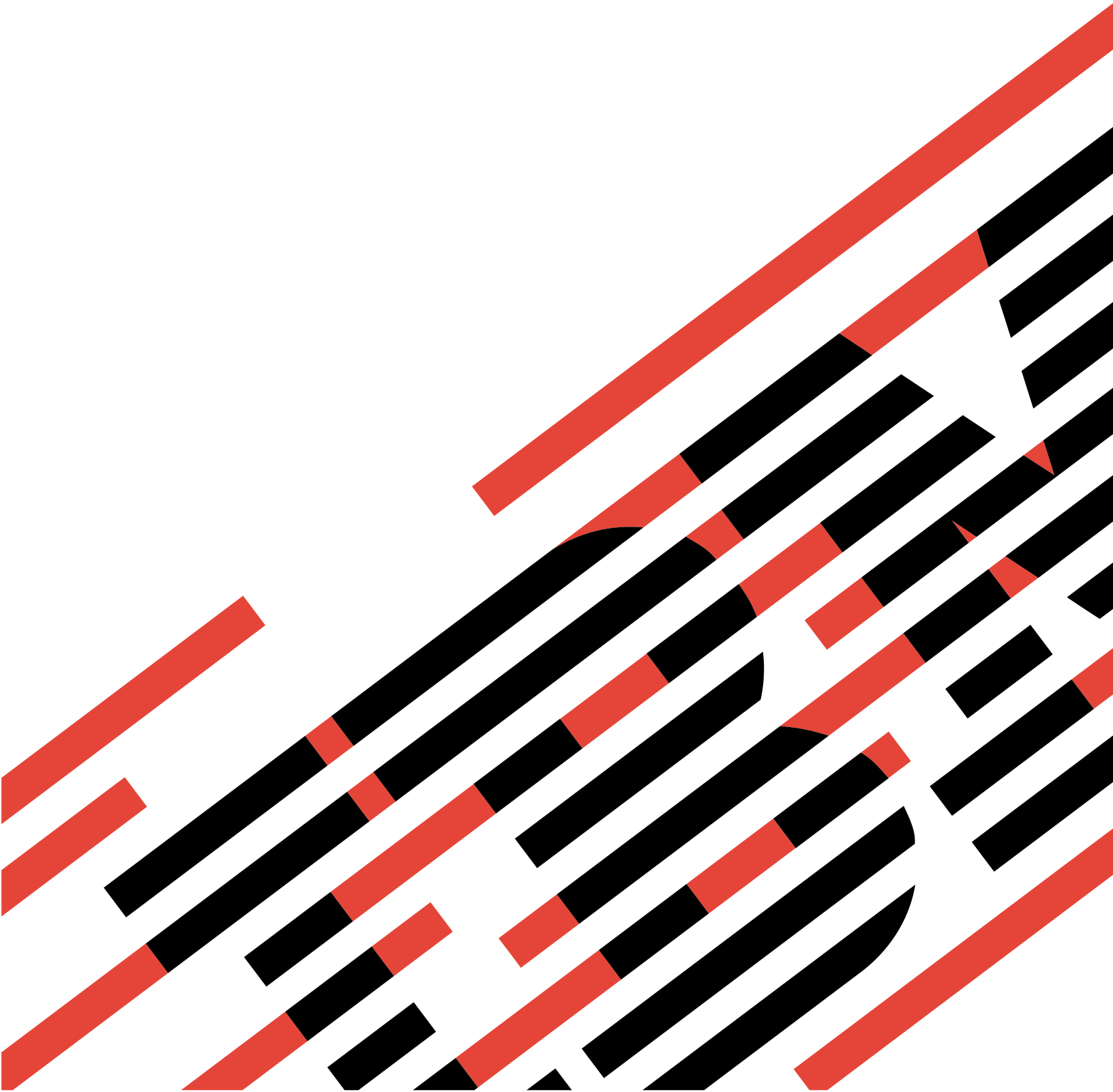
IBM

eserver

iSeries

Objektum aláírás és aláírás ellenőrzés



IBM

@server

iSeries

Objektum aláírás és aláírás ellenőrzés

Tartalom

Objektum aláírás és aláírás ellenőrzés

Az objektum aláírás és az aláírás ellenőrzés olyan biztonsági funkciók, amelyeket különféle iSeries objektumok sértetlenségének ellenőrzésére alkalmazhat. Az objektum aláírásához a digitális igazolás magánkulcsát használja, az igazolással pedig (amely tartalmazza a megfelelő nyilvános kulcsot) ellenőrzi a digitális aláírást. A digitális aláírás garantálja az objektum (amit aláír) időpontjának és tartalmának sértetlenségét. Az aláírás a hitelesség és a jogosultság visszautasíthatatlan ellenőrzése. Segítségével kimutatható az eredet ellenőrzése és a beavatkozás észlelése. Az objektum aláírása révén azonosíthatja az objektum eredetét, és lehetőséget kap az objektum változásainak észlelésére. Amikor az aláírást ellenőrzi egy objektumon, meghatározhatja, hogy változott-e az objektum tartalma az aláírás óta. Továbbá ellenőrizheti az aláírás forrását is, ami biztosíthatja az objektum eredetének megbízhatóságát.

Az alábbiak segítségével valósíthatja meg az iSeries szerveren az objektum aláírást és az aláírás ellenőrzést:

- Az API-k révén programozottan írhatja alá az objektumokat és ellenőrizheti az objektumokon található aláírásokat.
- A Digitális igazolás kezelő révén ugyancsak aláírhatja az objektumokat, és megtekintheti vagy ellenőrizheti az objektum aláírásokat.
- Az iSeries navigátor Kezelőközpontja révén is aláírhat objektumokat, ami más rendszerek általi használatra szánt terjesztési csomagok elkészítésének részeként valósul meg.
- A CL parancsok, mint például a Check Object Integrity (CHKOBJITG), révén ellenőrizheti az aláírásokat.

Olvassa át az alábbi témaköröket, ha többet kíván megtudni az objektumok aláírásának módszereiről, illetve arról, hogyan javíthatja biztonsági intézkedéseit az objektumok aláírásával:

A V5R2 újdonságai
Az itt leírtak segítségével megismerheti az iSeries objektum aláíró és aláírás ellenőrző funkcióit, valamint a dokumentációban bekövetkezett változásokat.

A témakör nyomtatása
Ismerteti a teljes témakör kinyomtatását PDF fájlként.

Objektum aláírási forgatókönyvek
Az itt leírt forgatókönyvek néhány jellemző helyzetet szemléltetnek az iSeries objektum aláíró és aláírás ellenőrző funkciók használatához. Mindegyik forgatókönyv tartalmaz konfigurálási feladatokat is, amelyeket el kell végezni ahhoz, hogy a forgatókönyv megvalósuljon a leírás szerint.

Objektum aláírási alapelvek
Az itt leírt alapelvek és információk segítségével tanulmányozhatja a digitális aláírásokat, az objektum aláírást és az aláírások ellenőrzésének folyamatát.

Az objektum aláírás és aláírás ellenőrzés előfeltételei
Tanulmányozhatja a konfigurációs előfeltételeket, valamint az objektumok aláírásánál és az aláírások ellenőrzésénél figyelembe veendő egyéb tervezési feltételeket.

Az aláírt objektumok kezelése
Az itt leírtak segítségével tanulmányozhatja az iSeries parancsokat és rendszerváltozókat, melyekkel kezelheti az aláírt objektumokat, valamint megismerheti, milyen hatással vannak az aláírt objektumok a biztonsági mentés és helyreállítás folyamatára.

Az objektum aláírás és aláírás ellenőrzés hibakeresése
Az itt leírtak révén tanulmányozhatja a problémák és a hibák megoldását, amelyekkel az objektumok aláírása és az aláírások ellenőrzése során találkozhat.

Az objektum aláíráshoz és az aláírás ellenőrzéshez kapcsolódó információk
Az itt leírtak között hivatkozásokat talál más forrásokhoz, ahol további ismertetést talál az objektumok aláírásáról és az aláírások ellenőrzéséről.

A V5R2 újdonságai

Az iSeries objektum aláíró és aláírás ellenőrző funkciói a V5R1 változatban jelentek meg először. Azonban néhány új funkció és javítás vált elérhetővé a V5R2 változatban.

Az objektum aláírási és az aláírás ellenőrzési funkciók újabb, vagy javított elemei a következők:

- **iSeries navigátor Kezelőközpont objektum aláírási funkció**
  A Kezelőközpont termék Definíciós varázslójával is aláírhat ezentúl olyan objektumokat, amelyeket összecsomagolva iSeries végpont rendszereknek terjeszt.
- **Parancs (*CMD) objektumok aláírása**
  Ezentúl parancs (*CMD) objektumok aláírására is lehetősége van. Eldöntheti, hogy az egész *CMD objektumot írja alá, vagy csak a *CMD objektum magját alkotó összetevőket.
- **Új aláírási és ellenőrzési API-k**
  Három új API áll rendelkezésére, amelyek révén programozott módon használhatja ki az OS/400 aláírási és ellenőrzési képességeinek előnyeit:
  - Sign Buffer (QYDOSGNB, QydoSignBuffer) API
    Ez az API lehetővé teszi a helyi rendszernek, hogy digitálisan aláírja a puffert, ami a megbízhatóságát igazolja. A puffer aláírása után a rendszer visszaadja a digitális aláírást az API hívójának. Például, az API felhasználásával aláírja egy XML fájl egyik részét, míg az aláírást az XML fájl másik része tárolja. Vagy, beolvassa az adatbázis fájl rekordjait a pufferbe, és az API segítségével aláírja őket.
  - Verify Buffer (QYDOVFYB, QydoVerifyBuffer)
    Ez az API lehetővé teszi a helyi rendszernek, hogy ellenőrizze a korábban aláírt puffer digitális aláírását.
  - Add Verifier (QYDOADDV, QydoAddVerifier) API
    Ez az API hozzáadja az igazolást a rendszer *SIGNATUREVERIFICATION igazolás tárolójához. Az így hozzáadott igazolással a rendszer ellenőrizheti az adott igazolással létrehozott objektumokon lévő aláírásokat. Az aláírások ellenőrzése lehetővé teszi a rendszernek az aláírt objektumok sértetlenségének ellenőrzését, ami bizonyosságul szolgál arra, hogy az objektumok nem változtak meg az aláírás óta. Ha az igazolás tároló nem létezik, az API létrehozza azt, és hozzáadja az igazolást.

    Megjegyzés: Biztonsági okokból az API nem teszi lehetővé az Igazolási hatóság (CA) igazolásának elhelyezését a *SIGNATUREVERIFICATION igazolás tárolóba. Amikor a CA igazolását hozzáadja az igazolás tárolóhoz, a rendszer az igazolások megbízható forrásának ismeri el a CA-t. Következésképpen, a rendszer a CA által kiadott igazolást úgy kezeli, mint amelyik megbízható forrásból ered. Ennek következtében, az API-val nem hozhat létre telepítési programot, amely elhelyezné a CA igazolást az igazolás tárolóba. A Digitális igazolás kezelőt kell ahhoz használni, hogy hozzáadja a CA igazolást az igazolás tárolóhoz. Így garantálja, hogy valaki kimondottan és kézi módon meghatározza, mely CA-kat tekintse a rendszer megbízhatónak. Így cselekedve megakadályozza annak lehetőségét, hogy a rendszer olyan forrásból importáljon igazolásokat, amelyeket az adminisztrátor tudta nélkül tekint a rendszer megbízhatónak.

    Ha azt akarja, hogy senki se használhassa ezt az API-t arra a célra, hogy ellenőrző igazolást adjon hozzá a *SIGNATUREVERIFICATION igazolás tárolóhoz a tudta nélkül, akkor vegye fontolóra az API letiltását a rendszeren. A Rendszer szervizeszközök (SST) segítségével utasíthatja vissza a biztonsággal kapcsolatos rendszerváltozók módosításait.

Az iSeries objektum aláírási és aláírás ellenőrzési képességeiről szóló leírások korábban az Információs központ Digitális igazolás kezelés című témakörének része volt. Most további módszerekkel bővült a paletta, amelyekkel aláírhat objektumokat és ellenőrizhet aláírásokat. Következésképpen, az Információs központban egy új témakör tárgyalja az objektum aláírási és aláírás ellenőrzési képességeket, ami könnyebbé teszi a róluk szóló tájékoztatás központosítását. A témakör javított és bővített információkat, mint például forgatókönyveket tartalmaz, melyek segítségével eldöntheti, hogy mikor és hogyan használhatja ezeket a képességeket biztonsági intézkedéseinek kiegészítéseként.

A témakör újabb, illetve módosított elemei:

- Forgatókönyvek annak meghatározására, hogy biztonsági intézkedéseinek kiegészítéseként hogyan alkalmazhatja legjobban az objektum aláírási és az aláírás ellenőrzési tulajdonságokat.
- Új fejezetek parancsok és rendszerváltozók leírására, amelyekkel kezelheti az aláírt objektumokat a rendszeren.
- Új fejezetek a tervezési és egyéb fogalmi információk leírására, amelyek az objektumok aláírásáról és az aláírás ellenőrzéséről szólnak.

Az új kiadás újdonságairól és módosításairól olvashat a Jegyzék a felhasználóknak .

A témakör nyomtatása

A PDF változat megtekintéséhez vagy letöltéséhez válassza ki az Objektum aláírás és aláírás ellenőrzést

(fájl méret 350 kb vagy kb. 44 oldal).

A PDF mentése munkaállomásra megjelenítés vagy nyomtatás céljából:

1. Nyissa meg a PDF fájlt a böngészőben (kattintson a fenti hivatkozásra).
2. Kattintson a böngésző **Fájl** menüjére.
3. Kattintson a **Mentés másként...** menüpontra.
4. Válassza ki azt a könyvtárat, ahová a PDF fájlt menteni szeretné.
5. Kattintson a **Mentés** gombra.

Ha szüksége van az Adobe Acrobat Reader programra a PDF megtekintéséhez vagy nyomtatásához, letöltheti egy példányát az Adobe webhelyéről (www.adobe.com/prodindex/acrobat/readstep.html) .

Objektum aláírási forgatókönyvek

Az iSeries szerver több különböző módszert biztosít az objektumok aláírásához és a rajtuk található aláírások ellenőrzéséhez. Üzleti és biztonsági igényeitől és céljaitól függ az, hogy melyik módszert választja az objektumok aláírására, és hogyan kezeli az aláírt objektumokat. Bizonyos esetekben csak az objektum aláírását kell ellenőrizni a rendszeren ahhoz, hogy meggyőződjön az objektum sértetlenségéről. Más esetekben dönthet úgy, hogy aláírja az objektumokat, amelyeket másoknak küld tovább. Az objektumok aláírása lehetővé teszi másoknak, hogy azonosítsák az objektumok eredetét, valamint ellenőrizzék az objektumok sértetlenségét.

Számos tényezőtől függ az, hogy melyik módszert fogja használni. Az itt bemutatott forgatókönyvek az objektum aláírások és az aláírás ellenőrzések legáltalánosabb jellemzőit írják le jellegzetes üzleti környezetben. Minden egyes forgatókönyv leírja az előfeltételeket, valamint az összes feladatot, amelyet végre kell hajtani a forgatókönyv leírás szerinti megvalósításához. Nézze át az alábbi forgatókönyveket, melyek segítségével meghatározhatja, hogyan használja az iSeries objektum aláírási és aláírás ellenőrzési funkcióit üzleti és biztonsági igényeinek megfelelően:

Forgatókönyv: Objektumok aláírása és aláírások ellenőrzése Digitális igazolás kezelővel
Ez a forgatókönyv egy olyan vállalatot ismertet, ahol alá akarják íratni a sebezhető alkalmazások nyilvános webszerveren lévő objektumait. Szeretnék, ha könnyebben meg tudnák határozni, hogy mikor történnek jogosulatlan változtatások az objektumokon. A társaság üzleti és biztonsági céljaitól függően a forgatókönyv leírja, hogyan használhatja elsődleges módszerként a Digitális igazolás kezelőt (DCM) az objektumok aláírására és az aláírások ellenőrzésére.

Forgatókönyv: Objektumok aláírása és aláírások ellenőrzése API-k segítségével
Ez a forgatókönyv egy olyan alkalmazás fejlesztési társaságot ismertet, ahol programozottan szeretnék aláírni az eladásra szánt alkalmazásokat. Szeretnék arról biztosítani ügyfeleiket, hogy az alkalmazások valóban tőlük érkeznek, és egyúttal lehetőséget nyújtani az alkalmazások jogosulatlan változtatásainak telepítéskori észleléséhez. A társaság üzleti igényei és biztonsági céljai alapján a forgatókönyv leírja, hogyan használhatja a Sign Object és az Add Verifier API-kat az objektumok aláírására és az aláírások ellenőrzésének engedélyezésére.

Forgatókönyv: Objektumok aláírása Kezelőközponttal
Ez a forgatókönyv egy olyan vállalatot ismertet, ahol alá akarják íratni azokat az objektumokat, amelyeket csomagolnak és több iSeries szervernek továbbítanak. A társaság üzleti igényei és biztonsági céljai alapján a forgatókönyv leírja, hogyan tudja az iSeries navigátor Kezelőközpont funkciójával összecsomagolni és aláírni az objektumokat, amelyeket azután más iSeries szervereknek továbbítanak.

Forgatókönyv: Objektumok aláírása és aláírások ellenőrzése DCM segítségével

Helyzet

A MyCo., Inc. iSeries rendszergazdájaként a cég két iSeries szerverének irányításáért felelős. Az egyik iSeries szerver a cég nyilvános webhelyét biztosítja. A társaság másik, úgynevezett belső iSeries termék szerverén fejleszti a nyilvános webhely tartalmát, valamint innen visszi át a fájlokat és a program objektumokat a nyilvános webszerverre a tesztelést követően.

A társaság nyilvános webszerverén általános cégtájékoztató információkat tartalmazó webhely van. A webhely különféle űrlapokat is tartalmaz, amelyeket az ügyfelek kitölthetnek a termékek regisztrációjához, valamint termék adatok, termék frissítések, terjesztési helyek, stb. lekéréséhez. Figyelembe kell vennie az űrlapokat nyújtó cgi-bin programok sebezhetőségét - amint tudja, tartalmuk változhat. Ennek következtében szeretné, ha tudná ellenőrizni a program objektumok sértetlenségét, és észlelni a jogosulatlan változtatásokat. Következésképpen úgy dönt, hogy digitálisan aláírja ezeket az objektumokat, hogy eleget tegyen a biztonsági elvárásoknak.

Tüzetesen átvizsgálta az OS/400 objektum aláírási tulajdonságait, és áttanulmányozta a módszereket, amelyek az objektumok aláírására és az aláírások ellenőrzésére szolgálnak. Mivel kevés számú iSeries szerver irányításáért felelős, és úgy gondolja, hogy nem kell majd gyakran aláírnia objektumokat, a Digitális igazolás kezelő (DCM) használata mellett dönt az ilyen jellegű feladatok elvégzéséhez. Ugyancsak elhatározza egy Helyi igazolási hatóság (CA) létrehozását, valamint magán igazolás használatát az objektumok aláírásához. A Helyi CA által objektum aláíráshoz kibocsátott magán igazolás korlátok közé szorítja a biztonsági technológia költségét, mivel nem kell vásárolnia igazolást egy jól ismert nyilvános CA-tól.

A példa hasznos tájékoztatást nyújt a beállítási lépésekről és az objektum aláírásról, amikor kevés számú iSeries szerveren kívánja az objektumokat aláírni.

A forgatókönyv előnyei

Ez a forgatókönyv a következő előnyökkel jár:

- Az objektumok aláírása lehetővé teszi a sebezhető objektumok sértetlenségének ellenőrzését, és könnyebben meghatározhatóvá válik, hogy változtak-e az objektumok az aláírás után. Ez csökkenthet bizonyos hibakeresési feladatokat, melyeket végrehajt a jövőben az alkalmazások és egyéb rendszer problémák követéséhez.
- A DCM grafikus felhasználói kezelőfelületét (GUI) használva az objektumok aláírására és az objektum aláírások ellenőrzésére, lehetővé válik, hogy Ön és mások is a vállalaton belül gyorsan és könnyen végrahajtsák az ilyen feladatokat.
- Az objektumok aláírásához és az aláírások ellenőrzéséhez DCM eszközt használva, csökkentheti a biztonsági stratégia részét képező objektum aláírás megismerésére és használatára fordított időt.
- Az objektumok aláírásához Helyi Igazolási hatóság (CA) által kiadott igazolást felhasználva, olcsóbbá teszi az objektumok aláírásának megvalósítását.

