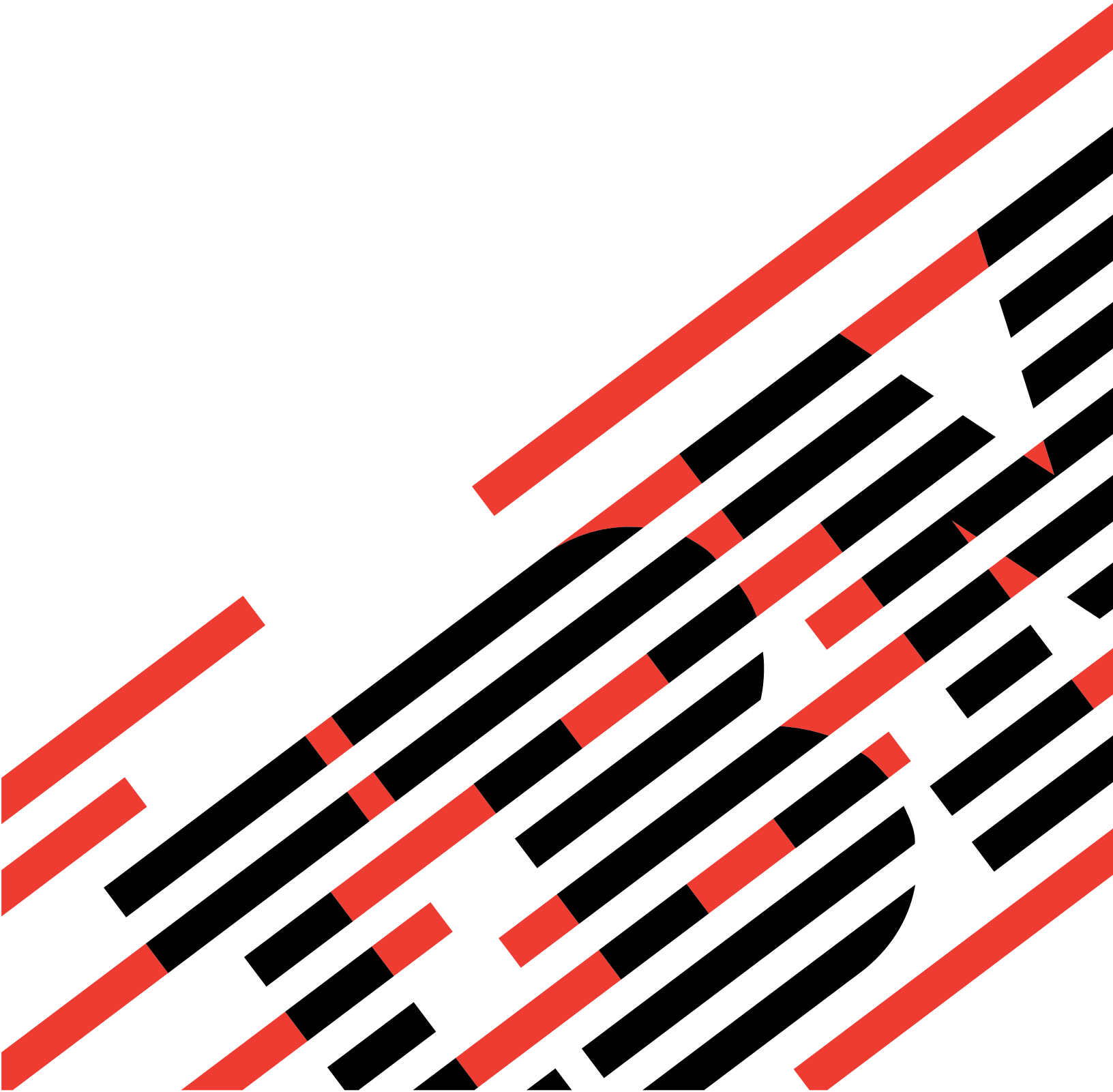
IBM

eserver

iSeries

Potpisivanje objekta i provjera potpisa



IBM

@server

iSeries

Potpisivanje objekta i provjera potpisa

Sadržaj

Potpisivanje objekta i provjera potpisa

Potpisivanje objekta i provjera potpisa su sposobnosti sigurnosti koje možete primjeniti za provjeru cjelovitosti raznolikih iSeries objekata. privatni ključ digitalnog certifikata upotrebljavate za potpis objekta i certifikat (koji sadrži odgovarajući javni ključ) upotrebljavate za provjeru digitalnog potpisa. Digitalni potpis osigurava cjelovitost vremena i sadržaja objekta kojeg potpisujete. Potpis je priznati dokaz vjerodostojnosti i ovlaštenja. Može se upotrebljavati za dokaz porijekla i otkrivanje neovlaštenja. 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 primjeniti iSeries potpisivanje objekta i provjeru potpisa pomoću:

- API-jeva za potpis objekata i programatsku provjeru potpisa na objektima.
- Upravitelja digitalnih certifikata za potpis objekata i za gledanje ili provjeru potpisa objekata.
- iSeries Navigator Management Central za potpis objekata kao dio distributivnog paketa za korištenje drugih sistema.
- CL naredbi, 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 u V5R2
Pročitajte ove informacije da se upoznate sa 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 potpisivanja objekata
Upotrijebite ove informacije da pregledate scenarije koji objašnjavaju neke tipične situacije za upotrebu sposobnosti iSeries potpisivanja objekata i provjeru potpisa. Svaki scenario također pruža zadatke za konfiguraciju koje morate obaviti da primjenite scenario prema opisu.

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

Preduvjeti za potpisivanje objekta i provjeru potpisa
Upotrijebite ove informacije da naučite još o preduvjetima konfiguracija kao i o drugim razmatranjima planiranja za potpisivanje objekata i provjeravanje potpisa.

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

Rješavanje problema kod potpisivanja objekata i provjere potpisa.
Koristite se ovim informacijama da naučite kako riješiti probleme i greške koje se mogu susresti pri potpisivanju objekata i provjeri potpisa.

Srodne informacije za potpisivanje objekata i provjeru potpisa
Koristite se ovim informacijama da nađete veze na druge resurse da naučite još o potpisivanju objekata i provjeri potpisa objekata.

Što je novo u V5R2

Sposobnosti potpisivanja objekata i provjere potpisa za iSeries su prvo uvedene u V5R1. Međutim, postoje neke nove funkcije i poboljšanja koja su na raspolaganju u V5R2.

Nove ili poboljšane funkcije za potpisivanje objekta i provjeru potpisa uključuju:

- Funkcija potpisivanja objekta Središnjeg Upravljanja **iSeries Navigatora**
  Sada možete upotrebljavati čarobnjaka Definicije proizvoda Središnjeg Upravljanja za potpis objekata koje pakirate za distribuciju iSeries krajnjim sistemima.
- **Potpis objekata naredbe (*CMD)**
  Sada možete potpisivati objekte naredbi (*CMD) . Možete izabrati da li potpisati cijeli objekt *CMD ili potpisati samo glavne komponente *CMD objekta.
- **Novi API-jevi za potpisivanje i provjere.**
  Možete upotrebljavati tri nova API-ja da programatski iskoristite poboljšanja za OS/400 sposobnosti potpisivanja i provjera:
  - API za potpis Međuspremnika QYDOSGNB, QydoSignBuffer)
    Ovaj API dopušta lokalnom sistemu da digitalno potpiše međuspremnik da time potvrdi da je pouzdan. Nakon potpisivanja međuspremnika, sistem vraća digitalni potpis pozivatelju API-ja. Na primjer, možete upotrijebiti ovaj API za potpis dijela XML datoteke i pohranjivanje potpisa u drugi dio XML datoteke. Ili možete učitati slogove datoteke baze podataka u međuspremnik i upotrijebiti API da ih potpišete.
  - Provjera međuspremnika QYDOVFYB, QydoVerifyBuffer)
    Ovaj API dopušta lokalnom sistemu provjeru digitalnog potpisa na prethodno potpisanom međuspremniku.
  - API za dodavanje provjeriteljaQYDOADDV, QydoAddVerifier)
    Ovaj API dodaje certifikat sistemskoj memoriji certifikata *SIGNATUREVERIFICATION. Sistem može zatim upotrijebiti dodani certifikat za provjeru potpisa na objektima koji su kreirali certifikat. Provjeravanjem potpisa dopušta se sistemu provjera cjelovitosti potpisanih objekata da provjeri da se objekti nisu promijenili od kada su bili potpisani. Ako ne postoji memorija certifikata, ovaj API ju kreira kad dodaje certifikate.

    Bilješka: Radi sigurnosnih razloga ovaj API ne dopušta umetanje certifikata Izdavača certifikata (CA) u memoriju certifikata *SIGNATUREVERIFICATION. Kad dodajete CA certifikat memoriji certifikata, sistem smatra da je CA pouzdani izvor certifikata. Radi toga, sistem postupa sa certifikatom, kojeg je izdao CA, kao sa 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 memoriji da se osigurate da netko mora određeno i ručno kontrolirati kojim CA-ovim vjeruje sistem. Na taj način se sprječava mogućnost da sistem može importirati certifikate sa izvora koje administrator nije svjesno naveo kao pouzdanim.

    Ako želite spriječiti bilo koga da upotrebljava ovaj API za dodavanje certifikata provjere memoriji certifikata *SIGNATUREVERIFICATION bez vašeg znanja, trebate razmisliti o onemogućavanju ovog API-ja na sistemu. To možete učiniti upotrebom Alata sistemskih usluga (SST) da ne dopustite promjene sistemskih vrijednosti koje se odnose na sigurnost. .

Ranije su informacije o svojstvima iSeries potpisivanja objekta i provjeri potpisa bili dostupni kao dio poglavlja Informacijskog Centra Upravljanja digitalnim certifikatima. Sada postoje dodatne metode koje možete upotrebljavati za potpis objekata i provjeru potpisa. Radi toga je na raspolaganju ovo novo poglavlje Informacijskog Centra da olakša upotrebu sposobnosti potpisivanja objekta i provjeru potpisa pružajući centralizirane informacije o upotrebi ovih sposobnosti. Ovo poglavlje pruža poboljšane i potpunije informacije, kao scenarije za pomoć u određivanju kad i kako upotrijebiti ove sposobnosti za nadopunu politike sigurnosti.

Nove ili poboljšane informacije za ovo poglavlje uključuju:

- Scenarije koje možete upotrebljavati za pomoć u određivanju kako najbolje iskoristiti sposobnosti potpisivanja objekta i provjere potpisa za nadopunu politike sigurnosti.
- Nove odlomke koji opisuju naredbe i sistemske vrijednosti koje možete upotrebljavati za upravljanje potpisanim objektima na sistemu.
- Nove odlomke koji opisuju planiranje i druge konceptualne informacije za potpisivanje objekata i provjere potpisa.

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

Ispis ovog poglavlja

Da pogledate ili učitate PDF verziju, izaberite Potpisivanje objekta i provjera potpisa (datoteka veličine 350 kb ili oko 44 stranica).

Da spremite PDF na radnu stanicu za gledanje ii ispisivanje:

1. Otvorite PDF u pretražitelju (kliknite vezu gore).
2. U izborniku pretražitelja kliknite **Datoteka**.
3. Kliknite **Spremi kao..**
4. Pomaknite se u direktorij u koji želite spremiti PDF.
5. Kliknite **Spremi**.

Ako trebate da Adobe Acrobat Reader pogleda ili ispiše PDF, možete učitati kopiju sa Adobe Web stranice (www.adobe.com/prodindex/acrobat/readstep.html) .

Scenariji potpisivanja objekata

iSeries poslužitelj pruža nekoliko različitih metoda za potpisivanje objekata i provjeru potpisa na objektima. Kako izabirete potpisati objekte i kako radite sa potpisanim objektima razlikuje se ovisno o poslu i potrebama sigurnosti i ciljevima. U nekim slučajevima možda trebate samo provjeriti potpise objekata na sistemu da se uvjerite da je cjelovitost objekta netaknuta. U drugim slučajevima, možda izaberete potpisati objekte koje distribuirate drugima. Potpisivajem objekata dopušta se drugima identificirati porijeklo objekata i provjeriti cjelovitost objekata.

