i nije se mijenjala od ove postavke. Default postavka osigurava da poslužitelj može provjeriti potpise objekata čim se vrate potpisani objekti.
5. Sistemski administrator za iSeries A mora imati posebno ovlaštenje *ALLOBJ za potpisivanje objekata ili korisnički profil mora biti ovlašten za aplikaciju potpisivanja objekta.
6. Sistemski administrator ili bilo tko, tko kreira spremište certifikata u DCM-u, mora imati posebna ovlaštenja *SECADM i *ALLOBJ.
7. Sistemski administrator ili drugi na svim drugim iSeries poslužiteljima moraju imati posebno ovlaštenje *AUDIT za provjeru potpisa objekata.

Koraci zadatka konfiguracije

Postoje dva skupa zadataka koje morate dovršiti za primjenu ovog scenarija: Jedan skup zadataka omogućuje konfiguriranje iSeries A, kao Lokalnog izdavača certifikata (CA) i za potpisivanje i provjeru potpisa objekata. Drugi skup zadataka omogućuje konfiguriranje iSeries B za provjeru potpisa objekata koje kreira iSeries A.

iSeries A koraci zadatka

Morate dovršiti svaki od ovih zadataka na iSeries A da kreirate privatni Lokalni CA i da potpisujete objekte i provjeravate potpise objekata kao što opisuje ovaj scenarij:
1. Završite sve korake preduvjeta da instalirate i konfigurirate sve potrebne iSeries proizvode
2. Upotreba DCM-a za kreiranje Lokalnog izdavača certifikata (CA) za izdavanje certifikata za potpisivanje objekata.
3. Upotreba DCM-a za kreiranje definicije aplikacije
4. Upotreba DCM-a za dodjelu certifikata definiciji aplikacije za potpisivanje objekta
5. Upotreba DCM-a za potpisivanje cgi-bin programskih objekata
6. Upotreba DCM-a za eksport certifikata koje ostali sistemi moraju koristiti za provjeru potpisa objekata
   Morate eksportirati kopiju certifikata Lokalnog CA i kopiju certifikata za potpisivanje objekta kao certifikat provjere potpisa u datoteku.
7. Prijenos datoteka certifikata na javni iSeries poslužitelj poduzeća (iSeries B) tako da vi i ostali možete provjeriti potpise koje kreira iSeries A

iSeries B koraci zadataka

Ako namjeravate obnoviti potpisane objekte koje prenesete na javne Web poslužitelje u ovom scenariju (iSeries B), morate završiti zadatke konfiguracije provjere potpisa na iSeries B da bi mogli prenijeti potpisane objekte. Konfiguracija provjere potpisa mora biti dovršena prije nego što možete uspješno provjeriti potpise kad vraćate potpisane objekte na javnom Web poslužitelju.

Na iSeries B, morate dovršiti ove zadatke da provjerite potpise na objektima kao što opisuje scenarij:

8. Upotreba Upravitelja digitalnih certifikata (DCM) za kreiranje *SIGNATUREVERIFICATION spremišta certifikata
9. Upotreba DCM-a za import certifikata Lokalnog CA i certifikata provjere potpisa
10. Upotreba DCM-a za provjeru potpisa na prenesenim objektima

Detalji scenarija: Upotreba DCM-a za potpisivanje objekata i provjeru potpisa

Dovršite sljedeće korake zadataka da konfigurirate i upotrebljavate Upravitelja digitalnih certifikata za potpisivanje objekata kao što opisuje ovaj scenarij.

Korak 1: Izvođenje svih koraka preduvjeta

Morate dovršiti sve zadatke preduvjeta da instalirate i konfigurirate sve potrebne iSeries proizvode prije izvođenja određenih zadataka konfiguracije za primjenu ovog scenarija.

Korak 2: Kreiranje Lokalnog izdavača certifikata za izdavanje privatnih certifikata za potpisivanje objekata

Kad upotrebljavate Upravitelja digitalnih certifikata (DCM) za kreiranje Lokalnog izdavača certifikata (CA), taj postupak zahtijeva dovršavanje niza obrazaca. Ti obrasci vas vode kroz postupak kreiranja CA i dovršavanje drugih zadataka potrebnih za početak upotrebe digitalnih certifikata za Sloj sigurnih utičnica (SSL), potpisivanje objekata i provjeru potpisa. Iako u ovom scenariju ne trebate konfigurirati certifikate za SSL, morate dovršiti sve obrasce u zadatku da konfigurirate sistem za potpisivanje objekata.

Da koristite DCM za kreiranje i upravljanje Lokalnim CA, izvedite ove korake:

1. Pokrenite DCM.
2. U navigacijskom okviru DCM-a izaberite **Kreiranje Izdavača certifikata (CA)** za prikaz slijeda obrazaca.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite upitnik (**?**) na vrhu stranice da pristupite online pomoći.
3. Dovršite sve obrasce za ovaj vođeni zadatak. Kad obavljate ovaj zadatak morate napraviti sljedeće:
   a. Osigurati identifikacijske informacije za Lokalnog CA.
   b. Instalirati certifikat Lokalnog CA u pretražitelj tako da softver može prepoznati Lokalnog CA i provjeriti valjanost certifikata koje izdaje Lokalni CA.
   c. Navesti podatke politike za Lokalnog CA.
   d. Upotrijebiti novog Lokalnog CA za izdavanje certifikata poslužitelja ili klijenta kojeg aplikacije mogu upotrijebiti za SSL veze.

      Bilješka: Iako ovaj scenarij ne koristi ovaj certifikat, morate ga kreirati prije nego što možete upotrebljavati Lokalni CA za izdavanje potrebnog certifikata za potpisivanje objekata. Ako opozovete zadatak bez kreiranja certifikata, morate kreirati certifikat za potpisivanje objekata i *OBJECTSIGNING spremište certifikata u kojoj je on odvojeno pohranjen.
   e. Izabrati aplikacije koje mogu upotrebljavati certifikat poslužitelja ili klijenta za SSL veze.

      Bilješka: Za svrhu ovog scenarija nemojte izabrati nikakvu aplikaciju i kliknite **Nastavak** da se prikaže sljedeći obrazac.
   f. Upotrijebiti novi Lokalni CA za izdavanje certifikata za potpisivanje objekata kojeg aplikacije mogu upotrijebiti za digitalno potpisivanje objekata. Ovaj podzadatak kreira *OBJECTSIGNING spremište certifikata. To je spremište certifikata koje upotrebljavate za upravljanje certifikatima za potpisivanje objekata.
   g. Izabrati aplikacije kojima će vaš lokalni CA vjerovati.

Bilješka: Za svrhe ovog scenarija nemojte izabrati nikakvu aplikaciju i kliknite **Nastavak** da se završi ovaj zadatak.

Sada kada ste kreirali Lokalni CA i certifikat za potpisivanje objekata, morate definirati aplikaciju za potpisivanje objekata da upotrijebite certifikat prije nego što možete potpisivati objekte.

Korak 3: Kreiranje definicije aplikacije za potpisivanje objekata

Nakon kreiranja certifikata za potpisivanje objekata morate upotrijebiti Upravitelja digitalnih certifikata (DCM) da definirate aplikaciju za potpisivanje objekata koju možete upotrijebiti za potpisivanje objekata. Definicija aplikacije ne treba se odnositi na stvarnu aplikaciju. Definicija aplikacije koju kreirate može opisati tip ili grupu objekata koje ste htjeli potpisati. Definiciju trebate da možete imati ID aplikacije za pridruživanje sa certifikatom i da omogućite postupak potpisivanja.

Da upotrijebite DCM za kreiranje definicije aplikacije za potpisivanje objekata, slijedite ove korake:
1. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** da se otvori spremište certifikata.
2. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
3. U navigacijskom okviru izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
4. Izaberite **Dodavanje aplikacije** iz popisa zadataka da se prikaže obrazac za definiranje aplikacije.
5. Popunite obrazac i kliknite **Dodaj**.

Sada morate dodijeliti certifikat za potpisivanje objekata aplikaciji koju ste kreirali.

Korak 4: Dodjela certifikata definiciji aplikacije za potpisivanje objekata.

Da dodijelite certifikat aplikaciji za potpisivanje objekata, slijedite ove korake:
1. U DCM navigacijskom okviru izaberite **Upravljanje certifikatima** da se prikaže popis zadataka.
2. Iz popisa zadataka izaberite **Dodjela certifikata** da prikažete listu certifikata za trenutno spremište certifikata.
3. Izaberite certifikat s popisa i kliknite **Dodjela aplikacijama** da prikažete listu definicija aplikacija za trenutno spremište certifikata.
4. Izaberite jednu ili više aplikacija s popisa i kliknite **Nastavak**. Prikazuje se stranica poruke ili za potvrdu dodjele certifikata ili za prikaz informacija o greški ako se desio problem.

Kad dovršite ovaj zadatak, spremni ste upotrebljavati DCM za potpisivanje objekata programa koje će javni Web poslužitelj poduzeća (iSeries B) upotrebljavati.

Korak 5: Potpisivanje objekata programa

Da upotrijebite DCM za potpisivanje objekata programa za upotrebu na javnom Web poslužitelju poduzeća (iSeries B), slijedite ove korake:
1. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** da se otvori spremište certifikata.
2. Unesite lozinku za *OBJECTSIGNING spremište certifikata i kliknite **Nastavak**.
3. Nakon osvježenja navigacijskog okvira, izaberite **Upravljanje potpisivim objektima** za prikaz popisa zadataka.
4. Iz popisa zadataka izaberite **Potpisivanje objekta** za prikaz popisa definicija aplikacija koje možete koristiti za potpisivanje objekata.
5. Izaberite aplikaciju koju ste definirali u prethodnom koraku i kliknite **Potpisivanje objekta**. Prikazat će se obrazac koji vam omogućuje da navedete smještaj objekata koje želite potpisati.
6. U dobiveno polje unesite potpuno kvalificirano ime i stazu datoteke objekta ili direktorija objekata koje želite potpisati i kliknite **Nastavak**. Ili unesite lokaciju direktorija i kliknite **Pregled** da vidite sadržaje direktorija i da izaberete objekte za potpisivanje.

   Bilješka: Morate započeti ime objekta s vodećom kosom crtom ili možete naići na grešku. Možete također koristiti određene generičke znakove za opis direktorija kojeg želite potpisati. Ti generički znakovi su zvjezdica

(*****), koja navodi *bilo koji broj znakova* i upitnik (**?**), koji navodi *bilo koji pojedinačni znak*. Na primjer, da potpišete sve objekte u specifičnom direktoriju, možete unijeti /mydirectory/*, a da potpišete sve programe u određenoj knjižnici, možete unijeti /QSYS.LIB/QGPL.LIB/*.PGM. Te generičke znakove možete upotrebljavati samo u zadnjem dijelu imena staze; na primjer,/mydirectory*/filename ima za posljedicu poruku o greški. Ako želite koristiti funkciju **Pregled** da vidite popis knjižnica ili sadržaj direktorija, morate unijeti zamjenski znak kao dio imena staze prije nego kliknete **Pregled**.

7. Izaberite opcije obrade koje želite upotrebljavati za potpisivanje izabranog objekta ili objekata i kliknite **Nastavak**.

   Bilješka: Ako odlučite čekati rezultate posla, prikazati će se datoteka rezultata izravno u vašem pretražitelju. Rezultati trenutnog posla se pridodaju kraju datoteke rezultata. Prema tome, datoteka može sadržavati rezultate od svakog prethodnog posla osim onih od trenutnog posla. Možete upotrebljavati polje podataka u datoteci da odredite koje se linije u datoteci primjenjuju u trenutnom poslu. Polje podataka je u formatu YYYYMMDD. Prvo polje u datoteci može biti ili ID poruke (ako se desila greška za vrijeme obrade objekta) ili polje datuma (pokazujući datum kad se posao obrađivao).
8. Specifirajte potpuno kvalificirano ime i stazu datoteke za korištenje u pohranjivanju rezultata posla za potpisivanje objekta i kliknite **Nastavak**. Ili unesite lokaciju direktorija i kliknite **Pregled** da pogledate sadržaje direktorija te da izaberete datoteku za pohranjivanje rezultata posla. Prikazuje se poruka koja pokazuje da je posao poslan na izvođenje za potpis objekata. Da vidite rezultate posla, pogledajte **QOBJSGNBAT** u dnevniku posla.

Da se osigurate da vi ili drugi mogu provjeravati potpise, morate eksportirati potrebne certifikate u datoteku i prenijeti datoteku certifikata na iSeries B. Morate također dovršiti sve zadatke za konfiguraciju provjere potpisa na iSeries B prije prijenosa potpisanih objekata programa na iSeries B. Konfiguracija provjere potpisa mora biti dovršena prije nego što možete uspješno provjeriti potpise kad vraćate potpisane objekte na iSeries B.

Korak 6: Eksport certifikata za omogućavanje provjere potpisa na iSeries B

Potpisivanje objekata za zaštitu cjelovitosti sadržaja zahtijeva da vi i drugi imate način za provjeru vjerodostojnosti potpisa. Da provjerite potpise objekata na istom sistemu koji potpisuje objekte iSeries A), morate upotrijebiti DCM za kreiranje *SIGNATUREVERIFICATION spremišta certifikata. To spremište certifikata mora sadržavati kopiju certifikata za potpisivanje objekata i kopiju certifikata CA za CA koji izdao certifikat za potpisivanje.

Da omogućite drugima provjeru potpisa, morate ih opskrbiti s kopijom certifikata koji je potpisao objekt. Kad upotrebljavate Lokalnog izdavača certifikata (CA) za izdavanje certifikata, morate i njega opskrbiti s kopijom certifikata Lokalnog CA.

Da upotrijebite DCM za provjeru potpisa na istom sistemu koji potpisuje objekte (iSeries A u ovom scenariju) slijedite ove korake:

1. U navigacijskom okviru kliknite **Kreiranje novog spremišta certifikata** i izaberite***SIGNATUREVERIFICATION** kao spremište certifikata za kreiranje.
2. Izaberite **Da** da kopirate postojeće certifikate za potpisivanje objekata u novo spremište certifikata kao certifikate za provjeru potpisa.
3. Odredite lozinku za novo spremište certifikata i kliknite **Nastavak** za kreiranje spremišta certifikata. Sada možete upotrebljavati DCM za provjeru potpisa objekata na istom sistemu kojeg upotrebaljavate za potpisivanje objekata.

Da upotrijebite DCM za eksport kopije certifikata Lokalnog CA i kopije certifikata za potpisivanje objekata kao certifikata za provjeru potpisa, tako da možete provjeravati potpise objekata na drugim sistemima (iSeries B), slijedite ove korake:

1. U navigacijskom okviru izaberite **Upravljanje certifikatima** i zatim izaberite zadatak **Eksport certifikata**.
2. Izaberite **Izdavač certifikata (CA)** i kliknite **Nastavak** da se prikaže popis CA certifikata koje možete eksportirati.
3. Izaberite certifikat Lokalnog CA koji ste kreirali ranije s popisa i kliknite **Eksport**.
4. Navedite **Datoteku** kao odredište eksportiranja i kliknite **Nastavak**.
5. Navedite potpuno kvalificirano ime staze i datoteke za eksportirani certifikat Lokalnog CA i kliknite **Nastavak** da eksportirate certifikat.
6. Kliknite **OK** da izađete iz stranice za potvrdu Eksporta. Sada možete eksportirati kopiju certifikata za potpisivanje objekta.

7. Ponovno izaberite zadatak **Eksport certifikata**.
8. Izaberite **Potpisivanje objekata** da se prikaže popis certifikata za potpisivanje objekata koje možete eksportirati.
9. Izaberite odgovarajući certifikat za potpisivanje objekta s popisa i kliknite **Eksport**.
10. Izaberite **Datoteku, kao certifikat provjere potpisa** za destinaciju i kliknite **Nastavak**.
11. Navedite potpuno kvalificirano ime staze i datoteke za eksportirani certifikat provjere potpisa i kliknite **Nastavak** da eksportirate certifikat.

Sada možete prenijeti ove datoteke na iSeries krajnje sisteme na kojima namjeravate provjeravati potpise koje ste kreirali sa certifikatom.

Korak 7: Prijenos datoteka certifikata na javni poslužitelj poduzeća iSeries B

Morate prenijeti datoteke certifikata koje ste kreirali na iSeries A na iSeries B, javni Web poslužitelj poduzeća u ovom scenariju prije nego što ih možete konfigurirati za provjeru objekata koje potpisujete. Možete upotrijebiti nekoliko različitih metoda za prijenos datoteka certifikata. Na primjer, možete koristiti FTP ili distribuciju paketa Središnjeg Upravljanja za prijenos podataka.

Korak 8: Zadaci provjere potpisa: Kreiranje *SIGNATUREVERIFICATION spremišta certifikata

Da provjerite potpise objekata na iSeries B (javni Web poslužitelj poduzeća) iSeries B mora imati kopiju odgovarajućeg certifikata za provjeru potpisa u *SIGNATUREVERIFICATION spremištu certifikata. Budući da ste upotrebljavali certifikat, kojeg je izdao Lokalni CA, za potpisivanje objekata, to spremište certifikata mora također sadržavati kopiju certifikata Lokalnog CA.

Da kreirate *SIGNATUREVERIFICATION spremište certifikata, slijedite ove korake:
1. Pokrenite DCM.
2. U navigacijskom okviru Upravitelja digitalnih certifikata (DCM) izaberite **Kreiranje novog spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za kreiranje.

   Bilješka: Ako imate pitanja o tome kako popuniti specifičan obrazac dok koristite DCM, izaberite upitnik (**?**) na vrhu stranice da pristupite online pomoći.
3. Odredite lozinku za novo spremište certifikata i kliknite **Nastavak** za kreiranje spremišta certifikata. Sada možete importirati certifikate u spremište i upotrebljavati ih za provjeru potpisa objekata.

Korak 9: Zadaci provjere potpisa: Import certifikata

Da se provjeri potpis na objektu, *SIGNATUREVERIFICATION spremište certifikata mora sadržavati kopiju certifikata za provjeru potpisa. Ako je certifikat za potpisivanje privatni, ovo spremište certifikata mora također imati kopiju certifikata Lokalnog izdavača certifikata (CA) koji je izdao certifikat za potpisivanje. U ovom scenariju, oba certifikata su se eksportirala u datoteku i ta datoteka je prenešena na svaki krajnji iSeries sistem.

Da importirate ove certifikate u *SIGNATUREVERIFICATION spremište, slijedite ove korake:
1. U navigacijskom okviru DCM-a kliknite **Izbor spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za otvaranje.
2. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
3. Nakon osvježenja navigacijskog okvira izaberite **Upravljanje certifikatima** da se prikaže popis zadataka.
4. Iz popisa zadataka izaberite **Import certifikata**.
5. Izaberite **Izdavač certifikata (CA)** kao tip certifikata i kliknite **Nastavak**.

   Bilješka: Morate importirati certifikat Lokalnog CA prije importiranja privatnog certifikata za provjeru potpisa; inače postupak importiranja za certifikat provjere potpisa neće uspjeti.
6. Navedite potpuno kvalificirano ime staze i datoteke za datoteku certifikata CA i kliknite **Nastavak**. Prikazuje se poruka koja ili potvrđuje da je postupak importiranja uspio ili informira o greški ako postupak nije uspio.
7. Ponovno izaberite zadatak **Import certifikata**.
8. Izaberite **Provjera potpisa** kao tip certifikata za import i kliknite **Nastavak**.

9. Navedite potpuno kvalificirano ime staze i datoteke za certifikat provjere potpisa i kliknite **Nastavak**. Prikazuje se poruka koja ili potvrđuje da je postupak importiranja uspio ili informira o greški ako postupak nije uspio.

Sada možete upotrijebiti DCM na iSeries B za provjeru potpisa na objektima koje ste kreirali s odgovarajućim certifikatom za potpisivanje na iSeries A.