Célok

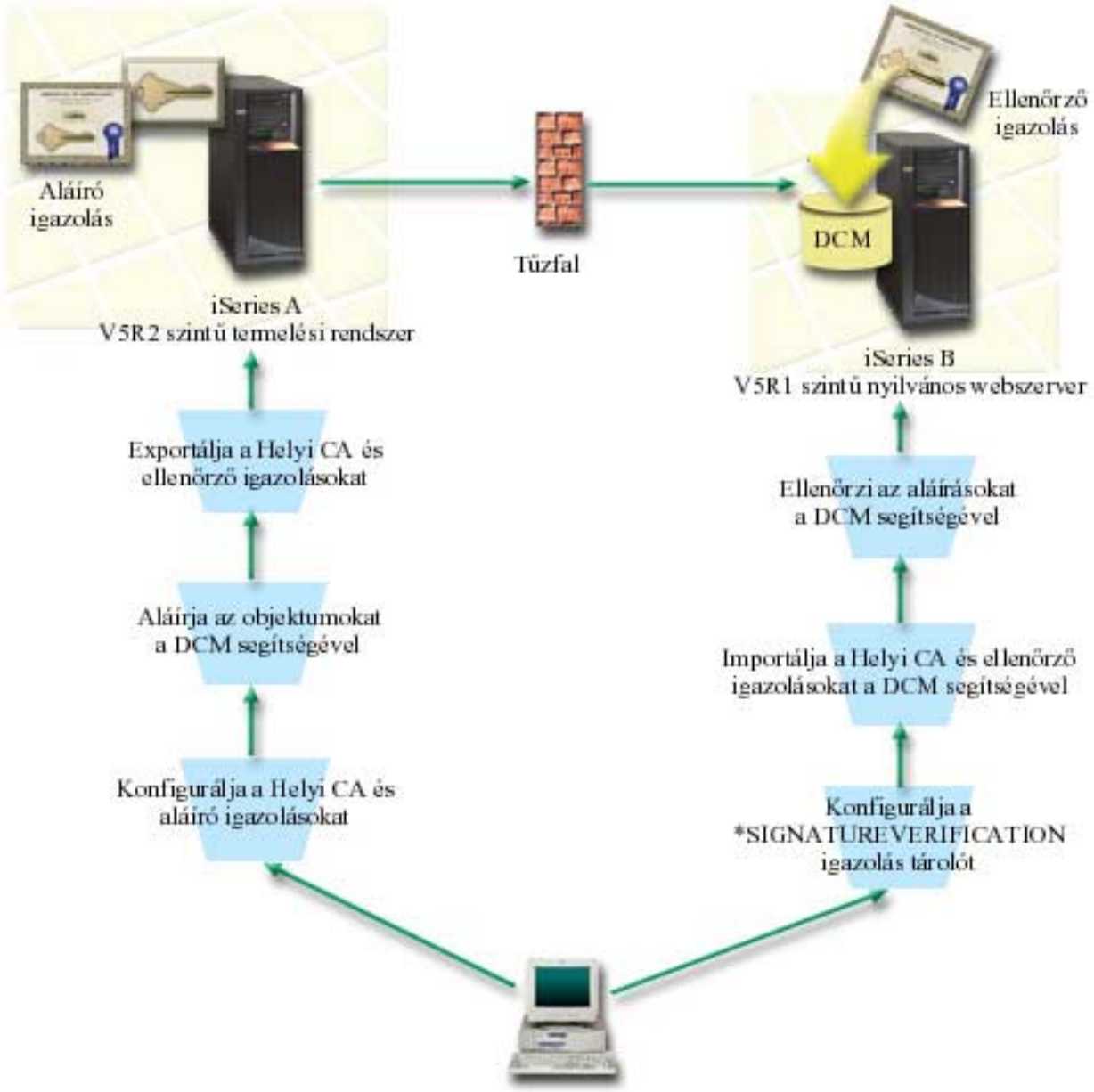
Ebben a forgatókönyvben digitálisan akarja aláírni az olyan sebezhető objektumokat, mint például a cgi-bin programokat (amelyek az űrlapokat generálják) a társaság nyilvános iSeries szerverén. A MyCo, Inc. rendszergazdájaként Digitális igazolás kezelőt (DCM) akar használni az ilyen objektumok aláírására, valamint az objektumokon lévő aláírások ellenőrzésére.

A forgatókönyv céljai a következők:

- A cég alkalmazásait és a nyilvános webszerver (iSeries B) egyéb sebezhető objektumait Helyi CA-tól származó igazolással kell aláírni, hogy kordában tartsa az alkalmazások aláírásának költségeit.
- A rendszergazdának és más kijelölt felhasználóknak könnyedén ellenőrizniük kell az iSeries szervereken lévő aláírásokat, hogy ellenőrizni tudják a társaság által aláírt objektumok forrását és hitelességét. Ahhoz, hogy ezt végrehajthassa, mindegyik iSeries szerveren legyen egy másolat a cég aláírás ellenőrző igazolásából, valamint a Helyi Igazolási hatóságtól (CA) eredő igazolásból a szerverek *SIGNATUREVERIFICATION igazolás tárolóiban.
- A cég alkalmazásain és egyéb objektumain lévő aláírások ellenőrzésével az iSeries adminisztrátorok és mások észlelhetik, hogy megváltozott-e az objektumok tartalma aláírásuk óta.
- A rendszergazdának DCM-et kell használni az objektumok aláírásához. Az objektumokon lévő aláírások ellenőrzéséhez ugyancsak DCM-et kell használni a rendszergazdának és másoknak.

Részletek

Az alábbi ábra szemlélteti az objektum aláírási és az aláírás ellenőrzési folyamatot, amely a forgatókönyv megvalósítását szolgálja:



Az ábra a forgatókönyvhöz tartozó következő pontokat szemlélteti:

iSeries A

- Az iSeries A szerveren OS/400 Verzió 5 Változat 2 (V5R2) fut.
- Az iSeries A szerver a társaság belső termelési szervere, amely egyúttal fejlesztési platform is a nyilvános webszerver (iSeries B) számára.
- Az iSeries A szerveren telepítve van a Cryptographic Access Provider 128-bit for iSeries (5722–AC3) termék.
- Az iSeries A szerveren telepítve és konfigurálva van a Digital Certificate Manager (OS/400 34-es opció), és az IBM HTTP Server (5722–DG1) termék.
- Az iSeries A szerver Helyi Igazolási hatóságként (CA) szerepel, és az objektum aláíró igazolás a rendszeren található.

- Az iSeries A szerver DCM segítségével írja alá az objektumokat. A szerver a társaság nyilvános alkalmazásainak és egyéb objektumainak elsődleges objektum aláíró rendszere.
- Az iSeries A szerver is konfigurálható az aláírás ellenőrzéséhez.

iSeries B
- Az iSeries B szerveren OS/400 Verzió 5 Változat 1 (V5R1) fut.
- Az iSeries B a társaság külső nyilvános webszervere a cég tűzfalán kívül.
- Az iSeries B szerveren telepítve van a Cryptographic Access Provider 128-bit (5722–AC3) termék.
- Az iSeries B szerveren telepítve és konfigurálva van a Digital Certificate Manager (OS/400 34-es opció), és az IBM HTTP Server (5722–DG1) termék.
- Az iSeries B szerver nem üzemeltet Helyi CA-t, és nem is ír alá objektumokat.
- Az iSeries B szerver konfigurációja megengedi az aláírás ellenőrzését a DCM segítségével, ami így létrehozza a *SIGNATUREVERIFICATION igazolás tárolót, és importálja a szükséges ellenőrző és Helyi CA igazolásokat.
- Az objektumokon lévő aláírások ellenőrzésére a DCM szolgál.

Előfeltételek és feltételezések

A forgatókönyv a következő előfeltételektől és feltételezésektől függ:
1. Az iSeries szerverek kielégítik a Digitális igazolás kezelő (DCM) telepítésének és használatának követelményeit.
2. Senki sem konfigurálta vagy használta korábban az iSeries szervereken lévő DCM-eket.
3. Az összes iSeries szerver a legmagasabb szintű telepített Cryptographic Access Provider 128-bit licencprogrammal (5722-AC3) rendelkezik.
4. A Verify object signatures during restore (QVFYOBJRST) rendszerváltozó alapértéke az összes forgatókönyvben 3 az iSeries szervereken, és nem is változik ez a beállítás. Az alapértelmezett beállítás garantálja, hogy a szerver ellenőrizheti az objektumok aláírásait, amikor visszaállítja az aláírt objektumokat.
5. Az iSeries A szerver rendszergazdájának *ALLOBJ különleges jogosultsággal kell rendelkeznie az objektumok aláírásához, vagy a felhasználói profilnak kell jogosultnak lenni az objektum aláíró alkalmazáshoz.
6. A rendszergazdának vagy valaki másnak, aki létrehozza az igazolás tárolót a DCM-ben, *SECADM és *ALLOBJ különleges jogosultsággal kell rendelkeznie.
7. A rendszergazdának vagy másoknak *AUDIT különleges jogosultsággal kell rendelkezni az objektum aláírások ellenőrzéséhez az összes iSeries szerveren.

Feladat lépések

A forgatókönyv megvalósításához két feladatsort kell végrehajtani: Az egyik feladatsor lehetővé teszi az iSeries A konfigurálását Helyi igazolási hatóságként (CA), valamint az objektumok aláírását és az aláírások ellenőrzését. A második feladatsor lehetővé teszi az iSeries B konfigurálását, hogy ellenőrizze az iSeries A által létrehozott objektum aláírásokat.

iSeries A feladatsor

Az összes alábbi feladatot végrehajtva az iSeries A szerveren hozzon létre egy Helyi CA-t, valamint írja alá az objektumokat és ellenőrizze az aláírásokat a forgatókönyv leírása szerint:
1. Hajtsa végre az előfeltételként megadott lépéseket, amelyek révén telepíti és konfigurálja az összes iSeries terméket.
2. A Digitális igazolás kezelő (DCM) segítségével hozza létre a Helyi igazolási hatóságot (CA), amely kiadja az objektum aláíró igazolást.

3. A DCM segítségével hozzon létre alkalmazás definíciót.
4. A DCM segítségével rendelje hozzá az igazolást az objektum aláíró alkalmazás definíciójához.
5. A DCM segítségével írja alá a cgi-bin program objektumokat.
6. A DCM segítségével exportálja az igazolásokat, amelyeket más rendszerek használnak az objektum aláírások ellenőrzéséhez. A Helyi CA igazolás és az objektum aláíró igazolás egy-egy példányát is exportálni kell egy fájlba, mint aláírás ellenőrző igazolás.
7. Az igazolás fájlokat vigye át a társaság nyilvános iSeries szerverére (iSeries B), hogy bárki ellenőrizni tudja az iSeries A által létrehozott aláírásokat.

iSeries B feladatsor

Ha szándékában áll visszaállítani olyan aláírt objektumokat, amelyeket a forgatókönyv szerint átvitt a nyilvános webszerverre (iSeries B), akkor hajtsa végre az aláírás ellenőrzésre vonatkozó konfigurációs feladatokat az iSeries B szerveren, mielőtt átvinné az aláírt objektumokat. Az aláírás ellenőrzés konfigurálását be kell fejezni ahhoz, hogy sikeresen ellenőrizhesse az aláírásokat, mikor visszaállítja az aláírt objektumokat a nyilvános webszerveren.

Az iSeries B szerveren hajtsa végre az alábbi feladatokat, és ellenőrizze az objektumokon lévő aláírásokat a forgatókönyvben leírtak szerint:

8. A Digitális igazolás kezelő (DCM) segítségével hozza létre a *SIGNATUREVERIFICATION igazolás tárolót.
9. A DCM segítségével importálja a Helyi CA igazolást és az aláírás ellenőrző igazolást.
10. A DCM segítségével ellenőrizze az aláírásokat az átvitt objektumokon.

Konfigurálási részletek

A következő feladatsorok végrehajtásával konfigurálja és használja a Digitális igazolás kezelőt az objektumok aláírására, ahogy a forgatókönyv írja.

1. lépés: Előfeltételt jelentő összes feladat végrehajtása

Végre kell hajtani az összes előfeltételt jelentő feladatot, amely révén telepíti és konfigurálja az összes szükséges iSeries terméket, mielőtt a forgatókönyv megvalósításához tartozó, jellemző konfigurálási feladatokat végrehajthatná.

2. lépés: Helyi igazolási hatóság létrehozása objektum aláíró igazolás kiadása céljából

Amikor Digitális igazolás kezelővel (DCM) hoz létre Helyi igazolási hatóságot (CA), űrlapok sorozatát kell kitöltenie a folyamat során. Ezek az űrlapok végigvezetik a CA létrehozásának folyamatán, valamint a Védett socket réteg (SSL), objektum aláírás és aláírás ellenőrzés céljára használt digitális igazolások használatának elkezdéséhez szükséges egyéb feladatok végrehajtásán. A forgatókönyv szerint ugyan nem kell konfigurálni igazolásokat az SSL funkcióhoz, de az összes űrlapot ki kell tölteni ahhoz, hogy konfigurálja a rendszert az objektumok aláírásához.

Kövesse az alábbi lépéseket, ha a DCM segítségével Helyi CA-t hoz létre és működtet:

1. Indítsa el a DCM funkciót.
2. A DCM navigációs keretén válassza ki az **Igazolási hatóság (CA) létrehozását** az űrlapok megjelenítéséhez.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
3. Töltse ki a teljes űrlapot. A feladat végrehajtásakor tegye a következőt:
   a. Adja meg a Helyi CA azonosítási információit.

b. Telepítse a Helyi CA igazolást a böngészőjében, hogy a szoftver felismerhesse a Helyi CA-t és ellenőrizhesse az általa kiadott igazolásokat.
c. Adja meg a Helyi CA stratégiai adatait.
d. Az új Helyi CA segítségével adja ki a szerver vagy a kliens igazolást, amelyet alkalmazásai az SSL kapcsolatokhoz használhatnak.

   Megjegyzés: A forgatókönyv ugyan nem használja ezt az igazolást, de létre kell hozni, mielőtt a Helyi CA segítségével kiadná a szükséges objektum aláíró igazolást. Ha az igazolás létrehozása nélkül félbehagyja a feladatot, létre kell hoznia az objektum aláíró igazolást és az *OBJECTSIGNING igazolás tárolót, amelyben külön tárolja.
e. Válassza ki azokat az alkalmazásokat, amelyek használhatják a szerver vagy a kliens igazolást az SSL kapcsolatokhoz.

   Megjegyzés: A forgatókönyv céljainak megfelelően ne válasszon ki egyetlen alkalmazást sem, hanem kattintson a **Folytatásra** a következő űrlap megjelenítéséhez.
f. Az új Helyi CA segítségével adjon ki egy objektum aláíró igazolást, melyet az alkalmazások használhatnak objektumok digitális aláírására. Az alfeladat létrehozza az *OBJECTSIGNING igazolás tárolót. Ez az a tároló, amelyet az objektum aláíró igazolások kezelésére használ.
g. Válassza ki az alkalmazásokat, amelyek megbízhatónak tekintik a Helyi CA-t.

   Megjegyzés: A forgatókönyv céljainak megfelelően ne válasszon ki egyetlen alkalmazást sem, hanem kattintson a **Folytatásra** a feladat befejezéséhez.

Most, hogy létrehozta a Helyi CA-t és az objektum aláíró igazolást, meg kell adni az igazolást használó objektum aláíró alkalmazást, mielőtt aláírhatna objektumokat.

3. lépés: Objektum aláíró alkalmazás definíciójának létrehozása

Miután létrehozta objektum aláíró igazolását, a Digitális igazolás kezelővel (DCM) meg kell adni az objektum aláíró alkalmazást, amelyet használni fog az objektumok aláírására. Az alkalmazás definíciónak nem kell hivatkozni egy tényleges alkalmazásra. A létrehozott alkalmazás definíció írja le az aláírni kívánt objektumcsoport típusát. Olyan definícióra van szükség, amely révén az alkalmazás azonosítót (ID) társíthatja az igazolással, hogy engedélyezze az aláírási folyamatot.

Kövesse az alábbi lépéseket, ha a DCM segítségével objektum aláíró alkalmazás definícióját hozza létre:

1. A navigációs kereten kattintson az **Igazolás tároló választására**, majd válassza ki a megnyitandó ***OBJECTSIGNING** igazolás tárolót.
2. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatásra**.
3. A navigációs kereten válassza az **Alkalmazások kezelését** a feladatlista megjelenítéséhez.
4. Válassza ki az **Alkalmazás hozzáadását** a feladatlistából, hogy megjelenítse az alkalmazás megadására szolgáló űrlapot.
5. Töltse ki az űrlapot, és kattintson a **Hozzáadásra**.

Most, hozzá kell rendelni az objektum aláíró igazolást a létrehozott alkalmazáshoz.

4. lépés: Igazolás hozzárendelése az objektum aláíró alkalmazás definíciójához

Kövesse az alábbi lépéseket, ha igazolást rendel hozzá az objektum aláíró alkalmazáshoz:

1. A DCM navigációs keretén válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
2. A feladatlistán válassza az **Igazolás hozzárendelése** feladatot az aktuális igazolás tárolóban lévő igazolások listájának megjelenítéséhez.

3. Válassza ki az igazolást a listából, és kattintson a **Hozzárendelés alkalmazásokhoz** feladatra, hogy megjelenítse az aktuális igazolás tárolóhoz tartozó alkalmazás definíciók listáját.
4. Válasszon ki egy vagy több alkalmazást a listából, és kattintson a **Folytatásra**. Egy üzenetlap jelenik meg, amely vagy megerősíti az igazolás hozzárendelését, vagy hiba információt közöl, ha probléma történt.

Amikor végrehajtja ezt a feladatot, készen áll arra, hogy a DCM segítségével aláírja a program objektumokat, amelyeket a társaság nyilvános webszervere (iSeries B) fog használni.

5. lépés: Program objektumok aláírása

Kövesse az alábbi lépéseket, amikor a DCM segítségével aláír olyan program objektumokat, amelyeket a társaság webszervere (iSeries B) használ:

1. A navigációs kereten kattintson az **Igazolás tároló választására**, majd válassza ki a megnyitandó ***OBJECTSIGNING** igazolás tárolót.
2. Írja be az *OBJECTSIGNING igazolás tárolóra vonatkozó jelszót, és kattintson a **Folytatásra**.
3. Miután frissül a navigációs keret, válassza az **Aláírható objektumok kezelését** a feladatlista megjelenítéséhez.
4. A feladatlistán válassza az **Objektum aláírása** feladatot az objektumok aláírásához használt alkalmazás definíciók listájának megjelenítéséhez.
5. Válassza ki az előző lépésben meghatározott alkalmazást, és kattintson az **Objektum aláírása** feladatra. A megjelenő űrlap lehetővé teszi az aláírásra szánt objektumok helyének megadását.
6. Az előbukkanó mezőbe írja be az aláírni szándékozott objektum vagy objektum könyvtár teljesen megadott útvonalnevét, és kattintson a **Folytatásra**. Vagy írja be az alkönyvtár nevét, és kattintson a **Tallóz** gombra a könyvtár tartalmának megtekintéséhez, hogy kiválaszthassa az aláírásra szánt objektumokat.

   Megjegyzés: Az objektum nevét per (slash) jellel kell kezdeni, vagy hibára számíthat. Bizonyos dzsóker karaktereket is használhat az aláírásra szánt alkönyvtár egy részének leírására. Ilyen karakter a csillag (*****), amely *bármennyi karaktert is jelenthet*, és a kérdőjel (**?**), amely *egyetlen tetszőleges karaktert jelent*. Például, az adott alkönyvtár összes objektumának aláírásához gépelje be a /alkönyvtár/* kifejezést. Az adott alkönyvtár összes programjának aláírásához gépelje be a /QSYS.LIB/QGPL.LIB/*.PGM kifejezést. Az ilyen dzsóker karaktereket csak az elérési útvonalnév utolsó részében használhatja, például az /alkönyvtár*/fájlnév hibaüzenetet eredményez. Ha a Tallóz funkcióval kívánja megtekinteni a könyvtár vagy a katalógus tartalmának listáját, a dzsóker karaktert az elérési útvonalnév részeként kell beírni, mielőtt rákattintana a **Tallóz** gombra.
7. Válassza ki a feldolgozási beállításokat, amelyeket alkalmazni akar a kiválasztott objektum vagy objektumok aláírásánál, és kattintson a **Folytatásra**.

   Megjegyzés: Ha úgy dönt, hogy vár a feladat eredményére, az eredményfájl közvetlenül a böngészőben jelenik meg. Az aktuális feladat eredménye az eredményfájl végéhez van hozzáfűzve. Következésképpen, a fájl tartalmazhatja korábbi feladatok eredményeit is, az aktuális feladatok eredményein túlmenően. A fájl dátum mezője révén határozhatja meg, hogy a fájl mely sorai tartoznak az aktuális feladathoz. A dátum mező YYYYMMDD formátumú. A fájl első mezője lehet üzenet ID (ha hiba történt az objektum feldolgozása közben) vagy dátum mező (a feladat feldolgozását jelző dátum).
8. Adja meg a fájl teljes elérési útvonalát és nevét, amelyet az objektum aláíró művelet eredményeinek tárolására használ, majd kattintson a **Folytatás** gombra. Vagy írja be az alkönyvtár helyét, és kattintson a **Tallóz** gombra a könyvtár tartalmának megtekintéséhez, hogy kiválaszthassa a feladat eredményeinek tárolására szolgáló fájlt. A megjelenő üzenet azt jelzi, hogy az objektumok aláírására szolgáló feladat elküldésre került. A feladat eredményeinek megtekintéséhez nézze meg a **QOBJSGNBAT** feladatot a naplóban.

Ahhoz, hogy saját maga vagy mások ellenőrizni tudják az aláírásokat, exportálja a szükséges igazolásokat egy fájlba, majd vigye át a fájlt az iSeries B szerverre. Hajtsa végre az aláírás ellenőrzéssel kapcsolatos összes konfigurálási feladatot is az iSeries B szerveren, mielőtt átviszi az aláírt program objektumokat az iSeries B szerverre. Az aláírás ellenőrzéssel kapcsolatos konfigurálást be kell fejezni ahhoz, hogy az aláírásokat sikeresen ellenőrizze, amikor visszaállítja az aláírt objektumokat az iSeries B szerveren.

6. lépés: Igazolások exportálása az aláírás ellenőrzés engedélyezéséhez az iSeries B szerveren

Az objektum tartalom sértetlenségének védelme érdekében történő aláírás megköveteli, hogy saját maga és mások is ellenőrizzék az aláírás hitelességét. Ha az objektum aláírásokat ugyanazon a rendszeren ellenőrzi, amely aláírta azokat (iSeries A), akkor a DCM segítségével hozza létre a *SIGNATUREVERIFICATION igazolás tárolót. Az igazolás tárolónak tartalmaznia kell az objektum aláíró igazolás és a CA igazolás egy-egy példányát is, mégpedig arra a CA-ra vonatkozóan, amelyik kiadta az aláíró igazolást.

Ahhoz, hogy mások ellenőrizni tudják az aláírást, juttassa el nekik annak az igazolásnak egy példányát, amely aláírta az objektumot. Amikor Helyi igazolási hatóságot (CA) használ fel az igazolás kiadásához, a Helyi CA igazolás egy példányát kell eljuttatnia az érdekelteknek.

Kövesse az alábbi lépéseket, ha az objektum aláírásokat ugyanazon a rendszeren ellenőrzi, amely aláírta az objektumokat (iSeries A ebben a forgatókönyvben):

1. A navigációs kereten válassza az **Új igazolás tároló létrehozását**, majd a ***SIGNATUREVERIFICATION** igazolás tárolót létrehozás céljából.
2. Az **Igen** gomb kiválasztásával másolja át a meglévő objektum aláíró igazolásokat az új igazolás tárolóba aláírás ellenőrző igazolásokként.
3. Adjon meg egy jelszót az új igazolás tárolóra, és kattintson a **Folytatásra**, hogy létrehozza az igazolás tárolót. Most a DCM segítségével ellenőrizheti az objektum aláírásokat ugyanazon a rendszeren, amelyet az objektumok aláírásához használt.