Koju metodu izabrati za upotrebu ovisi o raznolikim faktorima. Scenariji u ovom poglavlju opisuju neke od uobičajenijih ciljeva potpisivanja objekta i provjere potpisa u tipično poslovnom kontekstu. Svaki scenario također opisuje sve preduvjete i zadatke koje morate obaviti da primjenite scenario 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:

Scenario: Koristite Upravitelja digitalnih certifikata za potpis objekata i provjeru potpisa
Ovaj scenario opisuje poduzeće koje želi potpisati povredive objekte aplikacije na svojem Web poslužitelju. Žele biti sposobni lakše odrediti kad postoje neovlaštene promjene na ovim objektima. Na osnovu potreba posla poduzeća i sigurnosnih ciljeva ovaj scenario opisuje kako upotrebljavati Upravitelja digitalnih certifikata (DCM) kao primarnu metodu za potpisivanje objekata i provjeravanje potpisa objekata.

Scenario: Koristite API-jeve za potpisivanje objekata i provjeru potpisa
Ovaj scenario opisuje poduzeće za razvoj aplikacija koje želi programatski potpisivati aplikacije koje prodaje. Oni žele biti sposobni uvjeriti svoje korisnike da su aplikacije došle od njihovog poduzeća i da

ih opskrbljuju sa sredstvom za otkrivanje neovlaštenih promjena na aplikacijama kad ih instaliraju. Na osnovi potreba posla poduzeća i sigurnosnih ciljeva ovaj scenario opisuje kako upotrebljavati Potpis API Objekta i API-js za dodavanje provjeritelja za potpisivanje objekata i omogućavanje potpisa objekata.

Scenario: Koristite Središnje Upravljanje za potpisivanje objekata.
Ovaj scenario opisuje poduzeće koje želi potpisivati objekte koje pakira i distribuira višestrukim iSeries poslužiteljima. Na osnovi potreba posla poduzeća i sigurnosnih ciljeva ovaj scenario opisuje kako upotrebljavati funkciju iSeries Navigatorovog Središnjeg Upravljanja za pakiranje i potpisivanje objekata koje oni distribuiraju drugim iSeries poslužiteljima.

Scenario: Koristite DCM za potpis objekata i provjeru potpisa

Situacija

Kao iSeries administrator za MyCo., Inc. odgovorni ste za upravljanje dvama iSeries poslužiteljima vašeg poduzeća. Jedan od tih iSeries poslužitelja pruža javnu Web stranicu za vaše poduzeće. Upotrebljavate interni proizvodni iSeries poslužitelj poduzeća za razvoj sadržaja te javnu Web stranicu i prenosite objekte datoteke i programa javnom Web poslužitelju nakon što ga ispitate.

Javni Web poslužitelj poduzeća pruža Web stranicu sa 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. Vi ste zabrinuti za povredivost cgi-bin programa koji pružaju te obrasce; znate da se mogu mijenjati. Prema tome, želite biti sposobni provjeriti cjelovitost tih objekata i otkriti kad su na njima izvršene neovlaštene promjene. Radi toga ste odlučili digitalno potpisivati ove objekte da postignete sigurnosni cilj.

Istraživali 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 malog broja iSeries poslužitelja i smatrate da nećete često potpisivati objekte, odlučili ste uotrebljavati Upravitelja digitalnih certifikata DCM) za obavljanje 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 te 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 scenario ima sljedeće prednosti:

- Potpisivanje objekata pruža sredstvo provjere integriteta povredivih objekata i lakše određivanje da li su objekti promijenjeni nakon što su bili potpisani. Ovim se mogu smanjiti neka rješavanja problema koje ćete vršiti u budućnosti za slјeđenje 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 povredive objekte, kao cgi-bin programe koji generiraju obrasce, na javnom iSeries poslužitelju poduzeća. Kao sistemski administrator kod MyCo, Inc., želite upotrebljavati Upravitelja digitalnih certifikata (DCM) za potpisivanje ovih objekata i provjeru potpisa na objektima.

Ciljevi ovog scenarija su sljedeći:

- Aplikacije poduzeća i drugi povredivi objekti na javnom Web poslužitelju iSeries B) moraju se potpisati sa certifikatom Lokalnog CA da se ograniče troškovi aplikacije potpisivanja.
- Sistemski administratori i drugi naimenovani 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 certifikata (CA) u svakoj poslužiteljevoj memoriji certifikata *SIGNATUREVERIFICATION.
- Provjerom potpisa na aplikacijama poduzeća i drugim objektima iSeries administratori i drugi mogu otkriti da li je sadržaj objekata promjenjen 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 scenario:

iSeries A

- iSeries A izvodi OS/400 verzija 5 izdanje 2 (V5R2).
- iSeries A je interni proizvodni poslužitelj poduzeća i razvojna platforma za javni iSeries Web poslužitelj (iSeries B).
- iSeries A ima instaliranog Dobavljača kriptografičkog pristupa, 128-bita, za iSeries (5722–AC3).
- iSeries A ima instaliranog i konfiguriranog Upravitelja digitalnih certifikata (OS/400 opcija 34) i IBM HTTP poslužitelja (5722–DG1).
- iSeries A djeluje kao Lokalni izdavač certifikata (CA) i certifikat za potpisivanje objekta prebiva 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 izvodi OS/400 verziju 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 poslužitelja (5722–DG1).
- iSeries B ne radi sa Lokalnim CA niti iSeries B potpisuje objekte.
- iSeries B je konfiguriran da omogući provjeru potpisa upotrebom DCM-a za kreiranje memorije certifikata *SIGNATUREVERIFICATION i importiranje potrebne provjere i certifikata Lokalnog CA.
- DCM se upotrebljava za provjeru potpisa na objektima.

Preduvjeti i pretpostavke

Ovaj scenario ovisi o sljedećim preduvjetima i pretpostavkama:

1. Svi iSeries poslužitelji zadovoljavaju zahtjeve za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).
2. Niti jedan nije ranije konfigurirao ili upotrebljavao DCM na nijednom iSeries poslužitelju.
3. Svi iSeries poslužitelji imaju instaliranu najveću razinu 128-bitova licenciranog programa Dobavljača kriptografičkog pristupa (5722-AC3).
4. Default postavka za provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST) u sve iSeries poslužitelje scenarija 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 memoriju 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 zadataka

Postoje dva skupa zadataka koje morate dovršiti za primjenu ovog scenarija: Jedan skup zadataka omogućuje konfiguriranje iSeries A, kao Lokalnog izdavača certifika (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 zadataka

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 scenario:

1. Dovršite sve preduvjetne korake da instalirate i konfigurirate sve potrebne iSeries proizvode.
2. Upotrijebite Upravitelja digitalnih certifikata (DCM) za kreiranje Lokalnog izdavača certifikata (CA) za izdavanje certifikata potpisa objekta.
3. Upotrijebite DCM za kreiranje definicije aplikacije.
4. Upotrijebite DCM za dodjelu certifikata definiciji aplikacije za potpisivanje objekta.
5. Upotrijebite DCM za potpisivanje objekata cgi-bin programa .
6. Upotrijebite DCM za eksportiranje certifikata koje drugi sistemi moraju upotrebljavati za provjeru potpisa objekata. Morate eksportirati kopiju certifikata Lokalnog CA i kopiju certifikata za potpisivanje objekta kao certifikat provjere potpisa za datoteku.
7. Prijenos datoteka certifikata javnom iSeries poslužitelju poduzeća (iSeries B) tako da vi i drugi mogu provjeravati potpise koje kreira iSeries A.

iSeries B koraci zadataka

Ako namjeravate vratiti potpisane objekte koje prenosite javnom Web poslužitelju u ovom (iSeries scenariju B), trebate dovršiti ove zadatke konfiguracije provjere potpisa na iSeries B prije prijenosa potpisanih objekata. 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 scenario:

8. Upotrijebite Upravitelja digitalnih certifikata (DCM) za kreiranje memorije certifikata *SIGNATUREVERIFICATION .
9. Upotrijebite DCM za importiranje certifikata Lokalnog CA i certifikata provjere potpisa..
10. Upotrijebite DCM za provjeru potpisa na prenesenim objektima.

Detalji konfiguracije

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

Korak 1: Dovršite sve korake za preduvjete

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

Korak 2: Kreirajte Lokalnog izdavača certifikata da izdate privatni certifikat za potpisivanje objekata.

Kad upotrebljavate Upravitelja digitalnih certifikata (DCM) za kreiranje Lokalnog izdavača certifikata (CA), taj postupak zahtjeva da dovršite niz 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 upotrijebite DCM za kreiranje i djelovanje Lokalnog CA, slijedite sljedeće korake:

1. Početak DCM.
2. U okviru navigacije DCM-a, izaberite **Kreiraj Izdavača certifikata (CA)** da se prikaže niz obrazaca.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite gumb sa upitnikom **?**) na vrhu stranice da pristupite online pomoći.
3. Dovršite sve obrasce za ovaj vođeni zadatak. Kad obavite ovaj zadatak morate učiniti sljedeće:
   a. Pružite identifikacijske informacije za Lokalni CA.
   b. Instalirajte certifikat Lokalnog CA u pretražitelj tako da softver može prepoznati Lokalnog CA i provjeriti valjanost certifikata koje izdaje Lokalni CA.
   c. Navedite podatke politike za Lokalni CA.
   d. Upotrijebite novi Lokalni CA za izdavanje certifikata poslužitelja ili klijenta kojeg aplikacije mogu upotrijebiti za SSL veze.

      Bilješka: Iako ovaj scenario 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 memoriju certifikata *OBJECTSIGNING u kojoj je on posebno pohranjen.
   e. Izaberite aplikacije koje mogu upotrebljavati certifikat poslužitelja ili klijenta za SSL veze.

      Bilješka: Za svrhu ovog scenarija ne izaberite nikakvu aplikaciju i kliknite **Nastavak** da se prikaže sljedeći obrazac.
   f. Upotrijebite novi Lokalni CA za izdavanje certifikata za potpisivanje objekata kojeg aplikacije mogu upotrijebiti za digitalno potpisivanje objekata. Ovaj podzadatak kreira memoriju certifikata *OBJECTSIGNING.To je memorija certifikata koju upotrebljavate za upravljanje certifikatima za potpisivanje objekata.
   g. Navedite aplikacije koje imaju povjerenja u Lokalni CA.

      Bilješka: Za svrhu ovog scenarija ne izaberite 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: Kreirajte definiciju 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 se ne treba odnositi na stvarnu aplikaciju; definicija aplikacije koju kreirate treba opisivati tip ili grupu objekata koje namjeravate potpisivati. Definiciju trebate da imate ID aplikacije za pridruživanje sa certifikatom da se omogući postupak potpisivanja.

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

1. U navigacijskom okviru kliknite **Izbor Memorije certifikata** i izaberite ***OBJECTSIGNING** kao memoriju certifikata za otvaranje.
2. Kad se prikaže Memorija certifikata i stranica Lozinke, unesite lozinku koju ste naveli za memoriju certifikata kad ste je kreirali i kliknite **Nastavak**.
3. U navigacijskom okviru izaberite **Upravljanje aplikacijama** da se prikaže popis zadataka.
4. Izaberite **Dodaj aplikaciju** sa 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: Dodijelite certifikat 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. Sa popisa zadataka izaberite **Dodjela certifikata** da se prikaže popis certifikata za trenutnu memoriju certifikata.
3. Izaberite certifikat sa popisa i kliknite **Dodjeli aplikacijama** da se prikaže popis definicija aplikacija za trenutnu memoriju certifikata.
4. Izaberite jednu ili više aplikacija sa popisa i kliknite **Nastavak**. Stranica poruka prikaže bilo potvrdite dodjelu certifikata ili informaciju 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: Potpišite objekte 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 Memorije certifikata** i izaberite ***OBJECTSIGNING** kao memoriju certifikata za otvaranje.
2. Unesite lozinku za memoriju certifikata *OBJECTSIGNING i kliknite **Nastavak**.
3. Nakon osvježenja navigacijskog okvira izaberite **Upravljanje potpisivim objektima** da se prikaže popis zadataka.
4. Sa popisa zadataka izaberite **Potpisivanje objekta** da se prikaže popis definicija aplikacija koje možete upotrebljavati za potpisivanje objekata.
5. Izaberite aplikaciju koju ste definirali u prethodnom koraku i kliknite **Potpisivanje objekta**. Prikaže se obrazac koji vam omogućuje da navedete smještaj objekata koje želite potpisati.
6. U dobiveno polje unesite potpuno kvalificirano ime staze i ime datoteke objekta ili direktorija objekata koje želite potpisati i kliknite **Nastavak**. Ili unesite smještaj direktorija i kliknite **Pretraži** da pogledate sadržaje direktorija da izaberete objekte za potpisivanje.