Korak 10: Zadaci provjere potpisa: provjera potpisa na objektima programa

Da upotrijebite DCM za provjeru potpisa na prenesenim objektima programa, slijedite ove korake:
1. U navigacijskom okviru kliknite**Izbor spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** za otvaranje.
2. Unesite lozinku za *SIGNATUREVERIFICATION spremište certifikata i kliknite **Nastavak**.
3. Nakon osvježenja navigacijskog okvira, izaberite **Upravljanje potpisivim objektima** za prikaz popisa zadataka.
4. Iz popisa zadataka izaberite **Provjera potpisa objekta** za specifikaciju lokacija objekata za koje želite provjeru potpisa.
5. U dobiveno polje unesite potpuno kvalificirano ime i stazu datoteke objekta ili direktorija objekata za koje želite provjeriti potpise i kliknite**Nastavak**. Ili unesite lokaciju direktorija i kliknite **Pregled** da vidite sadržaje direktorija i da izaberete objekte za provjeru potpisa.

   Bilješka: Možete također koristiti određene generičke znakove za opis direktorija kojeg želite provjeriti. Ti generički znakovi su zvjezdica (*****), koja navodi *bilo koji broj znakova* i upitnik (**?**)koji specificira *bilo koji pojedinačni znak*. Na primjer, da potpišete sve objekte u specifičnom direktoriju, možete unijeti /mydirectory/*, a da potpišete sve programe u određenoj knjižnici, možete unijeti /QSYS.LIB/QGPL.LIB/*.PGM. Te generičke znakove možete upotrebljavati samo u zadnjem dijelu imena staze; na primjer,/mydirectory*/filename ima za posljedicu poruku o greški. Ako želite koristiti funkciju Pregled da vidite popis knjižnica ili sadržaj direktorija, morate unijeti zamjenski znak kao dio imena staze prije nego kliknete **Pregled**.
6. Izaberite opcije obrade koje želite upotrebljavati za provjeru potpisa na izabranom objektu ili objektima i kliknite **Nastavak**.

   Bilješka: Ako odlučite čekati rezultate posla, prikazati će se datoteka rezultata izravno u vašem pretražitelju. Rezultati trenutnog posla se pridodaju kraju datoteke rezultata. Radi toga datoteka može sadržavati rezultate bilo kojeg ranijeg posla uz one od trenutnog posla. Možete upotrebljavati polje podataka u datoteci da odredite koje se linije u datoteci primjenjuju u trenutnom poslu. Polje podataka je u formatu YYYYMMDD. Prvo polje u datoteci može biti bilo ID poruke (ako se desila greška za vrijeme obrade objekta) ili polje datuma (pokazujući datum kad se posao obrađivao).
7. Specifirajte potpuno kvalificirano ime i stazu datoteke za korištenje u pohranjivanju rezultata posla za provjeru potpisa objekta i kliknite**Nastavak** . Ili unesite lokaciju direktorija i kliknite **Pregled** da pogledate sadržaje direktorija te da izaberete datoteku za pohranjivanje rezultata posla. Prikazuje se poruka koja pokazuje da je posao poslan na izvođenje za provjeru potpisa objekata. Da vidite rezultate posla, pogledajte posao **QOBJSGNBAT** u dnevniku posla.

Scenarij: Upotreba API-ja za potpisivanje objekata i provjeru potpisa objekata

Situacija

Vaše poduzeće (MyCo, Inc.) je iSeries poslovni partner koji razvija aplikacije za korisnike. Kao razvijač softvera za poduzeće, odgovorni ste za pakiranje ovih aplikacija za distribuciju korisnicima. Trenutno upotrebljavate programe za pakiranje aplikacije. Korisnici mogu naručiti kompaktni disk (CD-ROM) ili mogu posjetiti vašu Web stranicu i učitati aplikaciju.

Vi ste u toku trenutnih industrijskih novosti, naročito novosti o sigurnosti. Radi toga znate da se korisnici opravdano brinu za izvor i sadržaj programa koje primaju ili učitavaju. Ponekad korisnici misle da primaju ili učitavaju proizvod od pouzdanog izvora, ali se ispostavi da to nije bio pravi izvor proizvoda. Ponekad se ta zbrka dešava kod korisnika koji instaliraju drugačiji proizvod od onog koji su očekivali. Ponekad se ispostavi da je instalirani proizvod zlonamjerni program ili je promijenjen i oštećuje sistem.

Iako ovi tipovi problema nisu uobičajeni za iSeries korisnike, želite uvjeriti korisnike da su aplikacije dobivene od vas stvarno od vašeg poduzeća. Također želite pružiti korisnicima način provjere cjelovitosti ovih aplikacija tako da mogu odrediti da li su promijenjene prije nego što ih instaliraju.

Na osnovi vašeg istraživanja odlučili ste da možete upotrebljavati svojstva OS/400 potpisivanja objekata da postignete svoje ciljeve sigurnosti. Digitalno potpisivanje aplikacija dopušta korisnicima da provjere da je vaše poduzeće legitimni izvor aplikacije koju primaju ili učitavaju. Budući da trenutno programatski pakirate aplikacije, odlučili ste da možete upotrebljavati API-je za lako dodavanje potpisivanja objekta vašoj postojećoj obradi pakiranja. Također odlučujete upotrijebiti javni certifikat za potpisivanje objekata tako da možete napraviti obradu provjere potpisa transparentnom za vaše korisnike kad instaliraju vaš proizvod.

Kao dio paketa aplikacije uključujete kopiju digitalnog certifikata kojeg ste upotrijebili kod potpisivanja objekta. Kad korisnik dobije paket aplikacije, može upotrebljavati javni ključ certifikata za provjeru potpisa na aplikaciji. Ova obrada omogućava korisniku identifikaciju i provjeru izvora aplikacije, kao i osiguranje da sadržaji objekata aplikacije nisu promijenjeni od kada su potpisani.

Ovaj primjer služi kao korisni uvod za korake potrebne u programatskom potpisivanju objekata za aplikacije koje razvijate i pakirate da ih drugi upotrebljavaju.

Prednosti scenarija

Ovaj scenarij ima sljedeće prednosti:
- Upotreba API-ja za pakiranje i programatsko potpisivanja objekata skraćuje vrijeme koje morate utrošiti za primjenu ove sigurnosti.
- Upotreba API-ja za potpisivanje objekata kad ih pakirate smanjuje broj koraka koje morate obaviti za potpisivanje objekata, jer je postupak potpisivanja dio postupka pakiranja.
- Potpisivanje paketa objekata omogućuje da lakše odredite da li su objekti promijenjeni nakon što su bili potpisani. Ovim se mogu smanjiti neka rješavanja problema koja ćete raditi u budućnosti za praćenje problema aplikacija za korisnike.
- Upotreba certifikata od javnog poznatog Izdavača certifikata (CA) za potpisivanje objekta dopušta upotrebu API-ja za dodavanje provjeritelja kao dijela izlaznog programa u programu za instalaciju proizvoda. Upotreba ovog API-ja omogućuje dodavanje javnog certifikata kojeg ste upotrebljavali za automatsko potpisivanje aplikacije na korisnički sistem. Time se osigurava da je provjera potpisa transparentna za vašeg korisnika.

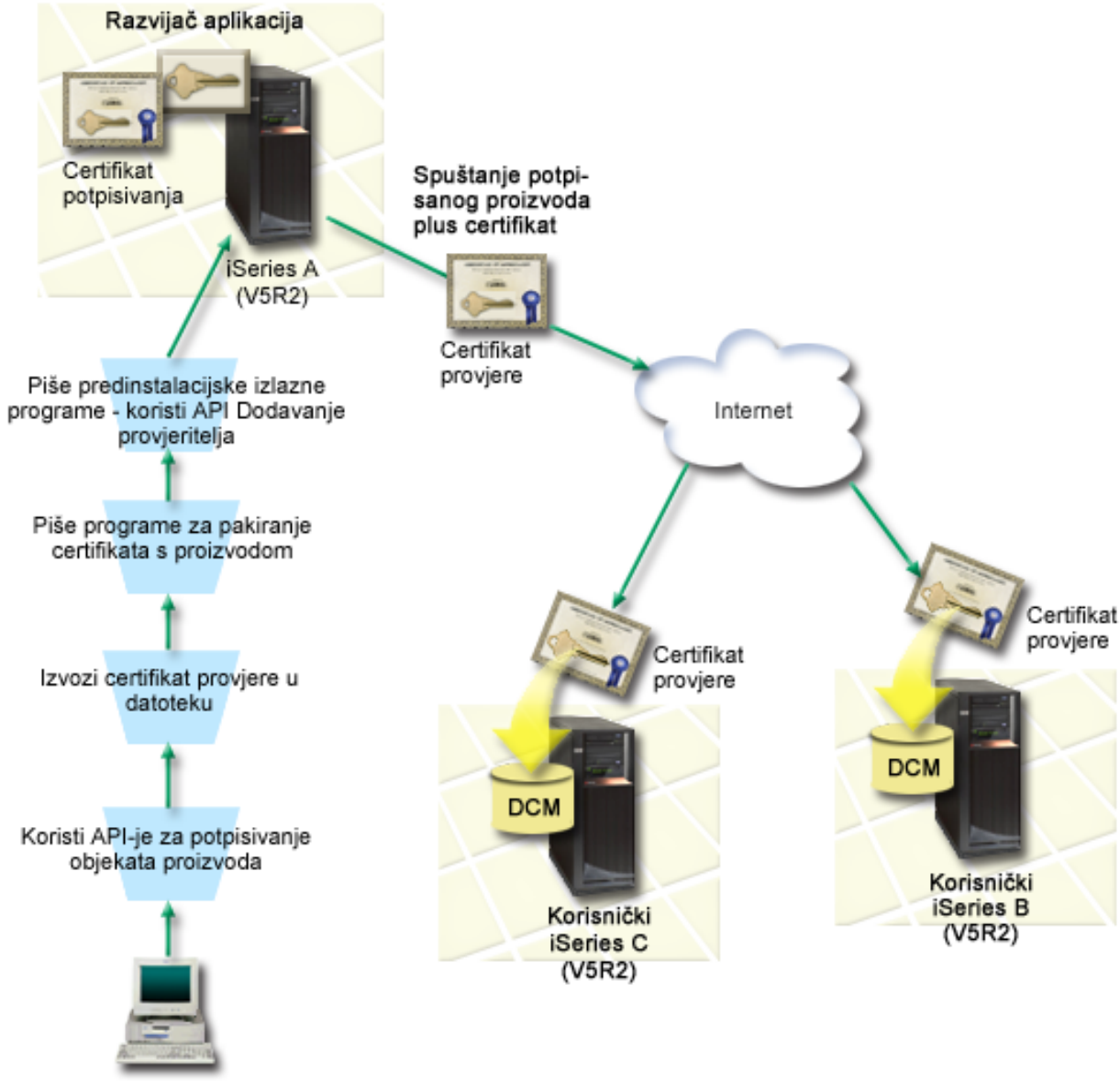
Ciljevi

U ovom scenariju, MyCo, Inc. želi programatski potpisivati aplikacije koje pakira i distribuira svojim korisnicima. Kao razvijač proizvodnje aplikacija pri MyCo, Inc, trenutno aplikacije vašeg poduzeća pakirate programski za distribuciju korisnicima. Radi toga želite upotrebljavati iSeries API-je za potpisivanje aplikacija i želite da korisnikov iSeries programatski provjeri potpis za vrijeme instalacije proizvoda.

Ciljevi ovog scenarija su sljedeći:
- Razvijač proizvoda poduzeća mora biti sposoban potpisivati objekte upotrebljavajući API za Potpisivanje objekata kao dio postojećeg postupka za programatsko pakiranje aplikacija.
- Aplikacije poduzeća moraju se potpisivati s javnim certifikatom da se osigura transparentnost postupka provjere potpisa za korisnika za vrijeme postupka instalacije proizvoda aplikacije.
- Poduzeće mora biti u mogućnosti upotrebljavati iSeries API-je za programatsko dodavanje potrebnih certifikata provjere potpisa u korisničko *SIGNATUREVERIFICATION spremište certifikata iSeries poslužitelja. Poduzeće mora biti sposobno programatski kreirati ovo spremište certifikata na korisnikovom iSeries poslužitelju kao dio postupka instalacije proizvoda ako već ne postoji.
- Korisnici moraju biti sposobni lako provjeriti digitalne potpise na aplikaciji poduzeća nakon instalacije proizvoda. Korisnici moraju biti sposobni provjeriti potpis tako da mogu utvrditi izvor i vjerodostojnost potpisane aplikacije kao i odrediti da li je napravljena promjena na aplikaciji od kad je potpisana.

Detalji

Sljedeća slika ilustrira postupak potpisivanja objekta i provjere potpisa za primjenu ovog scenarija:



Slika ilustrira sljedeće točke relevantne za ovaj scenarij:

Centralni sistem (iSeries A)

- iSeries A radi s OS/400 verzijom 5, izdanje 2 (V5R2).
- iSeries A pokreće program za pakiranje proizvoda razvijača aplikacija.
- iSeries ima instaliran Dobavljač kriptografičkog pristupa 128-bitni za iSeries (5722–AC3).
- iSeries A ima instaliran i konfiguriran Upravitelj digitalnih certifikata (OS/400 opcija 34) i IBM HTTP poslužitelj (5722–DG1).
- iSeries A je primarni sistem za potpisivanje objekata za proizvode aplikacije poduzeća. Potpisivanje objekta proizvoda za korisničku distribuciju postiže se na iSeries A izvođenjem ovih zadataka:
  1. Upotreba API-ja za potpisivanje proizvoda aplikacije poduzeća.
  2. Upotreba DCM-a za eksportiranje certifikata provjere potpisa u datoteku tako da korisnici mogu provjeravati potpisane objekte.
  3. Pisanje programa za dodavanje certifikata provjere potpisanom aplikacijskom proizvodu.

4. Pisanje predinstalacijskog izlaznog programa za proizvod koji upotrebljava API za Dodavanje provjeritelja. Ovaj API omogućuje postupku instalacije proizvoda da programski doda certifikat provjere u *SIGNATUREVERIFICATION spremište certifikata na korisnikovom iSeries poslužitelju (iSeries B i C).

Korisnički iSeries poslužitelji B i C

- iSeries B radi s OS/400 verzijom 5, izdanje 2 (V5R2).
- iSeries C radi s OS/400 verzijom 5, izdanje 2 (V5R2).
- iSeries B i C imaju instalirane i konfigurirane Upravitelja digitalnih certifikata (opcija 34) i IBM HTTP poslužitelj (5722–DG1).
- iSeries B i C kupuje i spušta aplikaciju s Web stranice poduzeća za razvoj aplikacija (koje je vlasnik iSeries A).
- iSeries B i C dobivaju kopiju certifikata za provjeru potpisa MyCo kada postupak instalacije aplikacija MyCo kreira *SIGNATUREVERIFICATION spremište certifikata na svakom od tih korisnikovih iSeries poslužitelja.

Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:
1. Svi iSeries poslužitelji zadovoljavaju zahtjeve za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).

   Bilješka: Zadovoljavanje preduvjeta za instaliranje i upotrebu DCM-a je neobavezni zahtjev za korisnike (iSeries B i C u ovom scenariju). Iako API za Dodavanje provjeritelja kreira *SIGNATUREVERIFICATION spremište certifikata kao dio postupka instalacije proizvoda, ako je potrebno, on je kreira s defaultnom lozinkom. Korisnici trebaju upotrebljavati DCM za promjenu defaultne lozinke da zaštite ovo spremište certifikata od neovlaštenog pristupa.
2. Nitko nije ranije konfigurirao ili upotrebljavao DCM na nijednom iSeries poslužitelju.
3. Svi iSeries poslužitelji imaju instaliranu najveću razinu licencnog programa Dobavljača kriptografičkog pristupa 128-bitni (5722-AC3).
4. Default postavka za provjeru potpisa objekata za vrijeme vraćanja (QVFYOBJRST) sistemske vrijednosti na sve iSeries poslužitelje u scenariju je 3 i nije se mijenjala od ove postavke. Default postavka osigurava da poslužitelj može provjeriti potpise objekata čim se vrate potpisani objekti.
5. Mrežni administrator za iSeries A mora imati posebno ovlaštenje *ALLOBJ za potpisivanje objekata ili korisnički profil mora biti ovlašten za aplikaciju potpisivanja objekata.
6. Sistemski administrator ili bilo tko (uključujući program), tko kreira spremište certifikata u DCM-u, mora imati posebna ovlaštenja *SECADM i *ALLOBJ.
7. Sistemski administrator ili drugi na svim drugim iSeries poslužiteljima moraju imati posebno ovlaštenje za korisnički profil *AUDIT za provjeru potpisa objekata.

Koraci zadatka konfiguracije

Morate dovršiti svaki od ovih zadataka na iSeries A da potpisujete objekte kao što opisuje ovaj scenarij:
1. Završite sve korake preduvjeta da instalirate i konfigurirate sve potrebne iSeries proizvode
2. Koristite DCM za kreiranje zahtjeva certifikata za dobivanje certifikata za potpisivanje objekata od poznatih javnih Izdavača certifikata (CA).
3. Koristite DCM za kreiranje definicije aplikacije za potpisivanje objekta
4. Koristite DCM za import certifikata za potpisivanje objekata i njihovu dodjelu vašoj definiciji aplikacije za potpisivanje objekta
5. Koristite DCM za eksport certifikata za potpis objekata kao certifikata za provjeru potpisa tako da ih vaši korisnici mogu koristiti za provjeru potpisa na objektima aplikacije
6. Ažurirajte svoj program za pakiranje aplikacije da koristi API Potpisivanje objekta za potpisivanje vaše aplikacije
7. Kreirajte izlazni program predinstalacije koji koristi API Dodavanje provjeritelja kao dio vašeg postupka pakiranja aplikacije
   Taj izlazni program omogućuje kreiranje *SIGNATUREVERIFICATION spremišta certifikata i dodavanje potrebnog certifikata za provjeru potpisa korisnikovom iSeries poslužitelju za vrijeme instaliranja proizvoda.
8. Neka korisnici koriste DCM za resetiranje default lozinke za *SIGNATUREVERIFICATION spremište certifikata na svojem iSeries poslužitelju

Detalji scenarija: Upotreba API-ja za potpisivanje objekata i provjeru potpisa objekata

Dovršite sljedeće korake zadatka da upotrijebite OS/400 API-je za potpisivanje objekata kako opisuje ovaj scenarij.

Korak 1: Izvođenje svih koraka preduvjeta

Morate dovršiti sve zadatke preduvjeta da instalirate i konfigurirate sve potrebne iSeries proizvode prije izvođenja određenih zadatka konfiguracije za primjenu ovog scenarija.

Korak 2: Upotreba DCM-a za dobivanje certifikata od javnih dobro poznatih CA

Ovaj scenarij pretpostavlja da niste ranije upotrebljavali Upravitelja digitalnih certifikata za kreiranje i upravljanje certifikatima. Radi toga, morate kreirati *OBJECTSIGNING spremište certifikata kao dio postupka za kreiranje certifikata za potpisivanje objekata. Ovo spremište certifikata, kad se kreira, daje zadatke koje trebate za kreiranje i upravljanje certifikatima za potpisivanje objekata. Da dobijete certifikat od javnog poznatog Izdavača certifikata (CA), upotrijebite DCM za kreiranje identifikacijskih informacija i para javno-privatnih ključeva za certifikat i pošaljite te informacije CA-u da dobijete certifikat.

Da kreirate informacije za zahtjev certifikata kojeg trebate dati javnom poznatom CA-u tako da možete dobiti certifikat za potpisivanje objekata, dovršite ove korake:

1. Pokrenite DCM.
2. U navigacijskom okviru DCM-a izaberite **Kreiranje novog spremišta certifikata** da dovršite vođeni zadatak i popunite seriju obrazaca. Ovi obrasci vas vode kroz postupak kreiranja spremišta certifikata i certifikata kojeg možete koristiti za potpisivanje objekata.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
3. Izaberite ***OBJECTSIGNING** kao spremište certifikata za kreiranje i kliknite **Nastavak**.
4. Izaberite **Da** da kreirate certifikat kao dio kreiranja *OBJECTSIGNING spremišta certifikata i kliknite **Nastavak**.
5. Izaberite **VeriSign ili drugog Internet Izdavača certifikata (CA)** kao potpisnika novog certifikata i kliknite **Nastavak** da se prikaže obrazac koji omogućuje pružanje identifikacijskih informacija za novi certifikat.
6. Dovršite obrazac i kliknite **Nastavak** da se prikaže stranica potvrde. Stranica potvrde prikazuje podatke zahtjeva certifikata koje morate dostaviti javnom Izdavaču certifikata (CA) koji će izdati vaš certifikat. Podaci za zahtjev za potpisivanje certifikata sastoje se od javnog ključa i drugih informacija koje ste naveli za novi certifikat.
7. Pažljivo kopirajte i preslikajte CSR podatke u obrazac molbe za certifikat ili u posebnu datoteku, što CA traži kod zahtjeva za certifikat. Morate upotrijebiti sve CSR podatke, uključujući početne i krajnje linije zahtjeva za novi certifikat. Kad napuštate ovu stranicu, podaci se gube i ne možete ih obnoviti.
8. Pošaljite obrazac molbe ili datoteku CA-u kojeg ste izabrali da izdaje i potpisuje vaše certifikate.
9. Čekajte da CA vrati potpisan, dovršen certifikat prije nego nastavite na sljedeći korak zadatka za ovaj scenarij.

