System i

Bezpečnostné podpisovanie objektov a kontrola podpisov

Verzia 6, vydanie 1

System i

Bezpečnostné podpisovanie objektov a kontrola podpisov

Verzia 6, vydanie 1

Poznámka

Pred použitím týchto informácií a produktu, ktorý podporujú, si prečítajte informácie v časti “Právne informácie”, na strane 45.

Toto vydanie sa vzťahuje na verziu 6, vydanie 1, úprava 0 produktu IBM i5/OS (číslo produktu 5761-SS1) a na všetky ďalšie vydania a úpravy, 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 kontrola podpisov

Nájdete tu informácie o bezpečnostných funkciách podpisovania objektov a kontroly podpisov i5/OS, ktoré môžete používať na zaistenie integrity objektov. Dozviete sa tu, ako používať jednu z metód i5/OS pre vytváranie digitálnych podpisov na objektoch v snahe identifikovať pôvod objektu a poskytnúť spôsob na zistenie zmien v objekte. Dozviete sa tiež, ako zlepšiť bezpečnosť systému kontrolovaním digitálnych podpisov na objektoch, vrátane objektov operačného systému, ako určiť, či došlo k zmene obsahu objektu od jeho podpísania.

Podpisovanie objektov a kontrola podpisov sú bezpečnostné funkcie, ktoré môžete použiť na kontrolovanie integrity rôznych objektov. 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 kontrolu podpisov môžete implementovať cez:

- API na naprogramované podpisovanie objektov a kontrolu podpisov.
- Správcu digitálnych certifikátov na podpisovanie objektov a na prezeranie, alebo overovanie podpisov.
- Riadiace centrum 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:

Poznámka: Použitím týchto príkladov kódu súhlasíte s podmienkami v časti “Licencia na kód a zrieknutie sa zodpovednosti” na strane 43.

Čo je nové vo vydaní V6R1

V tejto časti nájdete nové informácie o kolekcii tém o podpisovaní objektov a overovaní podpisov.

Overovanie integrity kontrolóra kódu

Počnúc vydaním V6R1 môžete pomocou rozhrania Check System (QydoCheckSystem) a pomocou príkazu Check Object Integrity (CHKOBJITG) overovať licenčné interné kódy (LIC).

Ako zistíte čo je nové alebo čo sa zmenilo

Aby ste mohli ľahšie identifikovať technické zmeny, informačné centrum používa tieto prvky:

- Značka  , ktorá označuje, kde začínajú nové alebo zmenené informácie.
- Značka , ktorá označuje, kde nové alebo zmenené informácie končia.

V súboroch PDF sú nové a zmenené informácie označené symbolom korekcie (|) na ľavom okraji.

Ak chcete získať ďalšie informácie o tom, čo je v tomto vydaní nové alebo zmenené, pozrite si časť Poznámka pre užívateľov.

Súbor PDF pre podpisovanie objektov a kontrolu podpisov

V tejto časti nájdete informácie o tlači celej témy o podpisovaní objektov a kontrole podpisov v systéme i5/OS ako súboru PDF.

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. Kliknite pravým tlačidlom myši na odkaz na súbor PDF vo vašom prehliadači.
2. Vyberte voľbu, ktorá ukladá súbor PDF lokálne.
3. Prejdite do adresára, kde chcete uložiť súbor PDF.
4. Kliknite na **Save**.

Preberanie programu Adobe Acrobat Reader

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

Pojmy podpisovania objektov

V tejto téme nájdete konceptuálne a referenčné informácie o digitálnych podpisoch v systéme i5/OS a o tom, ako procesy podpisovania a overovania podpisov objektov v systéme i5/OS fungujú.

Pred použitím funkcií podpisovania objektov a kontroly podpisov si môžete pozrieť niektoré z týchto konceptov:

Elektronické podpisy

V tejto téme nájdete informácie o elektronických podpisoch i5/OS a o zabezpečení, ktoré poskytujú.

Systém i5/OS poskytuje podporu pre elektronické podpisy pre digitálne certifikáty na elektronické ″podpísanie″ objektov. Elektronický podpis objektu je vytvorený je vytvorený formou šifrovania a je 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.

Podpora pre podpisovanie objektov rozširuje tradičné systémové nástroje na riadenie užívateľov, ktorí môžu meniť objekty. 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.

- **Podpisy celých objektov** Tento typ podpisu zahŕňa všetky okrem niektorých nepodstatných bajtov objektu.
- **Podpisy objektov jadra** 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.

Súvisiace koncepty

“Podpisovateľné objekty”
V tejto téme nájdete informácie o tom, ktoré objekty môžete podpísať a o voľbách príkazov i5/OS (*CMD) na podpisovanie objektov.

Súvisiace informácie

Správca digitálnych certifikátov (DCM)

Podpisovateľné objekty

V tejto téme nájdete informácie o tom, ktoré objekty môžete podpísať a o voľbách príkazov i5/OS (*CMD) na podpisovanie objektov.

Digitálne môžete podpisovať množstvo typov objektov i5/OS, bez ohľadu na metódu, ktorú použijete na ich podpísanie. 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 na serveri Integrated xSeries Server for System i používate server Windows 2000, v integrovanom súborovom systéme je dostupný súborový systém QNTC. Adresáre v tomto súborovom systéme sa nepovažujú za lokálne, pretože obsahujú súbory vlastnené operačným systémom Windows 2000. Takisto nemôžete podpísať prázdne objekty ani objekty skompilované pre vydanie staršie ako V5R1.

Podpisy objektov príkazov (*CMD)

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 celá 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.

Kompozícia podpisov objektov jadra 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
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
aktuálnej knižnice	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

Súvisiace koncepty

“Elektronické podpisy” na strane 2
V tejto téme nájdete informácie o elektronických podpisoch i5/OS a o zabezpečení, ktoré poskytujú.

Spracovanie podpisovania objektov

V tejto téme nájdete informácie o tom, ako funguje proces podpisovania objektov na systéme s operačným systémom i5/OS a aké parametre môžete pre tento proces nastaviť.

Pri podpisovaní objektov môžete pre proces podpisovania zadať nasledujúce možnosti:

Spracovanie pri chybe
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.

Duplicitné podpísanie objektu
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.

Rozsah podpisu objektu
Pri podpisovaní objektov *CMD určujete, či má aplikácia podpísať celý objekt, alebo len jeho jadro.

Spracovanie overovania podpisov

V tejto časti zistíte, ako funguje proces overovania podpisov objektov v systéme i5/OS a aké parametre môžete pre tento proces nastaviť.

Pri overovaní objektov môžete pre proces podpisovania zadať nasledujúce možnosti:

Spracovanie pri chybe
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.

Kontrola podpisov jadra verzus celé podpisy
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 dôveryhodným zdrojom (IBM), podpis sa musí zhodovať, inak proces kontroly 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 je 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 kontrolóra kódu

Táto téma poskytuje informácie o tom, ako môžete overiť integritu kontrolóra kódu, ktorý kontroluje integritu systému s operačným systémom i5/OS.

Vo vydaní V5R2 je i5/OS dodávané s funkciou kontroly kódu, ktorú môžete použiť na kontrolu integrity podpísaných objektov vo vašom systéme, vrátane celého kódu operačného systému, ktorý IBM dodáva a podpisuje pre váš systém. Od vydania V5R3 môžete použiť API Check System na overenie integrity kódu tejto funkcie samotnej, ako aj kľúčových objektov operačného systému. Teraz, IBM podpisuje licenčný interný kód (LIC) a na overenie kódu LIC môžete použiť API Check System (QydoCheckSystem) alebo príkaz Check Object Integrity (CHKOBJITG).

API QydoCheckSystem (Check System) poskytuje kontrolu integrity systému i5/OS. Toto rozhranie môžete použiť na kontrolu programov (*.PGM), služobných programov (*SRVPGM) a vybraných príkazových objektov (*CMD) v knižnici QSYS. Naviac, rozhranie Check System API testuje príkazy Restore Object (RSTOBJ), Restore Library (RSTLIB), Check Object Integrity (CHKOBJITG) a Verify Object API. 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.

Súvisiace úlohy

"Kontrola integrity kontrolóra kódu" na strane 40
Dozviete sa tu, ako skontrolovať integritu kontrolóra kódu na kontrolu integrity systému i5/OS.

Scenáre podpisovania objektov

Pozrite si scenáre, ktoré ilustrujú niektoré bežné situácie použitia funkcií na podpisovanie objektov a overovanie podpisov v systéme i5/OS. Každý scenár tiež predstavuje konfiguračné úlohy, ktoré musíte vykonať, aby ste mohli implementovať scenár tak, ako je opísaný.

Váš systém poskytuje niekoľko odlišných metód pre podpisovanie objektov a kontrolu podpisov objektov. 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. Tieto scenáre vám môžu pomôcť určiť spôsob použitia funkcií podpisovania objektov, ktorý je najvhodnejší pre vaše firemné a bezpečnostné potreby:

Scenár: Používanie DCM na podpisovanie objektov a overovanie podpisov

V tomto scenári je opísaná spoločnosť, ktorá potrebuje, aby boli citlivé objekty jej aplikácií podpísané na ich verejnom webovom servery. Potrebujú byť schopní jednoducho určiť, ak sa na týchto objektoch vyskytnú neautorizované zmeny. Vychádzajúc z týchto podnikateľských potrieb a bezpečnostných cieľov, tento scenár popisuje používanie manažéra Digital Certificate Manager (DCM) ako primárny spôsob podpisovania objektov v i5/OS.

Situácia

Ako administrátor v MyCo, Inc. ste zodpovedný za manažovanie dvoch systémov vašej spoločnosti. Jeden z týchto systémov poskytuje verejnú webovú lokalitu pre vašu spoločnosť. Na vývoj obsahu pre túto webovú lokalitu a presun súborov a programových objektov na verejný webový server po ich otestovaní používate interný produkčný systém spoločnosti.

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.

Oboznámili ste sa s možnosťami podpisovania objektov i5/OS a dozvedeli ste sa, že existuje niekoľko metód, ktoré môžete použiť na podpisovanie objektov a kontrolu podpisov objektov. Ste zodpovedný za manažovanie malého počtu systémov a myslíte, že podpisovanie objektov nebudete využívať často, preto ste sa na vykonávanie týchto úloh rozhodli pre používanie Správcu digitálnych certifikátov (DCM). 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 ku krokom, ktoré sú zahrnuté v nastavovaní a používaní podpisovania objektov, keď chcete podpisovať objekty v malom počte systémov.

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 digitálne podpísať citlivé objekty, ako sú programy cgi-bin, ktoré generujú formuláre vo verejnom serveri vašej spoločnosti. 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:

- Firemné aplikácie a iné citlivé objekty vo webovom serveri (Systém B) musia byť podpísané certifikátom vydaným Lokálnou CA, aby sa znížili náklady na podpisovanie aplikácií.
- Administrátori systému a iní určení užívatelia musia byť schopní jednoducho skontrolovať digitálne podpisy v systémoch, aby overili zdroj a autenticitu objektov, ktoré podpísala spoločnosť. Dosiahne sa to tým, že každý systém bude mať kópiu certifikátu na kontrolu podpisov od vašej spoločnosti a tiež certifikát lokálnej certifikačnej autority (CA) v pamäti certifikátov *SIGNATUREVERIFICATION každého servera.
- Kontrolou podpisov firemných aplikácií a iných objektov môžu administrátori a ostatní zisťovať, či bol obsah objektov zmenený od ich posledného podpísania.

