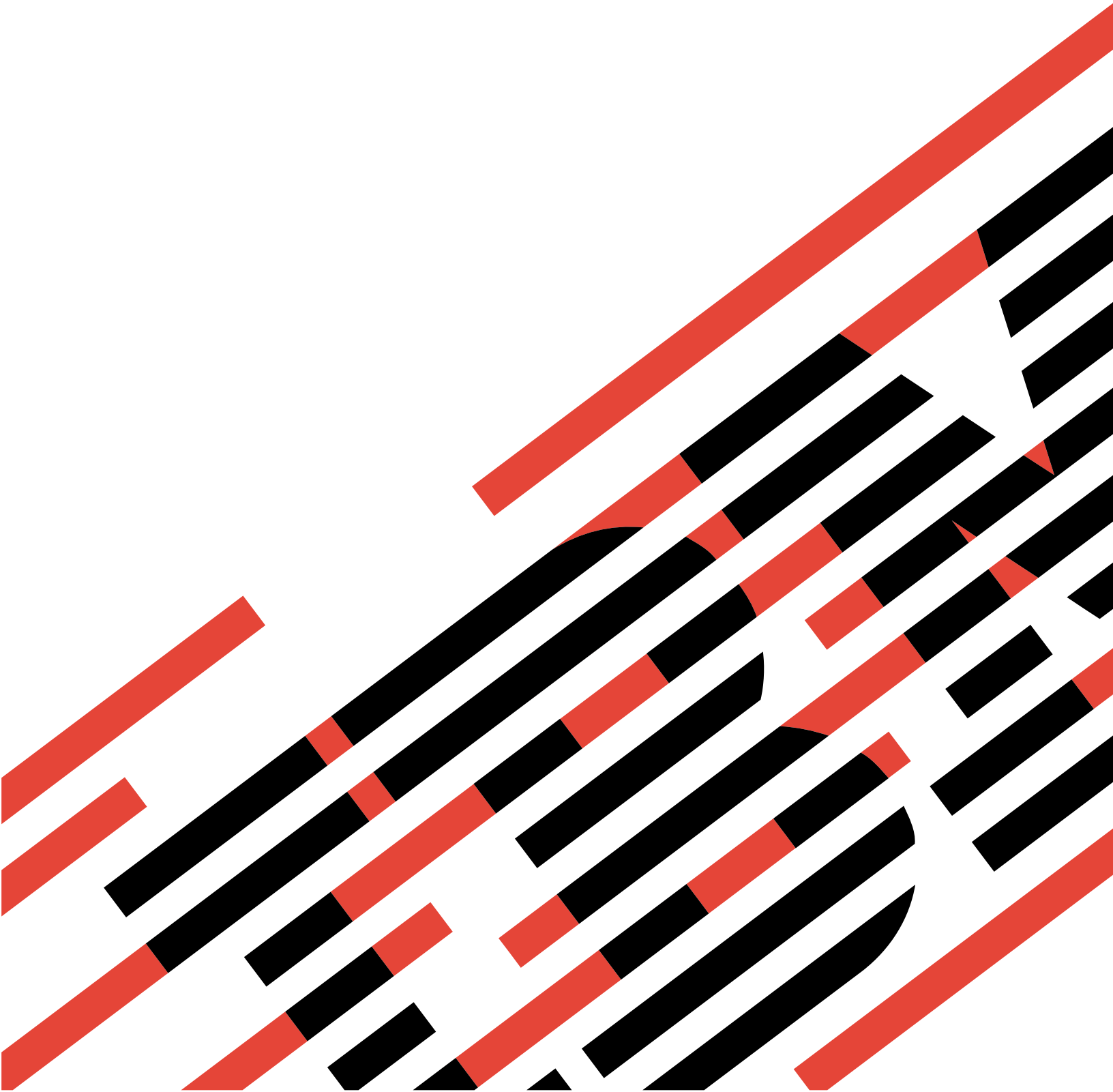
IBM

eserver

iSeries

Digitális igazolás kezelő



IBM

@server

iSeries

Digitális igazolás kezelő

Tartalom

Rész 1. Digitális igazolás kezelő

A digitális igazolás valójában egy elektronikus jogosítvány, amelyet az azonosság (identitás) ellenőrzésére használhat fel az elektronikus tranzakciókban. A hálózati biztonság fokozása érdekében növekvő számban használják a digitális igazolásokat. Például, a digitális igazolások nélkülözhetetlenek a Védett socket réteg (SSL) használatának konfigurálásához. Az SSL használata lehetővé teszi biztonságos kapcsolatok létesítését felhasználók és szerver alkalmazások között nem megbízható hálózaton keresztül (mint például Internet). Az SSL az egyik legjobb megoldást nyújtja az érzékeny adatok - mint például felhasználó nevek és jelszavak - bizalmas jellegének megőrzésére az Interneten. Sok iSeries szolgáltatás és alkalmazás, mint például FTP, Telnet, HTTP Server for iSeries és más egyebek rendelkeznek SSL támogatással az adatok védelme érdekében.

Az iSeries kiterjedt digitális igazolás támogatással rendelkezik, ami lehetővé teszi a digitális igazolások jogosítványként való felhasználását számos biztonsági alkalmazásban. Az igazolásokat felhasználhatja az SSL konfigurálásához, továbbá jogosítványként használhatja őket a kliens hitelesítéshez az SSL és a virtuális magánhálózati (VPN) tranzakciókban. A digitális igazolásokat és a hozzájuk tartozó biztonsági kulcsokat használhatja fel az objektumok aláírására is. Az objektumok aláírása lehetővé teszi a változtatások észlelését, vagy az objektumok tartalmának esetleges hamisítását az aláírások ellenőrzése révén, így biztosítva sértetlenségüket.

Az igazolások támogatását könnyedén kihasználhatja az iSeries rendszeren, amikor a Digital Certificate Manager (DCM) nevű ingyenes iSeries terméket használja, amellyel központilag kezelheti az igazolásokat az alkalmazások számára. A DCM lehetővé teszi az Igazolási hatóságtól (CA) beszerzett igazolások kezelését. A DCM segítségével létrehozhat és működtethet saját helyi CA-t, amely révén magán igazolásokat bocsáthat ki az alkalmazásoknak és a felhasználóknak saját szervezetén belül.

A tökéletes tervezésnek és a kiértékelésnek kulcsfontosságú szerepe van az igazolások biztonsági előnyeinek hatékony kihasználásában. Az alábbi témakörök tanulmányozásával megismerheti az igazolások működését, a DCM használatát az igazolások és az őket felhasználó alkalmazások kezeléséhez:

A V5R2 újdonságai
Ismerteti a Digitális igazolás kezelő újdonságait, valamint a témakörben bekövetkezett változtatásokat.

A témakör nyomtatása
Ismerteti a teljes témakör kinyomtatását PDF fájl segítségével.

Áttérés a DCM egy korábbi változatáról
Ismerteti azokat a végrehajtandó feladatokat és egyéb fontos szempontokat, amelyek akkor jelentkeznek, amikor a DCM meglévő verziójáról áttér a legújabbra.

DCM forgatókönyvek
Két forgatókönyvet ismertet, amelyek jól illusztrálják a tipikus igazolás megvalósítási sémákat, így segítve a saját iSeries biztonsági irányelvek végrehajtásának részeként az igazolás megvalósítás tervezését. Mindegyik forgatókönyv tartalmazza a konfigurálási feladatokat is, amelyeket el kell végezni ahhoz, hogy a forgatókönyvet a leírás szerint alkalmazza.

A digitális igazolás alapjai
Ismerteti és leírja az alapokat, hogy jobban érthető legyen, mi a digitális igazolás és hogyan működik. Tanulmányozhatja a különböző típusú igazolásokat, és a biztonsági irányelvek szerinti használatuk módját.

A DCM tervezése
Az itt leírtak segítségével eldöntheti, hogyan és mikor kell digitális igazolásokat használni, hogy ez összhangban legyen biztonsági céljaival. Tanulmányozhatja az előzetes követelményeket, amelyeket telepíteni kell, valamint a DCM használata előtt figyelembe veendő egyéb feltételeket.

A DCM konfigurálása
Az itt leírtak révén tanulmányozhatja az összes konfigurálási lehetőséget, ami révén a DCM alkalmassá válik az igazolások és azok kulcsainak kezelésére.

A DCM kezelése
Az itt leírtak révén tanulmányozhatja, hogyan lehet a DCM segítségével kezelni az igazolásokat és az őket használó alkalmazásokat. Megismerheti az objektumok digitális aláírásának módját, valamint a saját Igazolási hatóság létrehozását és működtetését.

A DCM hibakeresése
Az itt leírtak révén tanulmányozhatja néhány általános hiba feltárásának módját, amelyekkel a DCM használata során találkozhat.

A DCM-hez kapcsolódó információk
Itt hivatkozásokat talál más helyekre, ahol tovább tanulmányozhatja a digitális igazolásokat, a nyilvános kulcsokat, a Digitális igazolás kezelőt és az egyéb kapcsolódó témaköröket.

Fejezet 1. A V5R2 újdonságai

A V5R2 szintű Digitális igazolás kezelőben (DCM) és az iSeries digitális igazolással kapcsolatos funkcióiban az alábbi továbbfejlesztések történtek:

- **Igazolás hozzárendelési funkció**
  Ez az új DCM feladat lehetővé teszi, hogy gyorsabban és könnyebben hozzárendelje az igazolást egy vagy több alkalmazáshoz. A feladatot elérheti az **Igazolások kezelése** feladatlistából, vagy gyors útvonalon a **Szerver és igazolások kezelése** és az **Objektum aláíró igazolások kezelése** révén. Ez a funkció csak a *SYSTEM és az *OBJECTSIGNING igazolás tárolókra érvényes.
- **Parancs (*CMD) objektumok aláírása**
  Ezentúl a DCM segítségével létrehozhat digitális aláírásokat a parancs (*CMD) objektumokon is, amelyek révén ellenőrizheti sértetlenségüket. Továbbá, az igazolások hatókörére ezentúl a *CMD objektumokat is kiválaszthatja. Eldöntheti, hogy az egész *CMD objektumot írja alá, vagy csak a *CMD objektum magját alkotó összetevőket. Amikor a DCM felhasználásával nézi meg a *CMD objektumok aláírását, a DCM tájékoztatást ad az aláírás hatásköréről.
- **API-k a Helyi CA által aláírt felhasználói igazolások létrehozásához DCM nélkül**
  Mostantól két új API áll rendelkezésre, amelyek révén programozottan adhat ki Helyi igazolási hatóság (CA) által aláírt igazolásokat a nem iSeries felhasználóknak. Az API-k révén iSeries felhasználói profilok nélkül adhat ki igazolásokat a felhasználóknak. Továbbá, a felhasználók nem kell DCM-et használni, hogy egyedileg beszerezzék az igazolást a kliens hitelesítéshez.

A témakör újabb, illetve módosított elemei:

- Két új forgatókönyv, amelyek révén meghatározhatja, hogy biztonsági célkitűzéseit is figyelembe véve, hogyan alkalmazhatja legjobban az igazolásokat.
- Az újra szervezett információk könnyebbé és gyorsabbá teszik a DCM használatához szükséges részek megtalálását.

Az aktuális változat újdonságairól és a változásokról a következő dokumentáció ad felvilágosítást: Jegyzék a felhasználóknak  .

Fejezet 2. A témakör nyomtatása

A PDF verzió megjelenítéséhez vagy letöltéséhez válassza a Digitális igazolás kezelőt  (fájlméret kb. 468 KB vagy 110 oldal).

A PDF mentése a 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)  .

Fejezet 3. Áttérés a DCM korábbi változatáról

Amikor a Digitális igazolás kezelő (DCM) V4R3 változatáról tér át V5R2-re, a DCM automatikusan frissíti a meglévő helyi Igazolási hatóságot (CA) és a rendszer igazolás kulcscsomó fájljait. A DCM frissíti a default.kyr nevű fájlokat megfelelő igazolás tároló fájlokra, melyek neve default.kdb. A DCM áttelepíti a Hypertext Transfer Protocol (HTTP) és a Lightweight Directory Access Protocol (LDAP) szerverekhez tartozó kulcscsomó fájlokban lévő összes érvényes igazolást. A DCM a *SYSTEM igazolás tárolóba (default.kdb) telepíti át az érvényes igazolásokat.

Megjegyzés: Ha a DCM V4R4, V4R5 vagy V5R1 változatáról tér át, akkor semmilyen költöztetési feladatot sem kell elvégeznie, mivel az ezen verziókból eredő igazolás fájlok kompatíbilisek a V5R2 szinttel.

Kulcscsomó költöztetése igazolás tárolóba – V4R3 áttérés

A V5R2 DCM telepítése közben a rendszer a következő kulcscsomó fájlokat költözteti át:
- DCM alapértelmezett kulcscsomó fájlok.
- Kulcscsomók, amelyeket a HTTP Server konfigurációs fájlok használnak.
- Kulcscsomók, amelyeket az LDAP Server konfigurációs fájlok használnak.

Ha .kyr fájlt használ, amit a DCM nem frissített automatikusan, a DCM átalakítja kyr.kdb állománnyá, amikor első alkalommal dolgozik vele. Például először, amikor megadja a secure.kyr fájlt a DCM felhasználói kezelőfelületében, a DCM átalakítja a fájlt az új igazolás tárolóba kerülő secure.kyr.kdb állománnyá.

Megjegyzés: A kulcscsomók különböznek az igazolás tárolóktól, ezért át kell alakítani a kulcscsomó fájlokat (amit a DCM nem frissített automatikusan), amikor a DCM felhasználói kezelőfelületen dolgozik velük. Ha manuálisan megváltoztatja a fájl nevet .kdb kiterjesztésűre, hibajelzést kap, amikor ezt követően megpróbál dolgozni az ilyen fájlokkal a DCM felhasználói kezelőfelületében.

Ha megpróbálja törölni a secure.kyr fájlt a DCM segítségével, a DCM valójában archiválja azt és a secure.kyr.kdb fájlt törli.

Alapértelmezett igazolás tároló jelszó

Ha létezik a /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR fájl, a rendszer áttelepíti ezt a kulcscsomó fájlt és a többi, alkalmas kulcscsomó fájlt is a *SYSTEM igazolás tárolóba. A /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR fájlhoz tartozó eredeti jelszó lesz érvényes a *SYSTEM igazolás tárolóra is.

Ha a /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR fájl ugyan nem létezik, de egyéb más, áttelepítésre alkalmas kulcscsomó fájlok vannak (például a HTTP Server konfigurációs fájlok által használt kulcscsomó fájlok), a rendszer létrehozza a *SYSTEM igazolás tárolót DEFAULT jelszóval (csupa nagybetűvel) és befejezi az áttelepítést.

A fájl áttelepítési folyamat során előforduló hibákról és azok javításáról olvashat az Áttérési hibák és helyreállítási megoldások cím alatt.

Fejezet 4. DCM forgatókönyvek

Az iSeries által nyújtott Digitális igazolás kezelő és digitális igazolás támogatás lehetővé teszi, hogy az igazolások használatával a legkülönbözőbb módon javítsa biztonsági intézkedéseit. Az igazolások használatának különféle módja üzleti céljaitól és biztonsági igényeitől függ.

A digitális igazolások révén többféleképpen is javíthatja biztonságát. A digitális igazolások lehetővé teszik a Védett socket réteg (SSL) használatát, amellyel biztonságosan elérheti a webhelyeket és más Internet szolgáltatásokat. A digitális igazolásokat felhasználhatja a virtuális magánhálózat (VPN) típusú kapcsolatok konfigurálásához. Az igazolások kulcsaival digitálisan aláírhatja az objektumokat, vagy ellenőrizheti a digitális aláírásokat, hogy megbizonyosodjon az objektumok hitelességéről. Az ilyen digitális aláírások biztosítják az objektum eredetének megbízhatóságát, és védik sértetlenségét.

A digitális igazolásokkal tovább növelheti a rendszer biztonságát (a felhasználó nevek és a jelszavak helyett), amivel hitelesítheti és felhatalmazhatja a szerver és a felhasználók közötti szekciókat. A DCM segítségével társíthatja a felhasználó igazolását az adott felhasználó iSeries felhasználói profiljával. Az igazolás azután ugyanazzal a jogosultságokkal és engedélyekkel fog rendelkezni, mint a hozzátartozó profil.

Következésképpen, igen bonyolult lehet és számos tényezőtől függ az, hogyan használja az igazolásokat. Az itt bemutatott forgatókönyvek a digitális igazolások néhány legáltalánosabb biztonsági jellemzőit írják le jellegzetes üzleti környezetben. Minden egyes forgatókönyv leírja az összes szükséges rendszer és szoftver előfeltételt, valamint az összes konfigurációs feladatot, amelyet végre kell hajtani a forgatókönyv megvalósításához. Nézze át az alábbi forgatókönyveket, melyek segítségével meghatározhatja, hogy igényeinek megfelelően hogyan növelheti a biztonságot az igazolások révén:

Forgatókönyv: Nyilvános alkalmazások és erőforrások elérésének védelme igazolások segítségével
Ez a forgatókönyv ismerteti, mikor és hogyan használja az igazolásokat, hogy megvédje és korlátozza a nyilvános vagy extranet erőforrások elérését a nyilvános felhasználók részéről.

Forgatókönyv: Belső alkalmazások és erőforrások elérésének védelme igazolások segítségével
Ez a forgatókönyv ismerteti, mikor és hogyan használja az igazolásokat védelem és korlátozás céljából, és ez alapján mely erőforrásokat és alkalmazásokat érhetik el a belső felhasználók a belső szervereken.

Forgatókönyv: Nyilvános alkalmazások és erőforrások elérésének védelme igazolások segítségével

Helyzet

Egy biztosító társaságnál (MyCo., Inc) dolgozik, és a vállalati intraneten és extraneten található, különböző alkalmazások karbantartásáért felelős. Egy bizonyos alkalmazás, amelyért ugyancsak felelős, díjszabás számító alkalmazás, amely lehetővé teszi több száz független ügynöknek, hogy ajánlatokat készítsenek ügyfeleik számára. Mivel az alkalmazás által nyújtott adatok némiképp érzékenyek, bizonyos akar abban lenni, hogy csak a regisztrált ügynökök használhatják. Ráadásul még biztonságosabb elérési módot akar nyújtani az alkalmazás felhasználóinak, mint amit a jelenlegi felhasználónév és jelszó használata biztosít.

Érinti az is, hogy a jogosulatlan felhasználók elfoghatják az információt, amikor az áthalad egy megbízhatatlan hálózaton keresztül. A különböző ügynökök egymás között is megoszthatják az információkat anélkül, hogy erre jogosultak lennének.

Megfelelő vizsgálódások után úgy dönt, hogy a digitális igazolások nyújthatnak olyan védelmet, amilyenre szüksége van. Az igazolások lehetővé teszik a Védett socket réteg (SSL) használatát, ami védi a díjszabási adatok átvitelét. Ugyan azt akarja, hogy az összes ügynök igazolást használjon az alkalmazás eléréséhez, azt is tudja, hogy saját társaságánál és az ügynököknél is idő kell a kitűzött cél eléréséhez. Ezért ebben a pillanatban folytatni kívánja a jelenlegi felhasználónév és jelszó hitelesítési módszert, mivel az SSL megvédi az érzékeny adatok magán jellegét az átvitel alatt.

Az alkalmazás és felhasználóinak típusa, valamint a felhasználói hitelesítésre vonatkozó jövőbeli céljai alapján úgy dönt, hogy egy jólismert Igazolási hatóságtól (CA) kapott nyilvános igazolással konfigurálja az SSL kapcsolatot az alkalmazás számára.

A forgatókönyv előnyei

Ez a forgatókönyv a következő előnyökkel jár:
- Azzal, hogy a díjszabás számító alkalmazás eléréséhez digitális igazolást használó SSL kapcsolatot vesz igénybe, a szerver és a kliens között átvitt információk védettek és magán jellegűek lesznek.
- Azzal, hogy amikor csak lehet digitális igazolásokat használ a kliens hitelesítéshez, egy biztonságosabb módszert nyújt a jogosult felhasználók azonosításához. Még ahol erre nincs is lehetőség, a kliens hitelesítéshez használt felhasználónevet és jelszót megvédi és magán jellegét megőrzi az SSL szekció, ami biztonságosabbá teszi az ilyen érzékeny adatok cseréjét.
- Az alábbi vagy hasonló feltételek esetén praktikus választás, ha *nyilvános* digitális igazolásokat használ az alkalmazások és az adatok eléréséhez vagy korlátozásához:
  - Az adatok és az alkalmazások biztonsági igényei különböző fokúak.
  - Nagyon gyakori a forgalom a megbízható felhasználók között.
  - Nyilvános hozzáférést ad az alkalmazásokhoz és az adatokhoz, mint például Internet webhely vagy extranet alkalmazás.
  - Nem kíván működtetni saját Igazolási hatóságot (CA) a felhasználók nagy száma miatt, akik elérik az alkalmazásokat és az erőforrásokat, vagy egyéb adminisztrációs okok miatt.
- Azzal, hogy a díjszabás számító alkalmazást nyilvános igazolást használó SSL kapcsolattal konfigurálja, csökkenti a felhasználók által elvégzendő konfigurálási lépések számát, ami az alkalmazás eléréséhez szükséges. A legtöbb kliens szoftver tartalmazza a legismertebb CA-k igazolásait.

Célok

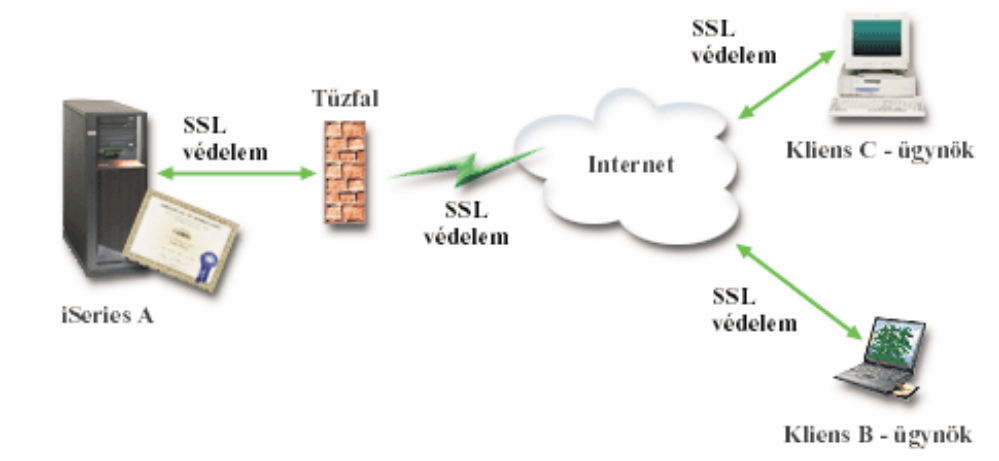
Ebben a forgatókönyvben a MyCo., Inc. digitális igazolások segítségével akarja megvédeni a díjszabás számító információit, amelyeket az alkalmazás nyújt a felhatalmazott nyilvános felhasználóknak. A társaság biztonságosabb módszert kíván alkalmazni az alkalmazás elérésére felhatalmazott felhasználók hitelesítésére is.

A forgatókönyv céljai a következők:
- A társaság nyilvános díjszabás számító alkalmazásának SSL kapcsolatot kell használni, hogy megvédje a felhasználóknak nyújtott adatok magán jellegét.
- Az SSL konfigurálását jólismert nyilvános Internet Igazolási hatóságtól (CA) beszerzett igazolásokkal kell végrehajtani.
- A jogosult felhasználóknak érvényes felhasználónevet és jelszót kell megadni ahhoz, hogy elérjék az alkalmazást SSL módban. Történetesen, a jogosult felhasználóknak

alkalmazniuk kell az alkalmazás elérését jelentő biztonsági hitelesítés két módszerének egyikét. Az ügynököknek a jólismert Igazolási hatóságtól (CA) kapott nyilvános digitális igazolást kell bemutatni, vagy egy érvényes felhasználónevet és jelszót.

Részletek

A következő ábra szemlélteti az adott forgatókönyvre vonatkozó hálózati konfigurációt:



Az ábra a következőket illusztrálja a forgatókönyvre vonatkozó helyzetről:

A társaság nyilvános szervere – iSeries A

- Az iSeries A az a szerver, amely otthont ad a társaság díjszabás számító alkalmazásának.
- Az iSeries A szerveren OS/400 Verzió 5 Változat 2 (V5R2) operációs rendszer fut.
- Az iSeries A szerveren telepítve van a titkosítás hozzáférési szolgáltató (5722–AC3).
- Az iSeries A szerveren telepítve és konfigurálva van a Digitális igazolás kezelő (OS/400 34-es opció) és az IBM HTTP Server for iSeries (5722–DG1).
- Az iSeries A szerveren fut a díjszabás számító alkalmazás, amely úgy van konfigurálva, hogy:
  - SSL módot igényel.
  - Jólismert Igazolási hatóságtól (CA) kapott nyilvános igazolásokat használ az SSL konfigurációhoz.
  - Felhasználó hitelesítést igényel felhasználónév és jelszó révén.
- Az iSeries A bemutatja igazolását, amellyel kezdeményezi az SSL szekciót, amikor a B és C kliensek elérik az alkalmazást.
- Az SSL szekció inicializálása után az iSeries A bekéri a B és C kliensektől az érvényes felhasználónevet és jelszót, mielőtt hozzáférést adna a díjszabás számító alkalmazáshoz.

Ügynök kliens rendszerei – Kliens B és C

- A kliens B és C független ügynökök, akiknek hozzáférésük van a díjszabás számító alkalmazáshoz.
- A kliens B és C rendelkezik a jólismert CA igazolásának egy példányával, amely kiadta a kliens szoftverekben telepített alkalmazás igazolást.
- B és C kliensnek hozzáférése van az iSeries A szerveren lévő díjszabás számító alkalmazáshoz. A szerver bemutatja igazolását a kliens szoftvereknek, hogy ellenőrizzék azonosságát, és kezdeményezzék az SSL szekciót.
- B és C klienseken található kliens szoftverek úgy vannak konfigurálva, hogy elfogadják az iSeries A igazolását, és SSL szekciót nyissanak.
- Az SSL szekció kezdete után B és C kliensnek érvényes felhasználónevet és jelszót kell benyújtania, mielőtt az iSeries A hozzáférést adna az alkalmazáshoz.

Előfeltételek és feltételezések

A forgatókönyv a következő előfeltételektől és feltételezésektől függ:

1. A díjszabás számító alkalmazás az iSeries A szerveren egy általános program, amely beállítható az SSL használatára. Az alkalmazások többsége, beleértve számos iSeries alkalmazást is, támogatja az SSL módot. Az SSL konfigurálási lépések eléggé változatosak az alkalmazásoktól függően. Következésképpen, a forgatókönyv nem szolgál különleges utasításokkal ahhoz, hogyan kell a díjszabás számító alkalmazást SSL használatra konfigurálni. A forgatókönyv az igazolások konfigurálására és kezelésére vonatkozóan tartalmaz utasításokat, amelyekre minden alkalmazásnak szüksége van az SSL használatához.
2. *Választhatóan*, a díjszabás számító alkalmazás lehetőséget ad igazolások kérésére kliens hitelesítés céljából. A forgatókönyv utasításokat tartalmaz arról, hogyan konfigurálhatja az igazolást megbízhatónak a Digitális igazolás kezelő (DCM) segítségével az ilyen támogatást nyújtó alkalmazások számára. Mivel a kliens hitelesítés konfigurálási lépései igen változatosak az alkalmazásoktól függően, ezért a forgatókönyv nem tartalmaz speciális utasításokat a díjszabás számító alkalmazás kliens hitelesítésének konfigurálásához.
3. Az iSeries A kielégíti a Digitális igazolás kezelő (DCM) telepítésének és használatának követelményeit.
4. Senki sem konfigurálta vagy használta korábban az iSeries A szerveren lévő DCM-et.
5. Akárki is hajtja végre a forgatókönyvben leírt feladatokat a DCM segítségével, *SECADM és *ALLOBJ különleges jogosultsággal kell rendelkeznie felhasználói profiljának.
6. Az iSeries A szerveren nincs telepítve az IBM 4758-023 PCI Cryptographic Coprocessor.

Feladat lépések

A forgatókönyv megvalósítása érdekében az alábbi feladatokat kell az iSeries A szerveren végrehajtani:

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 szerver igazolás kérést.
3. Konfigurálja az alkalmazást a Védett socket réteg (SSL) használatához.
4. A DCM segítségével importálja és rendelje hozzá az aláírt szerver vagy kliens igazolást az alkalmazásra vonatkozó alkalmazás ID-hez.
5. Indítsa el az alkalmazást SSL módban, ha szükséges.
6. *Választható feladat*: A DCM segítségével adja meg a megbízható CA-k listáját, hogy engedélyezni tudja az igazolásokon alapuló kliens hitelesítést az ilyen támogatást nyújtó alkalmazásoknak.

   Megjegyzés: A helyzet az, hogy a forgatókönyv szerint a díjszabás számító alkalmazás nem igényel igazolást kliens hitelesítéshez. Sok alkalmazás nyújt igazoláson alapuló kliens hitelesítési támogatást - a támogatás konfigurálása széles skálán változik az alkalmazásoktól függően. Ez a választható feladat segítséget nyújt annak megértéséhez, hogyan lehet a DCM révén engedélyezni a megbízható igazolásokat a kliens hitelesítéshez, ami az alkalmazások kliens hitelesítési támogatásának konfigurálásához nyújt alapot.

Konfigurálási részletek

A következő feladat lépéseinek végrehajtásával - az igazolásokat felhasználva - konfigurálhatja az alkalmazások és az erőforrások védett, nyilvános elérését.

1. lépés: Az előfeltételt jelentő feladatok végrehajtásával telepíti az összes szükséges iSeries terméket

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: Szerver vagy kliens igazolás kérés létrehozása

Először be kell szerezni a digitális igazolást egy nyilvános Igazolási hatóságtól (CA), hogy azután a Védett socket réteg (SSL) felhasználásával megvédje az alkalmazás adatkommunikációját, ahogy a forgatókönyv ismerteti. A nyilvános CA által az igazolás kiadásához kért adatokat létrehozhatja a Digitális igazolás kezelő (DCM) segítségével.

Hajtsa végre az alábbi lépéseket az igazolás beszerzési folyamatának elkezdéséhez:

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 az alkalmazások használhatnak SSL szekciókhoz) 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 a ***SYSTEM** beállítást, és kattintson a **Folytatásra**.
4. Válassza ki az **Igen** választ arra, hogy a *SYSTEM 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.

Miután a CA visszaadja az aláírt, komplett igazolást, konfigurálja az alkalmazást az SSL használatához, importálja az igazolást a *SYSTEM igazolás tárolóba, és rendelje hozzá az alkalmazáshoz az SSL mód használata érdekében.

3. lépés: Az alkalmazás konfigurálása SSL használatához

Amikor visszakapja az aláírt igazolást a nyilvános Igazolási hatóságtól (CA), folytathatja a folyamatot a Védett socket réteg (SSL) módú kommunikációk engedélyezésével, a nyilvános alkalmazások számára. Az aláírt igazolás kezelése előtt konfigurálja az alkalmazást az SSL használatára. Néhány alkalmazás, mint például a HTTP Server for iSeries, egyedi alkalmazás azonosítót (ID) generál, majd a Digitális igazolás kezelővel (DCM) regisztrálja azt, amikor az alkalmazást SSL használatához konfigurálja. Az alkalmazás azonosítót (ID) ismerni kell, mielőtt a DCM segítségével az azonosítóhoz rendelhetné az aláírt igazolást, és befejezhetné az SSL konfigurálási folyamatot.

Az alkalmazástól függően különféleképpen konfigurálhatja az alkalmazást az SSL használatához. A forgatókönyv nem tételez fel különleges forrást a díjszabás számító alkalmazás leírása számára, mivel több lehetőség is kínálkozik arra, hogy a MyCo., Inc. eljuttassa az alkalmazást az ügynökeinek.

Kövesse az alkalmazás dokumentációjában leírt utasításokat, amikor az alkalmazást SSL használatára konfigurálja. Nézze át az Információs központ SSL segítségével védett alkalmazások című témakörét, ha kíváncsi arra, hogyan konfigurálhat sok általános IBM alkalmazást SSL használathoz.

4. lépés: Az aláírt nyilvános igazolás importálása és hozzárendelése

Miután konfigurálta az alkalmazást az SSL használatához, a Digitális igazolás kezelő (DCM) segítségével importálja az aláírt igazolást, és rendelje hozzá az alkalmazáshoz.

