System i

Sigurnost
Potpisivanje objekata i provjera potpisa

Verzija 6 Izdanje 1

System i

Sigurnost
Potpisivanje objekata i provjera potpisa

Verzija 6 Izdanje 1

Napomena

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene”, na stranici 45.

Ovo izdanje se primjenjuje na verziju 6, izdanje 1, modifikaciju 0 za IBM i5/OS (broj proizvoda 5761-SS1) i na sva sljedeća izdanja i modifikacije dok se drukčije ne označi u novim izdanjima. Ova verzija ne radi na svim modelima računala smanjenog seta instrukcija (RISC) niti ne radi na CISC modelima.

Sadržaj

Potpisivanje objekata i provjera potpisa

Saznajte o i5/OS sigurnosnim sposobnostima potpisivanja objekta i provjeru potpisa koje možete koristiti za osiguranje integriteta objekata. Naučite kako možete koristiti jednu od nekoliko i5/OS metoda za kreiranje digitalnih potpisa na objektima za identifikaciju izvora objekta i osigurajte način za otkrivanje promjena na objektu. Također, naučite kako poboljšati sigurnost na sistemu provjerom digitalnih potpisa na objektima, uključujući objekte operativnog sistema, da biste odredili da li su nastale promjene nad sadržajima objekata nakon potpisivanja.

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

Potpisivanje objekta i provjeru potpisa možete primijeniti pomoću:

- API-ja za potpisivanje objekata i programske provjere potpisa na objektima.
- Upravitelja digitalnih certifikata za potpisivanje objekata i za gledanje ili provjeru potpisa objekata.
- iSeries Navigator Središnjeg upravljanja za potpisivanje objekata kao dio distributivnog paketa za korištenje drugih sistema.
- CL naredbe, kao Provjera integriteta objekta (CHKOBJITG) za provjeru potpisa.

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

Bilješka: Korištenjem primjera koda, slažete se s uvjetima “Informacije o odricanju od koda” na stranici 43.

Što je novo za V6R1

Pročitajte o promijenjenim informacijama u zbirci poglavlja Potpisivanje objekata i provjera potpisa.

Provjera integriteta funkcije za provjeru koda

Počevši od V6R1, možete provjeriti Licencni interni kod (LIC) upotrebom API-ja Provjera sistema (QydoCheckSystem) ili naredbe Provjera integriteta objekta (CHKOBJITG).

Kako vidjeti što ima novo ili je promijenjeno

Da vam pomogne da vidite gdje su napravljene tehničke promjene, informacijski centar koristi:

- Sliku » da označi gdje nova ili promijenjena informacija počinje.
- Sliku « da označi gdje nova ili promijenjena informacija završava.

U PDF datotekama možete vidjeti revizijske trake (|) na lijevoj margini, uz nove ili promijenjene informacije.

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

PDF datoteka za Potpisivanje objekata i provjeru potpisa

Koristite ove informacije za ispis cijelog poglavlja za i5/OS potpisivanje objekata i provjeru potpisa u obliku PDF datoteke.

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

Spremanje PDF datoteka:

Da spremite PDF na vašu radnu stanicu za gledanje ili ispis:

1. Desno kliknite na PDF vezu u vašem pretražitelju.
2. Kliknite opciju koja sprema lokalno PDF.
3. Izaberite direktorij u koji želite spremiti PDF.
4. Kliknite **Spremi**.

Spuštanje Adobe Acrobat Readera

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

Koncepti potpisivanja objekata

Ovo poglavlje sadrži koncept i upute za i5/OS digitalne potpise i opis kako radi potpisivanje i provjera potpisa za i5/OS objekte.

Prije početka korištenja sposobnosti potpisivanja objekta i provjere potpisa, pomoći će vam pregled nekih od ovih koncepata:

Digitalni potpisi

Ovo poglavlje sadrži informacije o tome što su i5/OS digitalni potpisi i kakvu zaštitu oni osiguravaju.

i5/OS daje podršku za upotrebu digitalnih certifikata za digitalno ″potpisivanje″ objekata. Digitalni potpis na objektu se kreira u šifriranom obliku i sličan je osobnom potpisu na pisanom dokumentu. Digitalni potpis pruža dokaz porijekla objekta i sredstvo za provjeru cjelovitosti objekta. Vlasnik digitalnog certifikata ″potpisuje″ objekt pomoću privatnog ključa certifikata. Primatelj objekta upotrebljava odgovarajući javni ključ certifikata za dešifriranje potpisa, čime se provjerava cjelovitost potpisanog objekta i provjerava pošiljatelja kao izvor.

Podrška za potpisivanje objekata proširuje tradicionalne sistemske alate za kontrolu promjena na objektima. Tradicionalne kontrole ne mogu zaštititi objekt od neovlaštene promjene dok je objekt u tranzitu kroz Internet ili drugu nepouzdanu mrežu. Budući da možete otkriti da li su sadržaji objekta promijenjeni od kad su potpisani, možete lakše odrediti da li je objekt kojeg dobivate u ovakvim slučajevima pouzdan.

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

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

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

certifikata (DCM) za rad s vašim vlastitim Lokalnim CA za izdavanje certifikata za potpisivanje objekata. Upotreba privatnih certifikata od Lokalnog CA za potpisivanje objekata je jeftinija od kupovine certifikata od poznatog javnog CA.

Tipovi digitalnih potpisa

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

- **Cijeli potpisi objekta** Ovaj tip potpisa uključuje sve osim nekoliko nepotrebnih bajtova objekta.
- **Potpisi jezgre objekta** Ovaj tip potpisa uključuje bitne bajtove *CMD objekta. Međutim, potpis ne sadrži one bajtove koji su podložni češćim promjenama. Ovaj tip potpisa omogućuje izvođenje nekih promjena na naredbi bez poništenja potpisa. Koje bajtove potpis jezgre objekta ne sadrži ovisi o specifičnim *CMD objektima. Na primjer potpisi jezgre ne sadrže defaulte parametara na *CMD objektima. Primjeri promjena koje neće poništiti potpis jezgre objekta uključuju:
  - Promjena defaulta naredbe.
  - Dodavanje programa za provjeru valjanosti naredbe koja ga nema.
  - Promjena parametra Gdje je dozvoljeno izvoditi.
  - Promjena parametra Dozvoli ograničene korisnike.

Srodni koncepti

"Potpisivi objekti"
Ovo poglavlje sadrži informacije o tome koje objekte možete potpisati i o opcijama potpisivanja objekata za i5/OS naredbe (*CMD).

Srodne informacije

Upravitelj digitalnih certifikata (DCM)

Potpisivi objekti

Ovo poglavlje sadrži informacije o tome koje objekte možete potpisati i o opcijama potpisivanja objekata za i5/OS naredbe (*CMD).

Možete digitalno potpisati i5/OS tipove objekata, bez obzira na metodu koje koristite za potpis. Možete potpisati svaki objekt (*STMF) kojeg pohranite u integrirani sistem datoteka, osim objekata koji su pohranjeni u knjižnici. Ako objekt ima pripojen Java program, taj program će se također potpisati. Možete potpisivati samo ove objekte u sistemu datoteka QSYS.LIB: programe (*PGM), pomoćne programe (*SRVPGM), module (*MODULE), SQL pakete (*SQLPKG), *FILE (samo spremanje datoteke) i naredbe (*CMD).

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

Naredbe (*CMD) potpisivanja objekta

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

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

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

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

Sastav jezgre potpisa objekta na *CMD objektima

Dio objekta	Odnos s potpisom jezgre objekta
Defaulti naredbi promijenjeni s CHGCMDDFT	Nisu dio potpisa jezgre objekta
Program za obradu naredbe i knjižnice	Uvijek uključeno kao dio potpisa jezgre objekta
REXX izvorna datoteka i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
REXX izvorni član	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Okolina REXX naredbe i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Ime REXX izlaznog programa, 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
Način u kojem je važeće	Nisu dio potpisa jezgre objekta
Gdje se dozvoljava izvođenje	Nisu dio potpisa jezgre objekta
Dozvoli ograničene korisnike	Nisu dio potpisa jezgre objekta
Knjige pomoći	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Grupa panela pomoći i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Identifikator pomoći	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Indeks traženja pomoći i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Trenutna knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Knjižnica proizvoda	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Program za nadjačavanje prompta i knjižnica	Uključeno ako se navede za naredbu kod potpisivanja, inače nije dio potpisa jezgre objekta
Tekst (opis)	Nije dio niti potpisa jezgre objekta niti potpisa cijelog objekta, jer se ne pohranjuje u objekt
Omogući grafičko korisničko sučelje (GUI)	Nisu dio potpisa jezgre objekta

Srodni koncepti

“Digitalni potpisi” na stranici 2
Ovo poglavlje sadrži informacije o tome što su i5/OS digitalni potpisi i kakvu zaštitu oni osiguravaju.

Obrada potpisivanja objekata

Ovo poglavlje sadrži informacije o tome kako radi obrada potpisivanja objekata na vašem sistemu koji izvodi i5/OS operativni sistem i koje parametre možete postaviti za tu obradu.

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

Obrada greške
Možete navesti koji tip obrade greške aplikacija koristi kada kreira potpise na više od jednog objekta. Možete navesti da aplikacija zaustavi potpisivanje objekata kad se desi greška ili da nastavi potpisivanje drugih objekata u obradi.

Dupliciranje potpisa objekta
Možete navesti kako aplikacija rukuje obradom potpisivanja kada aplikacija ponovno potpisuje objekt. Možete navesti da li ostaviti originalni potpis na mjestu ili zamijeniti originalni potpis s novim potpisom.

Objekti u poddirektorijima
Možete navesti kako aplikacija treba rukovati potpisivanjem objekata u poddirektorijima. Možete navesti da aplikacija pojedinačno potpisuje objekte u svakom poddirektoriju ili da aplikacija samo potpisuje one objekte u glavnom direktoriju zanemarujući sve poddirektorije.

Opseg potpisa objekta
Kad potpisujete objekte *CMD, možete navesti da li potpisati cijeli objekt ili potpisati samo jezgru objekta.

Obrada provjere potpisa

Naučite kako i5/OS radi provjeru potpisa objekta i koje parametre možete postaviti za tu obradu.

Možete navesti sljedeće opcije za obradu provjere potpisa.

Obrada greške
Možete navesti koji tip obrade greške aplikacija koristi kada provjerava potpise na više od jednog objekta. Možete navesti da aplikacija zaustavi provjeru potpisa kad se desi greška ili da nastavi provjeru potpisa drugih objekata u obradi.

Objekti u poddirektorijima
Možete navesti kako aplikacija treba rukovati provjerom potpisa objekata u poddirektorijima. Možete navesti da aplikacija pojedinačno provjerava objekte u svakom poddirektoriju ili da aplikacija provjerava samo potpise za one objekte u glavnom direktoriju zanemarujući sve poddirektorije.

Provjera potpisa jezgre protiv provjere potpisa cijelog objekta
Postoje sistemska pravila koja određuju kako sistem rukuje potpisima jezgre i cijelog objekta za vrijeme obrade provjere. Ta pravila su sljedeća:

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

Funkcija provjere integriteta provjere koda

Ovo poglavlje sadrži informacije o tome kako možete provjeriti integritet funkcije provjere koda koju koristite za provjeru integriteta vašeg sistema koji izvodi i5/OS operativni sistem.

U V5R2, i5/OS se otpremao s funkcijom provjere koda koju ste mogli koristiti za provjeru integriteta potpisanih objekata na vašem sistemu, uključujući sav kod operativnog sistema koji IBM otprema i potpisuje za vaš sistem. Počevši od V5R3, možete koristiti novi API Provjera sistema, za provjeru integriteta same funkcije za provjeru koda, kao i ključnih objekata operativnog sistema. Sada, IBM potpisuje Licencni interni kod (LIC) i možete koristiti API Provjera sistema (QydoCheckSystem) ili naredbu Provjera integriteta objekta (CHKOBJITG) za provjeru LIC-a.

API Provjera sistema (QydoCheckSystem) osigurava provjeru integriteta i5/OS sistema. Ovaj API možete koristiti za provjeru programa (*PGM) i pomoćnih programa (*SRVPGM) i izabranih objekata naredbi (*CMD) u QSYS knjižnici. Dodatno, API Provjera sistema testira naredbu Vraćanje objekta(RSTOBJ), naredbu Vraćanje knjižnice (RSTLIB), naredbu Provjera integriteta objekta (CHKOBJITG) i API Provjera objekta. Ovaj test osigurava da ove naredbe i API izvještavaju o greškama provjere potpisa kada je to prikladno. Na primjer, kada objekt koji je dao sistem nije potpisan ili sadrži nevažeći potpis.

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

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

Srodni zadaci

"Provjera integriteta funkcije provjere koda" na stranici 40
Naučite kako provjeriti integritet funkcije provjere koda koju koristite za provjeru i5/OS integriteta sistema.

Scenariji potpisivanja objekata

Pregledajte scenarije koji ilustriraju neke tipične situacije za upotrebu i5/OS sposobnosti za potpisivanje objekata i provjeru potpisa. Svaki scenarij također sadrži konfiguracijske zadatke koje morate izvesti da bi primijenili scenarij kako je opisano.

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

Koju metodu ćete izabrati za upotrebu ovisi o različitim faktorima. Scenariji u ovom poglavlju opisuju neke od uobičajenijih ciljeva potpisivanja objekta i provjere potpisa u tipično poslovnom kontekstu. Svaki scenarij također opisuje sve preduvjete i zadatke koje morate obaviti da primijenite scenarij prema opisu. Pregledajte ove scenarije da naučite kako možete koristiti sposobnosti potpisivanja objekta na način koji najbolje odgovara vašim poslovnim i sigurnosnim potrebama:

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

Ovaj scenarij opisuje poduzeće koje želi potpisati ranjive aplikacijske objekte na svom javnom Web poslužitelju. Oni žele mogućnost lakšeg određivanja postojanja neovlaštenih promjena na ovim objektima. Bazirano na poslovnim potrebama poduzeća i ciljevima sigurnosti, ovaj scenarij opisuje kako se koristi Upravitelj digitalnih certifikata (DCM) kao primarna metoda za upotrebu i5/OS sposobnosti za potpisivanje objekata.

Situacija

Kao administrator za MyCo, Inc. odgovorni ste za upravljanje dvaju sistema vašeg poduzeća. Jedan od tih sistema predstavlja javni Web poslužitelj vašeg poduzeća. Interni proizvodni sistem poduzeća koristite za razvoj sadržaja za javni Web poslužitelj i prijenos datoteka i objekata programa na javni Web poslužitelj nakon testiranja.

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

Istraživali ste i5/OS sposobnosti potpisivanja objekta i saznali da postoji nekoliko metoda koje možete koristiti za potpisivanje objekata i provjeru potpisa objekata. Kako niste odgovorni za upravljanje malim brojem sistema i nemate potrebu za čestim potpisivanjem objekata, odlučili ste koristiti Upravitelj digitalnih certifikata (DCM) za izvođenje ovih zadataka. Također ste odlučili kreirati Lokalnog izdavača certifikata (CA) i upotrebljavati privatni certifikat za potpisivanje objekata. Upotreba privatnog certifikata kojeg je izdao Lokalni CA za potpisivanje objekata ograničava trošak upotrebe sigurnosne tehnologije, jer ne morate kupiti certifikat od poznatog CA.