Kövesse az alábbi lépéseket, amikor a DCM segítségével exportálja a Helyi CA igazolás egy példányát, valamint az objektum aláíró igazolás egy példányát aláírás ellenőrző igazolásként, ami által ellenőrizheti az objektum aláírásokat egy másik rendszeren (iSeries B):

1. A navigációs kereten válassza az **Igazolások kezelése**, majd utána az **Igazolás exportálása** feladatot.
2. Válassza az **Igazolási hatóságot (CA)**, és kattintson a **Folytatásra** az exportálásra szánt CA igazolások felsorolásának megjelenítéséhez.
3. Válassza ki a korábban létrehozott Helyi CA igazolást a listából, és kattintson az **Export** gombra.
4. Exportálási célként adjon meg **Fájlt**, és kattintson a **Folytatásra**.
5. Adja meg az exportált Helyi CA igazolás teljes elérési útvonalát és fájlnevét, majd kattintson a **Folytatás** gombra az igazolás exportálásához.
6. Kattintson az **OK** gombra az Exportálás jóváhagyása lap megjelenítéséhez. Most exportálhatja az objektum aláíró igazolás egy példányát.
7. Válassza újra az **Igazolás exportálása** feladatot.
8. Válassza az **Objektum aláírást** az exportálható objektum aláíró igazolások listájának megjelenítéséhez.
9. Válassza ki a megfelelő objektum aláíró igazolást a listából, és kattintson az **Export** gombra.
10. Célként válasszon ki **Fájlt, mint aláírás ellenőrző igazolást**, és kattintson a **Folytatásra**.
11. Adja meg az aláírás ellenőrző igazolás teljes elérési útvonalát és fájlnevét, majd kattintson a **Folytatás** gombra az igazolás exportálásához.

Most átviheti ezeket a fájlokat az iSeries végpont rendszerekre, ahol ellenőrizni kívánja az adott igazolással létrehozott aláírásokat.

7. lépés: Igazolás fájlok átvitele a társaság nyilvános iSeries B szerverére

Az iSeries A szerveren létrehozott igazolás fájlokat át kell vinni a forgatókönyvben nyilvános webszerverként működő iSeries B szerverre, mielőtt konfigurálhatná őket az aláírt objektumok ellenőrzésére. Több különböző módszert is használhat az igazolás fájlok átvitelére. Például, használhatja a Fájlátviteli protokolt (FTP) vagy a Kezelőközpont csomag terjesztési funkcióját a fájlok eljuttatásához.

8. lépés: Aláírás ellenőrzési feladatok - *SIGNATUREVERIFICATION igazolás tároló létrehozása

Ahhoz, hogy ellenőrizhesse az objektum aláírásokat az iSeries B szerveren (a társaság nyilvános webszervere), az iSeries B szerver *SIGNATUREVERIFICATION igazolás tárolójában ott kell lenni a megfelelő aláírás ellenőrző igazolás egy példányának. Mivel, az objektumok aláírásához Helyi CA által kibocsátott igazolást használt, ezért az igazolás tárolónak tartalmaznia kell a Helyi CA igazolás egy példányát.

A *SIGNATUREVERIFICATION igazolás tároló létrehozásához kövesse ezeket a lépéseket:

1. Indítsa el a DCM funkciót.
2. A Digitális igazolás kezelő (DCM) navigációs keretén válassza ki az **Új igazolás tároló létrehozását**, majd a ***SIGNATUREVERIFICATION** igazolás tárolót létrehozás céljából.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban a DCM használata során, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
3. Adjon meg egy jelszót az új igazolás tárolóra, és kattintson a **Folytatásra**, hogy létrehozza az igazolás tárolót. Most importálhatja az igazolásokat a tárolóba, amelyek révén ellenőrizheti az objektum aláírásokat.

9. lépés: Aláírás ellenőrzési feladatok - igazolások importálása

Ahhoz, hogy ellenőrizze egy objektumon az aláírást, a *SIGNATUREVERIFICATION tárolónak tartalmaznia kell az aláírás ellenőrző igazolás egy példányát. Ha az aláírási igazolás magán igazolás, akkor az igazolás tárolónak tartalmaznia kell az aláírási igazolást kiadó Helyi igazolási hatóság (CA) igazolásának egy példányát is. A tárgyalt forgatókönyvben mindkét igazolást egy fájlba exportálta, és ezt a fájlt vitte át minden egyes iSeries végpont rendszerre.

Kövesse az alábbi lépéseket, amikor importálja ezeket az igazolásokat a *SIGNATUREVERIFICATION tárolóba:

1. A DCM navigációs keretén kattintson az **Igazolás tároló választása**, majd a ***SIGNATUREVERIFICATION** elemre, mint megnyitandó igazolás tárolóra.
2. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatásra**.
3. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
4. A feladatlistából válassza az **Igazolás importálását**.
5. Válassza az **Igazolási hatóságot (CA)** az igazolás típusának, és kattintson a **Folytatásra**.

   Megjegyzés: A Helyi CA igazolást a magán aláírás ellenőrző igazolást megelőzően kell importálni, egyébként az aláírás ellenőrző igazolás importálása meghiúsul.
6. Adja meg a CA igazolás fájl teljes elérési útvonalát és nevét, majd kattintson a **Folytatás** gombra. Egy üzenet jelenik meg, ami vagy megerősíti, hogy az importálási folyamat sikeresen megtörtént, vagy hibainformációkat közöl, ha a folyamat hibát észlelt.
7. Válassza újra az **Igazolás importálása** feladatot.
8. Az igazolás típusának válassza ki az **Aláírás ellenőrzést**, és kattintson a **Folytatásra**.

9. Adja meg az aláírás ellenőrző igazolás fájl teljes elérési útvonalát és nevét, majd kattintson a **Folytatás** gombra. Egy üzenet jelenik meg, ami vagy megerősíti, hogy az importálási folyamat sikeresen megtörtént, vagy hibainformációkat közöl, ha a folyamat hibát észlelt.

Ezután a DCM segítségével ellenőrizheti az objektumok aláírását az iSeries B szerveren, amelyeket az iSeries A szerveren hozott létre.

10. lépés: Aláírás ellenőrzési feladatok - aláírás ellenőrzése program objektumokon

Kövesse az alábbi lépéseket, amikor DCM segítségével ellenőrzi az átvitt program objektumokon lévő aláírásokat:

1. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SIGNATUREVERIFICATION** elemre, az igazolás tároló megnyitása céljából.
2. Írja be a *SIGNATUREVERIFICATION igazolás tárolóra vonatkozó jelszót, és kattintson a **Folytatásra**.
3. Miután frissül a navigációs keret, válassza az **Aláírható objektumok kezelését** a feladatlista megjelenítéséhez.
4. A feladatok listájából válassza ki az **Objektum aláírások ellenőrzését**, hogy megadja azoknak az objektumoknak a helyét, amelyeknél ellenőrizni kívánja az aláírásokat.
5. Az előbukkanó mezőbe írja be az objektum vagy az objektumok könyvtárának teljesen megadott útvonalnevét, amelyeknél ellenőrizni kívánja az aláírást, és kattintson a **Folytatásra**. Vagy írja be az alkönyvtár helyét, és kattintson a **Tallóz** gombra a könyvtár tartalmának megtekintéséhez, hogy kiválaszthassa az aláírás ellenőrzésre szánt objektumokat.

   Megjegyzés: Bizonyos dzsóker karaktereket is használhat az ellenőrzésre szánt alkönyvtár egy részének leírására. Ilyen karakter a csillag (*****), amely *bármennyi karaktert is jelenthet*, és a kérdőjel (**?**), amely *egyetlen tetszőleges karaktert jelent*. Például, az adott alkönyvtár összes objektumának aláírásához gépelje be a /alkönyvtár/* kifejezést. Az adott alkönyvtár összes programjának aláírásához gépelje be a /QSYS.LIB/QGPL.LIB/*.PGM kifejezést. Az ilyen dzsóker karaktereket csak az elérési útvonalnév utolsó részében használhatja, például az /alkönyvtár*/fájlnév hibaüzenetet eredményez. Ha a Tallóz funkcióval kívánja megtekinteni a könyvtár vagy a katalógus tartalmának listáját, a dzsóker karaktert az elérési útvonalnév részeként kell beírni, mielőtt rákattintana a **Tallóz** gombra.
6. Válassza ki a feldolgozási beállításokat, amelyeket alkalmazni akar a kiválasztott objektum vagy objektumok aláírásának ellenőrzéséhez, és kattintson a **Folytatásra**.

   Megjegyzés: Ha úgy dönt, hogy vár a feladat eredményére, az eredményfájl közvetlenül a böngészőben jelenik meg. Az aktuális feladat eredménye az eredményfájl végéhez van hozzáfűzve. Következésképpen, a fájl tartalmazhatja korábbi feladatok eredményeit is, az aktuális feladatok eredményein túlmenően. A fájl dátum mezője révén határozhatja meg, hogy a fájl mely sorai tartoznak az aktuális feladathoz. A dátum mező YYYYMMDD formátumú. A fájl első mezője lehet üzenet ID (ha hiba történt az objektum feldolgozása közben) vagy dátum mező (a feladat feldolgozását jelző dátum).
7. Adja meg a fájl teljes elérési útvonalát és nevét, amelyet az aláírás ellenőrző művelet eredményeinek tárolására használ, majd kattintson a **Folytatás** gombra. Vagy írja be az alkönyvtár helyét, és kattintson a **Tallóz** gombra a könyvtár tartalmának megtekintéséhez, hogy kiválaszthassa a feladat eredményeinek tárolására szolgáló fájlt. A megjelenő üzenet azt jelzi, hogy az objektumok aláírásának ellenőrzésére szolgáló feladat elküldésre került. A feladat eredményeinek megtekintéséhez nézze meg a **QOBJSGNBAT** feladatot a naplóban.

Forgatókönyv: Objektumok aláírása és objektum aláírások ellenőrzése API-k segítségével

Helyzet

Vállalata (MyCo, Inc.) iSeries üzleti partner, amely alkalmazásokat fejleszt az ügyfelek számára. A társaság szoftver fejlesztőjeként felelős az alkalmazások csomagolásáért a vásárlóknak történő terjesztés érdekében. Jelenleg programokat használ az alkalmazás csomagolásához. A vásárlók megrendelhetik kompakt lemez (CD-ROM) formájában, illetve ellátogathatnak a Webhelyre, és letölthetik onnan az alkalmazást.

Ismereteit ipari újságokkal és különösen biztonsági kiadványokkal tartja szinten. Következésképpen jól tudja, hogy a vásárlók jogosan aggódnak az általuk megkapott vagy letöltött programok forrása és tartalma iránt. Sokszor megtörténik az, hogy a vásárlók megkapják vagy letöltik a terméket egy megbízhatónak vélt helyről, amiről aztán kiderül, hogy az adott terméknek nem valódi forráshelye. Időnként ez azzal a zavaró eredménnyel végződik, hogy a vásárló egy másik terméket telepít, és nem az elvártat. Néha kiderül a telepített termékről, hogy egy rosszindulatú program, vagy megváltoztatja és tönkreteszi a rendszert.

Az ilyen típusú problémák ugyan nem általánosak az iSeries vásárlók esetén, mégis biztosítani szeretné őket arról, hogy a társaságától beszerzett alkalmazások valóban a társaságától származnak. Az alkalmazások sértetlenségének ellenőrzésével egy olyan módszert is biztosítani akar a számukra, hogy eldönthessék, megváltozott-e az alkalmazások tartalma a telepítés előtt.

Vizsgálatai alapján úgy döntött, hogy az OS/400 objektum aláíró funkcióját felhasználva teljesíti ilyen irányú biztonsági céljait. Az alkalmazások digitális aláírása lehetővé teszi a vásárlók számára annak ellenőrzését, hogy az általuk megkapott vagy letöltött alkalmazás legitim forrása valóban az Ön társasága. Mivel az alkalmazásokat pillanatnyilag programozottan csomagolja, úgy határoz, hogy API-k segítségével könnyedén hozzáadhatja az objektum aláírási műveletet a meglévő csomagolási folyamathoz. Másrészt úgy dönt, hogy nyilvános igazolást használ fel az objektumok aláírásához, amivel átláthatóvá teszi az aláírás ellenőrzési folyamatot a vásárlók számára a termék telepítésekor.

Az alkalmazási csomagba belefoglalja az objektum aláírására használt digitális igazolás egy példányát. Amikor a vásárló beszerzi az alkalmazási csomagot, az igazolás nyilvános kulcsával ellenőrizheti az alkalmazáson található aláírást. Ez a folyamat lehetővé teszi a vásárlónak, hogy azonosítsa és ellenőrizze az alkalmazás forrását, és arról is meggyőződhessen, hogy az alkalmazás objektum tartalma nem módosult-e az aláírás óta.

A példa hasznos tájékoztatást nyújt az objektumok programozott aláírására vonatkozó lépésekről, amit a mások számára fejlesztett és csomagolt alkalmazásoknál használ.

A forgatókönyv előnyei

Ez a forgatókönyv a következő előnyökkel jár:

- A csomagoláshoz és az objektumok programozottan történő aláírásához használt API-k csökkentik a biztonság megvalósításához szükséges időt.
- Az objektumok csomagoláskori aláírásához használt API-k csökkentik azon lépések számát, melyeket végre kell hajtani az objektumok aláírásához, mivel az aláírási művelet a csomagolási folyamat része.
- Az objektumokból álló csomag aláírása révén még könnyebben meghatározhatja, hogy megváltoztak-e az objektumok az aláírás után. Ez csökkenthet bizonyos hibakeresési feladatokat, melyeket végrehajt a jövőben a vásárló számára az alkalmazási problémák követéséhez.
- Ha az objektumok aláírásához egy jól ismert nyilvános Igazolási hatóságtól (CA) kapott igazolást használ, akkor a termék telepítési programjában lévő kilépési program részeként használhatja az Add Verifier API-t. Az API használatával automatikusan hozzáadhatja a vásárló rendszeréhez az alkalmazás aláírásához használt nyilvános igazolást. Ez biztosítja, hogy az aláírás ellenőrzés átlátható legyen a vásárló számára.

Célok

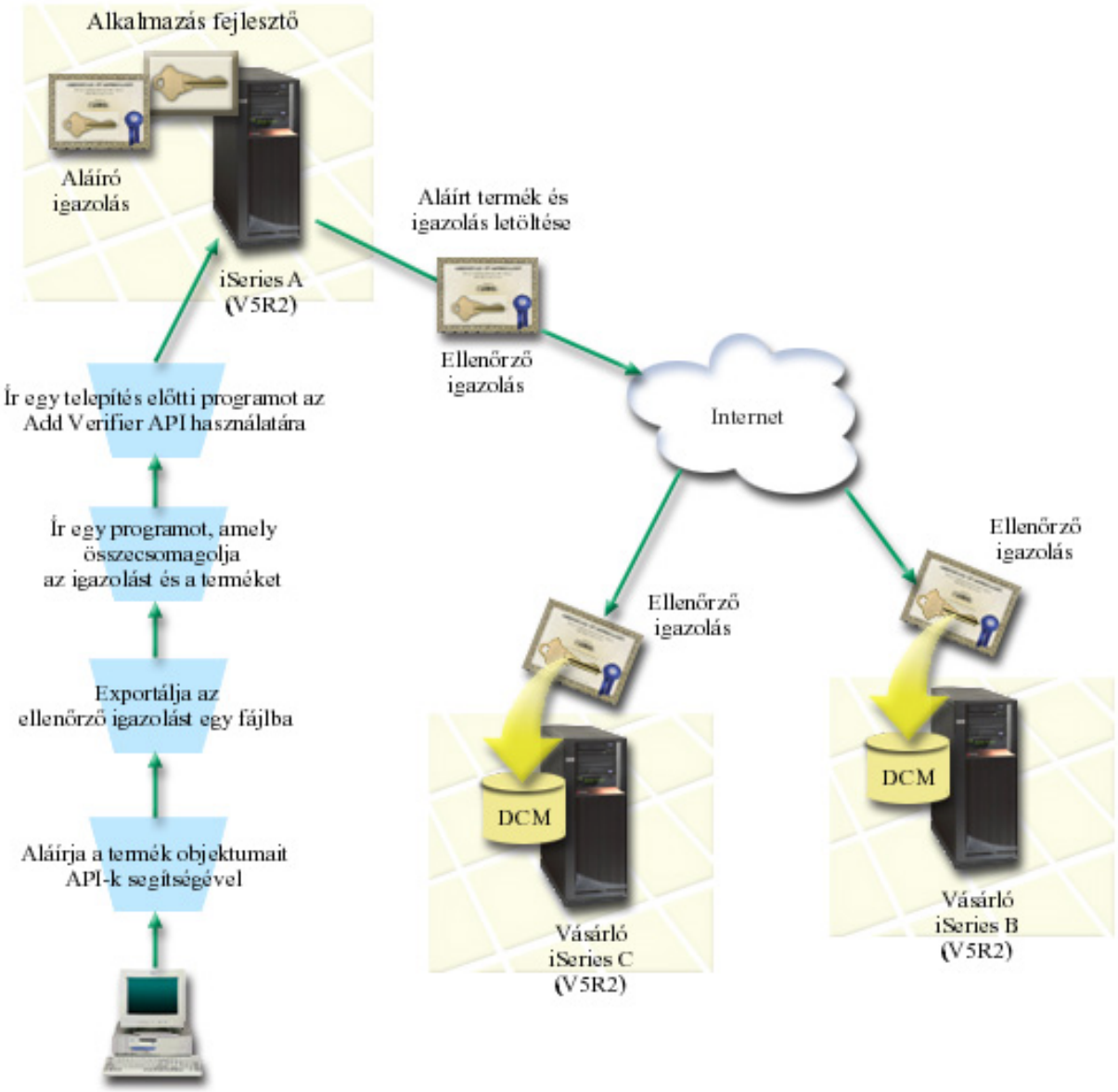
Ebben a forgatókönyvben a MyCo, Inc. programozottan kívánja aláírni az alkalmazásokat, amelyeket a cég csomagol és terjeszt vásárlóinak. A MyCo, Inc. alkalmazás előállítással foglalkozó fejlesztőjeként pillanatnyilag programozottan csomagolja a társaság alkalmazásait a vásárlóknak való terjesztéshez. Következésképpen, iSeries API-k segítségével akarja aláírni az alkalmazásokat, és a vásárlók iSeries szerverével is programozottan kívánja ellenőriztetni az aláírást a termék telepítése során.

A forgatókönyv céljai a következők:

- A társaság termelés fejlesztőjének kell aláírni az objektumokat a Sign Object API segítségével, a jelenlegi programozott csomagolási folyamat részeként.
- Az alkalmazásokat nyilvános igazolással kell aláírni, hogy az aláírás ellenőrzési folyamat átlátható legyen a vásárló számára a termék telepítési folyamata során.
- A társaságnak használni kell az iSeries API-kat ahhoz, hogy programozottan hozzáadja a szükséges aláírás ellenőrző igazolást a vásárló iSeries szerverének *SIGNATUREVERIFICATION igazolás tárolójához. A társaságnak programozottan létre kell hoznia az igazolás tárolót a vásárló iSeries szerverén a termék telepítési folyamatának részeként, ha még nem létezik.
- A vásárlónak lehetőséget kell biztosítani, hogy könnyedén ellenőrizze a társaság alkalmazásán lévő digitális aláírásokat. A vásárlóknak úgy kell ellenőrizni az aláírást, hogy meg tudjanak győződni az aláírt alkalmazás forrásáról és hitelességéről, valamint az aláírás óta esetlegesen bekövetkezett változtatásokról.

Részletek

Az alábbi ábra szemlélteti az objektum aláírási és az aláírás ellenőrzési folyamatot, amely a forgatókönyv megvalósítását szolgálja:



Az ábra a forgatókönyvhöz tartozó következő pontokat szemlélteti:

Központi rendszer (iSeries A)

- Az iSeries A szerveren OS/400 Verzió 5 Változat 2 (V5R2) fut.
- Az iSeries A szerveren fut az alkalmazás fejlesztő termékcsomagoló programja.
- Az iSeries A szerveren telepítve van a Cryptographic Access Provider 128-bit for iSeries (5722–AC3) termék.
- Az iSeries A szerveren telepítve és konfigurálva van a Digital Certificate Manager (OS/400 34-es opció), és az IBM HTTP Server (5722–DG1) termék.
- Az iSeries A szerver a társaság termékeinek elsődleges objektum aláíró rendszere. A következő feladatok végrehajtásával teljesítheti a vásárlóknak szánt termékobjektumok aláírását az iSeries A szerveren:
  1. A társaság termékeinek aláírása API-k segítségével.
  2. Az aláírás ellenőrző igazolás exportálása egy fájlba a DCM segítségével, hogy a vásárlók ellenőrizhessék az aláírt objektumokat.

3. Egy program írása, amellyel hozzáadja az ellenőrző igazolást az aláírt termékhez.
4. Egy telepítés előtti kilépési program írása a termék számára, amely használja az Add Verifier API-t. Ez az API lehetővé teszi, hogy a termék telepítési folyamata programozottan hozzáadja az ellenőrző igazolást a vásárló iSeries szerverén lévő *SIGNATUREVERIFICATION igazolás tárolóhoz (iSeries B és C).

Vásárló iSeries szerverei (B és C)

- Az iSeries B szerveren OS/400 Verzió 5 Változat 2 (V5R2) fut.
- Az iSeries C szerveren OS/400 Verzió 5 Változat 2 (V5R2) fut.
- Az iSeries B és C szerveren telepítve és konfigurálva van a Digital Certificate Manager (34-es opció), és az IBM HTTP Server (5722–DG1) termék.
- Az iSeries B és C vásárol és letölt egy alkalmazást a fejlesztő társaság webhelyéről (a társaságé az iSeries A szerver).
- Az iSeries B és C megkapja a MyCo aláírás ellenőrző igazolásának egy példányát, amikor a MyCo alkalmazás telepítési folyamata létrehozza a *SIGNATUREVERIFICATION igazolás tárolót minden egyes vásárló iSeries szerverén.