Korak 3: Kreiranje definicije aplikacije za potpisivanje objekata

Sada kad ste poslali zahtjev za certifikat poznatom javnom CA-u, možete upotrijebiti DCM za definiranje aplikacije za potpisivanje objekata koju možete upotrijebiti za potpisivanje objekata. Definicija aplikacije ne treba se odnositi na stvarnu aplikaciju. Definicija aplikacije koju kreirate može opisati tip ili grupu objekata koje ste htjeli potpisati. Definiciju trebate da možete imati ID aplikacije za pridruživanje sa certifikatom i da omogućite postupak potpisivanja.

Da upotrijebite DCM za kreiranje definicije aplikacije za potpisivanje objekata, slijedite ove korake:

1. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** da se otvori spremište certifikata.
2. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
3. U navigacijskom okviru izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
4. Izaberite **Dodavanje aplikacije** iz popisa zadataka da se prikaže obrazac za definiranje aplikacije.
5. Dovršite obrazac i kliknite **Dodaj**.

Jednom kada nazad primite potpisani certifikat od CA, možete certifikat dodijeliti aplikaciji koju ste kreirali.

Korak 4: Import potpisanog javnog certifikata i dodjela aplikaciji za potpisivanje objekata

Da importirate certifikat i dodijelite ga aplikaciji da omogućite potpisivanje objekata, slijedite ove korake:
1. Pokrenite DCM.
2. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** da se otvori spremište certifikata.
3. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
4. Nakon osvježenja navigacijskog okvira izaberite **Upravljanje certifikatima** da se prikaže popis zadataka.
5. Iz popisa zadataka izaberite **Import certifikata** da započnete postupak importiranja potpisanog certifikata u spremište certifikata.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite upitnik (**?**) na vrhu stranice da pristupite online pomoći.
6. Izaberite **Dodjela certifikata** iz popisa zadataka **Upravljanje certifikatima** da se prikaže popis certifikata za trenutno spremište certifikata.
7. Izaberite certifikat s popisa i kliknite **Dodjela aplikacijama** da prikažete listu definicija aplikacija za trenutno spremište certifikata.
8. Izaberite vašu aplikaciju s popisa i kliknite **Nastavak**. Prikazuje se stranica ili s porukom potvrde za vaš izbor dodjela ili s porukom o grešci ako se dogodio problem.

Kad dovršite ovaj zadatak spremni ste potpisivati aplikacije i druge objekte upotrebljavajući OS/400 API-je. Međutim, da se osigurate da vi ili drugi mogu provjeravati potpise, morate eksportirati potrebne certifikate u datoteku i prenijeti ih svakom iSeries poslužitelju koji instalira potpisane aplikacije. Korisnici iSeries poslužitelja moraju zatim biti sposobni upotrebljavati certifikat za provjeru potpisa na vašim aplikacijama dok se instaliraju. Možete upotrijebiti API-je za Dodavanje provjeritelja kao dijela programa za instaliranje aplikacije da napravite potrebne konfiguracije provjere potpisa za korisnike. Na primjer, možda ćete kreirati predinstalacijski izlazni program koji poziva API Dodavanje provjeritelja da konfigurirate iSeries poslužitelj vašeg korisnika.

Korak 5: Eksport certifikata za omogućavanje provjere potpisa na ostalim iSeries poslužiteljima

Za potpisivanje objekata trebate vi i drugi imati način za provjeru vjerodostojnosti potpisa i upotrebljavati ga za određivanje da li su napravljene promjene na potpisanim objektima. Da provjerite potpise na objektima na istom sistemu koji potpisuje objekte, morate upotrijebiti DCM za kreiranje *SIGNATUREVERIFICATION spremišta certifikata. To spremište certifikata mora sadržavati kopiju certifikata za potpisivanje objekata i kopiju certifikata CA za CA koji izdao certifikat za potpisivanje.

Da omogućite drugima provjeru potpisa, morate ih opskrbiti s kopijom certifikata koji je potpisao objekt. Kad upotrebljavate Lokalnog izdavača certifikata (CA) za izdavanje certifikata, morate i njega opskrbiti s kopijom certifikata Lokalnog CA.

Da upotrijebite DCM za provjeru potpisa na istom sistemu koji potpisuje objekte (iSeries A u ovom scenariju) slijedite ove korake:
1. U navigacijskom okviru kliknite **Kreiranje novog spremišta certifikata** i izaberite***SIGNATUREVERIFICATION** kao spremište certifikata za kreiranje.
2. Izaberite **Da** da kopirate postojeće certifikate za potpisivanje objekata u novo spremište certifikata kao certifikate za provjeru potpisa.
3. Odredite lozinku za novo spremište certifikata i kliknite **Nastavak** za kreiranje spremišta certifikata. Sada možete upotrebljavati DCM za provjeru potpisa objekata na istom sistemu kojeg upotrebaljavate za potpisivanje objekata.

Da upotrijebite DCM za eksportiranje kopije certifikata za potpisivanje objekata kao certifikata provjere potpisa, tako da drugi mogu provjeravati vaše potpise objekata, slijedite ove korake:
1. U navigacijskom okviru izaberite **Upravljanje certifikatima** i zatim izaberite zadatak **Eksport certifikata**.
2. Izaberite **Potpisivanje objekata** da se prikaže popis certifikata za potpisivanje objekata koje možete eksportirati.

3. Izaberite odgovarajući certifikat za potpisivanje objekta s popisa i kliknite **Eksport**.
4. Izaberite **Datoteku, kao certifikat provjere potpisa** za destinaciju i kliknite **Nastavak**.
5. Navedite potpuno kvalificirano ime staze i datoteke za eksportirani certifikat provjere potpisa i kliknite **Nastavak** da eksportirate certifikat.

Sada možete dodati ovu datoteku paketu instalacije aplikacije kojeg kreirate za vaš proizvod. Upotrebljavajući API za Dodavanje provjeritelja kao dijela instalacijskog programa, možete dodati ovaj certifikat korisnikovom *SIGNATUREVERIFICATION spremištu certifikata. Ovaj API će također kreirati ovo spremište certifikata ako već ne postoji. Program za instalaciju proizvoda može zatim provjeravati potpise na objektima aplikacija dok ih vraća na korisnikove iSeries poslužitelje.

Korak 6: Ažuriranje programa za pakiranje aplikacija da koristi iSeries API-je za potpisivanje vaše aplikacije

Sada kad datoteku certifikata za provjeru potpisa trebate dodati paketu aplikacija, možete upotrijebiti API Potpisivanje objekata za pisanje ili uređivanje postojeće aplikacije za potpisivanje knjižnica proizvoda dok ih pakirate za distribuciju korisnicima.

Da bolje shvatite kako upotrebljavati API Potpisivanja objekata kao dijela programa za pakiranje aplikacija, pregledajte sljedeće primjere kodova. Ovaj primjer koda snippet, pisan u C-u, nije potpuni program za pakiranje i potpisivanje; to je primjer dijela takvog programa koji poziva API Potpisivanje objekata. Ako odlučite upotrijebiti ovaj primjer programa, prilagodite ga vašim potrebama. Radi razloga sigurnosti IBM preporučuje da individualizirate primjer programa, a ne da koristite dobivene default vrijednosti.

Bilješka: IBM vam dodjeljuje neekskluzivnu licencu autorskih prava za upotrebu svih primjera koda iz kojih možete generirati slične funkcije oblikovane za vaše specifične potrebe. Sve primjere koda osigurao je IBM samo za svrhu ilustracije. Ovi primjeri nisu potpuno ispitani u svim uvjetima. IBM, prema tome, ne može jamčiti niti potvrditi pouzdanost, upotrebljivost ili funkcionalnost tih programa. Svi ovdje sadržani programi se isporučuju ″KAKVI JESU″, bez bilo kakvih jamstava. Neizravna jamstva o nekršenju, lakoj prodaji i sposobnosti za određenu svrhu se izričito poriču.

Promijenite ovaj kod snippet da odgovara vašim potrebama za upotrebu API-ja Potpisivanje objekata kao dijela programa pakiranja aplikacijskog proizvoda. Trebate proslijediti dva parametra ovom programu: ime knjižnice za potpisivanje i ime ID-a aplikacije za potpisivanje objekata; ID aplikacije je osjetljiv na mala i velika slova, dok ime knjižnice nije osjetljivo. Program koji pišete može pozvati ovaj snippet nekoliko puta ako se upotrebljavaju nekoliko knjižnica kao dio proizvoda kojeg potpisujete.

Bilješka: Pročitajte “Izjava o odricanju od koda” na stranici 42 radi važnih pravnih informacija.

```
/* ------------------------------------------------------------- */
/*                                                               */
/* AUTORSKO PRAVO (C) IBM CORP. 2002., 2004.                     */
/*                                                               */
/* Upotreba API Potpisa objekata za potpis jedne ili više knjižnica */
/*                                                               */
/* API će digitalno potpisati sve objekte u navedenoj knjižnici  */
/*                                                               */
/*                                                               */
/*                                                               */
/* IBM vam dodjeljuje neekskluzivnu licencu autorskih prava za   */
/* upotrebu primjera programskog koda iz kojeg generirate slične */
/* funkcije oblikovane za vaše posebne potrebe.                  */
/* Sve primjere koda IBM je osigurao samo za svrhu ilustracije   */
/* Ovi primjeru nisu u potpunosti                                */
/* ispitani u svim uvjetima. IBM, prema tome, ne može jamčiti    */
/* ili potvrditi pouzdanost, upotrebljivost ili funkcionalnost   */
/* ovih programa.  Svi ovdje sadržani progami se                 */
/* daju "KAKVI JESU" bez bilo kakvih jamstava.                   */
/* Podrazumijevana jamstva o nekršenju, iskoristivosti i         */
/* podobnosti za određenu svrhu se izričito poriču.              */
/*                                                               */
```

```
/*                                                                  */
/*                                                                  */
/* Parametri su sljedeći:  */
/*                                                                  */
/*  char *   ime knjižnice za potpisivanje                          */
/*  char *   ime ID-a aplikacije                                    */
/*                                                                  */

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

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

    /* parametri:

       char * knjižnica u kojoj se potpisuju objekti,
       char * identifikator aplikacije s kojom se potpisuje

     */

    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;    /* izuzeci povrata za svaku grešku */


    /* ------------------------------------ */
    /* sagradite ime staze dane imenu knjižnice */
    /* ------------------------------------ */
    memset(libname, '\00', 11); /* inicijalizirajte ime knjižnice. */
    for(lib_length = 0;
        ((*(argv[1] + lib_length) != ' ') &&
         (*(argv[1] + lib_length) != '\00'));
        lib_length++);
    memcpy(argv[1], libname, lib_length); /* unesite ime knjižnice*/

    /* izgradite ime staze parm za API poziv */
    sprintf(path_name, "/QSYS.LIB/%s.LIB/*", libname);
    path_length = strlen(path_name);

    /* ---------------------------- */
    /* nađite dužinu id-a aplikacje */
    /* ---------------------------- */
    for(applid_length = 0;
        ((*(argv[2] + applid_length) != ' ') &&
         (*(argv[2] + applid_length) != '\00'));
        applid_length++);

    /* ------------------------------- */
    /* potpišite sve objekte u ovoj knjižnici */
    /* ------------------------------- */
    QYDOSGNO  (path_name,             /* ime staze za objekt */
               &path_length,          /* dužina imena staze */
               "OBJN0100",            /* ime formata */
               argv[2],               /* identifikator aplikacije (ID) */
               &applid_length,        /* dužina ID-a aplikacije */
               "1",                   /* zamijenite duplikat potpisa */
               multi_objects,         /* kako rukovati višestrukim
                                         objektima */
               &multiobj_length,      /* dužina strukture višestrukih objekata
```

```
                                        koja se treba upotrebljavati
                                      (0=no mult.object struktura)*/
              &error_code);          /* kod greške */


      povrat 0;

 }
```

Korak 7: Kreiranje izlaznog programa predinstalacije koji koristi API Dodavanje provjeritelja

Sada kad imate programatsku obradu za potpisivanje aplikacije, možete upotrijebiti API za Dodavanje provjeritelja kao dijela programa za instaliranje da kreirate konačni proizvod za distribuciju. Na primjer, API Dodavanje provjeritelja dio je predinstaliranog izlaznog programa za osiguranje da je certifikat dodan u spremište certifikata prije vraćanja potpisanih objekta aplikacije. Time se omogućuje da instalacijski program provjerava potpise na objektima aplikacija dok se vraćaju na korisnikov iSeries poslužitelj.

Bilješka: Radi sigurnosnih razloga ovaj API ne dopušta umetanje certifikata Izdavača certifikata (CA) u *SIGNATUREVERIFICATION spremište certifikata. Kad dodajete CA certifikat spremištu certifikata, sistem smatra da je CA pouzdan izvor certifikata. Radi toga, sistem postupa sa certifikatom kojeg je izdao CA kao s onim čije je porijeklo od pouzdanog izvora. Prema tome, možete upotrebljavati API za kreiranje instalacijskog izlaznog programa da umetnete CA certifikat u memoriju certifikata. Morate upotrijebiti Upravitelja digitalnih certifikata za dodavanje CA certifikata u spremište da se osigurate da netko mora posebno i ručno kontrolirati kojim CA-ovima vjeruje sistem. Ako to napravite onemogućiti ćete da sistem može importirati certifikate iz izvora koje administrator nije svjesno naveo kao povjerljive.

Ako želite spriječiti da bilo tko koristi ovaj API za dodavanje certifikata za provjeru u vaše *SIGNATUREVERIFICATION spremište certifikata bez vašeg znanja, morate razmotriti onemogućavanje ovog API-ja na vašem sistemu. To možete učiniti upotrebljavajući Sistemske servisne alate (SST) da ne dopustite promjene sistemskih vrijednosti koje se odnose na sigurnost. .

Da bolje shvatite kako upotrebljavati API Potpisivanja objekata kao dijela programa za instaliranje aplikacija, pogledajte sljedeći primjer koda predinstalacijskog izlaznog programa. Ovaj primjer koda snippet, pisan u C-u, nije potpuni predinstalacijski izlazni program; to je prije primjer dijela programa koji poziva API Dodavanje provjeritelja. Ako odlučite upotrijebiti ovaj primjer programa, prilagodite ga vašim potrebama. Radi razloga sigurnosti IBM preporučuje da individualizirate primjer programa, a ne da koristite dobivene default vrijednosti.

Bilješka: IBM vam dodjeljuje neekskluzivnu licencu autorskih prava za upotrebu svih primjera koda iz kojih možete generirati slične funkcije oblikovane za vaše specifične potrebe. Sve primjere koda IBM dostavlja samo za ilustrativne svrhe. Ovi primjeri nisu bili temeljito testirani u svim uvjetima. IBM, prema tome, ne može jamčiti niti potvrditi pouzdanost, upotrebljivost ili funkcionalnost tih programa. Svi ovdje sadržani programi se isporučuju ″KAKVI JESU″, bez bilo kakvih jamstava. Neizravna jamstva o nekršenju, lakoj prodaji i sposobnosti za određenu svrhu se izričito poriču.

Promijenite ovaj kod snippet da odgovara vašim potrebama za upotrebu API-ja Dodavanje provjeritelja kao dijela predinstalacijskog izlaznog programa da dodate potrebni certifikat provjere potpisa korisnikovom iSeries poslužitelju kad instalira vaš proizvod.

Bilješka: Pročitajte “Izjava o odricanju od koda” na stranici 42 radi važnih pravnih informacija.

```
/* ------------------------------------------------------------ */
/*                                                              */
/* AUTORSKO PRAVO (C) IBM CORP. 2002., 2004.                    */
/*                                                              */
/* Upotreba API-ja Dodavanje provjeritelja za dodavanje certifikata */
/* u navedenu datoteku integriranog sistema datoteka u          */
/* *SIGNATUREVERIFICATION spremište certifikata.                */
/*                                                              */
/*                                                              */
```

```
/* Ovaj API će kreirati spremište certifikata ako već ne postoji.   */
/* Ako je spremište certifikata kreirano dobit će default           */
/* lozinku koja se treba čim prije promijeniti pomoću DCM-a.        */
/* Ovo upozorenje treba dati vlasnicima sistema koji                */
/* upotrebljavaju ovaj program.                                     */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* IBM vam dodjeljuje neekskluzivnu licencu autorskih prava za      */
/* upotrebu primjera programskog koda iz kojeg generirate slične    */
/* funkcije oblikovane za vaše posebne potrebe.                     */
/* Sve primjere koda IBM je osigurao samo za svrhu ilustracije      */
/* Ovi primjeru nisu u potpunosti                                   */
/* ispitani u svim uvjetima. IBM, prema tome, ne može jamčiti       */
/* ili potvrditi pouzdanost, upotrebljivost ili funkcionalnost      */
/* ovih programa.  Svi ovdje sadržani progami se                    */
/* daju "KAKVI JESU" bez bilo kakvih jamstava.                      */
/* Podrazumijevana jamstva o nekršenju, iskoristivosti i            */
/* podobnosti za određenu svrhu se izričito poriču.                 */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Parametri su sljedeći:  */
/*                                                                  */
/*  char *   ime staze datoteke integriranog sistema datoteka koje  */
/*           drži certifikat                                        */
/*  char *   oznaku certifikata za davanje certifikata              */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* ---------------------------------------------------------------- */

#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];

    /* nađite dužinu imena staze */
    for(pathname_length = 0;
        ((*(pathname + pathname_length) != ' ') &&
         (*(pathname + pathname_length) != '\00'));
        pathname_length++);

    /* nađite dužinu certifikatske oznake*/
    for(cert_label_length = 0;
        ((*(certlabel + cert_label_length) != ' ') &&
         (*(certlabel + cert_label_length) != '\00'));
        cert_label_length++);


    error_code.Bytes_Provided = 0;    /* izuzeci povrata za svaku grešku */

    QydoAddVerifier (pathname,         /* ime staze za datoteku sa certifikatom*/
                     &pathname_length, /* dužina imena staze */
                     "OBJN0100",            /* ime formata */
                     certlabel,        /* certifikatska oznaka */
                     &cert_label_length, /* dužina certifikatske oznake */
```

```
                    &error_code);          /* kod greške */

    povrat 0;
}
```

S ovim dovršenim zadacima možete pakirati aplikaciju i distribuirati ju korisnicima. Kad instaliraju aplikaciju, potpisani objekti aplikacija se provjeravaju kao dio instalacijske obrade. Kasnije mogu korisnici upotrebljavati Upravitelja digitalnih certifikata (DCM) za provjeru potpisa na objektima aplikacija. Time se omogućuje korisnicima da odrede da je izvor aplikacije pouzdan i da odrede da li su se desile promjene od kada ste potpisali aplikaciju.

Bilješka: Instalacijski program je možda kreirao *SIGNATUREVERIFICATION spremište certifikata s default lozinkom za korisnika. Morate svoje korisnike savjetovati da trebaju koristiti DCM za ponovno postavljanje lozinke spremišta certifikata što je prije moguće da se zaštite od neovlaštenog pristupa.

Korak 8: Neka korisnici ponovno postave default lozinku za *SIGNATUREVERIFICATION spremište certifikata

API Dodavanje provjeritelja je možda kreirao *SIGNATUREVERIFICATION spremište certifikata kao dio postupka instaliranja proizvoda na korisnikovom iSeries poslužitelju. Ako je API kreirao spremište certifikata, kreirao je za njega i default lozinku. Morate svoje korisnike savjetovati da trebaju koristiti DCM za ponovno postavljanje lozinke spremišta certifikata što je prije moguće da se zaštite od neovlaštenog pristupa.