- 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:

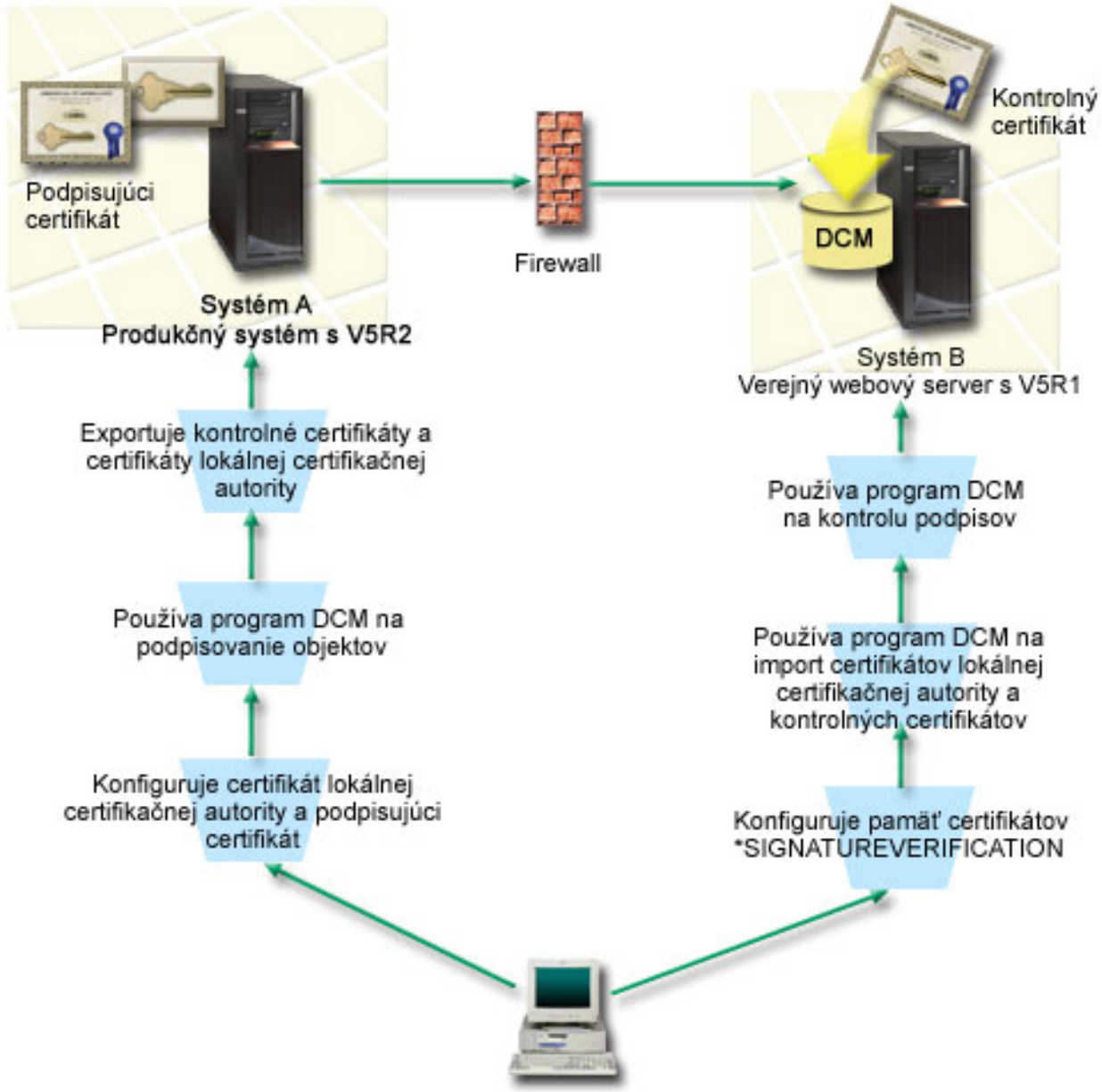

Diagram zobrazuje nasledujúce body súvisiace so scenárom:

Systém A

- Systém A je model System i s operačným systémom OS/400, verzia 5, vydanie 2 (V5R2).
- Systém A je interný produkčný systém spoločnosti a vývojová platforma pre verejný webový server System i (Systém B).
- Systém A obsahuje 128-bitového šifrovacieho poskytovateľa prístupu pre System i (5722–AC3).

- Na systéme A je nainštalovaná aplikácia Digital Certificate Manager (voľba 34) a IBM HTTP Server (5722–DG1).
- Systém A vystupuje ako lokálna certifikačná autorita (CA) a certifikát podpisujúci objekty sa nachádza v tomto systéme.
- Systém A používa DCM na podpisovanie objektov a je primárny systém na podpisovanie objektov pre verejné aplikácie spoločnosti a iné objekty.
- Systém A je nakonfigurovaný na povolenie kontroly podpisov.

Systém B
- Systém B je model System i s operačným systémom OS/400, verzia 5, vydanie 1 (V5R1).
- Systém B je externý verejný webový server spoločnosti mimo firewallu spoločnosti.
- Systém B má nainštalovaný produkt Cryptographic Access Provider 128-bit (5722–AC3).
- Na systéme B je nainštalovaná aplikácia Digital Certificate Manager (voľba 34) a IBM HTTP Server (5722–DG1).
- Systém B nefunguje ako lokálna CA, ani nepodpisuje objekty.
- Systém B je nakonfigurovaný na povolenie kontroly objektov pomocou DCM na vytvorenie pamäte certifikátov *SIGNATUREVERIFICATION a import potrebných certifikátov na kontrolu a certifikátov 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 systémy musia spĺňať požiadavky na inštaláciu a používanie Správcu digitálnych certifikátov (DCM).
2. V žiadnom z týchto systémov nebolo v minulosti nakonfigurované ani používané DCM.
3. Všetky systémy majú nainštalovanú najvyššiu úroveň licenčného programu Cryptographic Access Provider 128-bit (5722-AC3).
4. Predvolené nastavenie pre systémovú hodnotu kontroly podpisov objektov počas obnovy (QVFYOBJRST) vo všetkých systémoch v scenári je 3 a toto nastavenie sa nemôže zmeniť. Predvolené nastavenie zabezpečuje, že systém môže overovať podpisy objektov počas obnovovania podpísaných objektov.
5. Administrátor systému pre Systém A musí mať špeciálne oprávnenie *ALLOBJ na podpisovanie objektov, alebo užívateľský profil musí byť autorizovaný na aplikáciu podpisujúcu objekty.
6. Systémový administrátor, alebo ktokoľvek, kto vytvára sklad certifikátov v DCM, musí mať špeciálne oprávnenia *SECADM a *ALLOBJ.
7. Administrátor systému alebo ostatní vo všetkých ostatných systémoch musia mať špeciálne oprávnenie *AUDIT na kontrolu podpisov objektov.

Kroky úlohy konfigurácie

Sú dve množiny úloh, ktoré musíte vykonať pri implementácii tohto scenára: Jedna množina úloh vám dovolí nakonfigurovať Systém A ako lokálnu Certifikačnú autoritu (CA) a povolí podpisovanie a kontrolovanie podpisov objektov. Druhá množina úloh vám dovolí nakonfigurovať Systém B na kontrolu podpisov objektov, ktoré vytvorí Systém A.

Tieto kroky vykonajte podľa detailov scenárov dole.

Kroky úloh pre Systém A

Každú z týchto úloh musíte vykonať v Systéme A, aby ste vytvorili lokálnu CA a povolili podpisovanie a kontrolovanie objektov, ako opisuje tento scenár:
1. Nainštalujte a nakonfigurujte všetky vyžadované produkty System i
2. Pomocou DCM vytvorte lokálnu Certifikačnú autoritu (CA) na vydanie certifikátu podpisujúceho objekty
3. Pomocou DCM vytvorte definíciu aplikácie
4. Pomocou DCM priraďte certifikát k definícii aplikácií na podpisovanie objektov

5. Pomocou DCM podpíšte programové objekty cgi-bin
6. Pomocou DCM vyexportujte certifikáty, ktoré musia používať ostatné systémy na kontrolu podpisov objektov. Do súboru musíte vyexportovať kópiu certifikátu lokálnej CA aj kópiu certifikátu podpisujúceho objekty ako certifikát na kontrolu podpisov.
7. Preneste súbory s certifikátom do verejného servera spoločnosti (Systém B), aby ste vy aj ostatní mohli kontrolovať podpisy vytvorené Systémom A

Kroky úloh pre Systém B

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

V Systéme B musíte vykonať tieto úlohy na kontrolu podpisov objektov, ako opisuje tento scenár:

1. Pomocou Správcu digitálnych certifikátov (DCM) vytvorte pamäť certifikátov *SIGNATUREVERIFICATION
2. Pomocou DCM naimportujte certifikát lokálnej CA a certifikát na kontrolu podpisov
3. Pomocou DCM skontrolujte podpisy prenesených objektov

Súvisiace informácie

Správca digitálnych certifikátov (DCM)

Podrobnosti scenára: Používanie DCM na podpisovanie objektov a overovanie podpisov

Vykonajte nasledujúce úlohy, aby ste nakonfigurovali manažéra Digital Certificate Manager na podpisovanie objektov i5/OS.

Krok 1: Vykonajte všetky vyžadované kroky

Predtým, ako môžete vykonať špecifické konfiguračné úlohy na implementáciu tohto scenára, musíte dokončiť všetky vyžadované úlohy na inštaláciu a konfiguráciu všetkých vyžadovaných produktov System i.

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 kontrolu 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.

Ak chcete použiť DCM na vytvorenie a prevádzkovanie lokálnej CA, vykonajte tieto kroky: Keď ste už vytvorili lokálnu CA a certifikát podpisujúci objekty, musíte definovať aplikáciu na podpisovanie objektov, ktorá bude používať tento certifikát, až potom môžete podpisovať objekty.

1. Spustite DCM. Informácie nájdete v téme Spúšťanie DCM .
2. V navigačnom rámci DCM vyberte **Create a Certificate Authority (CA)**, čím zobrazíte sériu formulárov.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) na vrchu 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 Lokálnej CA.

d. Použite novú Lokálnu CA a vydajte serverový, alebo klientský 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 klientský, alebo serverový certifikát pre pripojenia SSL.

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

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 navigačnej časti kliknite na **Select a Certificate Store** a ako pamäť certifikátov na otvorenie vyberte ***OBJECTSIGNING**.
2. Po zobrazení stránky Certificate Store and Password zadajte heslo, ktoré ste zadali pre pamäť certifikátov pri jej vytvorení a kliknite na **Continue**.
3. V navigačnom rámci označte **Manage Applications** a zobrazte zoznam úloh.
4. V zozname úloh označte **Add application**, čím sa vám zobrazí formulár na definovanie aplikácie.
5. Vyplňte formulár a kliknite na **Add**.

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

Krok 4: Priradenie certifikátu k definícii aplikácie na podpisovanie objektov

Nasledovaním týchto krokov priradíte certifikát vašej aplikácii podpisujúcej objekty:

1. V navigačnom rámci DCM označte **Manage Certificates** a zobrazte zoznam úloh.
2. Zo zoznamu úloh vyberte **Assign certificate**, čím zobrazíte zoznam certifikátov v aktuálnom sklade certifikátov.
3. V zozname označte správny certifikát a kliknutím na **Assign to Applications** zobrazte zoznam definícií aplikácií v aktuálnom sklade certifikátov.
4. Označte v zozname jednu, alebo viac aplikácií a kliknite na **Continue**. Zobrazí sa vám stránka so správou potvrdzujúcou priradenie certifikátu, alebo poskytujúcou chybové informácie o probléme, ktorý sa vyskytol.

Po dokončení tejto úlohy ste pripravený používať DCM na podpisovanie programových objektov, ktoré bude používať verejný webový server (Systém B) vašej spoločnosti.