Előfeltételek és feltételezések

A forgatókönyv a következő előfeltételektől és feltételezésektől függ:

1. Az iSeries szerverek kielégítik a Digitális igazolás kezelő (DCM) telepítésének és használatának követelményeit.

   Megjegyzés: A DCM telepítésével és használatával kapcsolatos előfeltételek nem kötelezőek a vásárlók számára (iSeries B és C a forgatókönyvben). A termék telepítési folyamatának részeként az Add Verifier API ugyan létrehozza a *SIGNATUREVERIFICATION igazolás tárolót (ha szükséges), de az alapértelmezett jelszóval hozza létre. A vásárlóknak kell megváltoztatni (DCM segítségével) az alapértelmezett jelszót, hogy védjék az igazolás tárolót a jogosulatlan hozzáféréstől.
2. Senki sem konfigurálta vagy használta korábban az iSeries szervereken lévő DCM-eket.
3. Az összes iSeries szerver a legmagasabb szintű telepített Cryptographic Access Provider 128-bit licencprogrammal (5722-AC3) rendelkezik.
4. A Verify object signatures during restore (QVFYOBJRST) rendszerváltozó alapértéke az összes forgatókönyvben 3 az iSeries szervereken, és nem is változik ez a beállítás. Az alapértelmezett beállítás garantálja, hogy a szerver ellenőrizheti az objektumok aláírásait, amikor visszaállítja az aláírt objektumokat.
5. Az iSeries A szerver hálózati rendszergazdájának *ALLOBJ különleges jogosultsággal kell rendelkeznie az objektumok aláírásához, vagy a felhasználói profilnak kell jogosultnak lenni az objektum aláíró alkalmazáshoz.
6. A rendszergazdának vagy valaki másnak (beleértve a programot is), aki létrehozza az igazolás tárolót a DCM-ben, *SECADM és *ALLOBJ különleges jogosultsággal kell rendelkeznie.
7. A rendszergazdáknak vagy másoknak az összes többi iSeries szerveren *AUDIT különleges jogosultsággal kell rendelkezniük az objektum aláírások ellenőrzéséhez.

Feladat lépések

Az összes alábbi feladatot hajtsa végre az iSeries A szerveren az objektumok aláírásához a forgatókönyv leírása szerint:

1. Hajtsa végre az előfeltételként megadott lépéseket, amelyek révén telepíti és konfigurálja az összes szükséges iSeries terméket.

2. A DCM segítségével hozzon létre igazolás kérést, amely révén beszerezheti az objektum aláíró igazolást egy jól ismert nyilvános Igazolási hatóságtól (CA).
3. A DCM segítségével hozza létre egy objektum aláíró alkalmazás definícióját.
4. A DCM segítségével importálja az objektum aláíró igazolást, és rendelje hozzá az objektum aláíró alkalmazás definíciójához.
5. A DCM segítségével exportálja az objektum aláíró igazolást aláírás ellenőrző igazolásként, amely révén a vásárlók ellenőrizhetik az alkalmazás objektumain lévő aláírásokat.
6. Az alkalmazás csomagoló program átírásával foglalja bele az aláírás ellenőrző igazolást tartalmazó fájlt a termék részeként, és a Sign Object API segítségével írja alá az alkalmazást, amikor a vásárlók számára csomagolja.
7. Hozzon létre egy telepítés előtti kilépési programot, amely az Add Verifier API-t használja az alkalmazás csomagolási folyamat részeként. Ez a kilépési program lehetővé teszi, hogy létrehozza a *SIGNATUREVERIFICATION igazolás tárolót, és hozzáadja a szükséges aláírás ellenőrző igazolást a vásárló iSeries szerveréhez a termék telepítése során.
8. A DCM révén töröltesse a vásárlókkal a *SIGNATUREVERIFICATION igazolás tároló alapértelmezett jelszavát az iSeries szervereiken.

Konfigurálási részletek

Hajtsa végre a következő feladatokat, ha az OS/400 API-k segítségével objektumokat ír alá a forgatókönyvben leírtak szerint.

1. lépés: Előfeltételt jelentő összes feladat végrehajtása

Végre kell hajtani az összes előfeltételt jelentő feladatot, amely révén telepíti és konfigurálja az összes szükséges iSeries terméket, mielőtt a forgatókönyv megvalósításához tartozó, jellemző konfigurálási feladatokat végrehajthatná.

2. lépés: Igazolás beszerzése egy jól ismert nyilvános CA-tól DCM segítségével

Ez a forgatókönyv feltételezi, hogy korábban nem használt Digitális igazolás kezelőt (DCM) igazolások létrehozásához és kezeléséhez. Következésképpen, létre kell hozni az *OBJECTSIGNING igazolás tárolót az objektum aláíró igazolás létrehozásának folyamata során. A létrehozott igazolás tároló biztosítja azokat a feladatokat, amelyek az objektum aláíró igazolások létrehozásához és kezeléséhez szükségesek. Ahhoz, hogy beszerezze az igazolást egy jól ismert nyilvános Igazolási hatóságtól (CA), a DCM segítségével hozza létre az azonosító információkat, valamint a nyilvános-magán kulcspárokat az igazoláshoz, és küldje el ezeket a CA-nak.

Hajtsa végre az alábbi lépéseket a jól ismert CA számára szükséges igazolás kérési információk létrehozásához, hogy beszerezhesse az objektum aláíró igazolást:

1. Indítsa el a DCM funkciót.
2. A DCM navigációs keretén válassza ki az **Új igazolás tároló létrehozását** a feladat elindításához, és töltse ki az űrlapok sorozatát. Ezek az űrlapok végigvezetik az igazolás tároló és egy igazolás (amit objektumok aláírásához használhat) létrehozási folyamatán.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
3. A létrehozandó igazolás tárolónak válassza ki az ***OBJECTSIGNING** beállítást, és kattintson a **Folytatásra**.
4. Válassza ki az **Igen** választ arra, hogy az *OBJECTSIGNING igazolás tároló létrehozásának részeként hozzon-e létre igazolást, majd kattintson a **Folytatásra**.

5. Válassza a **VeriSign vagy egyéb Internet Igazolási hatóságot (CA)** az új igazolás aláírójának, és kattintson a **Folytatásra**, hogy megjelenítse az űrlapot, amelyen megadhatja az új igazolás azonosító információit.
6. Töltse ki az űrlapot, és kattintson a **Folytatásra** a jóváhagyási oldal megjelenítéséhez. Ez a jóváhagyási oldal megjeleníti az igazoláskérési adatokat, amelyeket eljuttatott a nyilvános Igazolási hatósághoz (CA), ami kiadta az igazolást. Az Igazolás aláírási kérés (CSR) adatok a nyilvános kulcsból és egyéb információkból állnak, amelyeket megadott az új igazolás számára.
7. Gondosan másolja majd illessze be a CSR adatokat az igazoláskérési űrlapra, vagy egy külön fájlba, amelyet a nyilvános CA megkövetel az igazolás kéréséhez. Az összes CSR adatra szükség van, beleértve a Kezdés (Begin) és az Új igazoláskérés vége (End New Certificate Request) sorokat is. Ha kilép a lapról, az adatok elvesznek, és nem tudja helyreállítani őket.
8. Küldje el a jelentkezési lapot vagy a fájlt az adott CA számára, amelyet kiválasztott arra, hogy kiadja és aláírja az igazolását.
9. Meg kell várni, amíg a CA visszaküldi az aláírt, komplett igazolást, mielőtt folytatná a forgatókönyv következő feladatának lépéseivel.

3. lépés: Objektum aláíró alkalmazás definíciójának létrehozása

Most, hogy elküldte igazolás kérését a jól ismert nyilvános CA-nak, a Digitális igazolás kezelővel (DCM) adja meg az objektum aláíró alkalmazást, amelyet használni fog az objektumok aláírására. Az alkalmazás definíciónak nem kell hivatkozni egy tényleges alkalmazásra. A létrehozott alkalmazás definíció írja le az aláírni kívánt objektumcsoport típusát. Olyan definícióra van szükség, amely révén az alkalmazás azonosítót (ID) társíthatja az igazolással, hogy engedélyezze az aláírási folyamatot.

Kövesse az alábbi lépéseket, ha a DCM segítségével objektum aláíró alkalmazás definícióját hozza létre:

1. A navigációs kereten kattintson az **Igazolás tároló választására**, majd válassza ki a megnyitandó ***OBJECTSIGNING** igazolás tárolót.
2. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatásra**.
3. A navigációs kereten válassza az **Alkalmazások kezelését** a feladatlista megjelenítéséhez.
4. Válassza ki az **Alkalmazás hozzáadását** a feladatlistából, hogy megjelenítse az alkalmazás megadására szolgáló űrlapot.
5. Töltse ki az űrlapot, és kattintson a **Hozzáadásra**.

Amint visszakapja az aláírt igazolást a CA-tól, hozzárendelheti a létrehozott alkalmazáshoz.

4. lépés: Aláírt nyilvános igazolás importálása és hozzárendelése az objektum aláíró alkalmazáshoz

Kövesse az alábbi lépéseket, amikor importálja az igazolást, és hozzárendeli az alkalmazáshoz az objektum aláírás engedélyezése céljából:

1. Indítsa el a DCM funkciót.
2. A navigációs kereten kattintson az **Igazolás tároló választására**, majd válassza ki a megnyitandó ***OBJECTSIGNING** igazolás tárolót.
3. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatásra**.
4. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
5. A feladatlistából válassza az **Igazolás importálását**, ami révén elkezdődik az aláírt igazolás importálási folyamata az igazolás tárolóba.

Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.

6. Válassza az **Igazolás hozzárendelését** az **Igazolások kezelése** feladatlistából az aktuális igazolás tárolóban található igazolások listájának megjelenítéséhez.
7. Válassza ki az igazolást a listából, és kattintson a **Hozzárendelés alkalmazásokhoz** feladatra, hogy megjelenítse az aktuális igazolás tárolóhoz tartozó alkalmazás definíciók listáját.
8. Válassza ki az alkalmazást a listából, és kattintson a **Folytatásra**. A lapon vagy egy nyugtázó üzenet jelenik meg a hozzárendelés kiválasztásáról, vagy egy hibaüzenet, ha probléma fordult elő.

Amikor végrehajtja ezt a feladatot, készen áll az alkalmazások és az objektumok aláírására az OS/400 API-k segítségével. Azonban ahhoz, hogy biztosan ellenőrizni tudja az aláírásokat, exportálja az igazolásokat egy fájlba, és vigye át őket az összes olyan iSeries szerverre, amely telepíti az aláírt alkalmazásokat. A vásárlók iSeries szerverei ezután ellenőrizni tudják az igazolás segítségével az alkalmazáson lévő aláírást a telepítés során. Az alkalmazás telepítőprogramjának részeként az Add Verifier API segítségével végezze el az aláírás ellenőrzéshez szükséges konfigurálást a vásárlók számára. Például, létrehozhat egy telepítés előtti kilépési programot, hogy hívja az Add Verifier API-t, amely konfigurálja a vásárló iSeries szerverét.

5. lépés: Igazolások exportálása az aláírás ellenőrzés engedélyezéséhez más iSeries szervereken

Az objektumok aláírása megköveteli, hogy saját maga és mások is ellenőrizzék az aláírás hitelességét, és ezzel meghatározza, hogy megváltoztak-e az aláírt objektumok. Ha az objektum aláírásokat ugyanazon a rendszeren ellenőrzi, amely aláírta az objektumokat, akkor a DCM segítségével hozza létre a *SIGNATUREVERIFICATION igazolás tárolót. Az igazolás tárolónak tartalmaznia kell az objektum aláíró igazolás és a CA igazolás egy-egy példányát is, mégpedig arra a CA-ra vonatkozóan, amelyik kiadta az aláíró igazolást.

Ahhoz, hogy mások ellenőrizni tudják az aláírást, juttassa el nekik annak az igazolásnak egy példányát, amely aláírta az objektumot. Amikor Helyi igazolási hatóságot (CA) használ fel az igazolás kiadásához, a Helyi CA igazolás egy példányát kell eljuttatnia az érdekelteknek.

Kövesse az alábbi lépéseket, ha az objektum aláírásokat ugyanazon a rendszeren ellenőrzi, amely aláírta az objektumokat (iSeries A ebben a forgatókönyvben):

1. A navigációs kereten válassza az **Új igazolás tároló létrehozását**, majd a ***SIGNATUREVERIFICATION** igazolás tárolót létrehozás céljából.
2. Az **Igen** gomb kiválasztásával másolja át a meglévő objektum aláíró igazolásokat az új igazolás tárolóba aláírás ellenőrző igazolásokként.
3. Adjon meg egy jelszót az új igazolás tárolóra, és kattintson a **Folytatásra**, hogy létrehozza az igazolás tárolót. Most a DCM segítségével ellenőrizheti az objektum aláírásokat ugyanazon a rendszeren, amelyet az objektumok aláírásához használt.

Kövesse az alábbi lépéseket, amikor a DCM segítségével exportálja az objektum aláíró igazolás egy példányát aláírás ellenőrző igazolásként, ami által mások ellenőrizhetik az objektum aláírásokat:

1. A navigációs kereten válassza az **Igazolások kezelése**, majd utána az **Igazolás exportálása** feladatot.
2. Válassza az **Objektum aláírást** az exportálható objektum aláíró igazolások listájának megjelenítéséhez.
3. Válassza ki a megfelelő objektum aláíró igazolást a listából, és kattintson az **Export** gombra.
4. Célként válasszon ki **Fájlt, mint aláírás ellenőrző igazolást**, és kattintson a **Folytatásra**.
5. Adja meg az aláírás ellenőrző igazolás teljes elérési útvonalát és fájlnevét, majd kattintson a **Folytatás** gombra az igazolás exportálásához.

Most hozzáadhatja a fájlt az alkalmazás telepítési csomagjához, amelyet a termékhez készít. A telepítőprogram részeként az Add Verifier API segítségével hozzáadhatja az igazolást a vásárló *SIGNATUREVERIFICATION igazolás tárolójához. Az API létrehozza az igazolás tárolót, ha még nem létezik. Ezután a termék telepítőprogramja ellenőrizheti az alkalmazási objektumokon található aláírásokat, amikor visszaállítja őket az iSeries szervereken.

6. lépés: Csomagoló program frissítése iSeries API-k használatára az alkalmazás aláírása céljából

Most, hogy rendelkezik az alkalmazás csomaghoz hozzáadandó, aláírás ellenőrző igazolást tartalmazó fájllal, a Sign Object API segítségével szerkesztés vagy írás útján aláírhatja a termék könyvtárakat, amikor csomagolja őket a vásárlók számára.

Nézze át az alábbi példaprogramot, hogy jobban megértse a Sign Object API használatát az alkalmazás csomagoló program részeként. Ez a példaprogram részlet (C nyelven írt) nem egy teljes aláíró és csomagoló program - sokkal inkább egy olyan program egy szakaszára mutat példát, amely hívja a Sign Object API-t. Ha a példaprogram használata mellett dönt, változtassa meg igényei szerint. Biztonsági okokból az IBM azt javasolja, hogy egyéniesítse a példaprogramot, és ne az alapértelmezett értékeket használja.

Megjegyzés: Az IBM nem kizárólagos szerzői jogi engedélyt ad az összes példaprogramhoz, amelyekből saját igényei szerint szabott, hasonló funkciójú programokat generálhat. Az IBM az összes példaprogramot csupán szemléltetési célból nyújtja. Ezek a példák nem kerültek minden állapotban tesztelésre. Az IBM így nem tudja garantálni a megbízhatóságukat, szervizelhetőségüket, de még a programok funkcióit sem. Az itt található összes programot úgy kapja meg meg ″AHOGY VAN″, mindennemű jótállás nélkül. A jogsértés kizárására, a kereskedelmi értékesítésre vagy egy adott célra való alkalmasságra vonatkozó sugallt jótállást az IBM ugyancsak kifejezetten elutasítja.

Változtassa meg igénye szerint úgy a példaprogramot, hogy az megfelelően használja a Sign Object API-t a terméket csomagoló program részeként. Két paramétert adjon át a programnak: az aláírandó könyvtár nevét és az objektum aláíró alkalmazás ID nevét. Az alkalmazás ID neve kis/nagybetű érzékeny, a könyvtár neve nem. A felhasználó által írt program többször is hívhatja ezt a példaprogramot, ha a termék részeként több könyvtárat is aláír.

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* SZERZŐI JOG (C) IBM CORP. 2002                                   */
/*                                                                  */
/* Sign Object API egy vagy több könyvtár aláírásához               */
/*                                                                  */
/* Az API digitálisan aláírja az adott könyvtár összes objektumát   */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* A kiadvány programozási forráskódokat tartalmaz saját            */
/* használatra.  Ez a példaprogram nem került tesztelésre           */
/* minden körülmény között.  Az IBM így nem tudja garantálni        */
/* a megbízhatóságukat, szervizelhetőségüket, de még a programok    */
/* funkcióit sem.  Az itt található összes programot úgy kapja      */
/* meg "AHOGY VAN".  A jogsértés kizárására, a kereskedelmi         */
/* értékesítésre vagy egy adott célra való alkalmasságra vonatkozó  */
/* sugallt jótállást az IBM ugyancsak kifejezetten elutasítja. Az   */
/* IBM nem szervizeli ezeket a programokat és fájlokat.             */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Paraméterek:                                                     */
/*                                                                  */
/*  kar *   az aláírandó könyvtár neve                              */
/*  kar *   az alkalmazás ID neve                                   */
/*                                                                  */

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

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

    /* paraméterek:

       kar * könyvtár, amelynek objektumait kell aláírni,
       kar * aláíró alkalmazás azonosítója

     */

    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;    /* visszajelzések hibák esetén */


    /* ------------------------------------ */
    /* útvonalnév felépítése könyvtárnév alap.*/
    /* ------------------------------------ */
    memset(libname, '\00', 11); /* könyvtárnév inicializálása */
    for(lib_length = 0;
        ((*(argv[1] + lib_length) != ' ') &&
         (*(argv[1] + lib_length) != '\00'));
        lib_length++);
    memcpy(argv[1], libname, lib_length); /* könyvtárnév kitöltése */

    /* útvonalnév paraméter API híváshoz */
    sprintf(path_name, "/QSYS.LIB/%s.LIB/*", libname);
    path_length = strlen(path_name);

    /* --------------------------- */
    /* alkalmazás id hossz keresés   */
    /* --------------------------- */
    for(applid_length = 0;
        ((*(argv[2] + applid_length) != ' ') &&
         (*(argv[2] + applid_length) != '\00'));
        applid_length++);

    /* ------------------------------ */
    /* összes obj. aláír. a könyvtárban */
    /* ------------------------------ */
    QYDOSGNO  (path_name,             /* objektum útvonalnév  */
               &path_length,          /* útvonalnév hossza  */
               "OBJN0100",            /* formátumnév  */
               argv[2],               /* alkalmazás azonosító (ID) */
               &applid_length,        /* alkalmazás ID hossza  */
               "1",                   /* ismétlődő aláírás cseréje */
               multi_objects,         /* több objektum kezelésének
                                            módja           */
               &multiobj_length,      /* a használandó, több
                                          objektumból álló
                                          szerkezet hossza
                                       (0=nem több obj. szerk.) */
               &error_code);          /* hibakód  */



       return 0;

