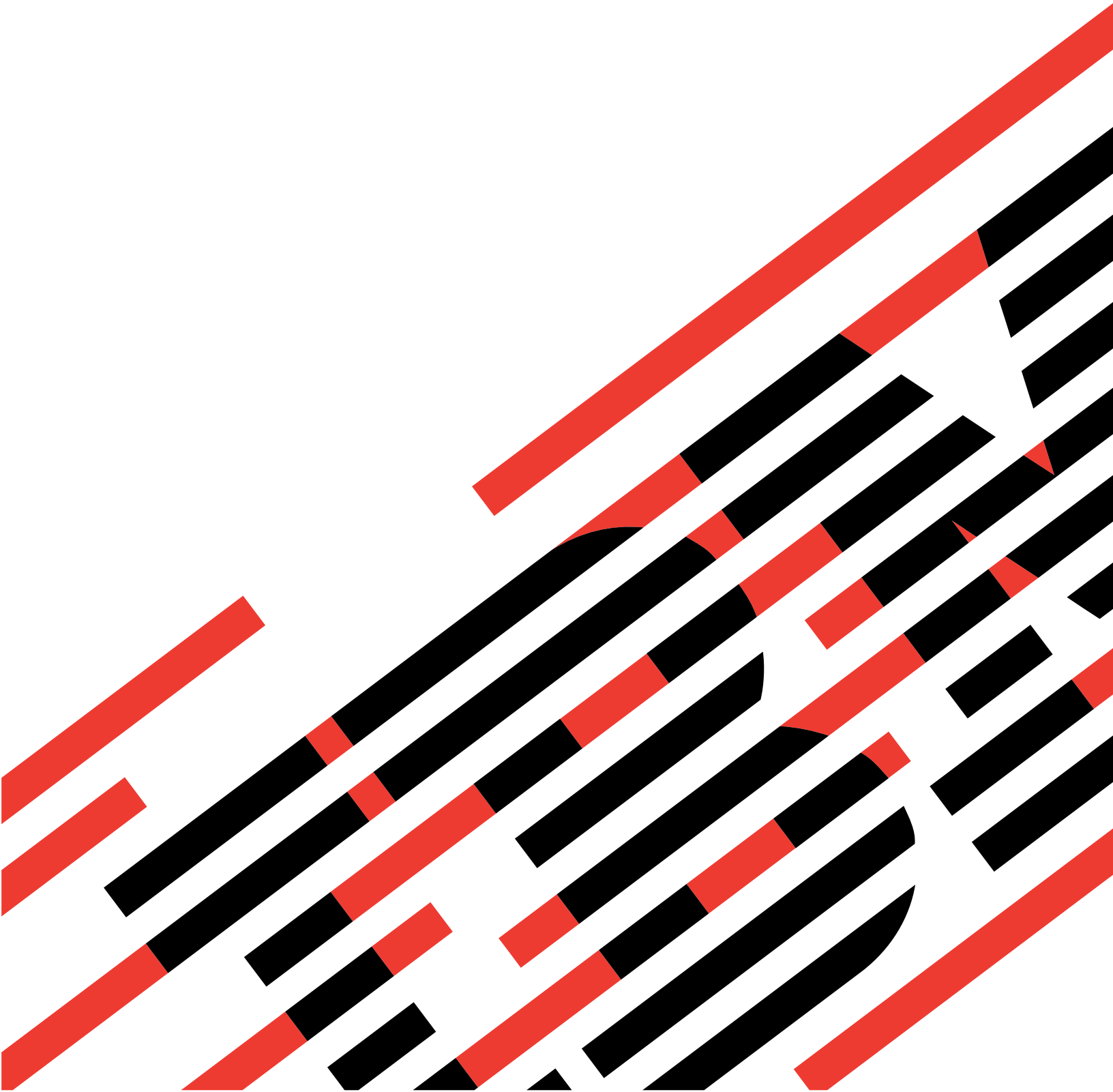
IBM

eserver

iSeries

Podpisovanie objektov a overovanie podpisov

Verzia 5, vydanie 3



IBM

@server

iSeries

Podpisovanie objektov a overovanie podpisov

Verzia 5, vydanie 3

Poznámka

Pred použitím týchto informácií a nimi podporovaného produktu si určite prečítajte informácie v časti “Právne informácie”, na strane 45.

Tretie vydanie (August 2005)

Toto vydanie sa týka verzie 5, vydania 3, modifikácie 0 produktu IBM Operating System/400 (číslo produktu 5722–SS1) a všetkých následných vydaní a modifikácií, ak v nových vydaniach nie je uvedené inak. Táto verzia nie je určená pre všetky modely RISC (reduced instruction set computer) ani pre všetky modely CISC.

Obsah

Podpisovanie objektov a overovanie podpisov

Podpisovanie objektov a overovanie podpisov sú bezpečnostné funkcie, ktoré môžete použiť na overovanie integrity mnohých objektov iSeries. Na podpísanie objektu použijete súkromný kľúč digitálneho certifikátu, a naopak certifikátom (ktorý obsahuje zodpovedajúci verejný kľúč) si overíte platnosť elektronického podpisu. Elektronický podpis zaručuje časovú a obsahovú neporušenosť objektu, ktorý podpisujete. Podpis poskytuje dôkaz pre autenticitu a autorizáciu. Môže byť použitý ako dôkaz pôvodu a na identifikovanie nepovolených zásahov. Podpísaním objektu určujete jeho zdroj a poskytujete spôsob, ako rozpoznať jeho zmeny. Keď overujete podpis na objekte, viete určiť, či v obsahu objektu boli od podpisu vykonané zmeny. Tiež môžete overiť zdroj podpisu, aby ste sa uistili o dôveryhodnosti pôvodu objektu.

Podpisovanie objektov a overovanie podpisov iSeries môžete implementovať:
- API na naprogramované podpisovanie objektov a overovanie podpisov.
- Správcu digitálnych certifikátov na podpisovanie objektov a na prezeranie, alebo overovanie podpisov.
- Riadiacu centrálu produktu iSeries Navigator na podpisovanie objektov ako súčasti distribúcie balíkov pre použitie na iných systémoch.
- CL príkazy, ako napríklad Check Object Integrity (CHKOBJITG) na overenie podpisu.

Viac sa môžete o týchto metódach podpisovania objektov a o tom, ako môže podpisovanie objektov zlepšiť vašu súčasnú bezpečnostnú politiku, naučiť v týchto témach:

Novinky vo verzii 5, vydanie 3
Tieto informácie vám objasnia viac o výhodách podpisovaní objektov a overovaní podpisov v novom vydaní iSeries, ako aj o zmenách v jeho dokumentácii.

Vytlačiť túto tému
Pomocou týchto informácií môžete vytlačiť celú túto tému ako súbor PDF.

Scenáre
Použite tieto informácie na zobrazenie scenárov ilustrujúcich niektoré typické situácie pre použitie schopností podpisovania objektov iSeries a kontroly podpisov. Každý scenár obsahuje aj úlohy, ktoré musíte vykonať pri konfigurácii, ak chcete scenár zrealizovať tak, ako je popísaný.

Koncepty
Vďaka informáciám o pojmoch a odkazoch zistite viac o elektronických podpisoch a o tom, ako fungujú procesy podpisovania objektov a overovania podpisov.

Požiadavky na podpisovanie objektov a overovanie podpisov
V tejto téme sa dozviete viac o nevyhnutných požiadavkách na konfiguráciu, ako aj ďalšie plánované okolnosti podpisovania objektov a overovania podpisov.

Spravovanie podpísaných objektov
Pomocou týchto informácií zistite viac o príkazoch a systémových hodnotách produktu iSeries, ktoré môžete používať pri práci s podpísanými objektmi a o tom, ako podpísané objekty ovplyvňujú procesy zálohovania a obnovy.

Odstraňovanie problémov pri podpisovaní objektov a overovaní podpisov
Tieto informácie vám poskytnú pomoc pri riešení problémov a chýb, ktoré by sa mohli pri podpisovaní objektov a overovaní podpisov objaviť.

Súvisiace informácie
Tu nájdete linky na ďalšie zdroje, z ktorých sa môžete naučiť viac o podpisovaní objektov a overovaní podpisov.

Tieto právne vyhlásenia sa týkajú príkladov kódu, poskytnutých v rámci tejto témy.

Novinky vo verzii 5, vydanie 3

Možnosť podpisovania objektov a overovania podpisov bola pre produkt iSeries prvý raz predstavená vo verzii V5R1. Avšak, vo verzii V5R3 sú dostupné niektoré nové funkcie a zlepšenia.

Nové, alebo vylepšené funkcie podpisovanie objektov a overovanie podpisov obsahujú:

- **Kontrola integrity systému iSeries**
  Od verzie V5R3 môžete kontrolovať integritu celého kódu dodaného spoločnosťou IBM pre váš systém iSeries.
- **Kontrola funkcie na kontrolu kódu**
  Od verzie V5R3 môžete kontrolovať integritu funkcie na kontrolu systémového kódu a iných podpísaných objektov vášho systému iSeries.

Viac informácií o novinkách a zmenách v tomto vydaní si môžete pozrieť v dokumente Poznámky pre užívateľov.

Ako zistiť, čo je nové alebo sa zmenilo

Na označenie miest s technickými zmenami používajú tieto informácie nasledujúce prostriedky:

- Obrázok na označenie miesta, kde začínajú nové alebo zmenené informácie.
- Obrázok na označenie miesta, kde končia nové alebo zmenené informácie.

Vytlačiť túto tému

Ak chcete zobraziť alebo prevziať verziu PDF tohto dokumentu, vyberte Podpisovanie objektov a kontrola podpisov (približne 605 KB).

Ukladanie súborov PDF:

Ak si chcete tento PDF súbor uložiť na svojej pracovnej stanici, aby ste si ho mohli neskôr prezerať, alebo vytlačiť:

1. Pravým tlačidlom myši kliknite na súbor PDF vo vašom prehliadači (pravým tlačidlom myši kliknite na vyššie uvedený odkaz).
2. Kliknite na položku ponuky **Save target as...**, ak používate program Internet Explorer. Kliknite na položku ponuky **Save Link As...**, ak používate program Netscape Communicator.
3. Prejdite do adresára, kde chcete uložiť súbor PDF.
4. Kliknite na **Save**.

Stiahnutie programu Adobe Acrobat Reader

Na zobrazenie alebo tlač týchto súborov PDF potrebujete program Adobe Acrobat Reader. Jeho kópiu si môžete stiahnuť z webovej lokality spoločnosti Adobe (www.adobe.com/products/acrobat/readstep.html).

Scenáre podpisovania objektov

Váš server iSeries poskytuje niekoľko rôznych metód podpisovania objektov a overovania podpisov na objektoch. To, ako sa rozhodne objekty podpisovať a ako s podpísanými objektmi pracujete, závisí na vašej obchodnej a bezpečnostnej politike a jej cieľoch. V niektorých prípadoch môžete potrebovať len overiť podpis na objekte vo vašom systéme, aby ste sa uistili, že je jeho integrita neporušená. Inokedy sa môžete rozhodnúť podpisovať objekty, ktoré zasielate iným. Podpísanie objektu vám umožní identifikovať pôvod objektu a skontrolovať, či je objekt neporušený.

To, ktorú z metód si vyberiete, závisí na mnohých faktoroch. Scenáre, ktoré nájdete v tejto téme, popisujú niekoľko najbežnejších cieľov podpisovania objektov a overovania podpisov aj s ich typickým obchodným pozadím. Každý zo scenárov popisuje aj nevyhnutné požiadavky a úlohy, ktoré musíte splniť, ak chcete scenár zrealizovať tak, ako je

popísaný. Preštudovanie týchto scenárov vám pomôže rozhodnúť sa, ako využiť možnosti podpisovania objektov v produkte iSeries spôsobom, ktorý najlepšie pokryje vaše obchodné a bezpečnostné potreby:

Scenario: Na podpísanie objektov a overenie podpisov použite Správcu digitálnych certifikátov (DCM)
Tento scenár popisuje firmu, ktorá potrebuje podpisovať nechránené objekty aplikácie na svojom verejnom webovom serveri. Potrebujú byť schopní jednoducho určiť, ak sa na týchto objektoch vyskytnú neautorizované zmeny. Zistíte, ako vzhľadom na obchodné potreby a bezpečnostné ciele firmy použiť Správcu digitálnych certifikátov (DCM), ako základnú metódu podpisovania objektov a overovania podpisov.

Scenár: Použite API na podpisovanie objektov aj na overovanie podpisov
Tu popisujeme firmu zaoberajúcu sa vývojom aplikácií, ktorá chce predávané aplikácie podpisovať automaticky. Chcú svojich zákazníkov uistiť, že aplikácie prichádzajú naozaj od ich spoločnosti a poskytnúť im spôsob, ako počas ich inštalácie rozpoznať neautorizované zmeny. Zistíte, ako vzhľadom na obchodné potreby a bezpečnostné ciele firmy použiť API podpisujúce objekty a API vkladajúce overovač a ako nimi podpisovať objekty a umožňovať ich overovanie.

Scenár: Podpisujte objekty pomocou Riadiacej centrály
V tomto prípade pôjde o spoločnosť, ktorá chce podpisovať ňou balené objekty odosielané na viaceré servery iSeries. Vysvetľuje sa tu, ako vzhľadom na obchodné potreby a bezpečnostné ciele firmy použiť funkciu Riadiacej centrály produktu iSeries Navigator na balenie a podpisovanie objektov, ktoré majú byť distribuované na iné servery iSeries.

Scenár: Na podpísanie objektov a overenie podpisov použite Správcu Digitálnych certifikátov (DCM)

Situácia

Ako administrátor produktov iSeries pre spoločnosť MyCo, Inc. ste zodpovedaný za riadenie dvoch serverov iSeries, ktoré patria vašej spoločnosti. Jeden z týchto serverov iSeries je verejným webovým serverom vašej firmy. Na vývoj obsahu a presun otestovaných súborov a objektov programov na tento verejný server používate firemný vnútorný produkčný server iSeries.

Verejný firemný server slúži aj ako všeobecná informačná webová stránka spoločnosti. Tento webový server obsahuje rôzne formuláre, ktoré zákazníci vypĺňajú pri registrácii produktov a vyžiadaní informácií o produktoch, upozornenia o aktualizácii produktov, informácie o umiestení distribuovaných produktov a tak ďalej. Ste si vedomý zraniteľnosti programov cgi-bin, ktoré poskytujú tieto formuláre; viete, že sa dajú zmeniť. Preto chcete mať možnosť kontrolovať neporušenosť týchto objektov a zistiť, ak na nich boli vykonané neautorizované zmeny. Následne ste sa rozhodli elektronickým podpisovaním týchto objektov zaistiť ich bezpečnosť.

Preskúmali ste možnosti podpisovania objektov v OS/400 a zistili ste, že existuje niekoľko spôsobov, ktorými môžete objekty podpisovať a overovať ich podpisy. Ste zodpovedný za riadenie malého počtu serverov iSeries a nemyslíte si, že budete potrebovať podpisovať objekty často, a preto ste sa rozhodli použiť produkt Správca digitálnych certifikátov (DCM) na vykonanie týchto úloh. Tiež ste sa rozhodli vytvoriť Lokálnu certifikačnú autoritu (CA) a použiť na podpisovanie objektov súkromný certifikát. Pri použití súkromného certifikátu vydaného Lokálnou CA nemusíte kupovať certifikát od uznávanej verejnej CA, čo obmedzí náklady na túto zabezpečovaciu technológiu.

Tento príklad slúži ako užitočný úvod k postupu, ako nakonfigurovať a používať podpisovanie objektov, ak chcete podpisovať objekty na niekoľkých serveroch iSeries.

Výhody scenára

Tento scenár poskytuje nasledujúce výhody:
- Podpisovanie objektov vám poskytuje spôsob ako skontrolovať bezúhonnosť nechránených objektov a ako jednoduchšie určiť, či boli tieto objekty od svojho podpisu zmenené. Toto vám môže v budúcnosti ušetriť čas pri vystopovaní a odstraňovaní problémov v aplikáciách a iných systémoch.

- S použitím grafického užívateľského rozhrania (GUI) DCM môžete vy, aj iní zamestnanci firmy podpisovať objekty a overovať podpisy rýchlo a jednoducho.
- Používanie DCM pri podpisovaní objektov a overovaní podpisov skráti čas, ktorý musíte stráviť pri pochopení a používaní podpisovania objektov ako súčasti vašej bezpečnostnej stratégie.
- Použitie certifikátu vydaného Lokálnou certifikačnou autoritou (CA) znižuje náklady na realizáciu podpisovania objektov.

Ciele

V tomto scenári chcete elektronicky podpisovať citlivé objekty, ako napríklad programy cgi-bin, ktoré generujú formuláre na vašom verejnom firemnom serveri iSeries. Ako administrátor systému v spoločnosti MyCo, Inc. chcete použiť produkt Správca digitálnych certifikátov (DCM) na podpísanie týchto objektov a na kontrolu podpisov na nich.

Ciele tohto scenáru sú nasledovné:
- Aby sa znížili náklady na podpisovanie, musia byť firemné aplikácie a iné citlivé objekty na verejnom webovom serveri (iSeries B) podpísané certifikátom od Lokálnej CA.
- Systémoví administrátori a ďalší určení užívatelia musia mať možnosť ľahko overiť elektronické podpisy na serveri iSeries, aby si mohli overiť pôvod a vierohodnosť podpísaných objektov firmy. Aby sme to dosiahli, musí mať každý zo serverov iSeries vo svojom sklade certifikátov *SIGNATUREVERIFICATION kópiu firemného certifikátu na overenie podpisov a certifikátu Lokálnej certifikačnej autority (CA).
- Overovaním podpisov na firemných aplikáciách a iných objektoch môžu administrátori iSeries a iní zistiť, či sa obsah objektov od posledného podpisu nezmenil.
- Systémový administrátor musí na podpisovanie objektov používať DCM; systémový administrátor a iní musia byť schopní použiť DCM na overenie podpisov na objektoch.

Detaily

Nasledujúci diagram objasňuje proces podpisovania objektov a overovania podpisov pri realizácii tohto scenára:

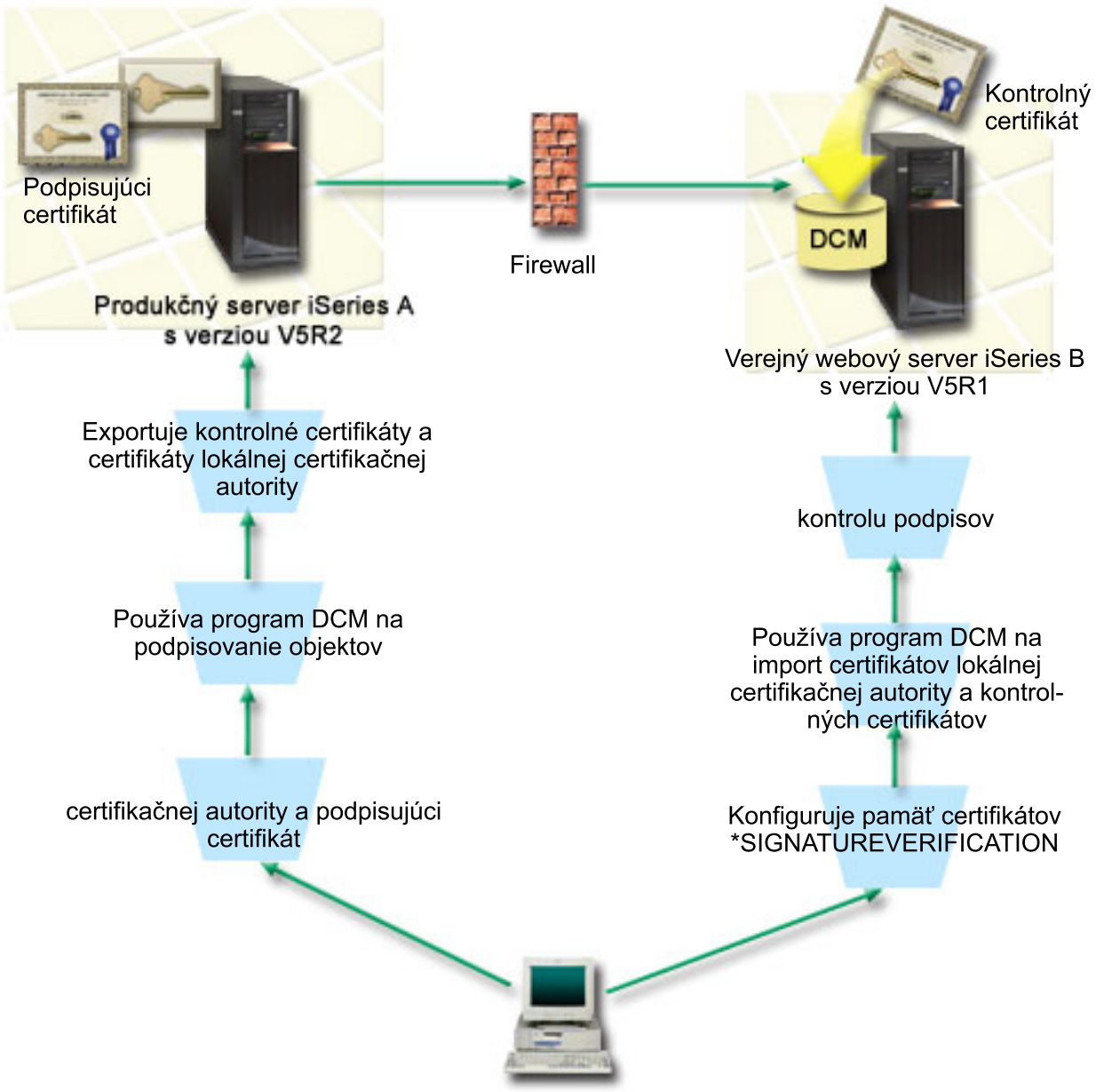


Diagram zobrazuje nasledujúce body súvisiace so scenárom:

iSeries A

- Na serveri iSeries A je spustený OS/400 verzia 5 vydanie 2 (V5R2).
- Server iSeries A je interný produkčný server spoločnosti a vývojová platforma pre verejný webový server iSeries (server iSeries B).
- Na serveri iSeries A je nainštalovaná 128-bitová verzia produktu Cryptographic Access Provider 128-bit for iSeries (5722–AC3).
- Na serveri iSeries A je nainštalovaný a nakonfigurovaný Správca digitálnych certifikátov (OS/400 možnosť 34) a IBM HTTP Server (5722–DG1).
- Server iSeries A vystupuje ako Lokálna certifikačná autorita (CA) a na tomto systéme je umiestnený aj certifikát na podpisovanie objektov.
- Server iSeries A používa na podpisovanie objektov DCM a je základným systémom na podpisovanie verejných firemných aplikácií a iných objektov.

- Server iSeries A je nakonfigurovaný tak, aby povoľoval overovanie podpisov.

iSeries B
- Na serveri iSeries B je spustený OS/400 verzia 5 vydanie 1 (V5R1).
- Server iSeries B je externý firemný verejný webový server za firemným firewallom.
- Na serveri iSeries B je nainštalovaná 128-bitová verzia Cryptographic Access Provider (5722–AC3).
- Na serveri iSeries B je nainštalovaný a nakonfigurovaný Správca digitálnych certifikátov (OS/400 možnosť 34) a IBM HTTP Server (5722–DG1).
- Server iSeries B nepracuje s lokálnou certifikačnou autoritou a server iSeries B nepodpisuje objekty.
- Server iSeries B je nakonfigurovaný tak, aby povoľoval overovanie podpisov s použitím DCM, vytvorenie skladu certifikátov *SIGNATUREVERIFICATION a import potrebných overovacích certifikátov a certifikátu Lokálnej CA.
- Program DCM sa používa na kontrolu podpisov na objektoch.