Kövesse az alábbi lépéseket, amikor importálja az igazolást, és hozzárendeli az alkalmazáshoz az SSL konfigurálás folyamatának végrehajtása céljából:

1. Indítsa el a DCM funkciót.
2. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SYSTEM** elemre, az igazolás tároló megnyitása céljából.
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 a *SYSTEM igazolás tárolóba.

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

A feladatok befejezésével elindíthatja az alkalmazást SSL módban, és elkezdheti az alkalmazás által nyújtott adatok védelmét.

5. lépés: Az alkalmazás elindítása SSL módban

Miután befejezte a folyamatot, amely révén importálta az igazolást és hozzárendelte az alkalmazáshoz, valószínűleg le kell állítani és újra kell indítani az alkalmazást SSL módban. Néhány esetben erre szükség van, mivel az alkalmazás futás közben nem feltétlenül tudja

meghatározni, hogy létezik-e igazolás hozzárendelés. Az alkalmazás dokumentációját átnézve meghatározhatja, hogy újra kell-e indítani az alkalmazást. Egyéb információkat is találhat az alkalmazás SSL módban történő indításáról.

6. lépés (választható): Megbízható CA lista megadása az alkalmazáshoz, amely igazolásokat igényel kliens hitelesítéshez

Az olyan alkalmazások esetén, amelyek támogatják az igazolások felhasználását kliens hitelesítéshez Védett socket réteg (SSL) szekció alatt, meg kell határozni, hogy elfogadja-e az igazolást az azonosság érvényes ellenőrzésének eszközéül. Az igazolás hitelesítésének egyik kritériuma, amelyet az alkalmazás használ, hogy az alkalmazás megbízik-e az Igazolási hatóságban (CA), amely kiadta az igazolást.

A helyzet az, hogy a forgatókönyv szerint a díjszabás számító alkalmazás nem igényel igazolást kliens hitelesítéshez. Sok alkalmazás nyújt igazoláson alapuló kliens hitelesítési támogatást - a támogatás konfigurálása széles skálán változik az alkalmazásoktól függően. Ez a választható feladat segítséget nyújt annak megértéséhez, hogyan lehet a DCM révén engedélyezni a megbízható igazolásokat a kliens hitelesítéshez, ami az alkalmazások kliens hitelesítési támogatásának konfigurálásához nyújt alapot.

Mielőtt meghatározhatná az alkalmazásra vonatkozó megbízható CA listát, bizonyos feltételeknek meg kell felelni:

- Az alkalmazásnak támogatni kell az igazolások használatát kliens hitelesítéshez.
- A DCM alkalmazás definíciójában meg kell adni, hogy használja-e az alkalmazás a megbízható CA listát.

Ha az alkalmazás definíciója azt jelzi, hogy az alkalmazás használja a megbízható CA listát, akkor először meg kell adni a listát, mielőtt az alkalmazás sikeresen végrehajthatna kliens hitelesítést. Ez biztosítja azt, hogy az alkalmazás csak azokat az igazolásokat fogja érvényesíteni, amelyeket a megadott listán szereplő CA adott ki. Ha a felhasználó vagy a kliens alkalmazás olyan CA-tól kapott igazolást mutat be, amelyik nincs megadva a megbízható CA-k listáján, az alkalmazás nem fogja azt elfogadni érvényes hitelesítés alapjául.

Hajtsa végre az alábbi lépéseket, ha a DCM segítségével megbízható CA listát ad meg egy alkalmazáshoz:

1. Indítsa el a DCM funkciót.
2. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SYSTEM** elemre, az igazolás tároló megnyitása céljából.
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 feladatlistán válassza a **CA állapot beállítása** feladatot a CA igazolások listájának megjelenítéséhez.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
6. Válassza ki az alkalmazás által megbízhatónak ítélendő CA igazolást a listából, és kattintson az **Engedélyezésre**, hogy megjelenítse a megbízható CA listát használó alkalmazásokat.
7. Válassza ki az alkalmazást a listából, amelyre vonatkozóan a kiválasztott CA-t hozzá kell adni a megbízható CA listához, és kattintson az **OK** gombra. A lap tetején egy üzenet tájékoztatja, hogy a kiválasztott alkalmazások megbízhatónak tartják a CA-t, és az általa kiadott igazolásokat.

Most konfigurálhatja az alkalmazást, hogy igazolásokat kérjen a kliens hitelesítéshez. Kövesse az alkalmazás dokumentációjában lévő utasításokat.

Forgatókönyv: Belső alkalmazások és erőforrások elérésének védelme igazolások segítségével

Helyzet

Ön a társaság (MyCo., Inc.) hálózati rendszergazdája. A társaság emberi erőforrás osztálya foglalkozik olyan kérdésekkel, mint jogi esetek és a feljegyzések magán jellege. A társaság alkalmazottai kérték, hogy online módon elérhessék a saját személyes juttatásaikról és egészségi állapotukról szóló információkat. A cég úgy reagált a kérésre, hogy létrehozott egy belső webhelyet, ahol az alkalmazottak elérik az információkat. Ön a felelős a belső webhely adminisztrálásáért.

Mivel az alkalmazottak földrajzilag elkülönülő két helyszínen tartózkodnak, és néhány alkalmazott gyakran utazik is, arra kell figyelnie, hogy az információ magán jellegű maradjon, miközben áthalad az Interneten keresztül. A társaság adatainak elérését hagyományosan felhasználónév és jelszó használatával korlátozza. Az adatok érzékeny és privát természete miatt felismeri, hogy a jelszón alapuló hozzáférés korlátozás nem feltétlenül elegendő. És mindezen túl, az emberek megoszthatják, elfelejthetik, sőt el is lophatják a jelszavakat.

Megfelelő vizsgálódások után úgy dönt, hogy a digitális igazolások nyújthatnak olyan védelmet, amilyenre szüksége van. Az igazolások lehetővé teszik a Védett socket réteg (SSL) használatát, ami védi az adatok átvitelét. Továbbá, ha igazolásokat használ jelszavak helyett, biztonságosabbá teheti a felhasználók hitelesítését, és az általuk elért emberi erőforrás információk korlátozását.

Ennek következtében úgy dönt, hogy saját Helyi igazolási hatóságot (CA) állít fel, minden alkalmazottnak igazolást ad ki, és az igazolásaikat társítja iSeries felhasználói profiljaikkal. Az ilyen típusú saját igazolás lehetővé teszi, hogy szigorúbban ellenőrizze az érzékeny adatok elérését, valamint az adatok magánjellegének vezérlését az SSL segítségével. Végtére is, az igazolások saját kézzel történő kiadásával növeli annak valószínűségét, hogy az adatok biztonságosak maradnak, és csak meghatározott egyedek érhetik el.

A forgatókönyv előnyei

Ez a forgatókönyv a következő előnyökkel jár:

- Azzal, hogy az emberi erőforrás webszerver eléréséhez digitális igazolást használó SSL kapcsolatot vesz igénybe, a szerver és a kliens között átvitt információk védettek és magán jellegűek lesznek.
- Azzal, hogy digitális igazolásokat használ a kliens hitelesítéshez, biztonságosabb módszert nyújt a jogosult felhasználók azonosításához.
- Az alábbi vagy hasonló feltételek esetén praktikus választás, ha *magán* digitális igazolásokat használ az alkalmazások és az adatok eléréséhez vagy korlátozásához:
  - Nagyfokú biztonságot igényel, kifejezetten a felhasználók hitelesítésével kapcsolatban.
  - Bizalmat érez a személyek iránt, akiknek kiadja az igazolásokat.
  - A felhasználók már rendelkeznek iSeries felhasználói profillal, amellyel vezérli az alkalmazásokhoz és az adatokhoz való hozzáférésüket.
  - Saját Igazolási hatóságot (CA) kíván működtetni.
- Ha magán igazolásokat használ kliens hitelesítéshez, könnyebben társíthatja össze az igazolást a jogosult felhasználó iSeries felhasználói profiljával. Az igazolás és a felhasználói profil ilyen társítása révén a HTTP Server meghatározhatja az igazolás tulajdonosának felhasználói profilját a hitelesítés során. A HTTP Server azután átválthat

erre a profilra, és alatta fut, vagy végrehajt olyan műveleteket az adott felhasználóra, amelyek a felhasználói profilban lévő információkon alapulnak.

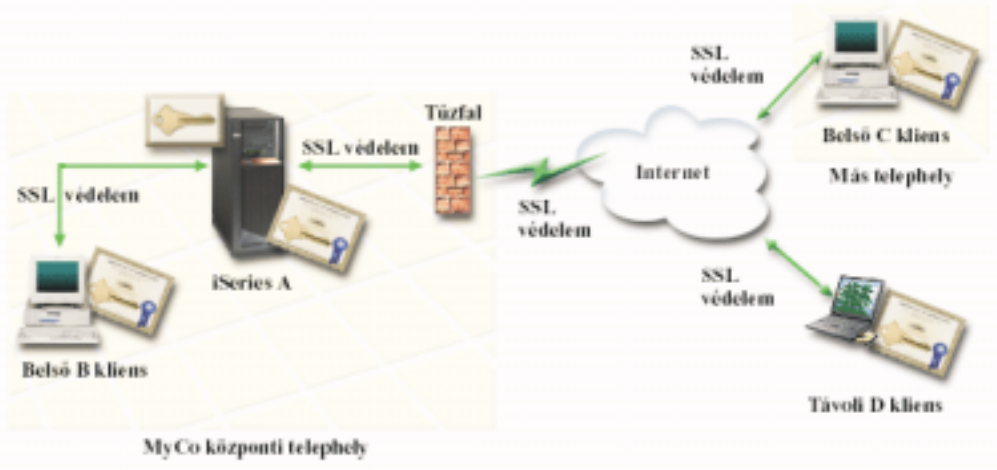
Célok

Ebben a forgatókönyvben a MyCo., Inc. digitális igazolások segítségével akarja megvédeni az érzékeny személyi adatokat, amelyeket az emberi erőforrás osztály belső webhelye nyújt a társaság alkalmazottainak. A társaság biztonságosabb módszert kíván alkalmazni a webhely elérésére felhatalmazott felhasználók hitelesítésére is.

A forgatókönyv céljai a következők:
- A társaság emberi erőforrás osztályának belső webhelye számára SSL kapcsolatot kell használni, hogy megvédje a felhasználóknak nyújtott adatok magán jellegét.
- Az SSL konfigurálását belső Helyi igazolási hatóságtól (CA) beszerzett magán igazolásokkal kell végrehajtani.
- A jogosult felhasználóknak érvényes igazolást kell megadni ahhoz, hogy elérjék az emberi erőforrások webhelyét SSL módban.

Részletek

A következő ábra szemlélteti az adott forgatókönyvre vonatkozó hálózati konfigurációt:



Az ábra a következőket illusztrálja a forgatókönyvre vonatkozó helyzetről:

A társaság emberi erőforrás webszervere – iSeries A
- Az iSeries A az a szerver, amely otthont ad a társaság webalapú emberi erőforrás alkalmazásának.
- Az iSeries A szerveren OS/400 Verzió 5 Változat 2 (V5R2) operációs rendszer fut.
- Az iSeries A szerveren telepítve van a titkosítás hozzáférési szolgáltató (5722–AC3).
- Az iSeries A szerveren telepítve és konfigurálva van a Digitális igazolás kezelő (OS/400 34-es opció) és az IBM HTTP Server for iSeries (5722–DG1).
- Az iSeries A szerveren fut az emberi erőforrás alkalmazás, amely úgy van konfigurálva, hogy:
  - SSL módot igényel.
  - Helyi igazolási hatóságtól (CA) kapott magán igazolást használ az SSL konfigurációhoz.
  - Igazolásokat igényel a kliens hitelesítéshez.
- Az iSeries A bemutatja igazolását, amellyel kezdeményezi az SSL szekciót, amikor a B, C és D kliensek elérik az alkalmazást.

- Az SSL szekció inicializálása után az iSeries A bekéri a B, C és D kliensektől az érvényes igazolást, mielőtt hozzáférést adna az emberi erőforrás alkalmazáshoz. Az igazolások ilyen fajta cseréje átlátható a B, C és D kliens felhasználók számára.

Alkalmazotti kliens rendszerek – B, C és D kliens

- A kliens B olyan alkalmazott, aki a MyCo's központi telephelyén dolgozik, ahol az iSeries A is található.
- A kliens C olyan alkalmazott, aki a MyCo's másik telephelyén dolgozik, ami földrajzilag elkülönül a központi telephelytől.
- A kliens D olyan alkalmazott, aki távoli módon dolgozik, gyakran utazik hivatalos üzleti útra, és biztonságos hozzáférésre van szüksége az emberi erőforrások webhelyhez, fizikai tartózkodási helyétől függetlenül.
- A kliens B, C és D a társaság alkalmazottai, akiknek hozzáférésük van az emberi erőforrás alkalmazáshoz.
- A kliens B, C és D mindegyike rendelkezik a Helyi CA igazolás egy példányával, amely kiadta a kliens szoftverekben telepített alkalmazás igazolást.
- A kliens B, C és D hozzáféréssel rendelkezik az iSeries A szerveren lévő emberi erőforrás alkalmazáshoz. A szerver bemutatja igazolását a kliens szoftvereknek, hogy ellenőrizzék azonosságát, és kezdeményezzék az SSL szekciót.
- A kliens B, C és D kliens szoftverei úgy vannak konfigurálva, hogy elfogadják az iSeries A igazolását, és SSL szekciót nyissanak.
- Az SSL szekció kezdete után B, C és D kliensnek érvényes igazolást kell benyújtania, mielőtt az iSeries A hozzáférést adna az alkalmazáshoz és annak erőforrásaihoz.

Előfeltételek és feltételezések

A forgatókönyv a következő előfeltételektől és feltételezésektől függ:

1. Az IBM HTTP Server for iSeries futtatja az emberi erőforrás alkalmazást az iSeries A szerveren. Két fajta HTTP Server for iSeries (eredeti és Apache alapú) van, és egy jelentősen megújult HTTP Server verzió lát napvilágot az itt leírtak kiadása után. Következésképpen, a forgatókönyv nem szolgál *különleges* utasításokkal ahhoz, hogyan kell a HTTP Server terméket SSL használatra konfigurálni. A forgatókönyv az igazolások konfigurálására és kezelésére vonatkozóan tartalmaz utasításokat, amelyekre minden alkalmazásnak szüksége van az SSL használatához.
2. A HTTP Server lehetőséget ad igazolások kérésére kliens hitelesítés céljából. A forgatókönyv utasításokat tartalmaz arról, hogyan konfigurálhatja az igazolás kezelői szükségleteket a Digitális igazolás kezelő (DCM) segítségével. Azonban, a forgatókönyv nem tartalmaz *speciális* konfigurációs utasításokat a HTTP Server kliens hitelesítésének konfigurálásához.
3. Az emberi erőforrások HTTP Server az iSeries A szerveren jelszavas védelmet használ.
4. Az iSeries A kielégíti a Digitális igazolás kezelő (DCM) telepítésének és használatának követelményeit.
5. Senki sem konfigurálta vagy használta korábban az iSeries A szerveren lévő DCM-et.
6. Akárki is hajtja végre a forgatókönyvben leírt feladatokat a DCM segítségével, *SECADM és *ALLOBJ különleges jogosultsággal kell rendelkeznie felhasználói profiljának.
7. Az iSeries A szerveren nincs telepítve az IBM 4758-023 PCI Cryptographic Coprocessor.

Feladat lépések

A forgatókönyv megvalósításához két feladatsort kell végrehajtani: Az egyik feladatsor lehetővé teszi az emberi erőforrás alkalmazás beállítását SSL használatra az iSeries A szerveren, és igazolások kérését felhasználói hitelesítés céljából. A másik feladatsor lehetővé teszi, hogy a kliens B, C és D részt vegyen az SSL szekcióban az emberi erőforrás alkalmazással, és beszerezze az igazolásokat a felhasználói hitelesítéshez.

Az emberi erőforrás webszerver alkalmazás feladatsorai

A forgatókönyv megvalósítása érdekében az alábbi feladatokat kell az iSeries A szerveren végrehajtani:

1. Hajtsa végre az előfeltételként megadott lépéseket, amelyek révén telepíti és konfigurálja az összes iSeries terméket.
2. Konfigurálja az emberi erőforrások HTTP szerverét SSL használatra, és jegyezze fel az alkalmazás ID-t a szerver példány számára.
3. A Digitális igazolás kezelő (DCM) segítségével létrehozhatja és működtetheti a saját Helyi CA hatóságot, amellyel igazolást adhat ki az emberi erőforrás HTTP Server számára. A feladatsor végrehajtása révén hozzárendeli az igazolást a webszerver alkalmazáshoz, és hozzáadja a CA-t az alkalmazás által megbízhatónak talált CA-k listájához.
4. Konfigurálja az emberi erőforrások webszervert, hogy igazolásokat kérjen a kliens hitelesítéshez.
5. Indítsa el az emberi erőforrások HTTP Server példányt SSL módban.

A kliens konfigurálás feladatsorai

A forgatókönyv megvalósítása érdekében az iSeries A szerveren lévő emberi erőforrás webszervert elérő összes felhasználónak (kliens B, C és D) végre kell hajtani az alábbi lépéseket:

6. Telepítse a Helyi CA igazolás egy példányát böngésző programjaikba.
7. Kérjen igazolást a Helyi CA-tól.

Konfigurálási részletek

A következő feladat lépéseinek végrehajtásával - az igazolásokat felhasználva - konfigurálhatja a belső alkalmazások és az erőforrások védett elérését.

1. lépés: Az előfeltételt jelentő feladatok végrehajtásával telepíti az összes szükséges iSeries terméket

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: Az emberi erőforrások HTTP Server konfigurálása SSL használatához

Az iSeries A szerveren futó emberi erőforrások HTTP Server termékhez beállított Védett socket réteg (SSL) konfigurációs lépései erőteljesen függnek attól, hogy eredeti vagy Apache verziójú szervert használ-e.

Olvassa el a Biztonságos szerver konfigurálása a HTTP Server számára című részt, ha kíváncsi a HTTP Server (eredeti) SSL használatra történő konfigurálásáról.

Olvassa el a Forgatókönyv: A JKL engedélyezi a Védett socket réteg (SSL) védelmet a HTTP szervereken (Apache meghajtású). A forgatókönyv tartalmazza az összes olyan feladatsort, amellyel létrehozza a virtuális gazdagépet, és konfigurálja azt az SSL használatára. Az SSL konfigurálásához tartozó lépéseket megtalálja az ″SSL engedélyezése virtuális gazdagép számára″ fejléc alatt.

A HTTP Server for iSeries (eredeti vagy Apache alapú) jelenlegi és jövőbeli változatainak konfigurálásáról a Web kiszolgálás című témakörben olvashat.

3. lépés: Helyi CA létrehozása és működtetése

Miután konfigurálja az emberi erőforrás HTTP szervert a Védett socket réteg (SSL) használatára, konfigurálni kell az igazolást a szerver számára az SSL kezdeményezése érdekében. A forgatókönyv céljai alapján úgy döntött, hogy Helyi igazolási hatóságot (CA) hoz létre és működtet, mely kiadja az igazolást a szervernek.

Amikor Digitális igazolás kezelővel (DCM) létrehozza a Helyi CA-t, a program végigvezeti a folyamaton, ami garantálja, hogy mindent beállított az SSL engedélyezéséhez az alkalmazás számára. Ez magában foglalja az igazolás hozzárendelését is, amelyet a Helyi CA ad ki a webszerver alkalmazásnak. Ezenkívül hozzáadja a Helyi CA hatóságot a webszerver alkalmazás megbízható CA-kat tartalmazó listájához. Ha a Helyi CA benne van az alkalmazás listájában, akkor az alkalmazás biztosan felismeri és hitelesíti azokat a felhasználókat, akik a Helyi CA által kiadott igazolásokat mutatják be.

Hajtsa végre az alábbi lépéseket, ha Digitális igazolás kezelővel (DCM) hoz létre és működtet Helyi CA-t, és ad ki igazolást az emberi erőforrás szerveralkalmazásnak:

1. Indítsa el a DCM funkciót.
2. A DCM navigációs keretén válassza ki az **Igazolási hatóság (CA) létrehozását** az űrlapok megjelenítéséhez. Ezek az űrlapok végigvezetik a Helyi CA létrehozásának folyamatán, valamint az SSL, objektum aláírás és aláírás ellenőrzés céljára használt digitális igazolások használatának elkezdéséhez szükséges egyéb feladatok végrehajtásán.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
3. Töltse ki az űrlapot. Az űrlapok segítségével elvégezheti a működő Helyi igazolási hatóság (CA) beállításához szükséges összes feladatot:
   a. Adja meg a Helyi CA azonosítási információit.
   b. Telepítse a Helyi CA igazolást a PC-jén vagy a böngészőjében, hogy a szoftver felismerhesse a Helyi CA-t és ellenőrizhesse az általa kiadott igazolásokat.
   c. Válassza ki a Helyi CA stratégiai adatait.

      Megjegyzés: Feltétlenül válassza ki, hogy a Helyi CA ki tudjon adni felhasználói igazolásokat.
   d. Az új Helyi CA segítségével adja ki a szerver vagy a kliens igazolást, amelyet alkalmazásai az SSL kapcsolatokhoz használhatnak.
   e. Válassza ki azokat az alkalmazásokat, amelyek használhatják a szerver vagy a kliens igazolást az SSL kapcsolatokhoz.

      Megjegyzés: Feltétlenül válassza ki az alkalmazás azonosítót (ID) az emberi erőforrások HTTP szervere számára.
   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.

      Megjegyzés: A forgatókönyv ugyan nem használ objektum aláíró igazolást, de azért hajtsa végre ezt a lépést. Ha félbehagyja a feladatot ennél a pontnál, a feladat befejeződik, és újabb feladatokat kell végrehajtani ahhoz, hogy befejezze az SSL igazolás konfigurálását.
   g. Válassza ki az alkalmazásokat, amelyek megbízhatónak tekintik a Helyi CA-t.

      Megjegyzés: Feltétlenül válassza ki az alkalmazás azonosítót (ID) az emberi erőforrások HTTP szervere számára, amely megbízhatónak tekinti a Helyi CA-t.

Most, hogy befejezte az igazolás konfigurálását, amelyet a webszerver alkalmazás igényel az SSL használatához, konfigurálhatja a webszerver alkalmazást, hogy igazolást kérjen a felhasználói hitelesítéshez.

4. lépés: Az emberi erőforrás webszerver konfigurálása, hogy igazolásokat kérjen a kliens hitelesítéshez

Az iSeries A szerveren futó emberi erőforrás HTTP Server termékhez beállított Védett socket réteg (SSL) konfigurációs lépései (amelyekkel igazolást kér a kliens hitelesítéshez) erőteljesen függnek attól, hogy az alkalmazás eredeti vagy Apache verzióját használja-e.

Olvassa el a Védelmi beállítások létrehozása a HTTP szerveren (eredeti) című részt, ha kíváncsi a HTTP Server (eredeti) konfigurálásáról, hogy igazolást kérjen a kliens hitelesítéshez.

Olvassa el a Forgatókönyv: A JKL engedélyezi a Védett socket réteg (SSL) védelmet a HTTP szervereken (Apache meghajtású) című részt, ha igazolásokat kér a kliens hitelesítéshez. Ez a HTTP Server forgatókönyv tartalmazza az összes olyan feladatsort, amellyel létrehozza a virtuális gazdagépet, és konfigurálja azt SSL és igazolás használatára a kliens hitelesítéshez. Az SSL és az igazolás kliens hitelesítésre való konfigurálásához tartozó lépéseket megtalálja az ″SSL engedélyezése virtuális gazdagép számára″ fejléc alatt.

A HTTP Server for iSeries (eredeti vagy Apache alapú) jelenlegi és jövőbeli változatainak konfigurálásáról a Web kiszolgálás című témakörben olvashat.

5. lépés: Az emberi erőforrás webszerver elindítása SSL módban

Lehet, hogy le kell állítani és újra el kell indítani a HTTP szervert ahhoz, hogy a szerver bizonyosan meghatározhassa az igazolás hozzárendelések meglétét, és segítségükkel kezdeményezhesse az SSL szekciókat.

A Konfigurálás és az Adminisztráció űrlapok segítségével állítsa le és indítsa újra a HTTP szervert (eredeti), valamint kövesse az alábbi lépéseket:

1. Kattintson az **Adminisztrációra**.
2. Kattintson a **HTTP szerverek kezelésére**.
3. Válassza ki a szervert.
4. Írja be az indítási paraméterek értékeit az űrlapon található mezőkbe.
5. Kattintson a **Start** gombra.

Megjegyzés: Ha a szerver futott, amikor az igazolást hozzárendelte, állítsa le, majd indítsa el a szervert. Az **Újraindításra** kattintással nem biztos, hogy a szerver meg tudja határozni az igazolások körében történt módosításokat, amelyek a futás alatt következtek be.

A Konfigurálás és az Adminisztráció űrlapok segítségével állítsa le és indítsa újra a HTTP szervert (Apache alapú), valamint kövesse az alábbi lépéseket:

1. Kattintson az **Adminisztrációra**.
2. A menü baloldalán kattintson az **Általános szerver adminisztráció** alatt lévő **HTTP szerverek kezelésére**.
3. Válassza ki a szervert, amellyel dolgozni akar, majd kattintson a **Start** vagy a **Stop** gombra. Olvassa el az online súgót, ha többet szeretne megtudni az indítási paraméterekről.

A HTTP Server for iSeries (eredeti vagy Apache alapú) jelenlegi és jövőbeli változatainak konfigurálásáról többet megtudhat a Web kiszolgálás című témakörben.

A feladatok befejezésével elindíthatja az emberi erőforrás alkalmazást SSL módban, és elkezdheti az alkalmazás által nyújtott adatok védelmét.

6. lépés: A helyi CA igazolás egy példányának telepítése a felhasználók böngésző programjába

Amikor a felhasználó eléri a Védett socket réteg (SSL) kapcsolatot biztosító szervert, a szerver egy igazolást mutat fel a kliens szoftvernek az azonosság ellenőrzése céljából. A kliens szoftvernek ellenőriznie kell a szerver igazolását, mielőtt a szerver létrehozhatná a szekciót. Ahhoz, hogy a kliens szoftver ellenőrizni tudja a szerver igazolását, rendelkeznie kell a szerver igazolását kiadó Igazolási hatóságra (CA) vonatkozó igazolás egy, helyben tárolt példányával. Ha a szerver egy nyilvános Internet CA igazolását használja, akkor a böngészőnek vagy más egyéb kliens szoftvernek már rendelkeznie kell a CA igazolás egy példányával. Ha - ahogy a forgatókönyvben van - a szerver egy magán CA által kibocsátott igazolást mutat fel, akkor minden felhasználónak telepíteni kell a CA igazolás egy példányát a Digitális igazolás kezelő (DCM) segítségével.

Minden felhasználónak (kliens B, C és D) végre kell hajtani az alábbi lépéseket, hogy beszerezzék a Helyi CA igazolás egy példányát:

1. Indítsa el a DCM funkciót.
2. A navigációs kereten válassza ki a **Helyi CA igazolás telepítése saját PC-re** feladatot, amely révén megjelenik egy lap, ahol letöltheti a helyi CA igazolást a böngészőjébe, vagy letárolhatja egy fájlba a rendszeren.
3. Válassza ki az igazolás telepítése opciót. Az opció letölti a Helyi CA igazolást a böngészőbe megbízható gyökérként. Ez garantálja azt, hogy a böngésző biztonságos kommunikációs szekciókat létesíthet azokkal a webszerverekkel, amelyek ugyancsak az adott CA igazolását használják. A böngésző program ablakok sorát jeleníti meg, amelyek segítik a telepítés végrehajtását.
4. Kattintson az **OK** gombra, hogy visszatérjen a Digitális igazolás kezelő honlapjára.

7. lépés: Minden felhasználó kérjen igazolást a Helyi CA-tól

A korábbi lépésekben úgy konfigurálta az emberi erőforrás webszervert, hogy kérjen igazolásokat a felhasználói hitelesítéshez. A felhasználóknak Helyi CA-tól kapott érvényes igazolást kell bemutatni ahhoz, hogy hozzáférést kapjanak a webszerverhez. Minden felhasználónak a Digitális igazolás kezelő (DCM) segítségével kell beszerezni az igazolást az **Igazolás létrehozása** feladattal. Ahhoz, hogy a helyi CA-tól be lehessen szerezni az igazolást, a CA előírásainak meg kell engedni, hogy a CA kiadhasson felhasználói igazolásokat.

Minden felhasználónak (kliens B, C és D) végre kell hajtani az alábbi lépéseket, hogy beszerezzék az igazolást:

1. Indítsa el a DCM funkciót.
2. A navigációs kereten válassza ki az **Igazolás létrehozását**.
3. Válassza ki a **Felhasználói igazolást** a létrehozandó igazolás típusának. Megjelenik egy űrlap, amelyen megadhatja az azonosítási információkat az igazolás számára.
4. Töltse ki az űrlapot, és kattintson a **Folytatásra**.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
5. Ezen a ponton a DCM a böngészővel dolgozik együtt, hogy létrehozza a magán és a nyilvános kulcsot az igazolás számára. A böngésző megjeleníthet egy olyan ablakot, amely végigvezeti ezen a folyamaton. Kövesse a böngésző feladatokra vonatkozó utasításait. Miután a böngésző előállítja a kulcsokat, egy megerősítés lap jelenik meg, amely azt jelzi, hogy a DCM létrehozta az igazolást.

6. Telepítse az új igazolást a böngésző szoftverbe. A böngésző megjeleníthet egy olyan ablakot, amely végigvezeti ezen a folyamaton. Kövesse a feladat elvégzéséhez adott böngésző utasításokat.
7. Kattintson az **OK** gombra a feladat befejezéséhez.

A feldolgozás közben a Digitális igazolás kezelő automatikusan társítja az igazolást az iSeries felhasználói profillal.

Fejezet 5. A digitális igazolás alapjai

Mielőtt a rendszer és a hálózati biztonság növelése érdekében megkezdené a digitális igazolások használatát, ismerje meg őket és az általuk nyújtott előnyöket.

A digitális igazolás valójában egy digitális jogosítvány, ami megerősíti az igazolás tulajdonosának kilétét, hasonlóan mint ahogy az útlevél. Az Igazolási hatóságnak (CA) nevezett megbízható partner adja ki a digitális igazolásokat a felhasználóknak és a szervereknek, illetve a kliens alkalmazásoknak. A CA iránti bizalom az alapja annak, hogy az igazolást érvényes jogosítványnak tekintjük.

A digitális igazolások alapjairól a következő témakörök szólnak:

Megkülönböztetett név
Az itt leírtak alapján tanulmányozhatja a digitális igazolások azonosítási jellemzőit.

Digitális aláírások
Az itt leírtak segítségével tanulmányozhatja a digitális aláírásokat, és az objektum sértetlenségében játszott szerepüket.

Nyilvános - magánkulcs pár
Az itt leírtak alapján tanulmányozhatja a digitális igazolásokhoz tartozó biztonsági kulcsokat.

Igazolási hatóság (CA)
Az itt leírtak alapján tanulmányozhatja az Igazolási hatóságokat (CA) és más egyedeket, amelyek digitális igazolásokat adnak ki.

CRL helyek
Az itt leírtak segítségével tanulmányozhatja az Igazolás visszavonási listát (CRL), és annak használatát az igazolások hitelesítésének és érvényesítésének folyamatában.

Igazolás tárolók
Az itt leírtak segítségével tanulmányozhatja az igazolás tárolót, továbbá a tárolók és tartalmuk kezelését Digitális igazolás kezelővel (DCM).

Titkosítás
Az itt leírtak segítségével tanulmányozhatja a titkosítást, valamint azt, hogy a digitális igazolások hogyan használják fel a titkosítási funkciókat a biztonság növelése érdekében.

Védett socket réteg (SSL)
Itt az SSL rövid leírását olvashatja el.

Megkülönböztetett név

Minden egyes CA rendelkezik olyan előírással, ami meghatározza, hogy milyen azonosítási információkat igényel az igazolás kiadása céljából. Egyes nyilvános Internet Igazolási hatóságok kevés adatot kérnek, például nevet és e-mail címet. Más nyilvános CA-k több adatot is kérhetnek, és megkövetelhetik az azonosítási információk szigorú ellenőrzését az igazolás kiadása előtt. Például, a Public Key Infrastructure Exchange (PKIX) szabványt támogató CA-k kérhetik, hogy az igénylő ellenőrizze az azonosítási adatokat a Regisztrációs hatóságon (RA) keresztül az igazolás kiadása előtt. Következésképpen, ha az igazolásokat jogosítványokként akarja elfogadni és használni, nézze át a CA-ra vonatkozó követelményeket, hogy meghatározza, a követelmények kielégítik-e biztonsági igényeit.