Neka korisnici dovrše ove korake za ponovno postavljanje lozinke *SIGNATUREVERIFICATION spremišta certifikata:
1. Pokrenite DCM.
2. U navigacijskom okviru kliknite**Izbor spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** za otvaranje.
3. Kad se prikaže stranica Spremište certifikata i Lozinka, kliknite **Ponovno postavljanje lozinke** da se prikaže stranica Ponovno postavljanje lozinke spremišta certifikata.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite upitnik (**?**) na vrhu stranice da pristupite online pomoći.
4. Navedite novu lozinku za spremište, ponovno ju unesite za potvrdu, izaberite politiku isteka lozinke ili kliknite **Nastavak**.

Scenarij: Upotreba iSeries Navigator Središnjeg Upravljanja za potpisivanje objekata

Situacija

Vaše poduzeće (MyCo, Inc.) razvija aplikacije koje distribuira višestrukim iSeries poslužiteljima na višestrukim mjestima u poduzeću. Kao mrežni administrator odgovorni ste za sigurnost ažuriranja i instaliranja ovih aplikacija na svim iSeries poslužiteljima poduzeća. Trenutno koristite iSeries Navigator funkcije Središnjeg upravljanja za lakše pakiranje i distribuiranje tih aplikacija i izvođenje ostalih administrativnih zadataka za koje ste odgovorni. Međutim, trošite više vremena nego što ste htjeli prateći i ispravljajući probleme s ovim aplikacijama zbog neovlaštenih promjena na objektima. Radi toga želite bolje osigurati cjelovitost ovih objekata potpisujući ih digitalno.

Istražili ste sposobnosti OS/400 potpisivanja objekta i naučili da, počevši od V5R2, Središnje Upravljanje dopušta potpisivanje objekata kad ih pakirate i distribuirate. Upotrebljavajući Središnje Upravljanje možete djelotvorno i relativno lako zadovoljiti sigurnosne ciljeve vašeg poduzeća. Također ste odlučili kreirati Lokalnog izdavača certifikata (CA) i upotrebljavati ga za izdavanje certifikata za potpisivanje objekata. Upotreba certifikata kojeg je izdao Lokalni CA za potpisivanje objekata ograničava trošak korištenja ove tehnologije sigurnosti, jer ne morate kupiti certifikat od javnog dobro poznatog CA.

Ovaj primjer služi kao korisni uvod za korake uključene u konfiguriranje i upotrebu potpisivanja objekata za aplikacije koje distribuirate višestrukim iSeries poslužiteljima poduzeća.

Prednosti scenarija

Ovaj scenarij ima sljedeće prednosti:
- Upotreba Središnjeg Upravljanja za pakiranje i potpisivanja objekata skraćuje vrijeme koje morate utrošiti za distribuciju potpisanih objekata iSeries poslužiteljima poduzeća.
- Upotrebom Središnjeg Upravljanja za potpisivanje objekata smanjuje se broj koraka koje morate obaviti za potpisivanje objekata, jer je postupak potpisivanja dio postupka pakiranja.
- Potpisivanje paketa objekata omogućuje da lakše odredite da li su objekti promijenjeni nakon što su bili potpisani. Ovim se mogu smanjiti neka rješavanja problema koja ćete raditi u budućnosti za praćenje problema aplikacija.
- Upotreba certifikata kojeg je izdao Lokalni izdavač certifikata (CA) za potpisivanje objekata pojeftinjuje primjenu potpisivanja objekata.

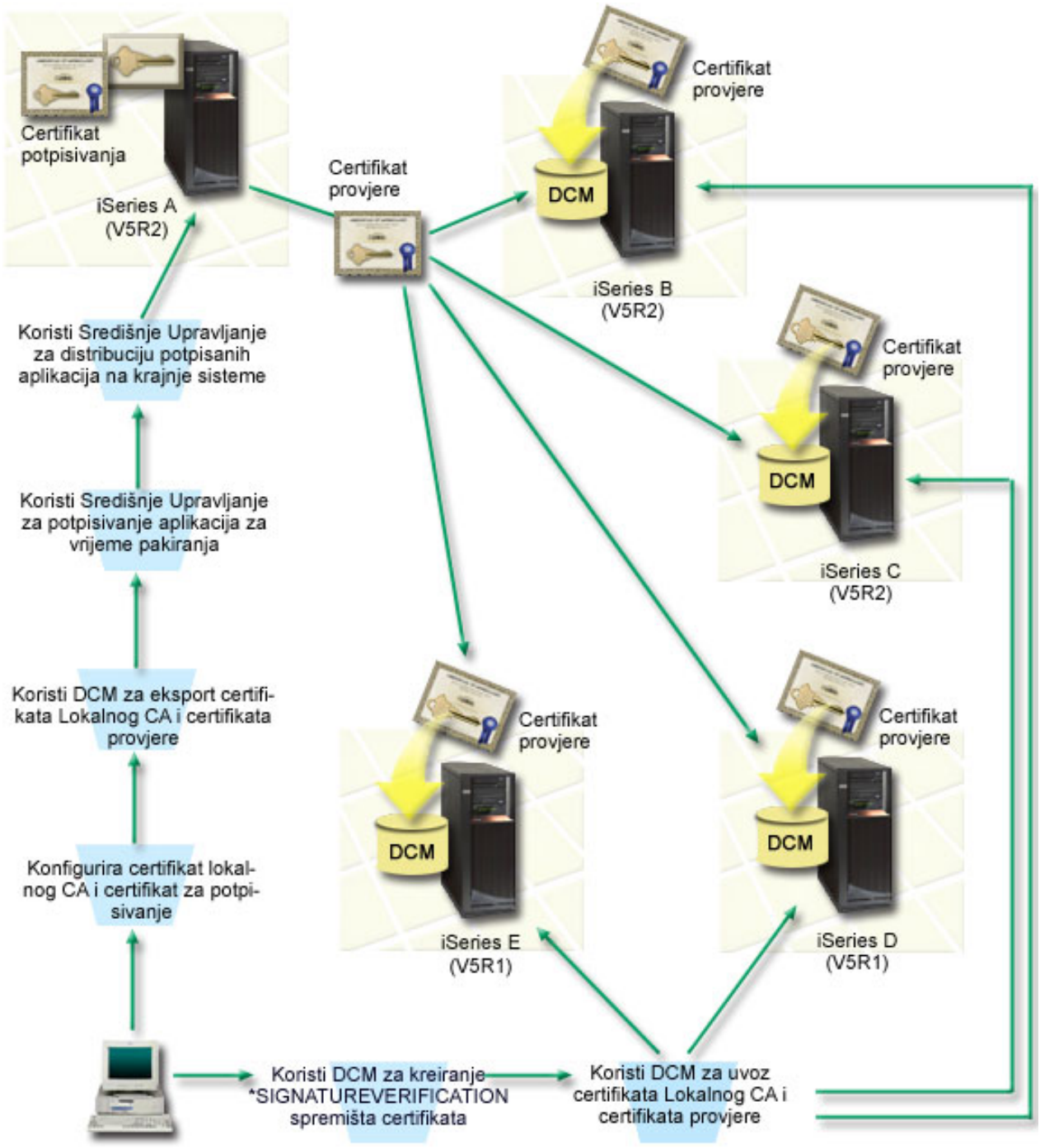
Ciljevi

U ovom scenariju, MyCo, Inc. želi digitalno potpisivati aplikacije koje distribuira višestrukim iSeries poslužiteljima u poduzeću. Kao administrator mreže pri MyCo, Inc. već koristite Središnje upravljanje za razne iSeries administrativne zadatke. Radi toga želite proširiti trenutnu upotrebu Središnjeg Upravljanja za potpisivanje aplikacija poduzeća koje distribuirate drugim iSeries poslužiteljima.

Ciljevi ovog scenarija su sljedeći:
- Aplikacije poduzeća se moraju potpisivati sa certifikatom kojeg je izdao Lokalni CA da se ograniče troškovi potpisivanja aplikacija.
- Sistemski administratori i drugi ovlašteni korisnici moraju moći lako provjeriti digitalne potpise na svim iSeries poslužiteljima da provjere izvor i vjerodostojnost objekata koje je potpisalo poduzeće. Da se to postigne svaki iSeries poslužitelj mora imati kopiju certifikata poduzeća za provjeru potpisa i certifikat Lokalnog izdavača certifika (CA) u *SIGNATUREVERIFICATION spremištu certifikata svakog poslužitelja.
- Provjerom potpisa na aplikacijama poduzeća omogućuje se da iSeries administratori i drugi mogu otkriti da li su sadržaji objekata promijenjeni od kada su bili potpisani.
- Administratori moraju moći upotrebljavati Središnje Upravljanje za pakiranje, potpisivanje i distribuciju njihove aplikacije njihovim iSeries poslužiteljima.

Detalji

Sljedeća slika ilustrira postupak potpisivanja objekta i provjere potpisa za primjenu ovog scenarija:



Slika ilustrira sljedeće točke relevantne za ovaj scenarij:

Centralni sistem (iSeries A)

- iSeries A radi s OS/400 verzijom 5, izdanje 2 (V5R2).
- iSeries A služi kao centralni sistem s kojeg se izvode funkcije Središnjeg Upravljanja, uključujući pakiranje i distribuiranje aplikacija poduzeća.
- iSeries ima instaliran Dobavljač kriptografičkog pristupa 128-bitni za iSeries (5722–AC3).
- iSeries A ima instaliran i konfiguriran Upravitelj digitalnih certifikata (OS/400 opcija 34) i IBM HTTP poslužitelj (5722–DG1).
- iSeries A djeluje kao Lokalni izdavač certifikata (CA) i certifikat za potpisivanje objekta se nalazi na tom sistemu.

- iSeries A je primarni sistem za potpisivanje objekata za aplikacije poduzeća. Potpisivanje objekta proizvoda za korisničku distribuciju postiže se na iSeries A izvođenjem ovih zadataka:
  1. Upotreba DCM-a za kreiranje Lokalnog CA-a i upotreba Lokalnog CA za kreiranje certifikata za potpisivanje objekta.
  2. Upotreba DCM-a za eksportiranje kopije certifikata Lokalnog CA i certifikata za provjeru potpisa u datoteku tako da sistemi krajnjih točaka (iSeries B, C, D i E) mogu provjeriti potpisane objekte.
  3. Upotreba Središnjeg Upravljanja za potpisivanje objekata aplikacija i njihovo pakiranje s datotekama certifikata provjere.
  4. Upotreba Središnjeg Upravljanja za distribuciju potpisanih aplikacija i datoteka certifikata krajnjim sistemima.

Krajnji sistemi (iSeries poslužitelji B, C, D i E)

- iSeries B i C rade s OS/400 verzijom 5, izdanje 2 (V5R2).
- iSeries D i E rade s OS/400 verzijom 5, izdanje 1 (V5R1).
- iSeries B, C, D i E imaju instalirane i konfigurirane Upravitelja digitalnih certifikata (opcija 34) i IBM HTTP poslužitelj (5722–DG1).
- iSeries B, C, D i E primaju kopiju certifikata za provjeru potpisa poduzeća i Lokalnog CA iz središnjeg sistema (iSeries A) kada sistem primi potpisanu aplikaciju.
- DCM se upotrebljava za kreiranje *SIGNATUREVERIFICATION spremišta certifikata i importiranje certifikata Lokalnog CA i certifikata provjere u ovo spremište certifikata.

Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:
1. Svi iSeries poslužitelji zadovoljavaju zahtjeve za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).
2. Nitko nije ranije konfigurirao ili upotrebljavao DCM na nijednom iSeries poslužitelju.
3. iSeries A zadovoljava zahtjeve za instaliranje i upotrebu iSeries Navigatora i Središnjeg Upravljanja.
4. Poslužitelj Središnjeg Upravljanja mora raditi na svim iSeries krajnjim sistemima.
5. Svi iSeries poslužitelji imaju instaliranu najveću razinu licencnog programa Dobavljača kriptografičkog pristupa 128-bitni (5722-AC3).
6. Default postavka za provjeru potpisa objekata za vrijeme vraćanja (QVFYOBJRST) sistemske vrijednosti na sve iSeries poslužitelje u scenariju je 3 i nije se mijenjala od ove postavke. Default postavka osigurava da poslužitelj može provjeriti potpise objekata čim se vrate potpisani objekti.
7. Mrežni administrator za iSeries A mora imati posebno ovlaštenje *ALLOBJ za potpisivanje objekata ili korisnički profil mora biti ovlašten za aplikaciju potpisivanja objekata.
8. Mrežni administrator ili bilo tko (uljučujući program), tko kreira spremište certifikata u DCM-u, mora imati posebna ovlaštenja *SECADM i *ALLOBJ.
9. Sistemski administrator ili drugi na svim drugim iSeries poslužiteljima moraju imati posebno ovlaštenje za korisnički profil *AUDIT za provjeru potpisa objekata.

Koraci zadatka konfiguracije

Postoje dva skupa zadataka koje morate dovršiti za primjenu ovog scenarija: Jedan skup zadataka omogućuje konfiguriranje iSeries A, za upotrebu Središnjeg Upravljanja za potpisivanje i distribuiranje aplikacija. Drugi skup zadataka omogućuje sistemskom administratoru i drugima da provjeravaju potpise na tim aplikacijama na svim drugim iSeries poslužiteljima.

Koraci zadatka potpisivanja objekata

Morate dovršiti svaki od ovih zadataka na iSeries A da potpisujete objekte kao što opisuje ovaj scenarij:
1. Završite sve korake preduvjeta da instalirate i konfigurirate sve potrebne iSeries proizvode
2. Koristite DCM za kreiranje Lokalnog izdavača certifikata (CA) za izdavanje privatnog certifikata za potpis objekta.
3. Koristite DCM za kreiranje definicije aplikacije.
4. Koristite DCM za dodjelu certifikata definiciji aplikacije za potpisivanje objekta

5. Koristite DCM za eksport certifikata koje ostali sistemi moraju koristiti za provjeru potpisa objekata
   Morate eksportirati kopiju certifikata Lokalnog CA i kopiju certifikata za potpisivanje objekta kao certifikat provjere potpisa u datoteku.
6. Prenesite datoteke certifikata na svaki iSeries krajnji sistem na kojem želite provjeriti potpise.
7. Koristite Središnje Upravljanje iSeries Navigatora za potpisivanje objekata aplikacije

Koraci zadatka provjere potpisa

Ove zadatke konfiguracije provjere potpisa morate završiti na iSeries krajnjim sistemima da bi mogli koristiti Središnje Upravljanje za prijenos potpisanih aplikacija objekata na njih. Konfiguracija provjere potpisa mora biti dovršena prije nego što možete uspješno provjeriti potpise kad vraćate potpisane objekte na krajnje sisteme.

Na svakom iSeries krajnjem sistemu, morate dovršiti ove zadatke za provjeru potpisa na objektima kao što opisuje ovaj scenarij:
8. Koristite DCM za kreiranje *SIGNATUREVERIFICATION spremišta certifikata
9. Koristite DCM za import certifikata Lokalnog CA i certifikata provjere potpisa

Detalji scenarija: Upotreba Središnjeg Upravljanja iSeries Navigatora za potpisivanje objekata

Dovršite sljedeće korake zadataka za konfiguraciju i upotrebu Središnjeg Upravljanja za potpisivanje objekata kao što opisuje ovaj scenarij.

Korak 1: Izvođenje svih koraka preduvjeta

Morate dovršiti sve zadatke preduvjeta da instalirate i konfigurirate sve potrebne iSeries proizvode prije izvođenja određenih zadataka konfiguracije za primjenu ovog scenarija.

Korak 2: Kreiranje Lokalnog izdavača certifikata za izdavanje privatnih certifikata za potpisivanje objekata

Kad upotrebljavate Upravitelja digitalnih certifikata (DCM) za kreiranje Lokalnog izdavača certifikata (CA), taj postupak zahtijeva dovršavanje niza obrazaca. Ti obrasci vas vode kroz postupak kreiranja CA i dovršavanje drugih zadataka potrebnih za početak upotrebe digitalnih certifikata za Sloj sigurnih utičnica (SSL), potpisivanje objekata i provjeru potpisa. Iako u ovom scenariju ne trebate konfigurirati certifikate za SSL, morate dovršiti sve obrasce u zadatku da konfigurirate sistem za potpisivanje objekata.

Da koristite DCM za kreiranje i rad s Lokalnim CA, izvedite ove korake:
1. Pokrenite DCM.
2. U navigacijskom okviru DCM-a izaberite **Kreiranje Izdavača certifikata (CA)** za prikaz slijeda obrazaca.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite upitnik (**?**) na vrhu stranice za pristup online pomoći.
3. Popunite sve obrasce u ovom vođenom zadatku. Kad obavljate ovaj zadatak morate napraviti sljedeće:
   a. Osigurati identifikacijske informacije za Lokalnog CA.
   b. Instalirati certifikat Lokalnog CA u pretražitelj tako da softver može prepoznati Lokalnog CA i provjeriti valjanost certifikata koje izdaje Lokalni CA.
   c. Navesti podatke politike za Lokalnog CA.
   d. Upotrijebiti novog Lokalnog CA za izdavanje certifikata poslužitelja ili klijenta kojeg aplikacije mogu upotrijebiti za SSL veze.

      Bilješka: Iako ovaj scenarij ne koristi ovaj certifikat, morate ga kreirati prije nego što možete upotrebljavati Lokalni CA za izdavanje potrebnog certifikata za potpisivanje objekata. Ako opozovete zadatak bez kreiranja certifikata, morate kreirati certifikat za potpisivanje objekata i *OBJECTSIGNING spremište certifikata u kojoj je on odvojeno pohranjen.
   e. Izabrati aplikacije koje mogu upotrebljavati certifikat poslužitelja ili klijenta za SSL veze.

Bilješka: Za svrhu ovog scenarija nemojte izabrati nikakvu aplikaciju i kliknite **Nastavak** da se prikaže sljedeći obrazac.

f. Upotrijebiti novi Lokalni CA za izdavanje certifikata za potpisivanje objekata kojeg aplikacije mogu upotrijebiti za digitalno potpisivanje objekata. Ovaj podzadatak kreira *OBJECTSIGNING spremište certifikata. To je spremište certifikata koje upotrebljavate za upravljanje certifikatima za potpisivanje objekata.

g. Izabrati aplikacije kojima će vaš lokalni CA vjerovati.

Bilješka: Za svrhe ovog scenarija nemojte izabrati nikakvu aplikaciju i kliknite **Nastavak** da se završi ovaj zadatak.

Sada kada ste kreirali Lokalni CA i certifikat za potpisivanje objekata, morate definirati aplikaciju za potpisivanje objekata da upotrijebite certifikat prije nego što možete potpisivati objekte.

Korak 3: Kreiranje definicije aplikacije za potpisivanje objekata

Nakon kreiranja certifikata za potpisivanje objekata morate upotrijebiti Upravitelja digitalnih certifikata (DCM) da definirate aplikaciju za potpisivanje objekata koju možete upotrijebiti za potpisivanje objekata. Definicija aplikacije ne treba se odnositi na stvarnu aplikaciju. Definicija aplikacije koju kreirate može opisati tip ili grupu objekata koje ste htjeli potpisati. Definiciju trebate da možete imati ID aplikacije za pridruživanje sa certifikatom i da omogućite postupak potpisivanja.

Da upotrijebite DCM za kreiranje definicije aplikacije za potpisivanje objekata, slijedite ove korake:

1. U navigacijskom okviru kliknite **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** da se otvori spremište certifikata.
2. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
3. U navigacijskom okviru izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
4. Izaberite **Dodavanje aplikacije** iz popisa zadataka da se prikaže obrazac za definiranje aplikacije.
5. Dovršite obrazac i kliknite **Dodaj**.

Sada morate dodijeliti certifikat za potpisivanje objekata aplikaciji koju ste kreirali.

Korak 4: Dodjela certifikata definiciji aplikacije za potpisivanje objekata.