Požiadavky a predpoklady

Tento scenár je závislý na nasledujúcich požiadavkách a predpokladoch:
1. Všetky servery iSeries musia spĺňať požiadavky na inštaláciu a používanie Správcu digitálnych certifikátov (DCM).
2. Na žiadnom z týchto serverov iSeries zatiaľ nikto DCM nekonfiguroval, ani nepoužíval.
3. Na všetkých serveroch iSeries je nainštalovaná najvyššia úroveň 128-bitovej verzie licencovaného programu Cryptographic Access Provider (5722-AC3).
4. Predvolená hodnota systémovej premennej verify object signatures during restore (QVFYOBJRST) v tomto scenári na všetkých serveroch iSeries je 3 a jej nastavenia neboli zmenené. Toto predvolené nastavenie zabezpečuje, aby bolo možné overovať podpisy počas obnovy objektov na serveri.
5. Systémový administrátor servera iSeries A musí mať na podpisovanie objektov špeciálne oprávnenie *ALLOBJ, alebo musí byť profil užívateľa autorizovaný na využívanie aplikácií na podpisovanie objektov.
6. Systémový administrátor, alebo ktokoľvek, kto vytvára sklad certifikátov v DCM, musí mať špeciálne oprávnenia *SECADM a *ALLOBJ.
7. Na overovanie podpisov musí mať systémový administrátor, alebo ktokoľvek na všetkých ostatných serveroch iSeries špeciálne oprávnenie *AUDIT.

Kroky konfigurácie

Aby ste mohli zrealizovať tento scenár, musíte splniť dve skupiny úloh: Jedna skupina úloh vám umožní nakonfigurovať server iSeries A ako Lokálnu certifikačnú autoritu (CA), ako aj podpisovať a overovať podpisy objektov. Druhá skupina úloh vám umožňuje nakonfigurovať server iSeries B tak, aby overoval podpisy, ktoré vytvára server iSeries A.

Zoznam úloh pre server **iSeries A**

Na to, aby ste na serveri iSeries A vytvorili súkromnú Lokálnu CA a aby ste mohli podpisovať objekty a overovať podpisy na nich tak, ako je to popísané v tomto scenári, musíte splniť každú z týchto úloh:
1. Dokončite všetky potrebné kroky na inštaláciu a konfiguráciu všetkých potrebných produktov iSeries.
2. Použite program DCM na vytvorenie lokálnej certifikačnej autority (CA) na vydanie certifikátu podpisujúceho objekty..
3. Použite program DCM na vytvorenie definície aplikácie.
4. Použite program DCM na priradenie certifikátu k definícii aplikácie na podpisovanie objektov.
5. Použite program DCM na podpísanie objektov programov cgi-bin.
6. Použite program DCM na export certifikátov, ktoré musia použiť ostatné systémy na kontrolu podpisov objektov. Ako certifikát na overovanie podpisov musíte do súborov exportovať kópiu certifikátu Lokálnej CA, ako aj kópiu certifikátu na podpisovanie objektov.
7. Presuňte súbory certifikátov do verejného servera iSeries spoločnosti (server iSeries B), aby mohli všetci kontrolovať podpisy vytvorené serverom iSeries A.

Zoznam úloh pre server **iSeries B**

Ak plánujete obnoviť podpísané objekty, ktoré prenášate do verejného webového servera v tomto scenári (server iSeries B), musíte pred prenosom podpísaných objektov vykonať tieto konfiguračné úlohy kontroly podpisov na serveri iSeries B. Konfigurácia podpisovania objektov musí byť vykonaná skôr, než budete úspešne overovať podpisy počas obnovy podpísaných objektov na verejnom webovom serveri.

Aby ste mohli overovať podpisy na objektoch tak, ako je to popísané v tomto scenári, musíte na serveri iSeries B splniť tieto úlohy:

8. Použite program Správca digitálnych certifikátov (DCM) na vytvorenie pamäte certifikátov *SIGNATUREVERIFICATION.
9. Použite program DCM na import certifikátu lokálnej certifikačnej autority a certifikátu na kontrolu podpisu.
10. Použite program DCM na kontrolu podpisov na prenesených objektoch.

Detaily scenára: Použitie programu DCM na podpis objektov a kontrolu podpisov

Aby ste mohli nakonfigurovať a používať Správcu digitálnych certifikátov na podpisovanie objektov tak, ako je to popísané v tomto scenári, musíte splniť nasledujúce úlohy.

Krok 1: Dokončite všetky vyžadované kroky

Skôr, než vykonáte špecifické úlohy pre realizáciu tohto scenára, musíte splniť všetky úlohy spomenuté v požiadavkách na inštaláciu nevyhnutných produktov iSeries.

Krok 2: Vytvorte lokálnu certifikačnú autoritu na vydanie súkromného certifikátu podpisujúceho objekty

Proces vytvárania Lokálnej certifikačnej autority (CA) pomocou Správcu digitálnych certifikátov (DCM) si vyžaduje vyplnenie série formulárov. Tieto formuláre vás sprevádzajú procesom vytvárania CA a napĺňania ďalších úloh, ktoré sú nevyhnutné ak chcete začať používať digitálne certifikáty pre SSL, podpisovanie objektov a overovanie podpisov. Aj napriek tomu, že v tomto scenári nepotrebujete konfigurovať certifikáty pre SSL, aby ste systém nakonfigurovali na podpisovanie objektov, musíte vyplniť všetky formuláre v tejto úlohe.

Pri použití DCM na vytvorenie a prevádzkovanie Lokálnej CA, nasledujte tieto kroky:

1. Spustite DCM.
2. V navigačnom rámci DCM označte **Vytvoriť Certifikačnú autoritu (CA)**, čím zobrazíte sériu formulárov.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) navrchu stránky a dostanete sa k online pomoci.
3. Vyplňte všetky formuláre v tejto riadenej úlohe. Pri vypĺňaní tejto úlohy musíte urobiť nasledovné:
   a. Poskytnúť identifikačné údaje pre Lokálnu CA.
   b. Nainštalovať certifikát Lokálnej CA do vášho prehliadača, aby bol váš softvér schopný Lokálnu CA rozoznať a overiť platnosť certifikátov, ktoré vydala.
   c. Zadajte údaje o politike pre vašu Lokálnu CA.
   d. Použite novú Lokálnu CA a vydajte serverový, alebo klientsky certifikát, ktorý môže vaša aplikácia využívať na pripojenia SSL.

      Poznámka: Aj napriek tomu, že ho v tomto scenári nepoužijete, musíte tento certifikát vytvoriť, aby ste mohli používať Lokálnu CA na vydanie certifikátu, ktorý potrebujete, teda certifikátu na podpisovanie objektov. Ak túto úlohu zrušíte bez vytvorenia certifikátu, musíte vytvoriť svoj certifikát na podpisovanie objektov a sklad certifikátov *OBJECTSIGNING, v ktorom bude uložený, osobitne.
   e. Označte aplikácie, ktoré môžu používať tento klientsky, alebo serverový certifikát pre pripojenia SSL.

      Poznámka: Pre účely tohto scenára neoznačujte žiadne aplikácie a kliknutím na **Pokračovať** zobrazte ďalší formulár.
   f. S použitím novej Lokálnej CA to vydajte certifikát na podpisovanie objektov, ktorý budú môcť aplikácie využívať na digitálne podpisovanie. Táto úloha vytvorí sklad certifikátov *OBJECTSIGNING. To je sklad certifikátov, ktorý používate pri spravovaní certifikátov na podpisovanie objektov.
   g. Vyberte aplikácie, ktoré majú dôverovať vašej lokálnej certifikačnej autorite.

Poznámka: Pre účely tohto scenára neoznačujte žiadne aplikácie a kliknutím na **Pokračovať** ukončite úlohu.

Teraz, keď ste vytvorili Lokálnu CA a certifikát na podpisovanie objektov, musíte pred tým, než začnete podpisovať objekty, definovať aplikácie, ktoré ho budú používať.

Krok 3: Vytvorte definíciu aplikácie na podpisovanie objektov

Po tom, čo ste vytvorili svoj certifikát na podpisovanie objektov, musíte s použitím Správcu digitálnych certifikátov (DCM) definovať aplikáciu, ktorú budete pri podpisovaní objektov využívať. Definícia aplikácie nemusí odkazovať na skutočnú aplikáciu; definícia aplikácie, ktorú vytvoríte, môže opisovať typ alebo skupinu objektov, ktoré plánujete podpísať. Definíciu potrebujete, aby ste obdržali ID aplikácie, ku ktorému priradíte certifikát, čím povolíte podpisovanie objektov.

Pri použití DCM na vytvorenie definície aplikácie podpisujúcej objekty nasledujte tieto kroky:
1. V navigačnom rámci kliknite na **Vybrať sklad certifikátov** a označte ***OBJECTSIGNING** ako sklad certifikátov, ktorý chcete otvoriť.
2. Keď sa zobrazí stránka Sklad certifikátov a heslo, napíšte heslo, ktoré ste zadali pri vytváraní tohto skladu certifikátov a kliknite na **Pokračovať**.
3. V navigačnom rámci označte **Spravovať aplikácie** a zobrazte zoznam úloh.
4. V zozname úloh označte **Pridať aplikáciu**, čím sa vám zobrazí formulár na definovanie aplikácie.
5. Vyplňte formulár a kliknite na **Pridať**.

Teraz musíte aplikácii, ktorú ste vytvorili, priradiť certifikát na podpisovanie objektov.

Krok 4: Priraďte certifikát k definícii aplikácie na podpisovanie objektov

Nasledovaním týchto krokov priradíte certifikát vašej aplikácii podpisujúcej objekty:
1. V navigačnom rámci DCM označte **Spravovať certifikáty** a zobrazte zoznam úloh.
2. Zo zoznamu úloh vyberte **Priradiť certifikát**, čím zobrazíte zoznam certifikátov v aktuálnom sklade certifikátov.
3. V zozname označte správny certifikát a kliknutím na **Priradiť aplikácii** zobrazte zoznam definícií aplikácií v aktuálnom sklade certifikátov.
4. Označte v zozname jednu, alebo viac aplikácií a kliknite na **Pokračovať**. Zobrazí sa vám stránka so správou potvrdzujúcou priradenie certifikátu, alebo poskytujúcou chybové informácie o probléme, ktorý sa vyskytol.

Po vykonaní tejto úlohy ste pripravený používať DCM pri podpisovaní objektov programov, ktoré bude verejný firemný webový server (iSeries B) používať.

Krok 5: Podpíšte programové objekty

Pri práci s DCM na podpisovanie objektov programov, ktoré použijete na verejnom firemnom webovom serveri (iSeries B), postupujte podľa týchto krokov:
1. V navigačnom rámci kliknite na **Označiť sklad certifikátov** a vyberte ***OBJECTSIGNING** ako certifikačný sklad, ktorý chcete otvoriť.
2. Zadajte heslo pre sklad certifikátov *OBJECTSIGNING a kliknite na **Pokračovať**.
3. Keď sa obnoví obsah navigačného rámca, označte **Spravovať podpisovateľné objekty** a zobrazte zoznam úloh.
4. Zo zoznamu úloh vyberte **Podpísať objekt** a zobrazte zoznam definícií aplikácií, ktoré môžete na podpísanie objektov použiť.
5. Označte aplikáciu, ktorú ste v predchádzajúcom kroku definovali a kliknite na **Podpísať objekt**. Zobrazený formulár vám umožňuje zadať umiestnenie objektu, ktorý chcete podpisovať.
6. Do ponúknutého poľa zapíšte úplný názov cestu a súboru objektu, alebo adresára objektov, ktoré chcete podpisovať a kliknite na **Pokračovať**. Môžete tiež zadať umiestnenie adresára a kliknúť na **Prehľadávať**, čím zobrazíte obsah adresára a môžete v ňom vybrať objekty určené na podpísanie.

   Poznámka: Názov objektu musíte zadať s lomkou na začiatku, inak môže dôjsť k chybe. Na popísanie časti adresára, ktorú chcete podpísať, môžete tiež použiť niektoré zástupné znaky. Tieto zástupné znaky predstavujú hviezdička (*****), ktorá zastupuje *akékoľvek množstvo znakov* a otáznik (**?**), ktorý zastupuje

akýkoľvek jeden znak. Napríklad, ak chcete podpísať všetky objekty v špecifickom adresári, môžete zadať /mojadresar/*; na podpísanie všetkých programov v špecifickej knižnici môžete zadať /QSYS.LIB/QGPL.LIB/*.PGM. Tieto zástupné znaky môžete použiť len v poslednej časti názvu cesty; napríklad napísanie /mojadresar*/nazovsuboru skončí chybovou správou. Ak chcete použiť funkciu **Prehľadať** na zobrazenie obsahu knižnice alebo adresára, musíte pred kliknutím na tlačidlo **Prehľadať** zadať zástupný znak ako časť názvu cesty.

7. Určite svoju voľbu procesu, ktorým chcete vybratý objekt, alebo objekty podpisovať a kliknite na **Pokračovať**.

   Poznámka: Ak ste sa rozhodli, že počkáte na výsledky úlohy, zobrazia sa tieto výsledky priamo vo vašom prehliadači. Výsledky aktuálnej úlohy sú pripojené na koniec súboru výsledkov. Preto môže súbor okrem výsledkov aktuálnej úlohy obsahovať aj výsledky akejkoľvek z predošlých úloh. Na určenie riadkov, ktoré sa vzťahujú na aktuálnu úlohu môžete použiť pole dátumu. Pole dátumu je vo formáte YYYYMMDD. Prvé pole v súbore môže byť buď ID správy (ak sa počas spracovania objektu vyskytla chyba) alebo pole dátumu (označujúce dátum, kedy bola úloha spracovaná).
8. Zadajte úplný názov cesty a súboru, do ktorého chcete uložiť výsledky úlohy tohto podpísania objektu a kliknite na **Pokračovať**. Alebo zadajte umiestnenie adresára a kliknite na **Prehľadávať**, čím zobrazíte obsah adresára a môžete v ňom vybrať súbor, do ktorého uložíte výsledky úlohy. Zobrazí sa správa, ktorá naznačuje, že bola odoslaná úloha na podpísanie objektov. Ak si chcete prezrieť jej výsledky, prezrite si úlohu **QOBJSGNBAT** v protokole úlohy.

Aby ste si zabezpečili, že vy, aj ostatní budete môcť overovať podpisy, musíte potrebné certifikáty exportovať do súboru a tento presunúť na server iSeries B. Predtým, než podpísané objekty programov presuniete na server iSeries B, musíte na serveri iSeries B splniť všetky konfiguračné úlohy pre overovania podpisov. Než budete môcť počas obnovy podpísaných objektov na serveri iSeries B úspešne overovať ich podpisy, musí byť táto konfigurácia overovania podpisov ukončená.

Krok 6: Vyexportujte certifikáty na umožnenie kontroly podpisov na serveri iSeries B.

Ak podpisujete objekty, aby ste zabezpečili bezúhonnosť ich obsahu, musíte pre vás, aj iných zabezpečiť spôsob overenia spoľahlivosti podpisu. Ak chcete podpisy objektov overovať na tom istom systéme, ktorý ich podpísal (iSeries A), musíte s použitím DCM vytvoriť sklad certifikátov *SIGNATUREVERIFICATION. Tento sklad certifikátov musí obsahovať kópiu certifikátu na podpisovanie objektov aj kópiu certifikátu CA, ktorá ho vydala.

Ak chcete ostatným umožniť overenie podpisu, musíte im poskytnúť kópiu certifikátu, ktorý ho podpísal. Ak na vydanie certifikátu používate Lokálnu certifikačnú autoritu (CA), musíte im tiež poskytnúť kópiu certifikátu Lokálnej CA.

Ak chcete pomocou DCM overovať podpisy na systéme, ktorý objekty podpísal (v tomto scenári iSeries A), musíte dodržať tieto kroky:

1. V navigačnom rámci vyberte **Vytvoriť nový sklad certifikátov** a označte ***SIGNATUREVERIFICATION** ako sklad certifikátov, ktorý chcete vytvoriť.
2. Kliknutím na **Áno** prekopírujete existujúce certifikáty na podpisovanie objektov do nového skladu certifikátov ako certifikáty na overovanie podpisov.
3. Zadajte heslo pre nový sklad certifikátov a kliknutím na **Pokračovať** ho vytvorte. Odteraz môžete s použitím DCM overovať podpísané objekty na systéme, ktorý používate aj na ich podpisovanie.

Ak chcete pomocou DCM exportovať kópiu certifikátu Lokálnej CA a kópiu certifikátu na podpisovanie objektov ako certifikáty na overovanie podpisov, aby ste mohli overovať podpisy aj na iných systémoch (iSeries B), vykonajte tieto kroky:

1. V navigačnom rámci vyberte **Spravovať certifikáty** a potom označte úlohu **Exportovať certifikát**.
2. Vyberte **Certifikačná autorita (CA)** a kliknutím na **Pokračovať** zobrazte zoznam certifikátov CA, ktoré môžete exportovať.
3. Vyberte zo zoznamu certifikát Lokálnej CA, ktorý ste predtým vytvorili a kliknite na **Export**.
4. Ako cieľ exportu označte **Súbor** a kliknite na **Pokračovať**.
5. Pre exportovaný certifikát Lokálnej CA zadajte úplný názov cesty a súboru a kliknutím na **Pokračovať** certifikát exportujte.
6. Kliknutím na **OK** zatvorte potvrdzovaciu stránku exportu. Teraz môžete exportovať kópiu certifikátu na podpisovanie objektov.

7. Znovu vyberte úlohu **Exportovať certifikát**.
8. Výberom **Podpisovanie objektov** zobrazte zoznam certifikátov na podpisovanie objektov, ktoré chcete exportovať.
9. Vyberte si zo zoznamu správny certifikát na podpisovanie objektov a kliknite na **Export**.
10. Ako cieľ označte **Uložiť ako certifikát na overovanie podpisov** a kliknite na **Pokračovať**.
11. Zadajte úplný názov cesty a súboru, kam chcete exportovať certifikát na overovanie podpisov a kliknutím na **Pokračovať** ho exportujte.

Teraz môžete tieto súbory presunúť na koncové systémy iSeries, na ktorých chcete overovať podpisy vytvorené týmto certifikátom.

Krok 7: Presuňte súbory certifikátu do verejného servera spoločnosti iSeries B.

Certifikačný súbor, ktorý ste vytvorili na serveri iSeries A musíte presunúť na server iSeries B, verejný firemný webový server skôr, než ho budete konfigurovať, aby overoval objekty, ktoré podpisujete. Na presun certifikačných súborov môžete použiť niekoľko metód. Na presun súborov môžete použiť napríklad protokol FTP (File Transfer Protocol) alebo distribúciu balíkov Centrálnym riadením.

Krok 8: Úlohy kontroly podpisov: Vytvorte pamäť certifikátov *SIGNATUREVERIFICATION.

Aby ste mohli na serveri iSeries B (verejný firemný webový server) overovať podpisy, musí byť v jeho certifikačnom sklade *SIGNATUREVERIFICATION uložená kópia patričného certifikátu na overovanie podpisov. Keďže ste na podpisovanie objektov použili certifikát Lokálnou CA, musí tento sklad certifikátov obsahovať aj kópiu certifikátu Lokálnej CA.

Sklad certifikátov *SIGNATUREVERIFICATION vytvoríte nasledovným postupom:
1. Spustite DCM.
2. V navigačnom rámci Správcu digitálnych certifikátov (DCM) vyberte **Vytvoriť nový sklad certifikátov** a označte ***SIGNATUREVERIFICATION** ako sklad certifikátov, ktorý chcete vytvoriť.

   Poznámka: Ak si nie ste istý, ako pri používaní DCM vyplniť konkrétny formulár, kliknite na tlačidlo označené otáznikom (**?**) navrchu stránky a dostanete sa k online pomoci.
3. Zadajte heslo pre nový sklad certifikátov a kliknutím na **Pokračovať** ho vytvorte. Teraz môžete do skladu importovať certifikáty a použiť ich na overovanie podpisov.

Krok 9: Úlohy kontroly podpisov: Naimportujte certifikáty.

Aby ste mohli overiť elektronický podpis, musí sklad *SIGNATUREVERIFICATION obsahovať certifikát na overovanie podpisov. Ak je certifikát, ktorým bol objekt podpísaný, súkromný, musí tento sklad certifikátov obsahovať aj kópiu certifikátu Lokálnej certifikačnej autority (CA), ktorá ho vydala. V tomto scenári boli oba certifikáty exportované do súboru a presunuté na každý koncový systém iSeries.

Ak chcete tieto certifikáty presunúť do skladu certifikátov *SIGNATUREVERIFICATION, postupujte takto:
1. V navigačnom rámci DCM kliknite na **Vybrať sklad certifikátov** a označte ***SIGNATUREVERIFICATION** ako sklad certifikátov, ktorý chcete otvoriť.
2. Keď sa zobrazí stránka Sklad certifikátov a heslo, napíšte heslo, ktoré ste zadali pri vytváraní tohto skladu certifikátov a kliknite na **Pokračovať**.
3. Keď sa obnoví obsah navigačného rámca, označte **Spravovať certifikáty** a zobrazte zoznam úloh.
4. Zo zoznamu úloh vyberte **Import certifikátov**.
5. Ako typ certifikátu vyberte **Certifikačná autorita (CA)** a kliknite na **Pokračovať**.

   Poznámka: Certifikát Lokálnej CA musíte importovať skôr, než súkromný certifikát na overovanie podpisov; inak proces importu certifikátu na overovanie podpisov zlyhá.
6. Zadajte úplný názov cesty a súboru certifikátu CA a kliknite na **Pokračovať**. Zobrazí sa správa, ktorá buď potvrdzuje, že bol proces importu úspešný, alebo poskytuje chybovú informáciu, ak proces zlyhal.
7. Znovu vyberte úlohu **Importovať certifikát**.

8. Ako typ importovaného certifikátu označte **Overovanie podpisov** a kliknite na **Pokračovať**.
9. Zadajte úplný názov cesty a súboru certifikátu na overovanie podpisov a kliknite na **Pokračovať**. Zobrazí sa správa, ktorá buď potvrdzuje, že bol proces importu úspešný, alebo poskytuje chybovú informáciu, ak proces zlyhal.

Teraz môžete použiť DCM na serveri iSeries B na overovanie podpisov objektov, ktoré ste vytvorili patričným podpisovacím certifikátom na serveri iSeries A.

Krok 10: Úlohy kontroly podpisov: Skontrolujte podpisy na programových objektoch.

Ak chcete overovať podpisy na presunutých objektoch programov s použitím DCM, dodržte tento postup:
1. V navigačnom rámci kliknite na **Vybrať sklad certifikátov** a vyberte ***SIGNATUREVERIFICATION** ako sklad, ktorý chcete otvoriť.
2. Zadajte heslo pre sklad certifikátov *SIGNATUREVERIFICATION a kliknite na **Pokračovať**.
3. Keď sa obnoví obsah navigačného rámca, označte **Spravovať podpisovateľné objekty** a zobrazte zoznam úloh.
4. V zozname úloh vyberte **Overiť podpis objektu** a zadajte umiestnenie objektu, ktorého podpis chcete overiť.
5. Do ponúknutého poľa zapíšte úplný názov cesty a súboru objektu, alebo adresára objektov, ktorých podpisy chcete overovať a kliknite na **Pokračovať**. Môžete tiež zadať umiestnenie adresára a kliknúť na **Prehľadávať**, čím zobrazíte obsah adresára a môžete v ňom vybrať objekty určené na overenie podpisu.

   Poznámka: Na určenie časti adresára, ktorú chcete overiť, môžete tiež použiť určité zástupné znaky. Tieto zástupné znaky predstavujú hviezdička (*****), ktorá zastupuje *akékoľvek množstvo znakov* a otáznik (**?**), ktorý zastupuje *akýkoľvek jeden znak*. Napríklad, ak chcete podpísať všetky objekty v špecifickom adresári, môžete zadať /mojadresar/*; na podpísanie všetkých programov v špecifickej knižnici môžete zadať /QSYS.LIB/QGPL.LIB/*.PGM. Tieto zástupné znaky môžete použiť len v poslednej časti názvu cesty; napríklad napísanie /mojadresar*/nazovsuboru skončí chybovou správou. Ak chcete použiť funkciu Prehľadať na zobrazenie obsahu knižnice alebo adresára, musíte pred kliknutím na tlačidlo **Prehľadať** zadať zástupný znak ako časť názvu cesty.
6. Určite svoju voľbu procesu, ktorým chcete vybratý objekt, alebo objekty overovať a kliknite na **Pokračovať**.