 }
```

7. lépés: Add Verifier API-t használó, telepítés előtti kilépési program létrehozása

Most, hogy programozott eljárása van az alkalmazás aláírásához, az alkalmazás telepítőprogramjának részét alkotó Add Verifier API segítségével létrehozhatja az eladásra szánt végső terméket. Például, a telepítés előtti kilépési program részeként használatos Add Verifier API garantálja azt, hogy az igazolás hozzáadódik az igazolás tárolóhoz az aláírt alkalmazási objektumok visszaállítása előtt. Ez lehetővé teszi a termék telepítőprogramjának, hogy ellenőrizze az alkalmazási objektumokon található aláírásokat, amikor visszaállítja őket a vásárló iSeries szerverén.

Megjegyzés: Biztonsági okokból az API nem teszi lehetővé az Igazolási hatóság (CA) igazolásának elhelyezését a *SIGNATUREVERIFICATION igazolás tárolóba. Amikor a CA igazolását hozzáadja az igazolás tárolóhoz, a rendszer az igazolások megbízható forrásának ismeri el a CA-t. Következésképpen, a rendszer a CA által kiadott igazolást úgy kezeli, mint amelyik megbízható forrásból ered. Ennek következtében, az API-val nem hozhat létre telepítési programot, amely elhelyezné a CA igazolást az igazolás tárolóba. A Digitális igazolás kezelőt kell ahhoz használni, hogy hozzáadja a CA igazolást az igazolás tárolóhoz. Így garantálja, hogy valaki kimondottan és kézi módon meghatározza, mely CA-kat tekintse a rendszer megbízhatónak. Így cselekedve megakadályozza annak lehetőségét, hogy a rendszer olyan forrásból importáljon igazolásokat, amelyeket az adminisztrátor tudta nélkül tekint a rendszer megbízhatónak.

Ha azt akarja, hogy senki se használhassa ezt az API-t arra a célra, hogy ellenőrző igazolást adjon hozzá a *SIGNATUREVERIFICATION igazolás tárolóhoz a tudta nélkül, akkor vegye fontolóra az API letiltását a rendszeren. A Rendszer szervizeszközök (SST) segítségével utasíthatja vissza a biztonsággal kapcsolatos rendszerváltozók módosításait.

Nézze át az alábbi telepítés előtti kilépési példaprogramot, hogy jobban megértse az alkalmazás telepítőprogramjának részét jelentő Add Verifier API használatát. Ez a példaprogram részlet (C nyelven írt) nem egy teljes telepítés előtti kilépési program - sokkal inkább egy olyan program egy szakaszára mutat példát, amely hívja az Add Verifier API-t. Ha a példaprogram használata mellett dönt, változtassa meg igényei szerint. Biztonsági okokból az IBM azt javasolja, hogy egyéniesítse a példaprogramot, és ne az alapértelmezett értékeket használja.

Megjegyzés: Az IBM nem kizárólagos szerzői jogi engedélyt ad az összes példaprogramhoz, amelyekből saját igényei szerint szabott, hasonló funkciójú programokat generálhat. Az IBM az összes példaprogramot csupán szemléltetési célból nyújtja. Ezek a példák nem kerültek minden állapotban tesztelésre. Az IBM így nem tudja garantálni a megbízhatóságukat, szervizelhetőségüket, de még a programok funkcióit sem. Az itt található összes programot úgy kapja meg meg ″AHOGY VAN″, mindennemű jótállás nélkül. A jogsértés kizárására, a kereskedelmi értékesítésre vagy egy adott célra való alkalmasságra vonatkozó sugallt jótállást az IBM ugyancsak kifejezetten elutasítja.

Változtassa meg igénye szerint úgy a példaprogramot, hogy az megfelelően használja a telepítés előtti kilépési program részét jelentő Add Verifier API-t, amellyel hozzáadhatja a szükséges aláírás ellenőrző igazolást a vásárló iSeries szerveréhez a termék telepítésekor.

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* SZERZŐI JOG (C) IBM CORP. 2002                                   */
/*                                                                  */
/* Az adott IFS fájlban lévő igazolás hozzáadása az Add Verifier API*/
/* segítségével a *SIGNATUREVERIFICATION igazolás tárolóhoz.        */
/*                                                                  */
/* Az API létrehozza az igazolás tárolót, ha nem létezik.           */
/* Ha létrehoz igazolás tárolót, az alapértelmezett jelszót állítja */
/* be, amelyet a DCM segítségével azonnal meg kell változtatni.     */
/* Erre figyelmeztetni kell a rendszer tulajdonosát, aki            */
/* használja ezt a programot.                                       */
/*                                                                  */
/*                                                                  */
/*                                                                  */
```

```
/* A kiadvány programozási forráskódokat tartalmaz saját           */
/* használatra.  Ez a példaprogram nem került tesztelésre          */
/* minden körülmény között.  Az IBM így nem tudja garantálni       */
/* a megbízhatóságukat, szervizelhetőségüket, de még a programok   */
/* funkcióit sem.  Az itt található összes programot úgy kapja     */
/* meg "AHOGY VAN".  A jogsértés kizárására, a kereskedelmi        */
/* értékesítésre vagy egy adott célra való alkalmasságra vonatkozó */
/* sugallt jótállást az IBM ugyancsak kifejezetten elutasítja. Az  */
/* IBM nem szervizeli ezeket a programokat és fájlokat.            */
/*                                                                 */
/*                                                                 */
/*                                                                 */
/* Paraméterek:                                                    */
/*                                                                 */
/*  kar *   az igazolást tartalmazó IFS fájl útvonalneve           */
/*  kar *   a tárolóhoz adandó igazolás címkéje                    */
/*                                                                 */
/*                                                                 */
/*                                                                 */
/* --------------------------------------------------------------- */

#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];

    /* útvonalnév hossz keresés */
    for(pathname_length = 0;
        ((*(pathname + pathname_length) != ' ') &&
         (*(pathname + pathname_length) != '\00'));
        pathname_length++);

    /* igazolás címke hossz keresés */
    for(cert_label_length = 0;
        ((*(certlabel + cert_label_length) != ' ') &&
         (*(certlabel + cert_label_length) != '\00'));
        cert_label_length++);


    error_code.Bytes_Provided = 0;     /* visszajelzések hibák esetén */

    QydoAddVerifier (pathname,         /* igazolást tartalmazó fájl útvonalneve*/
                     &pathname_length, /* útvonalnév hossza  */
                     "OBJN0100",       /* formátumnév  */
                     certlabel,        /* igazolás címke         */
                     &cert_label_length, /* igazolás címke hossza     */
                     &error_code);     /* hibakód          */

    return 0;
}
```

A feladatok befejezésével becsomagolhatja az alkalmazást és terjesztheti vásárlóinak. Amikor a vásárlók telepítik az alkalmazását, a telepítési folyamat részeként ellenőrzik az alkalmazás aláírt objektumait. Később a Digitális igazolás kezelő (DCM) segítségével ellenőrizheti az alkalmazás objektumain lévő aláírásokat. Ez lehetővé teszi a vásárlók számára annak meghatározását, hogy az alkalmazás forrása megbízható-e, valamint hogy történtek-e változások, amióta aláírta az alkalmazást.

Megjegyzés: A telepítőprogram lehet, hogy létrehozta a *SIGNATUREVERIFICATION igazolás tárolót alapértelmezett jelszóval a vásárló számára. Vásárlóinak javasolja, hogy a DCM segítségével töröljék az igazolás tároló jelszavát amint lehet, hogy megvédjék a jogosulatlan hozzáféréstől.

8. lépés: A *SIGNATUREVERIFICATION igazolás tároló alapértelmezett jelszavának töröltetése a vásárlókkal

Az Add Verifier API lehet, hogy létrehozta a *SIGNATUREVERIFICATION igazolás tárolót a termék telepítési folyamatának részeként a vásárló iSeries szerverén. Ha az API létrehozott igazolás tárolót, akkor azt alapértelmezett jelszóval hozta létre. Következésképpen, javasolja vásárlóinak, hogy a DCM segítségével töröljék a jelszót, ami védi az igazolás tárolót a jogosulatlan hozzáféréstől.

Vásárlóinak a következő lépéseket kell végrehajtaniuk a *SIGNATUREVERIFICATION igazolás tároló jelszavának törléséhez:

1. Indítsa el a DCM funkciót.
2. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SIGNATUREVERIFICATION** elemre, az igazolás tároló megnyitása céljából.
3. Amikor az Igazolás tároló és jelszó lap megjelenik, kattintson a **Jelszó törlésére**, hogy megjelenjen az Igazolás tároló jelszavának törlése lap.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
4. Adja meg a tároló új jelszavát, írja be újra megerősítés céljából, majd válassza ki az igazolás tárolóra vonatkozó jelszó lejárati szabályt, és kattintson a **Folytatásra**.

Forgatókönyv: Objektumok aláírása Kezelőközponttal

Helyzet

Társasága (MyCo, Inc.) alkalmazásokat fejleszt, amelyeket a cégen belül több helyszínen található több iSeries szervernek terjeszt. Hálózati rendszergazdaként felelős azért, hogy ezek az alkalmazások a társaság összes iSeries szerverén telepítésre és frissítésre kerüljenek. Jelenleg az iSeries navigátor Kezelőközpont funkcióját használja, ami megkönnyíti az alkalmazások csomagolását és elosztását, valamint egyéb adminisztrációs feladatok elvégzését, amiért felelős. Azonban, több időt tölt el az alkalmazások követésével és a problémák korrigálásával az objektumok jogosulatlan változtatásai miatt, mint amennyit szeretne. Következésképpen, biztonságosabbá szeretné tenni az objektumok sértetlenségét azzal, hogy digitálisan aláírja őket.

Tüzetesen átvizsgálta az OS/400 objektum aláírási tulajdonságait, valamint megismerte, hogy a V5R2 változattól kezdve a Kezelőközpont lehetővé teszi az objektumok aláírását, amikor csomagolja és elosztja őket. A Kezelőközpont használata hatékonyan és viszonylag egyszerűen kielégíti a társaság biztonsági céljait. Ugyancsak elhatározza egy Helyi igazolási hatóság (CA) létrehozását, amellyel igazolást ad ki az objektumok aláírásához. A Helyi CA által objektum aláíráshoz kibocsátott igazolás korlátok közé szorítja a biztonsági technológia költségét, mivel nem kell vásárolnia igazolást egy jól ismert nyilvános CA-tól.

A példa hasznos tájékoztatást nyújt a beállítási lépésekről és azon alkalmazások objektumainak aláírásáról, amelyeket a társaság több iSeries szerverének továbbít.

A forgatókönyv előnyei

Ez a forgatókönyv a következő előnyökkel jár:

- Az objektumok Kezelőközponttal történő csomagolása és aláírása csökkenti a ráfordítási időt, amikor az aláírt objektumokat a társaság több iSeries szerverére továbbítja.

- Ha Kezelőközpontot használ a csomagban lévő objektumok aláírásához, csökkenti azon lépések számát, melyeket végre kell hajtani az objektumok aláírásához, mivel az aláírási művelet a csomagolási folyamat része.
- Az objektumokból álló csomag aláírása révén még könnyebben meghatározhatja, hogy megváltoztak-e az objektumok az aláírás után. Ez csökkenthet bizonyos hibakeresési feladatokat, melyeket végrehajt a jövőben az alkalmazási problémák követéséhez.
- Az objektumok aláírásához Helyi Igazolási hatóság (CA) által kiadott igazolást felhasználva, olcsóbbá teszi az objektumok aláírásának megvalósítását.

Célok

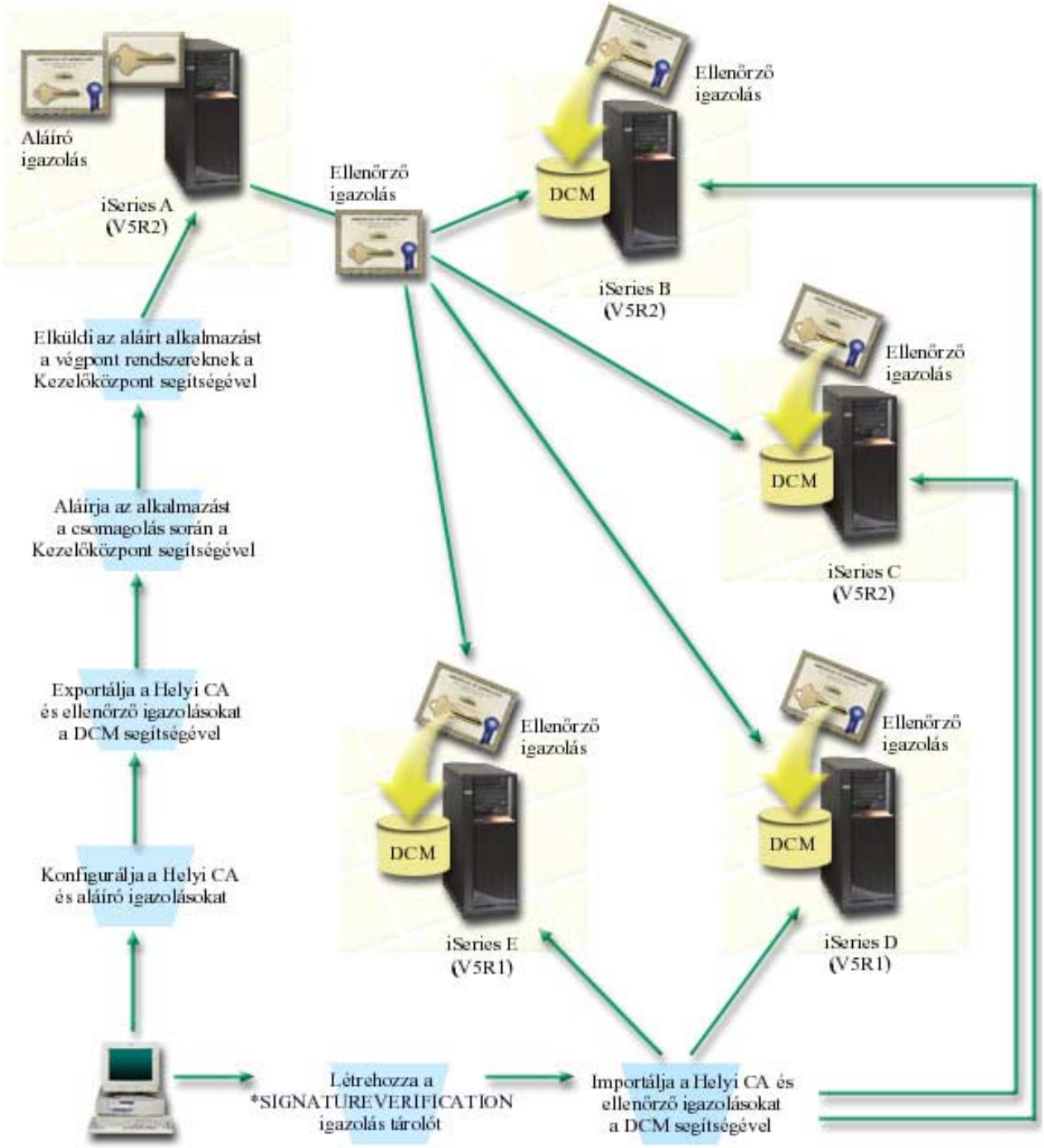
Ebben a forgatókönyvben a MyCo, Inc. digitálisan kívánja aláírni az alkalmazásokat, amelyeket a társaságon belül több iSeries szervernek továbbít. A MyCo, Inc. hálózati rendszergazdájaként már használta a Kezelőközpontot számos iSeries adminisztratív feladatra. Következésképpen, ki akarja terjeszteni a Kezelőközpont pillanatnyi használatát azzal, hogy aláírja a társaság alkalmazásait, amelyeket más iSeries szervereknek továbbít.

A forgatókönyv céljai a következők:

- A társaság alkalmazásait a Helyi CA által kiadott igazolással írja alá, hogy ezzel is korlátozza az alkalmazások aláírásának költségeit.
- A rendszergazdának és más kijelölt felhasználóknak könnyedén ellenőrizniük kell az összes iSeries szerveren lévő aláírást, hogy ellenőrizni tudják a társaság által aláírt objektumok forrását és hitelességét. Ahhoz, hogy ezt végrehajthassa, mindegyik iSeries szerveren legyen egy másolat a cég aláírás ellenőrző igazolásából, valamint a Helyi Igazolási hatóságtól (CA) eredő igazolásból a szerverek *SIGNATUREVERIFICATION igazolás tárolóiban.
- A cég alkalmazásain lévő aláírások ellenőrzésével az iSeries adminisztrátorok és mások észlelhetik, hogy megváltozott-e az objektumok tartalma aláírásuk óta.
- A rendszergazdák a Kezelőközponttal csomagolják, írják alá és terjesszék az alkalmazásokat a társaság iSeries szerverei felé.

Részletek

Az alábbi ábra szemlélteti az objektum aláírási és az aláírás ellenőrzési folyamatot, amely a forgatókönyv megvalósítását szolgálja:



Az ábra a forgatókönyvhöz tartozó következő pontokat szemlélteti:

Központi rendszer (iSeries A)

- Az iSeries A szerveren OS/400 Verzió 5 Változat 2 (V5R2) fut.
- Az iSeries A központi rendszerként szolgál, amelyen a Kezelőközpont fut, beleértve a társaság alkalmazásainak csomagolását és elosztását is.
- Az iSeries A szerveren telepítve van a Cryptographic Access Provider 128-bit for iSeries (5722–AC3) termék.

- Az iSeries A szerveren telepítve és konfigurálva van a Digital Certificate Manager (OS/400 34-es opció), és az IBM HTTP Server (5722–DG1) termék.
- Az iSeries A szerver Helyi Igazolási hatóságként (CA) szerepel, és az objektum aláíró igazolás a rendszeren található.
- Az iSeries A szerver a társaság alkalmazásainak elsődleges objektum aláíró rendszere. A következő feladatok végrehajtásával teljesítheti a vásárlóknak szánt termékobjektumok aláírását az iSeries A szerveren:
  1. A DCM révén hozzon létre egy Helyi CA-t, és ennek segítségével egy objektum aláíró igazolást.
  2. A DCM segítségével exportálja a Helyi CA igazolás, valamint az objektum aláíró igazolás egy-egy példányát egy fájlba, ami által a végpont rendszerek (iSeries B, C, D és E) ellenőrizhetik az aláírt objektumokat.
  3. A Kezelőközpont segítségével írja alá az alkalmazás objektumait és csomagolja össze őket az ellenőrző igazolások fájljával.
  4. A Kezelőközpontot felhasználva ossza el az aláírt alkalmazásokat és igazolás fájlokat a végpont rendszereknek.

Végpont rendszerek (iSeries B, C, D és E szerverek)

- Az iSeries B és C szerveren OS/400 Verzió 5 Változat 2 (V5R2) fut.
- Az iSeries D és E szerveren OS/400 Verzió 5 Változat 1 (V5R1) fut.
- Az iSeries B, C, D és E szerveren telepítve és konfigurálva van a Digital Certificate Manager (34-es opció), és az IBM HTTP Server (5722–DG1) termék.
- Az iSeries B, C, D és E szerverek megkapják a társaság aláírás ellenőrző igazolását és a Helyi CA igazolást is a központi rendszertől (iSeries A), amikor a rendszerek fogadják az aláírt alkalmazást.
- A DCM segítségével hozhatja létre a *SIGNATUREVERIFICATION igazolás tárolót, és importálhatja az ellenőrzéshez használatos igazolásokat a tárolóba.

Előfeltételek és feltételezések

A forgatókönyv a következő előfeltételektől és feltételezésektől függ:

1. Az iSeries szerverek kielégítik a Digitális igazolás kezelő (DCM) telepítésének és használatának követelményeit.
2. Senki sem konfigurálta vagy használta korábban az iSeries szervereken lévő DCM-eket.
3. Az iSeries A eleget tesz az iSeries navigátor és a Kezelőközpont telepítésére és használatára vonatkozó követelményeknek.
4. A Kezelőközpontnak az összes iSeries végpont rendszeren futni kell.
5. Az összes iSeries szerver a legmagasabb szintű telepített Cryptographic Access Provider 128-bit licencprogrammal (5722-AC3) rendelkezik.
6. A Verify object signatures during restore (QVFYOBJRST) rendszerváltozó alapértéke az összes forgatókönyvben 3 az iSeries szervereken, és nem is változik ez a beállítás. Az alapértelmezett beállítás garantálja, hogy a szerver ellenőrizheti az objektumok aláírásait, amikor visszaállítja az aláírt objektumokat.
7. Az iSeries A szerver hálózati rendszergazdájának *ALLOBJ különleges jogosultsággal kell rendelkeznie az objektumok aláírásához, vagy a felhasználói profilnak kell jogosultnak lenni az objektum aláíró alkalmazáshoz.
8. A hálózati rendszergazdának vagy valaki másnak, aki létrehozza az igazolás tárolót a DCM-ben, *SECADM és *ALLOBJ különleges jogosultsággal kell rendelkeznie.
9. A rendszergazdáknak vagy másoknak az összes többi iSeries szerveren *AUDIT különleges jogosultsággal kell rendelkezniük az objektum aláírások ellenőrzéséhez.

Feladat lépések

A forgatókönyv megvalósításához két feladatsort kell végrehajtani: Az egyik feladatsor lehetővé teszi az iSeries A szerver beállítását a Kezelőközpont használatához, ami révén az alkalmazásokat aláírja és terjeszti. A másik feladatsor lehetővé teszi a rendszergazdáknak és másoknak, hogy ellenőrizzék az alkalmazásokon lévő aláírásokat az összes többi iSeries szerveren.

Objektum aláírási feladatsor

Az összes alábbi feladatot hajtsa végre az iSeries A szerveren az objektumok aláírásához a forgatókönyv leírása szerint:

1. Hajtsa végre az előfeltételként megadott lépéseket, amelyek révén telepíti és konfigurálja az összes szükséges iSeries terméket.
2. A Digitális igazolás kezelő (DCM) segítségével hozza létre a Helyi igazolási hatóságot (CA), amely kiadja az objektum aláíró igazolást.
3. A DCM segítségével hozzon létre alkalmazás definíciót.
4. A DCM segítségével rendelje hozzá az igazolást az objektum aláíró alkalmazás definíciójához.
5. A DCM segítségével exportálja az igazolásokat, amelyeket más rendszerek használnak az objektum aláírások ellenőrzéséhez. A Helyi CA igazolás és az objektum aláíró igazolás egy-egy példányát is exportálni kell egy fájlba, mint aláírás ellenőrző igazolás.
6. Juttassa el az igazolás fájlokat minden egyes iSeries végpont rendszernek, amelyen ellenőrizni kívánja az aláírásokat.
7. A Kezelőközpont segítségével írja alá az alkalmazás objektumait.

Aláírás ellenőrzési feladatsor

Az aláírás ellenőrzéshez tartozó konfigurálási feladatok mindegyikét végre kell hajtani az összes iSeries végpont rendszeren, mielőtt a Kezelőközpont segítségével eljuttatná hozzájuk az aláírt alkalmazás objektumait. Az aláírás ellenőrzés konfigurálását be kell fejezni ahhoz, hogy sikeresen ellenőrizhesse az aláírásokat, mikor visszaállítja az aláírt objektumokat a végpont rendszereken.

Az összes iSeries végpont rendszeren hajtsa végre az alábbi feladatokat, és ellenőrizze az objektumokon lévő aláírásokat a forgatókönyvben leírtak szerint:

8. A Digitális igazolás kezelő (DCM) segítségével hozza létre a *SIGNATUREVERIFICATION igazolás tárolót.
9. A DCM segítségével importálja a Helyi CA igazolást és az aláírás ellenőrző igazolást.

Konfigurálási részletek

A következő feladatsorok végrehajtásával konfigurálja a Kezelőközpontot az objektumok aláírására, ahogy a forgatókönyv írja.

1. lépés: Előfeltételt jelentő összes feladat végrehajtása

Végre kell hajtani az összes előfeltételt jelentő feladatot, amely révén telepíti és konfigurálja az összes szükséges iSeries terméket, mielőtt a forgatókönyv megvalósításához tartozó, jellemző konfigurálási feladatokat végrehajthatná.

2. lépés: Helyi igazolási hatóság létrehozása objektum aláíró igazolás kiadása céljából

Amikor Digitális igazolás kezelővel (DCM) hoz létre Helyi igazolási hatóságot (CA), űrlapok sorozatát kell kitöltenie a folyamat során. Ezek az űrlapok végigvezetik a CA létrehozásának folyamatán, valamint a Védett socket réteg (SSL), objektum aláírás és aláírás ellenőrzés céljára használt digitális igazolások használatának elkezdéséhez szükséges egyéb feladatok végrehajtásán. A forgatókönyv szerint ugyan nem kell konfigurálni igazolásokat az SSL funkcióhoz, de az összes űrlapot ki kell tölteni ahhoz, hogy konfigurálja a rendszert az objektumok aláírásához.