Ovaj primjer služi kao koristan uvod u korake koji uključuju postavljanje i korištenje potpisivanja objekata ako želite potpisivati objekte na manjem broju sistema.

Prednosti scenarija

Ovaj scenarij ima sljedeće prednosti:

- Potpisivanje objekata pruža sredstvo provjere integriteta ranjivih objekata i lakše određivanje da li su objekti promijenjeni nakon što su bili potpisani. Ovim se mogu smanjiti neka rješavanja problema koje ćete raditi u budućnosti za praćenje aplikacija i drugih sistemskih problema.
- Upotrebom DCM-ovog grafičkog korisničkog sučelja za potpisivanje objekata i provjeru potpisa objekata dozvoljava se vama i drugima u poduzeću da lagano i brzo obavljate zadatke.
- Upotreba DCM-a za potpisivanje objekata i provjeru potpisa objekata smanjuje vrijeme koje morate utrošiti za učenje i upotrebu potpisivanja objekta kao dijela sigurnosne strategije.
- Upotreba certifikata kojeg je izdao Lokalni izdavač certifikata (CA) za potpisivanje objekata pojeftinjuje primjenu potpisivanja objekata.

Ciljevi

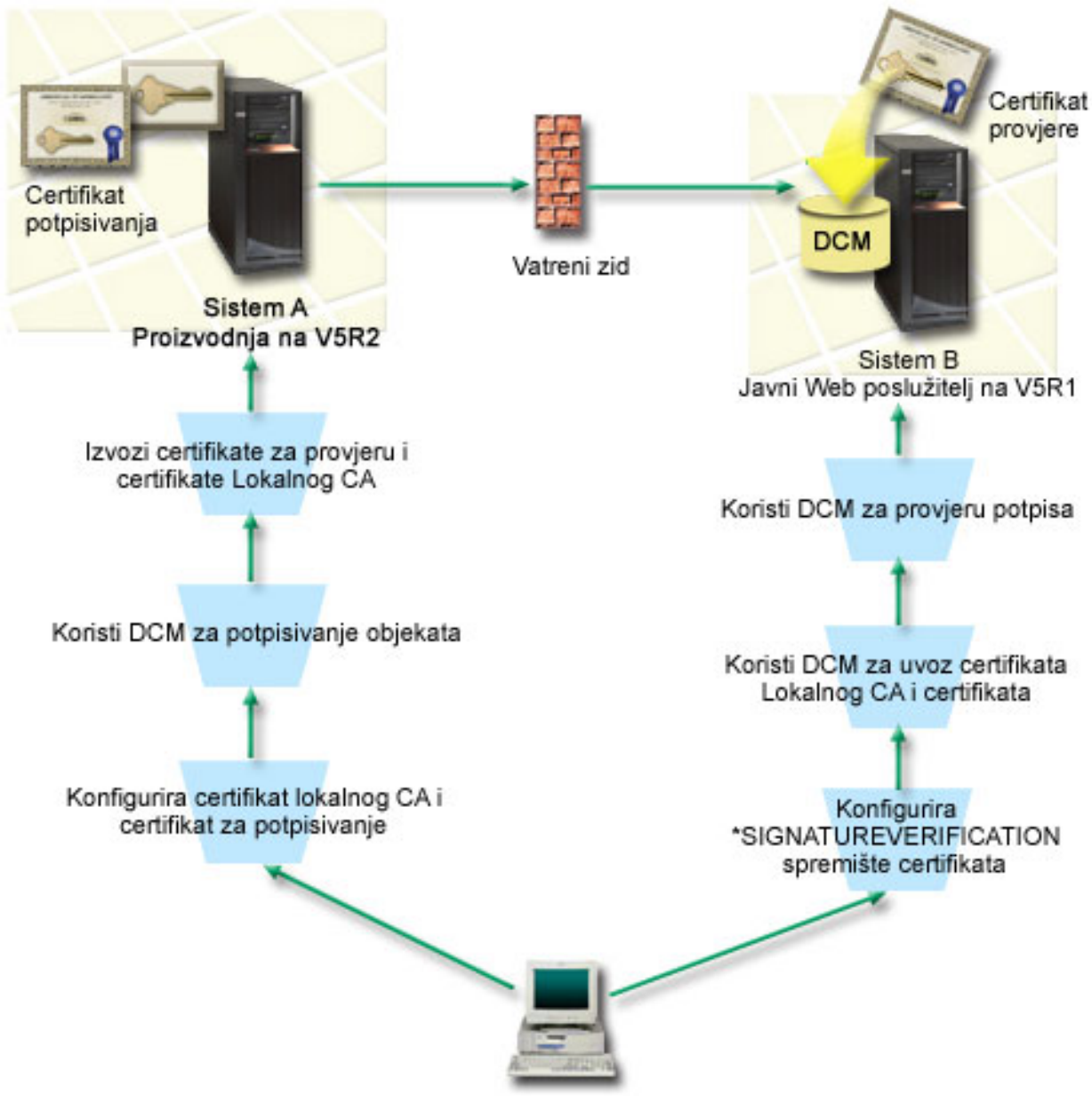
U ovom scenariju, želite digitalno potpisati ranjive objekte, kao što su cgi-bin programi koji generiraju obrasce, na javnom poslužitelju poduzeća. Kao sistemski administrator pri MyCo, Inc, želite koristiti Upravitelja digitalnog certifikata (DCM) za potpisivanje ovih objekata i provjeru potpisa na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

Ciljevi ovog scenarija su sljedeći:

- Aplikacije poduzeća i drugi ranjivi objekti na javnom Web poslužitelju (Sistem B) moraju se potpisati s certifikatom iz Lokalne CA za ograničavanje troškova potpisivanja aplikacija.
- Sistemski administratori i ostali korisnici moraju lako provjeravati digitalne potpise na sistemima za provjeru izvora i valjanosti potpisanih objekata poduzeća. Da bi vam ovo uspjelo, svaki sistem mora imati kopiju certifikata provjere potpisa poduzeća i certifikata Lokalnog Izdavača certifikata u svakom *SIGNATUREVERIFICATION spremištu certifikata.
- Provjerom potpisa na aplikacijama poduzeća i ostalim objektima, administratori i ostali mogu otkriti da li je sadržaj objekata promijenjen u odnosu na vrijeme kad su potpisani.
- Sistemski administrator mora upotrebljavati DCM za potpisivanje objekata; sistemski administrator i drugi moraju moći upotrebljavati DCM za provjeru potpisa objekata.

Detalji

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



Slika ilustrira sljedeće točke relevantne za ovaj scenarij:

Sistem A

- Sistem A je System i model koji izvodi OS/400 Verziju 5 Izdanje 2 (V5R2).
- Sistem A je interni, proizvodni sistem poduzeća i razvojna platforma za javni System i Web poslužitelj (Sistem B).
- Sistem A ima instaliran 128-bitni Dobavljač kriptografskog pristupa System i (5722–AC3).
- Sistem A ima instalirano i konfigurirano Upravitelja digitalnih certifikata (opcija 34) i IBM HTTP Server (5722–DG1).
- Sistem A ponaša se kao Lokalni Izdavač certifikata (CA) i na njemu se nalazi certifikat potpisivanja objekta.

- Sistem A koristi DCM za potpisivanje objekata i on je primarni sistem za potpisivanje objekata za javne aplikacije poduzeća i za druge objekte.
- Sistem A je konfiguriran za omogućavanje provjere potpisa.

Sistem B

- Sistem B je System i model koji izvodi OS/400 Verziju 5 Izdanje 1 (V5R1).
- Sistem B je vanjski javni Web poslužitelj poduzeća izvan vatrozida poduzeća.
- Sistem B ima instaliran Dobavljač kriptografskog pristupa 128-bitni (5722–AC3).
- Sistem B ima instalirano i konfigurirano Upravitelja digitalnih certifikata (opcija 34) i IBM HTTP Server (5722–DG1).
- Sistem B ne radi kao Lokalni CA, niti ne potpisuje objekte.
- Sistem B je konfiguriran za omogućavanje provjere potpisa korištenjem DCM-a za kreiranje *SIGNATUREVERIFICATION spremišta certifikata i import potrebne provjere i certifikata Lokalnog CA.
- DCM se koristi za provjeru potpisa objekata.

Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:

1. Svi sistemi odgovaraju zahtjevima za instaliranje i koriste Upravitelj digitalnih certifikata (DCM).
2. Nitko nije prethodno konfigurirao ili koristio DCM na ovim sistemima.
3. Svi sistemi imaju instalirani najviši nivo Cryptographic Access Provider 128-bit licencnog programa (5722-AC3).
4. Default postavka za provjeru potpisa objekata za vrijeme obnavljanja (QVFYOBJRST) sistemske vrijednosti na svim sistemima scenarija je 3 i nije se mijenjala. Default postavka osigurava da sistem može provjeriti potpise objekata kad vratite potpisane objekte.
5. Mrežni administrator Sistema A za potpisivanje objekata mora imati posebno ovlaštenje korisničkog profila *ALLOBJ, ili korisnički profil mora biti ovlašten od strane aplikacije potpisivanja objekta.
6. Sistemski administrator ili bilo tko, tko kreira spremište certifikata u DCM-u, mora imati posebna ovlaštenja *SECADM i *ALLOBJ.
7. Sistemski administratori ili ostali na svim ostalim sistemima za provjeru potpisa objekta moraju imati posebno ovlaštenje korisničkog profila *AUDIT.

Koraci konfiguracijskog zadatka

Postoje dva skupa zadataka koje morate dovršiti za implementaciju scenarija: Jedan skup zadataka vam omogućava da konfigurirate Sistem A kao Lokalnog Izdavača certifikata (CA) i da potpišete i provjerite potpise objekata. Drugi skup zadataka omogućava konfiguriranje Sistema B za provjeru potpisa objekta koje kreira Sistem A.

Pogledajte poglavlje s detaljima scenarija za dovršavanje ovih koraka.

Koraci zadatka za Sistem A

Morate dovršiti svaki od ovih zadataka na Sistemu A za kreiranje privatnog Lokalnog CA i za potpisivanje objekata i provjeru potpisa objekta kao što opisuje ovaj scenarij:

1. Dovršite sve korake preduvjeta za instalaciju i konfiguriranje svih potrebnih System i proizvoda
2. DCM koristite za kreiranje Lokalnog Izdavača certifikata (CA) za izdavanje certifikata potpisivanja objekta.
3. DCM koristite za kreiranje definicije aplikacije
4. DCM koristite za dodjelu certifikata definiciji aplikacije za potpisivanje objekata
5. DCM koristite za potpisivanje cgi-bin programskih objekata
6. DCM koristite za eksportiranje certifikata koji mogu koristiti ostali sistemi za provjeru potpisa objekata. Morate eksportirati kopiju certifikata Lokalnog CA i kopiju certifikata potpisivanja objekta kao certifikat provjere potpisa u datoteku.

7. Prenesite datoteke certifikata na javni poslužitelj poduzeća (Sistem B) tako da vi i drugi možete provjeriti potpise koje kreira Sistem A

Koraci zadatka za Sistem B

Ako namjeravate obnoviti potpisane objekte koje ste prenijeli na javni Web poslužitelj u ovom scenariju (Sistem B), trebate dovršiti ove zadatke konfiguracije provjere potpisa na Sistemu 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 Sistemu B, morate dovršiti sljedeće zadatke za provjeru potpisa objekata kao što opisuje ovaj scenarij:

1. Koristite Upravitelj digitalnih certifikata (DCM) za kreiranje *SIGNATUREVERIFICATION spremišta certifikata
2. DCM koristite za import Lokalnog CA certifikata i certifikata provjere potpisa
3. DCM koristite za provjeru potpisa na prenesenim objektima

Srodne informacije

Upravitelj digitalnih certifikata (DCM)

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

Dovršite sljedeće zadatke za konfiguriranje i upotrebu Upravitelja digitalnih certifikata za potpisivanje i5/OS objekata, prema opisu u ovom scenariju.

Korak 1: Dovršite sve korake preduvjeta

Morate dovršiti sve preduvjetne zadatke za instaliranje i konfiguriranje svih potrebnih System i proizvoda, prije nego što možete izvoditi specifične konfiguracijske zadatke za primjenu ovog scenarija.

Korak 2: Kreiranje Lokalnog Izdavača certifikata za izdavanje privatnog certifikata za potpisivanje objekata

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

Za korištenje DCM-a za kreiranje i upravljanje lokalnim CA, slijedite ove korake: Sad kada ste kreirali lokalni CA i certifikat potpisivanja objekta, morate definirati aplikaciju za potpisivanje objekata koja će koristiti certifikat prije nego što možete potpisati objekte.

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

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

      Bilješka: Iako ovaj scenarij ne koristi ovaj certifikat, morate ga kreirati prije nego što možete upotrebljavati Lokalni CA za izdavanje potrebnog certifikata za potpisivanje objekata. Ako opozovete zadatak bez

kreiranja certifikata, morate kreirati certifikat za potpisivanje objekata i *OBJECTSIGNING spremište certifikata u kojoj je on odvojeno pohranjen.

e. Izabrati aplikacije koje mogu upotrebljavati certifikat poslužitelja ili klijenta za SSL veze.

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

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

g. Izabrati aplikacije kojima će vaš lokalni CA vjerovati.

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

Korak 3: Kreiranje aplikacijske definicije potpisa 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 ne treba se odnositi na stvarnu aplikaciju. Definicija aplikacije koju kreirate može opisati tip ili grupu objekata koje ste htjeli potpisati. Definiciju trebate da možete imati ID aplikacije za pridruživanje sa certifikatom i da omogućite postupak potpisivanja.

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

1. U navigacijskom okviru, kliknite **Izaberite spremište certifikata** i izaberite ***OBJECTSIGNING** kao spremište certifikata za otvaranje.
2. Kad se prikaže spremište certifikata i stranica lozinke, pribavite lozinku koju ste pri kreiranju naveli za spremište certifikata i kliknite **Nastavi**.
3. U navigacijskom okviru izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
4. Izaberite **Dodavanje aplikacije** iz popisa zadataka da se prikaže obrazac za definiranje aplikacije.
5. Dovršite obrazac i kliknite **Dodaj**.

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

Korak 4: Dodjela certifikata definiciji aplikacije za potpisivanje objekata

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

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

Kad dovršite ovaj zadatak, spremni ste koristiti DCM za potpisivanje programskih objekata koje će koristiti javni Web poslužitelj (Sistem B) poduzeća.

Korak 5: Potpisivanje programskih objekata

Slijedite ove korake za potpisivanje objekata programa koje će koristiti javni Web poslužitelj (Sistem B) poduzeća:

1. U navigacijskom okviru, kliknite **Izbor spremišta certifikata** i izaberite ***OBJECTSIGNING** kao spremište certifikata za otvaranje.
2. Unesite lozinku za *OBJECTSIGNING spremište certifikata i kliknite **Nastavak**.