   Poznámka: Ak ste sa rozhodli, že počkáte na výsledky úlohy, zobrazia sa tieto výsledky priamo vo vašom prehliadači. Výsledky aktuálnej úlohy sú pripojené na koniec súboru výsledkov. Preto môže súbor okrem výsledkov aktuálnej úlohy obsahovať aj výsledky akejkoľvek z predošlých úloh. Na určenie riadkov, ktoré sa vzťahujú na aktuálnu úlohu môžete použiť pole dátumu. Pole dátumu je vo formáte YYYYMMDD. Prvé pole v súbore môže byť buď ID správy (ak sa počas spracovania objektu vyskytla chyba) alebo pole dátumu (označujúce dátum, kedy bola úloha spracovaná).
7. Zadajte úplný názov cesty a súboru, do ktorého chcete uložiť výsledky úlohy tohto overenia objektu a kliknite na **Pokračovať**. Alebo zadajte umiestnenie adresára a kliknite na **Prehľadávať**, čím zobrazíte obsah adresára a môžete v ňom vybrať súbor, do ktorého uložíte výsledky úlohy. Zobrazí sa správa, ktorá naznačuje, že bola odoslaná úloha na overenie podpisov objektu. Ak si chcete prezrieť jej výsledky, prezrite si úlohu **QOBJSGNBAT** v protokole úlohy.

Scenár: Použitie API na podpisovanie objektov a overovanie podpisov

Situácia

Vaša spoločnosť (MyCo, s.r.o.) je obchodným partnerom iSeries, ktorý vyvíja aplikácie pre zákazníkov. Pre firmu pracujete ako vývojár softvéru a ste zodpovedný za balenie týchto aplikácií pred ich distribúciou zákazníkom. Na balenie aplikácií momentálne používate programy. Zákazníci si môžu objednať kompaktný disk (CD-ROM), alebo navštíviť vašu webovú stránku a aplikáciu si stiahnuť.

Udržiavate si prehľad vo svojom odbore, najmä pokiaľ ide o bezpečnosť. Preto viete, že zákazníkov oprávnene znepokojuje pôvod a obsah programov, ktoré dostávajú alebo sťahujú. Stáva sa, že klienti predpokladajú, že obdržali alebo stiahli produkt z dôveryhodného zdroja, ale zistia, že to nebol pravý zdroj produktu. To niekedy vyústi až do situácie, keď si zákazníci nainštalujú iný produkt, než očakávali. Niekedy vysvitne, že tento nainštalovaný produkt je škodiaci program, alebo že bol produkt zmenený a poškodil systém.

Aj napriek tomu, že toto sa v prípade klientov iSeries nestáva často, chcete svojich zákazníkov ubezpečiť, že aplikácie, ktoré dostanú, pochádzajú skutočne z vašej spoločnosti. Tiež chcete klientom poskytnúť spôsob, ako si overiť neporušenosť týchto aplikácií, takže vedia ešte pred inštaláciou určiť, či boli súbory zmenené.

Na základe svojho prieskumu ste sa rozhodli, že na zaistenie bezpečnosti môžete použiť možnosti overovania podpisov v OS/400. Elektronické podpisovanie vašich aplikácií dáva vašim zákazníkom možnosť overiť, že je vaša firma skutočne pôvodcom aplikácií, ktoré si stiahnu, alebo obdržia. Keďže už balíte aplikácie pomocou programov, rozhodli ste sa, že na jednoduché pridanie podpisovania objektov k vášmu procesu balenia môžete využiť API. Tiež ste sa rozhodli podpisovať objekty verejným certifikátom, aby bol proces overovania podpisu pri inštalácii produktu transparentný.

Do aplikačného balíka zahrniete aj kópiu elektronického certifikátu, ktorým ste objekty podpísali. Keď zákazník obdrží aplikačný balík, môže verejný kľúč certifikátu použiť na overenie jeho podpisu. To klientovi umožní určiť a overiť si zdroj aplikácie, ako aj to, či sa jej obsah od podpisu nezmenil.

Tento príklad slúži ako užitočný úvod k postupu, keď pomocou programov podpisujete objekty aplikácií, ktoré balíte a zasielate na ďalšie použitie.

Výhody scenára

Tento scenár poskytuje nasledujúce výhody:
- Podpisovanie objektov programami s využitím API znižuje množstvo času, ktorý musíte stráviť pri realizácii tohto bezpečnostného opatrenia.
- Využitie API pri podpise objektov počas balenia znižuje počet krokov, ktoré musíte pri podpisovaní vykonať, keďže sa tento proces stáva súčasťou procesu balenia.
- Podpisovanie balíka objektov vám umožní jednoducho určiť, či sa objekty od svojho podpisu zmenili. Toto vám môže v budúcnosti ušetriť čas pri vystopovaní a odstraňovaní klientskych problémov s aplikáciami.
- Ak na podpisovanie objektov využijete certifikát od známej Certifikačnej autority (CA), môžete ako súčasť ukončovacieho programu inštalácie vášho produktu použiť API vkladajúce overovač. To vám umožní automaticky pridať do zákazníkovho systému verejný certifikát, ktorým ste aplikáciu podpísali. Takto zabezpečíte, že bude overovanie podpisu pre klienta transparentné.

Ciele

V tomto scenári chce MyCo, s.r.o. programami podpisovať aplikácie, ktoré balí a distribuuje svojim zákazníkom. Ako vývojár produkčných aplikácií v spoločnosti MyCo, Inc. v súčasnosti programovo balíte aplikácie spoločnosti určené pre distribúciu zákazníkom. Preto chcete na podpisovanie aplikácií použiť API iSeries a umožniť tak serveru iSeries vášho klienta aby mohol počas inštalácie overovať podpisy.

Ciele tohto scenára sú nasledovné:
- Produkčný vývojár spoločnosti musí mať v rámci už existujúceho procesu balenia aplikácie možnosť podpisovať objekty pomocou API podpisujúceho objekty.
- Firemné aplikácie musia byť podpísané verejný certifikátom, aby bol proces overovania podpisu počas inštalácie pre zákazníka transparentný.
- Firma musí mať možnosť pridať automaticky pomocou API iSeries certifikát na overovanie podpisov do klientovho skladu certifikátov *SIGNATUREVERIFICATION na serveri iSeries. V prípade, že tento sklad ešte neexistuje, musí mať firma možnosť v rámci inštalácie produktu automaticky vytvoriť tento sklad certifikátov na klientovom serveri iSeries .
- Zákazníci musia mať možnosť jednoducho si po inštalácii overiť elektronické podpisy na aplikáciách firmy. Zákazníci musia mať možnosť overiť si tieto podpisy, aby sa mohli uistiť o pôvode a bezúhonnosti podpisovanej aplikácie, ako aj o tom, či boli na aplikácii od jej podpisu vykonané nejaké zmeny.

Detaily

Nasledujúci diagram objasňuje proces podpisovania objektov a overovania podpisov pri realizácii tohto scenára:

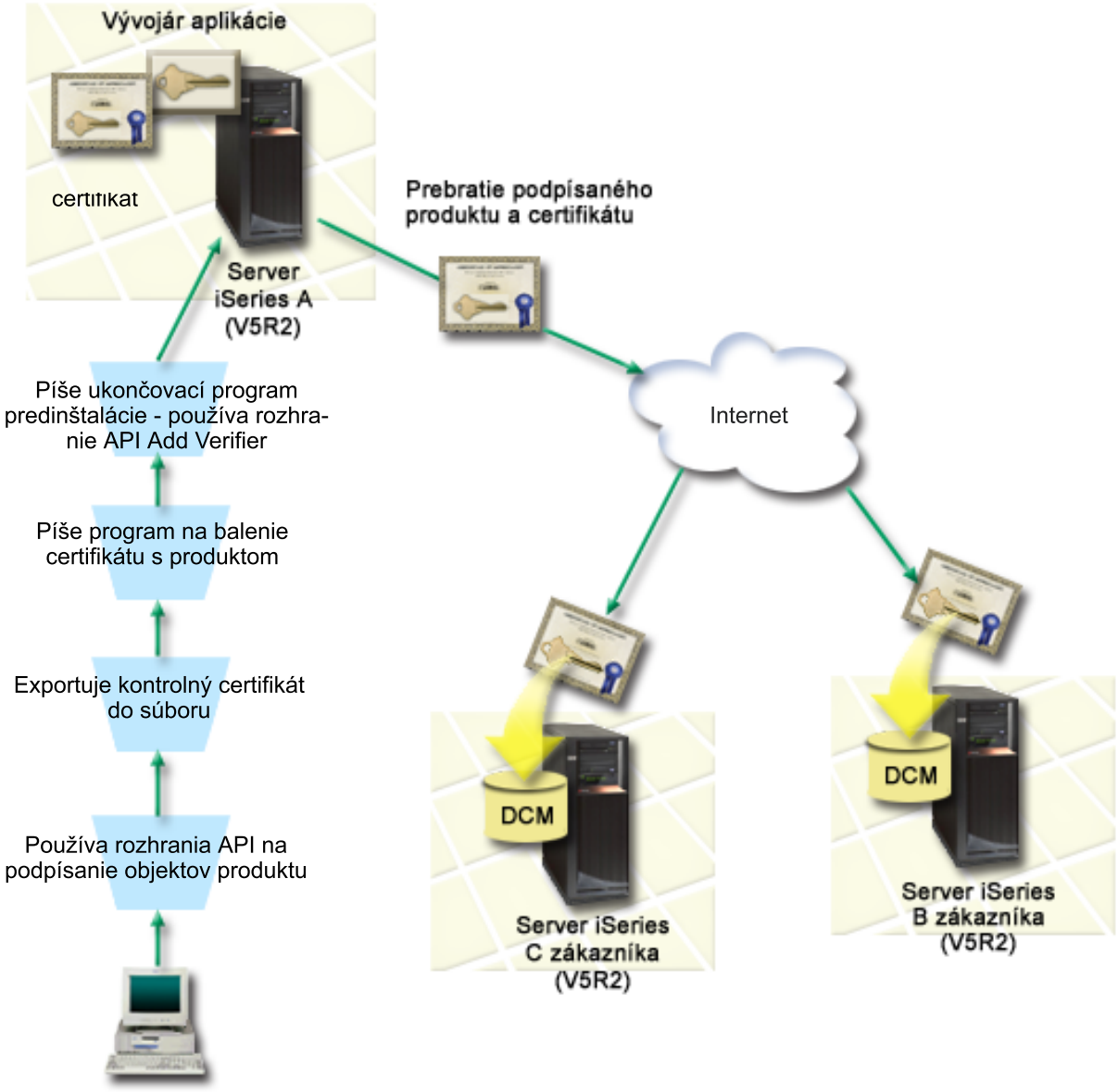


Diagram zobrazuje nasledujúce body súvisiace so scenárom:

Centrálny systém (iSeries A)

- Na serveri iSeries A je spustený OS/400 verzia 5 vydanie 2 (V5R2).
- Program vývojára aplikácií na balenie aplikácií je spustený na serveri iSeries A.
- Na serveri iSeries A je nainštalovaná 128-bitová verzia produktu Cryptographic Access Provider 128-bit for iSeries (5722–AC3).
- Na serveri iSeries A je nainštalovaný a nakonfigurovaný Správca digitálnych certifikátov (OS/400 možnosť 34) a IBM HTTP Server (5722–DG1).
- Server iSeries A je základný systém na podpisovanie objektov aplikačných produktov firmy. Podpisovanie objektov produktov určených na distribúciu zákazníkom sa uskutočňuje na serveri iSeries A vykonaním týchto úloh:
  1. Na podpisovanie firemných produktov využívať API.
  2. Na export certifikátu na overovanie podpisu do súboru, aby mohol zákazník overovať podpísané objekty, využívať DCM.
  3. Napísanie programu na pridávanie overovacieho certifikátu do podpísanej aplikácie.

4. Napísanie programu ukončenia predinštalácie produktu, ktorý využíva API vkladajúce overovač. Toto rozhranie API umožňuje inštalačnému procesu produktu programovo pridať certifikát kontroly do pamäte certifikátov *SIGNATUREVERIFICATION na serveri iSeries zákazníka (servery iSeries B a C).

Zákaznícke servery iSeries B a C

- Na serveri iSeries B je spustený OS/400 verzia 5 vydanie 2 (V5R2).
- Na serveri iSeries C je spustený OS/400 verzia 5 vydanie 2 (V5R2).
- Na serveroch iSeries B a C je nainštalovaný a nakonfigurovaný Správca digitálnych certifikátov (možnosť 34) a IBM HTTP Server (5722–DG1).
- Servery iSeries B a C kúpia a prevezmú aplikáciu z webovej lokality vývojárskej spoločnosti aplikácie (ktorá vlastní server iSeries A).
- Servery iSeries B a C získajú kópiu certifikátu na kontrolu podpisu spoločnosti MyCo pri vytvorení pamäte certifikátov *SIGNATUREVERIFICATION inštalačným procesom v každom serveri iSeries zákazníka.

Požiadavky a predpoklady

Tento scenár je závislý na nasledujúcich požiadavkách a predpokladoch:
1. Všetky servery iSeries musia spĺňať požiadavky na inštaláciu a používanie Správcu digitálnych certifikátov (DCM).

   Poznámka: Splnenie požiadaviek na inštaláciu a používanie DCM je pre zákazníkov voliteľná podmienka (v tomto scenári servery iSeries B a C). Aj keď API vkladajúce overovač počas inštalačného procesu vytvorí sklad certifikátov *SIGNATUREVERIFICATION, v prípade potreby ho vytvorí s predvoleným heslom. Aby sa zabránilo neautorizovanému prístupu, musí zákazník na zmenu predvoleného hesla použiť DCM.
2. Na žiadnom z týchto serverov iSeries zatiaľ nikto DCM nekonfiguroval, ani nepoužíval.
3. Na všetkých serveroch iSeries je nainštalovaná najvyššia úroveň 128-bitovej verzie licencovaného programu Cryptographic Access Provider (5722-AC3).
4. Predvolená hodnota systémovej premennej verify object signatures during restore (QVFYOBJRST) v tomto scenári na všetkých serveroch iSeries je 3 a jej nastavenia neboli zmenené. Toto predvolené nastavenie zabezpečuje, aby bolo možné overovať podpisy počas obnovy objektov na serveri.
5. Systémový administrátor servera iSeries A musí mať na podpisovanie objektov špeciálne oprávnenie *ALLOBJ, alebo musí byť profil užívateľa autorizovaný na využívanie aplikácií na podpisovanie objektov.
6. Systémový operátor, alebo ktokoľvek iný (vrátane programu), kto vytvára sklad certifikátov cez DCM, špeciálne oprávnenia užívateľského profilu *SECADM a *ALLOBJ.
7. Na overovanie podpisov musí mať systémový administrátor, alebo ktokoľvek iný na všetkých ostatných serveroch iSeries špeciálne oprávnenie *AUDIT.

Kroky konfiguračnej úlohy

Na to, aby ste na serveri iSeries A mohli podpisovať objekty tak, ako je to popísané v tomto scenári, musíte splniť každú z týchto úloh:
1. Dokončite všetky potrebné kroky na inštaláciu a konfiguráciu všetkých potrebných produktov iSeries.
2. Použite program DCM na vytvorenie požiadavky o certifikát, určenej na získanie certifikátu podpisujúceho objekty od známej verejnej certifikačnej autority (CA).
3. Použite program DCM na vytvorenie definície aplikácie na podpisovanie objektov.
4. Použite program DCM na import podpisujúceho certifikátu podpísaného objektu do vašej definície aplikácie na podpisovanie objektov.
5. Použite program DCM na export vášho certifikátu podpisujúceho objekty ako certifikátu na kontrolu podpisu, ktorý môžu použiť vaši zákazníci na kontrolu podpisu na vašich aplikačných objektoch.
6. Zaktualizujte váš program na balenie aplikácií, aby na podpis vašej aplikácie použil rozhranie API Sign Object.
7. Vytvorte ukončovací program predinštalácie, ktorý používa rozhranie API Add Verifier ako časť procesu balenia aplikácie.
   Tento ukončovací program vám umožní počas procesu inštalácie vytvoriť na serveri iSeries sklad certifikátov *SIGNATUREVERIFICATION a pridať doň požadovaný certifikát na overovanie podpisov.

8. Nariaďte zákazníkom použitie programu DCM na vynulovanie predvoleného hesla pre pamäť certifikátov *SIGNATUREVERIFICATION v ich serveri iSeries.

Detaily scenára: Používanie rozhraní API na podpisovanie objektov a kontrolu podpisov na objektoch

Aby ste mohli použiť API OS/400 na podpisovanie objektov tak, ako je to popísané v tomto scenári, musíte splniť nasledujúce úlohy.

Krok 1: Dokončite všetky vyžadované kroky

Skôr, než vykonáte špecifické úlohy pre realizáciu tohto scenára, musíte splniť všetky úlohy spomenuté v požiadavkách na inštaláciu nevyhnutných produktov iSeries.

Krok 2: Použite program DCM na získanie certifikátu od známej verejnej certifikačnej autority

Tento scenár predpokladá, že ste Správcu digitálnych certifikátov (DCM) doteraz na vytváranie a spravovanie certifikátov nepoužili. Preto musíte ako súčasť vytvárania certifikátu na podpisovanie objektov vytvoriť aj sklad certifikátov *OBJECTSIGNING. Po jeho vytvorení vám tento sklad certifikátov poskytne možnosti, ako vytvoriť a spravovať certifikáty na podpisovanie objektov. Ak chcete získať certifikát od známej Certifikačnej autority (CA), musíte použiť DCM na vytvorenie identifikačných údajov a páru verejného a súkromného kľúča certifikátu a odovzdať tieto informácie CA, ktorá vám vydá certifikát.

Informácie na žiadosť o certifikát, ktoré musíte pre získanie certifikátu na podpisovanie objektov poskytnúť CA, vytvoríte vykonaním týchto krokov:

1. Spustite DCM.
2. Výberom **Vytvoriť nový sklad certifikátov** v navigačnom rámci DCM, spustite riadenú úlohu a vyplňte sériu formulárov. Tieto formuláre vás prevedú procesom vytváranie skladu certifikátov a certifikátu, ktorý môžete používať na podpisovanie objektov.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) navrchu stránky a dostanete sa k online pomoci.
3. Označte ***OBJECTSIGNING** ako sklad certifikátov, ktorý chcete vytvoriť a kliknite na **Pokračovať**.
4. Výberom **Áno** vytvorte certifikát ako súčasť vytvorenia skladu certifikátov *OBJECTSIGNING a kliknite na **Pokračovať**.
5. Ako podpisovateľa nového certifikátu označte **VeriSign, alebo iná Internetová Certifikačná autorita (CA)** a kliknutím na **Pokračovať** zobrazte formulár, ktorý vám umožní vytvoriť identifikačné údaje nového certifikátu.
6. Vyplňte formulár a kliknutím na **Pokračovať** zobrazte potvrdzovaciu stránku. Na tejto potvrdzovacej stránke sú zobrazené údaje na žiadosť o certifikát, ktoré musíte poskytnúť Certifikačnej autorite (CA), ktorá vydá váš certifikát. Údaje Žiadosti o podpis certifikátu (CSR) pozostávajú z verejného kľúča a ďalších informácií, ktoré ste zadali pri vytváraní certifikátu.
7. Starostlivo nakopírujte a vložte údaje CSR formulára žiadosti o certifikát, alebo do osobitného súboru, ktorý verejná CA pri žiadosti o certifikát požaduje. Musíte použiť všetky údaje CSR, vrátane riadkov Začiatku a Ukončenia žiadosti o nový certifikát. Keď túto stránku zavriete, údaje sa stratia a ich obnova nie je možná.
8. Formulár žiadosti, alebo súbor, odošlite CA, ktorú ste si vybrali na vydanie a podpísanie vášho certifikátu.
9. Kým pokročíte k ďalším krokom tohto scenára, počkajte, kým vám CA vráti podpísaný certifikát.

Krok 3: Vytvorte definíciu aplikácie na podpisovanie objektov

Po tom, čo ste svoju žiadosť certifikát odoslali známej CA, môžete s použitím DCM definovať aplikáciu, ktorú budete pri podpisovaní objektov využívať. Definícia aplikácie nemusí odkazovať na skutočnú aplikáciu; definícia aplikácie, ktorú vytvoríte, môže opisovať typ alebo skupinu objektov, ktoré plánujete podpísať. Definíciu potrebujete, aby ste obdržali ID aplikácie, ku ktorému priradíte certifikát, čím povolíte podpisovanie objektov.

Pri použití DCM na vytvorenie definície aplikácie podpisujúcej objekty nasledujte tieto kroky:

1. V navigačnom rámci kliknite na **Vybrať sklad certifikátov** a označte ***OBJECTSIGNING** ako sklad certifikátov, ktorý chcete otvoriť.

2. Keď sa zobrazí stránka Sklad certifikátov a heslo, napíšte heslo, ktoré ste zadali pri vytváraní tohto skladu certifikátov a kliknite na **Pokračovať**.
3. V navigačnom rámci označte **Spravovať aplikácie** a zobrazte zoznam úloh.
4. V zozname úloh označte **Pridať aplikáciu**, čím sa vám zobrazí formulár na definovanie aplikácie.
5. Vyplňte formulár a kliknite na **Pridať**.

Po prijatí podpísaného certifikátu od certifikačnej autority ho môžete priradiť aplikácii, ktorú ste vytvorili.

Krok 4: Naimportujte podpísaný verejný certifikát a priraďte ho aplikácii na podpisovanie objektov.

Ak chcete importovať váš certifikát a jeho priradením aplikácii povoliť podpisovanie objektov, postupujte takto:
1. Spustite DCM.
2. V navigačnom rámci kliknite na **Vybrať sklad certifikátov** a označte ***OBJECTSIGNING** ako sklad certifikátov, ktorý chcete otvoriť.
3. Keď sa zobrazí stránka Sklad certifikátov a heslo, napíšte heslo, ktoré ste zadali pri vytváraní tohto skladu certifikátov a kliknite na **Pokračovať**.
4. Keď sa obnoví obsah navigačného rámca, označte **Spravovať certifikáty** a zobrazte zoznam úloh.
5. Výberom **Importovať certifikát** zo zoznamu úloh spustite proces importu podpísaného certifikátu do skladu certifikátov.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) navrchu stránky a dostanete sa k online pomoci.
6. Zo zoznamu úloh **Spravovať certifikáty** vyberte **Priradiť certifikát** a zobrazte zoznam certifikátov v aktuálnom sklade certifikátov.
7. V zozname označte správny certifikát a kliknutím na **Priradiť aplikácii** zobrazte zoznam definícií aplikácií v aktuálnom sklade certifikátov.
8. Označte v zozname svoju aplikáciu a kliknite na **Pokračovať**. Zobrazí sa stránka s potvrdením úspešného priradenia, alebo s chybovou správou, ak sa vyskytol nejaký problém.

Po vykonaní tejto úlohy ste pripravený podpisovať aplikácie a iné objekty s použitím API OS/400. Aby ste si však zabezpečili, že vy, aj iní budete môcť overovať podpisy, musíte exportovať nevyhnutné certifikáty do súboru a presunúť ich na akékoľvek servery iSeries, na ktoré sa inštalujú vaše aplikácie. Zákaznícke servery iSeries musia byť schopné počas inštalácie použiť certifikáty pri overovaní podpisov na vašich aplikáciách. Ako súčasť procesu inštalácie môžete na nevyhnutné nakonfigurovanie overovania podpisov u vašich zákazníkov použiť API vkladajúce overovač. Môžete napríklad vytvoriť ukončovací program predinštalácie, ktorý volá rozhranie API za účelom konfigurácie servera iSeries vášho zákazníka.

Krok 5: Vyexportujte certifikáty na umožnenie kontroly podpisov v ostatných serveroch iSeries.

Podpisovanie objektov si nevyhnutne vyžaduje, aby ste vy, aj iní, mali možnosť overiť si bezúhonnosť podpisu a určiť, či boli na podpísaných objektoch vykonané zmeny. Ak chcete overovať podpisy objektov na rovnakom systéme, ktorý ich podpisuje, musíte s použitím DCM vytvoriť sklad certifikátov *SIGNATUREVERIFICATION. Tento sklad certifikátov musí obsahovať kópiu certifikátu na podpisovanie objektov aj kópiu certifikátu CA, ktorá ho vydala.