   Bilješka: Morate započeti ime objekta sa vodećom kosom crtom ili možete naići na grešku. Možete upotrijebiti također određene generičke znakove za opis dijela 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, za potpisivanje svih objekata u navedenom direktoriju možete unijeti /mydirectory/*; za potpisivanje svih programa u navedenoj 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 upotrijebiti funkciju Pretraži da pogledate popis sadržaja knjižnica ili direktorija trebate unijeti generički znak kao dio imena staze prije klika na **Pretraži**.

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

   Bilješka: Ako odlučite čekati rezultate posla, datoteka rezultata se prikaže izravno u 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).

8. Navedite potpuno kvalificirano ime staze i datoteke za upotrebu kod pohranjivanja rezultata posla za operaciju potpisivanja objekta i kliknite **Nastavak** . Ili unesite smještaj direktorija i kliknite **Pretraži** da pogledate sadržaje direktorija radi izbora datoteke za pohranjivanje rezultata posla. Prikaže se poruka koja pokazuje da je posao poslan za potpisivanje objekata. Da vidite rezultate posla, pogledajte posao **QOBJSGNBAT** u dnevniku posla.

Da se osigurate da vi ili drugi mogu provjeravati potpise, morate eksportirati potrebne certifikate datoteci 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: Eksportirajte certifikate da omogućite provjeru potpisa na iSeries B

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

Da dozvolite drugima provjeru potpisa, morate ih opskrbiti sa kopijom certifikata koji je potpisao objekt. Kad upotrebljavate Lokalnog izdavača certifikata (CA) za izdavanje certifikata, morate i njega opskrbiti sa 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 Nove memorije certifikata** i izaberite***SIGNATUREVERIFICATION** kao memoriju certifikata za kreiranje.
2. Izaberite **Da** da kopirate postojeće certifikate za potpisivanje objekata u novu memoriju certifikata kao certifikate za provjeru potpisa.
3. Navedite lozinku za novu memoriju certifikata i kliknite **Nastavak** da kreirate memoriju certifikata. Sada možete upotrebljavati DCM za provjeru potpisa objekata na istom sistemu kojeg upotrebljavate 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 **Eksportiraj certifikat**.
2. Izaberite **Izdavač certifikata (CA)** i kliknite **Nastavak** da se prikaže popis certifikata CA koje možete eksportirati.
3. Izaberite certifikat Lokalnog CA kojeg ste kreirali ranije sa popisa i kliknite **Eksportiraj**.
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 objekata.
7. Ponovo izaberite zadatak **Eksportiraj certifikat**.
8. Izaberite **Potpisivanje objekata** da se prikaže popis certifikata za potpisivanje objekata koje možete eksportirati.
9. Izaberite prikladni certifikat za potpisivanje objekta sa popisa i kliknite **Eksportiraj**.
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 certifikatima.

Korak 7: Prenesite datoteke 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 upotrijebiti Protokol za prijenos datoteka (FTP) ili distribuciju paketa Središnjeg Upravljanja za prijenos datoteka.

Korak 8: Zadaci provjere potpisa: Kreirajte memoriju certifikata *SIGNATUREVERIFICATION

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

Da kreirate memoriju certifikata *SIGNATUREVERIFICATION , slijedite ove korake:

1. Početak DCM-a.
2. U navigacijskom okviru Upravitelja digitalnih certifikata (DCM) izaberite **Kreiranje Nove memorije certifikata** i izaberite ***SIGNATUREVERIFICATION** kao memoriju certifikata za kreiranje.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac dok upotrebljavate DCM, izaberite gumb sa upitnikom **?**) na vrhu stranice da pristupite online pomoći.
3. Navedite lozinku za novu memoriju certifikata i kliknite **Nastavak** da kreirate memoriju certifikata. Sada možete importirati certifikate u memoriju i upotrebljavati ih za provjeru potpisa objekata.

Korak 9: Zadaci provjere potpisa: Importirajte certifikate

Da se provjeri potpis na objektu, memorija *SIGNATUREVERIFICATION mora sadržavati kopiju certifikata za provjeru potpisa. Ako je certifikat za potpisivanje privatni, ova memorija 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 se prenijela svakom iSeries krajnjem sistemu.

Da importirate ove certifikate u memoriju *SIGNATUREVERIFICATION, slijedite ove korake:

1. U navigacijskom okviru DCM-a kliknite **Izbor Memorije certifikata** i izaberite ***SIGNATUREVERIFICATION** kao memoriju certifikata za otvaranje.
2. Kad se prikažu Memorija certifikata i stranica Lozinke, unesite lozinku koju ste naveli za memoriju certifikata kad ste je kreirali i kliknite **Nastavak**.
3. Nakon osvježenja navigacijskog okvira izaberite **Upravljanje certifikatima** da se prikaže popis zadataka.
4. Sa popisa zadataka izaberite **Importiraj certifikat**.
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 certifikat CA i kliknite **Nastavak**. Prikaže se poruka koja ili potvrđuje da je postupak importiranje uspio ili informira o greški ako postupak nije uspio.
7. Ponovo izaberite zadatak **Importiraj certifikat**.
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**. Prikaže 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 sa odgovarajućim certifikatom za potpisivanje na iSeries A.

Korak 10: Zadaci provjere potpisa: Provjerite potpis na objektima programa

Da upotrijebite DCM za provjeru potpisa na prenesenim objektima programa, slijedite ove korake:

1. U navigacijskom okviru kliknite **Izbor Memorije certifikata** i izaberite ***SIGNATUREVERIFICATION** kao memoriju certifikata za otvaranje.
2. Unesite lozinku za memoriju certifikata *SIGNATUREVERIFICATION i kliknite **Nastavak**.
3. Nakon osvježenja navigacijskog okvira izaberite **Upravljanje potpisivim objektima** da se prikaže popis zadataka.
4. Sa popisa zadataka izaberite **Provjera potpisa objekta** da navedete smještaj objekata za koje želite provjeriti potpise.
5. U dobiveno polje unesite potpuno kvalificirano ime staze i ime datoteke objekta ili direktorija objekata za koje želite provjeriti potpise i kliknite **Nastavak**. Ili unesite smještaj direktorija i kliknite **Pretraži** da pogledate sadržaje direktorija da izaberete objekte za provjeru potpisa.

   Bilješka: Možete upotrijebiti također određene generičke znakove za opis dijela direktorija kojeg želite provjeriti. Ti generički znakovi su zvjezdica *****), koja specificira *bilo koji broj znakova*, i upitnik **?**)koji specificira *bilo koji pojedinačni znak*. Na primjer, za potpisivanje svih objekata u navedenom direktoriju možete unijeti /mydirectory/*; za potpisivanje svih programa u navedenoj 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 upotrijebiti funkciju Pretraži da pogledate popis sadržaja knjižnica ili direktorija trebate unijeti generički znak kao dio imena staze prije klika na **Pretraži**.
6. Izaberite opcije obrada koje želite upotrebljavati za provjeru potpisa na izabranom objektu ili objektima i kliknite **Nastavak**.

   Bilješka: Ako odlučite čekati rezultate posla, datoteka rezultata se prikaže izravno u 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. Navedite potpuno kvalificirano ime staze i datoteke za upotrebu kod pohranjivanja rezultata posla za operaciju provjere potpisa i kliknite **Nastavak** . Ili unesite smještaj direktorija i kliknite **Pretraži** da pogledate sadržaje direktorija da izaberete datoteku za pohranjivanje rezultata posla.Prikaže se poruka koja pokazuje da je posao poslan za provjeru potpisa objekata.Da vidite rezultate posla, pogledajte posao **QOBJSGNBAT** u dnevniku posla.

Scenario: Upotrijebite API-jeve za potpisivanje objekata i provjerite potpise 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 tijeku 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 nije točni izvor proizvoda. Ponekad se ta zbrka dešava kod korisnika koji instaliraju drugačiji proizvod od onog kojeg 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-jeve da lako dodajete potpisivanje objekta vašoj postojećoj obradi pakiranja. Također odlučujete upotrijebiti javni certifikat za potpisivanje objekata tako da možete učiniti 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 aplikacija 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 scenario ima sljedeće prednosti:

- Upotreba API-jeva za pakiranje i programatsko potpisivanja objekata skraćuje vrijeme koje morate utrošiti za primjenu ove sigurnosti.
- Upotreba API-jeva 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 koje ćete vršiti u budućnosti za slijeđenje 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. Upotrebom ovog API-ja omogućuje se dodavanje javnog certifikata kojeg ste upotrebljavali za automatsko potpisivanje aplikacije za 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 kod MyCo, Inc., trenutno programatski pakirate aplikacije poduzeća za distribuciju korisnicima. Radi toga želite upotrebljavati iSeries API-jeve za potpisivanje aplikacija i imati korisnikovu iSeries programatsku provjeru potpisa za vrijeme instalacije proizvoda.

Ciljevi ovog scenarija su sljedeći:

- Razvijač proizvoda poduzeća mora biti sposoban potpisivati objekte upotrebljavajući API za Potpis objekta kao dio postojećeg postupka za programatsko pakiranje aplikacija.
- Aplikacije poduzeća moraju se potpisivati sa javnim certifikatom da se osigura transparentnost postupka provjere potpisa za korisnika za vrijeme postupka instalacije proizvoda aplikacije.
- Poduzeće mora biti sposobno upotrebljavati iSeries API-jeve za programatsko dodavanje potrebnih certifikata provjere potpisa korisnikovoj memoriji certifikata *SIGNATUREVERIFICATION iSeries poslužitelja. Poduzeće mora biti sposobno programatski kreirati ovu memoriju 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 učinjena 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 scenario:

Centralni sistem (iSeries A)

- iSeries A izvodi OS/400 verziju 5, izdanje 2 (V5R2).
- iSeries A izvodi aplikaciju razvijačevog programa za pakiranje proizvoda.
- iSeries A ima instaliranog Dobavljača kriptografičkog pristupa, 128-bitova, za iSeries (5722–AC3).
- iSeries A ima instaliranog i konfiguriranog Upravitelja digitalnih certifikata (OS/400 opcija 34) i IBM HTTP poslužitelja (5722–DG1).
- iSeries A je primarni sistem za potpisivanje objekata za proizvode aplikacije poduzeća. Potpisivanje objekta proizvoda za distribuciju korisnicima se postiže na iSeries A obavljanjem ovih zadataka:
  1. Upotreba API-jeva za potpisivanje proizvoda aplikacije poduzeća.
  2. Upotreba DCM-a za eksportiranje certifikata provjere potpisa datoteci 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. Taj API omogućava da postupak instalacije proizvoda programatski dodaje certifikat provjere memoriji certifikata *SIGNATUREVERIFICATION na korisnikovom iSeries poslužitelju (iSeries B i C).

Korisnički iSeries poslužitelji B i C

- iSeries B izvodi OS/400 verziju 5, izdanje 2 (V5R2).
- iSeries C izvodi OS/400 verziju 5, izdanje 2 (V5R2).
- iSeries B i C imaju instalirane i konfigurirane Upravitelja digitalnih certifikata (opcija34) i IBM HTTP poslužitelja (5722–DG1).
- iSeries B i C kupuju i učitavaju aplikaciju sa Web stranice poduzeća za razvoj aplikacija (koja posjeduje iSeries A).
- iSeries B i C dobivaju MyCo-ovu kopiju certifikata provjere potpisa kad postupak instalacije MyCo-ove aplikacije kreira memoriju certifikata *SIGNATUREVERIFICATION na svakom od tih korisnikovih iSeries poslužitelja.