Krok 5: Podpísanie programových objektov

Ak chcete použiť DCM na podpísanie programových objektov na použitie verejným webovým serverom (Systém B) spoločnosti, vykonajte tieto kroky:

1. V navigačnej časti kliknite na **Select a Certificate Store** a ako pamäť certifikátov na otvorenie vyberte ***OBJECTSIGNING**.
2. Zadajte heslo pre sklad certifikátov *OBJECTSIGNING a kliknite na **Continue**.
3. Keď sa obnoví obsah navigačného rámca, označte **Manage Signable Objects** a zobrazte zoznam úloh.
4. Zo zoznamu úloh vyberte **Sign an object** a zobrazte zoznam definícií aplikácií, ktoré môžete na podpísanie objektov použiť.
5. Vyberte aplikáciu, ktorú ste definovali v predošlom kroku a kliknite na **Sign an object**. 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 **Continue**. Môžete tiež zadať umiestnenie adresára a kliknúť na **Browse**, čím zobrazíte obsah adresára a môžete v ňom vybrať objekty určené na podpísanie.

   Poznámka: Názov objektu musíte zadať s lomítkom na začiatku, inak môže dôjsť k chybe. Na popísanie časti adresára, ktorú chcete podpísať, môžete tiež použiť niektoré zástupné znaky. Týmito zástupnými znakmi sú hviezdička (*****), ktorá zastupuje *ľubovoľný počet znakov*, a otáznik (**?**), ktorý zastupuje *ľubovoľný 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 **Browse** na zobrazenie obsahu knižnice alebo adresára, musíte pred kliknutím na tlačidlo **Browse** zadať zástupný znak ako časť názvu cesty.
7. Určite svoju voľbu procesu, ktorým chcete vybraný objekt, alebo objekty podpisovať a kliknite na **Continue**.

   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 field (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 **Continue**. Alebo zadajte umiestnenie adresára a kliknite na **Browse**, 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.

Ak chcete zaručiť, že vy a ostatní môžete kontrolovať podpisy, musíte vyexportovať potrebné certifikáty do súboru a preniesť súbor s certifikátmi do Systému B. Musíte tiež vykonať všetky úlohy konfigurácie kontroly podpisov v Systéme B ešte pred prenosom podpísaných programových objektov do Systému B. Konfiguráciu kontroly podpisov musíte vykonať pred obnovou podpísaných objektov v Systéme B, aby bolo možné úspešne skontrolovať podpisy.

Krok 6: Export certifikátov, aby ste povolili kontrolu podpisov v Systéme B

Ak podpisujete objekty, aby ste zabezpečili bezúhonnosť ich obsahu, musíte pre vás, aj iných zabezpečiť spôsob overenia spoľahlivosti podpisu. Ak chcete kontrolovať podpisy v rovnakom systéme, ktorý podpisuje objekty (Systém A), musíte použiť DCM na vytvorenie pamäte 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 použiť DCM, aby ste mohli skontrolovať podpisy v rovnakom systéme, ktorý podpisuje tieto objekty (Systém A v tomto scenári), vykonajte tieto kroky:

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

Ak chcete pomocou DCM exportovať kópiu certifikátu Lokálnej CA a kópiu certifikátu na podpisovanie objektov ako certifikát na kontrolu podpisov, aby ste mohli overovať podpisy objektov v iných systémoch (Systém B), vykonajte tieto kroky:

1. V navigačnom rámci vyberte **Manage Certificates** a potom označte úlohu **Export certificate**.
2. Vyberte **Certificate Authority (CA)** a kliknutím na **Continue** 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 vyberte **File** a kliknite na **Continue**.
5. Pre exportovaný certifikát Lokálnej CA zadajte úplný názov cesty a súboru a kliknutím na **Continue** certifikát exportujte.
6. Kliknutím na **OK** zatvorte Potvrdzovaciu stránku exportu. Teraz môžete exportovať kópiu certifikátu na podpisovanie objektov.
7. Znovu vyberte úlohu **Export certificate**.
8. Výberom **Object signing** zobrazte zoznam certifikátov na podpisovanie objektov, ktoré chcete exportovať.
9. Vyberte správny certifikát podpisujúci objekty zo zoznamu a kliknite na **Export**.
10. Ako cieľ označte **File, as a signature verification certificate** a kliknite na **Continue**.
11. Zadajte úplný názov cesty a súboru, kam chcete exportovať certifikát na kontrolu podpisov a kliknutím na **Continue** ho exportujte.

Teraz môžete preniesť tieto súbory do koncových systémov, v ktorých chcete kontrolovať podpisy, ktoré ste vytvorili certifikátom.

Krok 7: Prenos súborov s certifikátom do verejného servera spoločnosti (Systém B)

Súbory s certifikátom, ktoré ste vytvorili v Systéme A, musíte preniesť do Systému B (v tomto scenári verejný webový server spoločnosti), aby ste ho mohli nakonfigurovať na kontrolu vami podpísaných objektov. 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: Vytvorenie pamäte certifikátov *SIGNATUREVERIFICATION

Ak chcete kontrolovať podpisy v Systéme B (verejný webový server spoločnosti), Systém B musí mať kópiu zodpovedajúceho certifikátu na kontrolu podpisov v pamäti certifikátov *SIGNATUREVERIFICATION. 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. Informácie nájdete v téme Spúšťanie DCM .
2. V navigačnom rámci DCM vyberte **Create New Certificate Store** 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 (**?**) na vrchu stránky a dostanete sa k online pomoci.

3. Zadajte heslo pre nový sklad certifikátov a kliknutím na **Continue** ho vytvorte. Teraz môžete do skladu importovať certifikáty a použiť ich na overovanie podpisov.

Krok 9: Úlohy kontroly podpisov: Import certifikátov

Aby ste mohli overiť elektronický podpis, musí sklad *SIGNATUREVERIFICATION obsahovať certifikát na kontrolu 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 vyexportované do súboru a tento súbor bol prenesený do každého koncového systému.

Ak chcete naimportovať tieto certifikáty do pamäte certifikátov *SIGNATUREVERIFICATION, vykonajte tieto kroky: Teraz môžete používať DCM v Systéme B na kontrolu podpisov objektov, ktoré ste vytvorili zodpovedajúcim podpisujúcim certifikátom v Systéme A.

1. V navigačnom rámci DCM kliknite na **Select a Certificate Store** a označte ***SIGNATUREVERIFICATION** ako sklad certifikátov, ktorý chcete otvoriť.
2. Po zobrazení stránky Certificate Store and Password zadajte heslo, ktoré ste zadali pre pamäť certifikátov pri jej vytvorení a kliknite na **Continue**.
3. Po obnovení navigačného rámca vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
4. Zo zoznamu úloh vyberte **Import certificate**.
5. Ako typ certifikátu vyberte **Certificate Authority (CA)** a kliknite na **Continue**.

   Poznámka: Certifikát lokálnej CA musíte importovať skôr, než súkromný certifikát na kontrolu podpisov; inak proces importu certifikátu na overovanie podpisov zlyhá.
6. Zadajte plný názov cesty a súboru certifikátu CA a kliknite na **Continue**. Zobrazí sa správa, ktorá buď potvrdzuje, že bol proces importu úspešný, alebo poskytuje chybovú informáciu, ak proces zlyhal.
7. Znovu vyberte úlohu **Import certificate**.
8. Ako typ importovaného certifikátu označte **Signature verification** a kliknite na **Continue**.
9. Zadajte plný názov cesty a súboru certifikátu na overovanie podpisov a kliknite na **Continue**. Zobrazí sa správa, ktorá buď potvrdzuje, že bol proces importu úspešný, alebo poskytuje chybovú informáciu, ak proces zlyhal.

Krok 10: Úlohy kontroly podpisov: Kontrola podpisu programových objektov

Ak chcete overovať podpisy na presunutých objektoch programov s použitím DCM, dodržte tento postup:

1. V navigačnej časti kliknite na **Select a Certificate Store** a ako pamäť certifikátov na otvorenie vyberte ***SIGNATUREVERIFICATION**.
2. Zadajte heslo pre sklad certifikátov *SIGNATUREVERIFICATION a kliknite na **Continue**.
3. Keď sa obnoví obsah navigačného rámca, označte **Manage Signable Objects** a zobrazte zoznam úloh.
4. V zozname úloh vyberte **Verify object signature** 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 **Continue**. Môžete tiež zadať umiestnenie adresára a kliknúť na **Browse**, 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 zástupnú znaky. Týmito zástupnými znakmi sú hviezdička (*****), ktorá zastupuje *ľubovoľný počet znakov*, a otáznik (**?**), ktorý zastupuje *ľubovoľný 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 Browse na zobrazenie obsahu knižnice alebo adresára, musíte pred kliknutím na tlačidlo **Browse** zadať zástupný znak ako časť názvu cesty.

6. Určite svoju voľbu procesu, ktorým chcete vybraný objekt, alebo objekty overovať a kliknite na **Continue**.

   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 field (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 **Continue**. Alebo zadajte umiestnenie adresára a kliknite na **Browse**, 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: Podpisovanie objektov a overovanie podpisov objektov pomocou rozhraní API

Tento scenár popisuje vývojársku spoločnosť, ktorá chce programovo podpisovať aplikácie, ktoré predáva. Chcú svojich zákazníkov uistiť, že aplikácie prichádzajú naozaj od ich spoločnosti a poskytnúť im spôsob, ako počas ich inštalácie rozpoznať neautorizované zmeny. Vychádzajúc z týchto podnikateľských potrieb a bezpečnostných cieľov, tento scenár popisuje používanie rozhrania API na podpisovanie objektov systému i5/OS a rozhrania API na pridávanie overovateľov systému i5/OS na podpisovanie objektov a overovanie podpisov.

Situácia

Vaša spoločnosť (MyCo, s.r.o.) je obchodný partner, 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 produkt z dôveryhodného zdroja, ale zistia, že to nebol skutočný 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.

Hoci tieto typy problémov nie sú bežné pre zákazníkov, chcete uistiť zákazníkov, že aplikácie, ktoré od vás získali, sú skutočne od 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 vášho prieskumu ste sa rozhodli, že na dosiahnutie bezpečnostných cieľov použijete podpisovanie objektov i5/OS. Elektronické podpisovanie vašich aplikácií dáva vašim zákazníkom možnosť, 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 klientských 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. Následne, chcete použiť systémové rozhrania API na podpísanie vašich aplikácií a nastaviť systém zákazníka na programovú kontrolu podpisu počas inštalácie produktu.

Ciele tohto scenáru 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.
- Spoločnosť musí byť schopná používať systémové rozhrania API na programové pridanie vyžadovaného certifikátu na kontrolu podpisov do pamäte certifikátov *SIGNATUREVERIFICATION v systéme zákazníka. Spoločnosť musí byť schopná programovo vytvoriť túto pamäť certifikátov v systéme zákazníka ako súčasť procesu inštalácie produktu, ak ešte neexistuje.
- 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 aplikácii od jej podpisu vykonané nejaké zmeny.