3. Nakon osvježenja navigacijskog okvira, izaberite **Upravljanje potpisivim objektima** za prikaz popisa zadataka.
4. Iz popisa zadataka izaberite **Potpisivanje objekta** za prikaz popisa definicija aplikacija koje možete koristiti za potpisivanje objekata.
5. Izaberite aplikaciju koju ste definirali prethodnim korakom i kliknite **Potpis objekta**. Prikazat će se obrazac koji vam omogućuje da navedete smještaj objekata koje želite potpisati.
6. U dobiveno polje unesite potpuno kvalificirano ime i stazu datoteke objekta ili direktorija objekata koje želite potpisati i kliknite **Nastavak**. Ili unesite lokaciju direktorija i kliknite **Pregled** da vidite sadržaje direktorija i da izaberete objekte za potpisivanje.

   Bilješka: Morate započeti ime objekta s vodećom kosom crtom ili možete naići na grešku. Možete također koristiti određene generičke znakove za opis direktorija kojeg želite potpisati. Generički znakovi su zvjezdica (*****), koja označava *bilo koji broj znakova* i upitnik (**?**), koji označava *bilo koji pojedinačan znak*. Na primjer, da potpišete sve objekte u specifičnom direktoriju, možete unijeti /mydirectory/*, a da potpišete sve programe u određenoj knjižnici, možete unijeti /QSYS.LIB/QGPL.LIB/*.PGM. Te generičke znakove možete upotrebljavati samo u zadnjem dijelu imena staze; na primjer,/mydirectory*/filename ima za posljedicu poruku o greški. Ako želite koristiti funkciju **Pregled** da vidite popis knjižnica ili sadržaj direktorija, morate unijeti zamjenski znak kao dio imena staze prije nego kliknete **Pregled**.
7. Izaberite opcije obrade koje želite upotrebljavati za potpisivanje izabranog objekta ili objekata i kliknite **Nastavak**.

   Bilješka: Ako odlučite čekati rezultate posla, prikazat će se datoteka rezultata izravno u vašem pretražitelju. Rezultati trenutnog posla se pridodaju kraju datoteke rezultata. Posljedično, datoteka može sadržavati rezultate s prethodnih poslova, u dodatku onima s trenutnog posla. Možete upotrebljavati polje podataka u datoteci da odredite koje se linije u datoteci primjenjuju u trenutnom poslu. Polje podataka je u formatu YYYYMMDD. Prvo polje u datoteci može biti ili ID poruke (ako se dogodila greška u toku obrade objekta) ili polje datuma (pokazuje datum obrade posla).
8. Specificirajte potpuno kvalificirano ime i stazu datoteke za korištenje u pohranjivanju rezultata posla za potpisivanje objekta i kliknite **Nastavak**. Unesite lokaciju direktorija i kliknite **Pregled** da pogledate sadržaje direktorija i da izaberete datoteku za pohranjivanje rezultata posla. Prikazuje se poruka koja pokazuje da je posao poslan na izvođenje za potpis objekata. Za pregled rezultata posla, pogledajte posao **QOBJSGNBAT** u dnevniku poslova.

Da biste osigurali da vi ili drugi možete provjeravati potpise, morate eksportirati potrebne certifikate u datoteku i datoteku certifikata prenijeti na Sistem B. Također, na Sistemu B morate dovršiti sve zadatke konfiguracije provjere potpisa prije prijenosa potpisanih programskih objekata na Sistem B. Konfiguracija provjere potpisa se mora dovršiti prije nego što možete uspješno provjeravati potpise za vrijeme vraćanja potpisanih objekata na sistem B.

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

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

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

Za korištenje DCM kako biste mogli provjeriti potpise na istom sistemu koji potpisuje objekte (u ovom scenariju Sistem A), slijedite ove korake:

1. U navigacijskom okviru kliknite **Kreiranje novog spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za kreiranje.
2. Izaberite **Da** da kopirate postojeće certifikate za potpisivanje objekata u novo spremište certifikata kao certifikate za provjeru potpisa.

3. Odredite lozinku za novo spremište certifikata i kliknite **Nastavak** za kreiranje spremišta certifikata. Sada možete upotrebljavati DCM za provjeru potpisa objekata na istom sistemu koji upotrebljavate za potpisivanje objekata.

Slijedite ove korake kako biste koristili DCM pri eksportiranju kopije Lokalnog CA certifikata i kopiranju certifikata potpisa objekta kao certifikat provjere potpisa da možete provjeriti potpise objekata na drugim sistemima (Sistem B):

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

Sada možete prenijeti ove datoteke na krajnji sistem na kojem namjeravate provjeriti potpise koje ste kreirali s certifikatom.

Korak 7: Prijenos datoteka certifikata na javni poslužitelj poduzeća, Sistem B

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

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

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

Da kreirate *SIGNATUREVERIFICATION spremište certifikata, slijedite ove korake:

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a .
2. U navigacijskom okviru Upravitelja digitalnih certifikata (DCM), izaberite **Kreiranje novog spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za kreiranje.

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

Korak 9: Zadaci provjere potpisa: Import certifikata

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

Za import tih certifikata u *SIGNATUREVERIFICATION pohranu, slijedite ove korake: Sada možete koristiti DCM na Sistemu B za provjeru potpisa objekata koje ste kreirali s odgovarajućim certifikatom potpisa na Sistemu A.

1. U navigacijskom okviru DCM-a kliknite **Izbor spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za otvaranje.
2. Kad se prikaže spremište certifikata i stranica lozinke, pribavite lozinku koju ste pri kreiranju naveli za spremište certifikata i kliknite **Nastavi**.
3. Nakon osvježavanja navigacijskog okvira, izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
4. Iz popisa zadataka izaberite **Import certifikata**.
5. Izaberite **Izdavač certifikata (CA)** kao tip certifikata i kliknite **Nastavak**.

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

Korak 10: Zadaci provjere potpisa: Provjera potpisa programskih objekata

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

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

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

   Bilješka: Ako odlučite čekati rezultate posla, prikazat će se datoteka rezultata izravno u vašem pretražitelju. Rezultati trenutnog posla se pridodaju kraju datoteke rezultata. Posljedično, datoteka može sadržavati

rezultate s prethodnih poslova, u dodatku onima s trenutnog posla. Možete upotrebljavati polje podataka u datoteci da odredite koje se linije u datoteci primjenjuju u trenutnom poslu. Polje podataka je u formatu YYYYMMDD. Prvo polje u datoteci može biti ili ID poruke (ako se dogodila greška u toku obrade objekta) ili polje datuma (pokazuje datum obrade posla).

7. Specificirajte potpuno kvalificirano ime i stazu datoteke za korištenje u pohranjivanju rezultata posla za provjeru potpisa objekta i kliknite **Nastavak**. Unesite lokaciju direktorija i kliknite **Pregled** da pogledate sadržaje direktorija i da izaberete datoteku za pohranjivanje rezultata posla. Prikazuje se poruka koja pokazuje da je posao poslan na izvođenje za provjeru potpisa objekata. Za pregled rezultata posla, pogledajte posao **QOBJSGNBAT** u dnevniku poslova.

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

Ovaj scenarij opisuje poduzeće za razvoj aplikacija koje želi programski potpisivati aplikacije koje prodaje. Oni žele moći uvjeriti svoje korisnike da su aplikacije došle iz njihovog poduzeća i žele im osigurati način za otkrivanje neovlaštenih promjena na aplikacijama kad ih instaliraju. Bazirano na poslovnim potrebama poduzeća i ciljevima sigurnosti, ovaj scenarij opisuje kako se koristi i5/OS API Potpisivanje objekata i i5/OS API Dodavanje provjeravatelja za potpisivanje objekata i provjeru potpisa.

Situacija

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

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

Iako ovi tipovi problema nisu uobičajeni za korisnike, želite uvjeriti korisnike da su aplikacije koje dobivaju od vas stvarno iz 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 istraživanja, odlučili ste da za ostvarenje sigurnosnih ciljeva, možete koristiti i5/OS sposobnosti potpisivanja objekata. Digitalno potpisivanje aplikacija dopušta korisnicima da provjere da je vaše poduzeće legitimni izvor aplikacije koju primaju ili učitavaju. Budući da trenutno programski pakirate aplikacije, odlučili ste da možete upotrebljavati API-je za lako dodavanje potpisivanja objekta vašoj postojećoj obradi pakiranja. Također odlučujete upotrijebiti javni certifikat za potpisivanje objekata tako da možete napraviti obradu provjere potpisa transparentnom za vaše korisnike kad instaliraju vaš proizvod.

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

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

Prednosti scenarija

Ovaj scenarij ima sljedeće prednosti:

- Upotreba API-ja za pakiranje i programsko potpisivanje objekata skraćuje vrijeme koje morate utrošiti za primjenu ove sigurnosti.
- Upotreba API-ja za potpisivanje objekata kad ih pakirate smanjuje broj koraka koje morate obaviti za potpisivanje objekata, jer je postupak potpisivanja dio postupka pakiranja.

- Potpisivanje paketa objekata omogućuje da lakše odredite da li su objekti promijenjeni nakon što su bili potpisani. Ovim se mogu smanjiti neka rješavanja problema koja ćete raditi u budućnosti za praćenje problema aplikacija za korisnike.
- Upotreba certifikata od javnog poznatog Izdavača certifikata (CA) za potpisivanje objekta dopušta upotrebu API-ja za dodavanje provjeritelja kao dijela izlaznog programa u programu za instalaciju proizvoda. Upotreba ovog API-ja omogućuje dodavanje javnog certifikata kojeg ste upotrebljavali za automatsko potpisivanje aplikacije na korisnički sistem. Time se osigurava da je provjera potpisa transparentna za vašeg korisnika.

Ciljevi

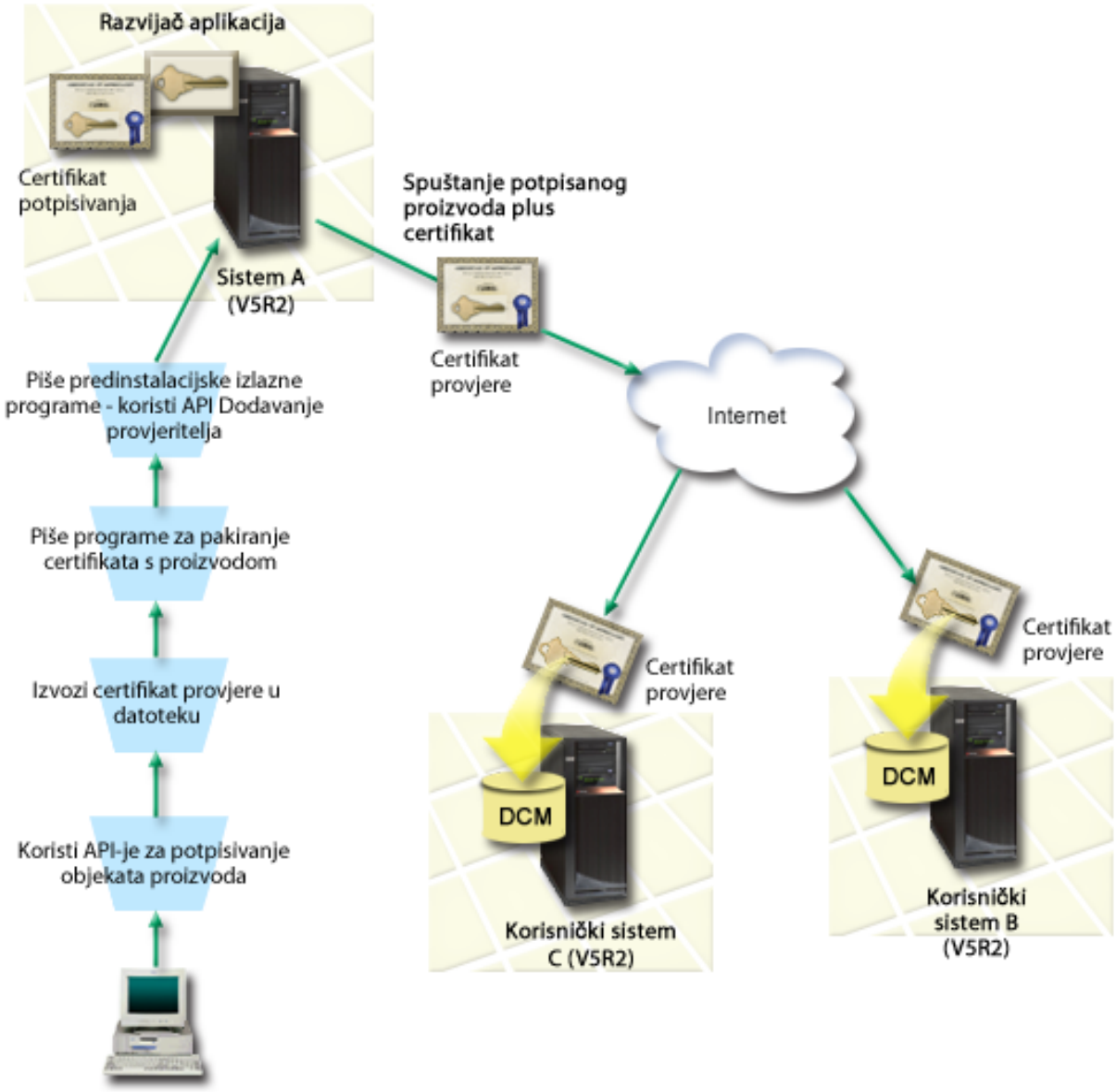
U ovom scenariju, MyCo, Inc. želi programski potpisivati aplikacije koje pakira i distribuira svojim korisnicima. Kao razvijač proizvodnje aplikacija pri MyCo, Inc, trenutno aplikacije vašeg poduzeća pakirate programski za distribuciju korisnicima. Želite koristiti sistemske API-je za potpisivanje aplikacija i želite da korisnički sistem automatski provjeri potpis za vrijeme instalacije proizvoda.

Ciljevi ovog scenarija su sljedeći:

- Razvijač proizvoda poduzeća mora moći potpisivati objekte pomoću API-ja za Potpisivanje objekata kao dio postojećeg postupka za programsko pakiranje aplikacija.
- Aplikacije poduzeća moraju se potpisivati s javnim certifikatom da se osigura transparentnost postupka provjere potpisa za korisnika za vrijeme postupka instalacije proizvoda aplikacije.
- Poduzeće mora moći koristiti sistemske API-je za programsko dodavanje potrebnog certifikata provjere potpisa *SIGNATUREVERIFICATION spremištu certifikata korisničkog sistema. Poduzeće mora biti u mogućnosti programski kreirati spremište certifikata na korisničkom sistemu kao dio instalacijskog procesa ako on već ne postoji.
- Korisnici moraju moći lako provjeriti digitalne potpise na aplikaciji poduzeća nakon instalacije proizvoda. Korisnici moraju moći provjeriti potpis tako da mogu utvrditi izvor i vjerodostojnost potpisane aplikacije kao i odrediti da li je napravljena promjena na aplikaciji od kad je potpisana.