Preduvjeti i pretpostavke

Ovaj scenario 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 neobvezni zahtjev za korisnike iSeries B i C u ovom scenariju. Iako API za Dodavanje provjeritelja kreira memoriju certifikata *SIGNATUREVERIFICATION kao dio postupka instalacije proizvoda, ako je potrebno, on je kreira sa defaultnom lozinkom. Korisnici trebaju upotrebljavati DCM za promjenu defaultne lozinke da zaštite ovu memoriju certifikata od neovlaštenog pristupa.
2. Niti jedan nije ranije konfigurirao ili upotrebljavao DCM na nijednom iSeries poslužitelju.
3. Svi iSeries poslužitelji imaju instaliranu najveću razinu od 128-bitova licenciranog programa Dobavljača kriptografičkog pristupa (5722-AC3).
4. Default postavka za provjeru potpisa objekata za vrijeme vraćanja (QVFYOBJRST) sistemske vrijednosti u sve iSeries poslužitelje scenarija 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 objekta.
6. Sistemski administrator ili bilo tko (uključujući program), tko kreira memoriju 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 zadataka

Morate dovršiti svaki od ovih zadataka na iSeries A da potpisujete objekte kao što opisuje ovaj scenario:

1. Dovršite sve preduvjetne korake da instalirate i konfigurirate sve potrebne iSeries proizvode.
2. Upotrijebite DCM za kreiranje zahtjeva za certifikat da dobijete certifikat za potpisivanje objekta od poznatog javnog Izdavača certifikata (CA).
3. Upotrijebite DCM za kreiranje definicije aplikacije za potpisivanje objekta.
4. Upotrijebite DCM za importiranje potpisanog certifikata za potpisivanje objekata i dodijelite ga definiciji aplikacije za potpisivanje objekata.
5. Upotrijebite DCM za eksportiranje certifikata za potpisivanje objekata kao certifikat provjere potpisa tako da ga korisnici mogu upotrebljavati za provjeravanje potpisa na objektima aplikacija.
6. Ponovo napišite program za pakiranje aplikacija da uključite datoteku certifikata provjere potpisa kao dio proizvoda i da upotrijebite API za Potpisivanje objekata da potpišete vašu aplikaciju dok je pakirate za distribuciju korisnicima.

7. Kreirajte predinstalacijski izlazni program koji upotrebljava API za Dodavanje provjeritelja kao dio obrade pakiranja aplikacije. Taj izlazni program omogućuje kreiranje memorije certifikata *SIGNATUREVERIFICATION i dodavanje potrebnog certifikata za provjeru potpisa korisnikovom iSeries poslužitelju za vrijeme instaliranja proizvoda.
8. Neka korisnici upotrebljavaju DCM za ponovno postavljanje default lozinke za memoriju certifikata *SIGNATUREVERIFICATION na njihovom iSeries poslužitelju.

Detalji konfiguracije

Dovršite sljedeće korake zadatka da upotrijebite OS/400 API-jeve za potpisivanje objekata kao opisuje ovaj scenario.

Korak 1: Dovršite sve korake za preduvjete

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

Korak 2: Upotrijebite DCM da dobijete certifikat od javnog poznatog CA.

Ovaj scenario pretpostavlja da niste ranije upotrebljavali Upravitelja digitalnih certifikata za kreiranje i upravljanje certifikatima. Radi toga, morate kreirati memoriju certifikata *OBJECTSIGNING kao dio postupka za kreiranje certifikata za potpisivanje objekata. Ova memorija certifikata, kad je kreirana, 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. Početak DCM-a.
2. U okviru navigacije DCM-a, izaberite **Kreiraj Novu memoriju certifikata** da započnete vođeni zadatak i dovršite niz obrazaca. Ovi obrasci vas vode kroz obradu kreiranja memorije certifikata i certifikata kojeg možete upotrebljavati za potpisivanje objekata.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite gumb sa upitnikom **?**) na vrhu stranice da pristupite online pomoći.
3. Izaberite ***OBJECTSIGNING** kao memoriju certifikata za kreiranje i kliknite **Nastavak** .
4. Izaberite **Da** da kreirate certifikat kao dio kreiranja memorije certifikata *OBJECTSIGNING 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. Ova stranica potvrde prikazuje podatke zahtjeva certifikata koje morate dati javnom Izdavaču certifikata (CA) koji će izdati certifikat. Podaci Zahtjeva za Certifikat potpisivanja (CSR) sastoje se od javnog ključa i drugih informacija koje ste naveli za novi certifikat.
7. Pažljivo kopirajte i zalijepite CSR podatke na obrazac molbe za certifikat ili u posebnu datoteku, koju CA treba za zahtjev za certifikat. Morate upotrijebiti sve CSR podatke, uključujući Početnu i Krajnju liniju 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 za izdavanje i potpisivanje certifikata.
9. Počekajte dok CA vrati potpisani i dovršeni certifikat prije nego što nastavite sa sljedećim korakom zadatka u ovom scenariju.

Korak 3: Kreirajte definiciju 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 se ne treba odnositi na stvarnu aplikaciju; definicija aplikacije koju kreirate treba opisivati tip ili grupu objekata koje namjeravate potpisivati. Definiciju trebate da možete imati ID aplikacije za pridruživanje sa certifikatom da se omogući postupak potpisivanja.

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

1. U navigacijskom okviru kliknite **Izbor Memorije certifikata** i izaberite ***OBJECTSIGNING** kao memoriju certifikata za otvaranje.
2. Kad se prikaže Memorija certifikata i stranica Lozinke, unesite lozinku koju ste naveli za memoriju certifikata kad ste je kreirali i kliknite **Nastavak**.
3. U navigacijskom okviru izaberite **Upravljanje aplikacijama** da se prikaže popis zadataka.
4. Izaberite **Dodaj aplikaciju** sa popisa zadataka da se prikaže obrazac za definiranje aplikacije.
5. Dovršite obrazac i kliknite **Dodaj**.

Kad primite potpisani certifikat natrag od CA, možete dodijeliti certifikat aplikaciji koju ste kreirali.

Korak 4: Importirajte potpisani javni certifikat i dodijelite ga aplikaciji za potpisivanje objekata.

Da importirate certifikat i dodijelite ga aplikaciji da omogućite potpisivanje objekata, slijedite ove korake:

1. Početak DCM-a.
2. U navigacijskom okviru kliknite **Izbor Memorije certifikata** i izaberite ***OBJECTSIGNING** kao memoriju certifikata za otvaranje.
3. Kad se prikaže Memorija certifikata i stranica Lozinke, unesite lozinku koju ste naveli za memoriju certifikata kad ste je kreirali i kliknite **Nastavak**.
4. Nakon osvježenja navigacijskog okvira izaberite **Upravljanje certifikatima** da se prikaže popis zadataka.
5. Sa popisa zadataka izaberite **Importiraj certifikat** da započmete postupak importiranje potpisanog certifikata u memoriju certifikata.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite gumb sa upitnikom **?**) na vrhu stranice da pristupite online pomoći.
6. Izaberite **Dodjela certifikata** sa popisa zadataka **Upravljanje certifikatima** da se prikaže popis certifikata za trenutnu memoriju certifikata.
7. Izaberite certifikat sa popisa i kliknite **Dodjeli aplikacijama** da se prikaže popis definicija aplikacija za trenutnu memoriju certifikata.
8. Izaberite aplikaciju sa popisa i kliknite **Nastavak**. Prikaže se stranica bilo sa porukom potvrde izbora dodjele ili sa porukom o greški ako se desio problem.

Kad dovršite ovaj zadatak spremni ste potpisivati aplikacije i druge objekte upotrebljavajući OS/400 API-jeve. 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-jeve za Dodavanje provjeritelja kao dijela programa za instaliranje aplikacije da vršite potrebne konfiguracije provjere potpisa za korisnike. Na primjer, možete kreirati predinstalacijski izlazni program koji poziva API-jeve za Dodavanje provjeritelja za konfiguraciju korisnikovog iSeries poslužitelja.

Korak 5: Eksportirajte certifikate da omogućite provjeru potpisa na drugim iSeries poslužiteljima

Za potpisivanje objekata trebate vi i drugi imati sredstvo za provjeru vjerodostojnosti potpisa i upotrebljavati ga za određivanje da li su vršene promjene na potpisanim objektima. Da provjerite potpise na objektima na

istom sistemu koji potpisuje objekte, morate upotrijebiti DCM za kreiranje memorije certifikata *SIGNATUREVERIFICATION. Ta memorija certifikata mora sadržavati kopiju certifikata za potpisivanje objekata i kopiju certifikata CA za CA koji izdao certifikat za potpisivanje.

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

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

1. U navigacijskom okviru kliknite **Kreiranje Nove memorije certifikata** i izaberite***SIGNATUREVERIFICATION** kao memoriju certifikata za kreiranje.
2. Izaberite **Da** da kopirate postojeće certifikate za potpisivanje objekata u novu memoriju certifikata kao certifikate za provjeru potpisa.
3. Navedite lozinku za novu memoriju certifikata i kliknite **Nastavak** da kreirate memoriju certifikata.Sada možete upotrebljavati DCM za provjeru potpisa objekata na istom sistemu kojeg upotrebljavate 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 **Eksportiraj certifikat**.
2. Izaberite **Potpisivanje objekata** da se prikaže popis certifikata za potpisivanje objekata koje možete eksportirati.
3. Izaberite prikladni certifikat za potpisivanje objekta sa popisa i kliknite **Eksportiraj**.
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 korisnikovoj memoriji certifikata *SIGNATUREVERIFICATION. Ovaj API će također kreirati ovu memoriju certifika ako već ne postoji. Program za instalaciju proizvoda može zatim provjeravati potpise na objektima aplikacija dok ih vraća na korisnikove iSeries poslužitelje.

Korak 6: Ažurirajte program pakiranja aplikacija da upotrijebite iSeries API-jeve za potpisivanje aplikacija.

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

Da bolje shvatite kako upotrebljavati API Objekata potpisivanja kao dijela programa za pakiranje aplikacija, pregledajte sljedeće primjere kodova. Ovaj primjer koda snippet, pisanog u C-u, nije potpuni program za pakiranje i potpisivanje; to je prije primjer tog dijela takvog programa koji poziva API Objekta za potpisivanje. Ako odlučite upotrijebiti ovaj primjer programa, prilagodite ga vašim potrebama. Radi razloga sigurnosti IBM preporučuje da individualizirate primjer programa radije nego upotrebljavati dobivene defaultne vrijednosti.

Bilješka: IBM vam dodjeljuje neekskluzivnu licencu autorskog prava za upotrebu svih primjera programirajućih kodova za koje možete generirati sličnu funkciju skrojenu prema vašim posebnim potrebama. Cijeli kod primjera je dobiven od IBM-a za ilustrativne svrhe. Ovi primjeri nisu potpuno ispitani u svim uvjetima. IBM, prema tome, ne može jamčiti ili uključiti pouzdanost, upotrebljivost ili

funkcioniranje ovih programa. Svi programi ovdje sadržani su isporučeni ″KAO ŠTO JESU″ bez bilo kakvih garancija. Uključene garancije nepovredljivosti, mogućnosti prodaje i ispravnosti za određene svrhe se izričito poriču.

Promjenite ovaj kod snippet da odgovara vašim potrebama za upotrebu API-ja za Objekt potpisivanja kao dijela programa pakiranja za aplikacijski proizvod. 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.

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2002                                     */
/*                                                                  */
/* Upotrijebite API Objekta za potpisivanje da potpišete jednu ili više knjižnica */
/*                                                                  */
/* API će digitalno potpisati sve objekte u navedenoj knjižnici */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Ovaj materijal sadrži izvorni kod programiranja vama na */
/* razmatranje. Ovaj primjer nije potpuno */
/* ispitan u svim uvjetima. IBM, prema tome, ne može */
/* jamčiti ili podrazumijevati pouzdanost, upotrebljivost ili funkcioniranje  */
/* ovih programa.  Svi ovdje sadržani programi su */
/* isporučeni "KAO ŠTO JESU".  PODRAZUMIJEVANJE GARANCIJE */
/* MOGUĆNOSTI PRODAJE I SPOSOBNOSTI ZA ODREĐENU SVRHU */
/* SE IZRIČITO PORIČU. IBM ne pruža nikakve programske usluge za */
/* ove programe i datoteke. */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* 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 sa kojim 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: Kreirajte predinstalacijski izlazni program koji upotrebljava API za Dodavanje provjeritelja

Sada kad imate programatsku obradu za potpisivanje aplikacije, možete upotrijebiti API za Dodavanje provjeritelja kao dijela programa za instaliranje da kreirate završni proizvod za distribuciju. Na primjer, možete upotrijebiti API za Dodavanje provjeritelja kao dio predinstalacijskog izlaznog programa da se uvjerite da je certifikat dodan memoriji certifikata prije vraćanja potpisanih objekata 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 memoriju certifikata *SIGNATUREVERIFICATION.Kad dodajete CA certifikat memoriji certifikata, sistem smatra da je CA pouzdan izvor certifikata. Radi toga, sistem postupa sa certifikatom kojeg je izdao CA kao sa onim čije je porijeklo od pouzdanog izvora. Prema tome, možete upotrebljavati API za kreiranje instalacijkog izlaznog programa da umetnete CA certifikat u memoriju certifikata. Morate upotrijebiti Upravitelja digitalnih certifikata za dodavanje CA certifikata memoriji da se osigurate da netko mora određeno i ručno kontrolirati kojim CA-ovim vjeruje sistem. Na taj način se sprječava mogućnost da sistem može importirati certifikate sa izvora koje administrator nije svjesno naveo kao pouzdanim.