Da dodijelite certifikat aplikaciji za potpisivanje objekata, slijedite ove korake:

1. U DCM navigacijskom okviru izaberite **Upravljanje certifikatima** da se prikaže popis zadataka.
2. Iz popisa zadataka izaberite **Dodjela certifikata** da prikažete listu certifikata za trenutno spremište certifikata.
3. Izaberite certifikat s popisa i kliknite **Dodjela aplikacijama** da prikažete listu definicija aplikacija za trenutno spremište certifikata.
4. Izaberite jednu ili više aplikacija s popisa i kliknite **Nastavak**. Prikazuje se stranica poruke ili za potvrdu dodjele certifikata ili za prikaz informacija o greški ako se desio problem.

Kad dovršite ovaj zadatak, spremni ste za potpisivanje objekata pomoću Središnjeg Upravljanja kad ih pakirate i distribuirate. Međutim, da se osigurate da vi ili drugi mogu provjeravati potpise, morate eksportirati potrebne certifikate u datoteku i prenijeti ih svim iSeries krajnjim sistemima. Trebate također dovršiti sve zadatke za konfiguriranje provjere potpisa na svakom iSeries krajnjem sistemu prije upotrebe Središnjeg Upravljanja za prijenos potpisanih objekata aplikacija na njih. Konfiguracija provjere potpisa mora biti dovršena prije nego što možete uspješno provjeriti potpise kad vraćate potpisane objekte na krajnje sisteme.

Korak 5: Eksportiranje certifikata za omogućavanje provjere potpisa na drugim iSeries sistemima

Potpisivanje objekata za zaštitu cjelovitosti sadržaja zahtijeva da vi i drugi imate način za provjeru vjerodostojnosti potpisa. Da provjerite potpise na objektima na istom sistemu koji potpisuje objekte, morate upotrijebiti DCM za kreiranje *SIGNATUREVERIFICATION spremišta certifikata. To spremište certifikata mora sadržavati kopiju certifikata za potpisivanje objekata i kopiju certifikata CA za CA koji izdao certifikat za potpisivanje.

Da omogućite drugima provjeru potpisa, morate ih opskrbiti s kopijom certifikata koji je potpisao objekt. Kad upotrebljavate Lokalnog izdavača certifikata (CA) za izdavanje certifikata, morate i njega opskrbiti s kopijom certifikata Lokalnog CA.

Da upotrijebite DCM za provjeru potpisa na istom sistemu koji potpisuje objekte (iSeries A u ovom scenariju) slijedite ove korake:
1. U navigacijskom okviru kliknite **Kreiranje novog spremišta certifikata** i izaberite***SIGNATUREVERIFICATION** kao spremište certifikata za kreiranje.
2. Izaberite **Da** da kopirate postojeće certifikate za potpisivanje objekata u novo spremište certifikata kao certifikate za provjeru potpisa.
3. Odredite lozinku za novo spremište certifikata i kliknite **Nastavak** za kreiranje spremišta certifikata. Sada možete upotrebljavati DCM za provjeru potpisa objekata na istom sistemu kojeg upotrebaljavate za potpisivanje objekata.

Da upotrijebite DCM za eksport kopije certifikata Lokalnog CA i kopije certifikata za potpisivanje objekata kao certifikata za provjeru potpisa, tako da možete provjeravati potpise objekata na drugim sistemima, slijedite ove korake:
1. U navigacijskom okviru izaberite **Upravljanje certifikatima** i zatim izaberite zadatak **Eksport certifikata**.
2. Izaberite **Izdavač certifikata (CA)** i kliknite **Nastavak** da se prikaže popis CA certifikata koje možete eksportirati.
3. Izaberite certifikat Lokalnog CA koji ste kreirali ranije s popisa i kliknite **Eksport**.
4. Navedite **Datoteku** kao odredište eksportiranja i kliknite **Nastavak**.
5. Navedite potpuno kvalificirano ime staze i datoteke za eksportirani certifikat Lokalnog CA i kliknite **Nastavak** da eksportirate certifikat.
6. Kliknite **OK** da izađete iz stranice za potvrdu Eksporta. Sada možete eksportirati kopiju certifikata za potpisivanje objekta.
7. Ponovno postavite zadatak **Eksport certifikata**.
8. Izaberite **Potpisivanje objekata** da se prikaže popis certifikata za potpisivanje objekata koje možete eksportirati.
9. Izaberite odgovarajući certifikat za potpisivanje objekta s popisa i kliknite **Eksport**.
10. Izaberite **Datoteku, kao certifikat provjere potpisa** za destinaciju i kliknite **Nastavak**.
11. Navedite potpuno kvalificirano ime staze i datoteke za eksportirani certifikat provjere potpisa i kliknite **Nastavak** da eksportirate certifikat.

Sada možete prenijeti ove datoteke na iSeries krajnje sisteme na kojima namjeravate provjeravati potpise koje ste kreirali sa certifikatom.

Korak 6: Prijenos datoteka certifikata na krajnje iSeries sisteme

Morate prenijeti datoteke certifikata koje ste kreirali na iSeries A na iSeries krajnje sisteme u ovom scenariju prije nego što ih možete konfigurirati za provjeru objekata koje potpisujete. Možete upotrijebiti nekoliko različitih metoda za prijenos datoteka certifikata. Na primjer, možete koristiti FTP ili distribuciju paketa Središnjeg Upravljanja za prijenos podataka.

Korak 7: Potpisivanje objekata pomoću Središnjeg Upravljanja

Postupak potpisivanja objekta za Središnje Upravljanje je dio postupka distribucije softverskog pakiranja. Trebate dovršiti sve zadatke konfiguriranja provjere potpisa na svakom iSeries krajnjem sistemu prije upotrebe Središnjeg Upravljanja za prijenos potpisanih objekata aplikacija na njih. Konfiguracija provjere potpisa mora biti dovršena prije nego što možete uspješno provjeriti potpise kad vraćate potpisane objekte na krajnje sisteme.

Za potpisivanje aplikacije koju distribuirate na iSeries krajnje sisteme kao što opisuje ovaj scenarij, slijedite ove korake:
1. Upotrijebite Središnje Upravljanje za pakiranje i distribuiranje softverskih proizvoda .
2. Kad dođete na panel **Identifikacija** u čarobnjaku **Definicije proizvoda**, kliknite **Napredno** da se prikaže panel **Napredna identifikacija**.
3. U polje **Digitalno potpisivanje** unesite ID aplikacije za aplikaciju potpisivanja objekta koju ste ranije kreirali i kliknite **OK**.

4. Dovršite čarobnjaka i nastavite obradu za pakiranje i distribuiranje softverskih proizvoda sa Središnjim Upravljanjem.

Korak 8: Zadaci provjere potpisa: Kreiranje *SIGNATUREVERIFICATION spremišta certifikata na iSeries krajnjim sistemima

Da provjerite potpise objekata na iSeries krajnjim sistemima u ovom scenariju, svaki sistem mora imati kopiju odgovarajućeg certifikata za provjeru potpisa u *SIGNATUREVERIFICATION spremištu certifikata. Ako je privatni certifikat potpisao objekte, to spremište certifikata mora također sadržavati kopiju certifikata Lokalnog CA.

Da kreirate *SIGNATUREVERIFICATION spremište certifikata, slijedite ove korake:
1. Pokrenite DCM.
2. U navigacijskom okviru Upravitelja digitalnih certifikata (DCM) izaberite **Kreiranje novog spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za kreiranje.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite upitnik (**?**) na vrhu stranice da pristupite online pomoći.
3. Odredite lozinku za novo spremište certifikata i kliknite **Nastavak** za kreiranje spremišta certifikata. Sada možete importirati certifikate u spremište i upotrebljavati ih za provjeru potpisa objekata.

Korak 9: Zadaci provjere potpisa: Import certifikata

Da se provjeri potpis na objektu, *SIGNATUREVERIFICATION spremište certifikata mora sadržavati kopiju certifikata za provjeru potpisa. Ako je certifikat za potpisivanje privatni, ovo spremište certifikata mora također imati kopiju certifikata Lokalnog izdavača certifikata (CA) koji je izdao certifikat za potpisivanje. U ovom scenariju, oba certifikata su se eksportirala u datoteku i ta datoteka je prenešena na svaki krajnji iSeries sistem.

Da importirate ove certifikate u *SIGNATUREVERIFICATION spremište, slijedite ove korake:
1. U navigacijskom okviru DCM-a kliknite **Izbor spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za otvaranje.
2. Kad se prikaže stranica Spremište certifikata i Lozinka, unesite lozinku koju ste specificirali za spremište certifikata kad ste ga kreirali i kliknite **Nastavak**.
3. Nakon osvježenja navigacijskog okvira izaberite **Upravljanje certifikatima** da se prikaže popis zadataka.
4. Iz popisa zadataka izaberite **Import certifikata**.
5. Izaberite **Izdavač certifikata (CA)** kao tip certifikata i kliknite **Nastavak**.

   Bilješka: Morate importirati certifikat Lokalnog CA prije importiranja privatnog certifikata za provjeru potpisa; inače postupak importiranja za certifikat provjere potpisa neće uspjeti.
6. Navedite potpuno kvalificirano ime staze i datoteke za datoteku certifikata CA i kliknite **Nastavak**. Prikazuje se poruka koja ili potvrđuje da je postupak importiranja uspio ili informira o greški ako postupak nije uspio.
7. Ponovno izaberite zadatak **Import certifikata**.
8. Izaberite **Provjera potpisa** kao tip certifikata za import i kliknite **Nastavak**.
9. Navedite potpuno kvalificirano ime staze i datoteke za certifikat provjere potpisa i kliknite **Nastavak**. Prikazuje se poruka koja ili potvrđuje da je postupak importiranja uspio ili informira o greški ako postupak nije uspio.

iSeries sistem može sada provjeravati potpise na objektima, koji su bili kreirani s odgovarajućim certifikatom potpisa, kad vraćate potpisane objekte.

Koncepti potpisivanja objekta

Prije nego što počnete upotrebljavati sposobnosti iSeries potpisivanja objekata i provjere potpisa možda ćete htjeti pregledati neke od ovih koncepata:

Digitalni potpisi
Naučite što su digitalni potpisi i koju zaštitu pružaju.

Potpisivi objekti
Naučite koje iSeries objekte možete potpisivati i o opcijama potpisa objekata naredbe (*CMD).

Obrada potpisivanja objekta
Naučite kako postupak potpisivanja objekta radi i koje parametre možete postaviti za obradu.

Obrada provjere potpisa
Naučite kako postupak provjere potpisivanja objekta radi i koje parametre možete postaviti za obradu.

| **Provjera integriteta funkcije provjere koda**
| Naučite kako možete provjeriti integritet funkcije provjere koda koju koristite za provjeru integriteta vašeg
| iSeries sistema.

Digitalni potpisi

OS/400 pruža podršku za upotrebu digitalnih certifikata za digitalno ″potpisivanje″ objekata. Digitalni potpis na objektu se kreira u šifriranom obliku i sličan je osobnom potpisu na pisanom dokumentu. Digitalni potpis pruža dokaz porijekla objekta i sredstvo za provjeru cjelovitosti objekta. Vlasnik digitalnog certifikata ″potpisuje″ objekt pomoću privatnog ključa certifikata. Primatelj objekta upotrebljava odgovarajući javni ključ certifikata za dešifriranje potpisa, čime se provjerava cjelovitost potpisanog objekta i provjerava pošiljatelja kao izvor.

Podrška za potpisivanje objekta povećava tradicionalne iSeries poslužiteljske alate za kontrolu tko može mijenjati objekte. Tradicionalne kontrole ne mogu zaštititi objekt od neovlaštene promjene dok je objekt u tranzitu kroz Internet ili drugu nepouzdanu mrežu. Budući da možete otkriti da li su sadržaji objekta promijenjeni od kad su potpisani, možete lakše odrediti da li je objekt kojeg dobivate u ovakvim slučajevima pouzdan.

Digitalni potpis je šifrirani matematički zbroj podataka u objektu. Objekt i njegovi sadržaji nisu pomoću digitalnog potpisa šifrirani i učinjeni privatnim; međutim, sam zbroj je šifriran da se spriječe neovlaštene promjene na njemu. Svatko tko se želi uvjeriti da objekt nije bio promijenjen u tranzitu i da objekt dolazi iz prihvatljivog i legitimnog izvora, može upotrijebiti javni ključ certifikata za potpisivanje da provjeri originalni digitalni potpis. Ako se potpis više ne podudara podaci su možda promijenjeni. U takvom slučaju primatelj može izbjeći upotrebu objekta i umjesto toga kontaktirati potpisnika da dobije drugu kopiju potpisanog objekta.

Potpis na objektu predstavlja sistem koji je potpisao objekt a ne određenog korisnika na tom sistemu (iako korisnik mora imati odgovarajuće ovlaštenje za korištenje certifikata za potpisivanje objekata).

Ako odlučite da upotreba digitalnog potpisa odgovara vašim potrebama i politikama sigurnosti, trebate provjeriti da li koristiti javne certifikate ili izdavati lokalne certifikate. Ako želite objekte distribuirati javnim korisnicima, razmotrite upotrebu certifikata za potpis objekata od javnih dobro poznatih Izdavača certifikata (CA). Upotreba javnih certifikata osigurava da drugi mogu lako i jeftino provjeriti potpise koje stavljate na objekte koje im distribuirate. Ako, međutim, namjeravate distribuirati objekte samo u vašoj organizaciji, možda ćete više htjeti upotrebljavati Upravitelja digitalnih certifikata (DCM) za rad s vašim vlastitim Lokalnim CA za izdavanje certifikata za potpisivanje objekata. Upotreba privatnih certifikata od Lokalnog CA za potpisivanje objekata je jeftinija od kupovine certifikata od poznatog javnog CA.

Tipovi digitalnih potpisa

Počevši od V5R2, možete potpisivati objekte naredbi (*CMD); također možete izabrati jedan od dva tipa potpisa za objekte *CMD: potpise jezgre objekta ili potpise cijelog objekta.

- **Potpisi cijelog objekta**
  Ovaj tip potpisa sadrži sve osim nekoliko nebitnih bajtova objekta.
- **Potpisi jezgre objekta**
  Ovaj tip potpisa sadrži bitne bajtove *CMD objekta. Međutim, potpis ne sadrži one bajtove koji su podložni češćim promjenama. Ovaj tip potpisa omogućuje izvođenje nekih promjena na naredbi bez poništenja potpisa. Koje bajtove potpis jezgre objekta ne sadrži ovisi o specifičnim *CMD objektima. Na primjer potpisi jezgre ne sadrže defaulte parametara na *CMD objektima. Primjeri promjena koje neće poništiti potpis jezgre objekta uključuju:

– Promjena defaulta naredbe.
– Dodavanje programa za provjeru valjanosti naredbe koja ga nema.
– Promjena parametra Gdje je dozvoljeno izvoditi.
– Promjena parametra Dozvoli ograničene korisnike.

Da naučite više o tome koje iSeries objekte možete potpisati i koje bajtove *CMD objekata potpis jezgre objekta sadrži, pogledajte Potpisivi objekti.

Potpisivi objekti

Možete digitalno potpisivati raznolike tipove OS/400 objekata, bez obzira na metodu potpisivanja koju upotrebljavate. Možete potpisati svaki objekt (*STMF) kojeg pohranite u integrirani sistem datoteka, osim objekata koji su pohranjeni u knjižnici. Ako objekt ima pripojen Java program, taj program će se također potpisati. Možete potpisivati samo ove objekte u sistemu datoteka QSYS.LIB: programe (*PGM), pomoćne programe (*SRVPGM), module (*MODULE), SQL pakete (*SQLPKG), *FILE (samo spremanje datoteke) i naredbe (*CMD).

Da bi se objekt mogao potpisati, mora se nalaziti na lokalnom sistemu. Na primjer, ako radite s Windows 2000 poslužiteljem na Integriranom xSeries poslužitelju za iSeries, dostupan vam je QNTC sistem datoteka u integriranom sistemu datoteka. Direktoriji u ovom sistemu datoteka ne smatraju se lokalnim, jer sadrže datoteke koje posjeduje operativni sistem Windows 2000. Također ne možete potpisati prazne objekte ili objekte koji su kompilirani za izdanje prije V5R1.

Potpisi objekata naredbe (*CMD)

Kada potpišete *CMD objekte, možete izabrati jedan od dva tipa digitalnog potpisa koji ćete primijeniti na *CMD objekt. Možete izabrati potpisivanje cijelog objekta ili potpisivanje samo jezgre objekta. Kad izaberete potpisivanje cijelog objekta, potpis se primjenjuje na sve osim nekoliko nebitnih bajtova objekta. Potpis cijelog objekta uključuje stavke sadržane u potpisu jezgre objekta.

Kad izaberete potpisivanje samo jezgre objekta, bitni bajtovi se zaštićuju potpisom, dok se bajtovi podložni češćim promjenama ne potpisuju. Koji bajtovi su nepotpisani ovisi o objektu *CMD, ali se mogu uključiti bajtovi koji između ostalog određuju način u kojem je objekt važeći ili određuju gdje je dozvoljeno izvođenje objekta. Na primjer, potpisi jezgre ne sadrže default parametre na *CMD objektima. Ovaj tip potpisa omogućuje izvođenje nekih promjena na naredbi bez poništenja njenog potpisa. Primjeri promjena koje neće poništiti ove tipove potpisa uključuju:
- Promjena defaulta naredbe.
- Dodavanje programa za provjeru valjanosti naredbe koja ga nema.
- Promjena parametra Gdje je dozvoljeno izvođenje.
- Promjena parametra Dozvoli ograničene korisnike.

Sljedeća tablica točno opisuje koji su bajtovi u objektu *CMD uključeni kao dio potpisa jezgre objekta.

Sastav potpisa jezgre objekta na *CMD objektima

Dio objekta	Odnos s potpisom jezgre objekta
Defaulti naredbi promijenjeni s CHGCMDDFT	Nisu dio potpisa jezgre objekta
Program za obradu naredbe i knjižnice	Uvijek uključeno kao dio potpisa jezgre objekta
REXX izvorna datoteka i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
REXX izvorni član	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Okolina REXX naredbe i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Ime REXX izlaznog progama, knjižnica i izlazni kod	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta

Dio objekta	Odnos s potpisom jezgre objekta
Program za kontrolu valjanosti i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Način u kojem je važeće	Nisu dio potpisa jezgre objekta
Gdje se dozvoljava izvođenje	Nisu dio potpisa jezgre objekta
Dozvoli ograničene korisnike	Nisu dio potpisa jezgre objekta
Knjige pomoći	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Grupa panela pomoći i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Identifikator pomoći	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Indeks traženja pomoći i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Trenutna knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Knjižnica proizvoda	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Program za nadjačavanje prompta i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Tekst (opis)	Nije dio niti potpisa jezgre objekta niti potpisa cijelog objekta, jer se ne pohranjuje u objekt
Omogući grafičko korisničko sučelje (GUI)	Nisu dio potpisa jezgre objekta

Obrada potpisivanja objekta

Kad potpisujete objekte možete navesti sljedeće opcije za obradu potpisivanja objekta.

- **Obrada greške**
  Možete navesti koji tip obrade greške aplikacija koristi kada kreira potpise na više od jednog objekta. Možete navesti da aplikacija zaustavi potpisivanje objekata kad se desi greška ili da nastavi potpisivanje drugih objekata u obradi.
- **Duplikat potpisa objekta**
  Možete navesti kako aplikacija rukuje obradom potpisivanja kada aplikacija ponovno potpisuje objekt. Možete navesti da li ostaviti originalni potpis na mjestu ili zamijeniti originalni potpis s novim potpisom.
- **Objekti u poddirektorijima**
  Možete navesti kako aplikacija treba rukovati potpisivanjem objekata u poddirektorijima. Možete navesti da aplikacija pojedinačno potpisuje objekte u svakom poddirektoriju ili da aplikacija samo potpisuje one objekte u glavnom direktoriju zanemarujući sve poddirektorije.
- **Djelokrug potpisa objekta**
  Kad potpisujete objekte *CMD, možete navesti da li potpisati cijeli objekt ili potpisati samo jezgru objekta.

Obrada provjere potpisa

Možete navesti sljedeće opcije za obradu provjere potpisa.