A megkülönböztetett név (DN) olyan fogalom, amely (az igazolás részeként) leírja az igazolás tulajdonosának azonosítási információit. Az igazolást kiadó CA azonosítási irányelveitől függően a DN különféle információkat tartalmazhat. A Digitális igazolás kezelő (DCM) segítségével kezelheti a magán Igazolási hatóságot és a magán igazolások kiadását. A DCM

segítségével generálhatja a DN információkat, és a nyilvános Internet CA által a szervezetnek kiadott igazolásokhoz tartozó kulcspárokat. A DN információk, amelyeket bármilyen típusú igazoláshoz biztosíthat, a következőket tartalmazzák:

- Igazolás tulajdonosának általános neve
- Szervezet
- Szervezeti egység
- Város
- Megye
- Ország

Amikor a DCM segítségével kiad magán igazolásokat, további DN információkat adhat meg az igazoláshoz:

- Verzió 4 IP cím
- Teljesen megadott tartománynév
- E-mail cím

Ezek a kiegészítő adatok igen hasznosak, ha igazolást kíván használni a virtuális magánhálózat (VPN) jellegű kapcsolat konfigurálásához.

Digitális aláírások

Elektronikus dokumentumon lévő digitális aláírás vagy egyéb objektum, amelyet titkosítás révén hoz létre, és ami megfelel az írott dokumentumon lévő személyes aláírásnak. 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 Igazolási hatóság (CA) aláírja az általa kiadott igazolásokat. Az aláírás egy olyan adatláncból áll, amely az Igazolási hatóság magánkulcsával lett titkosítva. Az igazoláson lévő aláírást bármely felhasználó ellenőrizheti, ha visszafejti az Igazolási hatóság nyilvános kulcsával.

A digitális aláírás olyan elektronikus aláírás, amelyet a felhasználó vagy az alkalmazás hoz létre az objektumon a digitális igazolás magánkulcsával. Az objektumon lévő digitális aláírás az aláíró azonosságának (az aláírási kulcs tulajdonosa) és az objektum eredetének egyedi elektronikus összekapcsolását biztosítja. Amikor digitális aláírást tartalmazó objektumhoz nyer hozzáférést, ellenőrizheti az objektumon lévő aláírást, hogy meggyőződjön az objektum forrásának valódiságáról (például, az alkalmazás, amit éppen letölt, valójában felhatalmazott forrásból jön, mint például IBM). Ez az ellenőrzési folyamat lehetővé teszi annak meghatározását is, hogy vajon nem történt-e jogosulatlan módosítás az objektumon az aláírás óta.

Példa a digitális aláírás működésére

Egy szoftverfejlesztő olyan iSeries alkalmazást írt, amelyet az Interneten keresztül (kényelmes és takarékos módszerként) kíván terjeszteni vásárlói részére. Azonban, azt is tudja, hogy a vásárlók megalapozottan aggódnak a programok Internetről való letöltésekor az olyan objektumokkal kapcsolatos problémák növekedése miatt, amelyek legitim programoknak látszanak, de valójában ártalmas (például vírus) programokat tartalmaznak.

Következésképpen úgy dönt, hogy digitálisan aláírja az alkalmazást, így vásárlói ellenőrizhetik, hogy valóban a fejlesztő cége az alkalmazás legitim forrása. Az alkalmazás aláírásához a digitális igazolás magánkulcsát használja. Az igazolást egy jólismert nyilvános Igazolási hatóságtól szerezte be. Majd ezután letölthető formában elérhetővé teszi az alkalmazást a vásárlók számára. A letöltési csomag részeként elhelyezi az objektum

aláírásához használt digitális igazolás egy példányát. Amikor a vásárló letölti az alkalmazási csomagot, ellenőrizheti az alkalmazáson lévő aláírást az igazolás nyilvános kulcsával. Ez a folyamat lehetővé teszi a vásárlónak, hogy azonosítsa és ellenőrizze az alkalmazást, és arról is meggyőződhessen, hogy az alkalmazás objektum nem módosult-e az aláírás óta.

Nyilvános - magánkulcs pár

Minden digitális igazoláshoz tartozik egy pár titkosítási kulcs. Ez a kulcspár magán- és nyilvános kulcsból áll. (Az aláírás ellenőrző igazolások kivételek ezen szabály alól, és csak nyilvános kulccsal rendelkeznek.)

A nyilvános kulcs a tulajdonos digitális igazolásának része, és mindenki számára elérhető. A magánkulcsot azonban védi a kulcs tulajdonosa, és csak ő érheti el. Ez a korlátozott hozzáférés biztosítja azt, hogy a kulcsot használó kommunikáció megmarad biztonságosnak.

Az igazolás tulajdonosa a kulcsok felhasználása révén kihasználhatja a kulcsok nyújtotta titkosítási funkció előnyeit. Például, az igazolás tulajdonosa az igazolás magánkulcsával ″aláírhatja″ és titkosíthatja a felhasználók és a szerverek között küldött adatokat, mint például üzeneteket, dokumentumokat és kód objektumokat. Az aláírt objektum címzettje az aláíró igazolásban lévő nyilvános kulcs segítségével fejtheti vissza az aláírást. Az ilyen digitális aláírások garantálják az objektum eredetének megbízhatóságát, és ellenőrzi annak sértetlenségét.

Igazolási hatóság (CA)

Az Igazolási hatóság (CA) egy megbízható központi adminisztrációs egyed, amely digitális igazolásokat bocsát ki a felhasználóknak és a szervereknek. A CA iránti bizalom az alapja annak, hogy az igazolást érvényes jogosítványnak tekintjük. A CA saját magánkulcsát használja az igazolás digitális aláírásához, amelyet kiad az igazolás eredetének ellenőrzése céljából. Mások a CA igazolások nyilvános kulcsát használhatják fel a CA által kiadott és aláírt igazolások hitelességének ellenőrzéséhez.

A CA lehet nyilvános kereskedelmi egyed, mint például a VeriSign, vagy egy magán egyed, amelyet egy szervezet működtet belső célokra. Számos üzleti vállalkozás nyújt kereskedelmi Igazolási hatóságot az Internet felhasználók számára. A Digitális igazolás kezelő (DCM) lehetővé teszi mind a nyilvános, mind a magán CA-k által kiadott igazolások kezelését.

A DCM segítségével működtethet saját helyi magán CA-t, amely révén magán igazolásokat bocsáthat ki a rendszereknek és a felhasználóknak. Amikor a CA kiad egy felhasználói igazolást, a DCM automatikusan összetársítja a felhasználó igazolását az iSeries rendszer felhasználói profiljával. Ez garantálja azt, hogy az igazolás hozzáférési és jogosultsági privilégiumai megegyeznek a tulajdonos felhasználói profiljának privilégiumaival.

Megbízható gyökér állapot

A megbízható gyökér kifejezés egy különleges kijelölésre utal, amelyet a CA igazolásban adnak meg. Ez a megbízható gyökér kijelölés lehetővé teszi a böngészőnek vagy más alkalmazásnak, hogy hitelesítse és elfogadja az Igazolási hatóság (CA) által kiadott igazolásokat.

Amikor letölti a CA igazolást a böngészőbe, a böngésző megengedi, hogy ezt kijelölje megbízható gyökérnek. Az igazolások használatát támogató egyéb alkalmazásokat is úgy kell konfigurálni, hogy kijelöljön egy CA-t (amiben megbízik), mielőtt az alkalmazás hitelesítené az adott CA által kiadott igazolásokat.

A DCM segítségével engedélyezheti vagy letilthatja az Igazolási hatóság (CA) igazolásának megbízható állapotát az igazolás tárolóban. Amikor engedélyezi a CA igazolást, megadhatja azokat az alkalmazásokat, amelyek használhatják a CA által kiadott igazolások hitelesítésére és elfogadására. Amikor letiltja a CA igazolást, nem adhatja meg azokat az alkalmazásokat, amelyek használhatnák a CA által kiadott igazolások hitelesítésére és elfogadására.

Igazolási hatóság eljárási adatai

Amikor a Digitális igazolás kezelővel létrehoz egy Igazolási hatóságot (CA), meghatározhatja a CA eljárási adatait. A CA eljárási adatai leírják az aláírási privilégiumokat. Az eljárási adatok meghatározzák:
- A CA ki tud-e adni és alá tud-e írni felhasználói igazolásokat.
- A CA által kiadott igazolások mennyi ideig érvényesek.

Igazolás visszavonási lista (CRL) helyek

Az Igazolás visszavonási lista (CRL) olyan fájl, amely felsorolja egy adott Igazolási hatóság (CA) összes érvénytelen és visszavont igazolását. A CA-k rendszeresen frissítik CRL listáikat, és nyilvánosságra hozzák őket mások számára az LDAP címtárakban. Kevés CA - mint például a finn SSH - az LDAP címtárakban teszi közzé a CRL listát, amelyeket közvetlenül elér. Ha a CA-k közreadják saját CRL listáikat, az igazolás jelzi ezt, mivel tartalmazza a CRL elosztási pont kiterjesztést Egyetemes erőforrás azonosító (URI) formátumban.

A Digitális igazolás kezelő (DCM) lehetővé teszi, hogy meghatározza és kezelje a CRL helyeket, s ezáltal még szigorúbbá váljon az igazolás hitelesítés, amelyet használ vagy másoktól elfogad. A CRL hely definíció leírja a CRL listát tároló LDAP szerver helyét és az elérhetőségére vonatkozó információkat.

Az alkalmazások, amelyek végrehajtják az igazolás hitelesítést, hozzáférnek a CRL helyhez, ha egy is definiálva van a kiadó CA-ra, s így ellenőrizhetik, hogy nem vonta-e vissza a CA az adott igazolást. A DCM lehetővé teszi, hogy meghatározza és kezelje a CRL hely-információkat, amelyekre az alkalmazásoknak szükségük van a CRL feldolgozás végrehajtásához az igazolás hitelesítés során. Példák alkalmazásokra és folyamatokra, amelyek végrehajthatnak CRL feldolgozást az igazolás hitelesítés során: virtuális magánhálózat (VPN) Internet kulcs csere (IKE) szerver, védett socket réteg (SSL) engedélyes alkalmazások és objektum aláíró folyamatok. Amikor definiál egy CRL helyet és társítja CA igazolással, a DCM végrehajtja a CRL feldolgozást az adott CA által kiadott igazolások ellenőrzési eljárásának részeként.

Igazolás tárolók

Az igazolás tároló egy speciális kulcs adatbázis fájl, amelyet a Digitális igazolás kezelő (DCM) használ a digitális igazolások tárolására. Az igazolás tároló őrzi az igazolás magánkulcsát is, hacsak helyette nem a 4758 Cryptographic Coprocessor kártyát választja a kulcs tárolásához. A DCM lehetővé teszi az igazolás tárolók több típusának létrehozását és kezelését. Az igazolás tárolók elérését a DCM vezérli jelszavak, valamint az igazolás tárolót alkotó IFS fájlok és IFS alkönyvtár hozzáférés vezérlése alapján.

Az igazolás tárolók osztályozása az általuk tartalmazott igazolások típusa alapján történik. Az egyes igazolás tárolókban elvégezhető kezelési feladatokat az adott igazolás tárolóban őrzött igazolás típusa határozza meg. A DCM segítségével a következő előre megadott igazolás tárolókat hozhatja létre és kezelheti:

Helyi igazolási hatóság (CA)
A DCM a helyi CA igazolás és a hozzátartozó magánkulcs tárolására használja ezt az igazolás tárolót, ha létrehoz helyi CA-t. Az itt tárolt igazolást használhatja fel a helyi CA által kiadott igazolások aláírására. Amikor a helyi CA kiad egy igazolást, a DCM elhelyezi a CA igazolás egy példányát (a magánkulcs nélkül) a megfelelő igazolás tárolóba (például *SYSTEM) hitelesítési célból. Az alkalmazások a CA igazolás segítségével ellenőrzik az igazolások eredetét, amit az SSL kapcsolat egyeztetése során tesznek meg, hogy jogosultságot adjanak az erőforrásokhoz.

***SYSTEM**
A DCM a szerver vagy a kliens igazolások kezeléséhez biztosítja ezt az igazolás tárolót, amelyet a Védett socket réteg (SSL) kommunikációs szekcióban résztvevő alkalmazások használnak. Az IBM iSeries alkalmazások (és számos más szoftverfejlesztő alkalmazása) csak a *SYSTEM igazolás tárolóban őrzött igazolásokat tudják használni. Amikor a DCM segítségével helyi CA-t hoz létre, a DCM létrehozza ezt az igazolás tárolót a folyamat részeként. Ha úgy dönt, hogy egy nyilvános CA-tól (mint például VeriSign) szerzi be az igazolásokat a szerver vagy a kliens alkalmazások számára, akkor saját kezűleg kell létrehozni ezt az igazolás tárolót.

***OBJECTSIGNING**
A DCM az objektumok digitális aláírásához használt igazolások kezeléséhez biztosítja ezt az igazolás tárolót. Az igazolás tároló feladatai megengedik, hogy létrehozzon digitális aláírásokat az objektumokon, valamint megjelenítse és ellenőrizze azokat. Amikor a DCM segítségével helyi CA-t hoz létre, a DCM létrehozza ezt az igazolás tárolót a folyamat részeként. Ha úgy dönt, hogy egy nyilvános CA-tól (mint például VeriSign) szerzi be az igazolásokat az objektumok aláírásához, akkor saját kezűleg kell létrehozni ezt az igazolás tárolót.

***SIGNATUREVERIFICATION**
A DCM az objektumokon lévő digitális aláírások hitelességének ellenőrzéséhez használt igazolások kezeléséhez biztosítja ezt az igazolás tárolót. Ahhoz, hogy ellenőrizze a digitális aláírást, az igazolás tárolónak tartalmaznia kell az objektumot aláíró igazolás egy példányát. Az igazolás tárolónak ugyancsak tartalmaznia kell a CA igazolás egy példányát is, mégpedig arra a CA-ra vonatkozóan, amelyik kiadta az aláíró igazolást. A kérdéses igazolásokat beszerezheti úgy, hogy (1) az aktuális rendszeren lévő objektum aláíró igazolást exportálja a tárolóba, vagy (2) az objektum aláírótól kapott igazolásokat importálja.

Egyéb rendszer igazolás tároló
Ez az igazolás tároló másodlagos tárolási helyet biztosít az SSL szekciókhoz használt szerver vagy kliens igazolások számára. Ezek a tárolók valójában felhasználó által megadott másodlagos igazolás tárolók az SSL igazolások számára. Az Egyéb rendszer igazolás tároló nevű opció lehetővé teszi az igazolások kezelését olyan alkalmazások számára, amelyeket az SSL_Init API használatára írtak, hogy az SSL szekciók létesítéséhez szükséges igazolások programozottan elérhetők és használhatók legyenek. Ez az API lehetővé teszi az alkalmazásnak, hogy az igazolás tárolóhoz rendelt alapértelmezett igazolást használja, és ne azt, amelyet a felhasználó kifejezetten megadott. A leggyakrabban akkor használja ezt az igazolás tárolót, amikor a DCM előző változatából telepíti át az igazolásokat, vagy amikor egy speciális igazoláskészletet hoz létre az SSL használathoz.

Megjegyzés: Ha az iSeries szerverén telepítve van a 4758 PCI Cryptographic Coprocessor, akkor választhat más tárolóhelyet is az igazolásaihoz tartozó magánkulcsok számára (az objektum aláíró igazolások kivételével). Választhatja azt, hogy a magánkulcsokat magában a ko-processzorban tárolja, illetve a segítségével titkosítja a magánkulcsot, és az igazolás tároló helyett egy speciális kulcsfájlban tárolja.

A DCM jelszavak révén vezérli az igazolás tárolók elérését. A DCM vezérli az integrált fájlrendszerbeli alkönyvtár és az igazolás tárolót alkotó fájlok elérését is. A Helyi igazolási hatóság (CA), a *SYSTEM, az *OBJECTSIGNING és a *SIGNATUREVERIFICATION igazolás tárolóknak megszabott elérési útvonaluk van az integrált fájlrendszeren belül, míg az Egyéb rendszer igazolás tárolók bárhol elhelyezkedhetnek az integrált fájlrendszerben.

Titkosítás

A titkosítás az adatok biztonságos állapotának megőrzését szolgáló tudomány. A titkosítás lehetővé teszi az információ tárolását vagy a másokkal való kommunikálást, miközben megakadályozza a kívülálló feleket abban, hogy megértsék a tárolt információt vagy a kommunikációt. A titkosítás átalakítja az érthető szöveget érthetetlen adatelemekre (rejtjeles szöveg - ciphertext). A visszafejtés visszaállítja az érthető szöveget az érthetetlen adatokból. Mindkét folyamat matematikai formulát vagy algoritmust és egy titkos adatrendezőt (kulcs) foglal magában.

A titkosításnak két típusa van:

- Az **osztott vagy titkos kulcs (szimmetrikus)** titkosításban egy kulcs van megosztva a két kommunikáló fél között. A titkosítás és a visszafejtés ugyanazt a kulcsot használja.
- A **nyilvános kulcs (aszimmetrikus)** titkosításban a titkosítás és a visszafejtés mindegyike különböző kulcsokat használ. Egy készlet egy kulcspárból áll, amely egy nyilvános és egy magánkulcsot jelent. A nyilvános kulcs szabadon terjeszthető, általában a digitális igazolások körén belül, míg a magánkulcsot a tulajdonosnak kell biztonságos helyen tartani. A két kulcs matematikailag ugyan összetartozik, de látszólag lehetetlen kideríteni a magánkulcsot a nyilvános kulcsból. Egy objektumot, mint például üzenetet, amelyet valakinek a nyilvános kulcsával titkosított, csak a hozzátartozó magánkulccsal lehet visszafejteni. Ehhez hasonlóan, a szerver vagy a felhasználó ″aláírhatja″ az objektumot a magánkulcs segítségével, és a fogadó fél a megfelelő nyilvános kulcsot felhasználva visszafejtheti a digitális aláírást, hogy ellenőrizze az objektum forrását és sértetlenségét.

Védett socket réteg (SSL)

A Védett socket réteg (SSL) protokoll eredetileg a Netscape által létrehozott ipari szabvány, amely a kliensek és a szerverek közötti szekció titkosítására szolgál. Az SSL aszimmetrikus vagy nyilvános kulcsot használó titkosítási eljárást alkalmaz a szerver és a kliens közötti szekció titkosításához. A kliens és a szerver alkalmazások egyeztetik a szekció kulcsot a digitális igazolások kicserélése során. A kulcs automatikusan lejár 24 óra után, és az SSL feldolgozás egy másik kulcsot hoz létre minden szerver kapcsolatnak és minden kliensnek. Következésképpen, még ha elfogják és visszafejtik is a szekció kulcsot jogosulatlan felhasználók (ami valószínűtlen), nem tudják felhasználni a későbbi szekciók lehallgatására.

Fejezet 6. A DCM tervezése

Ahhoz, hogy a Digitális igazolás kezelő (DCM) hatékonyan kezelni tudja a cég digitális igazolásait, a biztonsági irányelvek részeként átfogó tervet kell készíteni a digitális igazolások kezeléséről.

Az alábbi témakörök nyújtanak tájékoztatást a DCM használatának tervezéséről, valamint a digitális igazolások és a biztonsági irányelvek összetartozásáról:

A DCM használatának követelményei
Tanulmányozhatja, hogy milyen szoftvert kell telepíteni, valamint megismerheti, hogy mi szükséges a rendszer beállításához a DCM használata érdekében.

A digitális igazolások típusai
Az itt leírtak révén tanulmányozhatja a különböző típusú igazolásokat, amelyeket a DCM segítségével kezelhet.

A nyilvános és a magán igazolások összevetése
Az itt leírtak segítségével tanulmányozhatja annak meghatározását, hogy milyen típusú igazolás felel meg a legjobban üzleti igényeinek, ha már egyszer eldöntötte, hogyan kívánja alkalmazni őket, hogy kihasználhassa az általuk nyújtott többlet biztonság előnyeit. Használhat nyilvános Igazolási hatóságtól (CA) eredő igazolást, de létrehozhat és működtethet magán CA-t is az igazolások kiadása céljából. Az igazolások beszerzésének módja használatuk módjától függ.

Digitális igazolások Védett socket réteg (SSL) kommunikációkhoz
Az itt leírtak révén tanulmányozhatja, hogyan lehet az igazolásokat úgy használni, hogy az alkalmazások biztonságos kommunikációs szekciókat tudjanak létesíteni.

Digitális igazolások felhasználó hitelesítéshez
Az itt leírtak révén tanulmányozhatja, hogyan lehet az igazolásokat úgy használni, hogy az iSeries szerver erőforrásait elérő felhasználók fokozottabb hitelesítési eljáráson essenek át.

Digitális igazolások Virtuális magánhálózati (VPN) kapcsolatok hitelesítéséhez
Az itt leírtak révén tanulmányozhatja, hogyan lehet az igazolásokat a VPN kapcsolatok konfigurálásának részeként használni.

Digitális igazolások objektumok aláírásához
Az itt leírtak révén tanulmányozhatja, hogyan lehet az igazolásokat felhasználni az objektumok sérthetetlenségének garantálására, vagy az objektumon lévő digitális aláírás ellenőrzéséhez, ami hitelesítési célból történik.

Digitális igazolások objektum aláírások ellenőrzéséhez
Az itt leírtak révén tanulmányozhatja, hogyan lehet az igazolásokat felhasználni az objektumon lévő digitális aláírás ellenőrzéséhez, ami hitelesítési célból történik.

DCM beállítási követelmények

A Digitális igazolás kezelő (DCM) ingyenes iSeries funkció, amely lehetővé teszi a digitális igazolások központi kezelését az alkalmazások számára. A DCM sikeres használatához a következőket kell tenni:

- Telepítse a titkosítás elérését biztosító licencprogramot (5722–AC3). Ez a termék meghatározza a kulcs maximális hosszát, amelyet az export és import szabályokon alapuló titkosítási algoritmusnak engedélyez. A terméket telepíteni kell ahhoz, hogy létrehozhasson igazolást.
- Telepítse az OS/400 34-es opcióját. Ez a böngésző alapú DCM funkció.
- Telepítse az IBM HTTP Server for iSeries (5722–DG1) terméket, és indítsa el az *ADMIN szerver példányt.

- Győződjön meg arról, hogy a TCP úgy van konfigurálva a rendszeren, hogy használhatja a web böngészőt és a HTTP Server *ADMIN példányát a DCM funkció eléréséhez.

Megjegyzés: Addig nem tud létrehozni igazolásokat, amíg nem telepíti az összes szükséges terméket. Ha nincs telepítve valamelyik szükséges termék, a DCM hibaüzenetet jelenít meg, amely a hiányzó összetevő telepítésére ad utasítást.

A digitális igazolások típusai

A digitális igazolásokat többféleképpen osztályozzák. Ezek az osztályozások leírják az igazolások használatát. A Digitális igazolás kezelő (DCM) segítségével a következő igazolás típusokat kezelheti:

Igazolási hatóság (CA) igazolások
Az Igazolási hatóság igazolás valójában egy digitális jogosítvány, ami megerősíti az igazolást birtokló Igazolási hatóság (CA) kilétét. Az Igazolási hatóság igazolása tartalmazza a hatóság azonosító információit, valamint annak nyilvános kulcsát. Mások a CA igazolások nyilvános kulcsát használhatják fel a CA által kiadott és aláírt igazolások hitelességének ellenőrzéséhez. Az Igazolási hatóság igazolását aláírhatja egy másik CA, mint például VeriSign, vagy önmaga, ha független egyedről van szó. A Digitális igazolás kezelőben létrehozott CA független egyed. Mások a CA igazolások nyilvános kulcsát használhatják fel a CA által kiadott és aláírt igazolások hitelességének ellenőrzéséhez. Ahhoz, hogy az igazolás használható legyen SSL, objektum aláírása vagy objektumon lévő aláírás ellenőrzése céljára, rendelkezni kell a CA igazolás egy példányával arra a CA-ra vonatkozóan, amely kiadta az igazolást.

Szerver vagy kliens igazolások
A szerver vagy kliens igazolás egy digitális jogosítvány, amely azonosítja azt a szerver vagy kliens alkalmazást, amely felhasználja az igazolást a biztonságos kommunikációhoz. A szerver vagy a kliens igazolások tartalmazzák az alkalmazást birtokló szervezet azonosítására szolgáló információkat, mint például a rendszer megkülönböztetett nevét. Az igazolás tartalmazza a rendszer nyilvános kulcsát is. A szervernek digitális igazolás kell ahhoz, hogy használhassa a Védett socket réteg (SSL) protokollt a biztonságos kommunikációkhoz. A digitális igazolást támogató alkalmazások vizsgálhatják a szerver igazolását, hogy ellenőrizzék a szerver kilétét, amikor a kliens eléri a szervert. Az alkalmazás azután hitelesíti az igazolást, ami a kliens és a szerver közötti SSL titkosított szekció kezdeményezésének az alapja. A következő típusú igazolásokat csak a *SYSTEM igazolás tárolóban kezelheti.

Objektum aláíró igazolások
Az objektum aláíró igazolás az objektum digitális aláírására szolgáló igazolás. Az objektum aláírása révén ellenőrizheti az objektum sértetlenségét, és az objektum tulajdonjogának eredetét is. Az igazolással különféle objektumokat írhat alá, beleértve az integrált fájlrendszerbeli (IFS) és a *CMD objektumok többségét. Az aláírható objektumok teljes listáját az Objektum aláírás és aláírás ellenőrzés című témakör tartalmazza. Amikor az objektum aláírásához az objektum aláíró igazolás magánkulcsát használja, az objektum fogadójának rendelkeznie kell az aláírás ellenőrző igazolás egy példányával, hogy megfelelően hitelesíteni tudja az objektumon lévő aláírást. A következő típusú igazolásokat csak az *OBJECTSIGNING igazolás tárolóban kezelheti.

Aláírás ellenőrző igazolások
Az aláírás ellenőrző igazolás az objektum aláíró igazolás egy példánya magánkulcs nélkül. Az aláírás ellenőrző igazolás nyilvános kulcsát használhatja az objektum aláíró igazolással létrehozott digitális aláírás hitelesítéséhez. Az aláírás ellenőrzése révén meghatározhatja az objektum eredetét, és ellenőrizheti, hogy nem változott-e az aláírás óta. A következő típusú igazolásokat csak a *SIGNATUREVERIFICATION igazolás tárolóban kezelheti.

Felhasználói igazolások
A felhasználói igazolás valójában egy digitális jogosítvány, ami ellenőrzi az igazolást tulajdonló kliens vagy felhasználó azonosságát. Számos alkalmazás nyújt ilyen támogatást, ami lehetővé teszi, hogy a felhasználónév és a jelszó használata helyett az igazolások segítségével hitelesítse a felhasználókat az erőforrások számára. A Digitális igazolás kezelő (DCM) automatikusan társítja a magán CA által kiadott felhasználói igazolásokat a felhasználó iSeries felhasználói profiljával. A DCM segítségével társíthatja a más Igazolási hatóságok által kiadott igazolásokat is a felhasználó iSeries felhasználói profiljával.

Amikor a Digitális igazolás kezelővel (DCM) kezeli az igazolásokat, a DCM osztályozás szerint rendszerezi és helyezi el őket, valamint a hozzájuk tartozó magánkulcsokat is az igazolás tárolóba.

Megjegyzés: Ha az iSeries szerverén telepítve van az IBM 4758 PCI Cryptographic Coprocessor termék, akkor választhat egyéb magánkulcs tároló opciókat is az igazolásaihoz (az objektum aláíró igazolások kivételével). Választhatja azt, hogy a magánkulcsot magába a ko-processzorba tárolja. A ko-processzor segítségével titkosíthatja a magánkulcsot, és az igazolás tároló helyett eltárolhatja egy speciális kulcsfájlba. A felhasználói igazolások és azok magánkulcsai azonban tárolhatók a felhasználó rendszerén is, a böngésző szoftverben vagy a többi kliens szoftver csomag által használt fájlban.

A nyilvános és a magán igazolások összevetése

Ha egyszer az igazolások használata mellett dönt, akkor ki kell választania az igazolás megvalósítás típusát, amely a legjobban megfelel biztonsági igényeinek. Az igazolások megszerzéséhez az alábbi lehetőségekből választhat:

- Az igazolásokat egy nyilvános Internet Igazolási hatóságtól (CA) szerzi be.
- Saját CA-t működtet, amely kiadja a magán igazolásokat a felhasználók és az alkalmazások részére.
- A nyilvános Internet és a saját CA-tól eredő igazolások kombinációját használja.

Az, hogy melyik megoldást választja több tényezőtől függ, de az egyik legfontosabb a környezet, amelyben az igazolásokat használja. Az alábbiakban igyekszünk segítséget nyújtani, hogy jobban meg tudja határozni, melyik megoldás a megfelelőbb üzleti és biztonsági igényeihez.

Nyilvános igazolások használata

A nyilvános Internet CA-k bárkinek kiadnak igazolásokat, akik megfizetik az árát. Mindazonáltal, az Internet CA bizonyos mértékig ellenőrzi az egyedet, mielőtt kiadná az igazolást. Az ellenőrzés szintje változó, valójában a CA azonosítási irányelveitől függ. Mielőtt elhatározza az igazolások beszerzését a CA-tól, illetve megbízhatónak ítélné a CA által kiadott igazolásokat, meg kell vizsgálnia, hogy a CA azonosítási irányelveinek szigora megfelel-e biztonsági igényeinek. Amint a Public Key Infrastructure for X.509 (PKIX) szabványok kifejlődtek, néhány új nyilvános CA sokkal szigorúbb azonosítási szabályokat alkalmaz az igazolások kiadásához. Ahogy az ilyen PKIX CA-tól eredő igazolások beszerzési folyamata szigorodik, a CA által kibocsátott igazolások is egyre jobban garantálják, hogy a felhasználók biztonságosan hozzáférnek az alkalmazásokhoz. A Digitális igazolás kezelő (DCM) lehetővé teszi a PKIX CA igazolások használatát és kezelését.

Figyelembe kell venni a költségeket is, amelyek a nyilvános CA-nál az igazolások kiadásával kapcsolatban merülnek fel. Ha csak korlátozott számú szerver vagy kliens alkalmazás és felhasználó számára kell igazolásokat kiadni, a költségek lehet, hogy nem lesznek fontos tényezők. Azonban a költségek különösen fontosak lehetnek, ha nagyszámú *magán* felhasználója van, akiknek nyilvános igazolások kellenek a kliens hitelesítéshez. Ebben az esetben, tekintetbe kell venni az adminisztrációs és a programozási erőfeszítéseket is, amelyek a szerver alkalmazások konfigurálásához kell, hogy azok csak a nyilvános CA által kiadott igazolásokat fogadják el.

Ha nyilvános CA-tól eredő igazolásokat akar használni, időt és energiát takaríthat meg, mivel számos szerver-, kliens- és felhasználói alkalmazás úgy van konfigurálva, hogy felismeri a

jólismert nyilvános CA-k többségét. Sőt, esetleg sokkal több cég és felhasználó ismeri fel és bízik meg a jólismert nyilvános CA igazolásokban, mint azokban, amelyeket a saját magán CA-ja ad ki.

Magán igazolások használata

Ha saját Helyi CA-t hoz létre, igazolásokat tud kiadni korlátozott hatókörben, például a vállalaton vagy a szervezeten belül. A saját CA létrehozása és karbantartása lehetővé teszi, hogy csak azoknak a felhasználóknak adjon ki igazolást, akik a csoport megbízható tagjai. Ez jobb biztonságot nyújt, mivel szigorúbban tudja irányítani, hogy ki kapjon igazolásokat, és ennek következtében ki nyerjen hozzáférést az erőforrásokhoz. A lehetséges hátránya az, hogy a Helyi CA karbantartása időt és energiát igényel, amit be kell fektetni. Mindazonáltal, a Digitális igazolás kezelő (DCM) megkönnyíti ezt a folyamatot.

Amikor Helyi CA adja ki az igazolásokat a felhasználóknak a kliens hitelesítéshez, el kell döntenie, hogy társítani akarja-e a felhasználók igazolásait az iSeries felhasználói profilokkal. Lehetnek olyan felhasználói, akik saját maguk szerzik be igazolásaikat a Helyi CA-tól DCM segítségével, ha igazolásaikat társítani akarja iSeries felhasználói profillal. A V5R2 változattól kezdődően használhat API-kat, hogy programozottan adja ki az igazolásokat a nem iSeries felhasználóknak mégpedig úgy, hogy ezeknek a felhasználóknak nem kell rendelkezniük iSeries felhasználói profillal ahhoz, hogy használni tudják a magán igazolásokat a kliens hitelesítéshez.