Ako želite spriječiti bilo koga da upotrebljava ovaj API za dodavanje certifikata provjere memoriji certifikata *SIGNATUREVERIFICATION bez vašeg znanja, trebate razmisliti o onemogućavanju

ovog API-ja na sistemu. To možete učiniti upotrebljavajući alate sistemskih usluga (SST) da ne dopustite promjene sistemskih vrijednosti koje se odnose na sigurnost. .

Da bolje shvatite kako upotrebljavati API Objekata potpisivanja kao dijela programa za instaliranje aplikacija, pogledajte sljedeći primjer koda predinstalacijskog izlaznog programa. Ovaj primjer koda snippet, pisanog u C-u, nije potpuni predinstalacijski izlazni program; to je prije primjer tog dijela programa koji poziva API Objekta za potpisivanje. Ako odlučite upotrijebiti ovaj primjer programa, prilagodite ga vašim potrebama. Radi razloga sigurnostiIBM preporučuje da individualizirate primjer programa radije nego da upotrebljavate dobivene defaultne vrijednosti.

Bilješka: IBM vam dodjeljuje neekskluzivnu licencu autorskog prava za upotrebu svih primjera programirajućih kodova za koje možete generirati sličnu funkciju skrojenu prema vašim posebnim potrebama. Cijeli kod primjera je dobiven od IBM-a za ilustrativne svrhe. Ovi primjeri nisu potpuno ispitani u svim uvjetima.IBM, prema tome, ne može jamčiti ili uključiti pouzdanost, upotrebljivost ili fukcioniranje ovih programa. Svi programi ovdje sadržani su isporučeni ″KAO ŠTO JESU″ bez bilo kakvih garancija. Uključene garancije nepovredljivosti, mogućnosti prodaje i ispravnosti za određene svrhe se izričito poriču.