- **Obrada greške**
  Možete navesti koji tip obrade greške aplikacija koristi kada provjerava potpise na više od jednog objekta. Možete navesti da aplikacija zaustavi provjeru potpisa kad se desi greška ili da nastavi provjeru potpisa drugih objekata u obradi.
- **Objekti u poddirektorijima**
  Možete navesti kako aplikacija treba rukovati provjerom potpisa objekata u poddirektorijima. Možete navesti da aplikacija pojedinačno provjerava objekte u svakom poddirektoriju ili da aplikacija provjerava samo potpise za one objekte u glavnom direktoriju zanemarujući sve poddirektorije.

- **Provjera potpisa jezgre u odnosu na provjeru cijelog objekta**
  Postoje sistemska pravila koja određuju kako sistem rukuje potpisima jezgre i cijelog objekta za vrijeme obrade provjere. Ta pravila su sljedeća:
  - Ako nema potpisa na objektu, postupak provjere obavještava da objekt nije potpisan i nastavlja provjeravati sve druge objekte u postupku.
  - Ako je objekt potpisao pouzdani izvor sistema (IBM), potpis se mora podudarati ili postupak provjere ne uspijeva. Ako se potpis podudara, postupak provjere se nastavlja. Potpis je šifrirani matematički zbroj podataka u objektu; prema tome, smatra se da se potpis podudara ako se podaci u objektu za vrijeme provjere podudaraju s podacima u objektu kad je bio potpisan.
  - Ako objekt ima potpise cijelih objekata koji su pouzdani (na osnovi certifikata sadržanog u *SIGNATUREVERIFICATION spremištu certifikata), najmanje jedan od tih potpisa mora se podudarati ili postupak provjere ne uspijeva. Ako se najmanje jedan potpis cijelog objekta podudara, postupak provjere se nastavlja.
  - Ako objekt ima bilo koji potpis jezgre objekta koji je pouzdan, najmanje jedan od njih se mora podudarati s certifikatom *SIGNATUREVERIFICATION spremišta certifikata ili postupak provjere ne uspijeva. Ako se najmanje jedan potpis jezgre objekta podudara, postupak provjere se nastavlja.

Funkcija provjere integriteta provjeravatelja koda

Počevši od V5R2, OS/400 se isporučuje s funkcijom za provjeru koda koju koristite za provjeru integriteta potpisanih objekata na vašem sistemu, uključujući sav kod operativnog sistema koji IBM isporučuje i potpisuje za vaš iSeries sistem. Sada u V5R3, možete koristiti novi API za provjeru integriteta same funkcije za provjeru koda kao i ključnih objekata operativnog sistema.

API Provjera sistema (QydoCheckSystem) sadrži provjeru integriteta OS/400 sistema. Ovaj API možete koristiti za provjeru programa (*PGM) i pomoćnih programa (*SRVPGM) i izabranih objekata naredbi (*CMD) u QSYS knjižnici. Dodatno, API Provjera sistema testira naredbu Vraćanje objekta (RSTOBJ), naredbu Vraćanje knjižnice (RSTLIB), naredbu Provjera integriteta objekta (CHKOBJITG) i API Provjera objekta. Ovaj test osigurava da ove naredbe i API izvještavaju o greškama provjere potpisa kada je to prikladno. Na primjer, kada objekt koji je dao sistem nije potpisan ili sadrži nevažeći potpis.

API Provjera sistema šalje poruke pogreške o neuspjelim provjerama i ostalim pogreškama ili neuspjelim provjerama u dnevnik posla. Međutim, također možete navesti jednu ili dvije dodatne metode prijave pogreške, ovisno o tome kako ste postavili sljedeće opcije:

- Ako je sistemska vrijednost QAUDLVL postavljena u *AUDFAIL, tada API Provjera sistema generira slogove revizije za prijavu bilo kojeg neuspjeha i pogreške koje pronađu naredbe Vraćanje objekta (RSTOBJ), Vraćanje knjižnice (RSTLIB) i Provjera integriteta objekta (CHKOBJITG).
- Ako korisnik navede da API Provjera sistema koristi datoteku rezultata u integriranom sistemu datoteka, tada API kreira datoteku, ako ona ne postoji ili API dodaje datoteku u izvještaj o greškama ili neuspjehu koji API pronađe.

Da naučite više o tome kako koristiti API Provjera sistema za provjeru integriteta vašeg sistema pogledajte Funkcija provjere integriteta provjeritelja koda.

Preduvjeti potpisivanja objekata i provjere potpisa

Sposobnosti potpisivanja OS/400 objekta i provjere potpisa opskrbljuju vas s dodatnim snažnim sredstvom kontrole objekata na iSeries poslužitelju. Da iskoristite prednosti ovih sposobnosti, morate zadovoljiti preduvjete za njihovu upotrebu.

Preduvjeti potpisivanja objekata

Postoje brojne metode koje možete upotrebljavati za potpisivanje objekata, ovisno o vašim poslovnim i sigurnosnim potrebama.

- Možete koristiti Upravitelja digitalnih certifikata (DCM).
- Možete pisati program koji koristi API Potpisivanje objekta.

- Možete upotrebljavati funkciju Središnjeg Upravljanja iSeries Navigatora za potpisivanje objekata kad ih pakirate za distribuciju krajnjim iSeries sistemima.

Koju metodu ćete izabrati za potpisivanje objekata ovisi o vašim poslovnim i sigurnosnim potrebama. Bez obzira na metodu koju planirate upotrebljavati za potpisivanje objekata, morate osigurati da su zadovoljeni određeni uvjeti:
- Morate zadovoljiti preduvjete za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).
  - Morate upotrijebiti DCM za kreiranje *OBJECTSIGNING spremišta certifikata. Ovo spremište certifikata kreirate bilo kao dio postupka kreiranja Lokalnog izdavača certifikata (CA) ili kao dio postupka upravljanja certifikatima potpisivanja objekata od javnog Internet CA.
  - *OBJECTSIGNING spremište certifikata mora sadržavati najmanje jedan certifikat, bilo onaj koji ste kreirali pomoću Lokalnog CA ili onaj koji ste dobili od javnog Internet CA.
  - Morate upotrijebiti DCM za kreiranje najmanje jedne definicije aplikacije potpisivanja objekta za upotrebu za potpisivanje objekata.
  - Morate upotrijebiti DCM za dodjelu određenog certifikata definiciji aplikacije za potpisivanje objekta.
- iSeries korisnički profil koji potpisuje objekte mora imati posebno ovlaštenje *ALLOBJ. iSeries korisnički profil koji kreira *SIGNATUREVERIFICATION spremište certifikata mora imati posebna ovlaštenja *SECADM i *ALLOBJ.

Preduvjeti provjere potpisa

Postoje brojne metode koje možete upotrebljavati za provjeru potpisa na objektima:
- Možete koristiti Upravitelja digitalnih certifikata (DCM).
- Možete napisati program koji upotrebljava API Provjera objekta (QYDOVFYO).
- Možete upotrijebiti jednu od brojnih naredbi, kao naredbu Provjera cjelovitosti objekta (CHKOBJITG).

Koju metodu ćete izabrati za provjeru potpisa ovisi o vašim poslovnim i sigurnosnim potrebama. Bez obzira na metodu koju planirate upotrebljavati, morate osigurati da su zadovoljeni određeni preduvjeti:
- Morate zadovoljiti preduvjete za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).
- Morate kreirati *SIGNATUREVERIFICATION spremište certifikata. Ovo spremište certifikata možete kreirati na jedan od dva načina, ovisno o vašim potrebama. Možete ga kreirati pomoću Upravitelja digitalnih certifikata (DCM) za upravljanje certifikatima provjera potpisa . Ili ako upotrebljavate javni certifikat za potpisivanje objekata, ovo spremište možete kreirati pisanjem programa koji upotrebljava API za Dodavanje provjeritelja (QYDOADDV).

  Bilješka: API Dodavanje provjeritelja kreira spremište certifikata s default lozinkom. Za ponovno postavljanje ove default lozinke na jednu po vašem izboru trebate upotrijebiti DCM da se spriječi neovlašteni pristup spremištu certifikata.
- *SIGNATUREVERIFICATION spremište certifikata mora sadržavati kopiju certifikata koji je potpisao objekte. Ovaj certifikat možete dodati spremištu certifikata na jedan od dva načina. Možete upotrijebiti DCM na sistemu koji potpisuje za eksportiranje certifikata u datoteku i zatim upotrijebiti DCM na ciljnom sistemu za provjeru za import certifikata u spremište certifikata *SIGNATUREVERIFICATION. Ili ako upotrebljavate javni certifikat za potpisivanje objekata, možete dodati certifikat spremištu certifikata ciljnog sistema za provjeru, pisanjem programa koji upotrebljava API za Dodavanje provjeritelja.
- *SIGNATUREVERIFICATION spremište certifikata mora sadržavati kopiju certifikata CA koji je izdao certifikat koji je potpisao objekte. Ako koristite javni certifikat za potpisivanje objekata, spremište certifikata na ciljnom sistemu provjere može već imati kopiju potrebnog CA certifikata. Ako, međutim, upotrebljavate certifikat kojeg je izdao Lokalni CA za potpisivanje objekata, morate upotrijebiti DCM za dodavanje kopije certifikata Lokalnog CA u spremište certifikata na ciljnom sistemu za provjeru.

  Bilješka: Radi sigurnosnih razloga API Dodavanje provjeritelja ne dopušta umetanje certifikata od Izdavača certifikata (CA) u *SIGNATUREVERIFICATION spremište certifikata. Kad dodajete CA certifikat spremištu certifikata, sistem smatra da je CA pouzdan izvor certifikata. Radi toga, sistem postupa sa certifikatom kojeg je izdao CA kao s onim čije je porijeklo od pouzdanog izvora. Prema tome, možete upotrebljavati API za kreiranje instalacijskog izlaznog programa da umetnete CA certifikat u memoriju certifikata. Morate upotrijebiti Upravitelja digitalnih certifikata za dodavanje CA certifikata u spremište

da se osigurate da netko mora posebno i ručno kontrolirati kojim CA-ovima vjeruje sistem. Ako to napravite onemogućiti ćete da sistem može importirati certifikate iz izvora koje administrator nije svjesno naveo kao povjerljive.

Ako upotrebljavate certifikat kojeg je izdao Lokalni CA za potpisivanje objekata, morate upotrebljavati DCM na iSeries host poslužitelju Lokalnog CA za eksportiranje kopije certifikata Lokalnog CA u datoteku. Možete zatim upotrijebiti DCM na ciljnom iSeries poslužitelju provjere za importiranje certifikata Lokalnog CA u *SIGNATUREVERIFICATION spremište certifikata. Da spriječite moguću grešku, morate importirati certifikat Lokalnog CA u ovo spremište certifikata prije upotrebe API-ja Dodavanje provjeritelja za dodavanje certifikata za provjeru potpisa. Radi toga, ako upotrebljavate certifikat kojeg je izdao Lokalni CA, možda ćete ustanoviti da je lakše upotrebljavati DCM za importiranje CA certifikata i certifikata provjere u spremište certifikata.

Ako želite spriječiti da bilo tko koristi ovaj API za dodavanje certifikata za provjeru u vaše *SIGNATUREVERIFICATION spremište certifikata bez vašeg znanja, morate razmotriti onemogućavanje ovog API-ja na vašem sistemu. To možete učiniti upotrebljavajući Sistemske servisne alate (SST) da ne dopustite promjene sistemskih vrijednosti koje se odnose na sigurnost. .

- iSeries korisnički profil koji provjerava potpise mora imati posebno ovlaštenje *AUDIT. iSeries korisnički profil koji kreira *SIGNATUREVERIFICATION spremište certifikata ili mijenja njegovu lozinku mora imati posebna ovlaštenja *SECADM i *ALLOBJ.

Upravljanje potpisanim objektima

Počevši od V5R1, IBM je započeo potpisivanje OS/400 licencnih progama i PTF-ova kao način službenog označavanja da je operacijski sistem IBM porijekla i kao sredstvo otkrivanja neovlaštenih promjena koje su se desile na objektima sistema. Također, poslovni partneri i drugi prodavači mogu potpisivati aplikacije koje kupujete. Radi toga, čak i ako sami ne potpisujete objekte, trebate razumjeti kako se radi s potpisanim objektima i kako ti potpisani objekti utječu na rutinske sistemske administrativne zadatke.

Potpisani objekti primarno utječu na zadatke sigurnosnog kopiranja i obnavljanja, naročito kako spremate i obnavljate objekte na sistemu.

Sistemske vrijednosti i naredbe koje utječu na potpisane objekte
Naučite o sistemskim vrijednostima i naredbama koje možete upotrebljavati za upravljanje potpisanim objektima ili koje utječu na potpisane objekte kad ih izvodite.

Razmatranja o spremanju i vraćanju potpisanih objekata
Naučite kako potpisani objekti utječu na način obavljanja zadataka za spremanje i vraćanje za sistem.

Naredbe kontrolora koda za osiguranje cjelovitosti potpisa
Naučite o upotrebi naredbi za provjeru potpisa objekata za određivanje integriteta objekta.

Provjera integriteta funkcije provjere koda
Naučite kako možete provjeriti integritet funkcije provjere koda koju koristite za provjeru integriteta OS/400 sistema.

Sistemske vrijednosti i naredbe koje utječu na potpisane objekte

Da djelotvorno upravljate potpisanim objektima, trebate razumjeti kako sistemske vrijednosti i naredbe utječu na potpisane objekte. **Provjera potpisa objekata za vrijeme vraćanja sistemske vrijednosti** (QVFYOBJRST) određuje kako određene naredbe vraćanja utječu na potpisane objekte i kako sistem rukuje potpisanim objektima za vrijeme operacija vraćanja. Ne postoje CL naredbe koje su isključivo oblikovane za rad s potpisanim objektima na iSeries sistemu. Međutim, postoje brojne uobičajene CL naredbe koje upotrebljavate za upravljanje potpisanim objektima (ili za upravljanje infrastrukturnim objektima koje potpisivanje objekta čine mogućim). Druge naredbe mogu nepovoljno utjecati na potpisane objekte na sistemu uklanjanjem potpisa s objekata, čime uništavaju zaštitu koju pruža potpis.

Sistemske vrijednosti koje utječu na potpisane objekte

Provjera potpisa objekta za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST), član kategorije vraćanja od OS/400 sistemskih vrijednosti, određuje kako naredbe utječu na potpisane objekte na sistemu. Ta sistemska vrijednost, koja je dostupna preko iSeries Navigatora, kontrolira kako sistem rukuje s provjerom potpisa za vrijeme operacije vraćanja. Postavka koju upotrebljavate za ovu sistemsku vrijednost, u spoju s postavkama dviju drugih sistemskih vrijednosti utječe na operacije vraćanja za sistem. Ovisno o postavci koju izaberete za ovu vrijednost, ona može dopustiti ili ne dopustiti vraćanje objekata na osnovi njihovih stanja potpisa. (Na primjer, da li je objekt nepotpisan, da li ima nevažeći potpis, da li ga je potpisao pouzdani izvor itd.) Defaultna postavka za ovu sistemsku vrijednost dopušta vraćanje nepotpisanih objekata, ali osigurava da se potpisani objekti mogu vratiti samo ako imaju važeći potpis. Sistem definira objekt kao potpisan samo ako objekt ima potpis u kojeg sistem ima povjerenja; sistem zanemaruje druge ″nepouzdane″ potpise na objektu i postupa s tim objektima kao da su nepotpisani.

Postoji nekoliko vrijednosti koje možete upotrebljavati za sistemsku vrijednost QVFYOBJRST, u rasponu od zanemarivanja svih potpisa do zahtijevanja važećih potpisa za sve objekte koje vraća sistem. Ova sistemska vrijednost utječe samo na izvedbene objekte koji se vraćaju, kao programi (*PGM), naredbe (*CMD), pomoćni programi (*SRVPGM), SQL paketi (*SQLPKG) i moduli (*MODULE). Također se odnosi na objekte datoteke toka (*STMF) koji imaju pridružene Java programe koje je kreirala naredba Kreiranje Java programa (CRTJVAPGM). Ne odnosi se na datoteke spremanja (*SAV) ili datoteke integriranog sistema datoteka.

Da naučite još o upotrebi ovih i drugih sistemskih vrijednosti, pogledajte Pronalazač sistemske vrijednosti u Informacijskom Centru.

CL naredbe koje utječu na potpisane objekte

Postoji nekoliko CL naredbi koje dopuštaju rad s potpisanim objektima ili utječu na potpisane objekte na iSeries poslužitelju. Možete upotrebljavati raznolike naredbe za gledanje informacija o potpisu za objekte, za provjeru potpisa na objektima i spremanje i vraćanje objekta sigurnosti potrebnih za provjeru potpisa. Osim toga, postoji grupa naredbi koje, kad se izvode, mogu ukloniti potpise s objekata i poništiti sigurnost koju pruža potpis.

Naredbe za gledanje informacija o potpisu za objekt

- Naredba Prikaz opisa objekta (DSPOBJD).
  Ova naredba pokazuje imena i atribute navedenih objekata u navedenoj knjižnici ili u knjižnicama s popisa knjižnica niti. Možete upotrijebiti ovu naredbu da odredite da li je objekt potpisan i da pogledate informacije o potpisu.
- Naredbe integriranog sistema datoteka Prikaz veza objekta (DSPLNK) i Rad s vezama objekta (WRKLNK).
  Možete upotrebljavati bilo koju od ovih naredbi za prikaz informacija o potpisu za neki objekt u integriranom sistemu datoteka.

Naredbe za provjeru potpisa objekata

- Naredba Provjera cjelovitosti objekta (CHKOBJITG).
  Ova naredba omogućuje da odredite da li je na objektima sistema povrijeđena cjelovitost. Ovu naredbu možete upotrebljavati za provjeru potpisa na način vrlo sličan upotrebi kontrola virusa za određivanje kad je virus oštetio datoteke ili druge objekte na sistemu. Da naučite još o upotrebi ove naredbe s potpisanim i potpisivim objektima, pogledajte Naredbe kontrolora koda za osiguranje cjelovitosti potpisa .
- Naredba Provjera opcije proizvoda (CHKPRDOPT).
  Ova naredba izvještava o razlici između ispravne strukture i stvarne strukture softverskog proizvoda. Na primjer, naredba izvještava o greški ako je objekt izbrisan iz instaliranog proizvoda. Možete koristiti CHKSIG parametar za navođenje kako će naredba rukovati i izvještavati o mogućim problemima potpisa proizvoda. Da naučite još o upotrebi ove naredbe s potpisanim i potpisivim objektima, pogledajte Naredbe kontrolora koda za osiguranje cjelovitosti potpisa .
- Naredba Spremanje licencnog programa (SAVLICPGM).
  Ova naredba sprema kopiju objekata koji čine licencni program. Ona sprema licencni program u obliku kojeg može vratiti naredba Vraćanje licencnog progama (RSTLICPGM). Možete koristiti CHKSIG parametar za navođenje kako će naredba rukovati i izvještavati o mogućim problemima potpisa proizvoda. Da naučite još o upotrebi ove naredbe s potpisanim i potpisivim objektima, pogledajte Naredbe kontrolora koda za osiguranje cjelovitosti potpisa .

- Naredba Vraćanje (RST).
  Ova naredba vraća kopiju jednog ili više objekata koji se mogu koristiti u integriranom sistemu datoteka. Ova naredba također omogućuje vraćanje spremišta certifikata i njihovih sadržaja na sistemu. Međutim, ne možete upotrijebiti ovu naredbu za vraćanje *SIGNATUREVERIFICATION spremišta certifikata. Kako naredba vraćanja rukuje s potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).
- Naredba Vraćanje knjižnice (RSTLIB).
  Ova naredba vraća jednu knjižnicu ili grupu knjižnica koju je spremila naredba Spremanje knjižnice (SAVLIB). Naredba RSTLIB vraća cijelu knjižnicu, koja uključuje opis knjižnice, opise objekata i sadržaje objekata u knjižnici. Kako ta naredba rukuje s potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).
- Naredba Vraćanje licencnog programa (RSTLICPGM).
  Ova naredba učitava ili vraća licencni program, za početnu instalaciju ili za instalaciju novog izdanja. Kako ta naredba rukuje s potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).
- Naredba Vraćanje objekta (RSTOBJ).
  Ova naredba vraća jedan ili više objekata u pojedinačnu knjižnicu, koji su bili spremljeni na disketu, vrpcu, optičku memoriju ili datoteku pomoću pojedinačne naredbe. Kako ta naredba rukuje s potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).