Ak chcete ostatným umožniť overenie podpisu, musíte im poskytnúť kópiu certifikátu, ktorý ho podpísal. Ak na vydanie certifikátu používate Lokálnu certifikačnú autoritu (CA), musíte im tiež poskytnúť kópiu certifikátu Lokálnej CA.

Ak chcete pomocou DCM overovať podpisy na systéme, ktorý objekty podpísal (v tomto scenári iSeries A), musíte dodržať tieto kroky:
1. V navigačnom rámci vyberte **Vytvoriť nový sklad certifikátov** a označte ***SIGNATUREVERIFICATION** ako sklad certifikátov, ktorý chcete vytvoriť.
2. Kliknutím na **Áno** prekopírujete existujúce certifikáty na podpisovanie objektov do nového skladu certifikátov ako certifikáty na overovanie podpisov.
3. Zadajte heslo pre nový sklad certifikátov a kliknutím na **Pokračovať** ho vytvorte. Odteraz môžete s použitím DCM overovať podpísané objekty na systéme, ktorý používate aj na ich podpisovanie.

Ak chcete pomocou DCM exportovať kópiu certifikátu na podpisovanie objektov ako certifikát na overovanie objektov, aby mohli ostatní overovať vaše podpisy, vykonajte nasledujúce kroky:

1. V navigačnom rámci vyberte **Spravovať certifikáty** a potom označte úlohu **Exportovať certifikát**.
2. Výberom **Podpisovanie objektov** zobrazte zoznam certifikátov na podpisovanie objektov, ktoré chcete exportovať.
3. Vyberte si zo zoznamu správny certifikát na podpisovanie objektov a kliknite na **Export**.
4. Ako cieľ označte **Uložiť ako certifikát na overovanie podpisov** a kliknite na **Pokračovať**.
5. Zadajte úplný názov cesty a súboru, kam chcete exportovať certifikát na overovanie podpisov a kliknutím na **Pokračovať** ho exportujte.

Teraz môžete tento súbor pridať do inštalačného balíka, ktorý pre tento produkt vytvárate. S použitím API vkladajúceho overovač ako súčasti inštalačného programu môžete tento certifikát pridať do zákazníkovho skladu certifikátov *SIGNATUREVERIFICATION. Ak tento sklad certifikátov ešte neexistuje, toto API ho vytvorí. Inštalačný program vášho produktu potom môže počas obnovovania objektov aplikácie na klientovom serveri iSeries overiť ich podpisy.

Krok 6: Zaktualizujte váš program na balenie aplikácií, aby na podpis vašej aplikácie použil rozhrania API servera iSeries.

Teraz, keď už máte súbor certifikátu na overovanie podpisov, ktorý môžete pridať do vášho aplikačného balíka, môžete použiť API podpisujúce objekty na zápis do už existujúcej aplikácie, ktorým, počas balenia aplikácie pred distribúciou klientovi, podpíšete svoje produktové knižnice.

Aby ste lepšie pochopili použitie API podpisujúceho objekty ako súčasti vášho programu na balenie aplikácií, prezrite si nasledujúci príklad kódu. Tento vzorový úryvok kódu, napísaný v jazyku C, nie je úplným programom na podpisovanie a balenie aplikácií; je to skôr ukážka tej časti podobného programu, ktorá volá API podpisujúce objekty. Ak sa rozhodnete tento vzorový príklad použiť, zmeňte ho tak, aby vyhovoval vašim potrebám. Z bezpečnostných dôvodov vám IBM odporúča radšej si prispôsobiť tento príklad, než použiť predvolené hodnoty v ňom uvedené.

Poznámka: IBM vám udeľuje neexkluzívne právo na používanie všetkých príkladov programovania, z ktorých môžete vygenerovať podobnú funkciu prispôsobenú pre vaše vlastné špecifické potreby. Všetok vzorový kód poskytuje IBM len na ilustračné účely. Tieto príklady neboli dôkladne testované vo všetkých podmienkach. IBM preto nemôže garantovať, alebo predpokladať spoľahlivosť, použiteľnosť, alebo fungovanie týchto programov. Všetky tieto programy sú vám poskytnuté ″TAK AKO SÚ″ bez akýchkoľvek záruk žiadneho druhu. Vyplývajúce záruky neprekračovania, predajnosti, alebo vhodnosti pre konkrétny účel striktne odmietame.

Zmeňte tento úryvok kódu tak, aby vyhovoval vašim potrebám volania API podpisujúce objekty, ako súčasti programu na balenie vašich aplikácií. Do tohto programu potrebujete doplniť dva parametre: názov knižnice, ktorá má byť podpisovaná a názov ID aplikácie na podpisovanie objektov; ID aplikácie na veľké a malé písmená citlivý je, názov knižnice nie je. Vami napísaný program môže tento úryvok zavolať aj niekoľko krát, ak sú v časti, ktorú podpisujete použité viaceré knižnice.

Poznámka: Prečítajte si “Právne vyhlásenia” na strane 43, kde sú uvedené dôležité právne informácie.

```
/* ------------------------------------------------------------- */
/*                                                               */
/* COPYRIGHT (C) IBM CORP. 2002, 2004                            */
/*                                                               */
/* Use Sign Object API to sign one or more libraries             */
/*                                                               */
/* The API will digitally sign all objects in a specified library   */
/*                                                               */
/*                                                               */
/*                                                               */
/* IBM grants you a nonexclusive copyright license to use all       */
/* programming code examples from which you can generate similiar   */
/* function tailored to your own specific needs.                 */
/* All sample code is provided by IBM for illustrative purposes     */
/* only. These examples have not been thoroughly                 */
/* tested under all conditions.  IBM, therefore, cannot          */
```

```
/* guarantee or imply reliability, serviceability, or function      */
/* of these programs.  All programs contained herein are            */
/* provided to you "AS IS" without any warranties of any kind.      */
/* The implied warranties of non-infringement, merchantability and  */
/* fitness for a particular purpose are expressly disclaimed.       */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* The parameters are:                                              */
/*                                                                  */
/*  char *   name of the library to sign                            */
/*  char *   name of the application ID                             */
/*                                                                  */

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

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

    /* parameters:

       char * library to sign objects in,
       char * application identifier to sign with

     */

    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;     /* return exceptions for any errors  */


    /* ------------------------------------ */
    /* construct path name given library name */
    /* ------------------------------------ */
    memset(libname, '\00', 11); /* initialize library name */
    for(lib_length = 0;
        ((*(argv[1] + lib_length) != ' ') &&
         (*(argv[1] + lib_length) != '\00'));
        lib_length++);
    memcpy(argv[1], libname, lib_length); /* fill in library name */

    /* build path name parm for API call */
    sprintf(path_name, "/QSYS.LIB/%s.LIB/*", libname);
    path_length = strlen(path_name);

    /* ---------------------------- */
    /* find length of application id */
    /* ---------------------------- */
    for(applid_length = 0;
        ((*(argv[2] + applid_length) != ' ') &&
         (*(argv[2] + applid_length) != '\00'));
        applid_length++);

    /* ------------------------------ */
    /* sign all objects in this library */
    /* ------------------------------ */
    QYDOSGNO  (path_name,             /* path name to object         */
               &path_length,          /* length of path name         */
               "OBJN0100",       /* format name                       */
```

```
                argv[2],              /* application identifier (ID) */
                &applid_length,       /* length of  application ID   */
                "1",                  /* replace duplicate signature */
                multi_objects,        /* how to handle multiple
                                            objects                 */
                &multiobj_length,     /* length of multiple objects
                                          structure to use
                                        (0=no mult.object structure)*/
                &error_code);     /* error code                       */


        return 0;

}
```

Krok 7: Vytvorte ukončovací program predinštalácie, ktorý používa rozhranie API Add Verifier.

Teraz, keď už máte naprogramovaný proces podpisovania vašej aplikácie, môžete používať API vkladajúce overovač ako súčasť vášho inštalačného programu a vytvoriť tak konečný produkt pre distribúciu. Rozhranie API Add Verifier môžete napríklad použiť ako časť ukončovacieho programu predinštalácie na zabezpečenie pridania certifikátu do pamäte certifikátov pred obnovením podpísaných aplikačných objektov. To umožní vášmu inštalačnému programu overovať podpisy na objektoch vašej aplikácie počas ich obnovovania na klientovom serveri iSeries.

Poznámka: Z bezpečnostných dôvodov nemôže toto API pridať do skladu certifikátov *SIGNATUREVERIFICATION certifikát Certifikačnej autority (CA). Ak by ste to urobili, systém by automaticky považoval CA za dôveryhodný zdroj certifikátov. Následne systém predpokladá, že certifikát vydaný touto CA pochádza z dôveryhodného zdroja. Preto nemôžete toto API použiť na vytvorenie programu na ukončenie inštalácie, ktorý vloží CA certifikát do skladu certifikátov. Aby sa zabezpečilo, že niekto bude musieť špecificky a manuálne skontrolovať, ktorým CA môže systém dôverovať, musíte na pridanie CA certifikátu použiť Správcu digitálnych certifikátov (Digital Certificate Manager). Toto môže zabrániť možnosti importovať certifikáty zo zdrojov, ktoré administrátor nevedome označil ako dôveryhodné.

Ak chcete zabrániť použitiu tohto rozhrania API na pridanie certifikátu na kontrolu do vašej pamäte certifikátov *SIGNATUREVERIFICATION bez vášho vedomia, mali by ste zvážiť zakázanie tohto rozhrania API vo vašom systéme. To môžete spraviť, ak použijete nástroje na údržbu systému (system service tools - SST) a zakážete zmeny hodnôt súvisiacich s bezpečnosťou systému..

Aby ste lepšie pochopili použitie API vkladajúceho overovač ako súčasti inštalačného programu vašej aplikácie, prezrite si nasledujúci príklad kódu. Tento vzorový úryvok kódu, napísaný v jazyku C, nie je úplným programom na ukončenie predinštalácie; je to skôr ukážka tej časti podobného programu, ktorá volá API vkladajúce overovač. Ak sa rozhodnete tento vzorový príklad použiť, zmeňte ho tak, aby vyhovoval vašim potrebám. Z bezpečnostných dôvodov vám firma IBM odporúča, aby ste si radšej prispôsobili tento príklad, než použili v ňom uvedené predvolené hodnoty.

Poznámka: IBM vám udeľuje neexkluzívne právo na používanie všetkých príkladov programovania, z ktorých môžete vygenerovať podobnú funkciu prispôsobenú pre vaše vlastné špecifické potreby. Všetok vzorový kód poskytuje IBM len na ilustračné účely. Tieto príklady neboli dôkladne testované vo všetkých podmienkach. IBM preto nemôže garantovať, alebo predpokladať spoľahlivosť, použiteľnosť, alebo fungovanie týchto programov. Všetky tieto programy sú vám poskytnuté ″TAK AKO SÚ″ bez akýchkoľvek záruk žiadneho druhu. Vyplývajúce záruky neprekračovania, predajnosti, alebo vhodnosti pre konkrétny účel striktne odmietame.

Zmeňte tento úryvok kódu tak, aby vyhovoval vašim potrebám používania API vkladajúceho overovač ako súčasti programu na ukončenie predinštalácie, ktorý počas inštalácie produktu pridá na zákazníkov server iSeries požadovaný požadovaný certifikát na overovanie podpisov.

Poznámka: Prečítajte si “Právne vyhlásenia” na strane 43, kde sú uvedené dôležité právne informácie.

```
/* ------------------------------------------------------------ */
/*                                                              */
/* COPYRIGHT (C) IBM CORP. 2002, 2004                           */
/*                                                              */
/* Use Add Verifier API to add a certificate in the specified   */
/* integrated file system file to the *SIGNATUREVERIFICATION    */
/* certificate store.                                           */
/*                                                              */
/*                                                              */
/* The API will create the certificate store if it does not exist.  */
/* If the certificate store is created it will be given a default   */
/* password that should be changed using DCM as soon as possible.   */
/* This warning needs to be given to the owners of the system that  */
/* use this program.                                            */
/*                                                              */
/*                                                              */
/*                                                              */
/* IBM grants you a nonexclusive copyright license to use all   */
/* programming code examples from which you can generate similiar   */
/* function tailored to your own specific needs.                */
/* All sample code is provided by IBM for illustrative purposes     */
/* only. These examples have not been thoroughly                */
/* tested under all conditions.  IBM, therefore, cannot         */
/* guarantee or imply reliability, serviceability, or function  */
/* of these programs.  All programs contained herein are        */
/* provided to you "AS IS" without any warranties of any kind.  */
/* The implied warranties of non-infringement, merchantability and  */
/* fitness for a particular purpose are expressly disclaimed.   */
/*                                                              */
/*                                                              */
/*                                                              */
/* The parameters are:                                          */
/*                                                              */
/*  char *   path name to integrated file system  file that holds   */
/*           the certificate                                    */
/*  char *   certificate label to give certificate              */
/*                                                              */
/*                                                              */
/*                                                              */
/* ------------------------------------------------------------ */

#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];

    /* find length of path name */
    for(pathname_length = 0;
        ((*(pathname + pathname_length) != ' ') &&
         (*(pathname + pathname_length) != '\00'));
        pathname_length++);

    /* find length of certificate label */
    for(cert_label_length = 0;
        ((*(certlabel + cert_label_length) != ' ') &&
         (*(certlabel + cert_label_length) != '\00'));
        cert_label_length++);


    error_code.Bytes_Provided = 0;     /* return exceptions for any errors  */
```

```
    QydoAddVerifier (pathname,         /* path name to file with certificate*/
                     &pathname_length, /* length of path name               */
                     "OBJN0100",       /* format name                       */
                     certlabel,        /* certificate label                 */
                     &cert_label_length, /* length of certificate label     */
                     &error_code);     /* error code                        */

    return 0;
}
```

Po splnení všetkých týchto úloh môžete baliť svoje aplikácie a distribuovať ich svojim klientom. Keď si vašu aplikáciu inštalujú, ako súčasť inštalačného procesu prebieha aj overovanie podpísaných objektov aplikácie. Neskôr môžu zákazníci na overovanie podpísaných objektov vašej aplikácie použiť Správcu digitálnych certifikátov (DCM). To umožní vašim zákazníkom rozhodnúť sa, či je zdroj aplikácie dôveryhodný a určiť, či sa v aplikácii od vášho podpisu nevyskytli žiadne zmeny.

Poznámka: Váš inštalačný program možno vášmu klientovi vytvoril sklad certifikátov *SIGNATUREVERIFICATION s predvoleným prístupovým heslom. Z dôvodu ochrany pred neautorizovaným prístupom by ste mali poradiť vášmu zákazníkovi použitie programu DCM na vynulovanie hesla pre pamäť certifikátov čím skôr.

Krok 8: Nariaďte zákazníkom vynulovanie predvoleného hesla pre pamäť certifikátov *SIGNATUREVERIFICATION.

Ako súčasť inštalačného procesu mohlo API vkladajúce overovač vytvoriť na zákazníkovom serveri iSeries sklad certifikátov *SIGNATUREVERIFICATION. Ak API tento sklad vytvorilo, priradilo mu preddefinované heslo. Následne by ste mali z dôvodu ochrany pamäte certifikátov pred neautorizovaným prístupom poradiť vašim zákazníkom použitie programu DCM na vynulovanie tohto hesla.

Vaši zákazníci by mali vykonaním týchto krokov resetovať heslo k skladu certifikátov *SIGNATUREVERIFICATION:

1. Spustite DCM.
2. V navigačnom rámci kliknite na **Vybrať sklad certifikátov** a vyberte ***SIGNATUREVERIFICATION** ako sklad, ktorý chcete otvoriť.
3. Keď sa zobrazí stránka Sklad certifikátov a heslo, kliknutím na **Resetovať heslo** zobrazte stránku Resetovať heslo k certifikačnému skladu.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) navrchu stránky a dostanete sa k online pomoci.
4. Zadajte nové heslo k skladu, pre potvrdenie ho zadajte znova, určite politiku vypršania platnosti hesla pre tento certifikačný sklad a kliknite na **Pokračovať**.

Scenár: Použitie funkcie Centrálneho riadenia programu iSeries Navigator na podpisovanie objektov

Situácia

Vaša spoločnosť (MyCo, s.r.o.) vyvíja aplikácie, ktoré distribuuje na mnohé servery iSeries na mnoho miest spoločnosti. Ako sieťový administrátor ste zodpovedný za to, že sú všetky tieto aplikácie nainštalované a aktualizované na všetkých firemných serveroch iSeries. V súčasnosti používate funkciu programu iSeries Navigator s názvom Centrálne riadenie na jednoduché balenie a distribúciu týchto aplikácií a na vykonávanie ďalších administratívnych úloh, za ktoré ste zodpovedný. Strávite však priveľa času hľadaním a opravovaním problémov, ktoré vznikajú vďaka neautorizovaným zmenám v objektoch. Preto chcete zaistiť vyššiu bezpečnosť týchto objektov ich elektronickým podpisovaním.

Preskúmali ste možnosti podpisovania objektov v OS/400 a zistili ste, že počnúc V5R2 vám Riadiaca centrála umožňuje podpisovať objekty počas ich balenia a distribúcie. S použitím Riadiacej centrály môžete dosiahnuť bezpečnostné ciele vašej firmy efektívne a relatívne jednoducho. Tiež ste sa rozhodli vytvoriť Lokálnu certifikačnú

autoritu (CA) a použiť ju na vydanie certifikátu na podpisovanie objektov. Použitie certifikátu vydaného lokálnou certifikačnou autoritou na podpisovanie objektov obmedzuje náklady na túto zabezpečovaciu technológiu, pretože nemusíte kupovať certifikát od známej verejnej certifikačnej autority.

Tento príklad slúži ako užitočný úvod k postupu ako nakonfigurovať a používať podpisovanie objektov aplikácií, ktoré distribuujete na mnohé firemné servery iSeries.

Výhody scenára

Tento scenár poskytuje nasledujúce výhody:
- Balenie a podpisovanie objektov pomocou Riadiacej centrály znižuje množstvo času, ktoré musíte stráviť distribúciou podpísaných objektov na vaše firemné servery iSeries.
- Používanie Riadiacej centrály na podpisovanie zbalených objektov znižuje počet krokov, ktoré musíte pri podpisovaní vykonať, pretože proces podpisovania je súčasťou procesu balenia.
- Podpisovanie balíka objektov vám umožní jednoducho určiť, či sa objekty od svojho podpisu zmenili. Toto vám môže v budúcnosti ušetriť vyhľadávanie a odstraňovanie problémov s aplikáciami.
- Použitie certifikátu vydaného Lokálnou certifikačnou autoritou (CA) znižuje náklady na realizáciu podpisovania objektov.

Ciele

V tomto scenári chce firma MyCo, s.r.o. elektronicky podpisovať aplikácie, ktoré distribuuje v rámci firmy na mnohé servery iSeries. Ako administrátor siete v spoločnosti MyCo, Inc. už používate funkciu centrálneho riadenia na množstvo administratívnych úloh týkajúcich sa serverov iSeries. To chcete teraz rozšíriť aj o používanie Riadiacej centrály na podpisovanie firemných aplikácií, ktoré distribuujete na ďalšie servery iSeries.

Ciele tohto scenáru sú nasledovné:
- Firemné aplikácie musia byť podpísané certifikátom vydaným Lokálnou CA, aby sa znížili náklady na podpisovanie aplikácií.
- Systémoví administrátori a ďalší oprávnení užívatelia musia mať možnosť jednoducho overiť elektronický podpis v každom serveri iSeries a overiť si tak zdroj a neporušenosť podpísaných firemných objektov. Aby sme to dosiahli, musí mať každý zo serverov iSeries vo svojom sklade certifikátov *SIGNATUREVERIFICATION kópiu firemného certifikátu na overenie podpisov a certifikátu Lokálnej certifikačnej autority (CA).
- Overovanie podpisov na firemných aplikáciách umožňuje administrátorom iSeries a iným zistiť, či sa obsah objektov od ich podpísania zmenil.
- Administrátori musia mať možnosť využiť Riadiacu centrálu na balenie, podpisovanie a distribúciu ich aplikácií na servery iSeries.

Detaily

Nasledujúci diagram objasňuje proces podpisovania objektov a overovania podpisov pri realizácii tohto scenára:

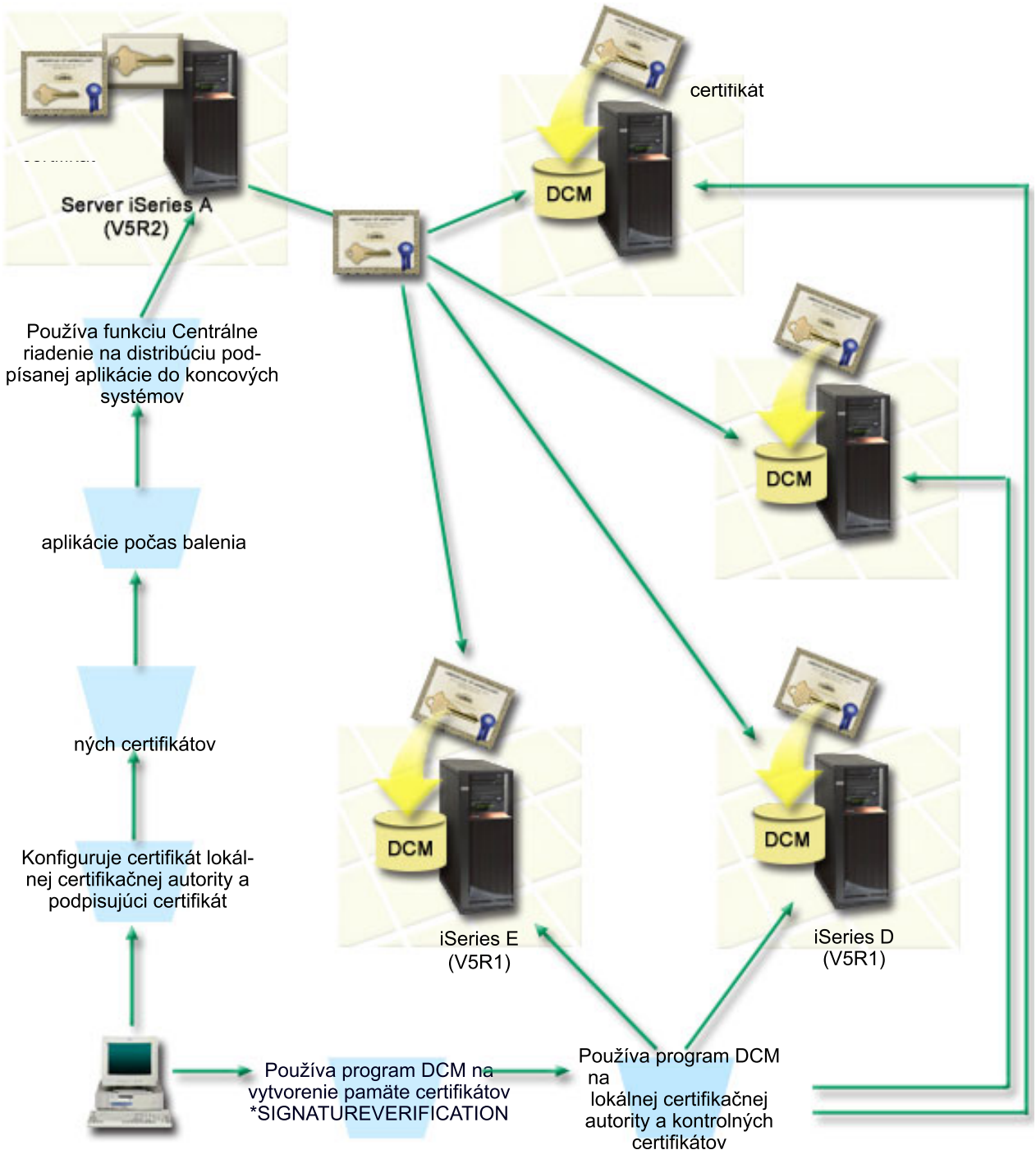


Diagram zobrazuje nasledujúce body súvisiace so scenárom:

Centrálny systém (iSeries A)

- Na serveri iSeries A je spustený OS/400 verzia 5 vydanie 2 (V5R2).
- Server iSeries A slúži ako centrálny systém, na ktorom je spustená Riadiaca centrála, vrátane balenia a distribúcie firemných aplikácií.
- Na serveri iSeries A je nainštalovaná 128-bitová verzia produktu Cryptographic Access Provider 128-bit for iSeries (5722–AC3).
- Na serveri iSeries A je nainštalovaný a nakonfigurovaný Správca digitálnych certifikátov (OS/400 možnosť 34) a IBM HTTP Server (5722–DG1).