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

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2002                                     */
/*                                                                  */
/* Upotrijebite API za Dodavanje provjeritelja da dodate certifikat u navedenoj */
/* IFS datoteci memoriji certifikata *SIGNATUREVERIFICATION. */
/*                                                                  */
/* Ovaj API će kreirati memoriju certifika ako već ne postoji. */
/* Ako je memorija certifikata kreirana dati će se default */
/* lozinka koja se treba što je prije moguće promijeniti pomoću DCM-a.*/
/* Ovo upozorenje treba dati vlasnicima sistema koji   */
/* upotrebljavaju ovaj program.                                                 */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Ovaj materijal sadrži izvorni kod programiranja vama na */
/* razmatranje. Ovaj primjer nije potpuno */
/* ispitan u svim uvjetima. IBM, prema tome, ne može */
/* jamčiti ili podrazumijevati pouzdanost, upotrebljivost ili funkcioniranje  */
/* ovih programa.  Svi ovdje sadržani progami su */
/* isporučeni "KAO ŠTO JESU".  PODRAZUMIJEVANJE GARANCIJE */
/* MOGUĆNOSTI PRODAJE I SPOSOBNOSTI ZA ODREĐENU SVRHU */
/* SE IZRIČITO PORIČU. IBM ne pruža nikakve programske usluge za */
/* ove programe i datoteke. */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Parametri su sljedeći:  */
/*                                                                  */
/*  char *   ime staze za IFS datoteku koja drži certifikatsku  */
/*  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;
}
```

Sa 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 provjeravanje 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 memoriju certifikata *SIGNATUREVERIFICATION sa defaultnom lozinkom za korisnika. Trebate savjetovati korisnicima da trebaju što je prije moguće upotrijebiti DCM za ponovno postavljanje lozinke za memoriju certifikata da je zaštite od neovlaštenog pristupa.

Korak 8: Neka korisnici ponovo postave defaultnu lozinku za memoriju certifikata *SIGNATUREVERIFICATION

API za Dodavanje provjeritelja je možda kreirao memoriju certifikata *SIGNATUREVERIFICATION kao dio postupka instaliranja proizvoda na korisnikovom iSeries poslužitelju. Ako je API kreirao memoriju certifikata, kreirao je za nju i defaultnu lozinku. Radi toga trebate savjetovati korisnike da upotrebljavaju DCM za ponovno postavljanje ove lozinke da se zaštiti memorija certifikata od neovlaštenog pristupa.

Neka korisnici dovrše ove korake za ponovno postavljanje lozinke memorije certifikata *SIGNATUREVERIFICATION:

1. Početak DCM-a.
2. U navigacijskom okviru kliknite **Izbor Memorije certifikata** i izaberite ***SIGNATUREVERIFICATION** kao memoriju certifikata za otvaranje.
3. Kad se prikaže Memorija certifikata i stranica Lozinke, kliknite **Ponovno postavljanje lozinke** da se prikaže stranica Ponovno postavljanje lozinke memorije certifikata.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite gumb sa upitnikom **?**) na vrhu stranice da pristupite online pomoći.

4. Navedite novu lozinku za memoriju, ponovo ju unesite da ju potvrdite, izaberite politiku isteka lozinke ili kliknite **Nastavak**.

Scenario: Koristite Središnje Upravljanje 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 upotrebljavate funkciju Središnjeg Upravljanja iSeries Navigatora za lakše pakiranje i distribuiranje ovih aplikacija i za obavljanje drugih administrativnih zadataka, za koje ste odgovorni. Međutim, trošite više vremena nego što ste htjeli prateći i korigirajući probleme sa ovim aplikacijama zbog neovlaštenih promjena na objektima. Radi toga želite bolje osigurati cjelinu ovih objekata potpisujući ih digitalno.

Istraživali ste sposobnosti OS/400 potpisivanja objekta i naučili da, započinjući u 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 upotrebe te sigurnosne tehnologije jer ne morate kupiti certifikat od poznatog CA.

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

Prednosti scenarija

Ovaj scenario 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 koje ćete vršiti 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 mrežni administrator kod MyCo, Inc., vi već upotrebljavate Središnje Upravljanje za brojne 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 naimenovani 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 svakiiSeries poslužitelj mora imati kopiju certifikata poduzeća za provjeru potpisa i certifikat Lokalnog izdavača certifika (CA) u svakoj poslužiteljovoj memoriji certifikata *SIGNATUREVERIFICATION.

- Provjerom potpisa na aplikacijama poduzeća omogućuje se da iSeries administratori i drugi mogu otkriti da li su sadržaji objekata promijenjen od kada su bili potpisani.
- Administratori moraju moći upotrebljavati Središnje Upravljanje za pakiranje, potpisivanje i zatim distribuirati 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 scenario:

Centralni sistem (iSeries A)
- iSeries A izvodi OS/400 verziju 5, izdanje 2 (V5R2).
- iSeries A služi kao centralni sistem sa kojeg se izvode funkcije Središnjeg Upravljanja, uključujući pakiranje i distribuiranje aplikacija poduzeća.
- iSeries A ima instaliranog Dobavljača kriptografičkog pristupa, 128-bitova, za iSeries (5722–AC3).
- iSeries A ima instaliranog i konfiguriranog Upravitelja digitalnih certifikata (OS/400 opcija 34) i IBM HTTP poslužitelja (5722–DG1).
- iSeries A djeluje kao Lokalni izdavač certifikata (CA) i certifikat za potpisivanje objekta prebiva na tom sistemu.
- iSeries A je primarni sistem za potpisivanje objekata za aplikacije poduzeća. Potpisivanje objekta proizvoda za distribuciju korisnicima se postiže na iSeries A obavljanjem ovih zadataka:
  1. Upotreba DCM-a za kreiranje Lokalnog CA-a i upotreba Lokalnog CA-a za kreiranje certifikata za potpisivanje objekta.
  2. Upotreba DCM-a za eksportiranje kopije certifikata Lokalnog CA i certifikata za provjeru potpisa datoteci tako da krajnji sistemi (iSeries B, C, D i E) mogu provjeravati potpisane objekte.
  3. Upotreba Središnjeg Upravljanja za potpisivanje objekata aplikacija i njihovo pakiranje sa datotekama certifikata provjera.
  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 izvode OS/400 verziju 5, izdanje 2 (V5R2).
- iSeries D i E izvode OS/400 verziju 5, izdanje 1 (V5R1).
- iSeries B, C, D i E imaju instalirane i konfigurirane Upravitelja digitalnih certifikata (opcija34) i IBM HTTP poslužitelje (5722–DG1).
- iSeries B, C, D i E primaju kopiju certifikata za provjeru potpisa od poduzeća i od Lokalnog CA sa centralnog sistema (iSeries A) kad sistemi primaju potpisanu aplikaciju.
- DCM se upotrebljava za kreiranje memorije certifikata *SIGNATUREVERIFICATION i importiranje certifikata Lokalnog CA i certifikata provjere u ovu memoriju certifikata.

Preduvjeti i pretpostavke

Ovaj scenario ovisi o sljedećim preduvjetima i pretpostavkama:
1. Svi iSeries poslužitelji zadovoljavaju zahtjeve za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).
2. Niti jedan nije ranije konfigurirao ili upotrebljavao DCM na nijednom iSeries poslužitelju.
3. iSeries A zadovoljava zahtjeve instaliranja i upotrebe iSeries Navigatora i Središnjeg Upravljanja.
4. Poslužitelj Središnjeg Upravljanja mora izvoditi na svim iSeries krajnjim sistemima.

5. Svi iSeries poslužitelji imaju instaliranu najveću razinu od 128-bitova licenciranog programa Dobavljača kriptografičkog pristupa (5722-AC3).
6. Default postavka za provjeru potpisa objekata za vrijeme vraćanja (QVFYOBJRST) sistemske vrijednosti u sve iSeries poslužitelje scenarija 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 memoriju 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 zadataka

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 za potpisivanja objekta

Morate dovršiti svaki od ovih zadataka na iSeries A da potpisujete objekte kao što opisuje ovaj scenario:

1. Dovršite sve preduvjetne korake da instalirate i konfigurirate sve potrebne iSeries proizvode.
2. Upotrijebite Upravitelja digitalnih certifikata (DCM) za kreiranje Lokalnog izdavača certifikata (CA) za izdavanje privatnog certifikata za potpisivanje objekta.
3. Uotrijebite DCM za kreiranje definicije aplikacije.
4. Upotrijebite DCM za dodjelu certifikata definiciji aplikacije za potpisivanje objekta.
5. Upotrijebite DCM za eksportiranje certifikata koje drugi sistemi moraju upotrebljavati za provjeru potpisa objekata.Morate eksportirati kopiju certifikata Lokalnog CA i kopiju certifikata za potpisivanje objekta kao certifikat provjere potpisa za datoteku.
6. Prenesite datoteke certifikata svakom iSeries krajnjem sistemu na kojem namjeravate provjeravati potpise.
7. Upotrijebite Središnje Upravljanje za potpisivanje objekata aplikacija. .

Koraci zadatka za provjeru potpisa

Trebate dovršiti ove zadatke za konfiguraciju 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 objetke na krajnje sisteme.

Na svakom iSeries krajnjem sistemu, morate dovršiti ove zadatke za provjeravanje potpisa na objektima kao što opisuje ovaj scenario:

8. Upotrijebite Upravitelja digitalnih certifikata (DCM) za kreiranje memorije certifikata *SIGNATUREVERIFICATION .
9. Upotrijebite DCM za importiranje certifikata Lokalnog CA i certifikata provjere potpisa..

Detalji konfiguracije

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

Korak 1: Dovršite sve korake za preduvjete

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

Korak 2: Kreirajte Lokalnog izdavača certifikata da izdate privatni certifikat za potpisivanje objekata.

Kad upotrebljavate Upravitelja digitalnih certifikata (DCM) za kreiranje Lokalnog izdavača certifikata (CA), taj postupak zahtjeva 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 upotrijebite DCM za kreiranje i djelovanje Lokalnog CA, slijedite sljedeće korake:

1. Početak DCM-a.
2. U okviru navigacije DCM-a, izaberite **Kreiraj Izdavača certifikata (CA)** da se prikaže niz obrazaca.

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

      Bilješka: Iako ovaj scenario 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 memoriju certifikata *OBJECTSIGNING u kojoj je on posebno pohranjen.
   e. Izaberite aplikacije koje mogu upotrebljavati certifikat poslužitelja ili klijenta za SSL veze.

      Bilješka: Za svrhu ovog scenarija ne izaberite nikakvu aplikaciju i kliknite **Nastavak** da se prikaže sljedeći obrazac.
   f. Upotrijebite novi Lokalni CA za izdavanje certifikata za potpisivanje objekata kojeg aplikacije mogu upotrijebiti za digitalno potpisivanje objekata.Ovaj podzadatak kreira memoriju certifikata *OBJECTSIGNING.To je memorija certifikata koju upotrebljavate za upravljanje certifikatima za potpisivanje objekata.
   g. Izaberite aplikacije koje imaju povjerenja u Lokalni CA.

      Bilješka: Za svrhe ovog scenarija ne izaberite 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: Kreirajte definiciju aplikacije za potpisivanje objekta

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 se ne treba odnositi na stvarnu aplikaciju; definicija aplikacije koju kreirate treba opisivati tip ili grupu objekata koje namjeravate potpisivati.Definiciju trebate da možete imati ID aplikacije za pridruživanje sa certifikatom da se omogući postupak potpisivanja.

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

1. U navigacijskom okviru kliknite **Izbor Memorije certifikata** i izaberite ***OBJECTSIGNING** kao memoriju certifikata za otvaranje.
2. Kad se prikaže Memorija certifikata i stranica Lozinke, unesite lozinku koju ste naveli za memoriju certifikata kad ste je kreirali i kliknite **Nastavak**.
3. U navigacijskom okviru izaberite **Upravljanje aplikacijama** da se prikaže popis zadataka.
4. Izaberite **Dodaj aplikaciju** sa 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: Dodijelite certifikat definiciji aplikacije za potpisivaje 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. Sa popisa zadataka izaberite**Dodjela certifikata** da se prikaže popis certifikata za trenutnu memoriju certifikata.
3. Izaberite certifikat sa popisa i kliknite **Dodjela aplikacijama** da se prikaže popis definicija aplikacija za trenutnu memoriju certifikata.
4. Izaberite jednu ili više aplikacija sa popisa i kliknite **Nastavak**. Stranica poruka prikaže bilo da potvrdite dodjelu certifikata ili informaciju 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 objetke na krajnje sisteme.

Korak 5: Eksportirajte certifikate da omogućite provjeru potpisa na drugim iSeries sistemima

Potpisivanje objekata za zaštitu cjelovitosti sadržaja zahtjeva da vi i drugi imate sredstvo za provjeru vjerodostojnosti potpisa.Da provjerite potpise na objektima na istom sistemu koji potpisuje objekte, morate upotrijebiti DCM za kreiranje memorije certifikata *SIGNATUREVERIFICATION.Ta memorija 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 sa kopijom certifikata koji je potpisao objekt. Kad upotrebljavate Lokalnog izdavača certifikata (CA) za izdavanje certifikata, morate i njega opskrbiti sa kopijom certifikata Lokalnog CA.

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

1. U navigacijskom okviru kliknite **Kreiranje Nove memorije certifikata** i izaberite***SIGNATUREVERIFICATION** kao memoriju certifikata za kreiranje.
2. Izaberite **Da** da kopirate postojeće certifikate za potpisivanje objekata u novu memoriju certifikata kao certifikate za provjeru potpisa.
3. Navedite lozinku za novu memoriju certifikata i kliknite **Nastavak** da kreirate memoriju 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 **Eksportiraj certifikat**.
2. Izaberite **Izdavač certifikata (CA)** i kliknite**Nastavak** da se prikaže popis certifikata CA koje možete eksportirati.
3. Izaberite certifikat Lokalnog CA kojeg ste kreirali ranije sa popisa i kliknite **Eksportiraj**.
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. Ponovo izaberite zadatak**Eksportiraj certifikat**.
8. Izaberite **Potpisivanje objekata** da se prikaže popis certifikata za potpisivanje objekata koje možete eksportirati.
9. Izaberite prikladni certifikat za potpisivanje objekta sa popisa i kliknite **Eksportiraj**.
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: Prenesite datoteke certifikata na iSeries krajnje 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 upotrijebiti Protokol za prijenos datoteka (FTP) ili distribuciju paketa Središnjeg Upravljanja za prijenos datoteka.

Korak 7: Potpisujte objekte 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 objetke na krajnje sisteme.

Za potpisivanje aplikacije koju distribuirate na iSeries krajnje sisteme kao što opisuje ovaj scenario, slijedite ove korake:

1. Upotrijebite Središnje Upravljanje za pakiranje i distribuiranje softverskih proizvoda .
2. Kad dođete na **Identifikacijski** panel u čarobnjaku **Definicija proizvoda**, kliknite **Napredna** 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: Kreirajte memoriju certifikata *SIGNATUREVERIFICATION 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 memoriji certifikata *SIGNATUREVERIFICATION. Ako je privatni certifikat potpisao objekte, ta memorija certifikata mora također sadržavati kopiju certifikata Lokalnog CA.

Da kreirate memoriju certifikata *SIGNATUREVERIFICATION , slijedite ove korake:

1. Početak DCM-a.
2. U navigacijskom okviru Upravitelja digitalnih certifikata (DCM) izaberite**Kreiranje Nove memorije certifikata** i izaberite ***SIGNATUREVERIFICATION** kao memoriju certifikata za kreiranje.