Megjegyzés: Mindegy melyik CA adja ki az igazolásokat, a rendszeradminisztrátor vezérli, hogy mely CA-kat tekintenek megbízhatónak a rendszeren lévő alkalmazások. Ha egy jólismert CA igazolásának egy példánya megtalálható a böngészőjében, akkor a böngészőben beállíthatók megbízhatónak az adott CA által kiadott szerver igazolások. Azonban. ha a CA igazolás nem a *SYSTEM igazolás tárolóban van, akkor a szerver nem tudja megbízhatónak elfogadni az adott CA által kiadott felhasználói vagy kliens igazolásokat. Ahhoz, hogy a CA által kiadott felhasználói igazolás megbízható legyen, meg kell kapni a CA igazolás egy példányát a CA-tól. Helyes fájlformátumban kell lenni, és hozzá kell adni az igazolást a DCM igazolás tárolóhoz.

Hasznosnak találhatja, ha átnéz néhány igazolás felhasználási forgatókönyvet, amelyek segítségével eldöntheti, hogy nyilvános vagy magán igazolások felelnek-e meg jobban üzleti és biztonsági igényeinek.

Kapcsolódó feladatok

Miután eldönti, hogyan akarja használni az igazolásokat, és milyen típust fog használni, nézze át az alábbi eljárásokat és tanulmányozza a Digitális igazolás kezelő használatát, hogy segítségükkel megvalósítsa tervét:

- Magán CA létrehozása és működése ismerteti azokat a feladatokat, amelyeket végre kell hajtani a CA működéséhez és a magán igazolások kiadásához.
- Nyilvános Internet CA-tól eredő igazolások kezelése ismerteti azokat a feladatokat, amelyeket végre kell hajtani a jólismert nyilvános CA-tól (beleértve a PKIX CA-kat is) származó igazolások használatához.
- Helyi CA használata más iSeries szervereken ismerteti azokat a feladatokat, amelyeket végre kell hajtani, ha a magán CA-tól eredő igazolásokat egynél több rendszeren kívánja használni.

Digitális igazolások SSL biztonságos kommunikációkhoz

A digitális igazolások segítségével Védett socket réteg (SSL) használatára konfigurálhatja az alkalmazásokat a biztonságos kommunikációs szekciók létesítése érdekében. Az SSL szekció létesítéséhez a szerver mindig rendelkezésre bocsátja igazolásának egy példányát, amelyet a kliens ellenőriz a kapcsolat által megkövetelt módon. Az SSL kapcsolat használata:

- Biztosítja a kliens vagy a végfelhasználó számára, hogy a saját helyszíne hiteles.
- Titkosított kommunikációs szekciót szolgáltat, ami garantálja, hogy az összeköttetésen áthaladó adatok magánjellegűek maradnak.

A szerver és a kliens alkalmazások együttműködnek az adatok biztonsága érdekében a következők szerint:

1. A szerver alkalmazás bemutatja az igazolást a kliens (felhasználói) alkalmazásnak, hogy az ellenőrizze a szerver azonosítását.
2. A kliens alkalmazás összeveti a szerver azonosítását az Igazolási hatóság által kiadott igazolás egy példányával. (A kliens alkalmazásnak hozzáféréssel kell rendelkeznie a tárgyhoz tartozó CA igazolásának helyileg tárolt példányához.)
3. A szerver és a kliens alkalmazások megegyeznek a szimmetrikus kulcsú titkosításban, és ezt használják a kommunikációs szekciók titkosításához.
4. Választhatóan, a szerver kérheti a klienstől az azonosítás ellenőrzését, mielőtt hozzáférést engedélyezne a kért erőforrásokhoz. Ahhoz, hogy az igazolásokkal ellenőrizhető legyen az azonosítás, a kommunikáló alkalmazásoknak támogatni kell az igazolások használatát a felhasználói hitelesítéshez.

Az SSL aszimmetrikus kulcs (nyilvános kulcs) algoritmust használ az SSL egyeztetési folyamat során, amikor is egyeztetés történik egy olyan szimmetrikus kulcsról, amely azután az alkalmazás adatainak titkosítására és visszafejtésére szolgál az adott SSL szekcióban. Ez azt jelenti, hogy a szerver és a kliens különböző szekció kulcsokat használnak, amelyek automatikusan lejárnak egy bizonyos idő után mindegyik kapcsolat esetén. Még egy valószínűtlen esemény kapcsán - amikor valaki elfog és visszafejt egy adott szekció kulcsot - sem lehet ezekből a szekció kulcsokból következtetni a jövőbeli kulcsokra.

Digitális igazolások felhasználói hitelesítéshez

Hagyományosan, a felhasználók felhasználónév és jelszó alapján kapnak hozzáférést az erőforrásokhoz az alkalmazástól vagy a rendszertől. A digitális igazolásokkal tovább növelheti a rendszer biztonságát (a felhasználó nevek és a jelszavak helyett), amivel hitelesítheti és felhatalmazhatja a számos szerver alkalmazás és a felhasználók közötti szekciókat. A Digitális igazolás kezelő (DCM) segítségével társíthatja a felhasználó igazolását az adott felhasználó iSeries felhasználói profiljával. Az igazolás azután ugyanazzal a jogosultságokkal és engedélyekkel fog rendelkezni, mint a hozzátartozó profil. A V5R2 változattól kezdve API-kat alkalmazhat, amelyek révén programozottan használhatja a saját Helyi igazolási hatóságot arra, hogy igazolásokat adjon ki nem iSeries felhasználók számára. Ezek az API-k lehetőséget adnak arra, hogy magán igazolásokat adjon ki a felhasználóknak, amikor nem akarja, hogy ezek a felhasználók iSeries felhasználói profillal rendelkezzenek.

A digitális igazolás elektronikus jogosítványként funkcionál, és azt ellenőrzi, hogy az őt előadó személy valóban az-e, akinek mutatja magát. Ilyen megközelítésben az igazolás útlevélhez hasonlítható. Az egyedi azonosítás valójában egy egyedi számot tartalmaz azonosítási célokból, valamint egy felismerhető kiadó hatóságot, amely ellenőrzi a jogosítvány hitelességét. Az igazolás esetében az Igazolási hatóság (CA) funkciója mint megbízható harmadik fél jelenik meg, amely kiadja az igazolást és ellenőrzi, hogy hiteles jogosítványnak tekinthető-e.

Az igazolások nyilvános kulcsokat és egy hozzátartozó magánkulcsot használnak hitelesítési célokból. A kiadó CA összerendeli ezeket a kulcsokat, valamint velük egyetemben további információkat az igazolás tulajdonosáról, hogy igazolni tudja magát azonosítási célokból.

Megnövekedett számú alkalmazás támogatja az igazolások használatát kliens hitelesítéshez az SSL szekció alatt. Pillanatnyilag az alábbi iSeries alkalmazások támogatják a kliens hitelesítést:

- Telnet szerver
- IBM HTTP Server (Apache eredetű és meghajtású)
- Directory Services (LDAP) szerver
- Kezelőközpont
- Client Access Express (beleértve az iSeries navigátort is)
- FTP szerver

Az idő haladtával újabb alkalmazások támogathatják a kliens hitelesítést, ezért olvassa el az adott alkalmazások dokumentációit, hogy eldönthesse, rendelkeznek-e ilyen támogatással.

Az igazolások szigorúbb felhasználói hitelesítést jelentenek több okból is:

- Előállhat az a lehetőség, hogy valaki elfelejti jelszavát. Éppen ezért, a felhasználóknak meg kell jegyezni vagy fel kell írni neveiket és jelszavaikat, hogy ne felejtsék el. Ennek eredményeképpen a jogosulatlan felhasználók könnyebben megszerezhetik a jogosult felhasználók neveit és jelszavait. Mivel az igazolásokat fájlban vagy más elektronikus helyen tárolja, a kliens alkalmazások (és nem a felhasználók) kezelik az igazolások elérését és bemutatását a hitelesítéshez. Ez garantálja, hogy a felhasználók valószínűleg sokkal kevésbé osztják meg igazolásaikat a jogosulatlan felhasználókkal, hacsak azok nem rendelkeznek hozzáféréssel a felhasználói rendszerhez. Az igazolásokat telepítheti intelligens (smart) kártyákra is, ami további védelmet jelent a jogosulatlan felhasználással szemben.
- Az igazolás tartalmaz egy magánkulcsot, amelyet sosem küld el az igazolással azonosítás céljából. Helyette a rendszer ezt használja a titkosítási és a visszafejtési folyamat alatt. Mások az igazoláshoz tartozó nyilvános kulcsot használhatják a magánkulccsal aláírt objektumok küldőjének ellenőrzésére.
- Sok rendszer kér jelszót, amelyek 8 karakteresek vagy rövidebb hosszúságúak, ami sebezhetőbbé teszi ezeket a jelszavakat a feltételezett támadásokkal szemben. Az igazolás titkosítási kulcsai több száz karakterből állnak. Ez a hossz a véletlenszerűséggel egyetemben garantálja, hogy a titkosítási kulcsokat sokkal nehezebb kitalálni, mint a jelszavakat.
- A digitális igazolások több olyan hasznosítási lehetőséggel bírnak, amit a jelszavak nem tudnak, mint például az adatok épsége és a titoktartás. Az igazolásokat és a hozzájuk tartozó kulcsokat a következőkre használhatja:
  - Garantálja az adatok épségét a változások észlelése útján.
  - Megvizsgálja, hogy egy művelet valóban megtörtént-e. Erre a ″nonrepudiation″ szakkifejezést használjuk.
  - Biztosítja az adatátvitel magánjellegét a Védett socket réteg (SSL) kapcsolattal, amely titkosítja a kommunikációs szekciókat.

Olvassa el az Alkalmazások biztonságossá tétele SSL segítségével című részt, ha többet akar megtudni az iSeries szerver alkalmazások konfigurálásáról, amikor igazolásokat használnak kliens hitelesítéshez az SSL szekció során.

Digitális igazolások VPN kapcsolatokhoz

A digitális igazolások segítségével létrehozhat iSeries virtuális magánhálózat (VPN) alapú összeköttetést. A dinamikus VPN összeköttetés mindkét végpontjának hitelesíteni kell a másikat, mielőtt aktívvá válna az összeköttetés. A végpont hitelesítést az Internet Key Exchange (IKE) szerver hajtja végre mindkét végponton. A sikeres hitelesítés után az IKE

szerverek egyeztetik a titkosítási metodikákat és algoritmusokat, amelyeket használni fognak a VPN kapcsolat biztonságossá tétele érdekében.

A V5R1 előtt az IKE szerverek csak előre megosztott kulcs segítségével tudták egymást hitelesíteni. Az előre megosztott kulcs kevésbé biztonságos, mivel ezt a kulcsot manuálisan kell a VPN másik végponján lévő adminisztrátorral közölni. Következésképpen, lehetőség nyílhat arra, hogy mások számára ismertté váljon a kulcs a közlési folyamat alatt.

A kockázat elkerülhető azzal, hogy digitális igazolások révén hitelesíti a végpontokat, és nem az előre megosztott kulcs használatával. Az IKE szerver hitelesítheti a többi szerver igazolását, hogy létrehozza az összeköttetést, egyeztesse a titkosítási metodikákat és algoritmusokat, amelyeket a szerverek fognak használni a kapcsolat biztonságossá tétele érdekében.

A Digital Certificate Manager (DCM) segítségével kezelheti az igazolásokat, amelyeket az IKE szerver használ fel dinamikus VPN kapcsolatok létesítéséhez. Először el kell dönteni, hogy nyilvános igazolásokat használ vagy magán igazolásokat ad ki az IKE szerver számára.

Egyes VPN megvalósítások azt igénylik, hogy az igazolás tartalmazzon másodlagos tárgynevet is, mint például egy tartománynév vagy egy e-mail cím, a szabványos megkülönböztető néven felül. Amikor a DCM segédprogram saját CA-t használ fel igazolás kiadására, megadhatja ezt a másodlagos nevet az igazoláshoz. A nevet megadva bizonyos lehet abban, hogy az iSeries VPN kapcsolat kompatíbilis más VPN megvalósításokkal, amelyek igényelhetik a nevet a hitelesítéshez.

Nézze át az alábbi forrásokat, ha többet kíván megtudni a VPN kapcsolatokhoz használt igazolások kezeléséről.

- Ha még sohasem használt DCM-et az igazolások kezeléséhez, az alábbi témakörök segítséget nyújtanak az első lépésekhez:
  - A Helyi, saját CA létrehozása és működtetése leírja, hogyan lehet a DCM segítségével magán igazolásokat kiadni az alkalmazásoknak.
  - A nyilvános Internet CA-tól eredő igazolások kezelése leírja, hogyan lehet a DCM segítségével kezelni a nyilvános CA által kiadott igazolásokat.
- Ha már a DCM segítségével kezeli az igazolásokat más alkalmazások számára, nézze át az alábbi forrásokat, ha többet kíván megtudni arról, hogyan adhatja meg az alkalmazásnak egy meglévő igazolás használatát, valamint mely igazolásokat fogadhatja el és hitelesítheti az alkalmazás:
  - Az igazolás hozzárendelése alkalmazáshoz leírja, hogyan lehet a DCM segítségével hozzárendelni egy meglévő igazolást az alkalmazáshoz, mint például az IKE szerverhez.
  - A megbízható CA lista megadása alkalmazáshoz leírja, hogyan lehet megadni azt, hogy melyik CA-kat tekinthet megbízhatónak az alkalmazás, amikor elfogadja az igazolásokat a kliens (vagy VPN) hitelesítéshez.

Digitális igazolások objektumok aláírásához

A V5R1 változat óta az OS/400 támogatja az igazolások használatát az objektumok digitális aláírásához. A digitálisan aláírt objektumok módot adnak arra, hogy ellenőrizze az objektum tartalmának sértetlenségét és eredetének forrását. Az objektum aláírási támogatás kibővíti a hagyományos iSeries rendszer 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, vagy amikor nem iSeries rendszeren tárolja az objektumot. A hagyományos vezérlések nem mindig tudják meghatározni, hogy történt-e jogosulatlan változtatás vagy manipulálás az objektummal. Az objektumokon lévő digitális aláírások garantáltan észlelik az aláírt objektumok változásait.

A digitális aláírás elhelyezése az objektumon a következőkből áll: az igazolás magánkulcsával az objektumban található adatok titkosított matematikai összegzésének hozzáadása az objektumhoz. Az aláírás védelmezi az adatokat a jogosulatlan változtatásoktól. 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.

Ha úgy dönt, hogy a digitális aláírás igénybe vétele megfelel biztonsági igényeinek és irányelveinek, akkor vizsgálja meg, hogy nyilvános vagy saját 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.

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). A Digitális igazolás kezelő (DCM) segítségével kezelheti az igazolásokat, amelyeket az objektumok aláírására vagy az objektumokon lévő aláírások ellenőrzésére használ. A DCM segítségével aláírhatja az objektumokat és ellenőrizheti az objektum aláírásokat.

Digitális igazolások objektum aláírások ellenőrzéséhez

A V5R1 változat óta az iSeries támogatja az igazolások használatát az objektumokon lévő digitális aláírások ellenőrzéséhez. Ha valaki bizonyos akar lenni, hogy az aláírt objektum nem változott a továbbítás alatt, és az objektum egy elfogadott, legitim forrásból ered, az aláíró igazolás nyilvános kulcsával ellenőrizheti 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. A digitális aláírások ellenőrzési folyamatának részeként el kell dönteni, hogy melyik Igazolási hatóságban hisz, és mely igazolásokban bízik meg az objektumok aláírásához. Amikor kiválaszt egy megbízható CA-t, azt is kiválaszthatja, hogy az igazolások megbízhatóak-e, amelyeket valaki a megbízható CA által kiadott igazolás segítségével hozott létre. Amikor nem megbízható CA-t választ, akkor vagy nem megbízható igazolásokat választ ki, amelyeket a CA kiad, vagy olyan aláírásokat, amelyeket valaki azokkal az adott igazolásokkal hozott létre.

Verify object restore (QVFYOBJRST) rendszerváltozó

Ha aláírás ellenőrzést kíván végrehajtani, akkor az első fontos eldöntendő kérdés az, hogy mennyire fontosak az aláírások a rendszeren visszaállítandó objektumok esetében. Ezt a QVFYOBJRST nevű rendszerváltozóval vezérelheti. 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 csak a visszaállítás alatt álló végrehajtható objektumokra van hatással, a mentési vagy az IFS fájlokra nem. A rendszerváltozókról többet megtudhat az Információs központ Rendszerváltozó kereső című részében.

A Digitális igazolás kezelő (DCM) segítségével megvalósíthatja az igazolást és a CA-val kapcsolatos döntéseit, valamint az objektum aláírások ellenőrzéséhez használt igazolások kezelését is. A DCM segítségével aláírhatja az objektumokat és ellenőrizheti az objektum aláírásokat.

Fejezet 7. A DCM konfigurálása

A Digitális igazolás kezelő (DCM) böngésző alapú felhasználói kezelőfelületet nyújt, melynek segítségével kezelheti a digitális igazolásokat az alkalmazások és a felhasználók számára. A felhasználói kezelőfelület két fő keretre oszlik: a navigációs és a feladat keretre.

A navigációs keret segítségével kiválaszthatja a feladatokat az igazolások vagy az alkalmazások kezeléséhez. Miközben néhány egyedi feladat közvetlenül a fő navigációs kereten jelenik meg, a legtöbb feladat kategóriákba csoportosítva a navigációs kereten található. Például az **Igazolások kezelése** egy feladat kategória, amely különféle egyedi feladatokat tartalmaz, mint például Igazolás megjelenítése, Igazolás megújítása, Igazolás importálása, és így tovább. Ha a navigációs kereten egy elem egynél több feladatot tartalmazó kategóriát jelöl, akkor tőle balra egy nyíl látható. A nyíl jelzi, hogy amikor kiválasztja a kategória hivatkozást, a feladatok bővített listája jelenik meg, ahol választhat, hogy melyik feladatot hajtja végre.

A **Gyors útvonal** kategória kivételével, az összes feladat a navigációs kereten úgynevezett irányított feladat, ami végigvezeti a felhasználót az adott feladat gyors és könnyű végrehajtásához szükséges lépések sorozatán. A Gyors útvonal kategória az igazolás és alkalmazás kezelési funkciók egy fürtjét adja, ami lehetővé teszi a gyakorlott DCM felhasználóknak a kapcsolódó feladatok választékának gyors elérését a központi lapról.

Az igazolás tárolótól (amelyben dolgozik) függ az, hogy milyen feladatok állnak rendelkezésre a navigációs kereten. A navigációs kereten látható kategóriák és a feladatok száma erősen függ azoktól a jogosultságoktól, amelyekkel az iSeries felhasználói profil rendelkezik. Csak az iSeries biztonsági felelőse vagy adminisztrátora tudja elérni a CA működtetéséhez, az alkalmazások által használt igazolások kezeléséhez, és az egyéb rendszerszintű műveletekhez tartozó összes feladatot. A biztonsági felelősnek vagy az adminisztrátornak *SECADM és *ALLOBJ különleges jogosultságokkal kell rendelkezni a feladatok megtekintéséhez és elvégzéséhez. Az ilyen különleges jogosultsággal nem rendelkező felhasználók csak a felhasználó igazolási funkciókat érhetik el.

Az alábbi témakörök révén tanulmányozhatja DCM konfigurálását, és az igazolások kezelésének elkezdését.

A DCM indítása
Megismerheti, hogyan érheti el a Digitális igazolás kezelő (Digital Certificate Manager) programot az iSeries rendszeren.

Igazolások beállítása első alkalommal
Tanulmányozhatja, hogyan kell elkezdeni a DCM használatát, és elvégezni az összes beállítást az igazolások használásához első alkalommal. Megismerheti, hogyan kell elkezdeni a nyilvános Internet Igazolási hatóságtól (CA) kapott igazolások kezelését, valamint hogyan kell létrehozni és működtetni saját helyi CA-t igazolások kiadása céljából.

A VeriSign webhely kitűnő forrás, ha még több oktatási anyaghoz szeretne jutni a digitális igazolások használatáról Internet környezetben, hogy tovább javítsa a rendszer és a hálózat biztonságát. A VeriSign webhely terjedelmes könyvtárral rendelkezik a digitális igazolások témaköréből, valamint számos egyéb Internet biztonsággal kapcsolatos tárgykörből. A könyvtárat itt érheti el: VeriSign Help Desk  .

A Digitális igazolás kezelő indítása

Mielőtt bármelyik funkcióját is használhatná, indítsa el a Digitális igazolás kezelőt (DCM). Hajtsa végre az alábbi feladatokat, hogy sikeresen el tudja indítani a DCM-et:

1. Telepítse az 5722 SS1 34-es opcióját. Ez a Digitális igazolás kezelő (Digital Certificate Manager).

   Telepítse az 5722 DG1 opciót. Ez az IBM HTTP Server for iSeries termék.

   Telepítse az 5722 AC3 opciót. Ez egy titkosítási termék, amely révén a V5R2 DCM nyilvános-magán kulcspárokat generál az igazolásokhoz az exportált igazolás fájlok titkosításához, valamint az importált igazolás fájlok visszafejtéséhez.
2. Az iSeries navigátorral indítsa el a HTTP Server *ADMIN példányát:
   a. Indítsa el az **iSeries navigátort**.
   b. Kattintson duplán az iSeries szerverre a fa nézetben.
   c. Kattintson duplán a **Hálózatra**.
   d. Kattintson duplán a **Szerverekre**.
   e. Kattintson duplán a **TCP/IP** elemre.
   f. Kattintson a jobb egérgombbal a **HTTP adminisztrálásra**.
   g. Kattintson a **Start** gombra.
3. Indítsa el a web böngészőt.
4. A böngésző segítségével menjen a rendszerén lévő iSeries Feladatlapra a http://*saját_rendszer_neve*:2001 címen.
5. Válassza ki a **Digitális igazolás kezelőt** az iSeries Feladatlapon található terméklistából a DCM funkció elérése érdekében.

Ha a DCM egy korábbi változatáról tér át, az oldal részletes tájékoztatással szolgál a rendszer frissítéséről.

Igazolások beállítása első alkalommal

A Digitális igazolás kezelő (DCM) baloldali kerete a navigációs keret. A keret segítségével a feladatok széles választékát használhatja fel az igazolások és az alkalmazások kezelésére, amelyek használják őket. A rendelkezésre álló feladatok attól függnek, hogy milyen igazolás tárolót (ha van) nyitott meg, és milyen felhasználói profil jogosultságai vannak. A feladatok többsége csak akkor elérhető, ha *ALLOBJ és *SECADM különleges jogosultsága van.

Amikor a Digitális igazolás kezelőt (DCM) első alkalommal használja, még nincs igazolás tároló (hacsak nem tért át a DCM előző változatáról). Következésképpen, a navigációs keret csak az alábbi feladatokat jeleníti meg, ha rendelkezik a szükséges jogosultságokkal:

- Felhasználói igazolások kezelése
- Új igazolási tároló létrehozása
- Igazolási hatóság (CA) létrehozása. (Megjegyzés: Miután a feladatot végrehajtotta egy magán CA létrehozásához, a feladat eltűnik a listából.)
- CRL helyek kezelése
- PKIX kérés hely kezelése

Ha már vannak is igazolás tárolók a rendszeren (például a DCM egy korábbi változatáról tér át), a DCM csak korlátozott számú feladatot vagy feladat kategóriát jelenít meg a baloldali navigációs kereten. Először a megfelelő igazolás tárolót kell elérni, mielőtt elkezdene dolgozni az igazolások és az alkalmazáskezelési feladatok többségével. Az adott igazolás tároló megnyitásához kattintson a navigációs kereten az **Igazolás tároló választása** elemre.

A DCM navigációs keretén találhatja a **Védett kapcsolat** gombot. A gomb segítségével előugrik egy másik böngésző ablak, amely biztonságos kapcsolatot kezdeményez a Védett socket réteg (SSL) protokoll felhasználásával. A funkció sikeres használatához először

konfigurálja az IBM HTTP Server for iSeries terméket SSL használatra, hogy biztonságos üzemmódban dolgozzon. Azután indítsa el a HTTP szervert biztonságos üzemmódban. Ha nem konfigurálta, és nem indította el a HTTP Server for SSL működését, hibaüzenetet fog látni, és a böngésző nem indítja el a biztonságos szekciót.

Első lépések

Annak ellenére, hogy igazolásokat kíván használni számos, biztonsággal kapcsolatos céllal összhangban, az első teendő attól függ, hogyan kívánja beszerezni az igazolásokat. Két elsődleges útja van annak, ahogy beszerezheti őket, amikor első alkalommal használja a DCM-et. Ez azon alapul, hogy szándékozik-e használni a nyilvános igazolásokat szemben a magán igazolások kiadásával:

Helyi CA létrehozása és működtetése révén igazolásokat bocsát ki az alkalmazások számára.

Igazolások kezelése nyilvános Internet CA segítségével az alkalmazások általi használatról szól.

Helyi CA létrehozása és működtetése

Miután gondosan átnézte biztonsági igényeit és irányelveit, úgy döntött, hogy Helyi igazolási hatóságot (CA) működtet, amely a magán igazolások kiadását végzi az alkalmazások számára. A Digitális igazolás kezelő (DCM) segítségével létrehozhatja és működtetheti a saját Helyi CA hatóságot. A DCM végigvezeti azon a feladatsoron, amely a CA létrehozásának folyamatát, valamint az alkalmazások számára igazolások kiadását eredményezi. A vezetett feladatsor garantálja, hogy minden olyannal rendelkezzen, ami a digitális igazolások használatának elkezdéséhez kell, s ezáltal az alkalmazások megfelelő konfigurálásával felhasználhatja SSL kapcsolatokhoz, objektumok aláírásához, valamint objektum aláírások ellenőrzéséhez.

Megjegyzés: A DCM használata előtt hozza létre és konfigurálja a webszervert, ha az igazolásokat IBM HTTP Server for iSeries termékkel kívánja használni. Amikor webszervert konfigurál SSL használattal, egy alkalmazás ID generálódik a szerver számára. Feltétlenül meg kell jegyezni ezt az alkalmazás ID-t, hogy a DCM segítségével meg tudja adni, melyik igazolást kell ennek az alkalmazásnak használni az SSL kapcsolathoz.

Ne állítsa le és ne indítsa újra a szervert addig, amíg a DCM segítségével a szerverhez hozzá nem rendeli az igazolást. Ha leállítja vagy újraindítja az *ADMIN webszerver példányt, mielőtt hozzárendelné az igazolást, a szerver nem fog elindulni és nem lesz képes hozzárendelni az igazolást a szerverhez a DCM segítségével.

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

1. DCM indítása.
2. A DCM navigációs keretén válassza ki az **Igazolási hatóság (CA) létrehozását** az űrlapok megjelenítéséhez. Ezek az űrlapok végigvezetik a Helyi CA létrehozásának folyamatán, valamint az SSL, objektum aláírás és aláírás ellenőrzés céljára használt digitális igazolások használatának elkezdéséhez szükséges egyéb feladatok végrehajtásán.

   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. Az űrlapok segítségével elvégezheti a működő Helyi igazolási hatóság (CA) beállításához szükséges összes feladatot:
   a. Válassza ki, hogyan tárolja a Helyi CA igazolás magánkulcsát. (Ez a lépés csak akkor jön elő, ha telepített IBM 4758–023 PCI Cryptographic Coprocessor kártyával rendelkezik az iSeries szerveren. Ha a rendszer nem rendelkezik titkosító

ko-processzorral, a DCM automatikusan a Helyi igazolási hatóság (CA) igazolás tárolójába helyezi el az igazolást és annak magánkulcsát.)

b. Adja meg a Helyi CA azonosítási információit.
c. Telepítse a Helyi CA igazolást a PC-jén vagy a böngészőjében, hogy a szoftver felismerhesse a Helyi CA-t és ellenőrizhesse a CA által kiadott igazolásokat.
d. Válassza ki a Helyi CA stratégiai adatait.
e. Az új Helyi CA segítségével adja ki a szerver vagy a kliens igazolást, amelyet alkalmazásai az SSL kapcsolatokhoz használhatnak. (Ha az iSeries rendelkezik telepített IBM 4758–023 PCI Cryptographic Coprocessor kártyával, akkor ennél a lépésnél kiválaszthatja, hogyan tárolja a szerver vagy a kliens igazolás magánkulcsát. Ha a rendszer nem rendelkezik ko-processzorral, a DCM automatikusan a *SYSTEM igazolás tárolóba helyezi el az igazolást és annak magánkulcsát. A DCM az alfeladat részeként létrehozza a *SYSTEM igazolás tárolót.)
f. Válassza ki azokat az alkalmazásokat, amelyek használhatják a szerver vagy a kliens igazolást az SSL kapcsolatokhoz.

   Megjegyzés: Ha a DCM segítségével előzőleg már létrehozta a *SYSTEM igazolás tárolót nyilvános Internet CA-tól eredő, SSL kapcsolatokhoz használt igazolások kezelése céljából, akkor nem kell ezt vagy az előző lépést végrehajtani.
g. 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.
h. Válassza ki azokat az alkalmazásokat, amelyek használhatják az objektum aláíró igazolást, hogy elhelyezhessék a digitális aláírásokat az objektumokon.

   Megjegyzés: Ha a DCM segítségével előzőleg már létrehozta az *OBJECTSIGNING igazolás tárolót nyilvános Internet CA-tól eredő, objektum aláíró igazolások kezelése céljából, akkor nem kell ezt vagy az előző lépést végrehajtani.
i. Válassza ki az alkalmazásokat, amelyek megbízhatónak tekintik a Helyi CA-t.

Amikor befejezi a feladatot, minden rendelkezésére áll ahhoz, hogy elkezdje az alkalmazások konfigurálását SSL használatához a biztonságos kommunikáció céljából.

Miután konfigurálja az alkalmazásokat, a felhasználók, akik SSL kapcsolaton keresztül érik el az alkalmazásokat, csak a DCM segítségével szerezhetik be a helyi CA igazolás egy példányát. Minden felhasználónak rendelkezni kell az igazolás egy példányával, hogy a felhasználó kliens szoftvere hitelesíteni tudja a szerver azonosságát az SSL egyeztetés folyamatában. A felhasználók a DCM segítségével fájlba másolhatják a Helyi CA igazolást, vagy letölthetik böngészőikbe. A kliens szoftvertől (amit a felhasználók az alkalmazás elérésére szolgáló SSL kapcsolat létesítéséhez használnak) függ az, hogy a felhasználók hogyan tárolják a Helyi CA igazolást.

A Helyi CA segítségével kiadhat igazolásokat a hálózat más iSeries rendszerein található alkalmazásoknak is.

Nézze át az alábbi témaköröket, ha többet kíván megtudni arról, hogyan lehet kezelni a felhasználói igazolásokat a DCM segítségével, hogyan szerezhetik be a felhasználók a Helyi CA igazolás egy példányát, hogy hitelesíteni tudják a CA által kiadott igazolásokat:

Felhasználói igazolások kezelése
Tanulmányozhatja, hogy a felhasználók hogyan szerezhetik be az igazolásokat a DCM segítségével, illetve hogyan társíthatják a meglévő igazolásokat iSeries felhasználói profiljaikkal.

API segítségével igazolások programozott kiadása nem iSeries felhasználóknak
Tanulmányozhatja, hogy a Helyi CA segítségével hogyan adhat ki magán igazolásokat a felhasználóknak anélkül, hogy az igazolás társítva lenne iSeries felhasználói profillal.

A magán CA igazolás egy példányának megszerzése
Tanulmányozhatja, hogyan szerezheti be a magán CA igazolás egy példányát, és hogyan telepítheti azt a saját PC-jén, hogy hitelesíteni tudja a CA által kiadott szerver igazolásokat.

Felhasználói igazolások kezelése

A felhasználók a Digitális igazolás kezelő (DCM) segítségével kezelhetik a számukra szükséges igazolásokat, amelyeket felhasználva részt vehetnek a Védett socket réteg (SSL) szekciókban.

Ha a felhasználók SSL kapcsolaton keresztül érik el a nyilvános vagy a belső szervereket, rendelkezniük kell annak az Igazolási hatóság (CA) igazolásának egy példányával, amely kiadta a szerver igazolását is. Rendelkezniük kell CA igazolással, hogy kliens szoftvereik ellenőrizni tudják a szerver igazolás hitelességét a kapcsolat létesítése céljából. Ha a szerver egy nyilvános CA igazolását használja, akkor a felhasználói szoftvernek már rendelkeznie kell a CA igazolás egy példányával. Következésképpen, sem a DCM adminisztrátornak, sem a felhasználóknak nem kell semmit sem tenni ahhoz, hogy egy SSL szekció résztvevői legyenek. Mindazonáltal, ha a szerver egy helyi CA igazolását használja, akkor a felhasználóknak meg kell szerezniük a helyi CA igazolás egy példányát, mielőtt bármilyen SSL szekciót létesíthetnének a szerverrel.