Kövesse az alábbi lépéseket, ha a DCM segítségével Helyi CA-t hoz létre és működtet:

1. Indítsa el a DCM funkciót.
2. A DCM navigációs keretén válassza ki az **Igazolási hatóság (CA) létrehozását** az űrlapok megjelenítéséhez.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
3. Töltse ki a teljes űrlapot. A feladat végrehajtásakor tegye a következőt:
   a. Adja meg a Helyi CA azonosítási információit.
   b. Telepítse a Helyi CA igazolást a böngészőjében, hogy a szoftver felismerhesse a Helyi CA-t és ellenőrizhesse az általa kiadott igazolásokat.
   c. Adja meg a Helyi CA stratégiai adatait.
   d. Az új Helyi CA segítségével adja ki a szerver vagy a kliens igazolást, amelyet alkalmazásai az SSL kapcsolatokhoz használhatnak.

      Megjegyzés: A forgatókönyv ugyan nem használja ezt az igazolást, de létre kell hozni, mielőtt a Helyi CA segítségével kiadná a szükséges objektum aláíró igazolást. Ha az igazolás létrehozása nélkül félbehagyja a feladatot, létre kell hoznia az objektum aláíró igazolást és az *OBJECTSIGNING igazolás tárolót, amelyben külön tárolja.
   e. Válassza ki azokat az alkalmazásokat, amelyek használhatják a szerver vagy a kliens igazolást az SSL kapcsolatokhoz.

      Megjegyzés: A forgatókönyv céljainak megfelelően ne válasszon ki egyetlen alkalmazást sem, hanem kattintson a **Folytatásra** a következő űrlap megjelenítéséhez.
   f. Az új Helyi CA segítségével adjon ki egy objektum aláíró igazolást, melyet az alkalmazások használhatnak objektumok digitális aláírására. Az alfeladat létrehozza az *OBJECTSIGNING igazolás tárolót. Ez az a tároló, amelyet az objektum aláíró igazolások kezelésére használ.
   g. Válassza ki az alkalmazásokat, amelyek megbízhatónak tekintik a Helyi CA-t.

      Megjegyzés: A forgatókönyv céljainak megfelelően ne válasszon ki egyetlen alkalmazást sem, hanem kattintson a **Folytatásra** a feladat befejezéséhez.

Most, hogy létrehozta a Helyi CA-t és az objektum aláíró igazolást, meg kell adni az igazolást használó objektum aláíró alkalmazást, mielőtt aláírhatna objektumokat.

3. lépés: Objektum aláíró alkalmazás definíciójának létrehozása

Miután létrehozta objektum aláíró igazolását, a Digitális igazolás kezelővel (DCM) meg kell adni az objektum aláíró alkalmazást, amelyet használni fog az objektumok aláírására. Az alkalmazás definíciónak nem kell hivatkozni egy tényleges alkalmazásra. A létrehozott alkalmazás definíció írja le az aláírni kívánt objektumcsoport típusát. Olyan definícióra van szükség, amely révén az alkalmazás azonosítót (ID) társíthatja az igazolással, hogy engedélyezze az aláírási folyamatot.

Kövesse az alábbi lépéseket, ha a DCM segítségével objektum aláíró alkalmazás definícióját hozza létre:

1. A navigációs kereten kattintson az **Igazolás tároló választására**, majd válassza ki a megnyitandó ***OBJECTSIGNING** igazolás tárolót.
2. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatásra**.
3. A navigációs kereten válassza az **Alkalmazások kezelését** a feladatlista megjelenítéséhez.
4. Válassza ki az **Alkalmazás hozzáadását** a feladatlistából, hogy megjelenítse az alkalmazás megadására szolgáló űrlapot.
5. Töltse ki az űrlapot, és kattintson a **Hozzáadásra**.

Most, hozzá kell rendelni az objektum aláíró igazolást a létrehozott alkalmazáshoz.

4. lépés: Igazolás hozzárendelése az objektum aláíró alkalmazás definíciójához

Kövesse az alábbi lépéseket, ha igazolást rendel hozzá az objektum aláíró alkalmazáshoz:

1. A DCM navigációs keretén válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
2. A feladatlistán válassza az **Igazolás hozzárendelése** feladatot az aktuális igazolás tárolóban lévő igazolások listájának megjelenítéséhez.
3. Válassza ki az igazolást a listából, és kattintson a **Hozzárendelés alkalmazásokhoz** feladatra, hogy megjelenítse az aktuális igazolás tárolóhoz tartozó alkalmazás definíciók listáját.
4. Válasszon ki egy vagy több alkalmazást a listából, és kattintson a **Folytatásra**. Egy üzenetlap jelenik meg, amely vagy megerősíti az igazolás hozzárendelését, vagy hiba információt közöl, ha probléma történt.

A feladat befejezésekor készen áll az objektumok aláírására a Kezelőközponttal, amikor csomagolja és elosztja őket. Azonban ahhoz, hogy biztosan ellenőrizni tudja az aláírásokat, exportálja az igazolásokat egy fájlba, és vigye át őket az összes iSeries végpont rendszerre. Az aláírás ellenőrzéshez tartozó konfigurálási feladatok mindegyikét végre kell hajtani az összes iSeries végpont rendszeren, mielőtt a Kezelőközpont segítségével eljuttatná hozzájuk az aláírt alkalmazás objektumait. Az aláírás ellenőrzés konfigurálását be kell fejezni ahhoz, hogy sikeresen ellenőrizhesse az aláírásokat, mikor visszaállítja az aláírt objektumokat a végpont rendszereken.

5. lépés: Igazolások exportálása az aláírás ellenőrzés engedélyezéséhez más iSeries rendszereken

Az objektum tartalom sértetlenségének védelme érdekében történő aláírás megköveteli, hogy saját maga és mások is ellenőrizzék az aláírás hitelességét. Ha az objektum aláírásokat ugyanazon a rendszeren ellenőrzi, amely aláírta az objektumokat, akkor a DCM segítségével hozza létre a *SIGNATUREVERIFICATION igazolás tárolót. Az igazolás tárolónak tartalmaznia kell az objektum aláíró igazolás és a CA igazolás egy-egy példányát is, mégpedig arra a CA-ra vonatkozóan, amelyik kiadta az aláíró igazolást.

Ahhoz, hogy mások ellenőrizni tudják az aláírást, juttassa el nekik annak az igazolásnak egy példányát, amely aláírta az objektumot. Amikor Helyi igazolási hatóságot (CA) használ fel az igazolás kiadásához, a Helyi CA igazolás egy példányát kell eljuttatnia az érdekelteknek.

Kövesse az alábbi lépéseket, ha az objektum aláírásokat ugyanazon a rendszeren ellenőrzi, amely aláírta az objektumokat (iSeries A ebben a forgatókönyvben):

1. A navigációs kereten válassza az **Új igazolás tároló létrehozását**, majd a ***SIGNATUREVERIFICATION** igazolás tárolót létrehozás céljából.
2. Az **Igen** gomb kiválasztásával másolja át a meglévő objektum aláíró igazolásokat az új igazolás tárolóba aláírás ellenőrző igazolásokként.
3. Adjon meg egy jelszót az új igazolás tárolóra, és kattintson a **Folytatásra**, hogy létrehozza az igazolás tárolót. Most a DCM segítségével ellenőrizheti az objektum aláírásokat ugyanazon a rendszeren, amelyet az objektumok aláírásához használt.

Kövesse az alábbi lépéseket, amikor a DCM segítségével exportálja a Helyi CA igazolás egy példányát, valamint az objektum aláíró igazolás egy példányát aláírás ellenőrző igazolásként, ami által ellenőrizheti az objektum aláírásokat más rendszereken:

1. A navigációs kereten válassza az **Igazolások kezelése**, majd utána az **Igazolás exportálása** feladatot.
2. Válassza az **Igazolási hatóságot (CA)**, és kattintson a **Folytatásra** az exportálásra szánt CA igazolások felsorolásának megjelenítéséhez.
3. Válassza ki a korábban létrehozott Helyi CA igazolást a listából, és kattintson az **Export** gombra.

4. Exportálási célként adjon meg **Fájlt**, és kattintson a **Folytatásra**.
5. Adja meg az exportált Helyi CA igazolás teljes elérési útvonalát és fájlnevét, majd kattintson a **Folytatás** gombra az igazolás exportálásához.
6. Kattintson az **OK** gombra az Exportálás jóváhagyása lap megjelenítéséhez. Most exportálhatja az objektum aláíró igazolás egy példányát.
7. Válassza újra az **Igazolás exportálása** feladatot.
8. Válassza az **Objektum aláírást** az exportálható objektum aláíró igazolások listájának megjelenítéséhez.
9. Válassza ki a megfelelő objektum aláíró igazolást a listából, és kattintson az **Export** gombra.
10. Célként válasszon ki **Fájlt, mint aláírás ellenőrző igazolást**, és kattintson a **Folytatásra**.
11. Adja meg az aláírás ellenőrző igazolás teljes elérési útvonalát és fájlnevét, majd kattintson a **Folytatás** gombra az igazolás exportálásához.

Most átviheti ezeket a fájlokat az iSeries végpont rendszerekre, ahol ellenőrizni kívánja az adott igazolással létrehozott aláírásokat.

6. lépés: Igazolás fájlok átvitele iSeries végpont rendszereknek

Az iSeries A szerveren létrehozott igazolás fájlokat át kell vinni a forgatókönyvben végpont rendszerekként működő iSeries szerverekre, mielőtt konfigurálhatná őket az aláírt objektumok ellenőrzésére. Több különböző módszert is használhat az igazolás fájlok átvitelére. Például, használhatja a Fájlátviteli protokolt (FTP) vagy a Kezelőközpont csomag terjesztési funkcióját a fájlok eljuttatásához.

7. lépés: Objektumok aláírása Kezelőközponttal

A Kezelőközponttal történő objektum aláírási folyamat a szoftver csomagolási és terjesztési folyamat része. Az aláírás ellenőrzéshez tartozó konfigurálási feladatok mindegyikét végre kell hajtani az összes iSeries végpont rendszeren, mielőtt a Kezelőközpont segítségével eljuttatná hozzájuk az aláírt alkalmazás objektumait. Az aláírás ellenőrzés konfigurálását be kell fejezni ahhoz, hogy sikeresen ellenőrizhesse az aláírásokat, mikor visszaállítja az aláírt objektumokat a végpont rendszereken.

Kövesse az alábbi lépéseket, amikor iSeries végpont rendszereknek szánt alkalmazást ír alá a forgatókönyvben leírtak szerint:

1. A Kezelőközpont segítségével csomagolja és ossza el a szoftver termékeket.
2. Amikor megjelenik a **Termék meghatározás** varázsló **Azonosítás** lapja, kattintson a **Továbbiakra**, hogy megjelenjen a **További azonosítás** panel.
3. A **Digitális aláírás** mezőbe írja be az előzőleg létrehozott objektum aláíró alkalmazás azonosítóját, és kattintson az **OK** gombra.
4. Fejezze be a varázslót, és folytassa a szoftver termékek csomagolási és elosztási folyamatát a Kezelőközponttal.

8. lépés: Aláírás ellenőrzési feladatok - *SIGNATUREVERIFICATION igazolás tárolók létrehozása iSeries végpont rendszereken

Ahhoz, hogy ellenőrizhesse az objektum aláírásokat az iSeries végpont rendszereken a forgatókönyv szerint, minden rendszer *SIGNATUREVERIFICATION igazolás tárolójában ott kell lenni a megfelelő aláírás ellenőrző igazolás egy példányának. Ha az objektumok aláírásához magán igazolást használt, az igazolás tárolónak tartalmaznia kell a Helyi CA igazolás egy példányát is.

A *SIGNATUREVERIFICATION igazolás tároló létrehozásához kövesse ezeket a lépéseket:

1. Indítsa el a DCM funkciót.

2. A Digitális igazolás kezelő (DCM) navigációs keretén válassza ki az **Új igazolás tároló létrehozását**, majd a ***SIGNATUREVERIFICATION** igazolás tárolót létrehozás céljából.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
3. Adjon meg egy jelszót az új igazolás tárolóra, és kattintson a **Folytatásra**, hogy létrehozza az igazolás tárolót. Most importálhatja az igazolásokat a tárolóba, amelyek révén ellenőrizheti az objektum aláírásokat.

9. lépés: Aláírás ellenőrzési feladatok - igazolások importálása

Ahhoz, hogy ellenőrizze egy objektumon az aláírást, a *SIGNATUREVERIFICATION tárolónak tartalmaznia kell az aláírás ellenőrző igazolás egy példányát. Ha az aláírási igazolás magán igazolás, akkor az igazolás tárolónak tartalmaznia kell az aláírási igazolást kiadó Helyi igazolási hatóság (CA) igazolásának egy példányát is. A tárgyalt forgatókönyvben mindkét igazolást egy fájlba exportálta, és ezt a fájlt vitte át minden egyes iSeries végpont rendszerre.

Kövesse az alábbi lépéseket, amikor importálja ezeket az igazolásokat a *SIGNATUREVERIFICATION tárolóba:

1. A DCM navigációs keretén kattintson az **Igazolás tároló választása**, majd a ***SIGNATUREVERIFICATION** elemre, mint megnyitandó igazolás tárolóra.
2. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatásra**.
3. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
4. A feladatlistából válassza az **Igazolás importálását**.
5. Válassza az **Igazolási hatóságot (CA)** az igazolás típusának, és kattintson a **Folytatásra**.

   Megjegyzés: A Helyi CA igazolást a magán aláírás ellenőrző igazolást megelőzően kell importálni, egyébként az aláírás ellenőrző igazolás importálása meghiúsul.
6. Adja meg a CA igazolás fájl teljes elérési útvonalát és nevét, majd kattintson a **Folytatás** gombra. Egy üzenet jelenik meg, ami vagy megerősíti, hogy az importálási folyamat sikeresen megtörtént, vagy hibainformációkat közöl, ha a folyamat hibát észlelt.
7. Válassza újra az **Igazolás importálása** feladatot.
8. Az igazolás típusának válassza ki az **Aláírás ellenőrzést**, és kattintson a **Folytatásra**.
9. Adja meg az aláírás ellenőrző igazolás fájl teljes elérési útvonalát és nevét, majd kattintson a **Folytatás** gombra. Egy üzenet jelenik meg, ami vagy megerősíti, hogy az importálási folyamat sikeresen megtörtént, vagy hibainformációkat közöl, ha a folyamat hibát észlelt.

Az iSeries rendszer most ellenőrizheti az objektumokon lévő aláírásokat (amelyeket a megfelelő aláírási igazolással hozott létre), mikor visszaállítja az aláírt objektumokat.

Objektum aláírási alapelvek

Mielőtt elkezdené használni az iSeries objektum aláírási és aláírás ellenőrzési funkcióit, hasznosnak találhatja néhány alábbi alapelv áttekintését:

Digitális aláírások
A digitális aláírások és az általuk nyújtott védelem megismerése.

Aláírható objektumok
Az itt leírtak ismertetik az aláírható iSeries objektumokat, valamint a parancs (*CMD) objektumok aláírási lehetőségeit.

Objektum aláírás feldolgozása
Ismerteti az objektum aláírási folyamat lefolyását, és az ehhez beállítható paramétereket.

Aláírás ellenőrzés feldolgozása
Ismerteti az objektum aláírás ellenőrzésének folyamatát, és az ehhez beállítható paramétereket.

Digitális aláírások

Az OS/400 támogatja a digitális igazolások használatát az objektumok digitális aláírásához. Az objektumon lévő digitális aláírást titkosítási eljárással hozza létre, és az írott dokumentumon lévő személyes aláíráshoz hasonló. A digitális aláírás révén ellenőrizheti az objektum eredetét és sértetlenségét. A digitális igazolás tulajdonosa az igazolás magánkulcsával ″írja alá″ az objektumot. Az objektum címzettje az igazolás megfelelő nyilvános kulcsával visszafejti az aláírást, amely ellenőrzi az aláírt objektum sértetlenségét és a küldőt, mint forrást.

Az objektum aláírási támogatás kibővíti a hagyományos iSeries szerver eszközöket az objektum változtatások felismerése terén. A hagyományos vezérlés nem tudja megvédeni az objektumot a jogosulatlan megváltoztatástól, amikor az Interneten vagy egyéb megbízhatatlan hálózaton keresztül halad át. Mivel észlelni tudja, hogy változott-e az objektum tartalma az aláírása óta, sokkal könnyebben eldöntheti, megbízhatónak tekintheti-e a megkapott objektumot ilyen esetekben.

A digitális aláírás az objektumban található adatok titkosított matematikai összegzése. Az objektumot és tartalmát ugyan nem titkosítja és nem teszi magán jellegűvé a digitális aláírás, azonban az összegzés titkosítva van, és megakadályozza saját maga jogosulatlan módosítását. Ha valaki meg akar győződni arról, hogy nem változott-e meg az objektum a továbbítás során, és hogy az objektum egy elfogadott, legitim forrásból ered-e, az aláíró igazolás nyilvános kulcsával ellenőrizze az eredeti digitális aláírást. Ha az aláírás nem egyezik, az adatok megváltozhattak. Ilyen esetben a címzett vagy elkerüli az objektum használatát, vagy felveszi a kapcsolatot az aláíróval, hogy beszerezze az aláírt objektum egy másik példányát.

Az objektumon lévő aláírás a rendszert képviseli (amely aláírta az objektumot), és nem a rendszer egy adott felhasználóját (bár a felhasználónak megfelelő jogosultsággal kell rendelkezni ahhoz, hogy az igazolást objektumok aláírásához használhassa).

Ha úgy dönt, hogy a digitális aláírás igénybe vétele megfelel biztonsági igényeinek és irányelveinek, akkor vizsgálja meg, hogy nyilvános vagy helyi igazolásokat adjon-e ki. Ha az objektumokat az általános nyilvánossághoz tartozó felhasználóknak kívánja terjeszteni, akkor fontolja meg a jólismert nyilvános Igazolási hatóságtól (CA) származó igazolások használatát az objektumok aláírásához. A nyilvános igazolások használata biztosítja azt, hogy mások könnyen és olcsón ellenőrizhetik az elküldött objektumokon elhelyezett aláírásokat. Ha azonban az objektumokat kizárólag saját szervezetén belül kívánja terjeszteni, akkor előnyben részesítheti a Digitális igazolás kezelő (DCM) használatát, amellyel saját Helyi CA-t működtethet az objektumokat aláíró igazolások kiadásához. Az objektumok aláírásához használt, Helyi CA-tól eredő magán igazolások olcsóbbak, mint ha egy jólismert nyilvános CA-tól vásárolja meg őket.

A digitális aláírások típusai

A V5R2 változattól kezdve a parancs (*CMD) objektumokat is aláírhatja. A *CMD objektumokat is kétféleképpen írhatja alá: az objektum magját jelentő részt vagy a teljes objektumot.

- **Teljes objektum aláírása**
  Az ilyen típusú aláírás magában foglalja az objektum összes, de néhány nem lényeges byte-ját is.
- **Objektum magjának aláírása**
  Az ilyen típusú aláírás a *CMD objektum lényeges byte-jait foglalja csupán magában. Így az aláírás nem tartalmazza azokat a byte-okat, amelyek ki vannak téve gyakori változtatásoknak. Az ilyen típusú aláírás lehetővé teszi a parancs bizonyos módosítását anélkül, hogy az aláírás érvénytelenné válna. Az, hogy az ilyen aláírásnál mely byte-ok nem vesznek részt az aláírás képzésében, az adott *CMD objektumtól függ.

Például, az aláírás nem foglalja magában a *CMD objektum paramétereinek alapértelmezett értékét. Példák olyan objektum változásokra, amelyek nem érvénytelenítik az ilyen típusú aláírást:

- Parancs alapértékeinek módosítása.
- Érvényesség ellenőrző program hozzáadása olyan parancshoz, amely nem rendelkezik ilyennel.
- ″Where allowed to run″ paraméter módosítása.
- ″Allow limited users″ paraméter módosítása.

Ha többet szeretne megtudni arról, hogy milyen iSeries objektumokat írhat alá, és a *CMD objektumok magjának aláírásakor mely byte-ok lesznek figyelembe véve, olvassa el az Aláírható objektumok című részt.

Aláírható objektumok

Az OS/400 objektumtípusok széles skáláját írhatja alá digitálisan, az aláíráshoz használt módszertől függetlenül. Az integrált fájlrendszerben tárolt bármely objektumot (*STMF) aláírhatja, kivéve a könyvtárban tárolt objektumokat. Ha az objektumhoz Java program is kapcsolódik, akkor a program is alá lesz írva. A QSYS.LIB fájlrendszerben csak a következő objektumokat írhatja alá: programok (*PGM), szervizprogramok (*SRVPGM), modulok (*MODULE), SQL csomagok (*SQLPKG), *FILE (csak mentési fájl) és parancsok (*CMD).

Az objektumnak a helyi rendszeren kell lenni az aláíráshoz. Például, ha Windows 2000 szervert működtet az Integrated xSeries Server for iSeries kiegészítőn, akkor rendelkezésére áll a QNTC fájlrendszer az integrált fájlrendszerben. A fájlrendszer katalógusai nem tekinthetők helyinek, mivel olyan fájlokat tartalmaznak, amelyeket a Windows 2000 operációs rendszer birtokol. Az üres objektumokat, vagy a V5R1 előtti szintre fordított objektumokat szintén nem tudja aláírni.

Parancs (*CMD) objektum aláírások

Amikor *CMD objektumokat ír alá, két aláírás típus egyikét alkalmazhatja a *CMD objektumra. Választhatja azt, hogy a teljes objektumot aláírja, vagy azt, hogy csak az objektum magját. Amikor a teljes objektum aláírását választja, az aláírás az objektum összes (s így néhány lényegtelen byte-jára is) vonatkozik. A teljes objektum aláírás magában foglalja az objektum magjára vonatkozó aláírás által tartalmazott fájlokat is.

Amikor az objektum magjának aláírását választja, a lényeges byte-okat védi az aláírás, míg a gyakrabban változó byte-okat nem írja alá. A *CMD objektumtól függ, hogy mely byte-okat nem írja alá, de többek között ilyenek lehetnek a módot meghatározó byte-ok (amelyben az objektum érvényes) vagy az objektum futásának engedélyezését meghatározó byte-ok. Például, az aláírás nem foglalja magában a *CMD objektum paramétereinek alapértelmezett értékét. Az ilyen típusú aláírás lehetővé teszi a parancs bizonyos módosítását anélkül, hogy az aláírás érvénytelenné válna. Példák olyan objektum változásokra, amelyek nem érvénytelenítik az ilyen típusú aláírásokat:

- Parancs alapértékeinek módosítása.
- Érvényesség ellenőrző program hozzáadása olyan parancshoz, amely nem rendelkezik ilyennel.
- ″Where allowed to run″ paraméter módosítása.
- ″Allow limited users″ paraméter módosítása.