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite gumb sa upitnikom **?**) na vrhu stranice da pristupite online pomoći.
3. Navedite lozinku za novu memoriju certifikata i kliknite **Nastavak** da kreirate memoriju certifikata.Sada možete importirati certifikate u memoriju i upotrebljavati ih za provjeru potpisa objekata.

Korak 9: Zadaci provjere potpisa:Importirajte certifikate

Da se provjeri potpis na objektu, memorija *SIGNATUREVERIFICATION mora sadržavati kopiju certifikata za provjeru potpisa.Ako je certifikat za potpisivanje privatni, ova memorija 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 se prenijela svakom iSeries krajnjem sistemu.

Da importirate ove certifikate u memoriju *SIGNATUREVERIFICATION, slijedite ove korake:

1. U navigacijskom okviru DCM-a kliknite **Izbor Memorije certifikata** i izaberite ***SIGNATUREVERIFICATION** kao memoriju certifikata za otvaranje.
2. Kad se prikažu Memorija certifikata i stranica Lozinke, unesite lozinku koju ste naveli za memoriju certifikata kad ste je kreirali i kliknite **Nastavak**.
3. Nakon osvježenja navigacijskog okvira izaberite **Upravljanje certifikatima** da se prikaže popis zadataka.
4. Sa popisa zadataka izaberite **Importiraj certifikat**.
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**. Prikaže se poruka koja ili potvrđuje da je postupak importiranja uspio ili informira o greški ako postupak nije uspio.
7. Ponovo izaberite zadatak **Importiraj certifikat**.
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**. Prikaže 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 sa odgovarajućim certifikatom potpisa, kad vraćate potpisane objekte.

Koncepti potpisivanja objekta

Prije nego što počnete upotrebljavati sposobnosti iSeries potpisivanja objekata i provjere potpisa možda ćete naći korisnim 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).

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

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

Digitalni potpisi

OS/400 pruža podršku za upotrebu digitalnih certifikata za digitalno ″potpisivanje″ objekata. Digitalni potpis na objektu se kreira u kriptografskom 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 certifikatovog privatnog ključa. Primatelj objekta upotrebljava certifikatov odgovarajući javni ključ za dešifriranje potpisa, koji provjerava cjelovitost potpisanog objekta i provjerava pošiljatelja kao izvor.

Podrška za potpisivanje objekta povećava tradicionalne iSeries poslužiteljske alate za kontroliranje tko može promijeniti objekte. Tradicionalne kontrole ne mogu zaštititi objekt od neovlaštenog uplitanja 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 je objekt porijeklom sa 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 promjenjeni. 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 potpisuje objekt, a ne određenog korisnika na tom sistemu (iako korisnik mora imati prikladno ovlaštenje za upotrebu certifikata za potpisivanje objekata).

Ako odlučite da upotreba digitalnih potpisa odgovara vašim sigurnosnim potrebama i politikama, trebate procijeniti da li trebate upotrebljavati javne certifikate u odnosu na izdavanje lokalnih certifikata. Ako namjeravate distribuirati objekte korisnicima u općenitu javnost, trebate razmotriti upotrebu certifikata od poznatog Izdavača certifikata (CA) za potisivanje objekata. Upotreba javnih certifikata osigurava da drugi mogu lako i jeftino provjeravati potpise koje stavljate na objekte koje njima distribuirate. Ako, međutim, namjeravate distribuirati objekte jedino u vašoj organizaciji, možda ćete više želiti upotrebljavati Upravitelja digitalnih certifikata (DCM) za djelovanje sa vašim vlastitim Lokalnim CA za izdavanje certifikata za potpisivanje objekata.Upotreba privatnih certifikata od Lokalnog CA za potpisivanje objekata je jeftinije od kupnje certifikata od poznatog javnog CA.

Tipovi digitalnih potpisa

Započinjući u V5R2, možete potpisivati objekte naredbi (*CMD); također možete izabrati jedan od dva tipa potpisa za objekte *CMD: potpisi jezgri objekata ili potpisi cijelog objekta.

- **Potpisi cijelih objekata**
  Ovaj tip potpisa pokriva sve osim nekoliko nebitnih bajtova objekta.
- **Potpisi jezgri objekata**
  Ovaj tip potpisa pokriva bitne bajtove objekta *CMD. Međutim, potpis ne pokriva one bajtove koji su podložni češćim promjenama. Ovaj tip potpisa omogućuje vršenje nekih promjena na naredbi bez

poništenja potpisa. Koje bajtove potpis jezgre objekta ne pokriva ovisi o određenom objektu *CMD; potpisi jezgri, na primjer, ne pokrivaju defaultne parametre na objektima *CMD. Primjeri promjena koje neće poništiti potpis jezgre objekta uključuju:

- Promjena defaultnih naredbi.
- Dodavanje programa za provjeravanje valjanosti naredbi koja ga nema.
- Mijenjanje Gdje se dozvoljava izvoditi parametar.
- Mijenjanje Dozvoli ograničene korisničke parametre.

Da naučite još o tome koje iSeries objekte možete potpisivati i koje bajtove od objekta *CMD pokriva potpis jezgre objekta, 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 sistema, osim objekata koji su pohranjeni u knjižnici. Ako objekt ima dodani Java program, taj program će se također potpisati. Možete potpisivati samo ove objekte u sistemu datoteka QSYS.LIB: programi (*PGM), uslužni programi (*SRVPGM), modules (*MODULE), SQL packages (*SQLPKG), *FILE (samo spremanje datoteke) i naredbe (*CMD).

Da se potpiše objekt, on mora prebivati na lokalnom sistemu. Na primjer, ako radite sa Windows 2000 poslužiteljem na Integriranom xSeries poslužitelju za iSeries, imate dostupan sistem datoteka QNTC u integriranom sistemu datoteka. Direktoriji u tom sistemu datoteka ne smatraju se lokalnim jer sadrže datoteke čiji je vlasnik Windows 2000 operacijski sistem. Također ne možete potpisivati prazne objekte ili objekte koji su kompilirani za ranije izdanje od V5R1.

Potpisi objekata naredbe (*CMD)

Kad potpisujete objekte naredbe *CMD, možete izabrati jedan od dva tipa potpisa za primjenu na objektu *CMD. Možete izabrati potpisivanje bilo cijelog objekta ili potpisivanje samo jezge objekta. Kad izaberete potpisati cijeli objekt, potpis se primjenjuje na sve osim nekoliko nebitnih bajtova objekta. Potpis cijelog objekta pokriva stavke sadržane u potpisu jezgre objekta.

Kad izaberete potpisati samo jezgru 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 mod u kojem je objekt važeći ili određuju gdje je dozvoljeno izvođenje objekta. Potpisi jezgri ne pokrivaju, na primjer, defaultne parametre na objektima *CMD. Ovaj tip potpisa omogućuje vršenje nekih promjena na naredbi bez poništenja njenog potpisa. Primjeri promjena koje neće poništiti ove tipove potpisa uključuju:

- Promjena defaultnih naredbi.
- Dodavanje programa za provjeravanje valjanosti naredbi koja ga nema.
- Mijenjanje Gdje se dozvoljava izvoditi parametar.
- Mijenjanje Dozvoli ograničene korisničke parametre.

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

Sastav potpisa objekta jezgre na objektima *CMD.

Dio objekta	Odnos prema potpisu jezgre objekta
Defaulti naredbi koje je promijenio CHGCMDDFT	Nije dio potpisa jezgre objekta
Program za obradu naredbe i knjižnice	Uvijek uključeno kao dio potpisa jezgre objekta
Izvorna datoteka REXX i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta.

Dio objekta	Odnos prema potpisu jezgre objekta
Izvorni član REXX	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta.
Okolina naredbe REXX i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta.
Ime izlaznog progama REXX, knjižnica i izlazni kod	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta.
Program za kontrolu valjanosti i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta.
Mod u kojem je važeći	Nije dio potpisa jezgre objekta
Gdje se dozvoljava izvođenje	Nije dio potpisa jezgre objekta
Dozvoli ograničenje korisnika	Nije 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 nije pohranjen u objekt.
Omogući grafičko korisničko sučelje (GUI)	Nije dio potpisa jezgre objekta

Obrada potpisivanja objekta

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

- **Obrada greške**
  Možete navesti koji tip obrade greške treba aplikacija upotrijebiti kad kreira potpise na više od jednog objekta. Možete navesti bilo da aplikacija zaustavi potpisivanje objekata kad se desi greška ili da nastavi potpisivanje drugih objekata u obradi.
- **Duplikat potpisa objekta**
  Možete navesti kako treba aplikacija rukovati sa obradom potpisivanja kad aplikacija ponovo potpisuje objekt. Možete navesti da li ostaviti originalni potpis na mjestu ili zamijeniti originalni potpis sa novim potpisom.
- **Objekti u poddirektorijima**
  Možete navesti kako treba aplikacija rukovati sa obradom potpisivanja 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.

Postupak provjere potpisa

Možete navesti sljedeće opcije za postupak potpisivanja objekta.

- **Obrada greške**
  Možete navesti koji tip obrade greške treba aplikacija upotrijebiti kad provjerava potpise na više od jednog objekta. Možete navesti bilo da aplikacija zaustavi provjeravanje objekata kad se desi greška ili da nastavi provjeravanje drugih objekata u obradi.
- **Objekti u poddirektorijima**
  Možete navesti kako treba aplikacija rukovati sa provjeravanjem potpisa na objektima 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 cjeline.**
  Postoje sistemska pravila koja određuju kako sistem treba rukovati sa potpisima jezgre i cjeline na objektima za vrijeme postupka 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 sa podacima u objektu kad je bio potpisan.
  - Ako objekt ima potpise cijelih objekata koji su pouzdani (na osnovi certifikata sadržanog u memoriji certifikata *SIGNATUREVERIFICATION), 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 mora se podudarati sa certifikatom memorije certifikata *SIGNATUREVERIFICATION ili postupak provjere ne uspjeva. Ako se najmanje jedan potpis jezgre objekta podudara, postupak provjere se nastavlja.

Potpisivanje objekta i preduvjeti provjere potpisa

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

Preduvjeti za potpisivanje objekata

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

- Možete upotrijebiti Upravitelja digitalnih certifikata (DCM).
- Možete napisati program koji upotrebljava API za Potpisivanje objekata..
- Možete upotrebljavati funkciju Središnjeg Upravljanja of iSeries Navigatora za potpisivanje objekata kad ih pakirate za distribuciju krajnjem sistemu iSeries sistema.

Koju metodu izabrati za potpisivanje objekata ovisi o vašim poslovnim i sigurnosnim potrebama. Bez obzira na metodu koju planirate upotrebljavati za potpisivanje objekata, morate se osigurati da su zadovoljeni određeni uvjeti:

- Morate zadovoljiti preduvjete za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).
  - Morate upotrijebiti DCM za kreiranje memorije certifikata *OBJECTSIGNING. Ovu memoriju certifikata kreirate bilo kao dio postupka kreiranja Lokalnog izdavača certifikata (CA) ili kao dio postupka upravljanja certifikatima potpisivanja objekata od javnog Internet CA.
  - Memorija certifikata *OBJECTSIGNING mora sadržavati najmanje jedan certifikat, bilo onaj kojeg ste kreirali pomoću Lokalnog CA ili onaj kojeg 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 memoriju certifikata *SIGNATUREVERIFICATION mora imati posebna ovlaštenja *SECADM i *ALLOBJ.

Preduvjeti provjere potpisa

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

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

  Bilješka: API za Dodavanje provjeritelja kreira memoriju certifikata sa defaultnom lozinkom. Za ponovno postavljanje ove defaultne lozinke na jednu iz vašeg izbora trebate upotrijebiti DCM da se spriječi neovlašteni pristup memoriji certifikata.
- Memorija certifikata *SIGNATUREVERIFICATION mora sadržavati kopiju certifikata koji je potpisao objekt. Ovaj certifikat možete dodati memoriju certifikata na jedan od dva načina. Možete upotrijebiti DCM na sistemu koji potpisuje za eksportiranje certifikata datoteci i zatim upotrijebiti DCM na ciljnom sistemu za provjeru za importiranje certifikata u memoriju certifikata *SIGNATUREVERIFICATION. Ili ako upotrebljavate javni certifikat za potpisivanje objekata, možete dodati certifikat memoriji certifikata od ciljnog sistema za provjeru pisanjem programa koji upotrebljava API za Dodavanje provjeritelja.
- Memorija certifikata *SIGNATUREVERIFICATION mora sadržavati kopiju certifikata od CA koji je izdao certifikat koji je potpisao objekte. Ako upotrebljavate javni certifikat za potpisivanje objekata, memorija certifikata na ciljnom sistemu za provjeru treba već imati kopiju potrebnog certifikata od CA. Ako, međutim, upotrebljavate certifikat kojeg je izdao Lokalni CA za potpisivanje objekata, morate upotrijebiti DCM za dodavanje kopije certifikata Lokalnog CA memoriji certifikata na ciljnom sistemu za provjeru.

  Bilješka: Radi sigurnosnih razloga API za Dodavanje provjeritelja ne dopušta umetanje certifikata od Izdavača certifikata (CA) u memoriju certifikata *SIGNATUREVERIFICATION.Kad dodajete certifikat od CA memoriji certifikata, sistem smatra da je CA pouzdan izvor certifikata. Radi toga, sistem postupa sa certifikatom kojeg je izdao CA kao sa onim čije je porijeklo od pouzdanog izvora. Prema tome, ne možete upotrebljavati API za kreiranje instalacijkog izlaznog programa da umetnete certifikat od CA u memoriju certifikata. Morate upotrijebiti Upravitelja digitalnih certifikata za dodavanje certifikata od CA memoriji certifikata da se osigurate da netko mora određeno i ručno kontrolirati kojim CA-ovima vjeruje sistem. Na taj način se sprječava mogućnost da sistem može importirati certifikate sa izvora koje administrator nije svjesno naveo kao pouzdanim.

  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 datoteci. Možete zatim upotrijebiti DCM na ciljnom iSeries poslužitelju provjere za importiranje certifikata Lokalnog CA u memoriju certifikata *SIGNATUREVERIFICATION. Da

spriječite moguću grešku, morate importirati certifikat Lokalnog Ca u ovu memoriju certifikata prije upotrebe API-ja za Dodavanje provjeritelja da dodate certifikat provjere potpisa. Radi toga, ako upotrebljavate certifikat kojeg je izdao Lokalni CA, možda ćete ustanoviti da je lakše upotrebljavati DCM za importiranje certifikata od CA i certifikata provjere u memoriju certifikata.

Ako želite spriječiti bilo koga da upotrebljava ovaj API za dodavanje certifikata provjere memoriji certifikata *SIGNATUREVERIFICATION bez vašeg znanja, trebate razmisliti o onemogućavanju ovog API-ja na sistemu. To možete učiniti pomoću alata sistemskih usluga (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 memoriju certifikata *SIGNATUREVERIFICATION ili mijenja njenu lozinku mora imati posebna ovlaštenja *SECADM i *ALLOBJ.

Upravljanje potpisanim objektima

Započinjući u V5R1, IBM je započeo potpisivanje OS/400. licenciranih progama i PTF-ova kao način službenog označavanja operacijskog sistema 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 sa potpisanim objektima i kako ti potpisani objekti utječu na rutinske sistemske administrativne zadatke.

Potpisani objekti primarno utječu na zadatke sigurnosne kopije 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 detalje o upotrebi naredbi za provjeru potpisa objekata za određivanje cjelovitosti objekta.

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 sa 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 sa provjerom potpisa za vrijeme operacije vraćanja. Postavka koju upotrebljavate za ovu sistemsku vrijednost, u spoju sa 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 sa tim objektima kao da su nepotpisani.