Detalji

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



Slika ilustrira sljedeće točke relevantne za ovaj scenarij:

Središnji sistem A

- Sistem A je System i model koji izvodi OS/400 Verziju 5 Izdanje 2 (V5R2).
- Sistem A izvodi aplikacijski program pakiranja proizvoda razvijača.
- Sistem A ima instaliran 128-bitni Dobavljač kriptografskog pristupa System i (5722–AC3).
- Sistem A ima instalirano i konfigurirano Upravitelja digitalnih certifikata (opcija 34) i IBM HTTP Server (5722–DG1).
- Sistem A je primarni sistem za potpisivanje objekata za aplikativne proizvode poduzeća. Potpisivanje objekta proizvoda za distribuciju korisnicima se postiže izvođenjem ovih zadataka na Sistemu A:
  1. Upotreba API-ja za potpisivanje proizvoda aplikacije poduzeća.

2. Upotreba DCM-a za eksportiranje certifikata provjere potpisa u datoteku tako da korisnici mogu provjeravati potpisane objekte.
3. Pisanje programa za dodavanje certifikata provjere potpisanom aplikacijskom proizvodu.
4. Pisanje predinstalacijskog izlaznog programa za proizvod koji upotrebljava API za Dodavanje provjeritelja. Ovaj API instalacijskom procesu za proizvod omogućava programsko dodavanje provjere certifikata u spremištu certifikata *SIGNATUREVERIFICATION korisničkog sistema (Sistemi B i C).

Korisnički sistemi B i C

- Sistem B je System i model koji izvodi OS/400 Verziju 5 Izdanje 2 (V5R2) ili neko kasnije izdanje od i5/OS.
- Sistem C je System i model koji izvodi OS/400 Verziju 5 Izdanje 2 (V5R2) ili neko kasnije izdanje od i5/OS.
- Sistemi B i C imaju konfiguriran i instaliran Digital Certificate Manager (opcija 34) i IBM HTTP poslužitelj (5722–DG1).
- Sistem B i C kupuju i spuštaju aplikaciju s Web stranice poduzeća za razvoj aplikacije (koja posjeduje Sistem A).
- Sistemi B i C dobivaju kopiju MyCo-ovog certifikata provjere potpisa kad instalacijski proces MyCo aplikacije kreira *SIGNATUREVERIFICATION spremište certifikata na svakom od ovih korisničkih sistema.

Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:

1. Svi sistemi odgovaraju zahtjevima za instaliranje i koriste Upravitelj digitalnih certifikata (DCM).

   Bilješka: Preduvjeti za instaliranje i korištenje DCM-a opcijski je zahtjev korisnicima (Sistemi B i C u ovom scenariju). Iako API za Dodavanje provjeritelja kreira *SIGNATUREVERIFICATION spremište certifikata kao dio postupka instalacije proizvoda, ako je potrebno, on je kreira s defaultnom lozinkom. Korisnici trebaju upotrebljavati DCM za promjenu defaultne lozinke da zaštite ovo spremište certifikata od neovlaštenog pristupa.
2. Nitko nije prethodno konfigurirao ili koristio DCM na ovim sistemima.
3. Svi sistemi imaju instalirani najviši nivo Cryptographic Access Provider 128-bit licencnog programa (5722-AC3).
4. Default postavka za provjeru potpisa objekata za vrijeme obnavljanja (QVFYOBJRST) sistemske vrijednosti na svim sistemima scenarija je 3 i nije se mijenjala. Default postavka osigurava da sistem može provjeriti potpise objekata kad vratite potpisane objekte.
5. Mrežni administrator za Sistem A mora imati korisnički profil s *ALLOBJ posebnim ovlaštenjem da bi mogao potpisivati objekte ili korisnički profil mora biti ovlašten za aplikaciju potpisivanja objekata.
6. Sistemski administrator ili bilo tko (uključujući program), tko kreira spremište certifikata u DCM-u, mora imati posebna ovlaštenja *SECADM i *ALLOBJ.
7. Sistemski administratori ili ostali na svim ostalim sistemima za provjeru potpisa objekta moraju imati posebno ovlaštenje korisničkog profila *AUDIT.

Koraci konfiguracijskog zadatka

Za potpisivanje objekata kao što je opisano u ovom scenariju, pogledajte poglavlje s detaljima scenarija za korake za dovršavanje svakog pojedinog zadatka na Sistemu A :

1. Dovršite sve korake preduvjeta za instalaciju i konfiguriranje svih potrebnih System i proizvoda
2. DCM koristite za kreiranje zahtjeva certifikata za dobivanje certifikata za potpisivanje objekta od poznatog, javnog Izdavača certifikata (CA)
3. DCM koristite za kreiranje definicije aplikacije za potpisivanje objekata
4. DCM koristite za import certifikata za potpisivanje potpisanog objekta i njegovu dodjelu definiciji aplikacije za potpisivanje objekata
5. DCM koristite za eksport certifikata za potpisivanje objekata kao certifikata za provjeru potpisa da bi ga mogli koristiti korisnici za provjeru potpisa aplikacijskih objekata
6. Ažurirajte program pakiranja aplikacija da se koristi API Potpisivanje objekta za potpisivanje aplikacije

7. Kreirajte predinstalacijski program izlaza koji koristi API Dodavanje provjere kao dio procesa pakiranja aplikacije. Ovaj program omogućuje kreiranje *SIGNATUREVERIFICATION spremišta certifikata i dodaje potrebni certifikat provjere potpisa korisničkom sistemu za vrijeme instalacije proizvoda.
8. Korisnici bi trebali koristiti DCM za ponovno postavljanje default lozinke *SIGNATUREVERIFICATION spremišta certifikata sistema

Srodne informacije

Upravitelj digitalnih certifikata (DCM)

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

Dovršite sljedeće korake zadataka za upotrebu i5/OS API-ja za potpisivanje objekata kako opisuje ovaj scenarij.

Korak 1: Dovršite sve korake preduvjeta

Morate dovršiti sve preduvjetne zadatke za instaliranje i konfiguriranje svih potrebnih System i proizvoda, prije nego što možete izvoditi specifične konfiguracijske zadatke za primjenu ovog scenarija.

Korak 2: DCM koristite za dobivanje certifikata iz javnog, poznatog CA

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

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

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

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

Korak 3: Kreiranje definicije potpisa objekta

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

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

1. U navigacijskom okviru, kliknite **Izaberite spremište certifikata** i izaberite ***OBJECTSIGNING** kao spremište certifikata za otvaranje.
2. Kad se prikaže spremište certifikata i stranica lozinke, pribavite lozinku koju ste naveli za spremište certifikata i kliknite **Nastavi**.
3. U navigacijskom okviru izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
4. Izaberite **Dodavanje aplikacije** iz popisa zadataka da se prikaže obrazac za definiranje aplikacije.
5. Dovršite obrazac i kliknite **Dodaj**.

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

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

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

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a .
2. U navigacijskom okviru, kliknite **Izaberite spremište certifikata** i izaberite ***OBJECTSIGNING** kao spremište certifikata za otvaranje.
3. Kad se prikaže spremište certifikata i stranica lozinke, pribavite lozinku koju ste naveli za spremište certifikata i kliknite **Nastavi**.
4. Nakon osvježavanja navigacijskog okvira, izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
5. Iz popisa zadataka izaberite **Import certifikata** da započnete postupak importiranja potpisanog certifikata u spremište certifikata.

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

Pri dovršetku zadatka, spremni ste za prijavljivanje aplikacija i ostalih objekata pomoću i5/OS API-ja. Međutim, da bi osigurali da ili vi ili ostali možete provjeriti potpise, morate eksportirati potrebne certifikate u datoteku i prenijeti ih na bilo koji sistem koji instalira označene aplikacije. Korisnički sistemi moraju biti omogućeni za korištenje certifikata kako bi pri instaliranju aplikacija mogli provjeriti potpis. Možete upotrijebiti API-je za Dodavanje provjeritelja kao dijela programa za instaliranje aplikacije da napravite potrebne konfiguracije provjere potpisa za korisnike. Na primjer, možete kreirati predinstalacijski program izlaza koji zove API Dodaj provjeru za konfiguriranje korisničkog sistema.

Korak 5: Eksport certifikata za omogućavanje provjere potpisa na drugim sistemima

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

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

Za korištenje DCM kako biste mogli provjeriti potpise na istom sistemu koji potpisuje objekte (u ovom scenariju Sistem A), slijedite ove korake:

1. U navigacijskom okviru kliknite **Kreiranje novog spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za kreiranje.
2. Izaberite **Da** da kopirate postojeće certifikate za potpisivanje objekata u novo spremište certifikata kao certifikate za provjeru potpisa.
3. Odredite lozinku za novo spremište certifikata i kliknite **Nastavak** za kreiranje spremišta certifikata. Sada možete upotrebljavati DCM za provjeru potpisa objekata na istom sistemu koji 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 **Eksport certifikata**.
2. Izaberite **Potpisivanje objekata** da se prikaže popis certifikata za potpisivanje objekata koje možete eksportirati.
3. Izaberite odgovarajući certifikat potpisivanja objekta s popisa i kliknite **Eksport**.
4. Izaberite **Datoteku, kao certifikat provjere potpisa** za destinaciju i kliknite **Nastavak**.
5. Navedite potpuno kvalificirano ime staze i datoteke za eksportirani certifikat provjere potpisa i kliknite **Nastavak** da eksportirate certifikat.

Sada možete dodati ovu datoteku paketu instalacije aplikacije kojeg kreirate za vaš proizvod. Upotrebljavajući API za Dodavanje provjeritelja kao dijela instalacijskog programa, možete dodati ovaj certifikat korisnikovom *SIGNATUREVERIFICATION spremištu certifikata. Ovaj API će također kreirati ovo spremište certifikata ako već ne postoji. Program instalacije proizvoda može provjeriti potpis na aplikacijskim objektima dok ih obnavlja na korisničkim sistemima.

Korak 6: Ažuriranje programa pakiranja aplikacija za upotrebu sistemskih API-ja za potpisivanje aplikacije

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

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

Bilješka: Korištenjem primjera koda, slažete se s uvjetima “Informacije o odricanju od koda” na stranici 43.

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

```
/* ------------------------------------------------------------- */
/*                                                               */
/* COPYRIGHT (C) IBM CORP. 2004, 2007                            */
/*                                                               */
/* Upotreba API Potpisa objekata za potpis jedne ili više knjižnica */
/*                                                               */
/* API će digitalno potpisati sve objekte u navedenoj knjižnici  */
/*                                                               */
/*                                                               */
/*                                                               */
/* IBM vam dodjeljuje neekskluzivnu licencu autorskih prava za   */
/* upotrebu primjera programskog koda iz kojeg generirate slične */
```

```
/* funkcije oblikovane za vaše posebne potrebe.                    */
/* Sve primjere koda IBM je osigurao samo za svrhu ilustracije     */
/* Ovi primjeru nisu u potpunosti                                  */
/* ispitani u svim uvjetima. IBM, prema tome, ne može jamčiti      */
/* ili potvrditi pouzdanost, upotrebljivost ili funkcionalnost     */
/* ovih programa.  Svi ovdje sadržani progami se                   */
/* daju "KAKVI JESU" bez bilo kakvih jamstava.                     */
/* Podrazumijevana jamstva o nekršenju, iskoristivosti i           */
/* podobnosti za određenu svrhu se izričito poriču.                */
/*                                                                 */
/*                                                                 */
/*                                                                 */
/* Parametri su sljedeći:  */
/*                                                                 */
/*  char *   ime knjižnice za potpisivanje                         */
/*  char *   ime ID-a aplikacije                                   */
/*                                                                 */

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

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

    /* parametri:

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

     */

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

    Qydo_Multi_Objects_T * multi_objects = NULL;
    multiobj_length = 0;
    error_code.Bytes_Provided = 0;    /* izuzeci povrata za svaku grešku */


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

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

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

    /* ------------------------------- */
    /* potpišite sve objekte u ovoj knjižnici */
```

```
    /* ------------------------------- */
    QYDOSGNO  (path_name,             /* ime staze za objekt */
               &path_length,          /* dužina imena staze */
               "OBJN0100",            /* ime formata */
               argv[2],               /* identifikator aplikacije (ID) */
               &applid_length,        /* dužina ID-a aplikacije */
               "1",                   /* zamijenite duplikat potpisa */
               multi_objects,         /* kako rukovati višestrukim
                                            objektima */
               &multiobj_length,      /* dužina strukture višestrukih objekata
                                         koja se treba upotrebljavati
                                       (0=no mult.object struktura)*/
               &error_code);          /* kod greške */



       povrat 0;

 }
```

Korak 7: Kreiranje predinstalacijskog programa izlaza koji koristi API dodaj provjeru

Sada kad imate programsku obradu za potpisivanje aplikacije, možete upotrijebiti API za Dodavanje provjeritelja kao dijela programa za instaliranje da kreirate konačni proizvod za distribuciju. Na primjer, API Dodavanje provjeritelja dio je predinstaliranog izlaznog programa za osiguranje da je certifikat dodan u spremište certifikata prije vraćanja potpisanih objekta aplikacije. Instalacijskom programu omogućava provjeru potpisa na aplikacijskim objektima dok se obnavljaju na korisničkim sistemima.

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

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

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

Bilješka: Korištenjem primjera koda, slažete se s uvjetima “Informacije o odricanju od koda” na stranici 43.