- Server iSeries A vystupuje ako Lokálna certifikačná autorita (CA) a na tomto systéme je umiestnený aj certifikát na podpisovanie objektov.
- Server iSeries A je základným systémom na podpisovanie objektov firemných aplikácií. Podpisovanie objektov produktov určených na distribúciu zákazníkom sa uskutočňuje na serveri iSeries A vykonaním týchto úloh:
  1. Pomocou DCM vytvorte Lokálne CA a ňou vytvorte certifikát na podpisovanie objektov.
  2. Pomocou programu DCM vyexportujte kópiu certifikátu lokálnej certifikačnej autority a certifikátu na kontrolu podpisu do súboru, čím umožníte koncovým systémom (servery iSeries B, C, D a E) kontrolovať podpísané objekty.
  3. Pomocou Riadiacej centrály podpíšte objekty aplikácie a zabaľte ich so súbormi overovacieho certifikátu.
  4. Pomocou Riadiacej centrály distribuujte podpísané aplikácie a certifikačné súbory na koncové systémy.

Servery koncových systémov (iSeries B, C, D a E)

- Na serveroch iSeries B a C je spustený OS/400 verzia 5 vydanie 2 (V5R2).
- Na serveroch iSeries D a E je spustený OS/400 verzia 5 vydanie 1 (V5R1).
- Na serveroch iSeries B, C, D a E je nainštalovaný a nakonfigurovaný Správca digitálnych certifikátov (možnosť 34) a IBM HTTP Server (5722–DG1).
- Servery iSeries B, C, D a E príjmu kópiu certifikátu spoločnosti na kontrolu podpisu a certifikátu lokálnej certifikačnej autority od centrálneho systému (server iSeries A), keď systémy príjmu podpísanú aplikáciu.
- DCM je používané na vytvorenie skladu certifikátov *SIGNATUREVERIFICATION a na importovanie certifikátu Lokálnej CA a overovacieho certifikátu do tohto skladu.

Požiadavky a predpoklady

Tento scenár je závislý na nasledujúcich požiadavkách a predpokladoch:

1. Všetky servery iSeries musia spĺňať požiadavky na inštaláciu a používanie Správcu digitálnych certifikátov (DCM).
2. Na žiadnom z týchto serverov iSeries zatiaľ nikto DCM nekonfiguroval, ani nepoužíval.
3. Server iSeries A spĺňa požiadavky na inštaláciu a používanie programu iSeries Navigator a jeho funkcie s názvom Centrálne riadenie.
4. Na všetkých koncových systémoch iSeries musí byť spustený server Riadiacej centrály.
5. Na všetkých serveroch iSeries je nainštalovaná najvyššia úroveň 128-bitovej verzie licencovaného programu Cryptographic Access Provider (5722-AC3).
6. Predvolená hodnota systémovej premennej verify object signatures during restore (QVFYOBJRST) v tomto scenári na všetkých serveroch iSeries je 3 a jej nastavenia neboli zmenené. Toto predvolené nastavenie zabezpečuje, aby bolo možné overovať podpisy počas obnovy objektov na serveri.
7. Systémový administrátor servera iSeries A musí mať na podpisovanie objektov špeciálne oprávnenie *ALLOBJ, alebo musí byť profil užívateľa autorizovaný na využívanie aplikácií na podpisovanie objektov.
8. Sieťový operátor, alebo ktokoľvek iný, kto vytvára sklad certifikátov cez DCM, musí mať špeciálne oprávnenia užívateľského profilu *SECADM a *ALLOBJ.
9. Na overovanie podpisov musí mať systémový administrátor, alebo ktokoľvek iný na všetkých ostatných serveroch iSeries špeciálne oprávnenie *AUDIT.

Kroky konfiguračnej úlohy

Aby ste mohli zrealizovať tento scenár, musíte splniť dve skupiny úloh: Jedna skupina vám umožňuje nastaviť server iSeries A tak, aby na podpisovanie a distribúciu objektov používal Riadiacu centrálu. Druhá skupina úloh umožňuje systémovým administrátorom a iným overovať podpisy týchto aplikácií na všetkých serveroch iSeries.

Zoznam úloh pre podpisovanie objektov

Na to, aby ste na serveri iSeries A mohli podpisovať objekty tak, ako je to popísané v tomto scenári, musíte splniť každú z týchto úloh:

1. Dokončite všetky potrebné kroky na inštaláciu a konfiguráciu všetkých potrebných produktov iSeries.
2. Použite program DCM na vytvorenie lokálnej certifikačnej autority (CA) na vydanie súkromného certifikátu podpisujúceho objekty.

3. Použite program DCM na vytvorenie definície aplikácie.
4. Použite program DCM na priradenie certifikátu k definícii aplikácie na podpisovanie objektov.
5. Použite program DCM na export certifikátov, ktoré musia použiť ostatné systémy na kontrolu podpisov objektov. Ako certifikát na overovanie podpisov musíte do súborov exportovať kópiu certifikátu Lokálnej CA, ako aj kópiu certifikátu na podpisovanie objektov.
6. Presuňte súbory certifikátov do každého koncového systému iSeries, v ktorom plánujete kontrolovať podpisy.
7. Použite funkciu centrálneho riadenia programu iSeries Navigator na podpísanie objektov aplikácie.

Zoznam úloh pre overovanie podpisov

Predtým, ako môžete použiť funkciu Centrálne riadenie na prenos podpísaných objektov aplikácie do koncových systémov iSeries, musíte v každom z nich vykonať nasledujúce konfiguračné úlohy kontroly podpisu. Skôr než budete môcť počas obnovy podpísaných objektov na koncovom systéme úspešne overovať podpisy, musí byť ukončená konfigurácia overovania podpisov.

Aby ste mohli overovať podpisy na objektoch tak, ako je to popísané v tomto scenári, musíte na každom koncovom systéme iSeries splniť tieto úlohy:
8. Použite program DCM na vytvorenie pamäte certifikátov *SIGNATUREVERIFICATION.
9. Použite program DCM na import certifikátu lokálnej certifikačnej autority a certifikátu na kontrolu podpisu.

Detaily scenára: Použitie funkcie Centrálne riadenie programu iSeries Navigator na podpisovanie objektov

Aby ste mohli používať Riadiacu centrálu na podpisovanie objektov tak, ako je to popísané v tomto scenári, musíte ju splnením nasledujúcich úloh nakonfigurovať.

Krok 1: Dokončite všetky vyžadované kroky

Skôr, než vykonáte špecifické úlohy pre realizáciu tohto scenára, musíte splniť všetky úlohy spomenuté v požiadavkách na inštaláciu nevyhnutných produktov iSeries.

Krok 2: Vytvorte lokálnu certifikačnú autoritu na vydanie súkromného certifikátu podpisujúceho objekty

Proces vytvárania Lokálnej certifikačnej autority (CA) pomocou Správcu digitálnych certifikátov (DCM) si vyžaduje vyplnenie série formulárov. Tieto formuláre vás sprevádzajú procesom vytvárania CA a napĺňania ďalších úloh, ktoré sú nevyhnutné ak chcete začať používať digitálne certifikáty pre SSL, podpisovanie objektov a overovanie podpisov. Aj napriek tomu, že v tomto scenári nepotrebujete konfigurovať certifikáty pre SSL, aby ste systém nakonfigurovali na podpisovanie objektov, musíte vyplniť všetky formuláre v tejto úlohe.

Pri použití DCM na vytvorenie a prevádzkovanie Lokálnej CA, nasledujte tieto kroky:
1. Spustite DCM.
2. V navigačnom rámci DCM označte **Vytvoriť Certifikačnú autoritu (CA)**, čím zobrazíte sériu formulárov.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) navrchu stránky a dostanete sa k online pomoci.
3. Vyplňte všetky formuláre v tejto riadenej úlohe. Pri vypĺňaní tejto úlohy musíte urobiť nasledovné:
   a. Poskytnúť identifikačné údaje pre Lokálnu CA.
   b. Nainštalovať certifikát Lokálnej CA do vášho prehliadača, aby bol váš softvér schopný Lokálnu CA rozoznať a overiť platnosť certifikátov, ktoré vydala.
   c. Zadajte údaje o politike pre vašu Lokálnu CA.
   d. Použite novú Lokálnu CA a vydajte serverový, alebo klientsky certifikát, ktorý môže vaša aplikácia využívať na pripojenia SSL.

      Poznámka: Aj napriek tomu, že ho v tomto scenári nepoužijete, musíte tento certifikát vytvoriť, aby ste mohli používať Lokálnu CA na vydanie certifikátu, ktorý potrebujete, teda certifikátu na podpisovanie objektov. Ak túto úlohu zrušíte bez vytvorenia certifikátu, musíte vytvoriť svoj certifikát na podpisovanie objektov a sklad certifikátov *OBJECTSIGNING, v ktorom bude uložený, osobitne.

e. Označte aplikácie, ktoré môžu používať tento klientsky, alebo serverový certifikát pre pripojenia SSL.

   Poznámka: Pre účely tohto scenára neoznačujte žiadne aplikácie a kliknutím na **Pokračovať** zobrazte ďalší formulár.

f. Použitím novej Lokálnej CA vydajte certifikát na podpisovanie objektov, ktorý budú môcť aplikácie využívať na digitálne podpisovanie. Táto úloha vytvorí sklad certifikátov *OBJECTSIGNING. To je sklad certifikátov, ktorý používate pri spravovaní certifikátov na podpisovanie objektov.

g. Vyberte aplikácie, ktoré majú dôverovať vašej lokálnej certifikačnej autorite.

   Poznámka: Pre účely tohto scenára neoznačujte žiadne aplikácie a kliknutím na **Pokračovať** ukončite úlohu.

Teraz, keď ste vytvorili Lokálnu CA a certifikát na podpisovanie objektov, musíte pred tým, než začnete podpisovať objekty, definovať aplikácie, ktoré ho budú používať.

Krok 3: Vytvorte definíciu aplikácie na podpisovanie objektov

Po tom, čo ste vytvorili svoj certifikát na podpisovanie objektov, musíte s použitím Správcu digitálnych certifikátov (DCM) definovať aplikáciu, ktorú budete pri podpisovaní objektov využívať. Definícia aplikácie nemusí odkazovať na skutočnú aplikáciu; definícia aplikácie, ktorú vytvoríte, môže opisovať typ alebo skupinu objektov, ktoré plánujete podpísať. Definíciu potrebujete, aby ste obdržali ID aplikácie, ku ktorému priradíte certifikát, čím povolíte podpisovanie objektov.

Pri použití DCM na vytvorenie definície aplikácie podpisujúcej objekty nasledujte tieto kroky:
1. V navigačnom rámci kliknite na **Vybrať sklad certifikátov** a označte ***OBJECTSIGNING** ako sklad certifikátov, ktorý chcete otvoriť.
2. Keď sa zobrazí stránka Sklad certifikátov a heslo, napíšte heslo, ktoré ste zadali pri vytváraní tohto skladu certifikátov a kliknite na **Pokračovať**.
3. V navigačnom rámci označte **Spravovať aplikácie** a zobrazte zoznam úloh.
4. V zozname úloh označte **Pridať aplikáciu**, čím sa vám zobrazí formulár na definovanie aplikácie.
5. Vyplňte formulár a kliknite na **Pridať**.

Teraz musíte aplikácii, ktorú ste vytvorili, priradiť certifikát na podpisovanie objektov.

Krok 4: Priraďte certifikát k definícii aplikácie na podpisovanie objektov

Nasledovaním týchto krokov priradíte certifikát vašej aplikácii podpisujúcej objekty:
1. V navigačnom rámci DCM označte **Spravovať certifikáty** a zobrazte zoznam úloh.
2. Zo zoznamu úloh vyberte **Priradiť certifikát**, čím zobrazíte zoznam certifikátov v aktuálnom sklade certifikátov.
3. V zozname označte správny certifikát a kliknutím na **Priradiť aplikácii** zobrazte zoznam definícií aplikácií v aktuálnom sklade certifikátov.
4. Označte v zozname jednu, alebo viac aplikácií a kliknite na **Pokračovať**. Zobrazí sa vám stránka so správou potvrdzujúcou priradenie certifikátu, alebo poskytujúcou chybové informácie o probléme, ktorý sa vyskytol.

Po vykonaní tejto úlohy ste pripravený počas balenia a distribúcie podpisovať objekty pomocou Riadiacej centrály. Aby ste si však zabezpečili, že vy aj iní budete môcť overovať podpisy, musíte exportovať nevyhnutné certifikáty do súborov a presunúť ich na všetky koncové systémy iSeries. Skôr než pomocou Riadiacej centrály presuniete podpísané objekty aplikácií na koncové systémy iSeries, musíte na všetkých koncových systémoch vyplniť všetky úlohy konfigurácie. Skôr než budete môcť počas obnovy podpísaných objektov na koncovom systéme úspešne overovať podpisy, musí byť ukončená konfigurácia overovania podpisov.

Krok 5: Vyexportujte certifikáty na umožnenie kontroly podpisov v ostatných systémoch iSeries.

Ak podpisujete objekty, aby ste zabezpečili bezúhonnosť ich obsahu, musíte pre vás, aj iných zabezpečiť spôsob overenia spoľahlivosti podpisu. Ak chcete overovať podpisy objektov na rovnakom systéme, ktorý ich podpisuje, musíte s použitím DCM vytvoriť sklad certifikátov *SIGNATUREVERIFICATION. Tento sklad certifikátov musí obsahovať kópiu certifikátu na podpisovanie objektov aj kópiu certifikátu CA, ktorá ho vydala.

Ak chcete ostatným umožniť overenie podpisu, musíte im poskytnúť kópiu certifikátu, ktorý ho podpísal. Ak na vydanie certifikátu používate Lokálnu certifikačnú autoritu (CA), musíte im tiež poskytnúť kópiu certifikátu Lokálnej CA.

Ak chcete pomocou DCM overovať podpisy na systéme, ktorý objekty podpísal (v tomto scenári iSeries A), musíte dodržať tieto kroky:
1. V navigačnom rámci vyberte **Vytvoriť nový sklad certifikátov** a označte ***SIGNATUREVERIFICATION** ako sklad certifikátov, ktorý chcete vytvoriť.
2. Kliknutím na **Áno** prekopírujete existujúce certifikáty na podpisovanie objektov do nového skladu certifikátov ako certifikáty na overovanie podpisov.
3. Zadajte heslo pre nový sklad certifikátov a kliknutím na **Pokračovať** ho vytvorte. Odteraz môžete s použitím DCM overovať podpísané objekty na systéme, ktorý používate aj na ich podpisovanie.

Ak chcete pomocou DCM exportovať kópiu certifikátu Lokálnej CA a kópiu certifikátu na podpisovanie objektov ako certifikát na overovanie podpisov, aby ste mohli overovať podpisy objektov na iných systémoch, vykonajte tieto kroky:
1. V navigačnom rámci vyberte **Spravovať certifikáty** a potom označte úlohu **Exportovať certifikát**.
2. Vyberte **Certifikačná autorita (CA)** a kliknutím na **Pokračovať** zobrazte zoznam certifikátov CA, ktoré môžete exportovať.
3. Vyberte zo zoznamu certifikát Lokálnej CA, ktorý ste predtým vytvorili a kliknite na **Export**.
4. Ako cieľ exportu označte **Súbor** a kliknite na **Pokračovať**.
5. Pre exportovaný certifikát Lokálnej CA zadajte úplný názov cesty a súboru a kliknutím na **Pokračovať** certifikát exportujte.
6. Kliknutím na **OK** zatvorte potvrdzovaciu stránku exportu. Teraz môžete exportovať kópiu certifikátu na podpisovanie objektov.
7. Znovu vykonajte úlohu **Exportovať certifikát**.
8. Výberom **Podpisovanie objektov** zobrazte zoznam certifikátov na podpisovanie objektov, ktoré chcete exportovať.
9. Vyberte si zo zoznamu správny certifikát na podpisovanie objektov a kliknite na **Export**.
10. Ako cieľ označte **Uložiť ako certifikát na overovanie podpisov** a kliknite na **Pokračovať**.
11. Zadajte úplný názov cesty a súboru, kam chcete exportovať certifikát na overovanie podpisov a kliknutím na **Pokračovať** ho exportujte.

Teraz môžete tieto súbory presunúť na koncové systémy iSeries, na ktorých chcete overovať podpisy vytvorené týmto certifikátom.

Krok 6: Presuňte súbory certifikátu do koncových systémov iSeries.

Musíte presunúť certifikačné súbory vytvorené na serveri iSeries A na koncové systémy iSeries skôr, než ich budete konfigurovať aby overovali objekty, ktoré ste podpisovali. Na presun certifikačných súborov môžete použiť niekoľko metód. Na presun súborov môžete použiť napríklad protokol FTP (File Transfer Protocol) alebo distribúciu balíkov Centrálnym riadením.

Krok 7: Podpíšte objekty pomocou funkcie Centrálne riadenie.

Proces podpisovania objektov Riadiacej centrály je súčasťou procesu balenia a distribúcie softvéru. Skôr než použijete Riadiacu centrálu na presun podpísaných aplikácií na koncové systémy iSeries, musíte na každom z nich vyplniť všetky úlohy konfigurácie overovania podpisov. Skôr než budete môcť počas obnovy podpísaných objektov na koncovom systéme úspešne overovať podpisy, musí byť ukončená konfigurácia overovania podpisov.

Ak chcete podpisovať aplikácie, ktoré distribuujete na koncové systémy iSeries tak, ako je to popísané v tomto scenári, dodržte tieto kroky:
1. Na balenie a distribúciu softvérových produktov použite Riadiacu centrálu.
2. Keď sa dostanete k panelu **Identifikácia** v **Sprievodcovi definovaním produktu**, kliknutím na **Rozšírený** zobrazte **Rozšírený identifikačný panel**.
3. Do poľa **Elektronické podpisy** zapíšte ID aplikácie na podpisovanie objektov, ktorú ste predtým vytvorili a kliknite na **OK**.

4. Dokončite vypĺňanie formulárov a pokračujte balením a distribúciou softvérových produktov pomocou Riadiacej centrály.

Krok 8: Úlohy kontroly podpisov: Vytvorte pamäť certifikátov *SIGNATUREVERIFICATION v koncových systémoch iSeries.

Aby ste mohli v tomto scenári overovať podpisy na koncových systémoch iSeries, musí byť na každom z nich uložená v sklade certifikátov *SIGNATUREVERIFICATION uložená kópia certifikátu na overovanie podpisov. Ak boli objekty podpísané súkromným certifikátom, musí tento certifikát na overovanie podpisov obsahovať aj kópiu certifikátu Lokálnej CA.

Sklad certifikátov *SIGNATUREVERIFICATION vytvoríte nasledovným postupom:
1. Spustite DCM.
2. V navigačnom rámci Správcu digitálnych certifikátov (DCM) vyberte **Vytvoriť nový sklad certifikátov** a označte ***SIGNATUREVERIFICATION** ako sklad certifikátov, ktorý chcete vytvoriť.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) navrchu stránky a dostanete sa k online pomoci.
3. Zadajte heslo pre nový sklad certifikátov a kliknutím na **Pokračovať** ho vytvorte. Teraz môžete do skladu importovať certifikáty a použiť ich na overovanie podpisov.

Krok 9: Úlohy kontroly podpisov: Naimportujte certifikáty.

Aby ste mohli overiť elektronický podpis, musí sklad *SIGNATUREVERIFICATION obsahovať certifikát na overovanie podpisov. Ak je certifikát, ktorým bol objekt podpísaný, súkromný, musí tento sklad certifikátov obsahovať aj kópiu certifikátu Lokálnej certifikačnej autority (CA), ktorá ho vydala. V tomto scenári boli oba certifikáty exportované do súboru a presunuté na každý koncový systém iSeries.

Ak chcete tieto certifikáty presunúť do skladu certifikátov *SIGNATUREVERIFICATION, postupujte takto:
1. V navigačnom rámci DCM kliknite na **Vybrať sklad certifikátov** a označte ***SIGNATUREVERIFICATION** ako sklad certifikátov, ktorý chcete otvoriť.
2. Keď sa zobrazí stránka Sklad certifikátov a heslo, napíšte heslo, ktoré ste zadali pri vytváraní tohto skladu certifikátov a kliknite na **Pokračovať**.
3. Keď sa obnoví obsah navigačného rámca, označte **Spravovať certifikáty** a zobrazte zoznam úloh.
4. Zo zoznamu úloh vyberte **Import certifikátov**.
5. Ako typ certifikátu vyberte **Certifikačná autorita (CA)** a kliknite na **Pokračovať**.

   Poznámka: Certifikát Lokálnej CA musíte importovať skôr, než súkromný certifikát na overovanie podpisov; inak proces importu certifikátu na overovanie podpisov zlyhá.
6. Zadajte úplný názov cesty a súboru certifikátu CA a kliknite na **Pokračovať**. Zobrazí sa správa, ktorá buď potvrdzuje, že bol proces importu úspešný, alebo poskytuje chybovú informáciu, ak proces zlyhal.
7. Znova vyberte úlohu **Importovať certifikát**.
8. Ako typ importovaného certifikátu označte **Overovanie podpisov** a kliknite na **Pokračovať**.
9. Zadajte úplný názov cesty a súboru certifikátu na overovanie podpisov a kliknite na **Pokračovať**. Zobrazí sa správa, ktorá buď potvrdzuje, že bol proces importu úspešný, alebo poskytuje chybovú informáciu, ak proces zlyhal.

Váš systém iSeries teraz môže počas obnovovania podpísaných objektov overovať ich podpisy vytvorené korešpondujúcim podpisovacím certifikátom.

Pojmy podpisovania objektov

Skôr než začnete využívať možnosti podpisovania objektov a overovania podpisov v systéme iSeries, mohlo by pre vás byť užitočné prezrieť si niektoré z týchto pojmov:

Elektronické podpisy
Zistite, čo sú to elektronické podpisy a akú ochranu poskytujú.

Podpisovateľné objekty
Dozviete sa, ktoré objekty iSeries môžete podpisovať a o možnostiach podpisovania príkazových (*CMD) objektov.

Proces podpísania objektu
Informácie o tom, ako prebieha proces podpisovania objektov a aké parametre pri ňom môžete zadať.

Proces overenia podpisu
Informácie o tom, ako prebieha proces overovania podpisov a aké parametre pri ňom môžete zadať.

| **Kontrola integrity funkcie na kontrolu kódu**
| Dozviete sa tu o kontrole integrity funkcie na kontrolu kódu, ktorú môžete použiť na kontrolu integrity systému
| iSeries.

Elektronické podpisy

Systém OS/400 poskytuje podporu využívania digitálnych certifikátov na elektronické ″podpisovanie″ objektov. Elektronický podpis objektu je vytvorený formou šifrovania a funguje ako osobný podpis na rukou písanom dokumente. Poskytuje dôkaz o pôvode objektu, ako aj spôsoby, ktorými je možné overiť bezúhonnosť objektu. Majiteľ elektronického certifikátu ″podpíše″ objekt použitím súkromného kľúča certifikátu. Príjemca objektu použije na odkódovanie podpisu zodpovedajúci verejný kľúč, ktorý overí neporušenosť podpísaného objektu a potvrdí, že zdrojom objektu je jeho odosielateľ.

Podpisovanie objektov rozširuje tradičné nástroje servera iSeries, ktoré kontrolujú oprávnenia na zmeny objektov. Tieto tradičné kontrolné mechanizmy nemôžu objekt ochrániť pred nepovolenými zásahmi počas jeho prenosu sieťou Internet, alebo inou nedôveryhodnou sieťou. Ak môžete overiť, či bol obsah objektov od ich podpisu zmenený, viete sa jednoduchšie rozhodnúť, či budete takto získanému objektu dôverovať.