Detaily

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

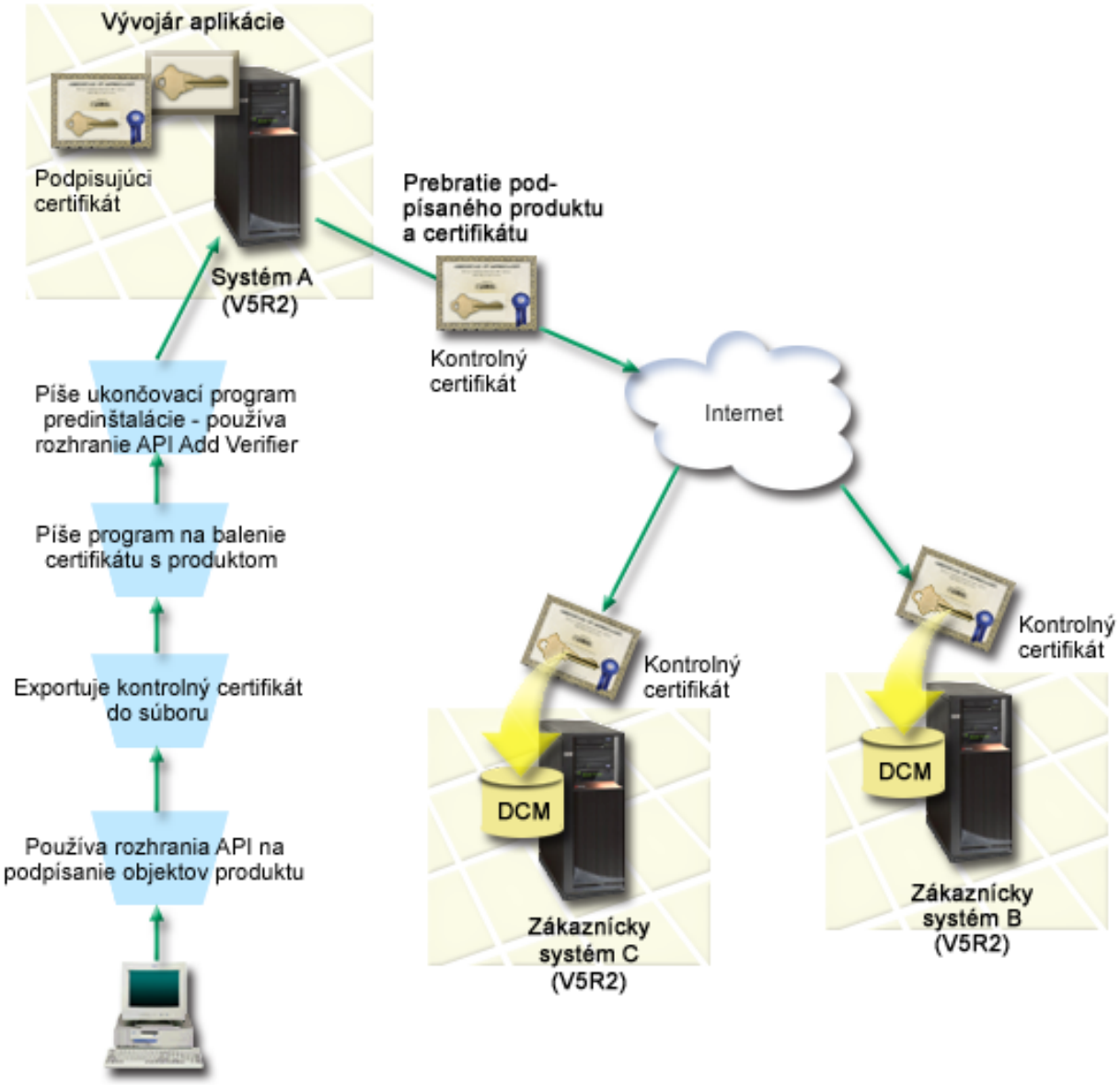

Diagram zobrazuje nasledujúce body súvisiace so scenárom:

Centrálny systém A

- Systém A je model System i s operačným systémom OS/400, verzia 5, vydanie 2 (V5R2).
- Systém A používa program na balenie produktov od vývojára aplikácií.
- Systém A obsahuje 128-bitového šifrovacieho poskytovateľa prístupu pre System i (5722–AC3).
- Na systéme A je nainštalovaná aplikácia Digital Certificate Manager (voľba 34) a IBM HTTP Server (5722–DG1).
- Systém A je primárny systém na podpisovanie objektov pre aplikačné produkty spoločnosti. Podpísanie objektov produktu pre distribúciu zákazníkovi sa vykoná v Systéme 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. Napísať program na pridávanie overovacieho certifikátu do podpísanej aplikácie.
4. Napísať program ukončenia predinštalácie produktu, ktorý využíva API vkladajúce overovač. Toto API dovoľuje procesu inštalácie produktu programovo pridať certifikát na kontrolu do pamäte certifikátov *SIGNATUREVERIFICATION v systéme zákazníka (Systémy B a C).

Systémy zákazníka B a C

- Systém B je model System i s operačným systémom OS/400, verzia 5, vydanie 2 (V5R2), alebo novšie vydanie operačného systému i5/OS.
- Systém C je model System i s operačným systémom OS/400, verzia 5, vydanie 2 (V5R2), alebo novšie vydanie operačného systému i5/OS.
- Systémy B a C majú nainštalované a nakonfigurované produkty Správca digitálnych certifikátov (voľba 34) a IBM HTTP Server (5722–DG1).
- Systémy B a C zakúpia a prevezmú aplikáciu z webovej lokality spoločnosti na vývoj aplikácií (ktorá vlastní Systém A).
- Systémy B a C získajú kópiu certifikátu na kontrolu podpisov spoločnosti MyCo, keď proces inštalácie aplikácie od MyCo vytvorí pamäť certifikátov *SIGNATUREVERIFICATION v každom z týchto systémov zákazníka.

Požiadavky a predpoklady

Tento scenár je závislý na nasledujúcich požiadavkách a predpokladoch:

1. Všetky systémy musia spĺňať požiadavky na inštaláciu a používanie Správcu digitálnych certifikátov (DCM).

   Poznámka: Splnenie požiadaviek pre inštaláciu a používanie DCM je voliteľnou požiadavkou pre zákazníkov (Systémy B a C v tomto scenári). 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. V žiadnom z týchto systémov nebolo v minulosti nakonfigurované ani používané DCM.
3. Všetky systémy majú nainštalovanú najvyššiu úroveň licenčného programu Cryptographic Access Provider 128-bit (5722-AC3).
4. Predvolené nastavenie pre systémovú hodnotu kontroly podpisov objektov počas obnovy (QVFYOBJRST) vo všetkých systémoch v scenári je 3 a toto nastavenie sa nemôže zmeniť. Predvolené nastavenie zabezpečuje, že systém môže overovať podpisy objektov počas obnovovania podpísaných objektov.
5. Administrátor siete pre Systém A musí mať špeciálne oprávnenie *ALLOBJ pre užívateľský profil na podpisovanie objektov, alebo užívateľský profil musí byť autorizovaný na aplikáciu podpisujúcu objekty.
6. Systémový operátor, alebo ktokoľvek iný (vrátane programu), kto vytvára sklad certifikátov cez DCM, špeciálne oprávnenia užívateľského profilu *SECADM a *ALLOBJ.
7. Administrátori systému alebo ostatní vo všetkých ostatných systémoch musia mať špeciálne oprávnenie *AUDIT pre užívateľský profil na kontrolu podpisov objektov.

Kroky úlohy konfigurácie

Ak chcete podpísať objekty, ako je opísané v tomto scenári, pozrite si detaily scenára dole, kde nájdete kroky na vykonanie každej z týchto úloh v Systéme A:

1. Nainštalujte a nakonfigurujte všetky vyžadované produkty System i
2. Pomocou DCM vytvorte požiadavku o certifikát na získanie certifikátu podpisujúceho objekty od verejnej, dobre známej Certifikačnej autority (CA)
3. Pomocou DCM vytvorte definíciu aplikácie na podpisovanie objektov

4. Pomocou DCM naimportujte podpísaný certifikát podpisujúci objekty a priraďte ho k vašej definícii aplikácie na podpisovanie objektov
5. Pomocou DCM vyexportujte váš certifikát podpisujúci objekty ako certifikát na kontrolu podpisov, aby ho mohli vaši zákazníci používať na kontrolu podpisov objektov vašej aplikácie
6. Zaktualizujte program na balenie aplikácie, aby použil API Sign Object na podpísanie vašej aplikácie
7. Vytvorte ukončovací program na spustenie pred inštaláciou, ktorý používa API Add Verifier ako súčasť procesu balenia vašej aplikácie. Tento ukončovací program vám dovoľuje vytvoriť pamäť certifikátov *SIGNATUREVERIFICATION a pridať požadovaný certifikát na kontrolu podpisov do systému zákazníka počas inštalácie produktu.
8. Oznámte zákazníkom, aby pomocou DCM nastavili predvolené heslo pre pamäť certifikátov *SIGNATUREVERIFICATION v ich systéme

Súvisiace informácie

Správca digitálnych certifikátov (DCM)

Podrobnosti scenára: Podpisovanie objektov a overovanie podpisov objektov pomocou rozhraní API

Vykonaním nasledujúcich krokov budete môcť použiť rozhrania API i5/OS na podpisovanie objektov, ako opisuje tento scenár.

Krok 1: Vykonajte všetky vyžadované kroky

Predtým, ako môžete vykonať špecifické konfiguračné úlohy na implementáciu tohto scenára, musíte dokončiť všetky vyžadované úlohy na inštaláciu a konfiguráciu všetkých vyžadovaných produktov System i.

Krok 2: Pomocou DCM získajte certifikát od verejnej, dobre známej CA

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. Informácie nájdete v téme Spúšťanie DCM .
2. Výberom **Create New Certificate Store** 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 (**?**) na vrchu stránky a dostanete sa k online pomoci.
3. Vyberte ***OBJECTSIGNING** ako pamäť certifikátov na vytvorenie a kliknite na **Continue**.
4. Výberom **Yes** vytvorte certifikát ako súčasť vytvorenia skladu certifikátov *OBJECTSIGNING a kliknite na **Continue**.
5. Ako podpisovateľa nového certifikátu označte **VeriSign or other Internet Certificate Authority (CA)** a kliknutím na **Continue** zobrazte formulár, ktorý vám umožní vytvoriť identifikačné údaje nového certifikátu.
6. Vyplňte formulár a kliknutím na **Continue** 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 navigačnej časti kliknite na **Select a Certificate Store** a ako pamäť certifikátov na otvorenie vyberte ***OBJECTSIGNING**.
2. Po zobrazení stránky Certificate Store and Password zadajte heslo, ktoré ste zadali pre pamäť certifikátov pri jej vytvorení a kliknite na **Continue**.
3. V navigačnom rámci označte **Manage Applications** a zobrazte zoznam úloh.
4. V zozname úloh označte **Add application**, čím sa vám zobrazí formulár na definovanie aplikácie.
5. Vyplňte formulár a kliknite na **Add**.

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

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

Ak chcete importovať váš certifikát a jeho priradením aplikácii povoliť podpisovanie objektov, nasledujte tento postup:

1. Spustite DCM. Informácie nájdete v téme Spúšťanie DCM .
2. V navigačnej časti kliknite na **Select a Certificate Store** a ako pamäť certifikátov na otvorenie vyberte ***OBJECTSIGNING**.
3. Po zobrazení stránky Certificate Store and Password zadajte heslo, ktoré ste zadali pre pamäť certifikátov pri jej vytvorení a kliknite na **Continue**.
4. Po obnovení navigačného rámca vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
5. Výberom **Import certificate** 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 (**?**) na vrchu stránky a dostanete sa k online pomoci.
6. Zo zoznamu úloh **Manage Certificates** vyberte **Assign certificate** a zobrazte zoznam certifikátov v aktuálnom sklade certifikátov.
7. V zozname označte správny certifikát a kliknutím na **Assign to Applications** zobrazte zoznam definícií aplikácií v aktuálnom sklade certifikátov.
8. Označte v zozname svoju aplikáciu a kliknite na **Continue**. Zobrazí sa stránka s potvrdením úspešného priradenia, alebo s chybovou správou, ak sa vyskytol nejaký problém.