Promijenite ovaj kod snippet da odgovara vašim potrebama za upotrebu API-ja Dodaj potpis kao dio predinstalacijskog programa izlaza za dodavanje potrebnog certifikata provjere potpisa na korisničkom sistemu za vrijeme instaliranja proizvoda.

```
/* ------------------------------------------------------------- */
/*                                                               */
/* COPYRIGHT (C) IBM CORP. 2004, 2007                            */
/*                                                               */
/* Upotreba API-ja Dodavanje provjeritelja za dodavanje certifikata */
/* u navedenu datoteku integriranog sistema datoteka u           */
/* *SIGNATUREVERIFICATION spremište certifikata.                 */
```

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

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

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

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

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

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


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

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

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

    povrat 0;
}
```

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

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

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

API Dodavanje provjeravatelja je možda kreirao *SIGNATUREVERIFICATION spremište certifikata kao dio instalacijskog procesa proizvoda na korisničkom sistemu. Ako je API kreirao spremište certifikata, kreirao je za njega i default lozinku. Morate svoje korisnike savjetovati da trebaju koristiti DCM za ponovno postavljanje lozinke spremišta certifikata što je prije moguće da se zaštite od neovlaštenog pristupa.

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

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a .
2. U navigacijskom okviru, kliknite **Izaberite spremište certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za otvaranje.
3. Kad se prikaže stranica Spremište certifikata i Lozinka, kliknite **Ponovno postavljanje lozinke** da se prikaže stranica Ponovno postavljanje lozinke spremišta certifikata.

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

Scenarij: Upotreba System i Navigator Središnjeg upravljanja za potpisivanje objekata

Ovaj scenarij opisuje poduzeće koje želi koristiti i5/OS sposobnosti potpisivanja objekata za potpisivanje objekata koje oni pakiraju i distribuiraju na više sistema. Bazirano na poslovnim potrebama poduzeća i sigurnosnim ciljevima, ovaj scenarij opisuje kako se koriste funkcije System i Navigator Središnjeg upravljanja za pakiranje i potpisivanje objekata koji se distribuiraju na druge sisteme.

Situacija

Vaše poduzeće (MyCo, Inc.) razvija aplikacije koje distribuiraju na više sistema, na više lokacija unutar poduzeća. Kao mrežni administrator, vi ste odgovorni za osiguranje instalacije i ažuriranja tih aplikacija na svim sistemima poduzeća. Trenutno koristite System i Navigator Središnje upravljanje za lakše pakiranje i distribuciju tih aplikacija i za izvođenje drugih administrativnih zadataka za koje ste odgovorni. Međutim, trošite više vremena nego što ste htjeli prateći i ispravljajući probleme s ovim aplikacijama zbog neovlaštenih promjena na objektima. Radi toga želite bolje osigurati cjelovitost ovih objekata potpisujući ih digitalno.

Istražili ste i5/OS sposobnosti za potpisivanje objekata i naučili da, počevši od V5R2, Središnje upravljanje omogućuje potpisivanje objekata prilikom pakiranja i distribucije. Upotrebljavajući Središnje upravljanje možete djelotvorno i relativno lako zadovoljiti sigurnosne ciljeve vašeg poduzeća. Također ste odlučili kreirati Lokalnog izdavača certifikata

(CA) i upotrebljavati ga za izdavanje certifikata za potpisivanje objekata. Upotreba certifikata kojeg je izdao Lokalni CA za potpisivanje objekata ograničava trošak korištenja ove tehnologije sigurnosti, jer ne morate kupiti certifikat od javnog dobro poznatog CA.

Ovaj primjer služi kao koristan uvod u korake koji uključuju konfiguriranje i korištenje potpisivanja objekta za aplikacije koje distribuirate na više sistema u poduzeću.

Prednosti scenarija

Ovaj scenarij ima sljedeće prednosti:

- Upotreba Središnjeg upravljanja za pakiranje i potpisivanje objekata smanjuje količinu vremena koju trebate utrošiti za distribuciju potpisanih objekata na sisteme vašeg poduzeća.
- Upotrebom Središnjeg Upravljanja za potpisivanje objekata smanjuje se broj koraka koje morate obaviti za potpisivanje objekata, jer je postupak potpisivanja dio postupka pakiranja.
- Potpisivanje paketa objekata omogućuje da lakše odredite da li su objekti promijenjeni nakon što su bili potpisani. Ovim se mogu smanjiti neka rješavanja problema koja ćete raditi u budućnosti za praćenje problema aplikacija.
- Upotreba certifikata kojeg je izdao Lokalni izdavač certifikata (CA) za potpisivanje objekata pojeftinjuje primjenu potpisivanja objekata.

Ciljevi

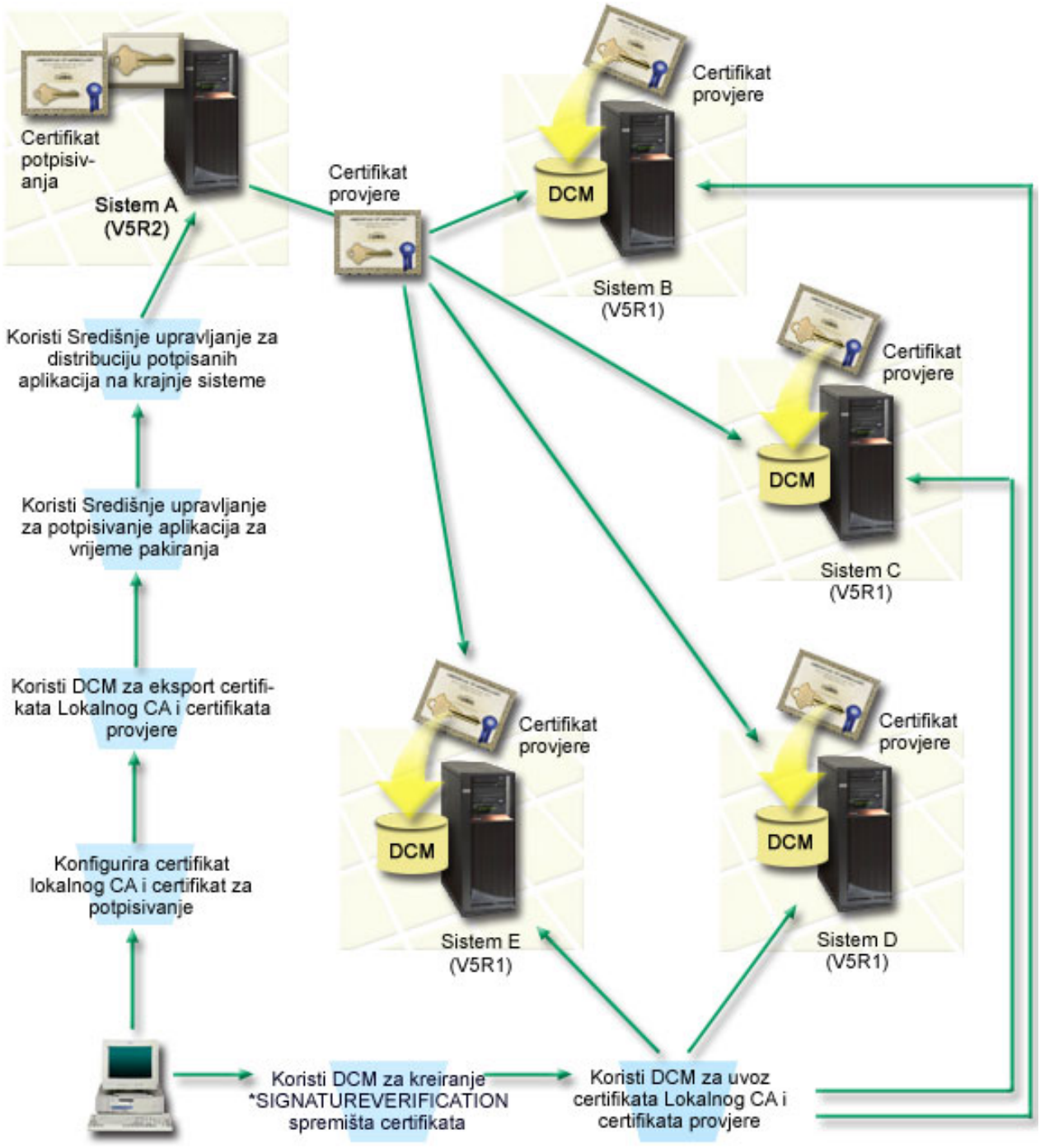
U ovom scenariju, MyCo, Inc. želi programski potpisivati aplikacije koje distribuira na više sistema unutar poduzeća. Kao mrežni administrator MyCo, Inc, već koristite Središnje upravljanje za većinu administrativnih zadataka. Posljedično, želite proširiti trenutno korištenje Središnjeg upravljanja za potpisivanje aplikacija poduzeća koje distribuirate na ostale sisteme.

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 posebni korisnici moraju moći lako provjeriti digitalne potpise na svim sistemima radi provjere porijekla i autentičnosti objekata koje je potpisalo poduzeće. Da bi ovo mogli napraviti, svaki sistem mora imati kopiju i certifikata za provjeru potpisa od poduzeća i certifikata Lokalnog izdavača certifikata (CA) u svakom sistemskom *SIGNATUREVERIFICATION spremištu certifikata.
- Provjerom potpisa na aplikacijama poduzeća i ostalim objektima, administratori i ostali mogu otkriti da li je sadržaj objekata promijenjen u odnosu na vrijeme kad su potpisani.
- Administratori moraju znati koristiti Središnje upravljanje za pakiranje, potpisivanje i distribuiranje njihovih aplikacija na njihove sisteme.

Detalji

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



Slika ilustrira sljedeće točke relevantne za ovaj scenarij:

Centralni sistem (Sistem A)

- Sistem A je System i model koji izvodi OS/400 Verziju 5 Izdanje 2 (V5R2).
- Sistem A služi kao središnji sistem s kojeg se izvode funkcije Središnjeg upravljanja, uključujući pakiranje i distribuciju aplikacija poduzeća.

- Sistem A ima instaliran 128-bitni Dobavljač kriptografskog pristupa System i (5722–AC3).
- Sistem A ima instaliran i konfiguriran Upravitelj digitalnih certifikata (opcija 34) i IBM HTTP Server (5722–DG1).
- Sistem A se ponaša kao Lokalni Izdavač certifikata (CA) i na njemu se nalazi certifikat potpisivanja objekta.
- Sistem A je primarni sistem za potpisivanje objekata za aplikacije poduzeća. Potpisivanje objekta proizvoda za distribuciju korisnicima se postiže izvođenjem ovih zadataka na Sistemu A:
  1. Upotreba DCM-a za kreiranje Lokalnog CA-a i upotreba Lokalnog CA za kreiranje certifikata za potpisivanje objekta.
  2. Upotreba DCM-a za eksportiranje kopije Lokalnog CA certifikata i certifikata provjere potpisa u datoteku tako da krajnji sistemi (Sistemi B, C, D i E) mogu provjeriti potpisane objekte.
  3. Upotreba Središnjeg upravljanja za potpisivanje objekata aplikacija i njihovo pakiranje s datotekama certifikata provjere.
  4. Upotreba Središnjeg upravljanja za distribuciju potpisanih aplikacija i datoteka certifikata krajnjim sistemima.

Krajnji sistemi (Sistemi B, C, D i E)

- Sistemi B i C su System i modeli koji izvode OS/400 Verzija 5 Izdanje 2 (V5R2).
- Sistemi D i E su System i modeli koji izvode OS/400 Verzija 5 Izdanje 1 (V5R1).
- Sistemi B, C, D i E imaju konfiguriran i instaliran Upravitelj digitalnih certifikata (opcija 34) i IBM HTTP poslužitelj (5722–DG1).
- Sistemi B, C, D i E primaju kopiju certifikata provjere potpisa poduzeća i Lokalnog CA iz centralnog sistema (Sistem A) kad sistemi prime potpisanu aplikaciju.
- DCM se upotrebljava za kreiranje *SIGNATUREVERIFICATION spremišta certifikata i importiranje certifikata Lokalnog CA i certifikata provjere u ovo spremište certifikata.

Preduvjeti i pretpostavke

Ovaj scenarij ovisi o sljedećim preduvjetima i pretpostavkama:

1. Svi sistemi odgovaraju zahtjevima za instaliranje i koriste Upravitelj digitalnih certifikata (DCM).
2. Nitko nije prethodno konfigurirao ili koristio DCM na ovim sistemima.
3. Sistem A je u skladu sa zahtjevima za instaliranje i upotrebu System i Navigator i Središnjeg upravljanja.
4. Poslužitelj Središnjeg upravljanja mora se izvoditi na svim krajnjim sistemima.
5. Svi sistemi imaju instaliranu najvišu razinu 128-bitnog Dobavljača kriptografskog pristupa (5722-AC3).
6. Default postavka za provjeru potpisa objekata za vrijeme obnavljanja (QVFYOBJRST) sistemske vrijednosti na svim sistemima scenarija je 3 i nije se mijenjala. Default postavka osigurava da sistem može provjeriti potpise objekata kad vratite potpisane objekte.
7. Mrežni administrator za Sistem A mora imati korisnički profil s *ALLOBJ posebnim ovlaštenjem da bi mogao potpisivati objekte ili korisnički profil mora biti ovlašten za aplikaciju potpisivanja objekata.
8. Sistemski administrator ili bilo tko, tko kreira spremište certifikata u DCM-u, mora imati posebna ovlaštenja korisničkog profila *SECADM i *ALLOBJ.
9. Sistemski administratori ili ostali na svim ostalim sistemima za provjeru potpisa objekta moraju imati posebno ovlaštenje korisničkog profila *AUDIT.

Koraci konfiguracijskog zadatka

Postoje dva skupa zadataka koje morate dovršiti za implementaciju scenarija: Jedan skup zadataka omogućava vam konfiguriranje Sistema A za korištenje Središnjeg upravljanja za potpisivanje i distribuciju aplikacija. Drugi skup zadataka omogućuje sistemskim administratorima i drugima da provjeravaju potpise na tim aplikacijama na svim drugim sistemima. Uputite se na temu detalja scenarija, opisanu ispod, za korake o dovršavanju tih zadataka.

Koraci zadatka potpisivanja objekata

Za potpisivanje objekata kao što je opisano u ovom scenariju, pogledajte poglavlje s detaljima scenarija za korake za dovršavanje svakog pojedinog zadatka na Sistemu A :

1. Dovršite sve korake preduvjeta za instalaciju i konfiguriranje svih potrebnih System i proizvoda
2. DCM koristite za kreiranje Lokalnog Izdavača certifikata (CA) za izdavanje privatnih certifikata potpisivanja objekta.
3. DCM koristite za kreiranje definicije aplikacije
4. DCM koristite za dodjelu certifikata definiciji aplikacije za potpisivanje objekata
5. DCM koristite za eksportiranje certifikata koji mogu koristiti ostali sistemi za provjeru potpisa objekata. Morate eksportirati kopiju certifikata Lokalnog CA i kopiju certifikata potpisivanja objekta kao certifikat provjere potpisa u datoteku.
6. Prenesite datoteke certifikata na svaki krajnji sistem na kojem namjeravate provjeriti potpise.
7. Koristite System i Navigator Središnje upravljanje za potpisivanje aplikacijskih objekata

Koraci zadatka provjere potpisa

Trebate dovršiti ove zadatke konfiguriranja provjere potpisa na svakom krajnjem sistemu prije korištenja Središnjeg upravljanja za prijenos potpisanih aplikacijskih objekata na njih. Konfiguracija provjere potpisa mora biti dovršena prije nego što možete uspješno provjeriti potpise kad vraćate potpisane objekte na krajnje sisteme.

Na svakom krajnjem sistemu, morate dovršiti ove zadatke za provjeru potpisa objekata kao što opisuje ovaj scenarij:

1. DCM koristite za kreiranje *SIGNATUREVERIFICATION spremišta certifikata
2. DCM koristite za import Lokalnog CA certifikata i certifikata provjere potpisa

Srodne informacije

Upravitelj digitalnih certifikata (DCM)

Detalji scenarija: Upotreba System i Navigator Središnjeg upravljanja za potpisivanje objekata

Dovršite sljedeći zadatak za konfiguriranje Središnjeg upravljanja za potpisivanje i5/OS objekata, kako je opisano u ovom scenariju.

Korak 1: Dovršite sve korake za preduvjete

Morate dovršiti sve preduvjetne zadatke za instaliranje i konfiguriranje svih potrebnih System i proizvoda, prije nego što možete izvoditi specifične konfiguracijske zadatke za primjenu ovog scenarija.

Korak 2: Kreiranje Lokalnog Izdavača certifikata za izdavanje privatnog certifikata za potpisivanje objekata

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

Za korištenje DCM-a za kreiranje i upravljanje lokalnim CA, slijedite ove korake: Sad kada ste kreirali lokalni CA i certifikat potpisivanja objekta, morate definirati aplikaciju za potpisivanje objekata koja će koristiti certifikat prije nego što možete potpisati objekte.

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

   Bilješka: Ako imate pitanja o tome kako dovršiti određeni obrazac u ovom vođenom zadatku, izaberite tipku upitnik (**?**) na vrhu stranice za pristup online pomoći.
3. Ispunite sve obrasce za ovaj zadatak. Kad obavljate ovaj zadatak morate napraviti sljedeće:

a. Osigurati identifikacijske informacije za Lokalnog CA.
b. Instalirati certifikat Lokalnog CA u pretražitelj tako da softver može prepoznati Lokalnog CA i provjeriti valjanost certifikata koje izdaje Lokalni CA.
c. Navesti podatke politike za Lokalnog CA.
d. Upotrijebiti novog Lokalnog CA za izdavanje certifikata poslužitelja ili klijenta kojeg aplikacije mogu upotrijebiti za SSL veze.

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

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

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

Korak 3: Kreiranje aplikacijske definicije potpisa 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 ne treba se odnositi na stvarnu aplikaciju. Definicija aplikacije koju kreirate može opisati tip ili grupu objekata koje ste htjeli potpisati. Definiciju trebate da možete imati ID aplikacije za pridruživanje sa certifikatom i da omogućite postupak potpisivanja.