Elektronický podpis je zakódovaný matematický súčet údajov v objekte. Samotný objekt a jeho obsah zakódované nie sú; súčet je zakódovaný, aby sa predišlo jeho neautorizovaným zmenám. Ktokoľvek, kto sa chce uistiť, že objekt nebol počas prenosu zmenený a že pochádza z prípustného a oprávneného zdroja, môže na overenie jeho podpisu použiť verejný kľúč certifikátu. Ak sa súčet v podpise nezhoduje s aktuálnym súčtom údajov v objekte, mohli byť tieto údaje zmenené. V takom prípade môže príjemca namiesto použitia objektu kontaktovať toho, kto objekt podpisoval a vyžiadať si jeho novú kópiu.

Podpis objektu reprezentuje systém, ktorý objekt podpisoval, nie konkrétneho užívateľa systému (hoci užívateľ musí mať na použitie podpisujúceho certifikátu primerané oprávnenia).

Ak zistíte, že použitie digitálnych podpisov spĺňa vaše bezpečnostné potreby a politiky, musíte sa rozhodnúť, či chcete používať verejné certifikáty alebo vydávať lokálne certifikáty. Ak plánujete distribuovať objekty na verejnosť, mali by ste zvážiť používanie certifikátov od známej verejnej certifikačnej autority (CA) na podpisovanie objektov. Použitie verejného certifikátu vám zabezpečí, že ostatní budú môcť jednoducho a cenovo nenáročne overovať podpisy na vami distribuovaných objektoch. Ak ale plánujete distribuovať objekty výhradne v rámci vlastnej organizácie, môžete uprednostniť Správcu digitálnych certifikátov (DCM), ktorým budete spravovať vlastnú Lokálnu CA a zakladať certifikáty na podpisovanie objektov. Použitie súkromných certifikátov vydaných Lokálnou CA je lacnejšie, než zakupovanie certifikátov od známej verejnej CA.

Typy digitálnych podpisov

Počnúc V5R2 môžete podpisovať príkazové (*CMD) objekty; môžete si tiež vybrať jeden z dvoch typov podpísania objektov *CMD: podpísanie jadra objektu, alebo podpísanie celého objektu.

- **Podpísanie celého objektu**
  Tento typ podpisu zahŕňa všetko okrem niekoľkých nepodstatných bajtov objektu.

- **Podpísanie jadra objektu**
  Tento typ podpisu zahŕňa podstatné bajty objektu *CMD. Avšak, podpis nezahŕňa bajty, ktoré sú predmetom častým zmien. To umožňuje, aby boli v príkaze vykonané určité zmeny, bez toho, aby sa stal podpis neplatným. Výber nezahrnutých bajtov závisí od špecifického objektu *CMD; tieto podpisy napríklad nezahŕňajú predvolené hodnoty parametrov objektov *CMD. Medzi príklady zmien, ktoré nezrušia platnosť takéhoto podpisu, patria:
  – Zmena štandardných hodnôt príkazu.
  – Pridanie programu na kontrolu platnosti k príkazu, ktorý ho zatiaľ nemá.
  – Zmena parametra Kde môže byť spustený.
  – Zmena parametra Povoliť limitovaných užívateľov.

Viac informácií o objektoch iSeries, ktoré môžete podpísať a nezahrnutých bajtoch objektu *CMD do podpisu jadra objektu, si môžete pozrieť v časti Podpisovateľné objekty.

Podpisovateľné objekty

Nezávisle na tom, akú metódu podpisovania si vyberiete, môžete elektronicky podpisovať mnoho typov objektov OS/400. Môžete podpisovať všetky objekty typu (*STMF), ktoré ukladáte do integrovaného súborového systému, okrem objektov, ktoré sú uložené v knižnici. Ak je k objektu pripojený aj program v jazyku Java, bude aj tento program podpísaný. V súborovom systéme QSYS.LIB môžete podpisovať len tieto objekty: programy (*PGM), obslužné programy (*SRVPGM), moduly (*MODULE), balíky SQL (*SQLPKG), *FILE (len úložný súbor) a príkazy (*CMD).

Objekt, ktorý chcete podpísať, musí byť umiestnený v lokálnom systéme. Napríklad, ak používate server Windows 2000 v integrovanom serveri xSeries Server for iSeries, máte v integrovanom súborovom systéme dostupný súborový systém QNTC. Adresáre v tomto súborovom systéme sa nepovažujú za lokálne, pretože obsahujú súbory, ktoré vlastní operačný systém Windows 2000. Takisto nemôžete podpísať prázdne objekty ani objekty skompilované pre vydanie staršie ako V5R1.

Popisy príkazových (*CMD) objektov

Pri podpisovaní objektov *CMD môžete zvoliť jeden z dvoch typov digitálnych podpisov, ktorý sa má aplikovať na objekt *CMD. Môžete si zvoliť buď podpísanie celého objektu, alebo len podpísanie jadra objektu. Ak sa rozhodnete pre podpis celého objektu, vzťahuje sa elektronický podpis na celý jeho obsah, okrem niekoľkých nepodstatných bajtov. V podpise celého objektu sú zahrnuté položky z podpisu jadra objektu.

Ak sa rozhodnete podpisovať len jadro objektu, sú podstatné údaje chránené podpisom, zatiaľ čo údaje, podliehajúce častejším zmenám, podpísané nie sú. To, ktoré údaje ostávajú nepodpísané, záleží na samotnom objekte *CMD, ale okrem iných to môžu byť bajty rozhodujúce o režime, v ktorom je objekt platný, alebo určujúce kde môže byť objekt spustený. Podpisy jadier objektov napríklad nezahŕňajú predvolené hodnoty parametrov objektov *CMD. Tento typ podpisu umožňuje vykonať na príkaze niektoré zmeny bez toho, aby sa podpis poškodil. Medzi príklady zmien, ktoré nepoškodia platnosť takýchto podpisov, patria:
- Zmena štandardných hodnôt príkazu.
- Pridanie programu na kontrolu platnosti k príkazu, ktorý ho zatiaľ nemá.
- Zmena parametra Kde môže byť spustený.
- Zmena parametra Povoliť limitovaných užívateľov.

Nasledujúca tabuľka popisuje, ktoré bajty objektu *CMD spadajú pod podpísanie jadra objektu.

Zloženie podpisu jadra objektu pre objekty *CMD

Časť objektu	Vzťah k podpisu jadra objektu
Štandardy príkazu zmenené CHGCMDDFT	Nie je súčasťou podpisu jadra objektu
Program na spustenie príkazu a knižnice	Je vždy zahrnutý ako časť podpisu jadra objektu
Zdrojový súbor a knižnica REXX	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu

Časť objektu	Vzťah k podpisu jadra objektu
Zdrojový člen REXX	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Príkazové prostredie a knižnica REXX	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Názov ukončovacieho programu, knižnica a kód ukončenia REXX	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Program a knižnica overovania platnosti	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Režim, v ktorom je platný	Nie je súčasťou podpisu jadra objektu
Kde môže byť spustený	Nie je súčasťou podpisu jadra objektu
Povoliť limitovaných užívateľov	Nie je súčasťou podpisu jadra objektu
Pomocná polička na knihy	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Skupina a knižnica panelu s pomocou	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Identifikátor pomoci	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Vyhľadávací index a knižnica pomoci	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Aktuálna knižnica	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Produktová knižnica	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Potvrdiť nahradenie programu a knižnice	Je súčasťou, ak je to zadané pri podpisovaní objektu, inak nie je súčasťou podpisu jadra objektu
Text (opis)	Nie je súčasťou podpisu jadra objektu, ani podpisu celého objektu, pretože nie je uložený v objekte
Povoliť grafické užívateľské rozhranie (GUI)	Nie je súčasťou podpisu jadra objektu

Spracovanie podpisovania objektu

Pri podpisovaní objektov môžete pre proces podpisovania zadať nasledujúce možnosti:

- **Spracovanie chyby**
  Pri vytváraní podpisov pre viac ako jeden objekt môžete zadať typ spracovania chyby, ktorý má aplikácia použiť. Podľa vášho zadania aplikácia pri objavení chyby buď zastaví proces podpisovania, alebo v ňom pokračuje podpísaním nasledujúceho objektu v poradí.
- **Zdvojené podpisy objektov**
  Môžete zadať, ako bude aplikácia obsluhovať proces podpisovania pri opakovanom podpísaní objektu. Rozhodujete, či má objektu ponechať originálny podpis, alebo ho má nahradiť novým.
- **Objekty v podadresároch**
  Môžete zadať, ako bude aplikácia obsluhovať podpisovanie objektov v podadresároch. Podľa vášho rozhodnutia aplikácia osobitne podpíše objekty v akomkoľvek podadresári, alebo, ignorujúc všetky podadresáre, podpíše len objekty v hlavnom adresári.
- **Rámec podpisu objektu**
  Pri podpisovaní objektov *CMD určujete, či má aplikácia podpísať celý objekt, alebo len jeho jadro.

Spracovanie overovania podpisu

Pri overovaní objektov môžete pre proces podpisovania zadať nasledujúce možnosti:

- **Spracovanie chyby**
  Môžete zadať, aký typ spracovania chyby bude aplikácia používať pri kontrole podpisov na viac ako jednom objekte. Podľa vášho zadania aplikácia pri objavení chyby buď zastaví proces overovania, alebo v ňom pokračuje overením nasledujúceho objektu v poradí.
- **Objekty v podadresároch**
  Môžete zadať, ako bude aplikácia obsluhovať kontrolu podpisov na objektoch v podadresároch. Podľa vášho rozhodnutia aplikácia osobitne overí objekty v akomkoľvek podadresári, alebo, ignorujúc všetky podadresáre, overí len objekty v hlavnom adresári.
- **Overovanie podpísaného jadra vs. celého objektu**
  O spôsobe obsluhy podpisov jadra objektu a podpisov celého objektu počas procesu kontroly rozhodujú systémové pravidlá. Tieto pravidlá sú nasledovné:
  - Ak sa na objekte nenachádza žiaden podpis, overovací proces nahlási, že objekt nie je podpísaný a pokračuje v overovaní ďalším objektom.
  - Ak bol objekt podpísaný zdrojom, ktorý je systémom označený ako dôveryhodný (IBM), musí sa súčet v podpise zhodovať so súčtom objektu, inak proces overovania zlyhá. Ak sa súčty zhodujú, proces overovania pokračuje. Podpis je zašifrovaný matematický súčet údajov v objekte; preto považujeme podpis za platný, ak súčet údajov v objekte v momente overovania súhlasí so súčtom tých istých údajov v momente podpisovania.
  - Ak má objekt akékoľvek podpisy celého objektu, ktoré sú dôveryhodné (teda ich certifikát je umiestnený v certifikačnom sklade *SIGNATUREVERIFICATION), musí byť aspoň jeden z týchto podpisov platný, inak proces overovania zlyhá. Ak je platný aspoň jeden podpis celého objektu, overovací proces pokračuje.
  - Ak má objekt akékoľvek podpisy jadra objektu, ktoré sú dôveryhodné, musí byť aspoň jeden z nich platný voči certifikátu v sklade certifikátov *SIGNATUREVERIFICATION, inak proces overovania zlyhá. Ak je platný aspoň jeden podpis jadra objektu, proces overovania pokračuje.

Funkcia kontroly integrity funkcie na kontrolu kódu

Od verzie V5R2 je systém OS/400 dodávaný s funkciou na kontrolu kódu, ktorú môžete použiť na kontrolu integrity podpísaných objektov vo vašom systéme vrátane celého kódu operačného systému, ktorý dodáva a podpisuje spoločnosť IBM pre váš systém iSeries. Od verzie V5R3 môžete na kontrolu integrity funkcie na kontrolu kódu a kľúčových objektov operačného systému použiť nové aplikačné programové rozhranie (API).

Kontrolu integrity systému OS/400 poskytuje rozhranie API Check System (QydoCheckSystem). Toto rozhranie môžete použiť na kontrolu programov (*.PGM), služobných programov (*SRVPGM) a vybratých príkazových objektov (*CMD) v knižnici QSYS. Okrem toho testuje rozhranie API Check System príkaz RSTOBJ (Restore object), príkaz RSTLIB (Restore Library), príkaz CHKOBJITG (Check Object Integrity) a rozhranie API Verify Object. Tento test kontrolujte, či tieto príkazy a rozhranie API Verify Object hlásia v prípade potreby chyby validácie podpisu; napríklad ak nie je objekt dodaný so systémom podpísaný, alebo ak obsahuje neplatný podpis.

Rozhranie API Check System hlási chybové správy pre zlyhania kontroly a iné chyby alebo zlyhania kontroly do protokolu úlohy. Avšak, v závislosti od nastavenia nasledujúcich volieb, môžete zadať aj jednu z dvoch ďalších metód hlásenia chýb:

- Ak je systémová hodnota QAUDLVL nastavená na *AUDFAIL, rozhranie API Check System API generuje auditovacie záznamy za účelom hlásenia všetkých zlyhaní a chýb, ktoré nájdu príkazy RSTOBJ (Restore Object), RSTLIB (Restore Library) a CHKOBJITG (Check Object Integrity).
- Ak užívateľ zadá, aby rozhranie API Check System používalo súbor výsledkov v integrovanom súborovom systéme, rozhranie API ho najprv vytvorí, ak neexistuje, a bude do neho pridávať hlásenia o všetkých chybách alebo zlyhaniach, ktoré zistí.

Ak sa chcete dozvedieť viac o používaní rozhrania API Check System API na kontrolu integrity vášho systému, pozrite si časť Kontrola integrity funkcie na kontrolu kódu.

Požiadavky na podpisovanie objektov a overovanie podpisov

Možnosti podpisovania objektov a overovania podpisov v OS/400 vám poskytujú ďalší významný spôsob kontroly objektov na vašom serveri iSeries. Aby ste ale mohli tieto možnosti využívať, musíte splniť niektoré nevyhnutné požiadavky.

Požiadavky na podpisovanie objektov

Je množstvo spôsobov, ktoré môžete pri podpisovaní objektov využiť: v závislosti na vašich obchodných a bezpečnostných potrebách:
- Môžete použiť program Správca digitálnych certifikátov (DCM).
- Môžete napísať program používajúci rozhranie API Sign Object.
- Môžete použiť funkciu Riadiacej centrály produktu iSeries Navigator, ktorou podpíšete objekty počas balenia pre distribúciu na koncové systémy iSeries.

To, ktorú z metód si vyberiete, záleží na vašich obchodných a bezpečnostných potrebách. Nezávisle na tom, ktorú metódu plánujete na podpisovanie objektov využiť, musíte zabezpečiť, aby boli splnené určité nevyhnutné podmienky:
- Musíte zabezpečiť splnenie požiadaviek na inštaláciu a používanie Správcu digitálnych certifikátov (DCM).
  - Musíte použiť DCM na vytvorenie skladu certifikátov *OBJECTSIGNING. Tento sklad vytvoríte buď počas vytvárania Lokálnej Certifikačnej autority (CA), alebo počas spravovania certifikátov od verejnej internetovej CA.
  - Sklad certifikátov *OBJECTSIGNING musí obsahovať aspoň jeden certifikát, či už ten vytvorený vašou Lokálnou CA alebo ten, ktorý ste získali od verejnej internetovej CA.
  - Musíte pomocou DCM vytvoriť aspoň jednu definíciu aplikácie na podpisovanie objektov.
  - Musíte pomocou DCM prideliť konkrétny certifikát tejto definícii aplikácie na podpisovanie objektov.
- Užívateľský profil iSeries, ktorý podpisuje objekty, musia mať špeciálne oprávnenie *ALLOBJ. Užívateľský profil iSeries, ktorý vytvára sklad certifikátov *SIGNATUREVERIFICATION, musí mať špeciálne oprávnenia *SECADM a *ALLOBJ.

Požiadavky na kontrolu podpisu

Je množstvo spôsobov, ktoré môžete pri overovaní podpisov využiť:
- Môžete použiť program Správca digitálnych certifikátov (DCM).
- Môžete napísať program, ktorý použije API overujúce podpisy (QYDOVFYO).
- Môžete použiť množstvo príkazov, ako napríklad príkaz Check Object Integrity (CHKOBJITG).

To, ktorú z metód si na overovanie podpisov vyberiete, záleží na vašich obchodných a bezpečnostných potrebách. Nezávisle na tom, ktorú metódu plánujete použiť, musíte zabezpečiť, aby boli splnené určité nevyhnutné podmienky:
- Musíte zabezpečiť splnenie požiadaviek na inštaláciu a používanie Správcu digitálnych certifikátov (DCM).
- Musíte vytvoriť sklad certifikátov *SIGNATUREVERIFICATION. Tento sklad certifikátov môžete, v závislosti na vašich potrebách, vytvoriť jedným z dvoch spôsobov. Môžete ho vytvoriť použitím Správcu digitálnych certifikátov (DCM), aby ste mohli spravovať svoje certifikáty na overovanie podpisov. Alebo, ak na podpisovanie objektov používate verejný certifikát, môžete tento sklad certifikátov vytvoriť napísaním programu, ktorý používa API vkladajúce overovač (QYDOADDV).

  Poznámka: API vkladajúce overovač vytvorí tento sklad certifikátov s predvoleným heslom. Na resetovanie tohto hesla vašim vlastným potrebujete použiť DCM, aby ste sa vyhli neautorizovému prístupu do skladu certifikátov.
- Certifikačný sklad *SIGNATUREVERIFICATION musí obsahovať kópiu certifikátu, ktorý objekty podpísal. Túto kópiu môžete do skladu certifikátov pridať dvoma spôsobmi. Môžete na podpisujúcom systéme použiť DCM, exportovať certifikát do súboru a potom tento súbor pomocou DCM cieľového overovacieho systému importovať ako certifikát do skladu certifikátov *SIGNATUREVERIFICATION. Alebo, ak na podpisovanie objektov používate verejný certifikát, môžete ho pridať do skladu certifikátov cieľového overovacieho systému napísaním programu, ktorý používa API vkladajúce overovač.
- Sklad certifikátov *SIGNATUREVERIFICATION musí obsahovať kópiu certifikátu CA použitej na vydanie certifikátu, ktorým bol objekt podpísaný. Ak na podpisovanie objektov používate verejný certifikát, môže už pamäť

certifikátov v cieľovom kontrolnom systéme obsahovať kópiu vyžadovaného certifikátu certifikačnej autority. Ak na podpisovanie objektov používate certifikát vydaný Lokálnou CA, musíte na pridanie kópie certifikátu Lokálnej CA do skladu certifikátov cieľového overovacieho systému použiť DCM tohto systému.

Poznámka: Z bezpečnostných dôvodov vám API vkladajúce overovač neumožní vložiť do skladu certifikátov *SIGNATUREVERIFICATION certifikát Certifikačnej autority (CA). Ak by ste to urobili, systém by automaticky považoval CA za dôveryhodný zdroj certifikátov. Následne systém predpokladá, že certifikát vydaný touto CA pochádza z dôveryhodného zdroja. Preto nemôžete toto API použiť na vytvorenie programu na ukončenie inštalácie, ktorý vloží CA certifikát do skladu certifikátov. Aby sa zabezpečilo, že niekto bude musieť špecificky a manuálne skontrolovať, ktorým CA môže systém dôverovať, musíte na pridanie CA certifikátu použiť Správcu digitálnych certifikátov (Digital Certificate Manager). Toto môže zabrániť možnosti importovať certifikáty zo zdrojov, ktoré administrátor nevedome označil ako dôveryhodné.

Ak na podpisovanie objektov používate certifikát vydaný Lokálnou CA, musíte na exportovanie kópie certifikátu Lokálnej CA použiť DCM na hostiteľskom serveri iSeries Lokálnej CA. Potom môžete pomocou DCM na cieľový overovací server iSeries importovať certifikát lokálnej CA do skladu certifikátov *SIGNATUREVERIFICATION. Ak chcete zabrániť možnej chybe, musíte pred použitím rozhrania API Add Verifier na pridanie certifikátu na kontrolu podpisu naimportovať do tejto pamäte certifikátov certifikát lokálnej certifikačnej autority. Preto by bolo v prípade, keď používate certifikát vydaný Lokálnou CA, jednoduchšie importovať do skladu certifikátov oba certifikáty (Lokálnej CA aj overovací certifikát) pomocou DCM .

Ak chcete zabrániť použitiu tohto rozhrania API na pridanie certifikátu na kontrolu do vašej pamäte certifikátov *SIGNATUREVERIFICATION bez vášho vedomia, mali by ste zvážiť zakázanie tohto rozhrania API vo vašom systéme. To môžete spraviť, ak použijete nástroje na údržbu systému (system service tools - SST) a zakážete zmeny hodnôt súvisiacich s bezpečnosťou systému..

- Užívateľský profil iSeries, ktorý overuje objekty, musí mať špeciálne oprávnenie *AUDIT. Užívateľský profil iSeries, ktorý vytvára sklad certifikátov *SIGNATUREVERIFICATION, alebo mení jeho heslo, musí mať špeciálne oprávnenie *SECADM a *ALLOBJ.

Spravovanie podpísaných objektov

Počnúc V5R1 začala firma IBM podpisovať licencované programy a súbory PTF v produkte OS/400, aby bola oficiálne firma IBM označená ako pôvodca tohto operačného systému a ako spôsob zisťovania, či sa v systéme objavili neautorizované zmeny. Rovnako môžu aplikácie, ktoré kupujte, podpisovať obchodní partneri a iní dodávatelia. Preto aj keď sami objekty nepodpisujete, potrebujete pochopiť, ako s podpísanými objektmi pracovať a ako ovplyvňujú rutinné administračné úlohy.

Podpísané objekty ovplyvňujú najmä úlohy zálohovania a obnovy, najmä to, ako objekty vo vašom systéme ukladáte a obnovujete.

Systémové hodnoty a príkazy, ktoré ovplyvňujú podpísané objekty
Zistite viac o systémových hodnotách a príkazoch, ktoré môžete využiť pri spravovaní podpísaných objektov, alebo ktoré majú pri svojom spustení na takéto objekty vplyv.

Vzťahy medzi podpísanými objektmi a procesmi ukladania a obnovy
Dozviete sa, ako úlohy ukladania a obnovy vo vašom systéme ovplyvňujú podpísané objekty.

Príkazy na kontrolu kódu používané na overenie integrity podpisu
Dozviete sa tu o používaní príkazov na kontrolu podpisov na objektoch za účelom zistenia integrity objektov.

| **Kontrola integrity funkcie na kontrolu kódu**
| Dozviete sa tu o spôsobe kontroly integrity funkcie na kontrolu kódu, ktorú používate na kontrolu integrity
| systému OS/400.

Systémové hodnoty a príkazy, ktoré ovplyvňujú podpísané objekty

Aby ste mohli efektívne spravovať podpísané objekty, potrebujete pochopiť, ako ich systémové hodnoty a príkazy ovplyvňujú. Systémová hodnota **Verify object signatures during restore** (QVFYOBJRST) určuje ako konkrétne obnovovacie príkazy ovplyvňujú podpísané objekty a ako s týmito objektmi systém zaobchádza počas operácií obnovovania. V systéme iSeries nie sú žiadne príkazy CL určené vyslovene len na prácu s podpísanými objektmi. Je tu však množstvo bežných príkazov CL, ktoré používate na spravovanie podpísaných objektov (alebo infraštruktúrnych objektov, ktoré podpisovanie objektov umožňujú). Ďalšie príkazy môžu podpísané objekty vo vašom systéme nepriaznivo ovplyvniť odstránením ich podpisov a teda zrušením ochrany, ktorú podpisy poskytujú.