Ezen túlmenően, ha a szerver alkalmazás támogatja és megköveteli a kliens hitelesítést az igazolások segítségével, akkor a felhasználóknak rendelkezniük kell egy elfogadható felhasználói igazolással ahhoz, hogy elérést kapjanak a szerver által nyújtott erőforrásokhoz. A biztonsági igényektől függően a felhasználók felmutathatnak egy nyilvános Internet CA-tól kapott igazolást, vagy esetleg a helyi CA által kiadott igazolást is. Ha a szerver alkalmazás hozzáférést biztosít az erőforrásokhoz azoknak a belső felhasználóknak, akiknek pillanatnyilag van iSeries felhasználói profilja, akkor a DCM segítségével hozzárendelheti igazolásaikat felhasználói profiljaikhoz. Ez a társítás garantálja, hogy a felhasználók ugyanazzal a hozzáférésekkel és korlátozásokkal rendelkeznek az erőforrásokhoz, amikor az igazolásokat bemutatva, a felhasználói profil elfogadja vagy visszautasítja.

A Digitális igazolás kezelő (DCM) lehetővé teszi az iSeries felhasználói profilhoz tartozó igazolások kezelését. Ha van *SECADM és *ALLOBJ különleges jogosultsággal bíró felhasználói profilja, kezelheti a felhasználói profilok igazolás hozzárendeléseit saját maga és mások számára. Amikor nincs megnyitva igazolás tároló, vagy amikor a helyi Igazolási hatóság (CA) igazolás tárolója van nyitva, válassza a **Felhasználói igazolások kezelését** a navigációs kereten a megfelelő feladatok elérése céljából. Ha egy eltérő igazolás tároló van nyitva, akkor a felhasználói igazolásra vonatkozó feladatok beépülnek az **Igazolások kezelése** alatt lévő feladatok közé.

*SECADM és *ALLOBJ különleges jogosultság nélküli felhasználói profillal rendelkező felhasználók csak saját igazolás hozzárendeléseiket tudják kezelni. Ők válasszák ki a **Felhasználói igazolások kezelését**. Ezáltal elérik azokat a feladatokat, amelyek lehetővé teszik a felhasználói profilokhoz társított igazolások megtekintését, az igazolások eltávolítását a felhasználói profilokból, vagy egy másik CA igazolásának hozzárendelését saját felhasználói profiljaikhoz. A felhasználói profilokra vonatkozó különleges jogosultságoktól függetlenül, a felhasználók beszerezhetnek felhasználói igazolást a helyi CA-tól, ha az **Igazolás létrehozása** feladatot választják ki a fő navigációs kereten.

Az alábbi témakörök nyújtanak tájékoztatást a DCM használatáról, a felhasználói igazolások létrehozásáról és kezeléséről:

Felhasználói igazolás létrehozása
Az itt leírtak alapján tanulmányozhatja, hogy a felhasználók hogyan használhatják a helyi CA-t igazolás kiadására, kliens hitelesítés céljából.

Felhasználói igazolás hozzárendelése
Az itt leírtak alapján tanulmányozhatja a birtokában lévő igazolás társítását felhasználói profiljával. Az igazolás származhat egy másik rendszer helyi CA hatóságától, vagy egy jólismert Internet CA hatóságtól. Mielőtt hozzárendelné az igazolást a felhasználói profilhoz, a kibocsátó CA-t ismernie kell a szervernek megbízható CA-ként, és az igazolás nem lehet még összetársítva egyetlen felhasználói profillal sem a rendszeren.

Felhasználói igazolás létrehozása: Ha digitális igazolásokat kíván használni a felhasználó hitelesítéshez, akkor a felhasználóknak rendelkezniük kell igazolásokkal. Ha a Digitális igazolás kezelő (DCM) segítségével helyi Igazolási hatóságot (CA) működtet, akkor felhasználhatja ezt a helyi CA-t az igazolások kiadására az egyes felhasználók számára. Minden egyes felhasználónak el kell érni a DCM-et, hogy beszerezze az igazolást az **Igazolás létrehozása** feladat elvégzésével. Ahhoz, hogy a helyi CA-tól be lehessen szerezni az igazolást, a CA előírásainak meg kell engedni, hogy a CA kiadhasson felhasználói igazolásokat.

Az alábbi lépéseket hajtsa végre ahhoz, hogy az igazolást beszerezze a helyi CA-tól:
1. DCM indítása.
2. A navigációs kereten válassza ki az **Igazolás létrehozását**.
3. Válassza ki a **Felhasználói igazolást** a létrehozandó igazolás típusának. Megjelenik egy űrlap, amelyen megadhatja az azonosítási információkat az igazolás számára.
4. Töltse ki az űrlapot, és kattintson a **Folytatásra**.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
5. Ezen a ponton a DCM a böngészővel dolgozik együtt, hogy létrehozza a magán és a nyilvános kulcsot az igazolás számára. A böngésző megjeleníthet egy olyan ablakot, amely végigvezeti ezen a folyamaton. Kövesse a böngésző feladatokra vonatkozó utasításait. Miután a böngésző előállítja a kulcsokat, egy megerősítés lap jelenik meg, amely azt jelzi, hogy a DCM létrehozta az igazolást.
6. Telepítse az új igazolást a böngésző szoftverbe. A böngésző megjeleníthet egy olyan ablakot, amely végigvezeti ezen a folyamaton. Kövesse a feladat elvégzéséhez adott böngésző utasításokat.
7. Kattintson az **OK** gombra a feladat befejezéséhez.

A feldolgozás közben a Digitális igazolás kezelő automatikusan társítja az igazolást az iSeries felhasználói profillal.

Ha egy másik CA-tól akar igazolást a kliens hitelesítéshez, hogy ugyanolyan jogosultságokkal rendelkezzenek, mint a felhasználói profiljaik, a felhasználó a DCM segítségével hozzárendelheti az igazolásokat felhasználói profiljaikhoz.

Felhasználói igazolás hozzárendelése: Ha digitális igazolásokat kíván használni a felhasználó hitelesítéshez, akkor a felhasználóknak rendelkezniük kell igazolásokkal. Ha a felhasználók nyilvános Internet Igazolási hatóságtól (CA) eredő igazolásokkal rendelkeznek, akkor a Digitális igazolás kezelő (DCM) segítségével hozzárendelheti ezeket az igazolásokat a felhasználói profilokhoz. Ez lehetővé teszi a felhasználóknak, hogy az ilyen igazolásaikat a DCM programmal kezeljék.

A **Felhasználói igazolás hozzárendelése** feladat használatához a felhasználónak biztonságos szekciót kell létesítenie ahhoz a HTTP szerverhez, amelyiken keresztül eléri a Digitális igazolás kezelőt (DCM). A szekció biztonságos voltát a DCM eléréséhez használt URL

címben lévő portszám határozza meg. Ha a 2001-es portot használta, amely az alapértelmezett érték a DCM eléréséhez, akkor nem biztonságos a szekció. A HTTP szervert is konfigurálni kell az SSL használatára, mielőtt biztonságos szekcióra váltana.

Amikor ezt a feladatot választja ki, egy új böngésző ablak jelenik meg. Ha a szekciója nem biztonságos, a DCM kéri, hogy kattintson a **Felhasználói igazolás hozzárendelése** feladatra, hogy egyet elindítson. A DCM utána kezdeményezi a Védett socket réteg (SSL) egyeztetését a böngészővel.

Az egyeztetések részeként a böngésző esetleg rákérdezhet arra, hogy megbízható-e az Igazolási hatóság (CA), amely kiadta a HTTP szervert azonosító igazolást. Ezenkívül arra is rákérdezhet, hogy elfogadja-e magát a szerver igazolását.

Miután megengedi a böngészőnek, hogy megbízhatónak vegye a CA-t és elfogadhatja a szerver igazolását, a szerver kérhet igazolást a kliens hitelesítéshez. A böngésző konfigurációs beállításától függően, a böngésző kérheti az igazolás kiválasztását hitelesítés céljára. Ha a böngészőnek van igazolása olyan CA-tól, amelyet a rendszer elfogad megbízhatónak, akkor a DCM egy külön ablakban megjeleníti az igazolás információit. Ha nincs ilyen elfogadható igazolás, akkor a szerver kérheti, hogy helyette adja meg a felhasználónevet és a jelszót hitelesítés céljából.

Mihelyt létrehozta a biztonságos szekciót, a DCM megpróbálja előhozni a megfelelő igazolást a böngészőből, és így már társíthatja azt a felhasználói profillal. Ha a DCM sikeresen beolvas egy vagy több igazolást, megtekintheti az igazolások információit, és kiválaszthatja, hogy melyiket társítja a felhasználói profillal.

Ha a DCM nem jelenít meg igazolást, akkor a felhasználó nem tudott olyan igazolást biztosítani, amelyet a DCM társítani tudna a felhasználói profiljával. Lehet, hogy a felhasználói igazolásokkal kapcsolatos problémák egyike a felelős. Például, a böngésző által tartalmazott igazolások már társítva vannak a felhasználói profillal.

Ha jobban szeretné, hogy a helyi CA adja ki az igazolásokat a felhasználóknak, akkor a felhasználóknak kell a felhasználói igazolásokat létrehozni.

API segítségével igazolások programozott kiadása nem iSeries felhasználóknak

A V5R2 változattól kezdve két új API áll rendelkezésre, melyek segítségével programozottan adhat ki igazolásokat nem iSeries felhasználóknak. A korábbi változatokban, amikor a Helyi igazolási hatóság (CA) segítségével adott ki igazolásokat a felhasználóknak, a rendszer automatikusan társította az igazolásokat iSeries felhasználói profiljaikkal. Következésképpen, ahhoz, hogy a Helyi CA kiadjon egy igazolást a felhasználónak kliens hitelesítéshez, olyan felhasználót kell választani, akinek van iSeries felhasználói profilja. Amikor a felhasználók igazolást szereznek be a Helyi CA-tól kliens hitelesítéshez, minden felhasználó a Digitális igazolás kezelő (DCM) segítségével tudja létrehozni a szükséges igazolásokat. Ennek következtében, minden felhasználónak rendelkeznie kell felhasználói profillal azon az iSeries szerveren, amelyen a DCM van, valamint érvényes bejelentkezéssel is az adott iSeries szerveren.

A felhasználói profil és az igazolás társításának számos előnye van, különösen amikor belső felhasználókat vesz figyelembe. Mindazonáltal, ezek a korlátozások és követelmények csökkentik a Helyi CA használatának praktikusságát, amikor nagyszámú felhasználónak kell kiadni felhasználói igazolásokat, és különösen akkor, ha nem akarja, hogy az adott felhasználóknak legyen iSeries felhasználói profilja. Ha nem akar felhasználói profilt adni ezeknek a felhasználóknak, kérje meg őket, hogy vegyenek igazolást egy jólismert CA-tól. Erre szükség van, ha igazolások révén akarja hitelesíteni a felhasználókat az alkalmazások számára.

Az új API-k kezelőfelületet nyújtanak ahhoz, hogy Helyi CA igazolás által aláírt felhasználói igazolásokat hozhasson létre tetszőleges felhasználói névhez. Az ilyen igazolás nem tartozik felhasználói profilhoz. A felhasználónak nem szükséges a DCM-et üzemeltető iSeries szerver felhasználójának lenni, és a DCM-re sincs szüksége az igazolás létrehozásához.

Két API van, egy-egy az uralkodó böngésző program számára, amelyet elindít, amikor a Net.Data segítségével létrehoz programot az igazolások kiadásához. A létrehozott alkalmazásnak grafikus felhasználói kezelőfelületetű (GUI) programot kell biztosítani a felhasználói igazolás létrehozásához, valamint a megfelelő API hívásához, amely a Helyi CA segítségével aláírja az igazolást.

Az API-k használatáról további tájékoztatást talál az alábbi lapokon:
- Generate and Sign User Certificate Request (QYCUGSUC) API.
- Sign User Certificate Request (QYCUSUC) API.

A magán CA igazolás egy példányának megszerzése

Amikor Védett socket réteg (SSL) kapcsolatot használó szerverhez kap hozzáférést, a szerver egy igazolást mutat fel a kliens szoftvernek az azonosság ellenőrzése céljából. A kliens szoftvernek ellenőriznie kell a szerver igazolását, mielőtt a szerver létrehozhatná a szekciót. Ahhoz, hogy a kliens szoftver ellenőrizni tudja a szerver igazolását, rendelkeznie kell a szerver igazolását kiadó Igazolási hatóságra (CA) vonatkozó igazolás egy, helyben tárolt példányával. Ha a szerver egy nyilvános Internet CA igazolását használja, akkor a böngészőnek vagy más egyéb kliens szoftvernek már rendelkeznie kell a CA igazolás egy példányával. Ha azonban a szerver egy magán CA által kibocsátott igazolást mutat fel, akkor be kell szerezni a CA igazolás egy példányát a Digitális igazolás kezelő (DCM) segítségével.

A DCM segítségével letöltheti a helyi CA igazolást közvetlenül a böngészőjébe, vagy egy fájlba másolhatja olyan módon, hogy a többi kliens szoftver elérhesse és használhassa azt. Ha böngészőt és más alkalmazásokat is használ a biztonságos kommunikációhoz, esetleg mindkét módszert használni kell a helyi CA igazolás telepítéséhez. Ha mindkét módszert használja, akkor először a böngészőbe telepítse az igazolást, csak azután másolja és illessze egy fájlba.

Ha a szerver alkalmazás megköveteli, hogy hitelesítse magát a helyi CA által kiadott igazolás bemutatásával, töltse le a helyi CA igazolást a böngészőbe, mielőtt kéri a felhasználói hitelesítést a helyi CA-tól.

Hajtsa végre az alábbi lépéseket ahhoz, hogy a DCM beszerezze a helyi CA igazolás egy példányát:
1. DCM indítása.
2. A navigációs kereten válassza ki a **Helyi CA igazolás telepítése saját PC-re** feladatot, amely révén megjelenik egy lap, ahol letöltheti a helyi CA igazolást a böngészőjébe, vagy letárolhatja egy fájlba a rendszeren.
3. Válassza ki a helyi CA igazolás megszerzésének módszerét.
   a. Válassza az **Igazolás telepítését**, hogy megbízható gyökérként letöltse a helyi CA igazolást a böngészőjébe. Ez garantálja azt, hogy a böngésző biztonságos kommunikációs szekciókat létesíthet azokkal a szerverekkel, amelyek ugyancsak az adott CA igazolását használják. A böngésző program ablakok sorát jeleníti meg, amelyek segítik a telepítés végrehajtását.
   b. Válassza az **Igazolás másolása és beillesztése** feladatot, hogy megjelenjen az a lap, amely tartalmazza a helyi CA igazolás speciálisan kódolt példányát. A lapon látható szöveges objektumot másolja a vágólapra. Később ezt az információt egy fájlba fogja beilleszteni. Ezt a fájlt a PC segédprogramja (mint például MKKF vagy IKEYMAN) használja, hogy tárolja a kliens programok által használt igazolásokat a PC-n. Mielőtt a kliens alkalmazások felismerhetnék és használhatnák a helyi CA igazolást

hitelesítéshez, konfigurálni kell az alkalmazásokat, hogy megbízható gyökérként felismerjék az igazolást. Kövesse az utasításokat, hogy az alkalmazások alkalmasak legyenek a fájl használatára.

4. Kattintson az **OK** gombra, hogy visszatérjen a Digitális igazolás kezelő honlapjára.

Nyilvános Internet CA igazolások kezelése

Miután gondosan átnézte biztonsági igényeit és irányelveit, úgy döntött, hogy nyilvános Internetes Igazolási hatóságtól (CA) - mint például VeriSign - származó igazolásokat kíván használni. Például, nyilvános webhelyet működtet, és Védett socket réteg (SSL) protokollal biztonságos kommunikációs szekciót kíván létrehozni, hogy bizonyos tranzakciók magánjellegét megőrizze. Mivel a webhely rendelkezésre áll az általános nyilvánosság számára, olyan igazolásokat akar használni, hogy a legtöbb web böngésző gyorsan felismerje.

Vagy például, alkalmazásokat fejleszt külső ügyfelek számára, és nyilvános igazolásokat akar felhasználni az alkalmazási csomagok digitális aláírásához. Az alkalmazási csomagok aláírása révén az ügyfelek bizonyosak lehetnek abban, hogy a csomag a vállalatától érkezett, és a továbbítás alatt jogosulatlan fél nem változtatta meg a programot. Nyilvános igazolást kíván használni, hogy az ügyfelek könnyen és olcsón ellenőrizhessék a csomagon lévő digitális aláírást. Az igazolással ellenőrizheti is az aláírást, mielőtt kiküldi a csomagot az ügyfeleknek.

Az ilyen nyilvános igazolásokat és alkalmazásokat központilag kezelheti a Digitális igazolás kezelő (DCM) irányított feladatsoraival. Felhasználhatja őket SSL kapcsolatok létesítéséhez, objektumok aláírásához, illetve az objektumokon lévő digitális aláírások ellenőrzéséhez.

Nyilvános igazolások kezelése

Amikor a DCM segítségével kezeli a nyilvános Internet CA igazolásokat, először létre kell hozni az igazolás tárolót. Az igazolás tároló egy speciális kulcs adatbázis fájl, amelyet a DCM használ a digitális igazolások és a hozzájuk tartozó magánkulcsok tárolására. A DCM lehetővé teszi az igazolás tárolók több típusának (amelyet a bennük tárolt igazolások típusa határoz meg) létrehozását és kezelését.

Az igazolás tároló (amelyet létrehoz) típusa, az igazolások kezeléséhez szükséges további lépések, valamint az őket használó alkalmazások attól függnek, hogyan tervezi meg az igazolások használatát. Olvassa át az alábbi témaköröket, ha kíváncsi arra, hogyan hozza létre a DCM a megfelelő igazolás tárolót, hogyan kezeli az alkalmazásokhoz használt nyilvános Internet igazolásokat:

- Nyilvános Internet igazolások kezelése SSL kommunikációs szekciókhoz.
- Nyilvános Internet igazolások kezelése objektumok aláírásához.
- Internet igazolások kezelése objektum aláírások ellenőrzéséhez.

A DCM lehetővé teszi a Public Key Infrastructure for X.509 (PKIX) Igazolási hatóságtól beszerzett igazolások kezelését.

Nyilvános Internet igazolások kezelése SSL kommunikációs szekciókhoz

A Digitális igazolás kezelő (DCM) segítségével kezelheti az alkalmazásokhoz használt nyilvános Internet igazolásokat, amelyekkel biztonságos kommunikációs szekciókat hozhat létre a Védett socket réteg (SSL) bevonásával. Ha nem használja fel a DCM-et a saját helyi Igazolási hatóság (CA) működtetéséhez, akkor először hozza létre a megfelelő igazolás tárolót, hogy kezelni tudja az SSL használatához szükséges nyilvános igazolásokat. Ez a *SYSTEM igazolás tároló lesz. Amikor létrehoz egy igazolás tárolót, a DCM végigvezeti az igazoláskérő információ létrehozási folyamatán, amelyet el kell juttatni a nyilvános CA számára, hogy megkapja az igazolást.

Kövesse az alábbi lépéseket, ha a DCM segítségével kezeli és használja a nyilvános Internet igazolásokat úgy, hogy az alkalmazások létre tudjanak hozni SSL kommunikációs szekciókat:

1. DCM indítása.
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 az alkalmazások használhatnak SSL szekciókhoz) 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 a ***SYSTEM** beállítást, és kattintson a **Folytatásra**.
4. Válassza ki az **Igen** választ arra, hogy a *SYSTEM 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.

   Megjegyzés: Ha az iSeries rendelkezik telepített IBM 4758–023 PCI Cryptographic Coprocessor elemmel, a DCM lehetővé teszi annak eldöntését, hogyan tárolja az igazoláshoz tartozó magánkulcsot. Ha a rendszer nem rendelkezik ko-processzorral, a DCM automatikusan a *SYSTEM igazolás tárolóba helyezi el a magánkulcsot. Ha segítségre van szüksége a magánkulcs tárolási módjának eldöntéséhez, olvassa el a DCM online súgóját.
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. Küldje el a jelentkezési lapot vagy a fájlt az adott CA számára, amelyet kiválasztott arra, hogy kiadja és aláírja az igazolását.

   Megjegyzés: Meg kell várni, amíg a CA visszaküldi az aláírt, komplett igazolást, mielőtt befejezné az eljárást.

   Megjegyzés: Ahhoz, hogy az igazolásokat HTTP Server for iSeries termékkel használja, hozzon létre és konfiguráljon egy webszervert, mielőtt a DCM segítségével kezelné az aláírt, komplett igazolást. Amikor webszervert konfigurál SSL használattal, egy alkalmazás ID generálódik a szerver számára. Feltétlenül meg kell jegyezni ezt az alkalmazás ID-t, hogy a DCM segítségével meg tudja adni, melyik igazolást kell ennek az alkalmazásnak használni az SSL kapcsolathoz.

   Ne állítsa le és ne indítsa újra a szervert addig, amíg a DCM segítségével a szerverhez hozzá nem rendeli az aláírt, komplett igazolást. Ha leállítja vagy újraindítja az *ADMIN webszerver példányt, mielőtt hozzárendelné az igazolást, a szerver nem fog elindulni és nem lesz képes hozzárendelni az igazolást a szerverhez a DCM segítségével.
8. Miután a nyilvános CA visszaküldi az aláírt igazolást, indítsa el a DCM-et.

9. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SYSTEM** elemre, az igazolás tároló megnyitása céljából.
10. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatásra**.
11. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
12. A feladatlistából válassza az **Igazolás importálását**, ami révén elkezdődik az aláírt igazolás importálási folyamata a *SYSTEM igazolás tárolóba. Miután befejezte az igazolás importálását, kijelölheti azokat az alkalmazásokat, amelyeknek használni kell az igazolást az SSL kommunikációhoz.
13. A navigációs kereten válassza az **Alkalmazások kezelését** a feladatlista megjelenítéséhez.
14. A feladatlistán válassza az **Igazolás hozzárendelés frissítését**, hogy megjelenjenek azok az SSL képes alkalmazások, amelyekhez hozzárendelhet igazolást.
15. Válasszon ki egy alkalmazást a listából, és kattintson az **Igazolás hozzárendelés frissítésére**.
16. Válassza ki az importált igazolást, és kattintson az **Új igazolás hozzárendelésére**. A DCM egy megerősítő üzenetet ad ki, amely szerint az igazolás kiválasztása megtörtént az alkalmazás számára.

    Megjegyzés: Egyes SSL képes alkalmazások támogatják az igazoláson alapuló kliens hitelesítést. Ha azt akarja, hogy egy ilyen alkalmazás képes legyen az igazolások hitelesítésére az erőforrásokhoz való hozzáférés előtt, adja meg a megbízható CA-k listáját az alkalmazás számára. Ez biztosítja azt, hogy az alkalmazás csak azokat az igazolásokat fogja érvényesíteni, amelyeket a megadott listán szereplő CA adott ki. Ha a felhasználó vagy a kliens alkalmazás olyan CA-tól kapott igazolást mutat be, amelyik nincs megadva a megbízható CA-k listáján, az alkalmazás nem fogja azt elfogadni érvényes hitelesítés alapjául.

Amikor befejezi a feladatot, minden rendelkezésére áll ahhoz, hogy elkezdje az alkalmazások konfigurálását SSL használatához a biztonságos kommunikáció céljából. Mielőtt a felhasználók elérhetnék ezeket az alkalmazásokat SSL szekcióból, rendelkezniük kell a szerver igazolást kiadó CA-ra vonatkozó CA igazolás példányával. Ha az igazolás egy jólismert Internet CA-tól ered, a felhasználók kliens szoftverei már lehet, hogy rendelkeznek a szükséges CA igazolás egy példányával. Ha a felhasználóknak be kell szerezni a CA igazolást, menjenek a CA webhelyére, és kövessék az ott megjelenő utasításokat.

Nyilvános Internet igazolások kezelése objektumok aláírásához

A Digitális igazolás kezelő (DCM) segítségével kezelheti a nyilvános Internet igazolásokat, az objektumok digitális aláírásához. Ha nem használja fel a DCM-et a saját helyi Igazolási hatóság (CA) működtetéséhez, akkor először hozza létre a megfelelő igazolás tárolót, hogy kezelni tudja a dokumentumok aláírásához szükséges nyilvános igazolásokat. Ez az *OBJECTSIGNING igazolás tároló lesz. Amikor létrehoz egy igazolás tárolót, a DCM végigvezeti az igazoláskérő információ létrehozási folyamatán, amelyet el kell juttatni a nyilvános Internet CA számára, hogy megkapja az igazolást.

Ahhoz, hogy az igazolást objektumok aláírásához lehessen használni, meg kell adni egy alkalmazás azonosítót (ID). Ez az alkalmazás ID vezérli, hogy mennyi jogosultság kell valakinek ahhoz, hogy aláírhasson egy objektumot egy adott igazolással, valamint egy másik hozzáférés vezérlési szintet is szolgáltat azon túl, amit a DCM. Alapértelmezés szerint az alkalmazás definíciója megköveteli a felhasználótól az *ALLOBJ különleges jogosultságot

ahhoz, hogy az alkalmazás igazolásával aláírhasson objektumokat. (Mindazonáltal, megváltoztathatja az alkalmazás ID által igényelt jogosultságot az iSeries navigátor segítségével.)

Hajtsa végre az alábbi feladatokat, ha a DCM segítségével kezeli és használja a nyilvános Internet igazolásokat objektumok aláírásához:

1. DCM indítása.
2. A DCM baloldali 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 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**. Megjelenik egy űrlap, 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. Küldje el a jelentkezési lapot vagy a fájlt az adott CA számára, amelyet kiválasztott arra, hogy kiadja és aláírja az igazolását.

   Megjegyzés: Meg kell várni, amíg a CA visszaküldi az aláírt, komplett igazolást, mielőtt befejezné az eljárást.
8. Miután a nyilvános CA visszaküldi az aláírt igazolást, indítsa el a DCM-et.
9. A baloldali navigációs kereten kattintson az **Igazolás tároló választása**, majd az ***OBJECTSIGNING** elemre, az igazolás tároló megnyitása céljából.
10. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatásra**.
11. A navigációs kereten válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
12. A feladatlistából válassza az **Igazolás importálását**, ami révén elkezdődik az aláírt igazolás importálási folyamata a *OBJECTSIGNING igazolás tárolóba. Miután befejezte az igazolás importálását, létrehozhat egy alkalmazás definíciót ahhoz, hogy az igazolás segítségével objektumokat írjon alá.
13. Miután frissül a baloldali navigációs keret, válassza az **Alkalmazások kezelését** a feladatlista megjelenítéséhez.
14. A feladatlistából válassza az **Alkalmazás hozzáadását**, hogy elkezdődjön az objektum aláíró alkalmazás definíció létrehozásának folyamata, ami révén az igazolás segítségével objektumokat írhat alá.
15. Töltse ki az űrlapot, hogy meghatározza az objektum aláíró alkalmazást, és kattintson a **Hozzáadás** gombra. Ez az alkalmazás definíció nem írja le ugyan az aktuális

alkalmazást, viszont leírja azokat az objektum típusokat, amelyeket tervei szerint aláír a speciális igazolással. Az űrlap kitöltéséhez használja az online súgót.

16. Kattintson az **OK** gombra, hogy nyugtázza az alkalmazás definíció jóváhagyást kérő üzenetét, és megjelenjen az Alkalmazások kezelése feladatlista.
17. A feladatlistán válassza az **Igazolás hozzárendelés frissítését** és kattintson a **Folytatásra**, hogy megjelenjenek azok az objektum aláíró alkalmazás azonosítók (ID), amelyekhez hozzárendelhet igazolást.
18. Válasszon ki egy alkalmazás ID-t a listából, és kattintson az **Igazolás hozzárendelés frissítésére**.
19. Válassza ki az importált igazolást, és kattintson az **Új igazolás hozzárendelésére**.

Amikor befejezi a feladatokat, minden rendelkezésére áll ahhoz, hogy elkezdje az objektumok aláírását, hogy azok sérthetetlenségét garantálja.

Amikor aláírt objektumokat terjeszt, az objektumokat fogadóknak V5R1 vagy újabb DCM változatot kell használni az objektumokon lévő aláírás érvényesítéséhez, hogy bizonyosak legyenek abban, az adatok nem változtak, és ellenőrizni tudják a küldő azonosságát. A fogadónak rendelkeznie kell az aláírás ellenőrző igazolás egy példányával ahhoz, hogy érvényesítse (ellenőrizze) az aláírást. Az aláírt objektumok részeként biztosítania kell az igazolás egy példányát.

A fogadónak rendelkeznie kell a CA igazolás egy példányával, mégpedig arra a CA-ra vonatkozóan, amelyik által kiadott igazolást használja az objektum aláírásához. Ha egy jólismert Internet CA-tól eredő igazolással írja alá az objektumokat, a fogadónál lévő DCM verziójának már rendelkeznie kell a szükséges CA igazolás egy példányával. Mindazonáltal, küldje el a CA igazolás egy példányát az aláírt objektummal egyetemben, ha úgy gondolja, hogy a fogadó esetleg még nem rendelkezik vele. Például, a helyi CA igazolás egy példányát küldje el, ha az objektumokat a helyi magán CA által kiadott igazolással írta alá. Biztonsági okokból egy külön csomagban küldje el a CA igazolást, vagy nyilvánosan tegye elérhetővé a CA igazolást azoknak, akiknek szükségük van rá.

Igazolások kezelése objektum aláírások ellenőrzéséhez

A Digitális igazolás kezelő (DCM) segítségével kezelheti az aláírás ellenőrző igazolásokat,amelyekkel érvényesítheti az objektumokon lévő digitális aláírásokat. Az objektum aláírásához az igazolás magánkulcsát használja, amellyel így létrehozza az aláírást. Amikor elküldi az aláírt objektumot másoknak, annak az igazolásnak egy példányát is vele kell küldeni, amellyel az objektumot aláírta. Ezt megteheti, ha a DCM segítségével aláírás ellenőrző igazolásként exportálja az objektum aláíró igazolást (az igazolás magánkulcsa nélkül). Az aláírás ellenőrző igazolást exportálhatja egy fájlba, amelyet azután másoknak elküldhet. Vagy, ha ellenőrizni akarja a létrehozott aláírásokat, exportálja az aláírás ellenőrző igazolást a *SIGNATUREVERIFICATION igazolás tárolóba.

Ahhoz, hogy érvényesnek tekinthesse az objektumon lévő aláírást, rendelkeznie kell annak az igazolásnak egy példányával, amellyel az objektumot aláírták. Az aláírási igazolás nyilvános kulcsát használja, amelyet maga az igazolás tartalmaz, hogy megvizsgálja és ellenőrizze a megfelelő magánkulccsal létrehozott aláírást. Ennek következtében, mielőtt ellenőrizni tudná egy objektum aláírását, meg kell szerezni az aláírási igazolás egy példányát attól, aki küldte az aláírt objektumokat.

Rendelkeznie kell az Igazolási hatóság (CA) igazolásának egy példányával is, még pedig arra a CA-ra vonatkozóan, amelyik által kiadott igazolással írták alá az objektumot. A CA igazolással ellenőrizheti az objektum aláírásához használt igazolás hitelességét. A DCM rendelkezik a közismert CA hatóságok CA igazolásainak egy-egy példányával. Ha azonban az

objektum egy másik nyilvános CA vagy egy magán CA által kibocsátott igazolással lett aláírva, akkor be kell szerezni a CA igazolás egy példányát, mielőtt ellenőrizni tudná az objektum aláírását.

Ahhoz, hogy a DCM segítségével ellenőrizze az objektum aláírásokat, először hozza létre a megfelelő igazolás tárolót (ez a *SIGNATUREVERIFICATION), amely révén a szükséges aláírás ellenőrző igazolásokat kezeli. Amikor létrehozza ezt az igazolás tárolót, a DCM automatikusan ″benépesíti″ a legjobban ismert nyilvános CA hatóságok igazolásainak egy-egy példányával.

Megjegyzés: Ha fel akar készülni az aláírások ellenőrzésére, amelyeket saját objektum aláíró igazolásaival hozott létre, akkor létre kell hozni a *SIGNATUREVERIFICATION igazolás tárolót, és másolja át az igazolásokat az *OBJECTSIGNING igazolás tárolóból az előbbibe. Ez még akkor is így igaz, ha az aláírás ellenőrzést az *OBJECTSIGNING igazolás tárolón belül kívánja végrehajtani.