Po dokončení tejto úlohy ste pripravený podpisovať aplikácie a ostatné objekty pomocou rozhraní API i5/OS. Na zaistenie, že vy aj ostatní budú môcť kontrolovať podpisy, musíte vyexportovať potrebné certifikáty do súboru a preniesť ich do každého systému, kam ste nainštalovali vaše podpísané aplikácie. Zákaznícke systémy potom musia dokázať používať certifikát na kontrolu podpisu vašich aplikácií pri ich inštalácii. Ako súčasť procesu inštalácie môžete na nevyhnutné nakonfigurovanie overovania podpisov u vašich zákazníkov použiť API vkladajúce overovač. Napríklad

môžete vytvoriť ukončovací program na spustenie pred inštaláciou, ktorý zavolá API Add Verifier na nakonfigurovanie systému vášho zákazníka.

Krok 5: Vyexportujte certifikáty, aby ste povolili kontrolu podpisov v iných systémoch

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 použiť DCM, aby ste mohli skontrolovať podpisy v rovnakom systéme, ktorý podpisuje tieto objekty (Systém A v tomto scenári), vykonajte tieto kroky:

1. V navigačnom rámci vyberte **Create New Certificate Store** a označte ***SIGNATUREVERIFICATION** ako sklad certifikátov, ktorý chcete vytvoriť.
2. Kliknutím na **Yes** prekopírujete existujúce certifikáty na podpisovanie objektov do nového skladu certifikátov ako certifikáty na kontrolu podpisov.
3. Zadajte heslo pre nový sklad certifikátov a kliknutím na **Continue** ho vytvorte. Odteraz môžete s použitím DCM overovať podpísané objekty na systéme, ktorý používate na aj 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 **Manage Certificates** a potom označte úlohu **Export certificate**.
2. Výberom **Object signing** zobrazte zoznam certifikátov na podpisovanie objektov, ktoré chcete exportovať.
3. Vyberte správny certifikát podpisujúci objekty zo zoznamu a kliknite na **Export**.
4. Ako cieľ označte **File, as a signature verification certificate** a kliknite na **Continue**.
5. Zadajte úplný názov cesty a súboru, kam chcete exportovať certifikát na kontrolu podpisov a kliknutím na **Continue** 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 skontrolovať podpis na objektoch vašej aplikácie pri ich obnove v systémoch zákazníka.

Krok 6: Zaktualizujte program na balenie aplikácie, aby použil systémové rozhrania API na podpísanie vašej aplikácie

Teraz, keď už máte súbor certifikátu na kontrolu 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 firma IBM odporúča, aby ste si radšej prispôsobili tento príklad, než použili predvolené hodnoty v ňom uvedené .

Poznámka: Použitím týchto príkladov kódu súhlasíte s podmienkami v časti “Licencia na kód a zrieknutie sa zodpovednosti” na strane 43.