Systémové hodnoty, ktoré ovplyvňujú podpísané objekty

Systémová hodnota **Verify object signatures during restore** (QVFYOBJRST), člen kategórie obnovy systémových hodnôt OS/400, určuje ako príkazy ovplyvňujú podpísané objekty vo vašom systéme. Táto systémová hodnota prístupná cez produkt iSeries Navigator, ovláda to, ako systém spracováva overovanie podpisov počas operácií obnovy. Nastavenia tejto systémovej hodnoty, spolu s nastavením ďalších dvoch systémových hodnôt, ovplyvňuje operácie obnovy vo vašom systéme. Vzhľadom na nastavenie, ktoré pre túto hodnotu vyberiete, môže povoliť, alebo znemožniť obnovovanie objektov v závislosti na stave ich podpisu. (Napríklad podľa toho, či je objekt nepodpísaný, má neplatný podpis, je podpísaný dôveryhodným zdrojom, a tak ďalej.) Predvolené nastavenie tejto hodnoty povoľuje obnovu nepodpísaných objektov, ale zabezpečuje, že môžu byť podpísané objekty obnovené len ak majú objekty platný podpis. Systém definuje objekt ako podpísaný, len ak má objekt podpis, ktorý systém považuje za dôveryhodný; ostatné ″nedôveryhodné″ podpisy na objektoch systém ignoruje a chová sa k nim, akoby boli nepodpísané.

Je niekoľko rôznych hodnôt, ktoré môžeme pre systémovú hodnotu QVFYOBJRST použiť, od ignorovania všetkých podpisov, po vyžadovanie platných podpisov pre všetky objekty, ktoré systém obnovuje. Táto systémová hodnota ovplyvňuje len spúšťané objekty, ktoré sú obnovované, ako programy (*PGM), príkazy (*CMD), obslužné programy (*SRVPGM), balíky SQL (*SQLPKG) a moduly (*MODULE). Takisto to platí pre objekty prúdových súborov (*STMF), ktoré majú priradené programy Java, vytvorené pomocou príkazu CRTJVAPGM (Create Java Program). Neplatí to pre úložné súbory (*SAV) ani pre súbory integrovaného súborového systému.

Viac sa o používaní tejto aj iných systémových hodnôt dozviete v System Value Finder v informačnom centre.

Príkazy CL, ktoré ovplyvňujú podpísané objekty

Je niekoľko CL príkazov, ktoré vám umožňujú pracovať s podpísanými objektmi, alebo ktoré ovplyvňujú podpísané objekty na vašom serveri iSeries. Môžete použiť množstvo príkazov na prezeranie informácií o podpise objektu, overenie jeho podpisu a na ukladanie a obnovovanie bezpečnostných objektov potrebných na overenie podpisu. Navyše je tu aj skupina príkazov, ktoré pri svojom spustení, môžu z objektu odstrániť podpis a tým zrušiť ochranu, ktorú podpisy poskytujú.

Príkazy na prezeranie informácií o podpisoch objektov

- Príkaz Display Object Description (DSPOBJD).
  Tento príkaz zobrazuje názvy a atribúty určených objektov v určenej knižnici, alebo v knižniciach zoznamu knižníc vlákna. Pomocou tohto príkazu môžete určiť, či je objekt podpísaný a prezrieť si informácie o jeho podpise.
- Príkazy integrovaného súborového systému Display Object Links (DSPLNK) a Work with Object Links (WRKLNK).
  Môžete použiť ktorýkoľvek z týchto príkazov v integrovanom súborovom systéme na zobrazenie informácií o podpise objektu.

Príkazy na overovanie podpisov objektov

- Príkaz Check Object Integrity (CHKOBJITG).
  Tento príkaz vám umožňuje určiť vo vašom systéme, či došlo k poškodeniu integrity objektu. Tento príkaz môžete použiť na overenie podpisu rovnakým spôsobom, ako používate antivírusový program, aby ste zistili, či vírus nepoškodil súbory, alebo iné objekty vo vašom systéme. Viac sa o použití tohto príkazu na podpísané a podpísateľné objekty dozviete v časti Príkazy na kontrolu kódu používané na overenie integrity podpisu.

- Príkaz Check Product Option (CHKPRDOPT).
  Tento príkaz upozorňuje na rozdiel medzi správnou štruktúrou a aktuálnou štruktúrou softvérového produktu. Tento príkaz napríklad nahlási chybu, ak je objekt vymazaný z nainštalovaného produktu. Na zadanie, ako má príkaz obslúžiť a hlásiť možné problémy s podpisom produktu, môžete použiť parameter CHKSIG. Viac sa o použití tohto príkazu na podpísané a podpísateľné objekty dozviete v časti Príkazy na kontrolu kódu používané na overenie integrity podpisu.
- Príkaz Save Licensed Program (SAVLICPGM).
  Tento príkaz ukladá kópiu objektu, ktorý tvorí licencovaný program. Ukladá licencovaný program vo forme, z ktorej môže byť obnovený príkazom Restore Licensed Program (RSTLICPGM). Na zadanie, ako má príkaz obslúžiť a hlásiť možné problémy s podpisom produktu, môžete použiť parameter CHKSIG. Viac sa o použití tohto príkazu na podpísané a podpísateľné objekty dozviete v časti Príkazy na kontrolu kódu používané na overenie integrity podpisu.
- Príkaz Restore (RST).
  Tento príkaz obnoví kópiu jedného alebo viacerých objektov, ktorá sa dá použiť v integrovanom súborovom systéme. Tento príkaz vám tiež umožní vo vašom systéme obnoviť certifikačné sklady a ich obsah. Nemôžete ho však použiť na obnovu certifikačného skladu *SIGNATUREVERIFICATION. To, ako sa tento príkaz vyrovná s obnovou podpísaných a nepodpísaných objektov, určuje systémová hodnota Verify object signatures during restore (QVFYOBJRST).
- Príkaz Restore Library (RSTLIB).
  Tento príkaz obnoví knižnicu, alebo skupinu knižníc, ktoré boli uložené príkazom Save Library (SAVLIB). Príkaz RSTLIB obnoví celú knižnicu, ktorá obsahuje opis knižnice, opisy objektov a obsah objektov v knižnici. To, ako tento príkaz spracuje podpísané a nepodpísané objekty, určuje systémová hodnota Verify object signatures during restore (QVFYOBJRST).
- Príkaz Restore Licensed Program (RSTLICPGM).
  Tento príkaz načíta a obnoví licencovaný program, či už pre počiatočnú inštaláciu, alebo pre inštaláciu nového vydania. To, ako tento príkaz spracuje podpísané a nepodpísané objekty, určuje systémová hodnota Verify object signatures during restore (QVFYOBJRST).
- Príkaz Restore object (RSTOBJ).
  Tento príkaz obnoví jeden, alebo viac objektov jednej knižnice, ktoré boli uložené na diskete, kazete, optickej jednotke, alebo v úložnom súbore len jedným zadaním príkazu. To, ako tento príkaz spracuje podpísané a nepodpísané objekty, určuje systémová hodnota Verify object signatures during restore (QVFYOBJRST).

Príkazy na ukladanie a obnovu skladu certifikátov

- Príkaz Save (SAV).
  Tento príkaz vám umožňuje uložiť kópiu jedného, alebo viacerých objektov, ktoré môžu byť použité v integrovanom súborovom systéme, vrátane skladov certifikátov. Tento príkaz ale nemôžete použiť na uloženie skladu certifikátov *SIGNATUREVERIFICATION.
- Príkaz Save Security Data (SAVSECDTA).
  Tento príkaz vám umožňuje uložiť všetky bezpečnostné informácie bez toho, aby musel systém prejsť do stavu obmedzenia. Môžete ním uložiť sklad certifikátov *SIGNATUREVERIFICATION a certifikáty, ktoré obsahuje. Nemôžete ním ale uložiť žiaden iný sklad certifikátov.
- Príkaz Save System (SAVSYS).
  Tento príkaz vám umožňuje uložiť kópiu licencovaného interného kódu a knižnicu QSYS vo formáte kompatibilnom s inštaláciou servera iSeries. Objekty inej knižnice neuloží. Tiež ním môžete uložiť bezpečnostné a konfiguračné objekty, ktoré je možné uložiť aj príkazmi SAVSECDTA a SAVCFG. Môžete ním uložiť sklad certifikátov *SIGNATUREVERIFICATION a certifikáty, ktoré obsahuje.
- Príkaz Restore (RST).
  Tento príkaz vám umožní obnoviť v systéme sklady certifikátov a ich obsah. Nemôžete ho však použiť na obnovu certifikačného skladu *SIGNATUREVERIFICATION.
- Príkaz Restore User Profiles (RSTUSRPRF).
  Tento príkaz vám umožní obnoviť základné časti užívateľského profilu, alebo skupinu užívateľských profilov uložených príkazmi Save System (SAVSYS), alebo Save Security Data (SAVSECDTA). Môžete ho použiť na obnovu skladu certifikátov *SIGNATUREVERIFICATION a uložených hesiel pre tento a všetky ostatné sklady certifikátov. Ak bude mať parameter SECDTA hodnotu *DCM a parameter USRPRF hodnotu *NONE môžete sklad

certifikátov *SIGNATUREVERIFICATION obnoviť bez obnovovania informácií o užívateľských profiloch. Ak chcete tento príkaz použiť na obnovu informácií o užívateľských profiloch a skladov certifikátov a ich hesiel, zadajte *ALL ako hodnotu parametra USRPRF.

Príkazy, ktoré odstraňujú, alebo rušia podpisy objektov

Keď na podpísaný objekt použijete nasledujúce príkazy, môžete to urobiť spôsobom, ktorý môže odstrániť alebo stratiť podpis z objektu. Odstránenie podpisu môže spôsobiť problémy s daným objektom. Minimálne už nebudete môcť overiť dôveryhodnosť zdroja, z ktorého objekt pochádza, ani nebudete môcť overiť podpis, aby ste zistili, či na objekte neboli vykonané zmeny. Používajte tieto príkazy len na objekty, ktoré ste vytvorili (a nie na objekty, ktoré získate od iných subjektov ako napríklad spoločnosti IBM alebo od predajcov). Ak sa obávate, že príkaz odstránil podpis z objektu, môžete použiť príkaz Display Object Description (DSPOBJD), či tam podpis stále je a v prípade potreby ho podpísať nanovo.

Poznámka: Ak si chcete overiť, či príkaz Save zrušil podpis objektu, musíte objekt obnoviť do inej knižnice, než je tá, na ktorú ste použili príkaz Save (napríklad QTEMP). Potom môžete použiť príkaz DSPOBJD a zistiť, či uložený objekt stratil svoj podpis.

- Príkaz Change Program (CHGPGM).
  Tento príkaz zmení atribúty programu bez toho, aby ho bolo nutné rekompilovať. Taktiež môžete tento príkaz použiť na nútené znovuvytvorenie programu, aj keď zadané atribúty sú rovnaké ako aktuálne atribúty.
- Príkaz Change Service Program (CHGSRVPGM).
  Tento príkaz zmení atribúty obslužného programu bez toho, aby ho bolo nutné rekompilovať. Taktiež môžete tento príkaz použiť na nútené znovuvytvorenie obslužného programu, aj keď zadané atribúty sú rovnaké ako aktuálne atribúty.
- Príkaz Clear Save File (CLRSAVF).
  Tento príkaz vyčistí obsah save file; vyčistí všetky existujúce záznamy zo save file a zredukuje množstvo priestoru, ktorý súbor zaberá.
- Príkaz Save (SAV).
  Tento príkaz uloží kópiu jedného, alebo viacerých objektov, ktoré môžu byť použité v integrovanom súborovom systéme. — Pri použití tohto príkazu môžete stratiť informácie o podpise z príkazového objektu (*CMD) na úložnom médiu, ak pre parameter TGTRLS zadáte staršiu hodnotu ako V5R2M0. Dôjde k strate podpisu, pretože príkazové objekty sa nedajú podpísať vo vydaniach starších ako V5R2.
- Príkaz Save Library (SAVLIB).
  Tento príkaz vám umožňuje uložiť kópiu jednej, alebo viacerých knižníc. Pri použití tohto príkazu môžete stratiť informácie o podpise z príkazového objektu (*CMD) na úložnom médiu, ak pre parameter TGTRLS zadáte staršiu hodnotu ako V5R2M0. Dôjde k strate podpisu, pretože vo verzii staršej ako V5R2 sa nedajú podpísať príkazové objekty.
- Príkaz Save Object (SAVOBJ).
  Tento príkaz ukladá kópiu jedného objektu, alebo skupiny objektov umiestnených v tej istej knižnici. Pri použití tohto príkazu môžete stratiť informácie o podpise z príkazového objektu (*CMD) na úložnom médiu, ak pre parameter TGTRLS zadáte staršiu hodnotu ako V5R2M0. K strate podpisu dôjde preto, že vo verzii staršej, než V5R2, nemôžu byť podpisované príkazové objekty.

Vzťahy medzi podpísanými objektmi a procesmi ukladania a obnovy

Je niekoľko systémových hodnôt, ktoré môžu ovplyvniť operácie obnovy na vašom serveri iSeries. Len jedna z týchto systémových hodnôt, systémová hodnota **kontrolovať podpisy objektu počas obnovy (QVFYOBJRST)**, určuje spôsob obsluhy podpísaných objektov systémom pri ich obnove. Nastavenia, ktoré si vyberiete pre túto systémovú hodnotu, určujú, ako proces obnovy spracováva overovanie nepodpísaných objektov, alebo objektov s neplatným podpisom.

Niektoré príkazy na ukladanie a obnovu ovplyvňujú podpísané objekty, alebo určujú, ako váš systém počas operácií ukladania a obnovy spracováva podpísané a nepodpísané objekty. Musíte vedieť o týchto príkazoch a ich vplyve na podpísané objekty, aby ste mohli lepšie manažovať váš systém a vyhýbať sa potenciálnym problémom, ktoré sa môžu vyskytnúť.

Tieto príkazy môžu počas operácií ukladania a obnovy overovať podpisy na objektoch:
- Príkaz Save Licensed Program (SAVLICPGM).
- Príkaz Restore (RST).
- Príkaz Restore Library (RSTLIB).
- Príkaz Restore Licensed Program (RSTLICPGM).
- Príkaz Restore object (RSTOBJ).

Tieto príkazy vám umožňujú ukladať a obnovovať sklady certifikátov; sklady certifikátov sú z hľadiska bezpečnosti citlivé objekty obsahujúce certifikáty, ktoré používate na podpisovanie objektov a overovanie podpisov:
- Príkaz Save (SAV).
- Príkaz Save Security Data (SAVSECDTA).
- Príkaz Save System (SAVSYS).
- Príkaz Restore (RST).
- Príkaz Restore User Profiles (RSTUSRPRF).

Niektoré príkazy na ukladanie, v závislosti na hodnotách parametrov, ktoré použijete, môžu stratiť podpis objektu a teda zrušiť ochranu, ktorú podpis objektu poskytuje. Napríklad, *každá* operácia uloženia, ktorá odkazuje na príkazový objekt (*CMD) s cieľovým vydaním starším ako V5R2M0, spôsobí uloženie príkazov bez podpisov. Odstránenie podpisu môže spôsobiť problémy s danými objektmi. Minimálne už nebudete môcť overiť dôveryhodnosť zdroja, z ktorého objekt pochádza, ani nebudete môcť overiť podpis, aby ste zistili, či na objekte neboli vykonané zmeny. Používajte tieto príkazy len na objekty, ktoré ste vytvorili (a nie na objekty, ktoré získate od iných subjektov ako napríklad spoločnosti IBM alebo od predajcov).

Poznámka: Ak si chcete overiť, či príkaz Save zrušil podpis objektu, musíte objekt obnoviť do inej knižnice, než je tá, na ktorú ste použili príkaz Save (napríklad QTEMP). Potom môžete použiť príkaz DSPOBJD a zistiť, či uložený objekt stratil svoj podpis.

Musíte vedieť o týchto možnostiach pre nasledujúce špecifické príkazy uloženia a takisto pre príkazy uloženia vo všeobecnosti:
- Príkaz Save (SAV).
- Príkaz Save Library (SAVLIB).
- Príkaz Save Object (SAVOBJ).

Viac informácií o tom, ako tieto príkazy počas operácií ukladania a obnovy ovplyvňujú podpísané objekty a podpisy objektov, nájdete v časti Systémové hodnoty a príkazy, ktoré ovplyvňujú podpísané objekty.

Príkazy na kontrolu kódu používané na overenie integrity podpisu

Na overovanie podpisov na objektoch môžete použiť Správcu digitálnych certifikátov (DCM), alebo API. Tiež môžete na overovanie podpisov použiť niekoľko príkazov. Tieto príkazy môžete použiť na overenie podpisu rovnakým spôsobom, ako používate antivírusový program, aby ste zistili, či vírus nepoškodil súbory, alebo iné objekty vo vašom systéme. Väčšina podpisov je overovaná, počas ich obnovy, alebo inštalácie na systém, napríklad použitím príkazu RSTLIB.

Ak chcete skontrolovať podpisy na objektoch, ktoré sa už v systéme nachádzajú, môžete si vybrať jeden z troch príkazov. Z týchto je príkaz Check Object Integrity (CHKOBJITG) vytvorený špeciálne na overovanie podpisov objektov. Kontrola podpisov je pre každý z týchto príkazov kontrolovaná parametrom CHKSIG. Tento parameter vám umožňuje kontrolovať všetky typy objektov, ktoré môžu byť podpísané, ignorovať všetky podpisy, alebo kontrolovať všetky podpísané objekty. Posledná z možností je zároveň predvolenou hodnotou tohto parametra.

Príkaz CHKOBJITG (Check Object Integrity)

Príkaz Check Object Integrity (CHKOBJITG) vám umožňuje určiť, či nedošlo k poškodeniu integrity objektov vo vašom systéme. Môžete tento príkaz využiť na kontrolu integrity poškodenia objektov, ktoré vlastnia konkrétni užívatelia, objektov, ktoré sa zhodujú so zadaným názvom cesty, alebo všetkých objektov systému. Záznam o porušení integrity sa objaví, keď je splnená jedna z týchto podmienok:

- Bol zmenený objekt príkazu, programu, modulu, alebo atribúty knižnice.
- Elektronický podpis objektu je určený ako neplatný. Podpis je zašifrovaný matematický súčet údajov v objekte; preto považujeme podpis za platný, ak sa údaje v objekte v momente overovania zhodujú s údajmi v objekte v momente podpisovania. Platnosť podpisu je založená na porovnaní zašifrovaného matematického súčtu, vytvoreného v momente, keď je objekt podpisovaný a zakódovaného matematického súčtu vytvoreného počas overovania podpisu. Proces overenia podpisu porovná tieto dva súčty. Ak ich hodnoty nie sú rovnaké, bol obsah objektu od jeho podpisu zmenený a podpis je považovaný za neplatný.
- Objekt má nesprávny doménový atribút pre typ objektu.
-

Ak príkaz detekuje narušenie integrity objektu, pridá do protokolového súboru databázy názov objektu, názov knižnice (alebo názov cesty), typ objektu, vlastníka objektu a typ zlyhania. Tento príkaz v určitých prípadoch vytvorí záznam v protokole, hoci tieto prípady nie sú porušením integrity. Príkaz vytvorí položku protokolu napríklad pre podpísateľné objekty bez digitálneho podpisu, pre objekty, ktoré nemôže skontrolovať a pre objekty vo formáte, ktorý vyžaduje zmeny, aby sa dal použiť v aktuálnej implementácii systému (konverzia IMPI na RISC).

Hodnota parametra CHKSIG kontroluje to, ako príkaz spracováva elektronické podpisy na objektoch. Pre tento parameter môžete zadať niektorú z troch hodnôt:
- *SIGNED – Ak zadáte túto hodnotu, skontroluje príkaz objekty s elektronickými podpismi. Záznam do protokolu vytvorí pre objekty, ktoré majú neplatný podpis. Toto je predvolená hodnota príkazu.
- *ALL – Zadaním tejto hodnoty skontroluje príkaz všetky podpisovateľné objekty a určí, ktoré z nich sú podpísané. Príkaz vytvorí záznam v protokole pre každý podpisovateľný objekt, ktorý nie je podpísaný a pre každý objekt s neplatným podpisom.
- *NONE – Po zadaní tejto hodnoty príkaz nekontroluje elektronické podpisy na objektoch.

Príkaz CHKPRDOPT (Check Product Option)

Príkaz Check Product Option (CHKPRDOPT) oznamuje rozdiel medzi správnou štruktúrou a aktuálnou štruktúrou softvérového produktu. Tento príkaz napríklad nahlási chybu, ak je objekt vymazaný z nainštalovaného produktu.

Hodnota parametra CHKSIG kontroluje to, ako príkaz spracováva elektronické podpisy na objektoch. Pre tento parameter môžete zadať niektorú z troch hodnôt:
- *SIGNED – Ak zadáte túto hodnotu, skontroluje príkaz objekty s elektronickými podpismi. Príkaz overuje podpis akéhokoľvek podpísaného objektu. Ak príkaz zistí, že podpis objektu nie je platný, odošle správu do protokolu úlohy a označí stav produktu ako chybový. Toto je predvolená hodnota príkazu.
- *ALL – Zadaním tejto hodnoty príkaz skontroluje všetky podpisovateľné objekty, aby zistil, či sú podpísané a aby overil podpisy na týchto objektoch. Príkaz odošle správu do protokolu úlohy pri každom podpisovateľnom objekte, ktorý nie je podpísaný; neoznačí ale stav produktu ako chybový. Ak príkaz zistí, že podpis objektu nie je platný, odošle správu do protokolu úlohy a zároveň označí stav produktu ako chybový.
- *NONE – Po zadaní tejto hodnoty príkaz nekontroluje elektronické podpisy na produktových objektoch.

Príkaz SAVLICPGM (Save Licensed Program)

Príkaz Save Licensed Program (SAVLICPGM) vám umožňuje uložiť kópiu objektu, ktorý tvorí licencovaný program. Ukladá licencovaný program vo forme, z ktorej môže byť obnovený príkazom Restore Licensed Program (RSTLICPGM).

Hodnota parametra CHKSIG kontroluje to, ako príkaz spracováva elektronické podpisy na objektoch. Pre tento parameter môžete zadať niektorú z troch hodnôt:
- *SIGNED – Ak zadáte túto hodnotu, skontroluje príkaz objekty s elektronickými podpismi. Príkaz overí podpisy akýchkoľvek podpísaných objektov, ale nepodpísané objekty nekontroluje. Ak príkaz zistí, že podpis na objekte nie je platný, identifikuje objekt odoslaním správy do protokolu úlohy a proces ukladania zlyhá. Toto je predvolená hodnota príkazu.

- *ALL – Zadaním tejto hodnoty príkaz skontroluje všetky podpisovateľné objekty, aby zistil, či sú podpísané a aby overil podpisy na týchto objektoch. Príkaz odošle správu do protokolu úlohy pre každý podpísateľný objekt bez podpisu; proces ukladania sa však neskončí. Ak príkaz zistí, že podpis na objekte nie je platný, odošle správu do protokolu úlohy a proces ukladania zlyhá.
- *NONE – Po zadaní tejto hodnoty príkaz nekontroluje elektronické podpisy na produktových objektoch.

Kontrola integrity funkcie na kontrolu kódu

Ak chcete na kontrolu integrity vášho systému iSeries použiť novú funkciu kontroly integrity funkcie na kontrolu kódu, musíte mať špeciálne oprávnenie *AUDIT.

Ak chcete skontrolovať funkciu na kontrolu kódu, spustite rozhranie API Check System (QydoCheckSystem) na zistenie, či nedošlo k zmenám v kľúčových objektoch operačného systému po ich podpísaní. Pri spustení rozhrania API sa kľúčové systémové objekty vrátane programov, služobných programov a vybratých príkazových objektov (*CMD) v knižnici QSYS kontrolujú nasledovne:

1. Kontrolujú sa všetky programové objekty (*PGM), na ktoré ukazuje tabuľka vstupných bodov systému.
2. Kontrolujú sa všetky služobné programy (*SRVPGM) v knižnici QSYS a integrita rozhrania API Verify Object.
3. Spustí sa rozhranie API Verify Object (QydoVerifyObject) na kontrolu integrity príkazov RSTOBJ (Restore Object), RSTLIB (Restore Library) a CKHOBJITG (Check Object Integrity).
4. Použijú sa príkazy RSTOBJ a RSTLIB na špeciálny úložný súbor (*SAV) na kontrolu správneho hlásenia chýb. Nedostatok chybových správ alebo nesprávne chybové správy indikujú potenciálny problém.
5. Vytvorí sa príkazový objekt (*CMD), ktorý je navrhnutý tak, aby pri kontrole zlyhal.
6. Na tento špeciálny príkazový objekt sa spustí príkaz CHKOBJITG a rozhranie API Verify Object na kontrolu správneho hlásenia chýb príkazom CHKOBJITG a rozhraním API Verify Object. Nedostatok chybových správ alebo nesprávne chybové správy indikujú potenciálny problém.