Hajtsa végre az alábbi feladatokat, ha a DCM segítségével kezeli az aláírás ellenőrző igazolásokat:

1. DCM indítása.
2. A DCM baloldali navigációs keretén válassza ki az **Új igazolás tároló létrehozását** a feladat elindításához, és töltse ki az űrlapok sorozatát.

   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 ***SIGNATUREVERIFICATION** beállítást, és kattintson a **Folytatásra**.

   Megjegyzés: Ha létezik az *OBJECTSIGNING igazolás tároló, akkor ennél a pontnál a DCM kéri annak megadását, hogy átmásolja-e az objektum aláíró igazolásokat az új igazolás tárolóba, mint aláírás ellenőrző igazolások. Ha a meglévő objektum aláíró igazolásokat kívánja használni az aláírások ellenőrzéséhez, válassza ki az **Igen** választ, és kattintson a **Folytatásra**. Ismernie kell az *OBJECTSIGNING igazolás tárolóhoz tartozó jelszót ahhoz, hogy átmásolja belőle az igazolásokat.
4. Adjon meg egy jelszót az új igazolás tárolóra, és kattintson a **Folytatásra**, hogy létrehozza az igazolás tárolót. Megjelenik a megerősítő oldal, ami jelzi, hogy az igazolás tároló létrehozása sikeresen megtörtént. Ettől kezdve a tároló segítségével kezelheti és használhatja az igazolásokat az objektum aláírások ellenőrzéséhez.

   Megjegyzés: Ha úgy hozta létre ezt a tárolót, hogy ellenőrizze a saját maga által aláírt objektumokon lévő aláírásokat, akkor ezt leállíttathatja. Amint létrehozza az új objektum aláíró igazolásokat, exportálja őket az *OBJECTSIGNING igazolás tárolóból ebbe az igazolás tárolóba. Ha nem exportálja őket, nem tudja ellenőrizni azokat az aláírásokat, amelyeket saját maga készített velük.

   Megjegyzés: Ha úgy hozta létre ezt az igazolás tárolót, hogy ellenőrizni tudja a más forrásokból kapott objektumok aláírásait, akkor folytassa ezzel az eljárással, hogy importálni tudja a szükséges igazolásokat az igazolás tárolóba.
5. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SIGNATUREVERIFICATION** elemre, az igazolás tároló megnyitása céljából.

6. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatásra**.
7. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
8. A feladatlistából válassza az **Igazolás importálását**. A feladat végigvezet az igazolások importálásának folyamatán, amely révén a szükséges igazolások az igazolás tárolóba kerülnek, hogy ellenőrizni tudja a kapott objektumok aláírásait.
9. Válassza ki az importálni kívánt igazolástípust. Válassza ki az **Aláírás ellenőrzést**, hogy importálja az aláírt objektumokkal kapott igazolást, és fejezze be az importálási feladatot.

   Megjegyzés: Ha az igazolás tároló még nem tartalmazza a CA igazolás egy példányát, még pedig arra a CA-ra vonatkozóan, amelyik kiadta az aláírás ellenőrző igazolást, akkor *először* a CA igazolást kell importálni. Hibaüzenetet kaphat az aláírás ellenőrző igazolás importálásakor, ha előzőleg nem importálta a CA igazolást.

Ettől kezdve használhatja az igazolásokat az objektum aláírások ellenőrzéséhez.

Fejezet 8. A DCM kezelése

Miután konfigurálta a Digitális igazolás kezelőt (DCM), számos igazoláskezelési feladat van, amelyeket végre kell hajtani. Az alábbi témakörök nyújtanak tájékoztatást arról, hogyan kezelheti a digitális igazolásokat a DCM segítségével:

Helyi CA révén igazolások kiadása más iSeries rendszereknek
Megismerheti, hogyan lehet az egyik rendszeren lévő Helyi CA segítségével igazolásokat kiadni, amelyeket azután más iSeries rendszereken használ fel.

Alkalmazások kezelése a DCM programban
Megismerheti, hogyan lehet kezelni az SSL képes alkalmazások vagy az objektum alíró alkalmazások számára készült alkalmazás definíciókat a DCM segítségével. A témakör tájékoztatást ad az alkalmazás definíciók létrehozásáról, valamint arról, hogyan kezelheti az igazolás hozzárendelést. Tanulmányozhatja a megbízható CA listák megadásának a módját. Az alkalmazások az igazolások elfogadásának alapjaként kezelik a listákat a kliens hitelesítésben.

Igazolások és alkalmazások ellenőrzése
Tanulmányozhatja, hogyan ellenőrizheti egy adott igazolás hitelességét, mielőtt az alkalmazás használná vagy elfogadná azt.

Igazolások hozzárendelése
Tanulmányozhatja, hogyan rendelheti gyorsan hozzá az igazolást egy vagy több alkalmazáshoz a biztonságos funkciók érdekében.

CRL helyek kezelése Tanulmányozhatja, hogyan adhatja meg és használhatja az Igazolás visszavonási lista (CRL) helyeket, amelyeket az alkalmazások használhatnak fel annak ellenőrzéséhez, hogy az általuk elfogadott igazolások érvényesek-e.

Igazolás kulcsok tárolása az IBM 4758 Cryptographic Coprocessor kártyán
Megismerheti, hogyan lehet a telepített társprocesszorral biztonságosabb tárolást nyújtani az igazolások magánkulcsai számára.

Kérési hely kezelés PKIX CA esetén
Megismerheti, hogy a DCM segítségével hogyan kezelheti az olyan nyilvános Internet CA-tól beszerzett igazolásokat, amely Public Key Infrastructure for X.509 (PKIX) szabvány szerint adja ki az igazolásokat.

Objektumok aláírása
Megismerheti, hogy a DCM segítségével hogyan kezelhet objektumok digitális aláírására szolgáló igazolásokat, ami biztosítja az objektumok sértetlenségét.

Objektum aláírások ellenőrzése
Megismerheti, hogyan ellenőrizheti az objektumokon lévő digitális aláírások hitelességét a DCM segítségével.

Helyi CA révén igazolások kiadása más iSeries rendszereknek

Lehet, hogy már használ egy saját Helyi Igazolási hatóságot (CA) a hálózat egyik iSeries rendszerén. Most ki akarja terjeszteni a Helyi CA használatát a hálózat egy másik iSeries rendszerére is. Például azt szeretné, hogy a Helyi CA szerver vagy kliens igazolásokat adjon ki másik iSeries rendszeren található alkalmazásnak SSL kommunikációs szekciók használatához. Illetve, a Helyi CA-tól eredő igazolásokat felhasználhatja másik iSeries szerveren tárolt objektumok aláírására.

A Digitális igazolás kezelő (DCM) használatával teljesítheti a célt. Néhány feladatot a Helyi CA-t üzemeltető iSeries szerveren hajt végre, míg másokat a másik iSeries rendszeren

(másodlagos), amely üzemelteti azokat az alkalmazásokat, melyekhez igazolást kíván kiadni. Ezt a másodlagos rendszert hívják célrendszernek. A célrendszeren végrehajtandó feladatok az adott rendszer kibocsátás szintjétől függnek.

Megjegyzés: Probléma merülhet fel, ha azon az iSeries rendszeren, amelyen Helyi CA-t üzemeltet, olyan kriptográfiai lehetőséget biztosító terméket használ, amely erősebb titkosítást nyújt a célrendszernél. (V5R2 esetén csak az 5722–AC3 kriptográfiai lehetőséget nyújtó termék áll rendelkezésre, mely a legerősebb elérhető termék. Azonban, a korábbi változatokban egyéb, szegényesebb termékeket (5722–AC1 vagy 5722–AC2) is telepíthetett, ami alacsonyabb szintű titkosítási funkciót jelent.) Amikor exportálja az igazolást (annak magánkulcsával), a rendszer titkosítja a fájlt, hogy védje tartalmát. Ha a rendszer erősebb rejtjelező terméket használ, mint a célrendszer, akkor a célrendszer nem tudja visszafejteni a fájlt az importálási folyamat során. Következésképpen, az import meghiúsulhat, illetve az igazolás esetleg nem lesz használható SSL szekciók létesítéséhez. Ez még akkor is igaz, ha olyan kulcsméretet használ az új igazoláshoz, amely megfelel a célrendszeren használt titkosítási terméknek.

A Helyi CA segítségével kiadhat igazolásokat más rendszereknek, ahol az igazolásokkal objektumokat írhat alá, vagy lehetnek olyan alkalmazások, amelyek SSL szekciók létesítéséhez használják. Amikor Helyi CA révén igazolást hoz létre másik iSeries rendszer számára, a DCM által létrehozott fájlok tartalmazzák a Helyi CA igazolás egy példányát, valamint számos nyilvános Internet CA igazolásának példányait.

A DCM-ben végrehajtandó feladatok kicsit változhatnak a Helyi CA által kiadott igazolás típusától, valamint a célrendszer változatszintjétől és feltételeitől függően.

Magán igazolások kiadása másik V5R2 vagy V5R1 szintű iSeries rendszeren való használatra

Hajtsa végre az alábbi lépéseket a Helyi CA-t üzemeltető rendszeren, ha a Helyi CA segítségével igazolásokat ad ki másik V5R2 vagy V5R1 szintű iSeries rendszernek:

1. DCM indítása.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
2. A navigációs kereten válassza ki az **Igazolások létrehozása** opciót az igazolás típusok listájának megjelenítéséhez, amit a Helyi CA felhasználhat az igazolás létrehozásához.

   A feladat befejezéséhez nem kell megnyitni igazolás tárolót. Ezek az utasítások feltételezik, hogy nem a megadott igazolás tárolóban dolgozik, hanem a Helyi Igazolási hatóság (CA) igazolás tárolójában. A feladatok végrehajtása előtt a Helyi CA-nak létezni kell az adott rendszeren.
3. Válassza ki a Helyi CA által kiadásra kerülő igazolás típusát, majd kattintson a **Folytatás** gombra a feladat elindításához, és töltse ki az űrlapokat. Válassza ki a **szerver vagy kliens igazolás létrehozását másik iSeries szervernek** (SSL szekciókhoz), vagy az **objektum aláíró igazolást másik iSeries szervernek** (egy másik rendszeren való használatra).

   Megjegyzés: Ha objektum aláíró igazolást készít egy másik rendszeren való használatra, akkor azon V5R1 vagy újabb szintű OS/400 operációs rendszernek kell futni ahhoz, hogy használni lehessen az igazolást. Mivel a célrendszer szintje V5R1 vagy újabb, a DCM-et üzemeltető rendszer nem kéri a célrendszer formátumának kiválasztását az új objektum aláíró igazoláshoz.

4. Amikor szerver vagy kliens igazolást hoz létre, annak az iSeries rendszernek a szintjét válassza ki, amelyiknek készíti az igazolást. Kattintson a **Folytatás** gombra az űrlap megjelenítéséhez, amellyel megadhatja az azonosítási információkat az új igazolás számára.

   Megjegyzés: A kiválasztott kibocsátási szint meghatározza a DCM által az új igazolás létrehozásához használt formátumot. Az űrlapon lévő azonosító információk mennyisége és típusa a kiválasztott kibocsátási szinttől függően változik. Ez biztosítja azt, hogy az igazolás fájlok kompatíbilisek az igazolást használni fogó iSeries rendszerrel.
5. Töltse ki az űrlapot, és kattintson a **Folytatásra** a jóváhagyási oldal megjelenítéséhez.

   Megjegyzés: Ha a célrendszeren van *OBJECTSIGNING vagy *SYSTEM nevű igazolás tároló, feltétlenül egyedi címkét és fájlnevet adjon meg az igazolásnak. Ha egyedi igazolás címkét és fájlnevet ad meg, könnyen importálni tudja az igazolást a célrendszeren meglévő igazolás tárolóba.

   A jóváhagyó oldal megjeleníti a DCM segítségével a célrendszer számára létrehozott fájlok neveit. A DCM a célrendszer megadott kibocsátási szintje alapján hozza létre a fájlokat. A DCM automatikusan elhelyezi a Helyi CA igazolás egy példányát a fájlokba.

   Megjegyzés: A DCM saját igazolás tárolójában hozza létre az új igazolásokat. Két fájlt állít elő: egy igazolás tároló fájlt (.KDB kiterjesztéssel), és egy kérés fájlt (.RDB kiterjesztéssel).
6. Fájlátviteli protokollal (FTP) vagy más módszerrel juttathatja el a fájlokat a célrendszerhez.

Magán igazolások kiadása másik V4R4 vagy V4R5 szintű iSeries rendszeren való használatra

Hajtsa végre az alábbi lépéseket a Helyi CA-t üzemeltető rendszeren, ha a Helyi CA segítségével igazolásokat ad ki másik V4R4 vagy V4R5 szintű iSeries rendszernek:

1. DCM indítása.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az online súgó elérése céljából.
2. A navigációs kereten válassza ki az **Igazolások létrehozása** opciót az igazolás típusok listájának megjelenítéséhez, amit a Helyi CA felhasználhat az igazolás létrehozásához.

   A feladat befejezéséhez nem kell megnyitni igazolás tárolót. Ezek az utasítások feltételezik, hogy nem a megadott igazolás tárolóban dolgozik, hanem a Helyi Igazolási hatóság (CA) igazolás tárolójában. A feladatok végrehajtása előtt a Helyi CA-nak létezni kell az adott rendszeren.
3. Válassza ki a Helyi CA által kiadásra kerülő igazolás típusát, majd kattintson a **Folytatás** gombra a feladat elindításához, és töltse ki az űrlapokat.

   Megjegyzés: Mivel az igazolást V4R4 vagy V4R5 szintű iSeries rendszeren való használatra készíti, válassza ki a **szerver vagy kliens igazolás másik iSeries szerver számára** opciót. A V5R1-nél alacsonyabb szintű célrendszerek nem tudják használni az objektum aláíró igazolásokat.
4. Válassza ki az iSeries (melynek az igazolást készíti) kibocsátási szintjét. Kattintson a **Folytatás** gombra az űrlap megjelenítéséhez, amellyel megadhatja az azonosítási információkat az új igazolás számára.

   Megjegyzés: A kiválasztott kibocsátási szint meghatározza a DCM által az új igazolás létrehozásához használt formátumot. Az űrlapon lévő azonosító információk mennyisége és típusa a kiválasztott kibocsátási szinttől

függően változik. Ez biztosítja azt, hogy az igazolás fájlok kompatíbilisek az igazolást használni fogó iSeries rendszerrel.

5. Töltse ki az űrlapot, és kattintson a **Folytatásra** a jóváhagyási oldal megjelenítéséhez.

   Megjegyzés: Ha a célrendszeren van *SYSTEM nevű igazolás tároló, feltétlenül egyedi címkét és fájlnevet adjon meg az igazolásnak. Ha egyedi igazolás címkét és fájlnevet ad meg, könnyen importálni tudja az igazolást a célrendszeren meglévő igazolás tárolóba.

   A jóváhagyó oldal megjeleníti a DCM segítségével a célrendszer számára létrehozott fájlok neveit. A DCM a célrendszer megadott kibocsátási szintje alapján hozza létre a fájlokat. A DCM automatikusan elhelyezi a Helyi CA igazolás egy példányát a fájlokba.

   Megjegyzés: A DCM saját igazolás tárolójában hozza létre az új igazolásokat. Két fájlt állít elő: egy igazolás tároló fájlt (.KDB kiterjesztéssel), és egy kérés fájlt (.RDB kiterjesztéssel).

Megjegyzés: Ha a V4R4 vagy V4R5 szintű rendszerek *SYSTEM igazolás tárolójában lévő fájlokban tárolt igazolásokat kívánja használni, akkor a Helyi CA igazolást közvetlenül nem importálhatja a .KDB és az .RDB fájlokból. Ez azért van így, mert a CA igazolás formátuma nem olyan, amelyet a DCM import funkciója felismerhetne vagy használhatna. Helyette a hoszt rendszer segítségével exportálja a Helyi CA igazolást egy önálló fájlba. Így a CA igazolás olyan formátumban lesz, amit már kezelni tudnak a korábbi szintekre vonatkozó import funkciók.

6. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SYSTEM** elemre, az igazolás tároló megnyitása céljából.
7. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a hoszt rendszeren történt létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatás** gombra.
8. A navigációs kereten válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
9. A feladatok listájából válassza az **Igazolás exportálását**.
10. Válassza az **Igazolási hatóságot (CA)** az exportálásra szánt igazolás típusának, és kattintson a **Folytatásra** a CA igazolások felsorolásának megjelenítéséhez.
11. Az igazolások listájából válassza ki a Helyi CA igazolást (például HELYI_IGAZOLÁSI_HATÓSÁG). Kattintson az **Export** gombra az űrlap megjelenítéséhez, amellyel kiválaszthatja a CA igazolás címzettjét.
12. Válassza ki a **Fájlt**, és kattintson a **Folytatás** gombra.
13. Adja meg az exportálandó fájl teljes elérési útvonalát és nevét, majd kattintson a **Folytatás** gombra. Megjelenik a megerősítő oldal, ami jelzi, hogy a DCM sikeresen exportálta a fájlt.

    Megjegyzés: Bizonyosodjon meg arról, hogy a fájlnak egyedi nevet és kiterjesztést ad. Például adjon sajátcafájl.exp nevet a fájlnak. Amikor nevet ad a fájlnak, ne használja a következő kiterjesztések egyikét sem a fájlhoz: .TXT, .KDB, .RDB vagy .KYR. A felsorolt kiterjesztés típusok használata problémát okozhat, amikor importálja a fájlt a célrendszeren.
14. Bináris fájlátviteli protokollal (FTP) vagy más módszerrel juttathatja el a létrehozott igazolás tároló fájlokat (.KDB és .RDB) a V4R4 vagy V4R5 szintű célrendszer számára. Az exportált Helyi CA igazolást tartalmazó fájl átviteléhez használja az ASCII FTP módot.

Az átvitt fájlok használata a célrendszeren

Miután a fájlok átvitele megtörténik, a célrendszeren lévő DCM kezeli az átvitt igazolás fájlokat. A végrehajtandó DCM feladatok aszerint változnak, hogy mi a célrendszer

kibocsátási szintje és milyen igazolás tárolók léteznek a célrendszeren. A hoszt rendszeren létrehozott igazolás típusa ugyancsak hatással van a célrendszeren végrehajtandó feladatokra. Olvassa át az alábbi témaköröket, ha kíváncsi arra, hogyan kezeli a DCM az átvitt igazolás fájlokat a célrendszeren:

- Magán igazolás használata SSL szekciókban V5R2 célrendszeren.
- Magán igazolás használata SSL szekciókban V5R1 célrendszeren.
- Magán igazolás használata objektum aláíráshoz V5R1 vagy V5R2 célrendszeren.
- Magán igazolás használata SSL szekciókban V4R5 vagy V4R4 célrendszeren.

Magán igazolás használata SSL szekciókban V5R2 célrendszeren

A Digitális igazolás kezelő (DCM) *SYSTEM igazolás tárolójában lévő igazolásokat az alkalmazások használják SSL szekciók létesítéséhez. Ha az SSL szekciók létesítésére szolgáló igazolások kezeléséhez sohasem használt DCM-et, akkor ez az igazolás tároló nem található meg a célrendszeren. A Helyi igazolási hatóság (CA) hoszt rendszerén létrehozott és a célrendszernek átküldött igazolás tároló fájlok használatára vonatkozó feladatok aszerint változnak, hogy létezik-e a *SYSTEM igazolás tároló. Ha a *SYSTEM igazolás tároló nem létezik, akkor az átvitt igazolás fájlok azt jelentik, hogy létre kell hozni a *SYSTEM igazolás tárolót. Ha létezik a *SYSTEM igazolás tároló a V5R2 szintű célrendszeren, akkor az átvitt igazolás fájlok használatához a következő két módszer egyikét választhatja:

- Átvitt fájlok használata más rendszer igazolás tárolójaként.
- Átvitt fájlok importálása a meglévő *SYSTEM igazolás tárolóba.

*SYSTEM igazolás tároló nem létezik

Ha a *SYSTEM igazolás tároló nem létezik a V5R2 rendszeren, amelyen használni akarja az átvitt igazolás tároló fájlokat, akkor az átvitt igazolás fájlokat *SYSTEM igazolás tárolóként használhatja. Kövesse az alábbi lépéseket a *SYSTEM igazolás tároló létrehozásához, valamint az igazolás fájlok V5R2 célrendszeren való használatához:

1. Bizonyosodjon meg arról, hogy a Helyi CA-t üzemeltető rendszeren létrehozott igazolás tároló fájlok (két fájl: egyik .KDB, másik .RDB kiterjesztésű) a /QIBM/USERDATA/ICSS/CERT/SERVER alkönyvtárban vannak.
2. Amint az átvitt igazolás fájlok a /QIBM/USERDATA/ICSS/CERT/SERVER alkönyvtárban vannak, nevezze át őket DEFAULT.KDB és DEFAULT.RDB névre. Azzal, hogy a fájlokat átnevezi a megfelelő alkönyvtárban, olyan komponenseket hoz létre, amelyek a *SYSTEM igazolás tárolót alkotják a célrendszer számára. Az igazolás tároló fájlok már tartalmazzák több nyilvános Internet CA igazolásának egy másolatát. Mindezt, valamint a Helyi CA igazolást a DCM adta hozzá az igazolás tároló fájlokhoz a létrehozás során.

   Figyelem: Ha a célrendszeren megtalálhatók a DEFAULT.KDB és a DEFAULT.RDB fájlok a /QIBM/USERDATA/ICSS/CERT/SERVER alkönyvtárban, akkor a *SYSTEM igazolás tároló pillanatnyilag létezik az adott célrendszeren. Következésképpen, nem kell átnevezni az átvitt fájlokat a javaslatnak megfelelően. Az alapértelmezett fájlok felülírása problémákat okoz, amikor a DCM-et, az átvitt igazolás tárolót és annak tartalmát használja. Helyette bizonyosodjon meg, hogy egyedi nevük van, és az átvitt igazolás tárolót **Más rendszer igazolás tárolójaként** használja. Ha a fájlokat Más rendszer igazolás tárolójaként használja, akkor nem tudja megadni a DCM segítségével, hogy mely alkalmazások használják az igazolásokat.
3. DCM indítása. Meg kell változtatni az átvitt fájlok átnevezésével létrehozott *SYSTEM igazolás tárolóra vonatkozó jelszót. A jelszó módosítása lehetővé teszi, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az igazolás tárolóban.

4. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SYSTEM** elemre, az igazolás tároló megnyitása céljából.
5. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a *hoszt* rendszeren adott meg az igazolás tárolónak, amikor igazolást hozott létre a V5R2 célrendszer számára, és kattintson a **Folytatás** gombra.
6. A navigációs kereten válassza ki az **Igazolás tároló kezelése**, majd a **Jelszó módosítása** feladatokat a listából. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához. Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat. Utána megadhatja, hogy mely alkalmazások használjanak igazolást az SSL szekciókhoz.
7. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SYSTEM** elemre, az igazolás tároló megnyitása céljából.
8. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az új jelszót, majd kattintson a **Folytatás** gombra.
9. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a navigációs keretben a feladatlista megjelenítéséhez.
10. A feladatlistán válassza az **Igazolás hozzárendelése** feladatot az aktuális igazolás tárolóban lévő igazolások listájának megjelenítéséhez.
11. Válassza ki a *hoszt* rendszeren létrehozott igazolást, és kattintson az **Alkalmazásokhoz rendelés** feladatra, hogy megjelenjen az SSL kapcsolatra felkészített alkalmazások listája, amelyekhez hozzárendelheti az igazolást.
12. Válassza ki az alkalmazásokat, amelyek használni fogják az igazolást az SSL szekciókhoz, és kattintson a **Folytatás** gombra. A DCM egy megerősítő üzenetet ad ki, amely szerint az igazolás kiválasztása megtörtént az alkalmazások számára.

    Megjegyzés: Egyes SSL képes alkalmazások támogatják az igazoláson alapuló kliens hitelesítést. Az ilyen támogatással rendelkező alkalmazás képes az igazolások hitelesítésére az erőforrásokhoz való hozzáférés előtt. Következésképpen, meg kell határozni a megbízható CA-k listáját az alkalmazás számára. Ez biztosítja azt, hogy az alkalmazás csak azokat az igazolásokat fogja érvényesíteni, amelyeket a megadott listán szereplő CA adott ki. Ha a felhasználó vagy a kliens alkalmazás olyan CA-tól kapott igazolást mutat be, amelyik nincs megadva a megbízható CA-k listáján, az alkalmazás nem fogja azt elfogadni érvényes hitelesítés alapjául.

A fenti feladatok végrehajtásával a célrendszeren lévő alkalmazások használni tudják a Helyi CA által kiadott igazolásokat más iSeries szerveren. Azonban, mielőtt használhatnák az adott alkalmazások az SSL kapcsolatokat, konfigurálja az alkalmazásokat az SSL használatához.

Mielőtt a felhasználó elérhetné a kiválasztott alkalmazásokat az SSL kapcsolaton keresztül, a felhasználó a DCM segítségével beszerzi a Helyi CA igazolás egy példányát a hoszt rendszertől. A Helyi CA igazolást egy fájlba kell átmásolni a felhasználó PC-jére, vagy le kell tölteni a felhasználó böngészőjébe, az SSL képes alkalmazás követelményeitől függően.

*SYSTEM igazolás tároló létezik — fájlok használata Más rendszer igazolás tárolójaként

Ha a V5R2 célrendszeren már van *SYSTEM igazolás tároló, akkor döntse el, hogyan kezeli az igazolás fájlokat. Választhatja azt, hogy az átvitt igazolás fájlokat **Más rendszer igazolás tárolójaként** használja. Választhatja azt is, hogy importálja a magán igazolást és a neki megfelelő Helyi CA igazolást a meglévő *SYSTEM igazolás tárolóba.

Ezek a tárolók valójában felhasználó által megadott másodlagos igazolás tárolók az SSL igazolások számára. Felhasználó által írt SSL képes alkalmazásoknak (amelyek nem használnak DCM API-kat az alkalmazás ID regisztráltatásához) szánt igazolások számára hozhatja létre és használhatja. Az Egyéb rendszer igazolás tároló nevű opció lehetővé teszi az

igazolások kezelését olyan alkalmazások számára, amelyeket az SSL_Init API használatára írtak, hogy az SSL szekciók létesítéséhez szükséges igazolások programozottan elérhetők és használhatók legyenek. Ez az API lehetővé teszi az alkalmazásnak, hogy az igazolás tárolóhoz rendelt alapértelmezett igazolást használja, és ne azt, amelyet a felhasználó kifejezetten megadott.

Az IBM iSeries alkalmazások (és számos más szoftverfejlesztő alkalmazása) csak a *SYSTEM igazolás tárolóban őrzött igazolásokat tudják használni. Ha úgy dönt, hogy az átvitt fájlokat Más rendszer igazolás tárolójaként használja, akkor nem tudja megadni a DCM segítségével, hogy mely alkalmazások használják az igazolásokat SSL szekcióhoz. Következésképpen, a szabványos iSeries SSL kapcsolatra felkészített alkalmazásokat nem lehet konfigurálni az adott igazolás használatára. Ha az igazolást fel akarja használni az iSeries alkalmazásokhoz, először importálja az igazolást az átvitt igazolás tároló fájlokból a *SYSTEM igazolás tárolóba.

Kövesse az alábbi lépéseket, ha az átvitt igazolás fájlokat Más rendszer igazolás tárolójaként kívánja elérni és kezelni:

1. DCM indítása.
2. A navigációs kereten kattintson az **Igazolás tároló választása** elemre, majd válassza a **Más rendszer igazolás tárolóját**, mint megnyitandó igazolás tárolót.
3. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az igazolás tároló fájl teljes elérési útvonalát és nevét (az egyik .KDB kiterjesztésű), amelyet átvitt a hoszt rendszerről. Adja meg a jelszót, amelyet a *hoszt* rendszeren adott meg az igazolás tárolónak, amikor igazolást hozott létre a V5R2 célrendszer számára, és kattintson a **Folytatás** gombra.
4. A navigációs kereten válassza ki az **Igazolás tároló kezelése**, majd a **Jelszó módosítása** feladatokat a listából. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához.

   Megjegyzés: Ne felejtse el kiválasztani az **Automatikus bejelentkezés** opciót, amikor megváltoztatja az igazolás tároló jelszavát. Az opció használata biztosítja azt, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az új tárolóban.

   Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat. Azután megadhatja, hogy a tárolóban lévő igazolás alapértelmezett igazolásként használatos-e.
5. A navigációs kereten kattintson az **Igazolás tároló választása** elemre, majd válassza a **Más rendszer igazolás tárolóját**, mint megnyitandó igazolás tárolót.
6. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az igazolás tároló fájl teljes elérési útvonalát és nevét, az új jelszót, és kattintson a **Folytatás** gombra.
7. Miután a navigációs keret frissül, válassza ki az **Igazolás tároló kezelése**, majd az **Alapértelmezett igazolás beállítása** feladatokat a listából.

Most, hogy létrehozta és konfigurálta a Más rendszer igazolás tárolóját, az SSL_Init API-t alkalmazó bármely alkalmazás használhatja a benne tárolt igazolást SSL szekció létesítéséhez.

***SYSTEM igazolás tároló létezik — meglévő *SYSTEM igazolás tárolóban lévő igazolások használata**

A V5R2 rendszer egy meglévő *SYSTEM igazolás tárolójában található (átvitt) igazolás tároló fájlokban lévő igazolásokat szintén használhatja. Ehhez importálni kell az igazolásokat az igazolás tároló fájlokból a meglévő *SYSTEM igazolás tárolóba. Azonban, az igazolásokat nem lehet közvetlenül importálni a .KDB és az .RDB fájlokból, mivel a formátumuk nem olyan, amelyet a DCM import funkciója felismerhetne vagy használhatna. Ahhoz, hogy használhassa az átvitt igazolásokat egy meglévő *SYSTEM igazolás tárolóból, a fájlokat Más rendszer igazolás tárolójaként nyissa meg, majd exportálja őket a *SYSTEM igazolás tárolóba.

Hajtsa végre az alábbi lépéseket a V5R2 célrendszeren, hogy exportálja az igazolásokat az igazolás tároló fájlokból a *SYSTEM igazolás tárolóba:

1. DCM indítása.
2. A navigációs kereten kattintson az **Igazolás tároló választása** elemre, majd adja meg a **Más rendszer igazolás tárolóját**, mint megnyitandó igazolás tárolót.
3. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az igazolás tároló fájl teljes elérési útvonalát és nevét (az egyik .KDB kiterjesztésű), amelyet átvitt a hoszt rendszerről. Adja meg a jelszót, amelyet a *hoszt* rendszeren adott meg az igazolás tárolónak, amikor igazolást hozott létre a V5R2 célrendszer számára, és kattintson a **Folytatás** gombra.
4. A navigációs kereten válassza ki az **Igazolás tároló kezelése**, majd a **Jelszó módosítása** feladatokat a listából. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához.

   Megjegyzés: Ne felejtse el kiválasztani az **Automatikus bejelentkezés** opciót, amikor megváltoztatja az igazolás tároló jelszavát. Az opció használata biztosítja azt, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az új tárolóban. Ha nem változtatja meg a jelszót és nem választja ki az Automatikus bejelentkezést, hibákkal számolhat, amikor az igazolásokat exportálja innen a *SYSTEM igazolás tárolóba.

   Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat.
5. A navigációs kereten kattintson az **Igazolás tároló választása** elemre, majd válassza a **Más rendszer igazolás tárolóját**, mint megnyitandó igazolás tárolót.
6. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az igazolás tároló fájl teljes elérési útvonalát és nevét, az új jelszót, és kattintson a **Folytatás** gombra.
7. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a navigációs keretben a feladatlista megjelenítéséhez, majd válassza az **Igazolás exportálását**.
8. Válassza az **Igazolási hatóságot (CA)** az exportálásra szánt igazolás típusának, és kattintson a **Folytatásra**.