Naredbe za spremanje i vraćanje spremišta certifikata

- Naredba Spremanje (SAV).
  Ova naredba omogućuje spremanje kopije jednog ili više objekata koji se mogu upotrebljavati u integriranom sistemu datoteka, uključujući spremišta certifikata. Međutim, ne možete upotrijebiti ovu naredbu za spremanje *SIGNATUREVERIFICATION spremišta certifikata.
- Naredba Spremanje sigurnosnih podataka (SAVSECDTA).
  Ova naredba omogućuje spremanje svih sigurnosnih informacija ne tražeći da sistem bude u ograničenom stanju. Upotreba ove naredbe omogućuje spremanje *SIGNATUREVERIFICATION spremišta certifikata i certifikata koje ono sadržava. Ova naredba ne sprema nikakvo drugo spremište certifikata.
- Naredba Spremanje sistema (SAVSYS).
  Ova naredba omogućuje spremanje kopije licencnog internog koda i knjižnice QSYS u formatu kompatibilnom s instalacijom iSeries poslužitelja. Ona ne sprema objekte iz nikakve druge knjižnice. Osim toga, ona omogućuje spremanje objekata sigurnosti i konfiguracije koje također možete spremiti pomoću naredbi SAVSECDTA i SAVCFG. Upotreba ove naredbe omogućuje spremanje *SIGNATUREVERIFICATION spremišta certifikata i certifikata koje ono sadržava.
- Naredba Vraćanje (RST).
  Ova naredba omogućuje vraćanje spremišta certifikata i njihovih sadržaja na sistem. Međutim, ne možete upotrijebiti ovu naredbu za vraćanje *SIGNATUREVERIFICATION spremišta certifikata.
- Naredba Vraćanje korisničkih profila (RSTUSRPRF).
  Ova naredba omogućuje vraćanje osnovnih dijelova korisničkog profila ili skupa korisničkih profila koji su spremljeni naredbom Spremanje sistema (SAVSYS) ili Spremanje sigurnosnih podataka (SAVSECDTA). Ovu naredbu možete upotrijebiti za vraćanje *SIGNATUREVERIFICATION spremišta certifikata i skrivenih lozinki za ovu i sve druge memorije certifikata. Možete vratiti *SIGNATUREVERIFICATION spremište certifikata bez vraćanja informacija o korisničkom profilu, navođenjem *DCM kao vrijednosti za parametar SECDTA i *NONE za parametar USRPRF. Da upotrijebite ovu naredbu za vraćanje informacija o korisničkom profilu i spremištu certifikata i njihovih lozinki, navedite *ALL za parametar USRPRF.

Naredbe koje mogu ukloniti ili izgubiti potpise s objekata

Kada koristite sljedeće naredbe na potpisanom objektu, to možete učiniti na način koji može ukloniti ili izgubiti potpis s objekta. Uklanjanje potpisa može uzrokovati probleme s objektima. U najboljem slučaju, nećete više moći provjeravati pouzdanost izvora objekta i nećete moći provjeravati potpis da otkrijete promjene na objektu. Koristite ove naredbe samo za one potpisane objekte koje ste kreirali (za razliku od potpisanih objekata koje dobijete od ostalih

poput IBM-a ili prodavača). Ako ste zabrinuti da je naredba uklonila ili izgubila neki objektov potpis, možete upotrijebiti naredbu Prikaz opisa objekta (DSPOBJD) da vidite da li je potpis još uvijek tamo i da li ga treba ponovno potpisati.

Bilješka: Da provjerite da li je naredba Spremanja izgubila objektov potpis, morate vratiti objekt u knjižnicu različitu od one iz koje ste ga spremili (na primjer, QTEMP). Zatim možete upotrijebiti naredbu DSPOBJD da odredite da li je objekt na mediju za spremanje izgubio svoj potpis.

- Naredba Promjenu programa (CHGPGM).
  Ova naredba mijenja atribute programa ne tražeći da ga rekompajlirate. Također, možete upotrebljavati ovu naredbu za prisilno ponovno kreiranje programa čak ako su navedeni atributi isti kao i trenutni atributi.
- Naredba Promjena servisnog programa (CHGSRVPGM).
  Ova naredba mijenja atribute servisnog programa ne tražeći da ga rekompajlirate. Također, možete upotrebljavati ovu naredbu za prisilno ponovno kreiranje servisnog programa čak ako su navedeni atributi isti kao i trenutni atributi.
- Naredba Brisanje datoteke za spremanje (CLRSAVF).
  Ova naredba briše sadržaje datoteke za spremanje; ona briše sve postojeće slogove iz datoteke za spremanje i smanjuje veličinu memorije koju koristi ova datoteka.
- Naredba Spremanje (SAV).
  Ova naredba sprema kopiju jednog ili više objekata koji se mogu upotrebljavati u integriranom sistemu datoteka. — Kada koristite ovu naredbu, možete izgubiti potpise objekata naredbe (*CMD) na mediju za spremanje ako navedete vrijednost raniju od V5R2M0 za TGTRLS parametar. Gubitak potpisa događa se, jer se objekti naredbe ne mogu potpisati u izdanju starijem od V5R2.
- Naredba Spremanje knjižnice (SAVLIB).
  Ova naredba omogućuje spremanje kopije jedne ili više knjižnica. Kada koristite ovu naredbu, možete izgubiti potpise objekata naredbe (*CMD) na mediju za spremanje ako navedete vrijednost raniju od V5R2M0 za TGTRLS parametar. Gubitak potpisa se dešava, jer objekti naredbi ne mogu biti potpisani u izdanjima ranijim od V5R2.
- Naredba Spremanje objekta (SAVOBJ).
  Ova naredba sprema kopiju pojedinačnog objekta ili grupe objekata smještenih u istoj knjižnici. Kada koristite ovu naredbu, možete izgubiti potpise objekata naredbe (*CMD) na mediju za spremanje ako navedete vrijednost raniju od V5R2M0 za TGTRLS parametar. Gubitak potpisa se dešava, jer se objekti naredbi ne mogu potpisati u izdanjima ranijim od V5R2.

Razmatranja o spremanju i vraćanju potpisanih objekata

Postoji nekoliko sistemskih vrijednosti koje mogu utjecati na operacije vraćanja za iSeries poslužitelj. Samo jedna od ovih sistemskih vrijednosti **provjera potpisa objekta u toku vraćanja (QVFYOBJRST)** sistemska vrijednost, određuje kako sistem rukuje potpisanim objektima kada ih vraća. Postavka koju izaberete za ovu sistemsku vrijednost dopušta određivanje kako postupak vraćanja rukuje s provjerom objekata bez potpisa ili s nevažećim potpisima.

Neke naredbe za spremanje i vraćanje utječu na potpisane objekte ili određuju kako sistem rukuje s potpisanim i nepotpisanim objektima za vrijeme operacija spremanja i vraćanja. Morate biti svjesni ovih naredbi i njihovog utjecaja na potpisane objekte tako da možete bolje upravljati vašim istemom i izbjegavati potencijalne probleme koji se mogu desiti.

Ove naredbe mogu provjeravati potpise na objektima za vrijeme operacija spremanja i vraćanja:
- Naredba Spremanje licencnog programa (SAVLICPGM).
- Naredba Vraćanje (RST).
- Naredba Vraćanje knjižnice (RSTLIB).
- Naredba Vraćanje licencnog programa (RSTLICPGM).
- Naredba Vraćanje objekta (RSTOBJ).

Ove naredbe omogućuju spremanje i vraćanje spremišta certifikata; spremišta certifikata su sigurnosno osjetljivi objekti koji sadrže certifikate koje upotrebljavate za potpisivanje objekata i provjeru potpisa:
- Naredba Spremanje (SAV).
- Naredba Spremanje sigurnosnih podataka (SAVSECDTA).

- Naredba Spremanje sistema (SAVSYS).
- Naredba Vraćanje (RST).
- Naredba Vraćanje korisničkih profila (RSTUSRPRF).

Neke naredbe za spremanje, ovisno o vrijednostima parametara koje upotrebljavate, mogu izgubiti potpis s objekta na mediju za spremanje, poništavajući time sigurnost koju pruža potpis. Na primjer, *bilo koja* operacija spremanja koja se odnosi na objekt naredbe (*CMD) s ciljnim izdanjem starijim od V5R2M0 uzrokuje da se naredba spremi bez potpisa. Uklanjanje potpisa može uzrokovati probleme s objektima. U najboljem slučaju, nećete više moći provjeravati pouzdanost izvora objekta i nećete moći provjeravati potpis da otkrijete promjene na objektu. Koristite ove naredbe samo za one potpisane objekte koje ste kreirali (za razliku od potpisanih objekata koje dobijete od ostalih poput IBM-a ili prodavača).

Bilješka: Da provjerite da li je naredba Spremanja izgubila objektov potpis, morate vratiti objekt u knjižnicu različitu od one iz koje ste ga spremili (na primjer, QTEMP). Zatim možete upotrijebiti naredbu DSPOBJD da odredite da li je objekt na mediju za spremanje izgubio svoj potpis.

Trebate biti svjesni ove mogućnosti za sljedeće specifične naredbe spremanja, kao i za naredbe spremanja općenito:
- Naredba Spremanje (SAV).
- Naredba Spremanje knjižnice (SAVLIB).
- Naredba Spremanje objekta (SAVOBJ).

Dodatne informacije o tome kako ove naredbe utječu na potpisane objekte i potpise objekata za vrijeme operacija spremanja i vraćanja, možete naći u Sistemske vrijednosti i naredbe koje utječu na potpisane objekte.

Naredbe kontrolora koda za osiguranje cjelovitosti potpisa

Možete upotrebljavati Upravitelja digitalnih certifikata (DCM) ili API-je za provjeru potpisa na objektima. Možete također upotrebljavati nekoliko naredbi za provjeru potpisa. Upotreba ovih naredbi omogućuje provjeru potpisa na način vrlo sličan upotrebi kontrolora virusa za određivanje kad je virus oštetio datoteke ili druge objekte na sistemu. Većina potpisa se provjerava kad se objekt vraća ili instalira na sistem, na primjer upotrebom naredbe RSTLIB.

Možete izabrati jednu od tri naredbi za provjeru potpisa na objektima koji već postoje na sistemu. Među njima je naredba Provjera cjelovitosti objekta (CHKOBJITG) oblikovana posebno za provjeru potpisa objekata. Provjeru potpisa za svaku od ovih naredbi kontrolira parametar CHKSIG. Taj parametar omogućuje provjeru potpisa kod svih tipova objekata koji se mogu potpisati, zanemarivanje svih potpisa ili provjeru samo onih objekata koji imaju potpise. Ova zadnja opcija je defaultna vrijednost za parametar.

Naredba Provjera integriteta objekta (CHKOBJITG)

Naredba Provjera cjelovitosti objekta (CHKOBJITG) omogućuje da se odredi da li je cjelovitost objekata na sistemu povrijeđena. Ovu naredbu možete upotrebljavati za provjeru povrede cjelovitosti za objekte koji posjeduju određene korisničke profile, objekte koji se podudaraju s određenim imenom staze ili sve objekte na sistemu. Unos u dnevnik za povredu cjelovitosti se dešava kad se zadovolji jedan od ovih uvjeta:
- Naredba, program, objekt modula ili atributi knjižnica su se promijenili.
- Određeno je da je digitalni potpis na objektu nevažeći. Potpis je šifrirani matematički zbroj podataka u objektu; prema tome, smatra se da se potpis podudara i da je važeći ako se podaci u objektu za vrijeme provjere podudaraju s podacima u objektu kad je bio potpisan. Određivanje nevažećeg potpisa se bazira na usporedbi šifriranog matematičkog zbroja koji se kreira kad se objekt potpisuje i šifriranog matematičkog zbroja napravljenog za vrijeme provjere potpisa. U postupku provjere potpisa uspoređuju se te dvije vrijednosti zbroja. Ako te vrijednosti nisu iste, sadržaji objekta su se promijenili od kad je objekt potpisan i smatra se da je potpis nevažeći.
- Objekt ima neispravan atribut domene za ovaj tip objekta.
-

Ako naredba otkrije kršenje integriteta za neki objekt, dodaje ime objekta, ime knjižnice (ili ime staze), tip objekta, vlasnika objekta i tip neuspjeha u datoteku dnevnika baze podataka. Naredba također kreira unos dnevnika u određenim drugim slučajevima, iako ti slučajevi ne predstavljaju povrede cjelovitosti. Na primjer, naredba kreira unos dnevnika za

objekte koji se mogu potpisati, ali nemaju digitalni potpis, objekte koje ne može provjeriti i objekte u formatu koji zahtijeva promjenu kako bi se mogao koristiti na trenutnoj implementaciji sistema (konverzija IMPI u RISC).

Vrijednost parametra CHKSIG kontrolira kako naredba rukuje s digitalnim potpisima na objektima. Možete navesti jednu od tri vrijednosti za ovaj parametar:
- *SIGNED – Kad navedete ovu vrijednost, naredba provjerava objekte s digitalnim potpisima. Naredba kreira unos dnevnika za svaki objekt s potpisom koji nije važeći. To je defaultna vrijednost.
- *ALL – Kad navedete ovu vrijednost, naredba provjerava sve potpisive objekte da odredi da li imaju potpis. Naredba kreira unos dnevnika za svaki potpisivi objekt koji nema potpis i za svaki objekt s potpisom koji nije važeći.
- *NONE – Kad navedete ovu vrijednost, naredba ne provjerava digitalne potpise na objektima.

Naredba Provjera opcije proizvoda (CHKPRDOPT)

Naredba Provjera opcije proizvoda (CHKPRDOPT) izvještava o razlici između ispravne strukture i stvarne strukture softverskog proizvoda. Na primjer, naredba izvještava o greški ako je objekt izbrisan iz instaliranog proizvoda.

Vrijednost parametra CHKSIG kontrolira kako naredba rukuje s digitalnim potpisima na objektima. Možete navesti jednu od tri vrijednosti za ovaj parametar:
- *SIGNED – Kad navedete ovu vrijednost, naredba provjerava objekte s digitalnim potpisima. Naredba provjerava potpise na svakom potpisanom objektu. Ako naredba odluči da potpis na objektu nije važeći, naredba šalje poruku dnevniku posla i identificira proizvod da je u stanju greške. To je defaultna vrijednost.
- *ALL – Kad navedete ovu vrijednost, naredba provjerava sve potpisive objekte da odredi da li imaju potpis i provjerava potpise na tim objektima. Naredba šalje poruku dnevniku posla o svakom potpisivom objektu koji nema potpis; međutim, naredba ne identificira proizvod da je s greškom. Ako naredba odluči da potpis na objektu nije važeći, šalje poruku dnevniku posla i identificira proizvod da je u stanju greške.
- *NONE – Kad navedete ovu vrijednost, naredba ne provjerava digitalne potpise na objektima proizvoda.

Naredba Spremanje licencnog programa (SAVLICPGM)

Naredba Spremanje licencnog progama (SAVLICPGM) omogućuje spremanje kopije objekata koji čine licencni program. Ona sprema licencni program u obliku kojeg može vratiti naredba Vraćanje licencnog progama (RSTLICPGM).

Vrijednost parametra CHKSIG kontrolira kako naredba rukuje s digitalnim potpisima na objektima. Možete navesti jednu od tri vrijednosti za ovaj parametar:
- *SIGNED – Kad navedete ovu vrijednost, naredba provjerava objekte s digitalnim potpisima. Naredba provjerava potpise na svakom potpisanom objektu, ali ne provjerava nepotpisane objekte. Ako naredba odluči da potpis na objektu nije važeći, šalje poruku dnevniku posla o identificiranju objekta i spremanje neće uspjeti. To je defaultna vrijednost.
- *ALL – Kad navedete ovu vrijednost, naredba provjerava sve potpisive objekte da odredi da li imaju potpis i provjerava potpise na tim objektima. Naredba šalje poruke dnevniku posla za bilo koji objekt koji se može potpisati, a koji nema potpis, međutim proces spremanja se ne završava. Ako naredba odluči da potpis na objektu nije važeći, šalje poruku dnevniku posla i spremanje neće uspjeti.
- *NONE – Kad navedete ovu vrijednost, naredba ne provjerava digitalne potpise na objektima proizvoda.

Provjera integriteta funkcije provjere koda

Za upotrebu nove funkcije za provjeru integriteta koda za provjeru integriteta vašeg iSeries sistema, morate imati *AUDIT specijalno ovlaštenje.

Da provjerite funkciju provjerivača koda, pokrenite API Provjera sistema (QydoCheckSystem) da odredite da li se bilo koji ključni operativni objekt sistema promijenio od kada je potpisan. Kada izvodite API on provjerava ključne objekte sistema, uključujući programe i servisne programe i izabrane objekte naredbi (*CMD) u knjižnici QSYS kao što slijedi:

1. Provjerava sve objekte programa (*PGM) na koje unos sistema tablica pokazivača pokazuje.
2. Provjerava sve objekte servisnih programa (*SRVPGM) u knjižnici QSYS i provjerava integritet API-ja Provjera objekta.

3. Izvodi API Provjera objekta (QydoVerifyObject) za provjeru integriteta naredbe Vraćanje objekta (RSTOBJ), naredbe Vraćanje knjižnice (RSTLIB) i naredbe Provjera integriteta objekta (CHKOBJITG).
4. Koristi naredbe RSTOBJ i RSTLIB na posebnoj datoteci za spremanje (*SAV) da se osigura da se greške ispravno prijavljuju. Nedostatak poruka greške ili netočna poruka greške pokazuje na mogući problem.
5. Kreira naredbeni (*CMD) objekt koji je oblikovan da ne uspije da bi ispravno provjerio.
6. Izvodi naredbu CHKOBJITG i API Provjera objekta na tom posebnom objektu naredbe da se osigura da naredba CHKOBJITG i API Provjera objekta ispravno prijavljuju greške. Nedostatak poruka greške ili netočna poruka greške pokazuje na mogući problem.

Da naučite kako protumačiti poruku greške koju generira funkcija provjere integriteta koda, pogledajte Tumačenje poruka greške provjere provjeritelja koda.

Rješavanje problema potpisanih objekata

Kada potpišete objekte i radite s potpisanim objektima, možete naići na greške koje vas spriječavaju da postignete svoje zadatke i ciljeve. Mnoge od čestih grešaka ili problema na koje možete naići spadaju u ove kategorije:

Rješavanje problema grešaka potpisivanja objekta
Ove informacije koristite da naučite o zajedničkim problemima na koje možete naići kada provjeravate digitalne potpise na objektima i da vidite kako ih možete ispraviti.

Rješavanje problema grešaka provjere potpisa
Koristite ove informacije da se upoznate s uobičajenim problemima spremišta certifikata i baze podataka ključeva, na koje možete naići i kako bi ih mogli ispraviti.

Poruke grešaka provjere interpretiranja provjeritelja koda
Koristite ove informacije da naučite koje poruke vraća funkcija provjere integriteta provjeravatelja koda i kako te poruke koristiti da osigurate da je funkcija provjere koda neoštećena, kao i moguća rješenja ako poruka pokazuje da su funkcija ili ključni objekti operativnog sistema oštećeni.

Rješavanje problema grešaka potpisivanja objekta

Koristite sljedeću tablicu da pronađete informacije za pomoć pri rješavanju nekih najčešćih problema na koje možete naići kada potpisujete objekte:

Problem	Moguće rješenje
Kod upotrebe API-ja za Potpisivanje objekata za potpis objekta s ciljnim izdanjem V4R5 ili ranijim, postupak potpisivanja ne uspijeva i objekt se ne potpisuje (poruka o greški CPFB721).	iSeries nema podršku potpisivanja objekata prije V5R1. Za one objekte koji vraćaju poruku greške CPFB721, morate ponovo kreirati te programe s ciljnim izdanjem V5R1 ili kasnijim da ih možete potpisati.

Rješavanje problema grešaka provjere potpisa

Koristite sljedeću tablicu da pronađete informacije za pomoć pri rješavanju nekih najčešćih problema na koje možete naići kada provjeravate digitalne potpise na objektima:

Problem	Moguće rješenje
Postupak vraćanja ne uspijeva za objekte bez potpisa.	Ako nedostatak potpisa nije zabrinjavajući, provjerite je li QVFYOBJRST sistemska vrijednost postavljena na 5. Vrijednost od 5 navodi da nepotpisani objekti ne mogu biti vraćeni. Promijenite vrijednost na 3 i pokušajte vraćanje ponovno.