Ak sa chcete dozvedieť viac o interpretácii chybových správ, ktoré generuje funkcia kontroly integrity kódu, pozrite si časť Interpretácia chybových správ kontroly kódu.

Odstraňovanie problémov s podpísanými objektmi

Pri podpisovaní a práci s podpísanými objektmi môže dôjsť k chybám, ktoré vám bránia dokončiť vaše úlohy a dosiahnuť vaše ciele. Väčšina bežných chýb alebo problémov, s ktorými sa stretnete, patrí do týchto kategórií:

Odstraňovanie chýb pri podpisovaní objektov
Prostredníctvom týchto informácií sa dozviete o bežných problémoch, s ktorými sa môžete stretnúť pri kontrole digitálnych podpisov na objektoch a o spôsobe ich opravy.

Odstraňovanie chýb pri kontrole podpisu
Prostredníctvom týchto informácií sa dozviete o bežných problémoch pri práci s pamäťou certifikátov a o kľúčových databázových problémoch, s ktorými sa môžete stretnúť a o spôsobe ich opravy.

Interpretácia chybových správ kontroly kódu
Prostredníctvom týchto informácií sa dozviete o správach, ktoré vracia funkcia kontroly integrity funkcie na kontrolu kódu a o možnostiach použitia týchto správ na kontrolu, že funkcia na kontrolu kódu nie je poškodená a takisto o možných riešeniach v prípade, keď správy indikujú možné poškodenie funkcie alebo kľúčových objektov operačného systému.

Odstraňovanie chýb pri podpisovaní objektov

Na nájdenie informácií o odstraňovaní bežnejších problémov, s ktorými sa môžete stretnúť pri podpisovaní objektov, môžete použiť nasledujúcu tabuľku:

Problém	Možné riešenie
Ak na podpísanie objektu použijem API podpisujúce objekty a cieľové vydanie je V4R5, alebo staršie, proces podpisovania zlyhá a objekt je nepodpísaný (chybová správa CPFB721).	iSeries neposkytuje podporu podpisovania objektov až do V5R1. Ak chcete podpísať objekty, ktoré vrátili chybovú správu CPFB721, musíte programy znova vytvoriť s cieľovým vydaním V5R1, alebo novším.

Odstraňovanie chýb pri kontrole podpisu

Na nájdenie informácií o odstraňovaní bežnejších problémov, s ktorými sa môžete stretnúť pri kontrole digitálnych podpisov na objektoch, môžete použiť nasledujúcu tabuľku:

Problém	Možné riešenie
Zlyhal proces obnovy nepodpísaných objektov.	Ak chýbajúci podpis nie je problémom, skontrolujte, či je systémová hodnota QVFYOBJRST nastavená na hodnotu 5. Hodnota 5 určuje, že nepodpísané objekty sa nemôžu obnoviť. Zmeňte túto hodnotu na 3 a pokúste sa znova o obnovu.
Zlyhal proces obnovy podpísaných objektov.	Toto sa mohlo stať, ak bol do systému presunutý sklad certifikátov *SIGNATUREVERIFICATION, ale nebol použitý DCM na zmenu jeho hesla. V takomto prípade nemôžu byť počas procesu obnovy certifikáty, ktoré sa v ňom nachádzajú, použité na overenie podpisov. Pomocou DCM zmeňte heslo certifikačného skladu. Ak neviete heslo, budete musieť vymazať pamäť certifikátov; potom ju znovu vytvorte a použite program DCM na zmenu hesla.
Pri obnove, alebo inštalácii produktu sa vracia chyba, pretože sa nepodarilo overiť podpis.	Ak nie je možné správne overiť podpis objektu, môže toto zlyhanie naznačovať, že bol objekt od svojho podpisu zmenený. Ak je problémom integrita objektu, nemeňte systémovú hodnotu QVFYOBJRST ani nevykonávajte ďalšie akcie, ktoré by mohli viesť k obnove sporného objektu. Mohlo by to obísť bezpečnosť poskytovanú kontrolou podpisu a zaviesť škodlivý objekt do vášho systému. Namiesto toho musíte kontaktovať signatára objektu za účelom zistenia vhodnej akcie, ktorú treba vykonať na vyriešenie problému.

Interpretácia chybových správ kontroly kódu

Nasledujúca tabuľka poskytuje zoznam správ, ktoré počas spracovania generuje funkcia na kontrolu kódu. Táto tabuľka však nepredstavuje súhrnný zoznam všetkých správ, ktoré môžete prijať. Namiesto toho obsahuje táto tabuľka zoznam tých správ, ktoré s veľkou pravdepodobnosťou indikujú úspešné dokončenie funkcie na kontrolu kódu alebo zaznamenanie vážneho problému. Detailný zoznam chybových správ si môžete pozrieť v dokumentácii k rozhraniu API Check System (QydoCheckSystem).

Takisto sa v tomto zozname nenachádza množstvo informačných správ, ktoré generuje funkcia na kontrolu kódu počas spracovania. Ak sa chcete dozvedieť viac o procese kontroly funkcie na kontrolu kódu, pozrite si časť Kontrola integrity funkcie na kontrolu kódu.

Tabuľka 1. Chybové správy kontroly kódu

Chybová správa	Možný problém a riešenie
CPFB729	Znamená, že proces kontroly funkcie na kontrolu kódu zlyhal a neskončil podľa očakávaní. Toto zlyhanie môže byť spôsobené množstvom problémov. Zobrazte protokol úlohy, kde nájdete detailnejšie chybové správy, pomocou ktorých môžete určiť presný pôvod zlyhania a možnú príčinu. Ak zistíte, že kľúčové objekty operačného systému zlyhali pri kontrole integrity, môže to znamenať, že objekt bol zmenený po jeho podpísaní pri dodávke operačného systému. Budete zrejme musieť preinštalovať operačný systém na zabezpečenie jeho integrity.
Pri zobrazení protokolu úlohy vidíte správy ako CPFB723, CPD37A1 alebo CPD37A0 pre tieto špecifické objekty: • Programové objekty (*PGM): – Objekt QYDONOSIG v knižnici QTEMP – Objekt QYDOBADSIG v knižnici QTEMP • Príkazové objekty (*CMD): – Objekt QYDOBADSIG v knižnici QTEMP – Objekt SIGNOFF v knižnici QTEMP	Znamená, že špeciálna množina objektov, ktorú používa funkcia na kontrolu kódu na testovanie integrity zlyhala podľa očakávaní. Toto zlyhanie znamená, že príkazy RSTOBJ, RSTLIB, CHKOBJITG a rozhranie API Verify Object hlásia chyby správne. Nie je potrebná žiadna ďalšia akcia.
CPFB723 pre každý ďalší objekt iný ako objekty uvedené doteraz v tejto tabuľke.	Znamená, že podpis na kľúčovom objekte operačného systému zlyhal pri kontrole. Toto zlyhanie môže znamenať, že objekt bol zmenený po jeho podpísaní pri dodávke operačného systému. Budete zrejme musieť preinštalovať operačný systém na zabezpečenie jeho integrity.
CPFB722 pre každý ďalší objekt iný ako objekty uvedené doteraz v tejto tabuľke.	Znamená, že kľúčový objekt operačného systému nemá podpis v situácii, keď sa podpis očakáva. Tento chýbajúci podpis môže znamenať, že objekt bol zmenený po jeho podpísaní pri dodávke operačného systému. Budete zrejme musieť preinštalovať operačný systém na zabezpečenie jeho integrity.
CPF72A pre každý ďalší objekt iný ako objekty uvedené doteraz v tejto tabuľke.	Znamená, že kľúčový objekt operačného systému zlyhal pri kontrole integrity. Toto zlyhanie môže znamenať, že objekt bol zmenený po jeho podpísaní pri dodávke operačného systému. Budete zrejme musieť preinštalovať operačný systém na zabezpečenie jeho integrity.

Ak budete niekedy potrebovať preinštalovať kód, ktorý kontroluje integritu funkcie na kontrolu kódu, musíte ho získať zo známeho a dobrého zdroja. Môžete napríklad načítať inštalačné médium, ktoré ste použili na inštaláciu súčasného vydania. Ak chcete obnoviť funkciu na kontrolu kódu, vykonajte z príkazového riadka systému OS/400 tieto kroky:

1. Spustite príkaz QSYS/DLTPGM QSYS/QYDOCHKS. Tento príkaz vymaže rozhranie API Check System (OPM, QYDOCHKS; ILE, QydoCheckSystem).
2. Spustite príkaz QSYS/DLTSRVPGM QSYS/QYDOCHK1. Tento príkaz vymaže služobný program funkcie na kontrolu kódu s rozhraním API Check System (OPM, QYDOCHKS; ILE, QydoCheckSystem).
3. Spustite príkaz QSYS/DLTF QSYS/QYDOCHKF. Tento príkaz vymaže úložný súbor obsahujúci objekty, ktoré používa funkcia na kontrolu kódu na testovanie zlých a chýbajúcich podpisov.
4. Spustite príkaz QSYS/RSTOBJ OBJ(QYDOCHK*) SAVLIB(QSYS) DEV(OPT01) OBJTYPE(*ALL) OPTFILE('Q5722SS1/Q5200M_/Q00/Q90'). Tento príkaz obnoví všetky potrebné objekty pre funkciu na kontrolu kódu z načítaného inštalačného média.

Informácie súvisiace s podpisovaním objektov a overovaním podpisov

Podpisovanie objektov a overovanie podpisov sú relatívne nové bezpečnostné technológie. Ak máte záujem lepšie pochopiť, ako tieto technológie fungujú, ponúkame vám krátky zoznam ďalších zdrojov, ktoré by vám pri tom mohli pomôcť:

- **Pomocná webová stránka firmy VeriSign**
  Webová stránka firmy VeriSign poskytuje rozsiahlu knižnicu tém o digitálnych certifikátoch, ako napríklad o podpisovaní objektov, ale aj množstvo iných tém o internetovej bezpečnosti.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Táto publikácia IBM Redbook sa zameriava na sieťové bezpečnostné vylepšenia vo V5R1. Tento Redbook obsahuje množstvo tém, vrátane opisu použitia funkcie podpisovania objektov iSeries, správcu digitálnych certifikátov, atď.

Právne vyhlásenia

Tento dokument obsahuje programátorské príklady.

IBM vám udeľuje neexkluzívne právo na používanie všetkých programátorských príkladov, z ktorých môžete vygenerovať podobnú funkciu prispôsobenú pre vaše vlastné špecifické potreby.

Všetok vzorový kód poskytuje IBM len na ilustračné účely. Tieto príklady neboli dôkladne testované vo všetkých podmienkach. IBM preto nemôže garantovať, alebo predpokladať spoľahlivosť, použiteľnosť, alebo fungovanie týchto programov.

Všetky tieto programy sú vám poskytnuté ″TAK AKO SÚ″ bez akýchkoľvek záruk žiadneho druhu. Vyplývajúce záruky neprekračovania, predajnosti, alebo vhodnosti pre konkrétny účel striktne odmietame.

Príloha. Právne informácie

Tieto informácie boli vyvinuté pre produkty a služby ponúkané v USA.

IBM nemusí ponúkať produkty, služby alebo vlastnosti opisované v tomto dokumente v iných krajinách. Informácie o aktuálne dostupných produktoch a službách vo vašej krajine získate od predstaviteľa lokálnej pobočky IBM. Žiadny odkaz na produkt, program alebo službu IBM nie je myslený tak a ani neimplikuje, že sa môže používať len tento produkt, program alebo služba od IBM. Namiesto nich sa môže použiť ľubovoľný funkčne ekvivalentný produkt, program alebo služba, ktorá neporušuje intelektuálne vlastnícke právo IBM. Vyhodnotenie a kontrola činnosti produktu, programu alebo služby inej ako od IBM je však na zodpovednosti užívateľa.

IBM môže mať patenty alebo podané prihlášky patentov týkajúcich sa predmetu opísanom v tomto dokumente. Získanie tohto dokumentu vám nedáva žiadnu licenciu na tieto patenty. Požiadavky o licencie môžete zasielať písomne na adresu:

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

Žiadosti o licencie týkajúce sa dvojbajtových (DBCS) informácií smerujte na oddelenie intelektuálneho vlastníctva IBM vo vašej krajine alebo ich pošlite písomne na adresu:

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

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s lokálnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU "TAK AKO JE" BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK NEPOŠKODENIA, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nedovoľujú zriecť sa vyjadrených alebo implikovaných záruk v určitých transakciách, preto sa vás toto vyhlásenie nemusí týkať.

Tieto informácie môžu obsahovať technické nepresnosti alebo typografické chyby. Tieto informácie sa periodicky menia; tieto zmeny budú začlenené do nových vydaní publikácie. IBM môže kedykoľvek bez ohlásenia spraviť zmeny a/alebo vylepšenia v produkte(och) a/alebo programe(och) opísanom v tejto publikácii.

Všetky odkazy v týchto informáciách na webové lokality iné ako od IBM sú poskytnuté len pre pohodlie a v žiadnom prípade neslúžia ako potvrdenie obsahu týchto webových lokalít. Materiály na týchto webových lokalitách nie sú časťou produktov IBM a použitie týchto webových lokalít je na vaše vlastné riziko.

| IBM môže použiť alebo distribuovať všetky vami poskytnuté informácie ľubovoľným spôsobom bez toho, aby voči vám
| vznikli akékoľvek záväzky.

Vlastníci licencií na tento program, ktorí chcú o ňom získať informácie za účelom povolenia: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto) a (ii) vzájomného použitia vymieňaných informácií by mali kontaktovať:

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

Rochester, MN 55901
U.S.A.

Takéto informácie môžu byť dostupné, môžu byť predmetom príslušných pojmov a podmienok a v niektorých prípadoch sú dostupné za poplatok.

Licenčný program opísaný v týchto informáciách a všetky licenčné materiály, ktoré sú preň dostupné, poskytuje IBM podľa podmienok zmluvy IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, alebo inej ekvivalentnej zmluvy medzi nami.

Všetky údaje o výkone, uvádzané v tomto dokumente boli získané v riadenom prostredí. Výsledky získané v iných prevádzkových prostrediach sa môžu podstatne odlišovať. Niektoré merania boli vykonané v systémoch vývojovej úrovne a nie je žiadna záruka, že tieto merania budú rovnaké vo všeobecne dostupných systémoch. Okrem toho, niektoré výsledky boli odhadnuté extrapoláciou. Skutočné výsledky sa môžu odlišovať. Užívatelia tohto dokumentu by si mali overiť použiteľnosť týchto údajov pre svoje špecifické prostredie.

Informácie o produktoch, iných ako od IBM, boli získané od poskytovateľov týchto produktov, z ich uverejnených oznámení alebo z iných, verejne dostupných zdrojov. IBM netestovala tieto produkty a nemôže potvrdiť presnosť ich výkonu, kompatibilitu ani žiadne iné tvrdenie týkajúce sa produktov, iných ako od IBM. Otázky k schopnostiam produktov, iných ako od IBM, by ste mali adresovať poskytovateľom týchto produktov.

Všetky vyhlásenia týkajúce sa budúceho smerovania alebo úmyslov IBM sú predmetom zmeny alebo zrušenia bez ohlásenia a vyjadrujú len zámery a ciele.

Tieto informácie obsahujú príklady údajov a hlásení používaných v každodenných firemných operáciách. Kvôli ich čo najlepšej ilustrácii obsahujú tieto príklady mená osôb, názvy spoločností, pobočiek a produktov. Všetky tieto mená a názvy sú vymyslené a akákoľvek podobnosť s menami, názvami a adresami používanými skutočnými osobami a spoločnosťami je čisto náhodná.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom kóde, ktoré ilustrujú programovacie techniky v rôznych platformách. Tieto vzorové materiály môžete kopírovať, modifikovať a distribuovať v ľubovoľnej forme bez platby IBM, pre účely vývoja, používania, marketingu alebo distribuovania aplikačných programov vyhovujúcich aplikačnému programovaciemu rozhraniu pre operačnú platformu, pre ktorú boli vzorové programy napísané. Tieto príklady neboli dôkladne testované vo všetkých podmienkach. IBM preto nemôže zaručiť alebo implikovať spoľahlivosť, prevádzkyschopnosť alebo funkčnosť týchto programov.

VZHĽADOM NA VŠETKY ZÁKONNÉ ZÁRUKY, KTORÉ NEMÔŽU BYŤ VYLÚČENÉ, IBM, JEJ VÝVOJÁRI PROGRAMOV A DODÁVATELIA NEDÁVAJÚ ŽIADNE ZÁRUKY ALEBO PODMIENKY, BUĎ PRIAME ALEBO IMPLIKOVANÉ, VRÁTANE NO BEZ OBMEDZENIA NA IMPLIKOVANÉ ZÁRUKY ALEBO PODMIENKY PREDAJNOSTI, VHODNOSTI NA URČITÝ ÚČEL A NEPORUŠENIA ZÁKONA, OHĽADNE PROGRAMU ALEBO TECHNICKEJ PODPORY, AK NEJAKÁ EXISTUJE.

V ŽIADOM PRÍPADE IBM, JEJ VYVOJÁRI PROGRAMOV ALEBO DODÁVATELIA, NEZODPOVEDAJÚ ZA NIČ Z NASLEDUJÚCEHO, AJ KEĎ BOLI O TEJTO MOŽNOSTI INFORMOVANÍ:

1. STRATA ALEBO POŠKODENIE DÁT;
2. ŠPECIFICKÉ, NÁHODNÉ ALEBO NEPRIAME ŠKODY, ANI ZA ŽIADNE VYPLÝVAJÚCE EKONOMICKÉ ŠKODY; ALEBO
3. UŠLÝ ZISK, STRATA OBCHODU, TRŽBY, DOBRÉHO MENA ALEBO PREDPOKLADANÝCH ÚSPOR.

NIEKTORÉ JURISDIKCIE NEPOVOĽUJÚ VYLÚČENIE ALEBO OBMEDZENIE NÁHODNÝCH ALEBO VYPLÝVAJÚCICH ŠKÔD, TAKŽE NIEKTORÉ ALEBO VŠETKY ZO SKÔR UVEDENÝCH OBMEDZENÍ ALEBO VYLÚČENÍ SA VÁS NEMUSIA TÝKAŤ.

Každá kópia alebo ľubovoľná časť týchto vzorových programov alebo každá odvodená práca musí obsahovať toto oznámenie o autorských právach:

© (názov vašej spoločnosti) (rok). Časti tohto kódu sú odvodené od vzorových programov IBM Corp. © Copyright IBM Corp. _uveďte rok alebo roky_. Všetky práva vyhradené.

Ak si prezeráte elektronickú kópiu týchto informácií, nemusia byť zobrazené fotografie ani farebné ilustrácie.

Ochranné známky

Nasledujúce pojmy sú ochranné známky spoločnosti International Business Machines v USA, v iných krajinách alebo v oboch:

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

Microsoft, Windows, Windows NT a logo Windows sú obchodné známky spoločnosti Microsoft Corporation v USA, v iných krajinách alebo v oboch.

Java a všetky ochranné známky založené na Java sú ochranné známky spoločnosti Sun Microsystems v USA, v iných krajinách alebo v oboch.

Ostatné názvy spoločnosti, produktov alebo služieb môžu byť ochranné známky alebo značky služieb iných.

Pojmy a podmienky pre preberanie a tlač publikácií

Oprávnenie na používanie informácií, ktoré ste si vybrali na stiahnutie, je udelené v prípade dodržiavania týchto podmienok a vášho potvrdenia ich akceptovania.

Osobne použitie: Tieto informácie môžete reprodukovať pre svoje osobné, nekomerčné použitie, za predpokladu, že budú zachované všetky oznamy o vlastníctve. Tieto informácie ani ich časti nesmiete distribuovať, zobrazovať ani z nich robiť odvodené práce, bez výslovného súhlasu IBM.

Komerčné použitie: Tieto informácie môžete reprodukovať, distribuovať a zobrazovať výhradne vo vašom podniku, za predpokladu, že budú zachované všetky oznamy o vlastníctve. Z týchto informácií ani zo žiadnej ich časti nesmiete robiť odvodené práce, ani ich reprodukovať, distribuovať alebo zobrazovať mimo váš podnik, bez výslovného súhlasu IBM.

Okrem toho, čo je výslovne udelené v tomto oprávnení, nie sú udelené žiadne iné oprávnenia, licencie alebo práva, vyjadrené ani implikované, na informácie alebo akékoľvek dáta, softvér alebo iné tu uvedené intelektuálne vlastníctvo.

IBM si vyhradzuje právo kedykoľvek stiahnuť udelené oprávnenia, podľa svojho uváženia, keď používanie týchto informácií škodí jej záujmom, alebo podľa rozhodnutia IBM, keď nie sú správne dodržiavané hore uvedené pokyny.

Tieto informácie nemôžete prevziať ani exportovať okrem prípadu, ak to dovoľujú všetky aplikovateľné zákony a regulácie, vrátane všetkých zákonov a regulácií USA pre export. IBM NEDÁVA ŽIADNU ZÁRUKU NA OBSAH TÝCHTO INFORMÁCIÍ. TIETO INFORMÁCIE SA POSKYTUJÚ ″TAK AKO SÚ″ A BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE ALE BEZ OBMEDZENIA NA IMPLIKOVANÉ ZÁRUKY PREDAJNOSTI, NEPORUŠENIA ZÁKONA A VHODNOSTI NA URČITÝ ÚČEL.

Všetok materiál je vlastníctvom IBM Corporation.

Stiahnutím alebo vytlačením informácií z tejto stránky ste vyjadrili svoj súhlas s týmito podmienkami.

Právne vyhlásenie o kóde

IBM vám udeľuje neexkluzívnu licenciu autorských práv na použitie všetkých príkladov programovacieho kódu, z ktorých môžete generovať podobné funkcie prispôsobené vašim vlastným špecifickým potrebám.

VZHĽADOM NA VŠETKY ZÁKONNÉ ZÁRUKY, KTORÉ NEMÔŽU BYŤ VYLÚČENÉ, IBM, JEJ VÝVOJÁRI PROGRAMOV A DODÁVATELIA NEDÁVAJÚ ŽIADNE ZÁRUKY ALEBO PODMIENKY, BUĎ PRIAME ALEBO IMPLIKOVANÉ, VRÁTANE NO BEZ OBMEDZENIA NA IMPLIKOVANÉ ZÁRUKY ALEBO PODMIENKY PREDAJNOSTI, VHODNOSTI NA URČITÝ ÚČEL A NEPORUŠENIA ZÁKONA, OHĽADNE PROGRAMU ALEBO TECHNICKEJ PODPORY, AK NEJAKÁ EXISTUJE.

V ŽIADOM PRÍPADE IBM, JEJ VYVOJÁRI PROGRAMOV ALEBO DODÁVATELIA, NEZODPOVEDAJÚ ZA NIČ Z NASLEDUJÚCEHO, AJ KEĎ BOLI O TEJTO MOŽNOSTI INFORMOVANÍ:

1. STRATA ALEBO POŠKODENIE DÁT;
2. ŠPECIFICKÉ, NÁHODNÉ ALEBO NEPRIAME ŠKODY, ANI ZA ŽIADNE VYPLÝVAJÚCE EKONOMICKÉ ŠKODY; ALEBO
3. UŠLÝ ZISK, STRATA OBCHODU, TRŽBY, DOBRÉHO MENA ALEBO PREDPOKLADANÝCH ÚSPOR.

NIEKTORÉ JURISDIKCIE NEPOVOĽUJÚ VYLÚČENIE ALEBO OBMEDZENIE NÁHODNÝCH ALEBO VYPLÝVAJÚCICH ŠKÔD, TAKŽE NIEKTORÉ ALEBO VŠETKY ZO SKÔR UVEDENÝCH OBMEDZENÍ ALEBO VYLÚČENÍ SA VÁS NEMUSIA TÝKAŤ.

Vytlačené v USA