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.

```
/* ------------------------------------------------------------- */
/*                                                               */
/* COPYRIGHT (C) IBM CORP. 2004, 2007                            */
/*                                                               */
/* 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 na spustenie pred inštaláciou, ktorý použije 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. Toto dovoľuje vášmu inštalačnému programu skontrolovať podpis objektov vašej aplikácie pri ich obnove v systéme zákazníka.

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 predvolené hodnoty v ňom uvedené .

Poznámka: Použitím tohto príkladu kódu súhlasíte s podmienkami, uvedenými v časti “Licencia na kód a zrieknutie sa zodpovednosti” na strane 43.

Nasledujúci kód zmeňte tak, aby vyhovoval vašim potrebám použitia API Add Verifier ako súčasti ukončovacieho programu na spustenie pred inštaláciou na pridanie vyžadovaného certifikátu na kontrolu podpisov do systému zákazníka, keď inštaluje váš produkt.

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2004, 2007                               */
/*                                                                  */
/* 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 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: Prestavte predvolené heslo pre pamäť certifikátov *SIGNATUREVERIFICATION

API Add Verifier mohlo vytvoriť pamäť certifikátov *SIGNATUREVERIFICATION ako súčasť procesu inštalácie produktu v systéme zákazníka. 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. Informácie nájdete v téme Spúšťanie DCM .
2. V navigačnej časti kliknite na **Select a Certificate Store** a ako pamäť certifikátov na otvorenie vyberte ***SIGNATUREVERIFICATION**.
3. Keď sa zobrazí stránka Sklad certifikátov a heslo, kliknutím na **Reset Password** zobrazte stránku Reset Certificate Store Password.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) na vrchu 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 **Continue**.

Scenár: Podpisovanie objektov pomocou riadiaceho centra System i Navigator

V tomto scenári je opísaná spoločnosť, ktorá chce na podpisovanie objektov, ktoré odosiela na niekoľko systémov, použiť funkcie systému i5/OS. Vychádzajúc z týchto podnikateľských potrieb a bezpečnostných cieľov, tento scenár popisuje používanie riadiaceho centra System i Navigator na balenie a podpisovanie objektov, ktoré distribuujú na iné systémy.

Situácia

Vaša spoločnosť (MyCo, s.r.o.) vyvíja aplikácie, ktoré distribuuje do viacerých systémov na viacerých miestach v spoločnosti. Ako správca siete ste zodpovedný za to, aby všetky tieto aplikácie boli nainštalované a aktualizované na všetkých podnikových systémoch. V súčasnosti na čo najjednoduchšie balenie a distribúciu týchto funkcií a vykonanie iných administračných úloh používate riadiace centrum systému System i Navigator. 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.

Oboznámili ste sa s funkciami na podpisovanie objektov v systéme i5/OS a zistili ste, že počnúc vydaním V5R2, riadiace centrum vám umožňuje podpisovať objekty pri balení a distribúcii. S použitím riadiaceho centra 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 ku krokom, ktoré sú zahrnuté v konfigurovaní a používaní podpisovania objektov pre aplikácie, ktoré distribuujete do viacerých systémov spoločnosti.

Výhody scenára

Tento scenár poskytuje nasledujúce výhody:

- Používanie riadiaceho centra na balenie a podpisovanie objektov znižuje čas potrebný na distribúciu podpísaných objektov na vaše podnikové systémy.
- Používanie riadiaceho centra 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 spoločnosť MyCo, Inc. digitálne podpisovať aplikácie, ktoré distribuuje do viacerých systémov v spoločnosti. Ako administrátor siete spoločnosti MyCo, Inc. už používate riadiace centrum na množstvo administratívnych úloh. Chcete rozšíriť vaše aktuálne používanie riadiaceho centra na podpisovanie aplikácií spoločnosti, ktoré distribuujete do iných systémov.

Ciele tohto scenáru sú nasledovné:

- Firemné aplikácie musia byť podpísané certifikátom vydaným Lokálnou CA, aby sa znížili náklady na podpisovanie aplikácií.
- Administrátori systémov a iní určení užívatelia musia byť schopní jednoducho overiť elektronické podpisy na všetkých systémoch, aby mohli overiť zdroj a pravosť podpísaných objektov spoločnosti. Na to musí byť v sklade certifikátov *SIGNATUREVERIFICATION všetkých systémov uložený certifikát na overovanie podpisov spoločnosti, ako aj certifikát lokálnej certifikačnej autority.

- Kontrola podpisov na aplikáciách spoločnosti dovoľuje administrátorom a ostatným zisťovať, či bol obsah objektov zmenený od ich podpísania.
- Administrátori musia byť schopní používať riadiace centrum na balenie, podpisovanie a následnú distribúciu ich aplikácií do ich systémov.

Detaily

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

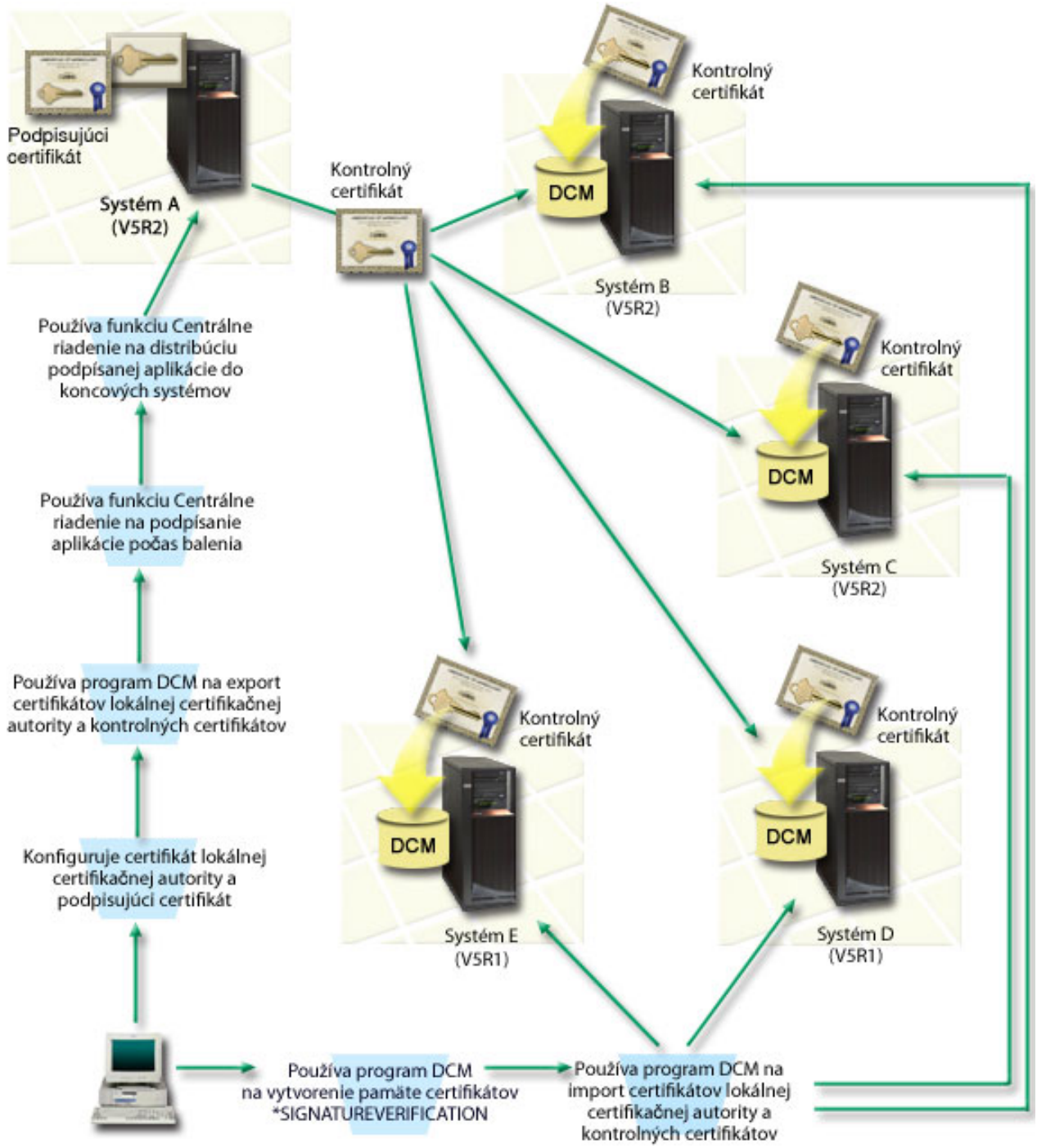

Diagram zobrazuje nasledujúce body súvisiace so scenárom:

Centrálny systém (Systém A)

- Systém A je model System i s operačným systémom OS/400, verzia 5, vydanie 2 (V5R2).
- Systém A slúži ako centrálny systém, z ktorého sa vykonávajú funkcie riadiaceho centra, vrátane balenia a distribúcie aplikácií spoločnosti.
- Systém A obsahuje 128-bitového šifrovacieho poskytovateľa prístupu pre System i (5722–AC3).
- Na systéme A je nainštalovaná aplikácia Digital Certificate Manager (voľba 34) a IBM HTTP Server (5722–DG1).
- Systém A vystupuje ako lokálna certifikačná autorita (CA) a certifikát podpisujúci objekty sa nachádza v tomto systéme.
- Systém A je primárny systém na podpisovanie objektov pre aplikácie spoločnosti. Podpísanie objektov produktu pre distribúciu zákazníkovi sa vykoná v Systéme A vykonaním týchto úloh:
  1. Pomocou DCM vytvorte Lokálne CA a ňou vytvorte certifikát na podpisovanie objektov.
  2. Pomocou DCM vyexportujte kópiu certifikátu lokálnej LA a certifikát na kontrolu podpisov do súboru, aby mohli koncové systémy (Systémy B, C, D a E) kontrolovať podpísané objekty.
  3. Pomocou riadiaceho centra podpíšte objekty aplikácie a zabaľte ich so súbormi overovacieho certifikátu.
  4. Pomocou riadiaceho centra distribuujte podpísané aplikácie a certifikačné súbory na koncové systémy.

Koncové systémy (Systémy B, C, D a E)

- Systémy B a C sú modely System i s operačným systémom OS/400, verzia 5, vydanie 2 (V5R2).
- Systémy D a E sú modely System i s operačným systémom OS/400, verzia 5, vydanie 1 (V5R1).
- Systémy B, C, D a E majú nainštalované a nakonfigurované produkty Správca digitálnych certifikátov (voľba 34) a IBM HTTP Server (5722–DG1).
- Systémy B, C, D a E dostanú kópiu certifikátu na kontrolu podpisov spoločnosti a certifikátu lokálnej CA z centrálneho systému (Systém A), keď systémy prijmú 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 systémy musia spĺňať požiadavky na inštaláciu a používanie Správcu digitálnych certifikátov (DCM).
2. V žiadnom z týchto systémov nebolo v minulosti nakonfigurované ani používané DCM.
3. Systém A vyhovuje požiadavkám na inštaláciu a používanie System i Navigator a riadiaceho centra.
4. Server riadiaceho centra musí byť spustený vo všetkých koncových systémoch.
5. Všetky systémy majú nainštalovanú najvyššiu úroveň licenčného programu Cryptographic Access Provider 128-bit (5722-AC3).
6. Predvolené nastavenie pre systémovú hodnotu kontroly podpisov objektov počas obnovy (QVFYOBJRST) vo všetkých systémoch v scenári je 3 a toto nastavenie sa nemôže zmeniť. Predvolené nastavenie zabezpečuje, že systém môže overovať podpisy objektov počas obnovovania podpísaných objektov.
7. Administrátor siete pre Systém A musí mať špeciálne oprávnenie *ALLOBJ pre užívateľský profil na podpisovanie objektov, alebo užívateľský profil musí byť autorizovaný na aplikáciu podpisujúcu objekty.
8. Sieťový operátor, alebo ktokoľvek iný, kto vytvára sklad certifikátov cez DCM, musí mať špeciálne oprávnenia užívateľského profilu *SECADM a *ALLOBJ.
9. Administrátori systému alebo ostatní vo všetkých ostatných systémoch musia mať špeciálne oprávnenie *AUDIT pre užívateľský profil na kontrolu podpisov objektov.

Kroky úlohy konfigurácie

Sú dve množiny úloh, ktoré musíte vykonať pri implementácii tohto scenára: Prvá množina úloh vám dovolí nastaviť Systém A na používanie riadiaceho centra na podpisovanie a distribuovanie aplikácií. Druhá množina úloh umožňuje

administrátorom systémov a iným užívateľom overovať podpisy týchto aplikácií na všetkých iných systémoch. Pozrite si detaily scenára dole, kde nájdete kroky na vykonanie týchto úloh.

Zoznam úloh pre podpisovanie objektov

Ak chcete podpísať objekty, ako je opísané v tomto scenári, pozrite si detaily scenára dole, kde nájdete kroky na vykonanie každej z týchto úloh v Systéme A:

1. Nainštalujte a nakonfigurujte všetky vyžadované produkty System i
2. Pomocou DCM vytvorte lokálnu Certifikačnú autoritu (CA) na vydanie súkromného certifikátu podpisujúceho objekty
3. Pomocou DCM vytvorte definíciu aplikácie.
4. Pomocou DCM priraďte certifikát k definícii aplikácií na podpisovanie objektov
5. Pomocou DCM vyexportujte certifikáty, ktoré musia používať ostatné systémy na kontrolu podpisov objektov. Do súboru musíte vyexportovať kópiu certifikátu lokálnej CA aj kópiu certifikátu podpisujúceho objekty ako certifikát na kontrolu podpisov.
6. Preneste súbory s certifikátmi do každého koncového systému, v ktorom chcete kontrolovať podpisy.
7. Pomocou riadiaceho centra System i Navigator podpíšte všetky objekty aplikácií

Zoznam úloh pre overovanie podpisov

Nasledujúce úlohy konfigurácie kontroly podpisov musíte vykonať v každom koncovom systéme, aby ste mohli použiť riadiace centrum na presun podpísaných objektov aplikácií do týchto systémov. Skôr než budete môcť počas obnovy podpísaných objektov na koncovom systéme úspešne overovať podpisy, musí byť ukončená konfigurácia overovania podpisov.

V každom koncovom systéme musíte vykonať nasledujúce kroky, aby ste mohli kontrolovať podpisy objektov, ako opisuje tento scenár:

1. Pomocou DCM vytvorte pamäť certifikátov *SIGNATUREVERIFICATION
2. Pomocou DCM naimportujte certifikát lokálnej CA a certifikát na kontrolu podpisov

   Súvisiace informácie

   Správca digitálnych certifikátov (DCM)

Podrobnosti scenára: Používanie riadiaceho centra System i Navigator na podpisovanie objektov

Vykonajte nasledujúce úlohy, aby ste nakonfigurovali riadiace centrum na podpisovanie objektov i5/OS.

Krok 1: Vykonajte všetky vyžadované kroky

Predtým, ako môžete vykonať špecifické konfiguračné úlohy na implementáciu tohto scenára, musíte dokončiť všetky vyžadované úlohy na inštaláciu a konfiguráciu všetkých vyžadovaných produktov System i.

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 kontrolu 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.

Ak chcete použiť DCM na vytvorenie a prevádzkovanie lokálnej CA, vykonajte tieto kroky: Keď ste už vytvorili lokálnu CA a certifikát podpisujúci objekty, musíte definovať aplikáciu na podpisovanie objektov, ktorá bude používať tento certifikát, až potom môžete podpisovať objekty.

1. Spustite DCM. Informácie nájdete v téme Spúšťanie DCM .
2. V navigačnom rámci DCM vyberte **Create a Certificate Authority (CA)**, čím zobrazíte sériu formulárov.

   Poznámka: Ak si nie ste istý, ako vyplniť konkrétny formulár v tejto riadenej úlohe, kliknite na tlačidlo označené otáznikom (**?**) na vrchu 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 Lokálnej CA.
   d. Použite novú Lokálnu CA a vydajte serverový, alebo klientský 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 klientský, alebo serverový certifikát pre pripojenia SSL.

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

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 navigačnej časti kliknite na **Select a Certificate Store** a ako pamäť certifikátov na otvorenie vyberte ***OBJECTSIGNING**.
2. Po zobrazení stránky Certificate Store and Password zadajte heslo, ktoré ste zadali pre pamäť certifikátov pri jej vytvorení a kliknite na **Continue**.
3. V navigačnom rámci označte **Manage Applications** a zobrazte zoznam úloh.
4. V zozname úloh označte **Add application**, čím sa vám zobrazí formulár na definovanie aplikácie.
5. Vyplňte formulár a kliknite na **Add**.

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

Krok 4: Priradenie certifikátu k definícii aplikácie na podpisovanie objektov

Nasledovaním týchto krokov priradíte certifikát vašej aplikácii podpisujúcej objekty:

1. V navigačnom rámci DCM označte **Manage Certificates** a zobrazte zoznam úloh.