Az alábbi táblázat ismerteti, hogy a *CMD objektum pontosan mely byte-jai alkotják az objektum magját, amelyek részt vesznek az aláírásban.

Objektum mag aláírásának összeállítása *CMD objektumoknál

Objektum része	Kapcsolata az objektum magjára vonatkozó aláírással
CHGCMDDFT által módosítható parancs alapértékek	Nem része az objektum magjára vonatkozó aláírásnak
A parancs és a könyvtár feldolgozásának programja	Mindig része az objektum magjára vonatkozó aláírásnak

Objektum része	Kapcsolata az objektum magjára vonatkozó aláírással
REXX forrásfájl és könyvtár	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
REXX forrás member	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
REXX parancs környezet és könyvtár	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
REXX kilépési program neve, könyvtára és kilépési kódja	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
Érvényesség ellenőrző program és könyvtár	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
Mód, amelyben érvényes	Nem része az objektum magjára vonatkozó aláírásnak
Ahol engedélyezve van a futása	Nem része az objektum magjára vonatkozó aláírásnak
Korlátozott felhasználók engedélyezése	Nem része az objektum magjára vonatkozó aláírásnak
Súgó könyvespolc	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
Súgó panelcsoport és könyvtár	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
Súgó azonosító	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
Súgó keresési index és könyvtár	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
Aktuális könyvtár	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
Termék könyvtár	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
Prompt felülbíráló program és könyvtár	Az objektum magjára vonatkozó aláírás része, ha az aláíráskor adja meg a parancs számára, egyébként nem része
Szöveg (leírás)	Nem része sem a részleges, sem a teljes objektum aláírásnak, mivel nem az objektumban tárolódik
Grafikus felhasználói kezelőfelület (GUI) engedélyezése	Nem része az objektum magjára vonatkozó aláírásnak

Objektum aláírás feldolgozása

Amikor objektumokat ír alá, a következő paramétereket adhatja meg az objektum aláírás feldolgozásához.

- **Hiba feldolgozás**
  Megadhatja, hogy milyen típusú hiba feldolgozást végezzen az alkalmazás, amikor egynél több objektumon hoz létre aláírásokat. Megadhatja azt, hogy hiba esetén az alkalmazás állítsa le az objektumok aláírását, vagy hogy folytassa az aláírási eljárást valamelyik másik objektumon.

- **Ismétlődő objektum aláírás**
  Megadhatja, hogyan kezelje az alkalmazás az aláírási folyamatot, amikor az alkalmazás újra aláírja az objektumot. Megadhatja azt, hogy hagyja változatlanul a helyén az eredeti aláírást, illetve azt, hogy cserélje le az eredeti aláírást az újjal.
- **Objektumok alkönyvtárakban**
  Megadhatja, hogyan kezelje az alkalmazás az alkönyvtárakban lévő aláírandó objektumokat. Megadhatja azt, hogy az alkalmazás egyedileg írja alá az alkönyvtárakban lévő objektumokat, vagy azt, hogy az alkalmazás csak a főkönyvtárban lévő objektumokat írja alá, és közben az összes alkönyvtárat hagyja figyelmen kívül.
- **objektum aláírás hatásköre**
  Amikor *CMD objektumokat ír alá, megadhatja, hogy a teljes objektumot írja alá vagy csak annak magját (részleges).

Aláírás ellenőrzés feldolgozása

A következő paramétereket adhatja meg az aláírás feldolgozáshoz.

- **Hiba feldolgozás**
  Megadhatja, hogy milyen típusú hiba feldolgozást végezzen az alkalmazás, amikor egynél több objektumon ellenőriz aláírásokat. Megadhatja azt, hogy hiba esetén az alkalmazás állítsa le az aláírás ellenőrzését, vagy hogy folytassa az aláírás ellenőrzését valamelyik másik objektumon.
- **Objektumok alkönyvtárakban**
  Megadhatja, hogyan kezelje az alkalmazás az alkönyvtárakban lévő objektumok aláírásának ellenőrzését. Megadhatja azt, hogy az alkalmazás egyedileg ellenőrizze az alkönyvtárakban lévő objektumok aláírását, vagy azt, hogy az alkalmazás csak a főkönyvtárban lévő objektumok aláírásait ellenőrizze, és közben az összes alkönyvtárat hagyja figyelmen kívül.
- **Részleges és teljes aláírás ellenőrzés**
  Rendszer szabályok vannak arra, hogyan kezelje a rendszer az objektumokon található részleges (vagy mag) és teljes aláírásokat az ellenőrzési folyamat során. A szabályok a következők:
  - Ha nincs aláírás az objektumon, az ellenőrzési folyamat jelenti, hogy az objektum nincs aláírva, és folytatja az ellenőrzést a következő objektumon.
  - Ha az objektum megbízható rendszerrel (IBM) lett aláírva, az aláírásoknak egyezni kell, vagy az ellenőrzés sikertelen lesz. Ha egyezik az aláírás, az ellenőrzési folyamat folytatódik. Az aláírás az objektum adatainak egyfajta titkosított, matematikai összegzése. Ennek következtében az aláírás akkor tekinthető egyezőnek, ha az objektum adatai az ellenőrzés során megegyeznek az objektum aláíráskori adataival.
  - Ha az objektum rendelkezik olyan teljes objektum aláírásokkal, amelyek megbízhatóak (a *SIGNATUREVERIFICATION igazolás tárolóban lévő igazolás alapján), akkor az aláírások legalább egyikének egyezni kell, vagy az ellenőrzési folyamat sikertelen lesz. Ha legalább egy teljes objektum aláírás egyezik, az ellenőrzési folyamat folytatódik.
  - Ha az objektum részleges objektum aláírásokkal rendelkezik, amelyek megbízhatóak, akkor legalább ezek egyikének egyezni kell a *SIGNATUREVERIFICATION igazolás tárolóban lévő igazolással, vagy az ellenőrzési folyamat sikertelen lesz. Ha legalább egy részleges objektum aláírás egyezik, az ellenőrzési folyamat folytatódik.

Objektum aláírás és aláírás ellenőrzés előfeltételei

Az OS/400 objektum aláírási és aláírás ellenőrzési funkciója további hatékony eszközt jelent az objektumok vezérlésében az iSeries szerveren. Ahhoz, hogy kihasználhassa a funkciók előnyeit, tegyen eleget használatuk előfeltételeinek.

Az objektum aláírás előfeltételei

Számtalan módszer áll rendelkezésére, amelyek révén objektumokat írhat alá (üzleti és biztonsági szükségleteitől függően):

- Használhatja a Digitális igazolás kezelőt (DCM).
- Írhat egy programot, amely a Sign Object API-t használja.
- Az iSeries navigátor Kezelőközpont funkciójával is aláírhat objektumokat, amikor összecsomagolja őket iSeries végpont rendszereknek való terjesztés céljából.

Az objektumok aláírásához választandó módszer üzleti és biztonsági elvárásaitól függ. Függetlenül az objektumok aláírásához használni kívánt módszertől, győződjön meg arról, hogy eleget tesz bizonyos előfeltételeknek:

- Eleget kell tennie a Digitális igazolás kezelő (DCM) telepítésével és használatával kapcsolatos előfeltételeknek.
  - A DCM segítségével kell létrehozni az *OBJECTSIGNING igazolás tárolót. Az igazolás tárolót létrehozhatja a Helyi igazolási hatóság (CA) létrehozási folyamatának részeként, vagy a nyilvános Internet CA-tól eredő objektum aláíró igazolások kezelési folyamatának részeként.
  - Az *OBJECTSIGNING igazolás tárolónak legalább egy igazolást tartalmaznia kell, amelyet vagy a Helyi CA segítségével hozott létre, vagy egy nyilvános Internet CA-tól szerzett be.
  - A DCM felhasználásával létre kell hozni legalább egy objektum aláíró alkalmazás definícióját, amelyet az objektumok aláírására használ.
  - A DCM segítségével hozzá kell rendelni az adott igazolást az objektum aláíró alkalmazás definíciójához.
- Az objektumokat aláíró iSeries felhasználói profilnak *ALLOBJ különleges jogosultsággal kell rendelkeznie. A *SIGNATUREVERIFICATION igazolás tárolót létrehozó iSeries felhasználói profilnak *SECADM és *ALLOBJ különleges jogosultsággal kell rendelkeznie.

Az aláírás ellenőrzés előfeltételei

Számtalan módszer áll rendelkezésére, amelyek révén ellenőrizheti az objektumokon lévő aláírásokat:

- Használhatja a Digitális igazolás kezelőt (DCM).
- Írhat egy programot amely a Verify Object (QYDOVFYO) API-t használja.
- Használhatja számtalan parancs egyikét, mint például a Check Object Integrity (CHKOBJITG) parancsot.

Az aláírások ellenőrzéséhez választandó módszer üzleti és biztonsági elvárásaitól függ. Függetlenül az használni kívánt módszertől, győződjön meg arról, hogy eleget tesz bizonyos előfeltételeknek:

- Eleget kell tennie a Digitális igazolás kezelő (DCM) telepítésével és használatával kapcsolatos előfeltételeknek.
- Létre kell hozni az *OBJECTSIGNING igazolás tárolót. Ezt a tárolót két módszer közül azzal hozhatja létre, amelyik igényének jobban megfelel. Létrehozhatja a Digitális igazolás kezelővel (DCM), amikor az aláírás ellenőrző igazolásokat kezeli. Vagy, ha nyilvános igazolást használ az objektumok aláírásához, akkor létrehozhatja az igazolás tárolót úgy is, hogy ír egy programot, amely az Add Verifier (QYDOADDV) API-t használja.

  Megjegyzés: Az Add Verifier API alapértelmezett jelszóval hozza létre az igazolás tárolót. A DCM segítségével meg kell változtatni ezt az alapértelmezett jelszót egy saját kiválasztású jelszóra a jogosulatlan hozzáférés megakadályozása érdekében.
- A *SIGNATUREVERIFICATION igazolás tároló tartalmazza az objektumot aláíró igazolás egy példányát. Az igazolást kétféleképpen adhatja hozzá az igazolás tárolóhoz. Az aláíró rendszeren a DCM segítségével exportálja az igazolást egy fájlba, majd az ellenőrzést végző rendszeren a DCM segítségével importálja az igazolást a *SIGNATUREVERIFICATION igazolás tárolóba. Vagy, ha nyilvános igazolást használ az objektumok aláírásához, akkor hozzáadhatja az igazolást az ellenőrzést végző rendszerek igazolás tárolójához úgy is, hogy ír egy programot, amely az Add Verifier API-t használja.
- A *SIGNATUREVERIFICATION igazolás tároló tartalmazza a CA igazolás egy példányát, amely kiadta az objektumokat aláíró igazolást. Ha nyilvános igazolást használ az objektumok aláírásához, akkor az ellenőrzést végző rendszer igazolás tárolójában már rendelkeznie kell a szükséges CA igazolás egy

példányával. Azonban, ha Helyi CA által kiadott igazolást használ az objektumok aláírásához, akkor a DCM segítségével kell hozzáadni a Helyi CA igazolás egy példányát az ellenőrzést végző rendszer igazolás tárolójához.

Megjegyzés: Biztonsági okokból az API nem teszi lehetővé az Igazolási hatóság (CA) igazolásának elhelyezését a *SIGNATUREVERIFICATION igazolás tárolóba. Amikor a CA igazolását hozzáadja az igazolás tárolóhoz, a rendszer az igazolások megbízható forrásának ismeri el a CA-t. Következésképpen, a rendszer a CA által kiadott igazolást úgy kezeli, mint amelyik megbízható forrásból ered. Ennek következtében, az API-val nem hozhat létre telepítési programot, amely elhelyezné a CA igazolást az igazolás tárolóba. A Digitális igazolás kezelőt kell ahhoz használni, hogy hozzáadja a CA igazolást az igazolás tárolóhoz. Így garantálja, hogy valaki kimondottan és kézi módon meghatározza, mely CA-kat tekintse a rendszer megbízhatónak. Így cselekedve megakadályozza annak lehetőségét, hogy a rendszer olyan forrásból importáljon igazolásokat, amelyeket az adminisztrátor tudta nélkül tekint a rendszer megbízhatónak.

Ha Helyi CA által kiadott igazolást használ az objektumok aláírásához, akkor a Helyi CA-t üzemeltető iSeries szerveren a DCM segítségével exportálja a Helyi CA igazolást egy fájlba. Majd ezután az aláírást ellenőrző iSeries szerveren a DCM segítségével importálja a Helyi CA igazolást a *SIGNATUREVERIFICATION igazolás tárolóba. Az esetleges hibák megakadályozása érdekében, először a Helyi CA igazolást importálja, mielőtt használná az Add Verifier API-t, amivel az aláírás ellenőrző igazolást adná hozzá. Következésképpen, ha Helyi CA által kibocsátott igazolást használ, egyszerűbbnek találhatja, hogy a DCM segítségével mind a CA igazolást, mind az aláírás ellenőrző igazolást importálja az igazolás tárolóba.

Ha azt akarja, hogy senki se használhassa ezt az API-t arra a célra, hogy ellenőrző igazolást adjon hozzá a *SIGNATUREVERIFICATION igazolás tárolóhoz a tudta nélkül, akkor vegye fontolóra az API letiltását a rendszeren. A Rendszer szervizeszközök (SST) segítségével utasíthatja vissza a biztonsággal kapcsolatos rendszerváltozók módosításait.

- Az aláírásokat ellenőrző iSeries felhasználói profilnak *AUDIT különleges jogosultsággal kell rendelkeznie. A *SIGNATUREVERIFICATION igazolás tárolót létrehozó vagy a jelszót módosító iSeries felhasználói profilnak *SECADM és *ALLOBJ különleges jogosultsággal kell rendelkeznie.

Az aláírt objektumok kezelése

A V5R1 változat óta az IBM aláírja az OS/400 licencprogramokat és PTF-eket. Így az operációs rendszeren jelezve van, hogy az IBM-től ered, másrészt észlelhető, ha a rendszer objektumoknál jogosulatlan változtatás történik. Az üzleti partnerek és más szállítók is aláírhatják az alkalmazásokat, amelyeket a felhasználó megvásárol. Következésképpen, még ha nem is ír alá saját maga objektumokat, ismerni kell az aláírt objektumok kezelését, valamint hatásukat a napi rendszer adminisztrációs feladatokra.

Az aláírt objektumok elsődlegesen a biztonsági mentési és helyreállítási feladatokra vannak hatással, különösen arra, hogyan mentheti az objektumokat és hogyan állíthatja vissza őket a rendszeren.

Aláírt objektumokra ható rendszerváltozók és parancsok
Megismerheti azokat a rendszerváltozókat és parancsokat, amelyekkel kezelheti az aláírt objektumokat, illetve amelyek hatással vannak az aláírt objektumokra, amikor futtatja őket.

Mentési és visszaállítási szempontok aláírt objektumoknál
Megismerheti, hogyan befolyásolják az aláírt objektumok a mentési és visszaállítási feladatok végrehajtását a rendszeren.

Kód ellenőrző parancsok az aláírás sértetlenségéért
Részletesen tanulmányozhatja az objektum aláírást ellenőrző parancsok használatát, amelyekkel meghatározhatja az objektum sértetlenségét.

Aláírt objektumokra ható rendszerváltozók és parancsok

Az aláírt objektumok hatékony kezeléséhez meg kell ismerni a rendszerváltozók és a parancsok hatását az aláírt objektumokra. A **Verify object signatures during restore** (QVFYOBJRST) rendszerváltozó meghatározza, hogy bizonyos visszaállítási parancsok hogyan hatnak az aláírt objektumokra, és a rendszer hogyan kezeli az aláírt objektumokat a visszaállítási műveletek során. Nincs olyan CL parancs, amely kizárólag aláírt objektumok kezelésére szolgálna az iSeries rendszeren. Ugyanakkor, számos általános CL parancs van, amelyekkel kezelhet aláírt objektumokat (vagy olyan infrastruktúra objektumokat, amelyek lehetővé teszik az objektum aláírását). Más parancsok ellentétesen hatnak az aláírt objektumokra a rendszeren. Például eltávolítják az aláírást az objektumról, amellyel hatástalanítják az aláírás nyújtotta védelmet.

Aláírt objektumokra hatással lévő rendszerváltozók

A **Verify object signatures during restore** (QVFYOBJRST) a visszaállításra vonatkozó OS/400 rendszerváltozók egyik tagja. Meghatározza, hogy milyen hatással vannak a parancsok az aláírt objektumokra a rendszeren. Ez a rendszerváltozó (amelyet az iSeries navigátoron keresztül ér el) vezérli, hogy a rendszer hogyan kezeli az aláírás ellenőrzését visszaállítás közben. A rendszerváltozó beállítása két másik rendszerváltozóval összekapcsolódva befolyásolja a visszaállítási műveleteket a rendszeren. Attól függően, hogy milyen értéket ad meg ide, vagy engedélyezi vagy letiltja az objektumok visszaállítását aláírásuk állapota alapján. (Például, ha nincs aláírva az objektum, vagy ha érvénytelen az aláírás, illetve ha megbízható forrás írta alá, stb.) A rendszerváltozó alapértéke megengedi az aláíratlan objektumok visszaállítását, míg az aláírt objektumok visszaállítását csak akkor engedi, ha az objektumok érvényes aláírással rendelkeznek. A rendszer csak akkor tekinti ″aláírtnak″ az objektumot, ha olyan aláírással rendelkezik, amelyet a rendszer megbízhatónak ítél. A rendszer figyelmen kívül hagyja az objektumon lévő egyéb, ″nem megbízható″ aláírásokat, és úgy kezeli az objektumot, mint a nem aláírtakat.

A QVFYOBJRST rendszerváltozó több értéket vehet fel, kezdve az összes aláírás mellőzésétől, egészen az érvényes aláírás megköveteléséig az összes olyan objektum számára, amelyet a rendszer visszaállít. A rendszerváltozó értéke csak a végrehajtható, visszaállítás alatt lévő objektumokra van hatással, mint például programokra (*PGM), parancsokra (*CMD), szerviz programokra (*SRVPGM), SQL csomagokra (*SQLPKG) és modulokra (*MODULE). A Create Java Program (CRTJVAPGM) parancs révén létrehozott Java programokhoz tartozó adatfolyam fájlokra (*STMF) is hatással van. Ugyanakkor hatástalan a mentési (*SAV) és az IFS fájlokra.

A rendszerváltozókról többet megtudhat az Információs központ Rendszerváltozó kereső című részében.

Aláírt objektumokra hatással lévő CL parancsok

Számos olyan CL parancs van, amelyik engedélyezi az aláírt objektumokkal történő műveleteket, vagy amelyik hatással van az iSeries szerveren található aláírt objektumokra. Különféle parancsokat használhat fel az objektumok aláírási információinak megtekintéséhez, az objektumokon lévő aláírások ellenőrzéséhez, valamint az aláírások ellenőrzéséhez szükséges biztonsági objektumok mentéséhez és visszaállításához. Továbbá, van a parancsoknak egy olyan csoportja, amelyek futáskor el tudják távolítani az aláírásokat az objektumokról, és így hatástalanítják az aláírás nyújtotta biztonságot.

Az objektum aláírásának megjelenítésére szolgáló parancsok

- Display Object Description (DSPOBJD) parancs.
  Ez a parancs megmutatja az adott könyvtárban vagy a feldolgozási szál könyvtárlistájának könyvtáraiban lévő megadott objektumok neveit és tulajdonságait. A parancs segítségével meghatározhatja, hogy az objektum alá van-e írva, és megtekintheti az aláírás információit.
- Display Object Links (DSPLNK) és Work with Object Links (WRKLNK) integrált fájlrendszer parancsok.
  A parancsok révén megjelenítheti az integrált fájlrendszerbeli objektum aláírásának információit.

Objektum aláírások ellenőrzésére szolgáló parancsok

- Check Object Integrity (CHKOBJITG) parancs.
  Ez a parancs lehetővé teszi annak meghatározását, hogy a rendszeren lévő objektumok épsége nem sérült-e. A parancs segítségével ellenőrizheti az aláírásokat, nagyon hasonlóan ahhoz, ahogy a vírus ellenőrző meghatározza, hogy a vírus rombolta-e a fájlokat vagy más objektumokat a rendszeren. A parancs aláírt vagy aláírható objektumokkal való használatáról többet megtudhat a Kód ellenőrző parancsok az aláírás épségének biztosításához című részben.
- Check Product Option (CHKPRDOPT) parancs.
  A parancs jelenti a helyes szerkezet és a tényleges szerkezet vagy a szoftvertermék közötti különbségeket. Például, a parancs hibát jelez, ha a telepített termék egyik objektumát törölte. A CHKSIG paraméter segítségével megadhatja, hogyan kezelje és jelentse a parancs a termék aláírásával kapcsolatos problémákat. A parancs aláírt vagy aláírható objektumokkal való használatáról többet megtudhat a Kód ellenőrző parancsok az aláírás épségének biztosításához című részben.
- Save Licensed Program (SAVLICPGM) parancs.
  Ez a parancs elmenti az objektumok egy példányát, amelyből egy licencprogram állítható elő. Olyan formában őrzi meg a licencprogramot, amelyet a Restore Licensed Program (RSTLICPGM) parancs vissza tud állítani. A CHKSIG paraméter segítségével megadhatja, hogyan kezelje és jelentse a parancs a termék aláírásával kapcsolatos problémákat. A parancs aláírt vagy aláírható objektumokkal való használatáról többet megtudhat a Kód ellenőrző parancsok az aláírás épségének biztosításához című részben.
- Restore (RST) parancs.
  Ez a parancs visszaállítja egy vagy több objektum egy példányát, amelyek az integrált fájlrendszerben (IFS) használhatók. Ezzel a paranccsal igazolás tárolókat is visszaállíthat a rendszeren tartalmukkal együtt. Azonban, nem lehet vele visszaállítani a *SIGNATUREVERIFICATION igazolás tárolót. A visszaállítás során a Verify object signatures (QVFYOBJRST) rendszerváltozó beállításától függ az, hogyan kezeli az aláírt és az aláírható objektumokat a visszaállítási parancs.
- Restore Library (RSTLIB) parancs.
  Ezzel a paranccsal olyan könyvtárat vagy könyvtárak csoportját állíthatja vissza, amelyeket a Save Library (SAVLIB) paranccsal mentett el. A RSTLIB parancs visszaállítja a teljes könyvtárat, ami magában foglalja a könyvtár és az objektum leírását, valamint a könyvtárban lévő objektumok tartalmát. A Verify object signatures (QVFYOBJRST) rendszerváltozó beállításától függ az, hogyan kezeli az aláírt és az aláírható objektumokat a visszaállítási parancs.
- Restore Licensed Program (RSTLICPGM) parancs.
  Ezzel a paranccsal licencprogramot tölthet be vagy állíthat vissza, akár kezdeti telepítés, akár új változat telepítése esetén. A Verify object signatures (QVFYOBJRST) rendszerváltozó beállításától függ az, hogyan kezeli az aláírt és az aláírható objektumokat a visszaállítási parancs.
- Restore object (RSTOBJ) parancs.
  Ezzel a paranccsal egyetlen könyvtár egy vagy több objektumát állíthatja vissza, amelyeket hajlékonylemezen, szalagon, optikai köteten vagy mentési fájlban mentett el. A Verify object signatures (QVFYOBJRST) rendszerváltozó beállításától függ az, hogyan kezeli az aláírt és az aláírható objektumokat a visszaállítási parancs.