Postoji nekoliko vrijednosti koje možete upotrebljavati za sistemsku vrijednost QVFYOBJRST, u rasponu od zanemarivanja svih potpisa do zahtjevanja važećih potpisa za sve objekte koje vraća sistem. Ova sistemska vrijednost utječe samo na izvedbene objekte koji se vraćaju, kao programi(*PGM), naredbe (*CMD), uslužni programi (*SRVPGM), SQL paketi (*SQLPKG) i moduli (*MODULE). Ovo se također odnosi na objekte stream datoteke (*STMF) koji su pridružili Java programe kreirane naredbom Kreiranje Java Program-a (CRTJVAPGM). Ovo se ne odnosi na datoteke za spremanje(*SAV) ili IFS datoteke.

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

CL naredbe koje utječu na potpisane objekte

Postoji nekoliko CL naredbi koje dopuštaju rad sa 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 sa 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 sa popisa nitnih knjižnica. Možete upotrijebiti ovu naredbu da odredite da li je objekt potpisan i da pogledate informacije o potpisu.
- Naredbe integriranog sistema datoteka Prikaz Veza objekata (DSPLNK) i Rad sa Vezama objekata . 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 za provjeru 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 sa potpisanim i potpisivim objektima, pogledajte Naredbe kontrolora koda za osiguranje cjelovitosti potpisa .
- Naredba za Provjeru 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 sa instaliranog proizvoda. Možete upotrijebiti parametar CHKSIG da navedete kako naredba treba rukovati i izvjestiti o mogućim problemima potpisa za taj proizvod. Da naučite još o upotrebi ove naredbe sa potpisanim i potpisivim objektima, pogledajte Naredbe kontrolora koda za osiguranje cjelovitosti potpisa .
- Naredba za Spremanje licenciranog programa(SAVLICPGM).
  Oca naredba sprema kopiju objekata koji čine licencirani program. Ona sprema licencirani program u obliku kojeg može vratiti naredba Vraćanje licenciranog progama (RSTLICPGM). Možete upotrijebiti parametar CHKSIG da navedete kako naredba treba rukovati i izvjestiti o mogućim problemima potpisa za taj proizvod. Da naučite još o upotrebi ove naredbe sa potpisanim i potpisivim objektima, pogledajte Naredbe provjeritelja koda za osiguranje cjelovitosti potpisa .
- Naredba Vraćanje (RST).
  Ova naredba vraća kopiju jednog ili više objekata koji se mogu upotrebljavati u integriranom sistemu datoteka (IFS). Ova naredba također omogućuje vraćanje memorija certifikata i njihovih sadržaja na sistemu. Međutim, ne možete upotrijebiti ovu naredbu za vraćanje memorije certifikata

*SIGNATUREVERIFICATION. Kako naredba vraćanja rukuje sa 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 Spremi knjižnicu (SAVLIB). Naredba RSTLIB vraća cijelu knjižnicu, koja uključuje opis knjižnice, opise objekata i sadržaje objekata u knjižnici. Kako ta naredba rukuje sa potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).
- Naredba za Vraćanje licenciranog programa(RSTLICPGM).
  Ova naredba učitava ili vraća licencirani program, bilo za početnu instalaciju ili instalaciju novog izdanja. Kako ta naredba rukuje sa potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).
- Naredba za 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 sa potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).

Naredbe za spremanje i vraćanje memorija certifikata.

- Naredba za Spremanje (SAV).
  Ova naredba omogućuje spremanje kopije jednog ili više objekata koji se mogu upotrebljavati u integriranom sistemu datoteka, uključujući memorije certifikata. Međutim, ne možete upotrijebiti ovu naredbu za spremanje memorije certifikata *SIGNATUREVERIFICATION.
- Naredba za Spremanje sigurnosnih podataka(SAVSECDTA).
  Ova naredba omogućuje spremanje svih sigurnosnih informacija ne tražeći da sistem bude u ograničenom stanju. Upotreba ove naredbe omogućuje spremanje memorije certifikata *SIGNATUREVERIFICATION i certifikata koje ona sadržava. Ova naredba ne sprema nikakvu drugu memoriju certifikata.
- Naredba za Spremanje sistema(SAVSYS).
  Ova naredba omogućuje spremanje kopije licenciranog internog koda i knjižnice QSYS u formatu kompatibilnom sa instalacijom iSeries poslužitelja. Ona ne sprema objekte sa 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 memorije certifikata *SIGNATUREVERIFICATION i certifikata koje ona sadržava.
- Naredba Vraćanje (RST).
  Ova naredba omogućuje vraćanje memorija certifikata i njihovih sadržaja na sistemu. Međutim, ne možete upotrijebiti ovu naredbu za vraćanje memorije certifikata *SIGNATUREVERIFICATION.
- Naredba za 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 memorije certifikata *SIGNATUREVERIFICATION i skrivenih lozinki za ovu i sve druge memorije certifikata. Možete vratiti memoriju certifikata *SIGNATUREVERIFICATION 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 memorija certifikata i njihovih lozinki, navedite *ALL za parametar USRPRF.

Naredbe koje mogu ukloniti ili izgubiti potpise sa objekata.

Kad upotrebljavate sljedeće naredbe na potpisanom objektu, to možete učiniti na način kojim možete ukloniti ili izgubiti potpis sa objekta. Uklanjanje potpisa može uzrokovati probleme sa objektom na koji se utječe. U najboljem slučaju, nećete više moći provjeravati pouzdanost izvora objekta i nećete moći provjeravati potpis da otkrijete promjene na objektu. Ove naredbe trebate upotrebljavati samo na onim potpisanim objektima koje ste kreirali (a ne na potpisanim objektima koje ste dobili od drugih kao 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 ako je potrebno ponovo potpisati.

Bilješka: Da provjerite da li je naredba Spremi izgubila objektov potpis, morate vratiti objekt u knjižnicu različitu od one od 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 za 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 trenutnim atributima.
- Naredba za Promjenu programa usluge (CHGSRVPGM).
  Ova naredba mijenja atribute programa usluge ne tražeći da ga rekompajlirate. Također, možete upotrebljavati ovu naredbu za prisilno ponovno kreiranje programa usluge čak ako su navedeni atributi isti trenutnim atributima.
- Naredba za Brisanje datoteke za spremanje (CLRSAVF).
  Ova naredba briše sadržaje datoteke za spremanje; ona briše sve postojeće slogove sa datoteke za spremanje i smanjuje veličinu memorije koju koristi ova datoteka.
- Naredba za Spremanje (SAV).
  Ova naredba sprema kopiju jednog ili više objekata koji se mogu upotrebljavati u integriranom sistemu datoteka.—Kad se upotrebljava ova naredba, možete izgubiti potpis sa objekata naredbi (*CMD) na mediju za spremanje ako navedete vrijednost raniju od V5R2M0 za parametar TGTRLS. Gubitak potpisa se dešava jer objekti naredbi ne mogu biti potpisani u izdanjima ranijim od V5R2.
- Naredba za Spremanje knjižnice (SAVLIB).
  Ova naredba omogućuje spremanje kopije jedne ili više knjižnica. Kad upotrebljavate ovu naredbu, možete izgubiti potpis sa objekata naredbi (*CMD) na mediju za spremanje ako navedete vrijednost raniju od V5R2M0 za parametar TGTRLS. Gubitak potpisa se dešava jer objekti naredbi ne mogu biti potpisani u izdanjima ranijim od V5R2.
- Naredba za Spremanje objekta (SAVOBJ).
  Ova naredba sprema kopiju pojedinačnog objekta ili grupe objekata smještene u istoj knjižnici. Kad upotrebljavate ovu naredbu, možete izgubiti potpis sa objekata naredbi (*CMD) na mediju za spremanje ako navedete vrijednost raniju od V5R2M0 za parametar TGTRLS. 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 tih sistemskih vrijednosti, **provjeravanje potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST)** , određuje kako sistem rukuje potpisanim objektima kad ih vraća. Postavka koju izaberete za ovu sistemsku vrijednost dopušta određivanje kako postupak vraćanja rukuje sa provjerom objekata bez potpisa ili sa nevažećim potpisima.

Neke naredbe za spremanje i vraćanje utječu na potpisane objekte ili određuju kako sistem rukuje sa potpisanim i nepotpisanim objektima za vrijeme operacija spremanja i vraćanja. Trebate shvatiti da trebate biti oprezni sa tim naredbama i njihovim utjecajem na potpisane objekte tako da možete bolje upravljati sistemom i izbjegavati potencijalne probleme koji se mogu desiti.

Ove naredbe mogu provjeravati potpise na objektima za vrijeme operacija spremanja i vraćanja:

- Naredba za Spremanje licenciranog programa (SAVLICPGM).
- Naredba Vraćanje (RST).
- Naredba Vraćanje knjižnice (RSTLIB).
- Naredba za Vraćanje licenciranog programa (RSTLICPGM).
- Naredba za Vraćanje objekta (RSTOBJ).

Ove naredbe omogućuju spremanje i vraćanje memorija certifikata; memorije certifikata su sigurnosno osjetljivi objekti koji sadrže certifikate koje upotrebljavate za potpisivanje objekata i provjeru potpisa:

- Naredba za Spremanje (SAV).
- Naredba za Spremanje sigurnosnih podataka (SAVSECDTA).
- Naredba za Spremanje sistema (SAVSYS).
- Naredba za Vraćanje (RST).
- Naredba za Vraćanje korisničkih profila (RSTUSRPRF).

Neke naredbe za spremanje, ovisno o vrijednostima parametara koje upotrebljavate, mogu izgubiti potpis sa objekta na mediju za spremanje, poništavajući time sigurnost koju pruža potpis. Na primjer, *svaka* operacija spremanja koja se odnosi na objekt naredbe (*CMD) sa ciljnim izdanjem ranijim od V5R2M0 uzrokuje spremanje naredbe bez potpisa. Uklanjanje potpisa može uzrokovati probleme sa objektima na koje se utječe. U najboljem slučaju, nećete više moći provjeravati pouzdanost izvora objekta i nećete moći provjeravati potpis da otkrijete promjene na objektu. Ove naredbe trebate upotrebljavati samo na onim potpisanim objektima koje ste kreirali (a ne na potpisanim objektima koje ste dobili od drugih kao IBM-a ili prodavača)

Bilješka: Da provjerite da li je naredba Spremi izgubila objektov potpis, morate vratiti objekt u knjižnicu različitu od one od 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 te mogućnosti za sljedeće određene naredbe za spremanje, kao i općenito za naredbe za spremanje:

- Naredba za Spremanje (SAV).
- Naredba za Spremanje knjižnice (SAVLIB).
- Naredba za 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-jeve 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 je objekt vraćen ili instaliran na sistemu, na primjer upotrebom naredbe RSTLIB.

Možete izabrati jednu od triju 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. Provjeravanje potpisa za svaku od ovih naredbi kontrolira parametar CHKSIG. Taj parametar omogućuje provjeru kod svih tipova objekata koji se mogu potpisati, potpise, zanemari sve potpise ili provjeri samo one objekte koji imaju potpise. Ova zadnja opcija je defaultna vrijednost za parametar.

Naredba za provjeru cjelovitosti objekta (CHKOBJITG)

Naredba za Provjeru 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 korisiničke profile, objekte koji se podudaraju sa 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 sa podacima u objektu kad je bio potpisan. Određivanje nevažećeg potpisa se osniva na usporedbi šifriranog matematičkog zbroja koji se kreira kad se objekt potpisuje i šifriranog

matematičkog zbroja učinjenog 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 povredu cjelovitosti za objekt, ona dodaje ime objekta, ime knjižnice (ili ime staze), tip objekta, vlasnika objekta i tip ili grešku datoteke 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 su potpisivi ali nemaju digitalni potpis, objekti koji se ne mogu provjeravati i objekti u obliku koji zahtjeva promjene da se može koristiti na trenutnoj sistemskoj implementaciji (konverzija IMPI u RISC).

Vrijednost parametra CHKSIG kontrolira kako naredba rukuje sa digitalnim potpisima na objektima. Možete navesti jednu od triju vrijednosti za ovaj parametar:
- *SIGNED – Kad navedete ovu vrijednost, naredba provjerava objekte sa digitalnim potpisima. Naredba kreira unos dnevnika za svaki objekt sa 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 sa potpisom koji nije važeći.
- *NONE – Kad navedete ovu vrijednost, naredba ne provjerava digitalne potpise na objektima.

Naredba za Provjeru opcije proizvoda (CHKPRDOPT)

Naredba za Provjeru Opcije proizvoda CHKPRDOPT izvještava o razlici između ispravne strukture i stvarne strukture softverskog proizvod. Na primjer, naredba izvještava o greški ako je objekt izbrisan sa instaliranog proizvoda.

Vrijednost parametra CHKSIG kontrolira kako naredba rukuje sa digitalnim potpisima na objektima. Možete navesti jednu od triju vrijednosti za ovaj parametar:
- *SIGNED – Kad navedete ovu vrijednost, naredba provjerava objekte sa digitalnim potpisima. Naredba provjerava potpise na svakom potpisanom objektu. Ako naredba odluči da potpis na objektu nije važeći, naredba pošalje 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 sa 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 za Spremanje licenciranog programa (SAVLICPGM)

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

Vrijednost parametra CHKSIG kontrolira kako naredba rukuje sa digitalnim potpisima na objektima. Možete navesti jednu od triju vrijednosti za ovaj parametar:
- *SIGNED – Kad navedete ovu vrijednost, naredba provjerava objekte sa 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 poruku dnevniku posla o svakom potpisivom objektu koji nema potpis; međutim, postupak spremanja 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.

Rješavanje problema kod potpisanih objekata

Možete upotrebljavati sljedeće tablice da nađete informacije koje vam pomažu rješavati neke od uobičajenijih problema koje možete susresti radeći sa sposobnostima potpisivanja i provjeravanja iSeries objekata.

Uobičajeni problemi potpisivanja objekata

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

Uobičajeni problemi provjere potpisa

Problem	Moguće rješenje
Postupak vraćanja ne uspjeva za objekte bez potpisa.	Ako pomanjkanje potpisa nije problem, provjerite da li je sistemska vrijednost QVFYOBJRST postavljena na 5. Vrijednost 5 navodi da se nepotpisani objekti ne mogu vratiti. Promijenite vrijednost na 3 i pokušajte vraćanje ponovo.
Postupak vraćanja ne uspjeva za objekte sa potpisima.	To se može desiti ako se memorija certifikata *SIGNATUREVERIFICATION prenijela u sistem i DCM se nije upotrijebio za promjenu njene lozinke. U takvom slučaju, certifikati, koje sadrži memorija, ne mogu se upotrijebiti za provjeru potpisa na objektima za vrijeme postupka vraćanja. Upotrijebite DCM za promjenu lozinke za memoriju certifikata. Ako ne znate lozinku, morati ćete izbrisati memoriju certifikata; ponovo je kreirajte i upotrijebite DCM da promijenite lozinku.
Kod vraćanja ili instaliranja proizvoda, dobivate grešku jer potpis ne uspjeva provjeriti.	Kad potpis objekta ne uspije ispravno provjeriti, greška može značiti da se objekt promijenio od kad je bio potpisan. Ako je u pitanju cjelovitost objekta, ne smijete promijeniti sistemsku vrijednost QVFYOBJRST ili obaviti druge akcije koje mogu omogućiti vraćanje sumnjivog objekta. Ako se to učini može se zaobići sigurnost koju pruža provjera potpisa i omogućiti postojanje štetnog objekta na sistemu. Umjesto toga, trebate kontaktirati potpisnika objekta da odredi poduzeti prikladnu akciju za rješavanje problema.

Srodne 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 Wired Network Security: OS/400 V5R1 DCM i Kriptografička proširenja**

  SG24-6168 
  Ova IBM Redbook fokusira se na V5R1 proširenja sigurnosti mreže. Redbook obrađuje mnoga poglavlja uključujući način upotrebe sposobnosti potpisivanja iSeries objekata, Upravitelja digitalnih certifikata (DCM) itd.

Tiskano u Hrvatskoj