2. Zo zoznamu úloh vyberte **Assign certificate**, čím zobrazíte zoznam certifikátov v aktuálnom sklade certifikátov.

3. V zozname označte správny certifikát a kliknutím na **Assign to Applications** zobrazte zoznam definícií aplikácií v aktuálnom sklade certifikátov.
4. Označte v zozname jednu, alebo viac aplikácií a kliknite na **Continue**. 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 riadiaceho centra. Na zaistenie, že vy aj ostatní budú môcť kontrolovať podpisy, musíte vyexportovať potrebné certifikáty do súboru a preniesť ich do každého koncového systému. V každom koncovom systéme musíte vykonať všetky úlohy konfigurácie kontroly podpisov, aby ste mohli použiť riadiace centrum na presun podpísaných objektov aplikácií do týchto systémov. Skôr než budete môcť počas obnovy podpísaných objektov na koncovom systéme úspešne overovať podpisy, musí byť ukončená konfigurácia overovania podpisov.

Krok 5: Vyexportujte certifikáty, aby ste povolili kontrolu podpisov v iných systémoch

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 použiť DCM, aby ste mohli skontrolovať podpisy v rovnakom systéme, ktorý podpisuje tieto objekty (Systém A v tomto scenári), vykonajte tieto kroky:

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

Ak chcete pomocou DCM exportovať kópiu certifikátu Lokálnej CA a kópiu certifikátu na podpisovanie objektov ako certifikát na kontrolu podpisov, aby ste mohli overovať podpisy objektov na iných systémoch, vykonajte tieto kroky:

1. V navigačnom rámci vyberte **Manage Certificates** a potom označte úlohu **Export certificate**.
2. Vyberte **Certificate Authority (CA)** a kliknutím na **Continue** 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 vyberte **File** a kliknite na **Continue**.
5. Pre exportovaný certifikát Lokálnej CA zadajte úplný názov cesty a súboru a kliknutím na **Continue** certifikát exportujte.
6. Kliknutím na **OK** zatvorte Potvrdzovaciu stránku exportu. Teraz môžete exportovať kópiu certifikátu na podpisovanie objektov.
7. Znovu vyberte úlohu **Export certificate**.
8. Výberom **Object signing** zobrazte zoznam certifikátov na podpisovanie objektov, ktoré chcete exportovať.
9. Vyberte správny certifikát podpisujúci objekty zo zoznamu a kliknite na **Export**.
10. Ako cieľ označte **File, as a signature verification certificate** a kliknite na **Continue**.
11. Zadajte úplný názov cesty a súboru, kam chcete exportovať certifikát na kontrolu podpisov a kliknutím na **Continue** ho exportujte.

Teraz môžete preniesť tieto súbory do koncových systémov, v ktorých chcete kontrolovať podpisy, ktoré ste vytvorili certifikátom.

Krok 6: Presun súborov s certifikátom do koncových systémov

Súbory s certifikátom, ktoré ste vytvorili v Systéme A, musíte preniesť do koncových systémov v tomto scenári, aby ste ich mohli nakonfigurovať na kontrolu objektov, 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 7: Podpísanie objektov cez riadiace centrum

Proces podpisovania objektov riadiaceho centra je súčasťou procesu balenia a distribúcie softvéru. V každom koncovom systéme musíte vykonať všetky úlohy konfigurácie kontroly podpisov, aby ste mohli použiť riadiace centrum na prenos podpísaných objektov aplikácie do týchto systémov. Skôr než budete môcť počas obnovy podpísaných objektov na koncovom systéme úspešne overovať podpisy, musí byť ukončená konfigurácia overovania podpisov.

Ak chcete podpísať aplikáciu, ktorú distribuujete do koncových systémov ako opisuje tento scenár, vykonajte tieto kroky:

1. Na balenie a distribúciu softvérových produktov použite riadiace centrum.
2. Keď sa dostanete k panelu **Identification** v sprievodcovi **Product Definition**, kliknutím na **Advanced** zobrazte panel **Advanced Identification**.
3. Do poľa **Digital signing** zadajte 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 riadiaceho centra.

Krok 8: Úlohy kontroly podpisov: Vytvorenie pamäte certifikátov *SIGNATUREVERIFICATION v koncových systémoch

Ak chcete skontrolovať podpisy objektov v koncových systémoch v tomto scenári, každý systém musí mať kópiu zodpovedajúceho certifikátu na kontrolu podpisov v pamäti certifikátov *SIGNATUREVERIFICATION. Ak boli objekty podpísané súkromným certifikátom, musí tento certifikát na kontrolu podpisov obsahovať aj kópiu certifikátu Lokálnej CA.

Sklad certifikátov *SIGNATUREVERIFICATION vytvoríte nasledovným postupom:

1. Spustite DCM. Informácie nájdete v téme Spúšťanie DCM .
2. V navigačnom rámci DCM vyberte **Create New Certificate Store** 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 (**?**) na vrchu stránky a dostanete sa k online pomoci.
3. Zadajte heslo pre nový sklad certifikátov a kliknutím na **Continue** ho vytvorte. Teraz môžete do skladu importovať certifikáty a použiť ich na overovanie podpisov.

Krok 9: Úlohy kontroly podpisov: Import certifikátov

Aby ste mohli overiť elektronický podpis, musí sklad *SIGNATUREVERIFICATION obsahovať certifikát na kontrolu 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 vyexportované do súboru a tento súbor bol prenesený do každého koncového systému.

Ak chcete naimportovať tieto certifikáty do pamäte certifikátov *SIGNATUREVERIFICATION, vykonajte tieto kroky: Váš systém teraz môže kontrolovať podpisy objektov, ktoré boli vytvorené zodpovedajúcim podpisujúcim certifikátom pri obnove podpísaných objektov.

1. V navigačnom rámci DCM kliknite na **Select a Certificate Store** a označte ***SIGNATUREVERIFICATION** ako sklad certifikátov, ktorý chcete otvoriť.

2. Po zobrazení stránky Certificate Store and Password zadajte heslo, ktoré ste zadali pre pamäť certifikátov pri jej vytvorení a kliknite na **Continue**.
3. Po obnovení navigačného rámca vyberte **Manage Certificates**, aby sa zobrazil zoznam úloh.
4. Zo zoznamu úloh vyberte **Import certificate**.
5. Ako typ certifikátu vyberte **Certificate Authority (CA)** a kliknite na **Continue**.

   Poznámka: Certifikát Lokálnej CA musíte importovať skôr, než súkromný certifikát na kontrolu podpisov; inak proces importu certifikátu na overovanie podpisov zlyhá.
6. Zadajte plný názov cesty a súboru certifikátu CA a kliknite na **Continue**. Zobrazí sa správa, ktorá buď potvrdzuje, že bol proces importu úspešný, alebo poskytuje chybovú informáciu, ak proces zlyhal.
7. Znovu vyberte úlohu **Import certificate**.
8. Ako typ importovaného certifikátu vyberte **Signature verification** a kliknite na **Continue**.
9. Zadajte plný názov cesty a súboru certifikátu na overovanie podpisov a kliknite na **Continue**. Zobrazí sa správa, ktorá buď potvrdzuje, že bol proces importu úspešný, alebo poskytuje chybovú informáciu, ak proces zlyhal.

Požiadavky na podpisovanie objektov a kontrolu podpisov

V tejto téme nájdete informácie o konfiguračných požiadavkách, ako aj iných problémoch plánovania pre podpisovanie objektov a overovanie podpisov na systéme s i5/OS.

Funkcie na podpisovanie objektov a overovanie podpisov v systéme i5/OS vám prinášajú ďalší silný nástroj na riadenie objektov vo vašom systéme. 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.
- Na podpisovanie objektov pri ich balení za účelom distribúcie do koncových systémov môžete používať riadiace centrum z iSeries Navigator.

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 intenetovej 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, ktorý podpisuje objekty, musí mať špeciálne oprávnenie *ALLOBJ. Užívateľský profil, ktorý vytvorí pamäť certifikátov *SIGNATUREVERIFICATION, musí mať špeciálne oprávnenia *SECADM a *ALLOBJ.

Požiadavky na kontrolu podpisov

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 napísanim 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 certifikačnou autoritou, musíte exportovať súbor certifikátu lokálnej certifikačnej autority na hostiteľskom systéme lokálnej certifikačnej autority pomocou DCM. Potom môžete pomocou DCM importovať tento súbor certifikátu na cieľovom overovacom systéme do skladiska 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..
- Systémový užívateľský profil, ktorý kontroluje podpisy, musí mať špeciálne oprávnenie *AUDIT. Užívateľský profil, ktorý vytvorí pamäť certifikátov alebo zmení heslo *SIGNATUREVERIFICATION, musí mať špeciálne oprávnenia *SECADM a *ALLOBJ.

Riadenie podpísaných objektov

V tejto časti nájdete informácie o systémových príkazoch a hodnotách v systéme i5/OS, ktoré môžete použiť na prácu s podpísanými objektmi a o tom, ako podpísané objekty ovplyvňujú procesy zálohovania a obnovy.

Počnúc od V5R1, spoločnosť IBM začala podpisovať licenčné programy i5/OS a opravy PTF ako oficiálne označenie operačného systému, že pochádza od IBM, a tiež ako prostriedok na zistenie neautorizovaných zmien systémových objektov. 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

V tejto téme nájdete informácie o systémových hodnotách a príkazoch i5/OS, ktoré môžete použiť na riadenie podpísaných objektov alebo ktoré majú vplyv na 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. Neexistujú žiadne príkazy CL, ktoré sú exkluzívne navrhnuté na prácu s podpísanými objektmi v systéme. 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 QVFYOBJRST (**Verify object signatures during restore**), člen kategórie obnovy zo systémových hodnôt i5/OS, určuje, ako príkazy ovplyvňujú podpísané objekty vo vašom systéme. Táto systémová hodnota prístupná cez produkt iSeries Navigator, ovláda to, ako systém spracúva 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). Týka sa tiež objektov prúdových súborov (*STMF), ktoré majú priradené programy Java, vytvorené príkazom CRTJVAPGM (Create Java Program). Neplatí to pre úložné súbory (*SAV) ani pre súbory integrovaného súborového systému.

Príkazy CL, ktoré ovplyvňujú podpísané objekty

Existuje niekoľko príkazov CL, ktoré vám dovoľujú pracovať s podpísanými objektmi, alebo ktoré ovplyvňujú podpísané objekty vo vašom systéme. 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 zobrazenie informácií o podpise objektu

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

Príkazy pre kontrolu 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. Ak sa chcete dozvedieť viac o používaní tohto príkazu pre podpísané a podpísateľné objekty, pozrite si časť Príkazy kontrolóra kódu na zaručenie integrity podpisov.
- 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. Ak sa chcete dozvedieť viac o používaní tohto príkazu pre podpísané a podpísateľné objekty, pozrite si časť Príkazy kontrolóra kódu na zaručenie integrity podpisov.
- 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. Ak sa chcete dozvedieť viac o používaní tohto príkazu pre podpísané a podpísateľné objekty, pozrite si časť Príkazy kontrolóra kódu na zaručenie integrity podpisov.
- 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 vysporiada 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 save file len jedným zadaním príkazu. To, ako tento príkaz spracuje podpísané a nepodpísané objekty, určuje systémová hodnota Verify object signatures during restore (QVFYOBJRST).

Príkazy pre ukladanie a obnovu pamätí 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 dovoľuje uložiť kópiu licenčného interného kódu a knižnice QSYS vo formáte, ktorý je kompatibilný s inštaláciou systému. 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, ktorými môžete odstrániť alebo odpojiť podpisy od 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. Tieto príkazy použite len na tie podpísané objekty, ktoré ste vytvorili (nie na objekty, ktoré ste získali od iných, napríklad od IBM alebo iných 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.

Súvisiace koncepty

"Úvahy o ukladaní a obnovovaní podpísaných objektov"
V tejto téme nájdete informácie o tom, ako podpísané objekty ovplyvňujú vaše úlohy ukladania a obnovovania vo vašom systéme s i5/OS.

Súvisiace informácie

Vyhľadávač systémových hodnôt

Úvahy o ukladaní a obnovovaní podpísaných objektov

V tejto téme nájdete informácie o tom, ako podpísané objekty ovplyvňujú vaše úlohy ukladania a obnovovania vo vašom systéme s i5/OS.

Existuje niekoľko systémových hodnôt, ktoré ovplyvňujú operácie obnovy pre váš systém. Len jediná z týchto systémových hodnôt, systémová hodnota **QVFYOBJRST (verify object signatures during restore)**, určuje, ako systém spracúva podpísané objekty pri ich obnove. Nastavenia, ktoré si vyberiete pre túto systémovú hodnotu, určujú, ako proces obnovy spracúva 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 spracúva 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 kontrolu 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. Tieto príkazy použite len na tie podpísané objekty, ktoré ste vytvorili (nie na objekty, ktoré ste získali od iných, napríklad od IBM alebo iných 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).