Igazolás tárolók mentésére és visszaállítására szolgáló parancsok

- Save (SAV) parancs.
  Ez a parancs elmenti egy vagy több objektum egy példányát, amelyek az integrált fájlrendszerben használhatók. Azonban, nem lehet vele elmenteni a *SIGNATUREVERIFICATION igazolás tárolót.
- Save Security Data (SAVSECDTA) parancs.
  Ezzel a paranccsal úgy mentheti el az összes biztonsági információt, hogy nem kell a rendszert korlátozott állapotba tenni. A parancs lehetővé teszi a *SIGNATUREVERIFICATION igazolás tároló és tartalmának mentését. A parancs semmilyen más igazolás tárolót nem ment el.
- Save System (SAVSYS) parancs.
  A parancs lehetővé teszi a belső kód (LIC) és a QSYS könyvtár mentését az iSeries szerver telepítésével kompatíbilis formában. Egyetlen más könyvtárból sem ment el objektumokat. Továbbá, lehetővé teszi a

biztonsági és a konfigurációs objektumok mentését, amelyeket SAVSECDTA és SAVCFG parancsokkal ugyancsak menthet. A parancs lehetővé teszi a *SIGNATUREVERIFICATION igazolás tároló és tartalmának mentését.

- Restore (RST) parancs.
  Ezzel a paranccsal igazolás tárolókat állíthat vissza a rendszeren tartalmukkal együtt. Azonban, nem lehet vele visszaállítani a *SIGNATUREVERIFICATION igazolás tárolót.
- Restore User Profiles (RSTUSRPRF) parancs.
  A parancs lehetővé teszi a Save System (SAVSYS) vagy a Save Security Data (SAVSECDTA) parancsokkal mentett felhasználói profil vagy profil halmaz alapvető részeinek visszaállítását. A parancsot alkalmazhatja a *SIGNATUREVERIFICATION igazolás tároló, valamint az ehhez és az összes többi igazolás tárolóhoz tartozó rejtett jelszavak visszaállításához. A *SIGNATUREVERIFICATION igazolás tárolót visszaállíthatja a felhasználói profil adatai nélkül is, ha *DCM értéket ad meg a SECDTA paraméterre és *NONE értéket az USRPRF paraméterre. Adjon meg *ALL értéket a USRPRF paraméterre, ha ezzel a paranccsal kívánja visszaállítani a felhasználói profil információit, valamint az igazolás tárolókat és jelszavaikat.

Aláírások eltávolítására vagy elhagyására szolgáló parancsok

Amikor az alábbi parancsokat alkalmazza egy aláírt objektumon, akkor ezt olyan módon is megteheti, hogy eltávolítja vagy lehagyja az aláírást az objektumról. Az aláírás eltávolítása problémákat okozhat az objektum szempontjából. Végül is, a továbbiakban nem tudja ellenőrizni az objektum forrását megbízhatóságra, és nem tudja az aláírás ellenőrzésével észlelni az objektum változásait. A parancsokat csak a saját maga által aláírt objektumokon alkalmazza (ellentétben azokkal az aláírt objektumokkal, amelyeket mástól szerez be, például IBM vagy szállítók). Ha aggódik amiatt, hogy a parancs esetleg eltávolította vagy elhagyta az objektum aláírást, a Display Object Description (DSPOBJD) parancs segítségével megnézheti, hogy az aláírás ott van-e, és írja újra alá, ha szükséges.

Megjegyzés: Ha ellenőrizni akarja, hogy a Save parancs elhagyta-e az objektum aláírását, akkor állítsa vissza az objektumot egy másik könyvtárba, mint ahonnan mentette (például QTEMP). Azután a DSPOBJD parancs segítségével meghatározhatja, hogy a mentési adathordozón lévő objektum rendelkezik-e aláírással.

- Change Program (CHGPGM) parancs.
  Ez a parancs módosítja a program tulajdonságait a program újrafordítása nélkül. A parancs segítségével elérheti a program ismételt előállítását még akkor is, ha a megadott tulajdonságok megegyeznek a pillanatnyi tulajdonságokkal.
- Change Service Program (CHGSRVPGM) parancs.
  Ez a parancs módosítja a szervizprogram tulajdonságait a program újrafordítása nélkül. A parancs segítségével elérheti a szervizprogram ismételt előállítását még akkor is, ha a megadott tulajdonságok megegyeznek a pillanatnyi tulajdonságokkal.
- Clear Save File (CLRSAVF) parancs.
  Ez a parancs törli a mentési fájl tartalmát, törli a mentési fájl összes meglévő rekordját, és csökkenti a fájl által használt tárolóterület nagyságát.
- Save (SAV) parancs.
  Ez a parancs elmenti egy vagy több objektum egy példányát, amelyek az integrált fájlrendszerben használhatók. — Amikor ezt a parancsot használja, elveszti a mentési adathordozón található parancs (*CMD) objektumokon lévő aláírást, ha a TGTRLS paraméterre V5R2M0 értéknél korábbit ad meg. Az aláírást azért veszíti el, mert a parancs objektumokat nem lehet aláírni a V5R2 előtti változatokban.
- Save Library (SAVLIB) parancs.
  Ez a parancs lehetővé teszi egy vagy több könyvtár egy példányának mentését. Amikor ezt a parancsot használja, elveszti a mentési adathordozón található parancs (*CMD) objektumokon lévő aláírást, ha a TGTRLS paraméterre V5R2M0 értéknél korábbit ad meg. Az aláírást azért veszíti el, mert a parancs objektumokat nem lehet aláírni a V5R2 előtti változatokban.
- Save Object (SAVOBJ) parancs.
  Ezzel a paranccsal egyetlen objektumot vagy egyazon könyvtárban található objektumcsoportot menthet.

Amikor ezt a parancsot használja, elveszti a mentési adathordozón található parancs (*CMD) objektumokon lévő aláírást, ha a TGTRLS paraméterre V5R2M0 értéknél korábbit ad meg. Az aláírást azért veszíti el, mert a parancs objektumokat nem lehet aláírni a V5R2 előtti változatokban.

Mentési és visszaállítási szempontok aláírt objektumoknál

Számos rendszerváltozó van, amelyek hatással vannak a visszaállítási műveletekre az iSeries szerveren. Közülük csupán egy (a **Verify object signatures during restore (QVFYOBJRST)** rendszerváltozó) határozza meg, hogyan kezelje a rendszer az aláírt objektumokat visszaállításuk során. A kérdéses rendszerváltozó értékének kiválasztásával eldöntheti, hogyan kezelje a visszaállítási művelet az érvénytelen aláírású vagy az aláírás nélküli objektumok ellenőrzését.

Néhány mentési és visszaállítási parancs hatással van az aláírt objektumokra, illetve meghatározzák, hogyan kezelje a rendszer az aláírt és az aláírás nélküli objektumokat a mentési és a visszaállítási műveletek során. Feltétlenül ismerkedjen meg ezekkel a parancsokkal és az aláírt objektumokra való hatásukkal, hogy jobban kezelhesse a rendszert, és elkerülje az esetleges problémákat.

Az alábbi parancsok ellenőrizhetik az objektumokat a mentési és a visszaállítási műveletek során:

- Save Licensed Program (SAVLICPGM) parancs.
- Restore (RST) parancs.
- Restore Library (RSTLIB) parancs.
- Restore Licensed Program (RSTLICPGM) parancs.
- Restore object (RSTOBJ) parancs.

Az alábbi parancsok lehetővé teszik, hogy mentse és visszaállítsa az igazolás tárolókat. Az igazolás tárolók biztonság érzékeny objektumok, amelyek objektumok aláírásához és aláírások ellenőrzéséhez szükséges igazolásokat tartalmaznak:

- Save (SAV) parancs.
- Save Security Data (SAVSECDTA) parancs.
- Save System (SAVSYS) parancs.
- Restore (RST) parancs.
- Restore User Profiles (RSTUSRPRF) parancs.

A használt paraméterértékektől függően, egyes mentési parancsok elhagyhatják az aláírást a mentési adathordozóra kerülő objektumról, ami hatástalanítja az aláírás nyújtotta biztonságot. Például, *minden olyan* mentési művelet során, amelyben (*CMD) objektumot V5R2M0 szintnél régebbi célváltozatra ment, aláírás nélkül lesz mentve az objektum. Az aláírás eltávolítása problémákat okozhat az objektumok szempontjából. Végül is, a továbbiakban nem tudja ellenőrizni az objektum forrását megbízhatóságra, és nem tudja az aláírás ellenőrzésével észlelni az objektum változásait. A parancsokat csak a saját maga által aláírt objektumokon alkalmazza (ellentétben azokkal az aláírt objektumokkal, amelyeket mástól szerez be, például IBM vagy szállítók).

Megjegyzés: Ha ellenőrizni akarja, hogy a Save parancs elhagyta-e az objektum aláírását, akkor állítsa vissza az objektumot egy másik könyvtárba, mint ahonnan mentette (például QTEMP). Azután a DSPOBJD parancs segítségével meghatározhatja, hogy a mentési adathordozón lévő objektum rendelkezik-e aláírással.

Erre a potenciális lehetőségre általánosságban is figyelni kell a mentési parancsoknál, de az alábbiaknál különösen:

- Save (SAV) parancs.
- Save Library (SAVLIB) parancs.
- Save Object (SAVOBJ) parancs.

Ha további információkra tart igényt a parancsok aláírt objektumokra és objektum aláírásokra gyakorolt hatásáról mentés és visszaállítás közben, olvassa el az Aláírt objektumokra ható rendszerváltozók és parancsok című részt.

Kód ellenőrző parancsok az aláírás sértetlenségéért

Digitális igazolás kezelő (DCM) vagy API-k segítségével ellenőrizheti az objektumokon lévő digitális aláírásokat. Több parancsot is felhasználhat az aláírások ellenőrzéséhez. A parancsok segítségével ellenőrizheti az aláírásokat, nagyon hasonlóan ahhoz, ahogy a vírus ellenőrző meghatározza, hogy a vírus rombolta-e a fájlokat vagy más objektumokat a rendszeren. Az aláírások többségét akkor ellenőrzi, amikor az objektumot visszaállítja vagy telepíti a rendszeren, például az RSTLIB parancs alkalmazásával.

A már rendszeren lévő objektumok aláírásainak ellenőrzéséhez három rendelkezésre álló parancs egyikét választhatja. A Check Object Integrity (CHKOBJITG) parancs kifejezetten az objektum aláírások ellenőrzésére szolgál. Az egyes parancsoknál az aláírás ellenőrzését a CHKSIG paraméter vezérli. Ez a paraméter lehetővé teszi, hogy ellenőrizze az összes objektumtípust esetleges aláírásra, figyelmen kívül hagyja az összes aláírást, illetve hogy csak az aláírt objektumokat ellenőrizze. A paraméter alapértelmezett érték az utolsó beállítás.

Check Object Integrity (CHKOBJITG) parancs

A Check Object Integrity (CHKOBJITG) parancs lehetővé teszi annak meghatározását, hogy a rendszeren lévő objektumok épsége nem sérült-e. A parancs segítségével ellenőrizheti azon objektumok sértetlenségét, amelyeket egy adott felhasználói profil tulajdonol, amelyeknek egy adott útvonalnévvel egyező elérési útvonaluk van, illetve a rendszeren lévő összes objektumot. Az objektum sérüléséről az alábbi feltételek egyikének teljesülése esetén készül naplóbejegyzés:

- A parancs, a program, a modul objektum vagy a könyvtár tulajdonságai megváltoztak.
- Az objektumon lévő digitális aláírás érvénytelennek minősül. Az aláírás az objektum adatainak egyfajta titkosított, matematikai összegzése. Ennek következtében az aláírás akkor tekinthető egyezőnek, ha az objektum adatai az ellenőrzés során megegyeznek az objektum aláíráskori adataival. Az aláírás érvénytelensége azon az alapon dől el, hogy az objektum aláírásakor létrehozott titkosított matematikai összegzést összehasonlítja az aláírás ellenőrzésekor előálló titkosított matematikai összegzéssel. Az aláírás ellenőrzési folyamat összehasonlítja a két összegzési értéket. Ha az értékek nem egyeznek, akkor az objektum tartalma megváltozott az aláírás óta, s ezért az aláírás érvénytelennek tekinthető.
- Az objektum tartomány attribútuma érvénytelen az objektumtípusra.

Ha a parancs az objektum sérülését észleli, akkor feljegyzi az objektum nevét, a könyvtár nevét (vagy az útvonal nevét), az objektum típusát, az objektum tulajdonosát és a hiba típusát a naplófájlba. A parancs néha más esetekben is készít naplóbejegyzést, még ha ezek nem is sérülésre vonatkoznak. Például, a parancs olyan objektumokról is készít bejegyzést, amelyek ugyan aláírhatók, de nincs hozzájuk digitális aláírás, vagy amelyek nem ellenőrizhetők, illetve olyan formátumban lévő objektumokról, amelyek módosítást igényelnek az aktuális rendszer használatához (IMPI - RISC konverzió).

A CHKSIG paraméter értéke vezérli, hogy a parancs hogyan kezelje az objektumokon lévő digitális aláírásokat. A paraméterre három lehetséges érték közül kell egyet megadni:

- *SIGNED – Amikor ezt adja meg, a parancs a digitális aláírással rendelkező objektumokat ellenőrzi. A parancs naplóbejegyzést készít minden olyan objektumról, amelynek érvénytelen az aláírása. Ez az alapértelmezett érték.
- *ALL – Amikor ezt az értéket adja meg, a parancs ellenőrzi az összes aláírható objektumot, hogy meghatározza, rendelkeznek-e aláírással. A parancs naplóbejegyzést készít minden olyan aláírható objektumról, amelynek nincs aláírása, valamint azokról is, amelyeknek az aláírása érvénytelen.
- *NONE – Amikor ezt az értéket adja meg, a parancs nem ellenőrzi az objektumokon lévő aláírásokat.

Check Product Option (CHKPRDOPT) parancs

A Check Product Option (CHKPRDOPT) parancs jelenti a helyes szerkezet és a tényleges szerkezet vagy a szoftvertermék közötti különbségeket. Például, a parancs hibát jelez, ha a telepített termék egyik objektumát törölte.

A CHKSIG paraméter értéke vezérli, hogy a parancs hogyan kezelje az objektumokon lévő digitális aláírásokat. A paraméterre három lehetséges érték közül kell egyet megadni:

- *SIGNED – Amikor ezt adja meg, a parancs a digitális aláírással rendelkező objektumokat ellenőrzi. A parancs ellenőrzi az aláírt objektumokon lévő aláírásokat. Ha a parancs meghatározza, hogy az objektumon lévő aláírás érvénytelen, a parancs üzenetet küld a feladatnaplóba és azonosítja a hibás állapotban lévő terméket. Ez az alapértelmezett érték.
- *ALL – Amikor ezt az értéket adja meg, a parancs ellenőrzi az összes aláírható objektumot, hogy meghatározza, rendelkeznek-e aláírással és ellenőrizze az objektumokon lévő aláírást. A parancs üzenetet küld a feladatnaplóba azokról az aláírható objektumokról, amelyek nincsenek aláírva. Azonban a parancs nem azonosítja hibásként a terméket. Ha a parancs meghatározza, hogy az objektumon lévő aláírás érvénytelen, a parancs üzenetet küld a feladatnaplóba és a terméket hibásnak állítja be.
- *NONE – Amikor ezt az értéket adja meg, a parancs nem ellenőrzi a termék objektumokon lévő aláírásokat.

Save Licensed Program (SAVLICPGM) parancs

A Save Licensed Program (SAVLICPGM) parancs lehetővé teszi az objektumok egy példányának mentését, amelyből egy licencprogram állítható elő. Olyan formában őrzi meg a licencprogramot, amelyet a Restore Licensed Program (RSTLICPGM) parancs vissza tud állítani.

A CHKSIG paraméter értéke vezérli, hogy a parancs hogyan kezelje az objektumokon lévő digitális aláírásokat. A paraméterre három lehetséges érték közül kell egyet megadni:

- *SIGNED – Amikor ezt adja meg, a parancs a digitális aláírással rendelkező objektumokat ellenőrzi. A parancs ellenőrzi az aláírt objektumokon lévő aláírásokat, de nem ellenőrzi az aláírás nélküli objektumokat. Ha a parancs meghatározza, hogy az objektumon lévő aláírás érvénytelen, a parancs üzenetet küld a feladatnaplóba és azonosítja az objektumot, a mentés pedig meghiúsul. Ez az alapértelmezett érték.
- *ALL – Amikor ezt az értéket adja meg, a parancs ellenőrzi az összes aláírható objektumot, hogy meghatározza, rendelkeznek-e aláírással és ellenőrizze az objektumokon lévő aláírást. A parancs üzenetet küld a feladatnaplóba azokról az aláírható objektumokról, amelyek nincsenek aláírva. Azonban a mentési folyamat nem fejeződik be. Ha a parancs meghatározza, hogy az objektumon lévő aláírás érvénytelen, a parancs üzenetet küld a feladatnaplóba és a mentés meghiúsul.
- *NONE – Amikor ezt az értéket adja meg, a parancs nem ellenőrzi a termék objektumokon lévő aláírásokat.

Aláírt objektumok hibaelhárítása

A következő táblázat hasznos információkkal szolgál az iSeries objektum aláírási és aláírás ellenőrző funkciói néhány olyan általános problémájának hibaelhárításáról, amelyekkel találkozhat a működés során.

Objektum aláírás általános problémái

Probléma	Lehetséges megoldás
Amikor Sign Object API-val ír alá V4R5 vagy korábbi szintű objektumot, az aláírási folyamat sikertelen lesz és az objektum nem lesz aláírva (CPFB721 hibaüzenet).	Az iSeries nem támogatja az objektum aláírást V5R1 előtti változatoknál. CPFB721 hibajelzést visszaadó objektumok esetén, hozza létre újból a kérdéses programokat V5R1 vagy újabb változaton, aláírás céljából.

Aláírás ellenőrzés általános problémái

Probléma	Lehetséges megoldás
A visszaállítás sikertelen aláírás nélküli objektumok esetén.	Ha az aláírás hiánya nem játszik szerepet, ellenőrizze, hogy a QVFYOBJRST rendszerváltozó 5-ös értékre van-e beállítva. Az 5-ös érték azt adja meg, hogy az aláírás nélküli objektumok nem állíthatók vissza. Változtassa meg 3-as értékre, és próbálja meg ismét a visszaállítást.
A visszaállítás sikertelen aláírással rendelkező objektumok esetén.	Ez akkor fordulhat elő, ha a *SIGNATUREVERIFICATION igazolás tárolót átvitte ugyan a rendszerre, de nem változtatta meg a tároló jelszavát a DCM segítségével. Ilyen esetben a tárolóban lévő igazolásokat nem tudja felhasználni az objektumokon lévő aláírások ellenőrzéséhez a visszaállítási folyamat alatt. A DCM segítségével változtassa meg az igazolás tároló jelszavát. Ha nem tudja a jelszót, akkor törölnie kell az igazolás tárolót, majd hozza létre újra, és a DCM segítségével változtassa meg a jelszót.
Amikor a terméket telepíti vagy visszaállítja, hibajelzést kap az aláírás ellenőrzésekor.	Amikor az objektum aláírás ellenőrzése sikertelen, a hiba jelezheti azt, hogy az objektum tartalma megváltozott az aláírása óta. Ha az objektum sértetlensége megkérdőjeleződik, ne változtassa meg a QVFYOBJRST rendszerváltozót, és ne hajtson végre egyéb műveletet sem, amely esetleg engedélyezné a kérdéses objektum visszaállítását. Ha így tenne, kijátszaná az aláírás ellenőrzés által nyújtott védelmet, és lehetővé tenné egy káros objektum bejutását a rendszerbe. Helyette, lépjen kapcsolatba az objektum aláírójával, és határozza meg a megfelelő lépéseket a probléma megoldása érdekében.

Az objektum aláíráshoz és az aláírás ellenőrzéshez kapcsolódó információk

Az objektum aláírás és az aláírás ellenőrzés viszonylag új biztonsági technológia. Az alábbi rövid felsorolás ízelítőt ad más forrásokból, ahol hasznos információkat talál, ha szélesebb áttekintés érdekli az új technológiáról és felhasználásáról:

- **VeriSign Help Desk webhely**
  A VeriSign webhely terjedelmes könyvtárral rendelkezik a digitális igazolások témaköréből, valamint az objektum aláírásról és egyéb Internet biztonsággal kapcsolatos tárgykörből.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Ez az IBM vörös könyv a V5R1 kiadás hálózati biztonsági továbbfejlesztéseire koncentrál. A piros könyv számos témakört tartalmaz, beleértve az iSeries objektum aláíró képességét, a Digitális igazolás kezelőt (DCM), a 4758 Cryptographic Coprocessor támogatást SSL kapcsolathoz, és így tovább.

Nyomtatva Dániában