Da upotrijebite DCM za kreiranje definicije aplikacije za potpisivanje objekata, slijedite ove korake:
1. U navigacijskom okviru, kliknite **Izaberite spremište certifikata** i izaberite ***OBJECTSIGNING** kao spremište certifikata za otvaranje.
2. Kad se prikaže spremište certifikata i stranica lozinke, pribavite lozinku koju ste pri kreiranju naveli za spremište certifikata i kliknite **Nastavi**.
3. U navigacijskom okviru izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
4. Izaberite **Dodavanje aplikacije** iz popisa zadataka da se prikaže obrazac za definiranje aplikacije.
5. Dovršite obrazac i kliknite **Dodaj**.

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

Korak 4: Dodjela certifikata definiciji aplikacije za potpisivanje objekata

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

Kad dovršite ovaj zadatak, spremni ste za potpisivanje objekata pomoću Središnjeg Upravljanja kad ih pakirate i distribuirate. Ipak, kako biste osigurali da ili vi ili ostali možete provjeriti potpise, morate eksportirati potrebne certifikate u datoteku i prenijeti ih na bilo koji sistem koji instalira označene aplikacije. Trebate dovršiti ove zadatke konfiguriranja provjere potpisa na svakom krajnjem sistemu prije korištenja Središnjeg upravljanja za prijenos potpisanih aplikacijskih objekata na njih. Konfiguracija provjere potpisa mora biti dovršena prije nego što možete uspješno provjeriti potpise kad vraćate potpisane objekte na krajnje sisteme.

Korak 5: Eksport certifikata za omogućavanje provjere potpisa na drugim sistemima

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

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

Za korištenje DCM kako biste mogli provjeriti potpise na istom sistemu koji potpisuje objekte (u ovom scenariju Sistem A), slijedite ove korake:

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

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

Sada možete prenijeti ove datoteke na krajnji sistem na kojem namjeravate provjeriti potpise koje ste kreirali s certifikatom.

Korak 6: Prijenos datoteka certifikata na krajnje sisteme

Morate prenijeti datoteke certifikata koje ste kreirali na Sistemu A, na krajnje sisteme u ovom scenariju prije nego ih možete konfigurirati za provjeru objekata koje potpisujete. Možete upotrijebiti nekoliko različitih metoda za prijenos

datoteka certifikata. Na primjer, možete koristiti FTP ili distribuciju paketa Središnjeg upravljanja za prijenos podataka.

Korak 7: Potpisivanje objekata korištenjem Središnjeg upravljanja

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

Za potpisivanje aplikacije koju distribuirate na krajnjim sistemima kao što ovaj scenarij opisuje, slijedite ove korake:

1. Upotrijebite Središnje Upravljanje za pakiranje i distribuiranje softverskih proizvoda .
2. Kad dođete na panel **Identifikacija** u čarobnjaku **Definicije proizvoda**, kliknite **Napredno** da se prikaže panel **Napredna identifikacija**.
3. U polje **Digitalno potpisivanje** unesite ID aplikacije za aplikaciju potpisivanja objekta koju ste ranije kreirali i kliknite **OK**.
4. Dovršite čarobnjaka i nastavite obradu za pakiranje i distribuiranje softverskih proizvoda sa Središnjim Upravljanjem.

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

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

Da kreirate *SIGNATUREVERIFICATION spremište certifikata, slijedite ove korake:

1. Pokrenite DCM. Pogledajte Pokretanje DCM-a .
2. U navigacijskom okviru Upravitelja digitalnih certifikata (DCM), izaberite **Kreiranje novog spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za kreiranje.

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

Korak 9: Zadaci provjere potpisa: Import certifikata

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

Za import tih certifikata u *SIGNATUREVERIFICATION spremište, slijedite ove korake: Vaš sistem sada može provjeriti potpise na objektima koji su kreirani s odgovarajućim potpisnim certifikatom pri obnavljanju objekta za potpisivanje.

1. U navigacijskom okviru DCM-a kliknite **Izbor spremišta certifikata** i izaberite ***SIGNATUREVERIFICATION** kao spremište certifikata za otvaranje.
2. Kad se prikaže spremište certifikata i stranica lozinke, pribavite lozinku koju ste pri kreiranju naveli za spremište certifikata i kliknite **Nastavi**.
3. Nakon osvježavanja navigacijskog okvira, izaberite **Upravljanje aplikacijama** za prikaz popisa zadataka.
4. Iz popisa zadataka izaberite **Import certifikata**.
5. Izaberite **Izdavač certifikata (CA)** kao tip certifikata i kliknite **Nastavak**.

Bilješka: Morate importirati certifikat Lokalnog CA prije importiranja privatnog certifikata za provjeru potpisa; inače postupak importiranja za certifikat provjere potpisa neće uspjeti.

6. Navedite potpuno kvalificirano ime staze i datoteke za datoteku certifikata CA i kliknite **Nastavak**. Prikazuje se poruka koja ili potvrđuje da je postupak importiranja uspio ili informira o greški ako postupak nije uspio.
7. Ponovno izaberite zadatak **Import certifikata**.
8. Izaberite **Provjera potpisa** kao tip certifikata za import i kliknite **Nastavak**.
9. Navedite potpuno kvalificirano ime staze i datoteke za certifikat provjere potpisa i kliknite **Nastavak**. Prikazuje se poruka koja ili potvrđuje da je postupak importiranja uspio ili informira o greški ako postupak nije uspio.

Potpisivanje objekata i preduvjeti provjere potpisa

Ovo poglavlje sadrži informacije o konfiguracijskim preduvjetima, kao i o ostalim razmatranjima za planiranje potpisivanja objekata i provjeru potpisa na vašem sistemu koji izvodi i5/OS operativni sistem.

i5/OS potpisivanje objekata i provjera potpisa vam daju dodatne, snažne načine za kontrolu objekata na vašem sistemu. Da iskoristite prednosti ovih sposobnosti, morate zadovoljiti preduvjete za njihovu upotrebu.

Preduvjeti za potpisivanje objekta

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

- Možete koristiti Upravitelja digitalnih certifikata (DCM).
- Možete pisati program koji koristi API Potpisivanje objekta.
- Funkciju Središnjeg upravljanja iSeries Navigatora koristite za potpisivanje objekata dok ih pakirate za distribuciju na krajnje sisteme.

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

- Morate zadovoljiti preduvjete za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).
  - Morate upotrijebiti DCM za kreiranje *OBJECTSIGNING spremišta certifikata. Ovo spremište certifikata kreirate bilo kao dio postupka kreiranja Lokalnog izdavača certifikata (CA) ili kao dio postupka upravljanja certifikatima potpisivanja objekata od javnog Internet CA.
  - *OBJECTSIGNING spremište certifikata mora sadržavati najmanje jedan certifikat, bilo onaj koji ste kreirali pomoću Lokalnog CA ili onaj koji ste dobili od javnog Internet CA.
  - Morate upotrijebiti DCM za kreiranje najmanje jedne definicije aplikacije potpisivanja objekta za upotrebu za potpisivanje objekata.
  - Morate upotrijebiti DCM za dodjelu određenog certifikata definiciji aplikacije za potpisivanje objekta.
- Korisnički profil koji potpisuje objekte mora imati posebno ovlaštenje *ALLOBJ. Korisnički profil koji kreira *SIGNATUREVERIFICATION spremište certifikata moraju imati *SECADM i *ALLOBJ posebna ovlaštenja.

Preduvjeti provjere potpisa

Postoje brojne metode koje možete upotrebljavati za provjeru potpisa na objektima:

- Možete koristiti Upravitelja digitalnih certifikata (DCM).
- Možete napisati program koji upotrebljava API Provjera objekta (QYDOVFYO).
- Možete upotrijebiti jednu od brojnih naredbi, kao naredbu Provjera cjelovitosti objekta (CHKOBJITG).

Koju metodu ćete izabrati za provjeru potpisa ovisi o vašim poslovnim i sigurnosnim potrebama. Bez obzira na metodu koju planirate upotrebljavati, morate osigurati da su zadovoljeni određeni preduvjeti:

- Morate zadovoljiti preduvjete za instaliranje i upotrebu Upravitelja digitalnih certifikata (DCM).

- Morate kreirati *SIGNATUREVERIFICATION spremište certifikata. Ovo spremište certifikata možete kreirati na jedan od dva načina, ovisno o vašim potrebama. Možete ga kreirati pomoću Upravitelja digitalnih certifikata (DCM) za upravljanje certifikatima za provjeru potpisa. Ili ako upotrebljavate javni certifikat za potpisivanje objekata, ovo spremište možete kreirati pisanjem programa koji upotrebljava API za Dodavanje provjeritelja (QYDOADDV).

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

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

  Ako koristite certifikat koji je izdao lokalni CA za potpisivanje objekata, morate koristiti DCM na host sistemu lokalnog CA za eksport kopije certifikata lokalnog CA u datoteku. Zatim možete koristiti DCM na ciljnom sistemu provjere za import certifikata lokalnog CA u *SIGNATUREVERIFICATION spremište certifikata. Da spriječite moguću grešku, morate importirati certifikat Lokalnog CA u ovo spremište certifikata prije upotrebe API-ja Dodavanje provjeritelja za dodavanje certifikata za provjeru potpisa. Radi toga, ako upotrebljavate certifikat kojeg je izdao Lokalni CA, možda ćete ustanoviti da je lakše upotrebljavati DCM za importiranje CA certifikata i certifikata provjere u spremište certifikata.

  Ako želite spriječiti da bilo tko koristi ovaj API za dodavanje certifikata za provjeru u vaše *SIGNATUREVERIFICATION spremište certifikata bez vašeg znanja, morate razmotriti onemogućavanje ovog API-ja na vašem sistemu. To možete učiniti upotrebljavajući Sistemske servisne alate (SST) da ne dopustite promjene sistemskih vrijednosti koje se odnose na sigurnost.
- Sistemski korisnički profil koji provjerava potpise mora imati *AUDIT posebno ovlaštenje. Korisnički profil koji kreira *SIGNATUREVERIFICATION spremište certifikata ili za njega mijenja lozinku, mora imati *SECADM i *ALLOBJ posebna ovlaštenja.

Upravljanje potpisanim objektima

Koristite ove informacije da bi naučili više o i5/OS sistemskim naredbama i sistemskim vrijednostima koje možete koristiti za rad s potpisanim objektima i kako potpisani objekti utječu na obrade sigurnosnog kopiranja i obnavljanja.

Počevši s V5R1, IBM je počeo potpisivati i5/OS licencne programe i PTF-ove kao način službenog označavanja da operativni sistem potiče iz IBM-a i kao način za otkrivanje neautoriziranih promjena na sistemskim objektima.

Također, poslovni partneri i drugi prodavači mogu potpisivati aplikacije koje kupujete. Radi toga, čak i ako sami ne potpisujete objekte, trebate razumjeti kako se radi s potpisanim objektima i kako ti potpisani objekti utječu na rutinske sistemske administrativne zadatke.

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

Sistemske vrijednosti i naredbe koje utječu na potpisane objekte

Ovo poglavlje sadrži informacije o i5/OS sistemskim vrijednostima i naredbama koje možete koristiti za upravljanje potpisanim objektima ili koje utječu na potpisane objekte kad ih izvodite.

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 samo dizajnirane za rad s potpisanim objektima na sistemu. Međutim, postoje brojne uobičajene CL naredbe koje upotrebljavate za upravljanje potpisanim objektima (ili za upravljanje infrastrukturnim objektima koje potpisivanje objekta čine mogućim). Druge naredbe mogu nepovoljno utjecati na potpisane objekte na sistemu uklanjanjem potpisa s objekata, čime uništavaju zaštitu koju pruža potpis.

Sistemske vrijednosti koje utječu na potpisane objekte

Sistemska vrijednost **Provjera potpisa objekta za vrijeme vraćanja** (QVFYOBJRST), član kategorije obnavljanja u i5/OS sistemskim vrijednostima, određuje kako naredbe utječu na potpisane objekte na sistemu. Ta sistemska vrijednost, koja je dostupna preko iSeries Navigatora, kontrolira kako sistem rukuje s provjerom potpisa za vrijeme operacije vraćanja. Postavka koju upotrebljavate za ovu sistemsku vrijednost, u spoju s postavkama dviju drugih sistemskih vrijednosti utječe na operacije vraćanja za sistem. Ovisno o postavci koju izaberete za ovu vrijednost, ona može dopustiti ili ne dopustiti vraćanje objekata na osnovi njihovih stanja potpisa. (Na primjer, da li je objekt nepotpisan, da li ima nevažeći potpis, da li ga je potpisao pouzdani izvor itd.) Defaultna postavka za ovu sistemsku vrijednost dopušta vraćanje nepotpisanih objekata, ali osigurava da se potpisani objekti mogu vratiti samo ako imaju važeći potpis. Sistem definira objekt kao potpisan samo ako objekt ima potpis u kojeg sistem ima povjerenja; sistem zanemaruje druge ″nepouzdane″ potpise na objektu i postupa s tim objektima kao da su nepotpisani.

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

CL naredbe koje utječu na potpisane objekte

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

Naredbe za pregled informacija o potpisu na objektu

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

Naredbe za provjeru potpisa objekta

- Naredba Provjera cjelovitosti objekta (CHKOBJITG). Ova naredba omogućuje da odredite da li je na objektima sistema povrijeđena cjelovitost. Ovu naredbu možete upotrebljavati za provjeru potpisa na način vrlo sličan upotrebi kontrola virusa za određivanje kad je virus oštetio datoteke ili druge objekte na sistemu. Da naučite još o upotrebi ove naredbe s potpisanim i potpisivim objektima, pogledajte Naredbe kontrolora koda za osiguranje cjelovitosti potpisa .
- Naredba Provjera opcije proizvoda (CHKPRDOPT). Ova naredba izvještava o razlici između ispravne strukture i stvarne strukture softverskog proizvoda. Na primjer, naredba izvještava o greški ako je objekt izbrisan iz instaliranog proizvoda. Možete koristiti CHKSIG parametar za navođenje kako će naredba rukovati i izvještavati o mogućim problemima potpisa proizvoda. Da naučite još o upotrebi ove naredbe s potpisanim i potpisivim objektima, pogledajte Naredbe kontrolora koda za osiguranje cjelovitosti potpisa .