Súvisiace koncepty

“Systémové hodnoty a príkazy, ktoré ovplyvňujú podpísané objekty” na strane 35
V tejto téme nájdete informácie o systémových hodnotách a príkazoch i5/OS, ktoré môžete použiť na riadenie podpísaných objektov alebo ktoré majú vplyv na podpísané objekty.

Príkazy kontrolóra kódu na overenie integrity podpisu

V tejto časti nájdete informácie o príkazoch systému i5/OS na kontrolu podpisov objektov na overenie integrity objektov.

Na overovanie podpisov na objektoch môžete použiť Správcu digitálnych certifikátov (DCM), alebo API. Tiež môžete na kontrolu 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 kontrolu 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)

Pomocou príkazu Check Object Integrity (CHKOBJITG) môžete zistiť, či nie je integrita objektov vo vašom systéme narušená. Môžete tento príkaz využiť na kontrolu integrity poškodenia objektov, ktoré vlastnia konkrétni užívatelia, objektov, ktoré sa zhodujú so zadaným názvom cesty, alebo všetky objekty 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 spracúva elektronické podpisy na objektoch. Pre tento parameter môžete zadať niektorú z troch hodnôt:

- *SIGNED – Keď zadáte túto hodnotu, príkaz skontroluje objekty s digitálnymi podpismi. Záznam do protokolu vytvorí pre objekty, ktoré majú neplatný podpis. Toto je predvolená hodnota príkazu.
- *ALL – Keď zadáte túto hodnotu, príkaz skontroluje všetky podpísateľné objekty a určí, či majú podpis. Príkaz vytvorí záznam v protokole pre každý podpisovateľný objekt, ktorý nie je podpísaný a pre každý objekt s neplatným podpisom.
- *NONE – Keď zadáte túto hodnotu, príkaz nekontroluje digitálne podpisy objektov.

Príkaz CHKPRDOPT (Check Product Option)

Príkaz Check Product Option (CHKPRDOPT) oznamuje rozdiel medzi správnu 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 spracúva elektronické podpisy na objektoch. Pre tento parameter môžete zadať niektorú z troch hodnôt:

- *SIGNED – Keď zadáte túto hodnotu, príkaz skontroluje objekty s digitálnymi 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 – Keď zadáte túto hodnotu, príkaz skontroluje všetky podpísateľné objekty a určí, či majú podpis a skontroluje podpis týchto objektov. 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 – Keď zadáte túto hodnotu, príkaz nekontroluje digitálne podpisy objektov produktu.

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 spracúva elektronické podpisy na objektoch. Pre tento parameter môžete zadať niektorú z troch hodnôt:

- *SIGNED – Keď zadáte túto hodnotu, príkaz skontroluje objekty s digitálnymi 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 – Keď zadáte túto hodnotu, príkaz skontroluje všetky podpísateľné objekty a určí, či majú podpis a skontroluje podpis týchto objektov. 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 – Keď zadáte túto hodnotu, príkaz nekontroluje digitálne podpisy objektov produktu.

Kontrola integrity kontrolóra kódu

Dozviete sa tu, ako skontrolovať integritu kontrolóra kódu na kontrolu integrity systému i5/OS.

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

Ak chcete skontrolovať kontrolóra 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 vybraných 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.
7. Overuje podpisy všetkých modulov licenčných interných kódov (LIC) a kontroluje, či sú vrátené chyby pre nepodpísané a individuálne podpísané moduly LIC.

Súvisiace koncepty

“Funkcia kontroly integrity funkcie kontrolóra kódu” na strane 6
Táto téma poskytuje informácie o tom, ako môžete overiť integritu kontrolóra kódu, ktorý kontroluje integritu systému s operačným systémom i5/OS.

Súvisiaci odkaz

“Pochopenie chybových správ kontrolóra kódu” na strane 41
V tejto téme nájdete informácie o chybových správach, ktoré môžu byť vrátené funkciou na overenie integrity

kontrolóra kódu na vašom systéme s operačným systémom i5/OS a ako môžete tieto správy použiť, aby ste zabezpečili správnosť fungovania kontrolóra kódu, ako aj možné riešenia, ak tieto správy informujú, že táto funkcia alebo kľúčové objekty operačného systému sú porušené.

Odstraňovanie problémov s podpísanými objektmi

Táto téma poskytuje informácie o príkazoch i5/OS a systémových hodnotách, ktoré môžete použiť na prácu s podpísanými objektmi, a o tom, ako podpísané objekty ovplyvňujú proces zálohovania a obnovy.

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 problémov s podpisovaním objektov

V tejto téme nájdete informácie o odstraňovaní najbežnejších problémov, s ktorými sa môžete stretnúť počas podpisovania objektov v operačnom systéme i5/OS.

Problém	Možné riešenie
Keď na podpisovanie objektu s cieľovým vydaním V4R5 alebo nižším použijete rozhranie Sign Object API, proces podpisovania zlyhá a objekt nebude podpísaný (chybová správa CPFB721).	Systém neposkytuje podporu pre podpisovanie objektov do verzie V5R1. Ak chcete podpísať objekty, ktoré vrátili chybovú správu CPFB721, musíte programy znova vytvoriť s cieľovým vydaním V5R1, alebo novším.

Odstraňovanie problémov s overovaním podpisov

V tejto téme nájdete informácie o tom, ako môžete vyriešiť najbežnejšie problémy, ktoré sa môžu vyskytnúť počas overovania podpisov objektov v systéme i5/OS.

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.

Pochopenie chybových správ kontrolóra kódu

V tejto téme nájdete informácie o chybových správach, ktoré môžu byť vrátené funkciou na overenie integrity kontrolóra kódu na vašom systéme s operačným systémom i5/OS a ako môžete tieto správy použiť, aby ste zabezpečili správnosť fungovania kontrolóra kódu, ako aj možné riešenia, ak tieto správy informujú, že táto funkcia alebo kľúčové objekty operačného systému sú porušené.

Nasledujúca tabuľka poskytuje zoznam správ, ktoré počas spracovania generuje funkcia overovania kontrolóra 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 procesu kontrolóra 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 kontrolór kódu počas spracovania. Ak sa chcete dozvedieť viac o procese kontroly kontrolóra kódu, pozrite si časť Kontrola integrity kontrolóra kódu.

Tabuľka 1. Chybové správy kontroly kódu

Chybová správa	**Možný problém a riešenie**
CPFB729	Znamená, že proces kontroly kontrolóra 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 kontrolór 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.
CPFB72A 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 kontrolóra 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 kontroly kódu, vykonajte nasledujúce kroky z príkazového riadka i5/OS:

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 kontrolóra 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 kontrolór 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 kontrolóra kódu z načítaného inštalačného média.

Súvisiace úlohy

"Kontrola integrity kontrolóra kódu" na strane 40
Dozviete sa tu, ako skontrolovať integritu kontrolóra kódu na kontrolu integrity systému i5/OS.

Súvisiace informácie pre podpisovanie objektov a kontrolu podpisov

Informácie, súvisiace s témami o podpisovaní objektov a kontrole podpisov nájdete na webových stránkach publikácií IBM Redbooks (vo formáte PDF). Všetky tieto súbory PDF môžete zobraziť a vytlačiť.

Podpisovanie objektov a kontrola 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 byť nápomocné:

- **Webová lokalita VeriSign Help Desk** Webová lokalita VeriSign poskytuje veľkú knižnicu tém pre digitálne certifikáty, ako je podpisovanie objektov, ako aj veľké množstvo tém o bezpečnosti v sieti Internet.
- **Publikácia IBM Redbooks IBM eServer iSeries Wired Network Security: i5/OS V5R1 DCM and Cryptographic Enhancements SG24-6168** popisuje vylepšenia sieťovej bezpečnosti v systéme V5R1. Táto publikácia Redbooks obsahuje mnohé témy, ako napríklad ako používať funkcie na podpisovanie objektov a aplikáciu Digital Certificate Manager (DCM) a iné.

Licencia na kód a zrieknutie sa zodpovednosti

IBM vám zaručuje nevýlučné licencie na autorské práva na používanie všetkých príkladov kódu, z ktorých môžete generovať podobné funkcie prispôsobené vašim špecifickým požiadavkám.

VZHĽADOM NA VŠETKY ZÁKONNÉ ZÁRUKY, KTORÉ NIE JE MOŽNÉ VYLÚČIŤ, IBM, JEJ VÝVOJOVÍ PRACOVNÍCI A DODÁVATELIA, NEDÁVAJÚ ŽIADNE ZÁRUKY, ČI UŽ VYJADRENÉ ALEBO MLČKY PREDPOKLADANÉ, VRÁTANE ALE BEZ OBMEDZENIA NA MLČKY PREDPOKLADANÉ ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL OHĽADOM PROGRAMU ALEBO TECHNICKEJ PODPORY (AK NEJAKÁ EXISTUJE).

ZA ŽIADNYCH OKOLNOSTÍ NIE SÚ IBM A ANI JEJ VÝVOJOVÍ PRACOVNÍCI A DODÁVATELIA ZODPOVEDNÍ ZA ČOKOĽVEK Z NASLEDUJÚCEHO, ANI V PRÍPADE UPOZORNENIA NA MOŽNOSŤ VYSKYTU TEJTO SITUÁCIE:

1. STRATA ALEBO POŠKODENIE ÚDAJOV;
2. PRIAME, ŠPECIÁLNE, NÁHODNÉ ALEBO NEPRIAME ŠKODY ALEBO ZA ŽIADNE NEPRIAME EKONOMICKÉ ŠKODY, ALEBO
3. UŠLÝ ZISK, STRATA OBCHODOV, PRÍJMOV, POVESTI ALEBO OČAKÁVANÝCH ÚSPOR.

NIEKTORÉ PRÁVNE SYSTÉMY NEUMOŽŇUJÚ VYLÚČENIE ALEBO OBMEDZENIE PRIAMYCH, NÁHODNÝCH ČI NÁSLEDNÝCH ŠKÔD, TAKŽE VYŠŠIE UVEDENÉ VYLÚČENIE ALEBO OBMEDZENIE SA NA VÁS NEMUSÍ VZŤAHOVAŤ.

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. Ak chcete získať informácie o produktoch a službách, ktoré sú aktuálne dostupné vo vašej oblasti, kontaktujte lokálneho zástupcu spoločnosti 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.

Spoločnosť IBM môže vlastniť patenty alebo mať podané žiadosti o patenty, týkajúce sa predmetnej veci popísanej v tomto dokumente. Získanie tohto dokumentu vám nedáva žiadnu licenciu na tieto patenty. Požiadavky o licencie môžete zasielať písomne na:

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:

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) opísaných 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 stránkach nie sú súčasťou materiálov pre tento IBM produkt a použitie týchto webových stránok 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 YBWA
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. Spoločnosť IBM tieto produkty netestovala a nemôže potvrdiť presnosť výkonu, kompatibilitu alebo akékoľvek iné tvrdenia súvisiace s produktmi, ktoré nie sú produktmi 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.

Všetky ceny IBM sú navrhované predajné ceny stanovené spoločnosťou IBM, sú aktuálne a sú predmetom zmeny bez ohlásenia. Dílerské ceny sa môžu líšiť.

Tieto informácie sú len pre účely plánovania. Tieto informácie sú predmetom zmeny pred sprístupnením opisovaných produktov.

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. STRATA ZISKU, 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:

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

Adobe, logo Adobe, PostScript a logo PostScript sú registrované ochranné známky alebo ochranné známky spoločnosti Adobe Systems Incorporated v Spojených štátoch a iných krajinách.

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

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

Linux je ochranná známka Linusa Torvaldsa v USA alebo iných krajinách.

UNIX je registrovaná ochranná známka spoločnosti Open Group v USA a iných krajinách.

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

Pojmy a podmienky

Oprávnenia na používanie týchto publikácií sú predmetom nasledujúcich pojmov a podmienok.

Osobné použitie: Tieto publikácie môžete reprodukovať pre svoje osobné, nekomerčné použitie za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia autora ich nemôžete distribuovať, zobrazovať ani odvádzať práce z týchto publikácií ani žiadnej ich časti.

Komerčné použitie: Tieto publikácie môžete reprodukovať, distribuovať a zobrazovať výlučne vo vašej spoločnosti za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia od autora nemôžete odvádzať práce z týchto publikácií ani reprodukovať, distribuovať a zobrazovať tieto publikácie ani žiadne ich časti.

S výnimkou ako je uvedené v týchto podmienkach, na publikácie ľubovoľné informácie, údaje, softvér alebo iné tu obsiahnuté intelektuálne vlastníctvo nemáte žiadne oprávnenia, licencie ani práva, vyjadrené ani implikované.

Spoločnosť IBM si vyhradzuje právo odobrať tu uvedené oprávnenia vždy, podľa vlastného uváženia, keď použitie týchto publikácií škodí autorovi, alebo ak spoločnosť IBM, že pokyny hore nie sú striktne dodržiavané.

Tieto informácie nemôžete prevziať ani exportovať okrem prípadu, ak to dovoľujú všetky aplikovateľné zákony a regulácie, vrátane všetkých zákonov a regulácií USA pre export.

SPOLOČNOSŤ IBM NERUČÍ ZA OBSAH TÝCHTO PUBLIKÁCIÍ. PUBLIKÁCIE SÚ POSKYTNUTÉ ″TAK AKO SÚ″ BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK PREDAJNOSTI, NEPOŠKODENIA A VHODNOSTI NA KONKRÉTNY ÚČEL.

Vytlačené v USA