   Megjegyzés: A Helyi CA igazolást exportálja az igazolás tárolóba, mielőtt szerver vagy kliens igazolást exportálna ugyanoda. Ha először szerver vagy kliens igazolást exportál, hibajelzést kaphat, mivel a Helyi CA igazolás nem található az igazolás tárolóban.
9. Válassza ki az exportálandó Helyi CA igazolást, és kattintson az **Export** gombra.
10. Válassza ki az exportált igazolás célpontját jelentő **Igazolás tárolót**, és kattintson a **Folytatás** gombra.
11. Írja be a *SYSTEM igazolás tárolót célként, adja meg a *SYSTEM tároló jelszavát, és kattintson a **Folytatás** gombra. A megjelenő üzenet az igazolás sikeres exportálását jelzi, vagy hiba információkat közöl, ha az exportálási folyamat meghiúsult.
12. Most exportálhatja a szerver vagy kliens igazolást a *SYSTEM igazolás tárolóba. Válassza újra az **Igazolás exportálása** feladatot.
13. Válassza a **Szerver vagy kliens** lehetőséget az exportálásra szánt igazolás típusának, és kattintson a **Folytatásra**.
14. Válassza ki a megfelelő, exportálandó szerver vagy kliens igazolást, és kattintson az **Export** gombra.
15. Válassza ki az exportált igazolás célpontját jelentő **Igazolás tárolót**, és kattintson a **Folytatás** gombra.
16. Írja be a *SYSTEM igazolás tárolót célként, adja meg a *SYSTEM tároló jelszavát, és kattintson a **Folytatás** gombra. A megjelenő üzenet az igazolás sikeres exportálását jelzi, vagy hiba információkat közöl, ha az exportálási folyamat meghiúsult.
17. Most hozzárendelheti az igazolást az alkalmazásokhoz SSL kapcsolat céljából. Kattintson az **Igazolás tároló választása**, majd a ***SYSTEM** elemre, az igazolás tároló megnyitása céljából.

18. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót a *SYSTEM igazolás tárolóhoz, és kattintson a **Folytatás** gombra.
19. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
20. A feladatlistán válassza az **Igazolás hozzárendelése** feladatot az aktuális igazolás tárolóban lévő igazolások listájának megjelenítéséhez.
21. Válassza ki a *hoszt* rendszeren létrehozott igazolást, és kattintson az **Alkalmazásokhoz rendelés** feladatra, hogy megjelenjen az SSL kapcsolatra felkészített alkalmazások listája, amelyekhez hozzárendelheti az igazolást.
22. Válassza ki az alkalmazásokat, amelyek használni fogják az igazolást az SSL szekciókhoz, és kattintson a **Folytatás** gombra. A DCM egy megerősítő üzenetet ad ki, amely szerint az igazolás kiválasztása megtörtént az alkalmazások számára.

    Megjegyzés: Egyes SSL képes alkalmazások támogatják az igazoláson alapuló kliens hitelesítést. Az ilyen támogatással rendelkező alkalmazás képes az igazolások hitelesítésére az erőforrásokhoz való hozzáférés előtt. Következésképpen, meg kell határozni a megbízható CA-k listáját az alkalmazás számára. Ez biztosítja azt, hogy az alkalmazás csak azokat az igazolásokat fogja érvényesíteni, amelyeket a megadott listán szereplő CA adott ki. Ha a felhasználó vagy a kliens alkalmazás olyan CA-tól kapott igazolást mutat be, amelyik nincs megadva a megbízható CA-k listáján, az alkalmazás nem fogja azt elfogadni érvényes hitelesítés alapjául.

A fenti feladatok végrehajtásával a célrendszeren lévő alkalmazások használni tudják a Helyi CA által kiadott igazolásokat más iSeries szerveren. Azonban, mielőtt használhatnák az adott alkalmazások az SSL kapcsolatokat, konfigurálja az alkalmazásokat az SSL használatához.

Mielőtt a felhasználó elérhetné a kiválasztott alkalmazásokat az SSL kapcsolaton keresztül, a felhasználó a DCM segítségével beszerzi a Helyi CA igazolás egy példányát a hoszt rendszertől. A Helyi CA igazolást egy fájlba kell átmásolni a felhasználó PC-jére, vagy le kell tölteni a felhasználó böngészőjébe, az SSL képes alkalmazás követelményeitől függően.

Magán igazolás használata SSL szekciókban V5R1 célrendszeren

A Digitális igazolás kezelő (DCM) *SYSTEM igazolás tárolójában lévő igazolásokat az alkalmazások használják SSL szekciók létesítéséhez. Ha az SSL szekciók létesítésére szolgáló igazolások kezeléséhez sohasem használt DCM-et a V5R1 célrendszeren, akkor ez az igazolás tároló nem található meg a célrendszeren. A Helyi igazolási hatóság (CA) hoszt rendszerén létrehozott és a célrendszernek átküldött igazolás tároló fájlok használatára vonatkozó feladatok aszerint változnak, hogy létezik-e a *SYSTEM igazolás tároló. Ha a *SYSTEM igazolás tároló nem létezik, akkor az átvitt igazolás fájlok azt jelentik, hogy létre kell hozni a *SYSTEM igazolás tárolót. Ha létezik a *SYSTEM igazolás tároló a V5R2 szintű célrendszeren, akkor az átvitt igazolás fájlok használatához a következő két módszer egyikét választhatja:

- Átvitt fájlok használata más rendszer igazolás tárolójaként.
- Átvitt fájlok importálása a meglévő *SYSTEM igazolás tárolóba.

*SYSTEM igazolás tároló nem létezik

Ha a *SYSTEM igazolás tároló nem létezik a V5R1 rendszeren, amelyen használni akarja az átvitt igazolás tároló fájlokat, akkor az átvitt igazolás fájlokat *SYSTEM igazolás tárolóként használhatja. Kövesse az alábbi lépéseket az igazolás fájlok V5R1 célrendszeren való használatához:

1. Bizonyosodjon meg arról, hogy a Helyi CA-t üzemeltető rendszeren létrehozott igazolás tároló fájlok (két fájl: egyik .KDB, másik .RDB kiterjesztésű) a /QIBM/USERDATA/ICSS/CERT/SERVER alkönyvtárban vannak.
2. Amint az átvitt igazolás fájlok a /QIBM/USERDATA/ICSS/CERT/SERVER alkönyvtárban vannak, nevezze át őket DEFAULT.KDB és DEFAULT.RDB névre. Azzal, hogy a fájlokat átnevezi a megfelelő alkönyvtárban, olyan komponenseket hoz létre, amelyek a *SYSTEM igazolás tárolót alkotják a célrendszer számára. Az igazolás tároló fájlok már tartalmazzák több nyilvános Internet CA igazolásának egy másolatát. Mindezt, valamint a Helyi CA igazolást a DCM adta hozzá az igazolás tároló fájlokhoz a létrehozás során.

   Figyelem: Ha a célrendszeren megtalálhatók a DEFAULT.KDB és a DEFAULT.RDB fájlok a /QIBM/USERDATA/ICSS/CERT/SERVER alkönyvtárban, akkor a *SYSTEM igazolás tároló pillanatnyilag létezik az adott célrendszeren. Következésképpen, nem kell átnevezni az átvitt fájlokat a javaslatnak megfelelően. Az alapértelmezett fájlok felülírása problémákat okoz, amikor a DCM-et, az átvitt igazolás tárolót és annak tartalmát használja. Helyette bizonyosodjon meg, hogy egyedi nevük van, és az átvitt igazolás tárolót **Más rendszer igazolás tárolójaként** használja. Ha a fájlokat Más rendszer igazolás tárolójaként használja, akkor nem tudja megadni a DCM segítségével, hogy mely alkalmazások használják az igazolásokat.
3. DCM indítása. Meg kell változtatni az átvitt fájlok átnevezésével létrehozott *SYSTEM igazolás tárolóra vonatkozó jelszót. A jelszó módosítása lehetővé teszi, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az igazolás tárolóban.
4. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SYSTEM** elemre, az igazolás tároló megnyitása céljából.
5. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót, amelyet a *hoszt* rendszeren adott meg az igazolás tárolónak, amikor igazolást hozott létre a V5R1 célrendszer számára, és kattintson a **Folytatás** gombra.
6. A navigációs kereten válassza ki az **Igazolás tároló kezelése**, majd a **Jelszó módosítása** feladatokat a listából. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához. Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat. Utána megadhatja, hogy mely alkalmazások használjanak igazolást az SSL szekciókhoz.
7. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SYSTEM** elemre, az igazolás tároló megnyitása céljából.
8. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az új jelszót, majd kattintson a **Folytatás** gombra.
9. Miután frissül a navigációs keret, válassza az **Alkalmazások kezelését** a navigációs keretben a feladatlista megjelenítéséhez.
10. A feladatlistán válassza az **Igazolás hozzárendelés frissítését**, hogy megjelenjenek azok az SSL képes alkalmazások, amelyekhez hozzárendelhet igazolást.
11. Válasszon ki egy alkalmazást a listából, és kattintson az **Igazolás hozzárendelés frissítésére**.
12. Válassza ki a *hoszt* rendszeren lévő Helyi CA által kiadott igazolást, és kattintson az **Új igazolás hozzárendelésére**. A DCM egy megerősítő üzenetet ad ki, amely szerint az igazolás kiválasztása megtörtént az alkalmazás számára.

    Megjegyzés: Egyes SSL képes alkalmazások támogatják az igazoláson alapuló kliens hitelesítést. Az ilyen támogatással rendelkező alkalmazás képes az igazolások hitelesítésére az erőforrásokhoz való hozzáférés előtt. Következésképpen, meg kell határozni a megbízható CA-k listáját az alkalmazás számára. Ez biztosítja azt, hogy az alkalmazás csak azokat az igazolásokat fogja érvényesíteni, amelyeket a megadott listán szereplő CA adott ki. Ha a felhasználó vagy a kliens alkalmazás olyan CA-tól kapott

igazolást mutat be, amelyik nincs megadva a megbízható CA-k listáján, az alkalmazás nem fogja azt elfogadni érvényes hitelesítés alapjául.

A fenti feladatok végrehajtásával a célrendszeren lévő alkalmazások használni tudják a Helyi CA által kiadott igazolásokat más iSeries szerveren. Azonban, mielőtt használhatnák az adott alkalmazások az SSL kapcsolatokat, konfigurálja az alkalmazásokat az SSL használatához.

Mielőtt a felhasználó elérhetné a kiválasztott alkalmazásokat az SSL kapcsolaton keresztül, a felhasználó a DCM segítségével beszerzi a Helyi CA igazolás egy példányát a hoszt rendszertől. A CA igazolást egy fájlba kell átmásolni a felhasználó PC-jére, vagy le kell tölteni a felhasználó böngészőjébe, az SSL képes alkalmazás követelményeitől függően.

***SYSTEM igazolás tároló létezik — fájlok használata Más rendszer igazolás tárolójaként**

Ha a V5R1 célrendszeren már van *SYSTEM igazolás tároló, akkor döntse el, hogyan kezeli az igazolás fájlokat. Választhatja azt, hogy az átvitt igazolás fájlokat **Más rendszer igazolás tárolójaként** használja. Választhatja azt is, hogy importálja a magán igazolást és a neki megfelelő Helyi CA igazolást a meglévő *SYSTEM igazolás tárolóba.

Ezek a tárolók valójában felhasználó által megadott másodlagos igazolás tárolók az SSL igazolások számára. Felhasználó által írt SSL képes alkalmazásoknak (amelyek nem használnak DCM API-kat az alkalmazás ID regisztráltatásához) szánt igazolások számára hozhatja létre és használhatja. Az Egyéb rendszer igazolás tároló nevű opció lehetővé teszi az igazolások kezelését olyan alkalmazások számára, amelyeket az SSL_Init API használatára írtak, hogy az SSL szekciók létesítéséhez szükséges igazolások programozottan elérhetők és használhatók legyenek. Ez az API lehetővé teszi az alkalmazásnak, hogy az igazolás tárolóhoz rendelt alapértelmezett igazolást használja, és ne azt, amelyet a felhasználó kifejezetten megadott.

Az IBM iSeries alkalmazások (és számos más szoftverfejlesztő alkalmazása) csak a *SYSTEM igazolás tárolóban őrzött igazolásokat tudják használni. Ha úgy dönt, hogy az átvitt fájlokat Más rendszer igazolás tárolójaként használja, akkor nem tudja megadni a DCM segítségével, hogy mely alkalmazások használják az igazolásokat SSL szekcióhoz. Következésképpen, a szabványos iSeries SSL kapcsolatra felkészített alkalmazásokat nem lehet konfigurálni az adott igazolás használatára. Ha az igazolást fel akarja használni az iSeries alkalmazásokhoz, először importálja az igazolást az átvitt igazolás tároló fájlokból a *SYSTEM igazolás tárolóba.

Kövesse az alábbi lépéseket, ha az átvitt igazolás fájlokat Más rendszer igazolás tárolójaként kívánja elérni és kezelni:

1. DCM indítása.
2. A navigációs kereten kattintson az **Igazolás tároló választása** elemre, majd válassza a **Más rendszer igazolás tárolóját**, mint megnyitandó igazolás tárolót.
3. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az igazolás tároló fájl teljes elérési útvonalát és nevét (az egyik .KDB kiterjesztésű), amelyet átvitt a hoszt rendszerről. Adja meg a jelszót, amelyet a *hoszt* rendszeren adott meg az igazolás tárolónak, amikor igazolást hozott létre a V5R1 célrendszer számára, és kattintson a **Folytatás** gombra.
4. A navigációs kereten válassza ki az **Igazolás tároló kezelése**, majd a **Jelszó módosítása** feladatokat a listából. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához.

   Megjegyzés: Ne felejtse el kiválasztani az **Automatikus bejelentkezés** opciót, amikor megváltoztatja az igazolás tároló jelszavát. Az opció használata biztosítja azt, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az új tárolóban.

Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat. Azután megadhatja, hogy a tárolóban lévő igazolás alapértelmezett igazolásként használatos-e.

5. A navigációs kereten kattintson az **Igazolás tároló választása** elemre, majd válassza a **Más rendszer igazolás tárolóját**, mint megnyitandó igazolás tárolót.
6. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az igazolás tároló fájl teljes elérési útvonalát és nevét, az új jelszót, és kattintson a **Folytatás** gombra.
7. Miután a navigációs keret frissül, válassza ki az **Igazolás tároló kezelése**, majd az **Alapértelmezett igazolás beállítása** feladatokat a listából.

Most, hogy létrehozta és konfigurálta a Más rendszer igazolás tárolóját, az SSL_Init API-t alkalmazó bármely alkalmazás használhatja a benne tárolt igazolást SSL szekció létesítéséhez.

***SYSTEM igazolás tároló létezik — meglévő *SYSTEM igazolás tárolóban lévő igazolások használata**

A V5R1 rendszer egy meglévő *SYSTEM igazolás tárolójában található (átvitt) igazolás tároló fájlokban lévő igazolásokat szintén használhatja. Ehhez importálni kell az igazolásokat az igazolás tároló fájlokból a meglévő *SYSTEM igazolás tárolóba. Azonban, az igazolásokat nem lehet közvetlenül importálni a .KDB és az .RDB fájlokból, mivel a formátumuk nem olyan, amelyet a DCM import funkciója felismerhetne vagy használhatna. Ahhoz, hogy használhassa az átvitt igazolásokat egy meglévő *SYSTEM igazolás tárolóból, a fájlokat Más rendszer igazolás tárolójaként nyissa meg, majd exportálja őket a *SYSTEM igazolás tárolóba.

Megjegyzés: Az eljárás leírja, hogyan használhatja fel Más rendszer igazolás tárolóját a célrendszeren ahhoz, hogy exportálja az igazolásokat az igazolás tároló fájlokból a *SYSTEM igazolás tárolóba. Az igazolások *SYSTEM igazolás tárolóhoz adásával elkerülheti a lehetséges problémák előfordulását, amikor a célrendszer gyengébb rejtjelezést nyújtó terméket (mint például 5722–AC2) használ, mint a hoszt rendszer.

Hajtsa végre az alábbi lépéseket a V5R1 célrendszeren, hogy exportálja az igazolásokat az igazolás tároló fájlokból a *SYSTEM igazolás tárolóba:

1. DCM indítása.
2. A navigációs kereten kattintson az **Igazolás tároló választása** elemre, majd adja meg a **Más rendszer igazolás tárolóját**, mint megnyitandó igazolás tárolót.
3. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az igazolás tároló fájl teljes elérési útvonalát és nevét (az egyik .KDB kiterjesztésű), amelyet átvitt a hoszt rendszerről. Adja meg a jelszót, amelyet a *hoszt* rendszeren adott meg az igazolás tárolónak, amikor igazolást hozott létre a V5R1 célrendszer számára, és kattintson a **Folytatás** gombra.
4. A navigációs kereten válassza ki az **Igazolás tároló kezelése**, majd a **Jelszó módosítása** feladatokat a listából. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához.

   Megjegyzés: Ne felejtse el kiválasztani az **Automatikus bejelentkezés** opciót, amikor megváltoztatja az igazolás tároló jelszavát. Az opció használata biztosítja azt, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az új tárolóban. Ha nem változtatja meg a jelszót és nem választja ki az Automatikus bejelentkezést, hibákkal számolhat, amikor az igazolásokat exportálja innen a *SYSTEM igazolás tárolóba.

   Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat.

5. A navigációs kereten kattintson az **Igazolás tároló választása** elemre, majd válassza a **Más rendszer igazolás tárolóját**, mint megnyitandó igazolás tárolót.
6. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az igazolás tároló fájl teljes elérési útvonalát és nevét, az új jelszót, és kattintson a **Folytatás** gombra.
7. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a navigációs keretben a feladatlista megjelenítéséhez, majd válassza az **Igazolás exportálását**.
8. Válassza az **Igazolási hatóságot (CA)** az exportálásra szánt igazolás típusának, és kattintson a **Folytatásra**.

   Megjegyzés: A Helyi CA igazolást exportálja az igazolás tárolóba, mielőtt szerver vagy kliens igazolást exportálna ugyanoda. Ha először szerver vagy kliens igazolást exportál, hibajelzést kaphat, mivel a Helyi CA igazolás nem található az igazolás tárolóban.
9. Válassza ki az exportálandó Helyi CA igazolást, és kattintson az **Export** gombra.
10. Válassza ki az exportált igazolás célpontját jelentő **Igazolás tárolót**, és kattintson a **Folytatás** gombra.
11. Írja be a *SYSTEM igazolás tárolót célként, adja meg a *SYSTEM tároló jelszavát, és kattintson a **Folytatás** gombra.
12. Most exportálhatja a szerver vagy kliens igazolást a *SYSTEM igazolás tárolóba. Válassza újra az **Igazolás exportálása** feladatot.
13. Válassza a **Szerver vagy kliens** lehetőséget az exportálásra szánt igazolás típusának, és kattintson a **Folytatásra**.
14. Válassza ki a megfelelő, exportálandó szerver vagy kliens igazolást, és kattintson az **Export** gombra.
15. Válassza ki az exportált igazolás célpontját jelentő **Igazolás tárolót**, és kattintson a **Folytatás** gombra.
16. Írja be a *SYSTEM igazolás tárolót célként, adja meg a *SYSTEM tároló jelszavát, és kattintson a **Folytatás** gombra. A megjelenő üzenet az igazolás sikeres exportálását jelzi, vagy hiba információkat közöl, ha az exportálási folyamat meghiúsult.
17. Most hozzárendelheti az igazolást az alkalmazásokhoz SSL kapcsolat céljából. Kattintson az **Igazolás tároló választása**, majd a ***SYSTEM** elemre, az igazolás tároló megnyitása céljából.
18. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg a jelszót a *SYSTEM igazolás tárolóhoz, és kattintson a **Folytatás** gombra.
19. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
20. A feladatlistán válassza az **Igazolás hozzárendelés frissítését**, hogy megjelenjenek azok az SSL képes alkalmazások, amelyekhez hozzárendelhet igazolást.
21. Válasszon ki egy alkalmazást a listából, és kattintson az **Igazolás hozzárendelés frissítésére**.
22. Válassza ki a *hoszt* rendszeren lévő Helyi CA által kiadott igazolást, és kattintson az **Új igazolás hozzárendelésére**. A DCM egy megerősítő üzenetet ad ki, amely szerint az igazolás kiválasztása megtörtént az alkalmazás számára.

    Megjegyzés: Egyes SSL képes alkalmazások támogatják az igazoláson alapuló kliens hitelesítést. Az ilyen támogatással rendelkező alkalmazás képes az igazolások hitelesítésére az erőforrásokhoz való hozzáférés előtt. Következésképpen, meg kell határozni a megbízható CA-k listáját az alkalmazás számára. Ez biztosítja azt, hogy az alkalmazás csak azokat az igazolásokat fogja érvényesíteni, amelyeket a megadott listán szereplő CA adott ki. Ha a felhasználó vagy a kliens alkalmazás olyan CA-tól kapott igazolást mutat be, amelyik nincs megadva a megbízható CA-k listáján, az alkalmazás nem fogja azt elfogadni érvényes hitelesítés alapjául.

A fenti feladatok végrehajtásával a célrendszeren lévő alkalmazások használni tudják a Helyi CA által kiadott igazolásokat más iSeries szerveren. Azonban, mielőtt használhatnák az adott alkalmazások az SSL kapcsolatokat, konfigurálja az alkalmazásokat az SSL használatához.

Mielőtt a felhasználó elérhetné a kiválasztott alkalmazásokat az SSL kapcsolaton keresztül, a felhasználó a DCM segítségével beszerzi a Helyi CA igazolás egy példányát a hoszt rendszertől. A CA igazolást egy fájlba kell átmásolni a felhasználó PC-jére, vagy le kell tölteni a felhasználó böngészőjébe, az SSL képes alkalmazás követelményeitől függően.

Magán igazolás használata objektum aláíráshoz V5R1 vagy V5R2 célrendszeren

A Digitális igazolás kezelő (DCM) *OBJECTSIGNING igazolás tárolójában lévő igazolásokat objektumok aláírására használhatja és kezelheti. Ha az objektumok aláírására szolgáló igazolások kezeléséhez sohasem használt DCM-et a célrendszeren, akkor ennek az igazolás tárolónak nem kell a célrendszeren lenni. A Helyi CA hoszt rendszerén létrehozott és a célrendszernek átküldött igazolás tároló fájlok használatához elvégzendő feladatok aszerint változnak, hogy létezik-e az *OBJECTSIGNING igazolás tároló. Ha az *OBJECTSIGNING igazolás tároló nem létezik, akkor az átvitt igazolás fájlok azt jelentik, hogy létre kell hozni az *OBJECTSIGNING igazolás tárolót. Ha az *OBJECTSIGNING igazolás tároló létezik a célrendszeren, akkor importálja ide az átvitt igazolásokat.

***OBJECTSIGNING igazolás tároló nem létezik**

A Helyi CA hoszt rendszerén létrehozott igazolás tároló fájlok használatához elvégzendő feladatok aszerint változnak, hogy használt-e valaha is DCM-et a célrendszeren objektum aláíró igazolások kezeléséhez.

Kövesse az alábbi lépéseket, ha nincs *OBJECTSIGNING igazolás tároló a V5R1 vagy a V5R2 célrendszeren, ahol az átvitt igazolás tároló fájlok találhatók:

1. Bizonyosodjon meg arról, hogy a Helyi CA-t üzemeltető rendszeren létrehozott igazolás tároló fájlok (két fájl: egyik .KDB, másik .RDB kiterjesztésű) a /QIBM/USERDATA/ICSS/CERT/SIGNING alkönyvtárban vannak.
2. Amint az átvitt igazolás fájlok a /QIBM/USERDATA/ICSS/CERT/SIGNING alkönyvtárban vannak, nevezze át őket SGNOBJ.KDB és SGNOBJ.RDB névre, ha szükséges. Azzal, hogy a fájlokat átnevezi a megfelelő alkönyvtárban, olyan komponenseket hoz létre, amelyek az *OBJECTSIGNING igazolás tárolót alkotják a célrendszer számára. Az igazolás tároló fájlok már tartalmazzák több nyilvános Internet CA igazolásának egy másolatát. Mindezt, valamint a Helyi CA igazolást a DCM adta hozzá az igazolás tároló fájlokhoz a létrehozás során.

   Figyelem: Ha a célrendszeren megtalálhatók az SGNOBJ.KDB és az SGNOBJ.RDB fájlok a /QIBM/USERDATA/ICSS/CERT/SIGNING alkönyvtárban, akkor az *OBJECTSIGNING igazolás tároló pillanatnyilag létezik az adott célrendszeren. Következésképpen, nem kell átnevezni az átvitt fájlokat a javaslatnak megfelelően. Az alapértelmezett objektum aláíró fájlok felülírása problémákat okoz, amikor a DCM-et, az átvitt igazolás tárolót és annak tartalmát használja. A fájlokból kétféleképpen kerülhetnek az igazolások az *OBJECTSIGNING igazolás tárolóba. A fájlban lévő igazolásokat exportálja ki egy sima fájlkészletbe, ahonnan importálhatja őket a meglévő *OBJECTSIGNING igazolás tárolóba. A másik lehetőség, hogy Más rendszer igazolás tárolójaként nyitja meg az átvitt fájlokat, és az ott lévő igazolásokat közvetlenül az *OBJECTSIGNING igazolás tárolóba exportálja. Bármelyik utat is követi, az igazolásoknak az *OBJECTSIGNING igazolás tárolóban kell lenni ahhoz, hogy kezelni tudja az őket alábbiak szerint használó alkalmazásokat.

3. DCM indítása. Meg kell változtatni az *OBJECTSIGNING igazolás tárolóra vonatkozó jelszót. A jelszó módosítása lehetővé teszi, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az igazolás tárolóban.
4. A navigációs kereten kattintson az **Igazolás tároló választására**, majd válassza ki a megnyitandó ***OBJECTSIGNING** igazolás tárolót.
5. Amikor a jelszó lap megjelenik, adja meg a jelszót, amelyet a hoszt rendszeren történt létrehozáskor adott meg az igazolás tárolóra, és kattintson a **Folytatás** gombra.
6. A navigációs kereten válassza ki az **Igazolás tároló kezelése**, majd a **Jelszó módosítása** feladatokat a listából. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához. Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat. Utána létrehozhat alkalmazás definíciót, hogy az igazolás segítségével objektumokat írjon alá.
7. Az igazolás tároló ismételt megnyitása után válassza az **Alkalmazások kezelését** a navigációs keretben a feladatlista megjelenítéséhez.
8. A feladatlistából válassza az **Alkalmazás hozzáadását**, hogy elkezdődjön az objektum aláíró alkalmazás definíció létrehozásának folyamata, ami révén az igazolás segítségével objektumokat írhat alá.
9. Töltse ki az űrlapot, hogy meghatározza az objektum aláíró alkalmazást, és kattintson a **Hozzáadás** gombra. Ez az alkalmazás definíció nem írja le ugyan az aktuális alkalmazást, viszont leírja azokat az objektum típusokat, amelyeket tervei szerint aláír a speciális igazolással. Az űrlap kitöltéséhez használja az online súgót.
10. Kattintson az **OK** gombra, hogy nyugtázza az alkalmazás definíció jóváhagyást kérő üzenetét, és megjelenjen az **Alkalmazások kezelése** feladatlista.
11. A feladatlistán válassza az **Igazolás hozzárendelés frissítését**, hogy megjelenjenek azok az objektum aláíró alkalmazás azonosítók (ID), amelyekhez hozzárendelhet igazolást.
12. Válasszon ki egy alkalmazás ID-t a listából, és kattintson az **Igazolás hozzárendelés frissítésére**.
13. Válassza ki a hoszt rendszeren lévő Helyi CA által létrehozott igazolást, és kattintson az **Új igazolás hozzárendelésére**.

Amikor befejezi a feladatokat, minden rendelkezésére áll ahhoz, hogy elkezdje az objektumok aláírását, hogy azok sérthetetlenségét garantálja.

Amikor aláírt objektumokat terjeszt, az objektumokat fogadóknak V5R1 vagy V5R2 DCM változatot kell használni az objektumokon lévő aláírás ellenőrzéséhez, hogy bizonyosak legyenek abban, az adatok nem változtak, és ellenőrizni tudják a küldő azonosságát. A fogadónak rendelkeznie kell az aláírás ellenőrző igazolás egy példányával ahhoz, hogy érvényesítse (ellenőrizze) az aláírást. Az aláírt objektumok részeként biztosítania kell az igazolás egy példányát.

A fogadónak rendelkeznie kell a CA igazolás egy példányával, mégpedig arra a CA-ra vonatkozóan, amelyik által kiadott igazolást használja az objektum aláírásához. Ha egy jólismert Internet CA-tól eredő igazolással írja alá az objektumokat, a fogadónál lévő DCM verziójának már rendelkeznie kell a szükséges CA igazolás egy példányával. Mindazonáltal, küldje el a CA igazolás egy példányát (egy külön csomagban) az aláírt objektummal egyetemben, ha szükséges. Például, a helyi CA igazolás egy példányát küldje el, ha az objektumokat a helyi CA által kiadott igazolással írta alá. Biztonsági okokból egy külön csomagban küldje el a CA igazolást, vagy nyilvánosan tegye elérhetővé a CA igazolást azoknak, akiknek szükségük van rá.

*OBJECTSIGNING igazolás tároló létezik

A V5R1 vagy V5R2 rendszer egy meglévő *OBJECTSIGNING igazolás tárolójában található (átvitt) igazolás tároló fájlokban lévő igazolásokat szintén használhatja. Ehhez importálni kell az igazolásokat az igazolás tároló fájlokból a meglévő *OBJECTSIGNING igazolás tárolóba.

Azonban, az igazolásokat nem lehet közvetlenül importálni a .KDB és az .RDB fájlokból, mivel a formátumuk nem olyan, amelyet a DCM import funkciója felismerhetne vagy használhatna. Az igazolásokat hozzáadhatja a meglévő *OBJECTSIGNING igazolás tárolóhoz, ha Más rendszer igazolás tárolójaként nyitja meg az átvitt fájlokat a V5R2 vagy V5R1 célrendszeren. Az igazolásokat azután közvetlenül exportálhatja az *OBJECTSIGNING igazolás tárolóba. Az objektum aláíró igazolás mellett exportálja a Helyi CA igazolást is az átvitt fájlokból.

Hajtsa végre az alábbi lépéseket a V5R1 vagy V5R2 célrendszeren, hogy exportálja az igazolásokat az igazolás tároló fájlokból közvetlenül az *OBJECTSIGNING igazolás tárolóba:

1. DCM indítása.
2. A navigációs kereten kattintson az **Igazolás tároló választása** elemre, majd adja meg a **Más rendszer igazolás tárolóját**, mint megnyitandó igazolás tárolót.
3. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az igazolás tároló fájlok teljes elérési útvonalát és nevét. Adja meg a jelszót, amelyet a hoszt rendszeren használt a létrehozásukkor, és kattintson a **Folytatás** gombra.
4. A navigációs kereten válassza ki az **Igazolás tároló kezelése**, majd a **Jelszó módosítása** feladatokat a listából. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához.

   Megjegyzés: Ne felejtse el kiválasztani az **Automatikus bejelentkezés** opciót, amikor megváltoztatja az igazolás tároló jelszavát. Az opció használata biztosítja azt, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az új tárolóban. Ha nem változtatja meg a jelszót és nem választja ki az Automatikus bejelentkezést, hibákkal számolhat, amikor az igazolásokat exportálja innen a *OBJECTSIGNING igazolás tárolóba.

   Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat.
5. A navigációs kereten kattintson az **Igazolás tároló választása** elemre, majd válassza a **Más rendszer igazolás tárolóját**, mint megnyitandó igazolás tárolót.
6. Amikor az Igazolás tároló és jelszó lap megjelenik, adja meg az igazolás tároló fájl teljes elérési útvonalát és nevét, az új jelszót, és kattintson a **Folytatás** gombra.
7. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a navigációs keretben a feladatlista megjelenítéséhez, majd válassza az **Igazolás exportálását**.
8. Válassza az **Igazolási hatóságot (CA)** az exportálásra szánt igazolás típusának, és kattintson a **Folytatásra**.

   Megjegyzés: A feladat leírása során feltételezzük, hogy a Más rendszer igazolás tárolójával való munka során szerver vagy kliens igazolásokkal dolgozik. Ez azért van, mert ez az igazolás tároló típus van kijelölve másodlagos tárolónak a *SYSTEM igazolás tárolóhoz. Azonban, ha itt használja az exportálási funkciót, a legegyszerűbben hozzáadhatja az átvitt fájlokban lévő igazolásokat a meglévő *OBJECTSIGNING igazolás tárolóhoz.
9. Válassza ki az exportálandó Helyi CA igazolást, és kattintson az **Export** gombra.

   Megjegyzés: A Helyi CA igazolást exportálja az igazolás tárolóba, mielőtt objektum aláíró igazolást exportálna ugyanoda. Ha először objektum aláíró igazolást exportál, hibajelzést kaphat, mivel a Helyi CA igazolás nem található az igazolás tárolóban.
10. Válassza ki az exportált igazolás célpontját jelentő **Igazolás tárolót**, és kattintson a **Folytatás** gombra.
11. Írja be az *OBJECTSIGNING igazolás tárolót célként, adja meg a tároló jelszavát, és kattintson a **Folytatás** gombra.