- Naredba Spremanje licencnog programa (SAVLICPGM). Ova naredba sprema kopiju objekata koji čine licencni program. Ona sprema licencni program u obliku kojeg može vratiti naredba Vraćanje licencnog programa (RSTLICPGM). Možete koristiti CHKSIG parametar za navođenje kako će naredba rukovati i izvještavati o mogućim problemima potpisa proizvoda. Da naučite još o upotrebi ove naredbe s potpisanim i potpisivim objektima, pogledajte Naredbe kontrolora koda za osiguranje cjelovitosti potpisa .
- Naredba Vraćanje (RST). Ova naredba vraća kopiju jednog ili više objekata koji se mogu koristiti u integriranom sistemu datoteka. Ova naredba također omogućuje vraćanje spremišta certifikata i njihovih sadržaja na sistemu. Međutim, ne možete upotrijebiti ovu naredbu za vraćanje *SIGNATUREVERIFICATION spremišta certifikata. Kako naredba vraćanja rukuje s potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).
- Naredba Vraćanje knjižnice (RSTLIB). Ova naredba vraća jednu knjižnicu ili grupu knjižnica koju je spremila naredba Spremanje knjižnice (SAVLIB). Naredba RSTLIB vraća cijelu knjižnicu, koja uključuje opis knjižnice, opise objekata i sadržaje objekata u knjižnici. Kako ta naredba rukuje s potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).
- Naredba Vraćanje licencnog programa (RSTLICPGM). Ova naredba učitava ili vraća licencni program, za početnu instalaciju ili za instalaciju novog izdanja. Kako ta naredba rukuje s potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).
- Naredba Vraćanje objekta (RSTOBJ). Ova naredba vraća jedan ili više objekata u pojedinačnu knjižnicu, koji su bili spremljeni na disketu, vrpcu, optičku memoriju ili datoteku pomoću pojedinačne naredbe. Kako ta naredba rukuje s potpisanim i potpisivim objektima određuje postavka za Provjeru potpisa objekata za vrijeme vraćanja sistemske vrijednosti (QVFYOBJRST).

Naredbe za spremanje i obnavljanje spremišta certifikata

- Naredba Spremanje (SAV). Ova naredba omogućuje spremanje kopije jednog ili više objekata koji se mogu upotrebljavati u integriranom sistemu datoteka, uključujući spremišta certifikata. Međutim, ne možete upotrijebiti ovu naredbu za spremanje *SIGNATUREVERIFICATION spremišta certifikata.
- Naredba Spremanje sigurnosnih podataka (SAVSECDTA). Ova naredba omogućuje spremanje svih sigurnosnih informacija ne tražeći da sistem bude u ograničenom stanju. Upotreba ove naredbe omogućuje spremanje *SIGNATUREVERIFICATION spremišta certifikata i certifikata koje ono sadrži. Ova naredba ne sprema nikakvo drugo spremište certifikata.
- Naredba Spremanje sistema (SAVSYS). Ova naredba omogućava spremanje kopije licencnog internog koda i QSYS knjižnice u format koji je kompatibilan s instalacijom sistema. Ona ne sprema objekte iz nikakve druge knjižnice. Osim toga, ona omogućuje spremanje objekata sigurnosti i konfiguracije koje također možete spremiti pomoću naredbi SAVSECDTA i SAVCFG. Upotreba ove naredbe omogućuje spremanje *SIGNATUREVERIFICATION spremišta certifikata i certifikata koje ono sadrži.
- Naredba Vraćanje (RST). Ova naredba omogućuje vraćanje spremišta certifikata i njihovih sadržaja na sistem. Međutim, ne možete upotrijebiti ovu naredbu za vraćanje *SIGNATUREVERIFICATION spremišta certifikata.
- Naredba Vraćanje korisničkih profila (RSTUSRPRF). Ova naredba omogućuje vraćanje osnovnih dijelova korisničkog profila ili skupa korisničkih profila koji su spremljeni naredbom Spremanje sistema (SAVSYS) ili Spremanje sigurnosnih podataka (SAVSECDTA). Ovu naredbu možete upotrijebiti za vraćanje *SIGNATUREVERIFICATION spremišta certifikata i skrivenih lozinki za ovu i sve druge memorije certifikata. Možete vratiti *SIGNATUREVERIFICATION spremište certifikata bez vraćanja informacija o korisničkom profilu,

navođenjem *DCM kao vrijednosti za parametar SECDTA i *NONE za parametar USRPRF. Da upotrijebite ovu naredbu za vraćanje informacija o korisničkom profilu i spremištu certifikata i njihovih lozinki, navedite *ALL za parametar USRPRF.

Naredbe koje mogu ukloniti ili izgubiti potpise s objekata

Kada koristite sljedeće naredbe na potpisanom objektu, to možete učiniti na način koji može ukloniti ili izgubiti potpis s objekta. Uklanjanje potpisa može uzrokovati probleme s objektima. U najboljem slučaju, nećete više moći provjeravati pouzdanost izvora objekta i nećete moći provjeravati potpis da otkrijete promjene na objektu. Koristite ove naredbe samo za one potpisane objekte koje ste kreirali (za razliku od potpisanih objekata koje dobijete od ostalih poput IBM-a ili prodavača). Ako ste zabrinuti da je naredba uklonila ili izgubila neki objektov potpis, možete upotrijebiti naredbu Prikaz opisa objekta (DSPOBJD) da vidite da li je potpis još uvijek tamo i da li ga treba ponovno potpisati.

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

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

Srodni koncepti

"Razmatranja o spremanju i vraćanju potpisanih objekata"
Ovo poglavlje sadrži informacije o tome kako potpisani objekti utječu na izvođenje operacija spremanja i vraćanja na vašem sistemu koji izvodi i5/OS operativni sistem.

Srodne informacije

Pronalazač sistemske vrijednosti

Razmatranja o spremanju i vraćanju potpisanih objekata

Ovo poglavlje sadrži informacije o tome kako potpisani objekti utječu na izvođenje operacija spremanja i vraćanja na vašem sistemu koji izvodi i5/OS operativni sistem.

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

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

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

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

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

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

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

Srodni koncepti

“Sistemske vrijednosti i naredbe koje utječu na potpisane objekte” na stranici 35
Ovo poglavlje sadrži informacije o i5/OS sistemskim vrijednostima i naredbama koje možete koristiti za upravljanje potpisanim objektima ili koje utječu na potpisane objekte kad ih izvodite.

Naredbe provjere koda za osiguranje cjelovitosti potpisa

Naučite o upotrebi i5/OS naredbi za provjeru potpisa objekata i određivanje integriteta objekata.

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

Možete izabrati jednu od tri naredbe za provjeru potpisa na objektima koji već postoje na sistemu. Među njima je naredba Provjera cjelovitosti objekta (CHKOBJITG) oblikovana posebno za provjeru potpisa objekata. Provjeru

potpisa za svaku od ovih naredbi kontrolira parametar CHKSIG. Taj parametar omogućuje provjeru potpisa kod svih tipova objekata koji se mogu potpisati, zanemarivanje svih potpisa ili provjeru samo onih objekata koji imaju potpise. Ova zadnja opcija je defaultna vrijednost za parametar.

Naredba Provjera cjelovitosti objekta (CHKOBJITG)

Naredba Provjera integriteta objekta (CHKOBJITG) vam omogućuje da odredite da li na objektima na vašem sistemu ima povreda integriteta. Ovu naredbu možete upotrebljavati za provjeru povrede cjelovitosti za objekte koji posjeduju određene korisničke profile, objekte koji se podudaraju s određenim imenom staze ili sve objekte na sistemu. Unos u dnevnik za povredu cjelovitosti se dešava kad se zadovolji jedan od ovih uvjeta:

- Naredba, program, objekt modula ili atributi knjižnica su se promijenili.
- Određeno je da je digitalni potpis na objektu nevažeći. Potpis je šifrirani matematički zbroj podataka u objektu; prema tome, smatra se da se potpis podudara i da je važeći ako se podaci u objektu za vrijeme provjere podudaraju s podacima u objektu kad je bio potpisan. Određivanje nevažećeg potpisa se bazira na usporedbi šifriranog matematičkog zbroja koji se kreira kad se objekt potpisuje i šifriranog matematičkog zbroja napravljenog za vrijeme provjere potpisa. U postupku provjere potpisa uspoređuju se te dvije vrijednosti zbroja. Ako te vrijednosti nisu iste, sadržaji objekta su se promijenili od kad je objekt potpisan i smatra se da je potpis nevažeći.
- Objekt ima neispravan atribut domene za ovaj tip objekta.

Ako naredba otkrije kršenje integriteta za neki objekt, dodaje ime objekta, ime knjižnice (ili ime staze), tip objekta, vlasnika objekta i tip neuspjeha u datoteku dnevnika baze podataka. Naredba također kreira unos dnevnika u određenim drugim slučajevima, iako ti slučajevi ne predstavljaju povrede cjelovitosti. Na primjer, naredba kreira unos dnevnika za objekte koji se mogu potpisati, ali nemaju digitalni potpis, objekte koje ne može provjeriti i objekte u formatu koji zahtijeva promjenu kako bi se mogao koristiti na trenutnoj implementaciji sistema (konverzija IMPI u RISC).

Vrijednost parametra CHKSIG kontrolira kako naredba rukuje s digitalnim potpisima na objektima. Možete navesti jednu od tri vrijednosti za ovaj parametar:

- *SIGNED – Navođenjem ove vrijednosti, naredba provjerava objekte s digitalnim potpisima. Naredba kreira unos dnevnika za svaki objekt s potpisom koji nije važeći. To je defaultna vrijednost.
- *ALL – Navođenjem ove vrijednosti, naredba provjerava sve objekte za potpis da bi se provjerilo da li imaju potpis. Naredba kreira unos dnevnika za svaki potpisivi objekt koji nema potpis i za svaki objekt s potpisom koji nije važeći.
- *NONE – Navođenjem ove vrijednosti, naredba ne provjerava digitalne potpise objekata.

Naredba Provjera opcije proizvoda (CHKPRDOPT)

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

Vrijednost parametra CHKSIG kontrolira kako naredba rukuje s digitalnim potpisima na objektima. Možete navesti jednu od tri vrijednosti za ovaj parametar:

- *SIGNED – Navođenjem ove vrijednosti, naredba provjerava objekte s digitalnim potpisima. Naredba provjerava potpise na svakom potpisanom objektu. Ako naredba odluči da potpis na objektu nije važeći, naredba šalje poruku dnevniku posla i identificira proizvod da je u stanju greške. To je defaultna vrijednost.
- *ALL – Navođenjem ove vrijednosti, naredba provjerava sve objekte za potpis da bi se provjerilo imaju li potpis i provjerava se potpis u objektima. Naredba šalje poruku dnevniku posla o svakom potpisivom objektu koji nema potpis; međutim, naredba ne identificira proizvod da je s greškom. Ako naredba odluči da potpis na objektu nije važeći, šalje poruku dnevniku posla i identificira proizvod da je u stanju greške.
- *NONE – Navođenjem ove vrijednosti, naredba ne provjerava digitalne potpise objekata proizvoda.

Naredba Spremanje licencnog programa (SAVLICPGM)

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

Vrijednost parametra CHKSIG kontrolira kako naredba rukuje s digitalnim potpisima na objektima. Možete navesti jednu od tri vrijednosti za ovaj parametar:

- *SIGNED – Navođenjem ove vrijednosti, naredba provjerava objekte s digitalnim potpisima. Naredba provjerava potpise na svakom potpisanom objektu, ali ne provjerava nepotpisane objekte. Ako naredba odluči da potpis na objektu nije važeći, šalje poruku dnevniku posla o identificiranju objekta i spremanje neće uspjeti. To je defaultna vrijednost.
- *ALL – Navođenjem ove vrijednosti, naredba provjerava sve objekte za potpis da bi se provjerilo imaju li potpis i provjerava se potpis u objektima. Naredba šalje poruke dnevniku posla za bilo koji objekt koji se može potpisati, a koji nema potpis, međutim proces spremanja se ne završava. Ako naredba odluči da potpis na objektu nije važeći, šalje poruku dnevniku posla i spremanje neće uspjeti.
- *NONE – Navođenjem ove vrijednosti, naredba ne provjerava digitalne potpise objekata proizvoda.

Provjera integriteta funkcije provjere koda

Naučite kako provjeriti integritet funkcije provjere koda koju koristite za provjeru i5/OS integriteta sistema.

Za korištenje nove funkcije provjere integriteta provjere koda za provjeru integriteta sistema, morate imati posebno ovlaštenje *AUDIT.

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

1. Provjerava sve objekte programa (*PGM) na koje unos sistema tablica pokazivača pokazuje.
2. Provjerava sve objekte servisnih programa (*SRVPGM) u knjižnici QSYS i provjerava integritet API-ja Provjera objekta.
3. Izvodi API Provjera objekta (QydoVerifyObject) za provjeru integriteta naredbe Vraćanje objekta (RSTOBJ), naredbe Vraćanje knjižnice (RSTLIB) i naredbe Provjera integriteta objekta (CHKOBJITG).
4. Koristi naredbe RSTOBJ i RSTLIB na posebnoj datoteci za spremanje (*SAV) da se osigura da se greške ispravno prijavljuju. Nedostatak poruka greške ili netočna poruka greške pokazuje na mogući problem.
5. Kreira naredbeni (*CMD) objekt koji je oblikovan da ne uspije da bi ispravno provjerio.
6. Izvodi naredbu CHKOBJITG i API Provjera objekta na tom posebnom objektu naredbe da se osigura da naredba CHKOBJITG i API Provjera objekta ispravno prijavljuju greške. Nedostatak poruka greške ili netočna poruka greške pokazuje na mogući problem.
7. Provjerava potpis svakog modula Licencnog internog koda (LIC) i provjerava da li su prijavljene greške kod nepotpisanih ili pogrešno potpisanih LIC modula.

Srodni koncepti

“Funkcija provjere integriteta provjere koda” na stranici 6
Ovo poglavlje sadrži informacije o tome kako možete provjeriti integritet funkcije provjere koda koju koristite za provjeru integriteta vašeg sistema koji izvodi i5/OS operativni sistem.

Srodne reference

“Interpretiranje poruka greške provjere provjeravatelja koda” na stranici 41
Ovo poglavlje sadrži informacije o porukama koje se vraćaju iz funkcije provjere integriteta provjeravatelja koda na vašem sistemu koji izvodi i5/OS operativni sistem i kako se te poruke koriste da se osigura da je funkcija provjeravatelja koda ispravna, kao i moguća rješenja ako poruka označava da su funkcija ili ključni objekti operativnog sistema možda neispravni.

Rješavanje problema kod potpisanih objekata

Ovo poglavlje sadrži informacije o i5/OS naredbama i sistemskim vrijednostima koje možete koristiti za rad s potpisanim objektima i kako potpisani objekti utječu na obrade sigurnosnog kopiranja i obnavljanja.