Problem	Moguće rješenje
Postupak vraćanja ne uspijeva za objekte s potpisima.	To se može desiti ako se *SIGNATUREVERIFICATION spremište certifikata prenijelo u sistem i DCM se nije upotrijebio za promjenu njegove lozinke. U takvom slučaju, certifikati, koje sadrži spremište se ne mogu upotrijebiti za provjeru potpisa na objektima za vrijeme postupka vraćanja. Upotrijebite DCM za promjenu lozinke za spremište certifikata. Ako ne znate lozinku, trebat ćete izbrisati spremište certifikata, ponovno ga kreirati i koristiti DCM da promijenite lozinku.
Kod vraćanja ili instaliranja proizvoda, dobivate grešku, jer se potpis ne uspijeva provjeriti.	Kad se potpis objekta ne uspije ispravno provjeriti, greška može značiti da se objekt promijenio od kad je bio potpisan. Ako je integritet objekta u pitanju, nemojte mijenjati QVFYOBJRST vrijednost sistema ili izvesti druge akcije koje mogu dozvoliti da se objekt vrati. To može dovesti do zaobilaženja sigurnosti koju daje provjera potpisa i omogućiti da se štetni objekt nađe na vašem sistemu. Umjesto toga morate se obratiti onome tko je potpisao objekt da odredite odgovarajuće akcije koje trebate poduzeti da riješite problem.

Poruke grešaka provjere interpretiranja provjeritelja koda

Sljedeća tablica dale popis poruka koje funkcija provjere provjeritelja koda generira u toku obrade. Ova tablica nije opsežan popis svih poruka koje možete primiti. Umjesto toga, tablica popisuje poruke za koje je najvjerojatnije da će pokazati da je provjera provjeritelja koda u potpunosti uspjela ili da je naišla na ozbiljni problem. Pogledajte dokumentaciju za API Provjera sistema (QydoCheckSystem) za detaljni popis poruka grešaka.

Također, broj poruka koje je generirala funkcija provjere provjeritelja koda dok obrađuje, su informacijske poruke i nisu ovdje ispisane. Da naučite više o tome kako radi postupak provjere provjeritelja koda, pogledajte Provjera integriteta funkcije provjeritelja koda.

Tablica 1. Poruka greške provjere provjeritelja koda

Poruka greške	Mogući problem i rješenje
CPFB729	Ukazuje da se postupak provjere provjeritelja koda nije uspio završiti kao što je očekivano. Ovaj neuspjeh može biti uzrokovan mnoštvom problema. Pogledajte dnevnik posla za detaljnije poruke greške da odredite pravu prirodu neuspjeha i mogućeg uzroka. Ako odredite da ključni objekt operativnog sistema nije prošao provjeru integriteta, taj neuspjeh pokazuje da je objekt promijenjen od kada je potpisan prilikom slanja operativnog sistema. Možda ćete trebati ponovno instalirati operativni sistem da provjerite integritet sistema.
Prilikom pregledavanja dnevnika posla, vidite poruke poput CPFB723, CPD37A1 ili CPD37A0 za ove specifične objekte: • Program (*PGM) objekti: – QYDONOSIG u knjižnici QTEMP – QYDOBADSIG u knjižnici QTEMP • Naredba (*CMD) objekti: – QYDOBADSIG u knjižnici QTEMP – SIGNOFF u knjižnici QTEMP	Pokazuje da posebni skup objekata koje koristi funkcija provjere provjeritelja koda za testiranje integriteta nije uspio prema očekivanjima. Ovaj neuspjeh pokazuje da naredba RSTOBJ, naredba RSTLIB, naredba CHKOBJITG i API Provjera objekta ispravno prijavljuju pogreške. Daljnje akcije nisu potrebne.
CPFB723 za bilo koji drugi objekt osim onih prethodno ispisanih u ovoj tablici.	Pokazuje da se potpis na ključnom objektu operativnog sistema nije uspio provjeriti. Ova naredba može pokazivati da je objekt promijenjen od kada je potpisan prilikom isporuke operativnog sistema. Možda ćete trebati ponovno instalirati operativni sistem da provjerite integritet sistema.

Tablica 1. Poruka greške provjere provjeritelja koda (nastavak)

Poruka greške	Mogući problem i rješenje
CPFB722 za bilo koji drugi objekt osim onih prethodno ispisanih u ovoj tablici.	Pokazuje da objekt operativnog sustava nema potpis kada je potpis očekivan. Taj nedostatak potpisa može značiti da je objekt promijenjen od kada je potpisan prilikom isporuke operativnog sustava. Možda ćete trebati ponovno instalirati operativni sustav da provjerite integritet sistema.
CPF72A za bilo koji drugi objekt osim onih prethodno ispisanih u ovoj tablici.	Pokazuje da ključni objekt operativnog sustava nije prošao provjeru integriteta. Ova naredba može pokazivati da je objekt promijenjen od kada je potpisan prilikom isporuke operativnog sustava. Možda ćete trebati ponovno instalirati operativni sustav da provjerite integritet sistema.

Ako ikada trebate ponovno instalirati kod koji provjerava integritet funkcije provjeravatelja koda, morate ga dobiti iz poznatog, dobrog izvora. Na primjer, možete učitati medij instalacije koji ste koristili za instaliranje trenutnog izdanja. Da vratite funkciju provjere integriteta koda slijedite ove korake na nekom OS/400 promptu za naredbe:

1. Izvedite naredbu QSYS/DLTPGM QSYS/QYDOCHKS. Ova naredba briše API Provjera sistema (OPM, QYDOCHKS; ILE, QydoCheckSystem).
2. Izvedite naredbu QSYS/DLTSRVPGM QSYS/QYDOCHK1. Ova naredba briše servisni program provjeritelja koda s API-jem Provjera sistema (OPM, QYDOCHKS; ILE, QydoCheckSystem).
3. Izvedite naredbu QSYS/DLTF QSYS/QYDOCHKF. Ova naredba briše datoteku spremanja koja sadrži objekte koje funkcija provjeritelja koda koristi za testiranje za loše potpise i bez potpisa.
4. Izvedite naredbu QSYS/RSTOBJ OBJ(QYDOCHK*) SAVLIB(QSYS) DEV(OPT01) OBJTYPE(*ALL) OPTFILE('Q5722SS1/Q5200M_/Q00/Q90'). Ova naredba vraća sve potrebne objekte funkcije provjere provjeritelja koda iz učitanog medija za instalaciju.

Povezane informacije za potpisivanje objekta i provjeru potpisa

Potpisivanje objekta i provjera potpisa su relativno nove sigurnosne tehnologije. Evo malog popisa drugih resursa koje možete smatrati korisnim ako ste zainteresirani za šire poznavanje ovih tehnologija i kako one rade:

- **Web stranica VeriSign Help Desk**
  Web stranica VeriSign pruža proširenu knjižnicu na poglavljima digitalnih certifikata kao potpisivanje objekta, kao i brojne druge Internet predmete sigurnosti.

- **IBM eServer iSeries Sigurnost ožičene mreže:OS/400 V5R1 DCM i Kriptografička proširenja SG24-6168**
  Ova IBM Redbook fokusira se na V5R1 proširenja sigurnosti mreže. Redbook sadrži mnoštvo tema uključujući kako koristiti iSeries sposobnosti prijave objekta, Upravitelja digitalnih certifikata (DSM) i tako dalje.

Izjava o odricanju od koda

Ovaj dokument sadrži primjere programiranja.

IBM vam dodjeljuje neekskluzivnu licencu autorskog prava za upotrebu svih primjera koda iz kojih možete generirati slične funkcije oblikovane za vaše specifične potrebe.

Sve primjere koda IBM dostavlja samo za ilustrativne svrhe. Ovi primjeri nisu bili temeljito testirani u svim uvjetima. IBM, prema tome, ne može jamčiti, ili potvrditi pouzdanost, upotrebljivost ili funkcionalnost tih programa.

Svi ovdje sadržani programi se isporučuju ″KAKVI JESU″, bez bilo kakvih jamstava. Neizravna jamstva o nekršenju, lakoj prodaji i sposobnosti za određenu svrhu se izričito poriču.

Dodatak. Napomene

Ove informacije su razvijene za proizvode i usluge koji se nude u SAD.

IBM možda ne nudi proizvode, usluge ili funkcije raspravljane u ovom dokumentu u drugim zemljama. Posavjetujte se sa svojim lokalnim IBM predstavnikom za informacije o proizvodima i uslugama koji su trenutno dostupni u vašem području. Bilo koje upućivanje na neki IBM proizvod, program ili uslugu nema namjeru tvrditi da se samo taj IBM proizvod, program ili usluga mogu koristiti. Bilo koji funkcionalno ekvivalentan proizvod, program ili usluga koji ne narušava nijedno IBM pravo na intelektualno vlasništvo, se može koristiti kao zamjena. Međutim, na korisniku je odgovornost da procijeni i verificira operacije bilo kojeg ne-IBM proizvoda, programa ili usluge.

IBM može imati patente ili prijavljene patente koji su još u postupku, a koji pokrivaju predmet o kojem se govori u ovom dokumentu. Posjedovanje ovog dokumenta vam ne daje nikakve licence na ove patente. Možete poslati upit za licence, u pismenom obliku, na:

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

Za upite o licenci koji se odnose na dvo-bajtne (DBCS) informacije, kontaktirajte IBM Odjel za intelektualno vlasništvo u vašoj zemlji ili pošaljite upite u pisanom obliku na:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106-0032, Japan

Sljedeći odlomak se ne primjenjuje na Ujedinjeno Kraljevstvo ili bilo koju drugu zemlju gdje su takve izjave nekonzistentne s lokalnim zakonima: INTERNATIONAL BUSINESS MACHINES CORPORATION DAJE OVU PUBLIKACIJU “KAKVA JE ”, BEZ IKAKVIH JAMSTAVA, BILO IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, UKLJUČENA JAMSTVA O NE-POVREĐIVANJU, PROĐI NA TRŽIŠTU ILI SPOSOBNOSTI ZA ODREĐENU SVRHU. Neke zemlje ne dozvoljavaju odricanje od izravnih ili posrednih jamstava u određenim transakcijama, zbog toga, se ova izjava možda ne odnosi na vas.

Ove informacije mogu sadržavati tehničke netočnosti ili tipografske pogreške. Povremeno se rade promjene na ovim informacijama; te promjene bit će uključene u nova izdanja ove publikacije. IBM može raditi poboljšanja i/ili promjene u proizvodu(ima) i/ili programu/ima opisanim u ovoj publikaciji, bilo kad, bez prethodne obavijesti.

Bilo koje upućivanje u ovim informacijama na ne-IBM Web stranice, služi samo kao pomoć i ni na kakav način ne služi za promicanje tih Web stranica. Materijali na tim Web stranicama nisu dio materijala za ovaj IBM proizvod i upotreba tih Web stranica je na vaš osobni rizik.

| IBM može koristiti ili distribuirati sve informacije koje vi dobavite, na bilo koji način za koji smatra da je prikladan i
| bez ikakvih obveza prema vama.

Vlasnici licence za ovaj program, koji žele imati informacije o njemu u svrhu omogućavanja: (i) izmjene informacija između neovisno kreiranih programa i drugih programa (uključujući i ovaj) i (ii) uzajamne upotrebe informacija koje su bile izmijenjene, trebaju kontaktirati:

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

Rochester, MN 55901
U.S.A.

Takve informacije mogu biti dostupne, uz odgovarajuće termine i uvjete, uključujući u nekim slučajevima i plaćanje pristojbe.

Licencni program koji je opisan u ovim informacijama i sav licencni materijal dostupan za njega, IBM osigurava pod uvjetima IBM Korisničkog ugovora, IBM međunarodnog ugovora o programskim licencama, IBM Ugovora o licenci za strojni kod ili sličnog ugovora između nas.

Svi podaci o izvedbi koji su ovdje sadržani su utvrđeni u kontroliranoj okolini. Stoga, rezultati koji su dobavljeni u drugim operacijskim okolinama mogu značajno varirati. Neka mjerenja su možda bila izvedena na sistemima na razvojnoj razini i ne postoji nikakvo jamstvo da će ta mjerenja biti ista na općenito dostupnim sistemima. Osim toga, neka mjerenja su možda bila procijenjena pomoću ekstrapolacije. Stvarni rezultati se mogu razlikovati. Korisnici ovog dokumenta bi trebali verificirati primjenljive podatke za njihovo određeno okruženje.

Informacije koje se tiču ne-IBM proizvoda su dobivene od dobavljača tih proizvoda, njihovih objavljenih najava ili drugih dostupnih javnih izvora. IBM nije testirao te proizvode i ne može potvrditi točnost performansi, kompatibilnosti ili bilo koji drugi zahtjev vezan uz ne-IBM proizvod. Pitanja o sposobnostima ne-IBM proizvoda bi trebala biti adresirana na dobavljače tih proizvoda.

Sve izjave u vezi budućih IBM namjera ili smjernica su podložne promjeni ili povlačenju bez prethodne obavijesti, te predstavljaju samo ciljeve i namjere.

Ove informacije sadrže primjere podataka i izvještaja koji se koriste u svakodnevnim operacijama. Radi što boljeg objašnjenja, ti primjeri uključuju imena pojedinaca, poduzeća, brandova i proizvoda. Sva ta imena su izmišljena i bilo koja sličnost s imenima i adresama koja se koriste u stvarnom poslovnom okruženju, je u potpunosti slučajna.

LICENCA ZAŠTIĆENA AUTORSKIM PRAVOM:

Ove informacije sadržavaju uzorke aplikacijskih programa na izvornom jeziku, koji objašnjavaju tehnike programiranja na raznolikim operacijskim platformama. Možete kopirati, modificirati i distribuirati te primjere programa u bilo kojem obliku bez plaćanja IBM-u, u cilju razvoja, korištenja, marketinga ili distribucije, u skladu sa sučeljem aplikativnog programiranja za operativnu platformu za koju su pisani primjeri programa. Ovi primjeri nisu bili temeljito testirani u svim uvjetima. IBM zbog toga ne može jamčiti ili potvrditi pouzdanost, upotrebljivost ili funkcioniranje tih programa.

PODLOŽNO BILO KOJIM ZAKONSKIM JAMSTVIMA KOJA SE NE MOGU ISKLJUČITI, IBM, NJEGOVI RAZVIJAČI PROGRAMA I DOBAVLJAČI NE DAJU JAMSTVA ILI UVJETE, IZRIČITE ILI POSREDNE, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA ILI UVJETE ZA PROĐU NA TRŽIŠTU, SPOSOBNOSTI ZA ODREĐENU SVRHU I NE-KRŠENJE, VEZANO UZ PROGRAM ILI TEHNIČKU PODRŠKU, UKOLIKO POSTOJE.

IBM, RAZVIJAČI PROGRAMA ILI DOBAVLJAČI NISU NITI U KOJIM UVJETIMA ODGOVORNI ZA BILO ŠTO OD SLJEDEĆEG, ČAK I AKO SU OBAVIJEŠTENI O TAKVOJ MOGUĆNOSTI:

1. GUBITAK ILI OŠTEĆENJE PODATAKA;
2. POSEBNE, SLUČAJNE ILI NEIZRAVNE ŠTETE, ILI EKONOMSKE POSLJEDIČNE ŠTETE; ILI
3. GUBITAK PROFITA, POSLA, ZARADE, DOBROG GLASA ILI UŠTEDE.

NEKA ZAKONODAVSTVA NE DOZVOLJAVAJU ISKLJUČENJE ILI OGRANIČENJE SLUČAJNIH ILI POSLJEDIČNIH ŠTETA, TAKO DA SE GORNJA OGRANIČENJA MOŽDA NE ODNOSE NA VAS.

Svaka kopija ili bilo koji dio ovih uzoraka programa ili bilo kojeg izvedenog rada mora sadržavati napomenu o autorskom pravu u obliku:

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

Ako gledate nepostojanu kopiju ovih informacija, možda se neće pojaviti boje i fotografije.

Zaštitni znaci

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

e(logo)server
eServer
IBM
iSeries
Operating System/400
OS/400
Redbooks
xSeries
400

Microsoft, Windows, Windows NT i Windows logo su zaštitni znaci Microsoft Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

Java i svi Java zasnovani zaštitni znaci su zaštitni znaci Microsystems, Inc. u Sjedinjenim Državama, drugim zemljama ili oboje.

Ostala imena poduzeća, proizvoda i usluga mogu biti zaštitni znaci ili servisne oznake drugih.

Termini i uvjeti za spuštanje i ispis publikacija

Dozvole za upotrebu informacija koje ste izabrali za spuštanje dodjeljuju se prema sljedećim terminima i uvjetima i nakon vašeg prihvaćanja.

Osobna upotreba: Možete reproducirati ove informacije za vašu osobnu, nekomercijalnu upotrebu, uz osiguranje da su sve napomene o vlasništvu sačuvane. Ne smijete distribuirati, prikazivati ili raditi izvedena djela iz ovih informacija, ili bilo kojeg njihovog dijela, bez izričite suglasnosti IBM-a.

Komercijalna upotreba: Možete reproducirati, distribuirati i prikazivati ove informacije isključivo unutar vašeg poduzeća, uz osiguranje da su sve napomene o vlasništvu sačuvane. Ne smijete izrađivati izvedene radove iz ovih informacija ili reproducirati, distribuirati ili prikazivati ove informacije ili bilo koji njihov dio izvan vašeg poduzeća, bez izričite dozvole IBM-a.

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

IBM rezervira pravo da bilo kad, po vlastitom nahođenju, povuče ovdje dodijeljene dozvole, ako je upotreba informacija štetna za njegove interese ili je ustanovljeno od strane IBM-a da gornje upute nisu bile ispravno slijeđene.

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune usklađenosti sa svim primjenjivim zakonima i propisima, uključujući sve zakone i propise o izvozu Sjedinjenih Država. IBM NE DAJE NIKAKVA JAMSTVA NA SADRŽAJ OVIH INFORMACIJA. INFORMACIJE SE DAJU ″KAKVE JESU″ I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA PROĐE NA TRŽIŠTU, NEKRŠENJA I PRIKLADNOSTI ZA ODREĐENU SVRHU.

Na sve materijale IBM Corporation ima autorsko pravo.

Spuštanjem i ispisom informacija s ove stranice, naznačili ste da se slažete s ovim terminima i uvjetima.

Informacije o odricanju od koda

IBM vam dodjeljuje neekskluzivnu licencu autorskog prava za upotrebu svih primjera programskog koda iz kojih možete generirati slične funkcije prilagođene vašim specifičnim potrebama.

PODLOŽNO BILO KOJIM ZAKONSKIM JAMSTVIMA KOJA SE NE MOGU ISKLJUČITI, IBM, NJEGOVI RAZVIJAČI PROGRAMA I DOBAVLJAČI NE DAJU JAMSTVA ILI UVJETE, IZRIČITE ILI POSREDNE, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA ILI UVJETE ZA PROĐU NA TRŽIŠTU, SPOSOBNOSTI ZA ODREĐENU SVRHU I NE-KRŠENJE, VEZANO UZ PROGRAM ILI TEHNIČKU PODRŠKU, UKOLIKO POSTOJE.

IBM, RAZVIJAČI PROGRAMA ILI DOBAVLJAČI NISU NITI U KOJIM UVJETIMA ODGOVORNI ZA BILO ŠTO OD SLJEDEĆEG, ČAK I AKO SU OBAVIJEŠTENI O TAKVOJ MOGUĆNOSTI:

1. GUBITAK ILI OŠTEĆENJE PODATAKA;
2. POSEBNE, SLUČAJNE ILI NEIZRAVNE ŠTETE, ILI EKONOMSKE POSLJEDIČNE ŠTETE; ILI
3. GUBITAK PROFITA, POSLA, ZARADE, DOBROG GLASA ILI UŠTEDE.

NEKA ZAKONODAVSTVA NE DOZVOLJAVAJU ISKLJUČENJE ILI OGRANIČENJE SLUČAJNIH ILI POSLJEDIČNIH ŠTETA, TAKO DA SE GORNJA OGRANIČENJA MOŽDA NE ODNOSE NA VAS.

Tiskano u Hrvatskoj