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

Rješavanje problema kod grešaka potpisivanja objekata

Ovo poglavlje sadrži informacije o tome kako možete riješiti neke uobičajene probleme koji se mogu desiti kod potpisivanja objekata na vašem sistemu koji izvodi i5/OS operativni sistem.

Problem	Moguće rješenje
Kod upotrebe API-ja Potpisivanje objekta za potpisivanje objekta s ciljnim izdanjem V4R5 ili ranijim, proces potpisivanje ne uspijeva i objekt se ne potpisuje (poruka greške CPFB721).	Sistem ne osigurava podršku potpisivanja objekta do V5R1. Za one objekte koji vraćaju poruku greške CPFB721, morate ponovno kreirati te programe s ciljnim izdanjem V5R1 ili kasnijim da ih možete potpisati.

Rješavanje problema grešaka provjere potpisa

Ovo poglavlje sadrži informacije o tome kako možete riješiti neke uobičajene probleme koji se mogu desiti kod provjere i5/OS digitalnih potpisa na objektima.

Problem	Moguće rješenje
Postupak vraćanja ne uspijeva za objekte bez potpisa.	Ako nedostatak potpisa nije zabrinjavajući, provjerite je li QVFYOBJRST sistemska vrijednost postavljena na 5. Vrijednost od 5 navodi da nepotpisani objekti ne mogu biti vraćeni. Promijenite vrijednost na 3 i pokušajte vraćanje ponovno.
Postupak vraćanja ne uspijeva za objekte s potpisima.	To se može desiti ako se *SIGNATUREVERIFICATION spremište certifikata prenijelo u sistem i DCM se nije upotrijebio za promjenu njegove lozinke. U takvom slučaju, certifikati, koje sadrži spremište se ne mogu upotrijebiti za provjeru potpisa na objektima za vrijeme postupka vraćanja. Upotrijebite DCM za promjenu lozinke za spremište certifikata. Ako ne znate lozinku, trebat ćete izbrisati spremište certifikata, ponovno ga kreirati i koristiti DCM da promijenite lozinku.
Kod vraćanja ili instaliranja proizvoda, dobivate grešku, jer se potpis ne uspijeva provjeriti.	Kad se potpis objekta ne uspije ispravno provjeriti, greška može značiti da se objekt promijenio od kad je bio potpisan. Ako je integritet objekta u pitanju, nemojte mijenjati QVFYOBJRST vrijednost sistema ili izvesti druge akcije koje mogu dozvoliti da se objekt vrati. To može dovesti do zaobilaženja sigurnosti koju daje provjera potpisa i omogućiti da se štetni objekt nađe na vašem sistemu. Umjesto toga morate se obratiti onome tko je potpisao objekt da odredite odgovarajuće akcije koje trebate poduzeti da riješite problem.

Interpretiranje poruka greške provjere provjeravatelja koda

Ovo poglavlje sadrži informacije o porukama koje se vraćaju iz funkcije provjere integriteta provjeravatelja koda na vašem sistemu koji izvodi i5/OS operativni sistem i kako se te poruke koriste da se osigura da je funkcija provjeravatelja koda ispravna, kao i moguća rješenja ako poruka označava da su funkcija ili ključni objekti operativnog sistema možda neispravni.

Sljedeća tablica dale popis poruka koje funkcija provjere provjeritelja koda generira u toku obrade. Ova tablica nije opsežan popis svih poruka koje možete primiti. Umjesto toga, tablica popisuje poruke za koje je najvjerojatnije da će

pokazati da je provjera provjeritelja koda u potpunosti uspjela ili da je naišla na ozbiljni problem. Pogledajte dokumentaciju za API Provjera sistema (QydoCheckSystem) za detaljni popis poruka grešaka.

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

Tablica 1. Poruka greške provjere provjeritelja koda

Poruka greške	**Mogući problem i rješenje**
CPFB729	Ukazuje da se postupak provjere provjeritelja koda nije uspio završiti kao što je očekivano. Ovaj neuspjeh može biti uzrokovan mnoštvom problema. Pogledajte dnevnik posla za detaljnije poruke greške da odredite pravu prirodu neuspjeha i mogućeg uzroka. Ako odredite da ključni objekt operativnog sistema nije prošao provjeru integriteta, taj neuspjeh pokazuje da je objekt promijenjen od kada je potpisan prilikom slanja operativnog sistema. Možda ćete trebati ponovno instalirati operativni sistem da provjerite integritet sistema.
Prilikom pregledavanja dnevnika posla, vidite poruke poput CPFB723, CPD37A1 ili CPD37A0 za ove specifične objekte: • Program (*PGM) objekti: – QYDONOSIG u knjižnici QTEMP – QYDOBADSIG u knjižnici QTEMP • Naredba (*CMD) objekti: – QYDOBADSIG u knjižnici QTEMP – SIGNOFF u knjižnici QTEMP	Pokazuje da posebni skup objekata koje koristi funkcija provjere provjeritelja koda za testiranje integriteta nije uspio prema očekivanjima. Ovaj neuspjeh pokazuje da naredba RSTOBJ, naredba RSTLIB, naredba CHKOBJITG i API Provjera objekta ispravno prijavljuju pogreške. Daljnje akcije nisu potrebne.
CPFB723 za bilo koji drugi objekt osim onih prethodno ispisanih u ovoj tablici.	Pokazuje da se potpis na ključnom objektu operativnog sistema nije uspio provjeriti. Ova naredba može pokazivati da je objekt promijenjen od kada je potpisan prilikom isporuke operativnog sistema. Možda ćete trebati ponovno instalirati operativni sistem da provjerite integritet sistema.
CPFB722 za bilo koji drugi objekt osim onih prethodno ispisanih u ovoj tablici.	Pokazuje da objekt operativnog sistema nema potpis kada je potpis očekivan. Taj nedostatak potpisa može značiti da je objekt promijenjen od kada je potpisan prilikom isporuke operativnog sistema. Možda ćete trebati ponovno instalirati operativni sistem da provjerite integritet sistema.
CPFB72A za bilo koji drugi objekt osim onih koji su prije ispisani u ovoj tablici.	Pokazuje da ključni objekt operativnog sistema nije prošao provjeru integriteta. Ova naredba može pokazivati da je objekt promijenjen od kada je potpisan prilikom isporuke operativnog sistema. Možda ćete trebati ponovno instalirati operativni sistem da provjerite integritet sistema.

Ako ikada trebate ponovno instalirati kod koji provjerava integritet funkcije provjeravatelja koda, morate ga dobiti iz poznatog, dobrog izvora. Na primjer, možete učitati medij instalacije koji ste koristili za instaliranje trenutnog izdanja. Za obnovu funkcije provjere provjeritelja koda, slijedite ove korake s i5/OS prompta za naredbe:

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

Srodni zadaci

“Provjera integriteta funkcije provjere koda” na stranici 40
Naučite kako provjeriti integritet funkcije provjere koda koju koristite za provjeru i5/OS integriteta sistema.

Informacije o potpisivanju objekta i provjeri potpisa

Web stranice i IBM Redbooks (u PDF formatu) sadrže informacije koje se odnose na zbirku poglavlja Potpisivanje objekata i provjera potpisa. Možete gledati ili ispisati bilo koju od PDF datoteka.

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:

- **VeriSign Help Desk Web stranica** Web stranica VeriSign sadrži opsežnu knjižnicu poglavlja o digitalnim certifikatima, kao što je potpisivanje objekta, kao i brojna ostala poglavlja koja se tiču sigurnosti na Internetu.
- **IBM eServer iSeries Sigurnost ožičene mreže: i5/OS V5R1 Poboljšanja DCM-a i kriptografije SG24-6168**

  Ova IBM Redbooks publikacija opisuje V5R1 poboljšanja mrežne sigurnosti. Redbooks publikacija sadrži mnogo poglavlja, uključujući način upotrebe sposobnosti za potpisivanje objekata, Upravitelj digitalnih certifikata (DCM) itd.

Informacije o odricanju od koda

IBM vam dodjeljuje neekskluzivnu licencu autorskog prava za korištenje svih primjera programskog koda s kojima možete generirati slične funkcije skrojene za vaše vlastite specifične potrebe.

PODLOŽNO BILO KOJIM JAMSTVIMA KOJA SE NE MOGU ISKLJUČITI, IBM, NJEGOVI RAZVIJAČI PROGRAMA I DOBAVLJAČI NE DAJU NIKAKVA JAMSTVA ILI UVJETE, BILO IZRAVNA ILI POSREDNA, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI NA, POSREDNA JAMSTVA ILI UVJETE ZA PROĐU NA TRŽIŠTU, SPOSOBNOSTI ZA ODREĐENU SVRHU I NEPOVREĐIVANJE, U ODNOSU NA PROGRAM ILI TEHNIČKU PODRŠKU, AKO POSTOJI.

NI POD KOJIM UVJETIMA IBM, NJEGOVI RAZVIJAČI PROGRAMA ILI DOBAVLJAČI NISU ODGOVORNI ZA BILO ŠTO OD SLJEDEĆEG, ČAK I AKO SU INFORMIRANI O TAKVOJ MOGUĆNOSTI:

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

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

Dodatak. Napomene

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

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

IBM može imati patente ili molbe za patente koje su još u toku, a koji pokrivaju predmet o kojem se govori u ovom dokumentu. Posjedovanje ovog dokumenta vam ne daje nikakvo pravo na te patente. Možete poslati upit za licence, u pismenom obliku, na:

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

Za upite o licenci u vezi s dvobajtnim (DBCS) informacijama, kontaktirajte IBM odjel intelektualnog vlasništva u vašoj zemlji ili pošaljite upite, u pismenom obliku na adresu:

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

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

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

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

IBM može koristiti ili distribuirati bilo koje informacije koje vi dostavite, na bilo koji način koji smatra prikladnim, bez ikakvih obveza prema vama.

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

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

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

Licencni program opisan u ovim informacijama i sav licencni materijal koji je za njega dostupan, IBM isporučuje pod uvjetima IBM Ugovora s korisnicima, IBM Internacionalnog ugovora o licenci za programe, IBM Ugovora o licenci za strojni kod ili bilo kojeg ekvivalentnog ugovora između nas.

Podaci o performansama sadržani u ovom dokumentu su utvrđeni u kontroliranom okruženju. Zbog toga se rezultati dobiveni u nekom drugom operativnom okruženju mogu značajno razlikovati. Neka mjerenja su možda napravljena na sistemima razvojne razine i zbog toga nema jamstva da će ta mjerenja biti ista na općenito dostupnim sistemima. Osim toga, neka mjerenja su možda procijenjena ekstrapoliranjem. Stvarni rezultati se mogu razlikovati. Korisnici ovog dokumenta bi trebali provjeriti primjenjivost podataka na njihovo specifično okruženje.

Informacije koje se odnose na ne-IBM proizvode su dobivene od dobavljača tih proizvoda, njihovih objavljenih najava ili drugih javno dostupnih izvora. IBM nije testirao te proizvode i ne može potvrditi koliko su točne tvrdnje o performansama, kompatibilnosti ili druge tvrdnje koje se odnose na ne-IBM proizvode. Pitanja o sposobnostima ne-IBM proizvoda bi trebala biti adresirana na dobavljače tih proizvoda.

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

Sve prikazane IBM cijene su predložene maloprodajne cijene, trenutne su i mogu se mijenjati bez prethodne obavijesti. Cijene kod zastupnika se mogu razlikovati.

Ove informacije su samo za potrebe planiranja. Ovdje sadržane informacije su podložne promjenama prije nego opisani proizvodi postanu dostupni.

Ove informacije sadrže primjere podataka i izvještaja koji se koriste u svakodnevnim poslovnim operacijama. Da bi ih se ilustriralo što je bolje moguće, primjeri uključuju imena pojedinaca, poduzeća, brandova i proizvoda. Sva ta imena su izmišljena, a svaka sličnost s imenima i adresama stvarnih poslovnih subjekata u potpunosti je slučajna.

AUTORSKO PRAVO LICENCE:

Ove informacije sadrže primjere aplikacijskih programa u izvornom jeziku, koji ilustriraju tehnike programiranja na različitim operativnim platformama. Možete kopirati, modificirati i distribuirati te primjere programa u bilo kojem obliku, bez plaćanja IBM-u, za svrhe razvoja, upotrebe, marketinga ili distribucije aplikacijskih programa, u skladu sa sučeljem programiranja aplikacija za operativnu platformu za koju su primjeri programa napisani. Ti primjeri nisu bili temeljito testirani u svim uvjetima. IBM, zbog toga, ne može jamčiti ili potvrditi pouzdanost, upotrebljivost ili funkcioniranje tih programa.

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

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

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

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

Svaka kopija ili bilo koji dio tih primjera programa ili iz njih izvedenih radova, mora uključivati sljedeću napomenu o autorskom pravu:

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

Ako gledate ove informacije na nepostojanoj kopiji, možda se neće pojaviti fotografije i ilustracije u boji.

Zaštitni znaci

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

Adobe
eServer
i5/OS
IBM
iSeries
OS/400
Redbooks
system i
xSeries

Adobe, Adobe logo, PostScript i PostScript logo su registrirani zaštitni znaci ili zaštitni znaci Adobe Systems Incorporated u Sjedinjenim Državama i drugim zemljama.

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

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

Linux je zaštitni znak Linus Torvalds u Sjedinjenim Državama, drugim zemljama ili oboje.

UNIX je registrirani zaštitni znak The Open Group u Sjedinjenim Državama i drugim zemljama.

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

Termini i uvjeti

Dozvole za upotrebu ovih publikacija se dodjeljuju prema sljedećim terminima i uvjetima.

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

Komercijalna upotreba: Možete reproducirati, distribuirati i prikazivati ove publikacije samo unutar vašeg poduzeća uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete raditi izvedena dijela iz ovih publikacija ili kopirati, distribuirati ili prikazivati te publikacije ili bilo koji njihov dio izvan vašeg poduzeća, bez izričite suglasnosti IBM-a.

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

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

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune usklađenosti sa svim primjenjivim zakonima i propisima, uključujući sve zakone i propise o izvozu Sjedinjenih Država.

IBM NE DAJE NIKAKVA JAMSTVA NA SADRŽAJ OVIH PUBLIKACIJA. PUBLIKACIJE SE DAJU ″KAKVE JESU″ I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA PROĐE NA TRŽIŠTU, NEKRŠENJA I PRIKLADNOSTI ZA ODREĐENU SVRHU.

Tiskano u Hrvatskoj