12. Most exportálhatja az objektum aláíró igazolást az *OBJECTSIGNING igazolás tárolóba. Válassza újra az **Igazolás exportálása** feladatot.
13. Válassza a **Szerver vagy kliens** lehetőséget az exportálásra szánt igazolás típusának, és kattintson a **Folytatásra**.
14. Válassza ki a megfelelő exportálandó igazolást, és kattintson az **Export** gombra.
15. Válassza ki az exportált igazolás célpontját jelentő **Igazolás tárolót**, és kattintson a **Folytatás** gombra.
16. Írja be az *OBJECTSIGNING igazolás tárolót célként, adja meg az *OBJECTSIGNING igazolás tároló jelszavát, és kattintson a **Folytatás** gombra. A megjelenő üzenet az igazolás sikeres exportálását jelzi, vagy hiba információkat közöl, ha az exportálási folyamat meghiúsult.

    Megjegyzés: Ahhoz, hogy az igazolást objektumok aláírásához lehessen használni, rendelje hozzá az igazolást egy objektum aláíró alkalmazáshoz.

Magán igazolás használata SSL szekciókban V4R5 vagy V4R4 célrendszeren

A Digitális igazolás kezelő (DCM) *SYSTEM igazolás tárolójában lévő igazolásokat az alkalmazások használják SSL szekciók létesítéséhez. Ha az SSL szekciók létesítésére szolgáló igazolások kezeléséhez sohasem használt DCM-et a V4R5 vagy V4R4 célrendszeren, akkor ez az igazolás tároló nem található meg a célrendszeren. A Helyi CA hoszt rendszerén létrehozott igazolás tároló fájlok két igazolást tartalmaznak. A fájlok a létrehozott szerver vagy kliens igazolást, valamint a Helyi CA aláíráshoz használt magán igazolását tartalmazza.

Az átküldött igazolás tároló fájlok használatához elvégzendő feladatok aszerint változnak, hogy létezik-e az *SYSTEM igazolás tároló. Ha a *SYSTEM igazolás tároló nem létezik, akkor az átvitt igazolás fájlok azt jelentik, hogy létre kell hozni a *SYSTEM igazolás tárolót. Ha létezik a *SYSTEM igazolás tároló a célrendszeren, akkor az átvitt igazolás fájlok használatához a következő két módszer egyikét választhatja:
- Átvitt fájlok használata Más rendszer igazolás tárolójaként.
- Átvitt fájlok importálása a meglévő *SYSTEM igazolás tárolóba.

***SYSTEM igazolás tároló nem létezik**

Kövesse az alábbi lépéseket, ha a *SYSTEM igazolás tároló nem létezik a V4R5 vagy V4R4 rendszeren, amelyen használni akarja az átvitt igazolás tároló fájlokat:

1. Bizonyosodjon meg arról, hogy a Helyi CA-t üzemeltető rendszeren létrehozott igazolás tároló fájlok (két fájl: egyik .KDB, másik .RDB kiterjesztésű) a /QIBM/USERDATA/ICSS/CERT/SERVER alkönyvtárban vannak.
2. Amint az átvitt igazolás fájlok a /QIBM/USERDATA/ICSS/CERT/SERVER alkönyvtárban vannak, nevezze át őket DEFAULT.KDB és DEFAULT.RDB névre. Azzal, hogy a fájlokat átnevezi a megfelelő alkönyvtárban, olyan komponenseket hoz létre, amelyek a *SYSTEM igazolás tárolót alkotják a célrendszer számára. Az igazolás tároló fájlok már tartalmazzák több nyilvános Internet CA igazolásának egy másolatát. Mindezt, valamint a Helyi CA igazolást a DCM adta hozzá az igazolás tároló fájlokhoz a létrehozás során.

    Figyelem: Ha a célrendszeren megtalálhatók a DEFAULT.KDB és a DEFAULT.RDB fájlok a /QIBM/USERDATA/ICSS/CERT/SERVER alkönyvtárban, akkor a *SYSTEM igazolás tároló pillanatnyilag létezik az adott célrendszeren. Következésképpen, nem kell átnevezni az átvitt fájlokat a javaslatnak megfelelően. Az alapértelmezett fájlok felülírása problémákat okoz, amikor a DCM-et, az átvitt igazolás tárolót és annak tartalmát használja. Helyette bizonyosodjon meg, hogy egyedi nevük van, és az átvitt igazolás tárolót **Más rendszer igazolás tárolójaként** használja. Ha a fájlokat Más rendszer

igazolás tárolójaként használja, akkor nem tudja megadni a DCM segítségével, hogy mely alkalmazások használják az igazolásokat.

3. DCM indítása. Meg kell változtatni az *SYSTEM igazolás tárolóra vonatkozó jelszót. A jelszó módosítása lehetővé teszi, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az igazolás tárolóban.
4. A navigációs keretben ellenőrizze, hogy látható-e a *SYSTEM tároló a legördülő listán, és válassza a **Rendszer igazolásokat** a rendelkezésre álló feladatok felsorolásának megjelenítéséhez. Az **Igazolás tároló és jelszó** ablak jelenik meg.
5. A megfelelő mezőkre írja be a megnyitandó *SYSTEM igazolás tároló nevét, valamint a jelszót, melyet a hoszt rendszeren a Helyi CA segítségével létrehozott fájloknál alkalmazott. Ilyenkor megváltoztathatja az igazolás tároló jelszavát.
6. A navigációs keret feladatlistáján válassza a **Jelszó módosítását**. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához. Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat.
7. Miután újra megnyitja a *SYSTEM igazolás tárolót, a **Biztonságos alkalmazások kezelése** feladat kiválasztásával megjelenik egy oldal, ahol az alkalmazásokhoz tartozó igazolásokat kezelheti.
8. Az alkalmazások listájából válassza ki az alkalmazást, amely használni fogja az átvitt magán igazolást az SSL szekciókhoz.
9. Kattintson a **Rendszer igazolás kezelésére**, és válassza ki azt az igazolást, amelyet a Helyi CA adott ki a hoszt rendszeren.
10. Kattintson az **Új igazolás hozzárendelésére**, hogy a megrendelt alkalmazás használja a kiválasztott igazolást.

Megjegyzés: Egyes SSL képes alkalmazások támogatják az igazoláson alapuló kliens hitelesítést. Az igazolások használata kliens hitelesítéshez biztosítja azt, hogy az alkalmazás érvényes igazolást kapjon, mielőtt hozzáférést engedélyez az általa vezérelt erőforrásokhoz. Az ilyen támogatással rendelkező alkalmazásokat úgy kell konfigurálni, hogy kijelöljön egy CA-t (amiben megbízik), mielőtt az alkalmazás hitelesítené az adott CA által kiadott igazolásokat. Az **Igazolási hatóságok kezelése** oldal segítségével biztosíthatja, hogy a CA igazolás megbízható állapotú legyen az igazolás tárolóban. Utána a **Biztonságos alkalmazások kezelése** oldal segítségével biztosíthatja, hogy az igazolást használó alkalmazások számára megbízható legyen a Helyi CA, amely kiadta az igazolást. Ez biztosítja azt, hogy az alkalmazás csak azokat az igazolásokat fogja érvényesíteni, amelyeket a megadott listán szereplő CA adott ki. Ha a felhasználó vagy a kliens alkalmazás olyan CA-tól kapott igazolást mutat be, amelyik nincs megadva megbízhatónak, az alkalmazás nem fogja azt elfogadni érvényes hitelesítés alapjául.

A fenti feladatok végrehajtásával a V4R5 vagy V4R4 célrendszeren lévő alkalmazások használni tudják egy másik iSeries szerveren lévő V5R2 Helyi CA által kiadott igazolást. Azonban, mielőtt használhatnák az adott alkalmazások az SSL kapcsolatokat, konfigurálja az alkalmazásokat az SSL használatához.

Mielőtt a felhasználó elérhetné a kiválasztott alkalmazásokat az SSL kapcsolaton keresztül, a felhasználó a DCM segítségével beszerzi a Helyi CA igazolás egy példányát a hoszt rendszertől. A CA igazolást egy fájlba kell átmásolni a felhasználó PC-jére, vagy le kell tölteni a felhasználó böngészőjébe, az SSL képes alkalmazás követelményeitől függően.

*SYSTEM igazolás tároló létezik — fájlok használata Más rendszer igazolás tárolójaként

Ha a V4R5 vagy V4R4 célrendszeren már van *SYSTEM igazolás tároló, akkor döntse el, hogyan kezeli az igazolás fájlokat. Az átvitt igazolás tároló fájlok két igazolást tartalmaznak:

a létrehozott szerver vagy kliens igazolást, valamint a Helyi CA aláíráshoz használt magán igazolását tartalmazza. Választhatja azt, hogy az átvitt igazolás fájlokat **Más** rendszer igazolás tárolójaként használja. Választhatja azt is, hogy importálja a magán igazolást és a neki megfelelő Helyi CA igazolást a meglévő *SYSTEM igazolás tárolóba.

Ha úgy dönt, hogy az átvitt fájlokat **Más** rendszer igazolás tárolójaként használja, akkor nem tudja megadni a DCM segítségével, hogy mely alkalmazások használják az igazolásokat SSL szekcióhoz. Ugyanakkor kijelölheti az igazolást az igazolás tároló alapértelmezett igazolásának. Az Egyéb rendszer igazolás tároló nevű opció lehetővé teszi az igazolások kezelését olyan alkalmazások számára, amelyeket az SSL_Init API használatára írtak, hogy az SSL szekciók létesítéséhez szükséges igazolások programozottan elérhetők és használhatók legyenek. Ez az API lehetővé teszi az alkalmazásnak, hogy az igazolás tárolóhoz rendelt alapértelmezett igazolást használja, és ne egy adott igazolást.

Kövesse az alábbi lépéseket, ha a *SYSTEM igazolás tároló létezik a V4R5 vagy V4R4 rendszeren, amelyen használni akarja az átvitt igazolás tároló fájlokat:

1. DCM indítása. Meg kell változtatni az átvitt igazolás tárolóra vonatkozó jelszót. A jelszó módosítása lehetővé teszi, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az igazolás tárolóban.
2. A navigációs keretben ellenőrizze, hogy látható-e a Más (Other) tároló a legördülő listán, és válassza a **Rendszer igazolásokat** a rendelkezésre álló feladatok felsorolásának megjelenítéséhez. Az **Igazolás tároló és jelszó** ablak jelenik meg.
3. A megfelelő mezőkben adja meg az igazolás tároló fájl teljes elérési útvonalát és nevét (.KDB kiterjesztésű), amelyet a Helyi CA hoszt rendszeréről vitt át. Írja be a jelszót, amelyet a fájl *hoszt* rendszeren való létrehozásakor használt. Ilyenkor megváltoztathatja az igazolás tároló jelszavát.
4. A navigációs kereten válassza ki a **Jelszó módosítását** a rendszer igazolási feladatok közül. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához.

   Megjegyzés: Ne felejtse el kiválasztani az **Automatikus bejelentkezés** opciót, amikor megváltoztatja az igazolás tároló jelszavát. Az opció használata biztosítja azt, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az új tárolóban.

   Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat. Azután megadhatja, hogy a tárolóban lévő igazolás alapértelmezett igazolásként használatos-e.
5. A navigációs keretben az **Igazolások kezelése** feladat kiválasztásával megjelenik egy lap, ahol számos igazoláskezelési feladatot hajthat végre.
6. Az igazolások listájából válassza ki azt az igazolást, amelyet az aktuális tároló alapértelmezett igazolásának szán, és kattintson az **Alapértelmezés beállítására**.

Most, hogy létrehozta és konfigurálta a Más rendszer igazolás tárolóját, az SSL_Init API-t alkalmazó bármely alkalmazás használhatja a benne tárolt igazolást SSL szekció létesítéséhez.

*SYSTEM igazolás tároló létezik — fájlok importálása meglévő *SYSTEM igazolás tárolóba

Mielőtt importálhatná az igazolásokat a *SYSTEM tárolóba V4R5 vagy V4R4 célrendszeren, először exportálja az igazolásokat a létrehozott igazolás tárolóból egy eltérő fájlformátumba. Azután importálhatja őket az új fájlokból a *SYSTEM igazolás tárolóba. Az átvitt igazolás tároló fájlok két igazolást tartalmaznak: a létrehozott szerver vagy kliens igazolást, valamint a Helyi CA aláíráshoz használt magán igazolását tartalmazza. Importálja a létrehozott szerver vagy kliens igazolásokat, valamint a Helyi CA magán igazolását is a *SYSTEM igazolás tárolóba.

Megjegyzés: A V4R5 vagy a V4R4 szintű DCM rendelkezésre álló exportálási funkciói nincsenek olyan mértékben kifejlesztve, mint a V5R2 esetében, és problémákat tapasztalhat, amikor a célrendszer segítségével exportálja a Helyi CA magán igazolását. Következésképpen, a V5R2 hoszt rendszer segítségével exportálja a Helyi CA igazolás *további* példányát egy külön fájlba, és ne a V4R4 vagy a V4R5 célrendszert használja az igazolás exportálására. Miután kiexportálta a Helyi CA igazolást a V5R2 hoszt rendszeren, manuálisan vigye át a Helyi CA igazolás exportált állományát a V4R4 vagy a V4R5 célrendszerre, és kövesse az eljárás később következő lépéseit, amellyel importálja a Helyi CA igazolást a *SYSTEM igazolás tárolóba. A Helyi CA igazolást azelőtt importálni kell, *mielőtt* importálja a magán igazolást, amelyet létrehozott vele. Ha először a magán igazolást importálja, hibajelzést kaphat, mivel a Helyi CA igazolás nem található az igazolás tárolóban.

Hajtsa végre az alábbi lépéseket a V4R5 vagy V4R4 célrendszeren, hogy exportálja az igazolást az igazolás tároló fájlokból:

1. DCM indítása.
2. A navigációs keretben ellenőrizze, hogy látható-e a Más (Other) tároló a legördülő listán, és válassza a **Rendszer igazolásokat** a rendelkezésre álló feladatok felsorolásának megjelenítéséhez. Az **Igazolás tároló és jelszó** ablak jelenik meg.
3. Adja meg az átvitt igazolás tároló fájlok teljes elérési útvonalát és nevét, az új jelszót, amelyet a *hoszt* rendszeren való létrehozásukkor használt, és kattintson az **OK** gombra. Ilyenkor megváltoztathatja az igazolás tároló jelszavát.
4. A navigációs kereten válassza ki a **Jelszó módosítását** a rendszer igazolási feladatok közül. Töltse ki az űrlapot az igazolás tároló jelszavának megváltoztatásához.

   Megjegyzés: Ne felejtse el kiválasztani az **Automatikus bejelentkezés** opciót, amikor megváltoztatja az igazolás tároló jelszavát. Az opció használata biztosítja azt, hogy a DCM tárolja az új jelszót, és ezáltal a DCM összes igazoláskezelési funkciója használható legyen az új tárolóban. Ha nem változtatja meg a jelszót és kiválasztja az Automatikus bejelentkezést, hibákkal számolhat, amikor az igazolásokat exportálja innen.

   Miután megváltoztatja a jelszót, újra meg kell nyitni az igazolás tárolót ahhoz, hogy kezelni tudja a benne levő igazolásokat.
5. A navigációs keretben válassza ki az **Igazolások kezelését** az igazolások listájának megjelenítéséhez.
6. Válassza ki a listából a magán igazolást, és kattintson az **Export** gombra az Igazolások exportálása lap megjelenítéséhez.
7. Töltse ki az Igazolások exportálása űrlapot.

   Megjegyzés: Bizonyosodjon meg arról, hogy a fájlnak egyedi nevet és kiterjesztést ad. Például adjon sajátfájl.exp nevet a fájlnak. Amikor nevet ad a fájlnak, ne használja a következő kiterjesztések egyikét sem a fájlhoz: .TXT, .KDB, .RDB vagy .KYR, mivel ezek hibát okozhatnak, amikor az igazolásokat importálja a fájlból. Válassza ki a célrendszer megfelelő kibocsátási szintjét, amely használni fogja az igazolást. A kiválasztott kibocsátási szint befolyásolja az exportált igazolás formátumát.
8. Kattintson az **OK** gombra. Az üzenet, amely szerint a DCM exportálta az igazolást a megadott fájlba, a lap tetején jelenik meg.

Ennél a pontnál használja a DCM-et az eredeti V5R2 hoszt rendszeren, exportálja a Helyi CA igazolás egy újabb példányát, és manuálisan vigye át a V4R4 vagy a V5R5 célrendszerre. Majd ugyanezen a célrendszeren a DCM segítségével exportálja a magán szerver vagy a kliens igazolást egy fájlba. Ezek után készen áll arra, hogy az így előkészített igazolásokat importálja a *SYSTEM igazolás tárolóba. A Helyi CA igazolást azelőtt importálni kell,

mielőtt importálja a magán igazolást, amelyet létrehozott vele. Ha először a magán igazolást importálja, hibajelzést kaphat, mivel a Helyi CA igazolás nem található az igazolás tárolóban.

Hajtsa végre az alábbi lépéseket a V4R5 vagy V4R4 célrendszeren ahhoz, hogy importálja az igazolásokat ezekből az exportált állományokból, és megadja az SSL kapcsolatra felkészített alkalmazásoknak az igazolások használatát:

1. DCM indítása.
2. A navigációs keretben ellenőrizze, hogy látható-e a *SYSTEM tároló a legördülő listán, és válassza a **Rendszer igazolásokat** a rendelkezésre álló feladatok felsorolásának megjelenítéséhez. Az **Igazolás tároló és jelszó** ablak jelenik meg.
3. Megnyitandó igazolás tárolónak adja meg a *SYSTEM tárolót, adja meg a jelszót, és kattintson a **Folytatásra**.
4. Most importálja a Helyi CA igazolást a V5R2 hoszt rendszeren létrehozott exportált állományból. A navigációs keretben válassza a **CA igazolás vételét** az űrlap megjelenéséhez.
5. Töltse ki, és kattintson az **OK** gombra az Igazolás vétele sikeres oldal megjelenítéséhez. Amikor a *SYSTEM igazolás tárolóban dolgozik, ez az oldal megjeleníti azoknak az alkalmazásoknak a listáját, melyek számára beállíthatja megbízhatónak az importált CA igazolást.

   Megjegyzés: Egyes SSL képes alkalmazások támogatják az igazoláson alapuló kliens hitelesítést. Az igazolások használata kliens hitelesítéshez biztosítja azt, hogy az alkalmazás érvényes igazolást kapjon, mielőtt hozzáférést engedélyez az általa vezérelt erőforrásokhoz. Az ilyen támogatással rendelkező alkalmazásokat úgy kell konfigurálni, hogy kijelöljön egy CA-t (amiben megbízik), mielőtt az alkalmazás hitelesítené az adott CA által kiadott igazolásokat. Ez biztosítja azt, hogy az alkalmazás csak azokat az igazolásokat fogja érvényesíteni, amelyeket a megadott listán szereplő CA adott ki. Ha a felhasználó vagy a kliens alkalmazás olyan CA-tól kapott igazolást mutat be, amelyik nincs megadva megbízhatónak, az alkalmazás nem fogja azt elfogadni érvényes hitelesítés alapjául.
6. Válassza ki azokat az alkalmazásokat, amelyek számára az adott CA igazolás megbízható, és kattintson az **OK** gombra. Megjelenik a Biztonságos alkalmazások állapota oldal, amely megerősíti, hogy a kiválasztott alkalmazások megbízhatónak ismerik el az új igazolást.
7. Most importálhatja a szerver igazolást. A navigációs keretben válassza ki az **Igazolások kezelését** az igazolások listájának megjelenítéséhez.
8. Kattintson az **Import** gombra az Igazolás importálása oldal megjelenítéséhez.
9. Töltse ki az Igazolás importálása űrlapot, és kattintson az **OK** gombra, hogy visszatérjen az Igazolások kezelése oldalhoz. Feltétlenül adja meg a fájl nevét, amely tartalmazza az exportált szerver vagy kliens igazolást, valamint a célváltozatot, ami megegyezik az igazolás korábbi exportálásakor megadottal. Az üzenet, amely szerint a DCM hozzáadta az igazolást a pillanatnyi igazolás tárolóhoz, a lap tetején jelenik meg. Az importált igazolásnak az igazolások listájában kell megjelenni.
10. Adja meg, hogy mely alkalmazások használják az importált magán igazolást az SSL szekciókhoz. A navigációs keretben a **Biztonságos alkalmazások kezelése** feladat kiválasztásával megjelenik egy lap, ahol az alkalmazásokhoz tartozó igazolásokat kezelheti.
11. Válasszon ki egy alkalmazást a listából, és kattintson a **Rendszer igazolás kezelésére** azon igazolások megjelenítéséhez, amelyeket megadhat a kiválasztott alkalmazáshoz SSL szekciók létesítése céljából.
12. Válassza ki az igazolást a listából, és kattintson az **Új igazolás hozzárendelésére**, hogy hozzárendelje a kiválasztott igazolást a megadott alkalmazáshoz. Az igazolás kiválasztását megerősítő üzenet jelenik meg az oldal tetején.

A fenti feladatok végrehajtásával a V4R4 vagy V4R5 célrendszeren lévő alkalmazások használni tudják egy másik iSeries szerveren lévő Helyi CA által kiadott igazolást. Azonban, mielőtt használhatnák az adott alkalmazások az SSL kapcsolatokat, konfigurálja az alkalmazásokat az SSL használatához.

Mielőtt a felhasználó elérhetné a kiválasztott alkalmazásokat az SSL kapcsolaton keresztül, a felhasználó a DCM segítségével beszerzi a Helyi CA igazolás egy példányát a hoszt rendszertől. A CA igazolást egy fájlba kell átmásolni a felhasználó PC-jére, vagy le kell tölteni a felhasználó böngészőjébe, az SSL képes alkalmazás követelményeitől függően.

Alkalmazások kezelése a DCM programban

A Digitális igazolás kezelő (DCM) segítségével különféle kezelési feladatokat hajthat végre SSL képes és objektum aláíró alkalmazásokon. Például kezelheti, hogy alkalmazásai mely igazolásokat használhatják Védett socket réteg (SSL) kommunikációs szekcióhoz. Az alkalmazás típusa és az igazolás tároló (amelyben dolgozik) alapján a végrehajtható alkalmazáskezelési feladatok változóak. Az alkalmazásokat csak a *SYSTEM vagy az *OBJECTSIGNING igazolás tárolóból kezelheti.

Míg a DCM által nyújtott alkalmazáskezelési feladatok többsége könnyen megismerhető, egy kevés részük kevésbé ismert marad. Az alábbi témakörök adnak további tájékoztatást ezekről a feladatokról:

Alkalmazás definíció létrehozása leírja az alkalmazások típusát, amelyet megadhat és kezelhet.

Igazolás hozzárendelések kezelése leírja az alkalmazás által SSL szekció létesítéséhez vagy objektumok aláírására használt igazolás hozzárendelésének és megváltoztatásának módját.

Megbízható CA lista megadása leírja, mikor kell és mikor tudja megadni, hogy mely Igazolási hatóságokat fogadhatja el megbízhatónak az alkalmazás az igazolások ellenőrzéséhez és elfogadásához.

A többi DCM feladatról szóló leírást az online súgó tartalmazza.

Alkalmazás definíció létrehozása

A DCM-ben két fajta alkalmazás definícióval dolgozhat: SSL protokollt használó szerver vagy kliens alkalmazások számára készült alkalmazás definíciókkal, valamint objektumok aláírásához készült definíciókkal.

Ahhoz, hogy a DCM kész legyen az SSL alkalmazás definíciókkal és igazolásaikkal való munkára, az alkalmazást regisztrálni kell a DCM segítségével, mint alkalmazás definíciót, amely egyedi alkalmazás ID-vel rendelkezik. Az alkalmazás fejlesztők API (QSYRGAP, QsyRegisterAppForCertUse) segítségével regisztrálják az SSL képes alkalmazásokat, hogy az alkalmazás ID automatikusan létrejöjjön a DCM-ben. Az összes IBM iSeries SSL képes alkalmazás regisztrációja a DCM segítségével történik, s így az igazolást is könnyedén hozzájuk rendelheti, hogy SSL szekciót tudjanak létesíteni. Az írt és a vásárolt alkalmazások számára is megadhat alkalmazás definíciót, és létrehozhat hozzá alkalmazás ID-t magán a DCM-en belül. A *SYSTEM igazolás tárolóban kell dolgoznia, amikor SSL alkalmazás definíciót hoz létre kliens- vagy szerver alkalmazások számára.

Ahhoz, hogy az igazolást objektumok aláírásához lehessen használni, először meg kell adni egy alkalmazást, amelyre az igazolást használja. Az SSL alkalmazás definícióval ellentétben, az objektum aláíró alkalmazás nem írja le a valódi alkalmazást. Helyette, a létrehozott alkalmazás definíció írja le az aláírni kívánt objektumcsoport típusát. Az *OBJECTSIGNING igazolás tárolóban kell dolgoznia, amikor objektum aláíró alkalmazás definíciót hoz létre.

Kövesse az alábbi lépéseket az alkalmazás definíció létrehozásához:

1. DCM indítása.
2. Kattintson az **Igazolás tároló választására**, majd válassza ki a megfelelő igazolás tárolót. (Az alkalmazás definíciótól - amit létrehoz - függően ez lehet a *SYSTEM vagy az *OBJECTSIGNING igazolás tároló.)

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az on-line súgó elérése céljából.
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. A navigációs kereten válassza az **Alkalmazások kezelését** a feladatlista megjelenítéséhez.
5. Válassza ki az **Alkalmazás hozzáadását** a feladatlistából, hogy megjelenítse az alkalmazás megadására szolgáló űrlapot.

   Megjegyzés: Ha a *SYSTEM igazolás tárolóban dolgozik, a DCM kérni fogja annak megadását, hogy a szerver vagy a kliens alkalmazás definíciót akarja-e hozzáadással bővíteni.
6. Töltse ki az űrlapot, és kattintson a **Hozzáadásra**. Az alkalmazás definícióra megadható információk változóak, függően az alkalmazás típusától, amelyet definiál. Ha éppen szerver alkalmazást definiál, megadhatja, hogy az alkalmazás használhat-e igazolásokat a kliens hitelesítéshez, és hogy szükség van-e kliens hitelesítésre. Azt is megadhatja, hogy az alkalmazásnak kötelező-e használni a megbízható CA-k listáját az igazolások hitelesítéséhez.

Igazolás hozzárendelése alkalmazáshoz

A Digitális igazolás kezelővel (DCM) kell hozzárendelni az igazolást az alkalmazáshoz, mielőtt az alkalmazás végrehajtana valamilyen biztonságos funkciót, mint például Védett socket réteg (SSL) szekció vagy objektum aláírás. Kövesse az alábbi lépéseket, ha igazolást akar hozzárendelni egy alkalmazáshoz, vagy ha az alkalmazásra vonatkozó igazolás hozzárendelést kívánja megváltoztatni:

1. DCM indítása.
2. Kattintson az **Igazolás tároló választására**, majd válassza ki a megfelelő igazolás tárolót. (Az alkalmazás típusától - amelyhez egy igazolást rendel hozzá - függően ez lehet a *SYSTEM vagy az *OBJECTSIGNING igazolás tároló.)

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az on-line súgó elérése céljából.
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. A navigációs kereten válassza az **Alkalmazások kezelését** a feladatlista megjelenítéséhez.
5. Ha a *SYSTEM igazolás tárolóban van, válassza ki a kezelni kívánt alkalmazástípust. (Értelemszerűen válassza a **Szerver** vagy a **Kliens** alkalmazást.)
6. A feladatlistán válassza az **Igazolás hozzárendelés frissítését**, hogy megjelenjenek azok az alkalmazások, amelyekhez hozzárendelhet igazolást.
7. Válasszon ki egy alkalmazást a listából, és kattintson az **Igazolás hozzárendelés frissítésére** azon igazolások megjelenítéséhez, amelyeket hozzárendelhet az adott alkalmazáshoz.
8. Válasszon ki egy igazolást a listából, és kattintson az **Új igazolás hozzárendelésére**. A DCM egy megerősítő üzenetet ad ki, amely szerint az igazolás kiválasztása megtörtént az alkalmazás számára.

   Megjegyzés: Ha olyan SSL képes alkalmazáshoz rendel hozzá igazolást, amelyik támogatja az igazolás felhasználását kliens hitelesítés céljára, adja meg a megbízható CA-k listáját az alkalmazás számára. Ez biztosítja azt, hogy az alkalmazás csak azokat az igazolásokat fogja érvényesíteni, amelyeket a

megadott listán szereplő CA adott ki. Ha a felhasználó vagy a kliens alkalmazás olyan CA-tól kapott igazolást mutat be, amelyik nincs megadva a megbízható CA-k listáján, az alkalmazás nem fogja azt elfogadni érvényes hitelesítés alapjául.

Amikor eltávolítja vagy megváltoztatja egy alkalmazás igazolását, az alkalmazás vagy felismeri vagy nem a változást, ha az alkalmazás éppen fut, miközben megváltoztatja az igazolás hozzárendelést. Például, a Client Access Express szerverek automatikusan alkalmazzák az igazolás változtatásokat, amelyeket végez. Azonban lehet, hogy le kell állítani és el kell indítani a Telnet szervereket (IBM HTTP Server for iSeries vagy más alkalmazások), mielőtt az alkalmazásokra érvényesülne az igazolásokban végrehajtott változtatások.

A V5R2 változattól kezdve használhatja az Igazolás hozzárendelés feladatot, amikor az igazolást egyszerre több alkalmazáshoz kívánja hozzárendelni.

Megbízható CA lista megadása alkalmazáshoz

Az olyan alkalmazások esetén, amelyek támogatják az igazolások felhasználását kliens hitelesítéshez Védett socket réteg (SSL) szekció alatt, meg kell határozni, hogy elfogadja-e az igazolást az azonosság érvényes ellenőrzésének eszközéül. Az igazolás hitelesítésének egyik kritériuma, amelyet az alkalmazás használ, hogy az alkalmazás megbízik-e az Igazolási hatóságban (CA), amely kiadta az igazolást.

A Digitális igazolás kezelő (DCM) segítségével megadhatja, hogy az alkalmazás melyik CA hatóságban bízhat meg, amikor kliens hitelesítést végez az igazolások révén. Az alkalmazások által megbízhatónak ítélt CA hatóságokat a megbízható CA listán keresztül kezelheti.

Mielőtt meghatározhatná az alkalmazásra vonatkozó megbízható CA listát, bizonyos feltételeknek meg kell felelni:
- Az alkalmazásnak támogatni kell az igazolások használatát kliens hitelesítéshez.
- Az alkalmazás definíciójában meg kell adni, hogy használja-e az alkalmazás a megbízható CA listát.

Ha az alkalmazás definíciója azt jelzi, hogy az alkalmazás használja a megbízható CA listát, akkor először meg kell adni a listát, mielőtt az alkalmazás sikeresen végrehajthatna kliens hitelesítést. Ez biztosítja azt, hogy az alkalmazás csak azokat az igazolásokat fogja érvényesíteni, amelyeket a megadott listán szereplő CA adott ki. Ha a felhasználó vagy a kliens alkalmazás olyan CA-tól kapott igazolást mutat be, amelyik nincs megadva a megbízható CA-k listáján, az alkalmazás nem fogja azt elfogadni érvényes hitelesítés alapjául.

Amikor felvesz egy CA-t a megbízhatók listájába egy adott alkalmazás számára, győződjön meg arról, hogy a CA szintén engedélyezve van.

Kövesse az alábbi lépéseket, ha megbízható CA listát ad meg egy alkalmazáshoz:
1. DCM indítása.
2. Kattintson a **Igazolás tároló választása**, majd a *SYSTEM elemre, az igazolás tároló megnyitása céljából.

   Megjegyzés: Ha kérdései lennének az adott űrlap kitöltésével kapcsolatban, válassza ki a kérdőjelet (**?**) a lap tetején az on-line súgó elérése céljából.
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. A navigációs kereten válassza az **Alkalmazások kezelését** a feladatlista megjelenítéséhez.
5. A feladatlistából válassza a **Megbízható CA lista megadását**.

6. Válassza ki az alkalmazás típusát (szerver vagy kliens), amelyre meg akarja adni a listát, és kattintson a **Folytatásra**.
7. Válasszon ki egy alkalmazást a listából, és kattintson a **Folytatásra** azon CA igazolások megjelenítéséhez, amelyeket a lista megadásához használhat fel.
8. Válassza ki azokat a CA-kat, amelyeket megbízhatónak ítél az alkalmazás számára, és kattintson az **OK** gombra. A DCM egy megerősítő üzenetet ad ki a listára kerültek kiválasztásáról.

   Megjegyzés: A listáról kiválaszthat egyedi CA-kat, de azt is megadhatja, hogy az alkalmazás tekintse megbízhatónak a listában lévő összes CA-t, vagy egyet sem. Mielőtt a listához adná a CA igazolást, módjában áll megtekinteni vagy ellenőrizni.

Igazolások és alkalmazások ellenőrzése

A Digitális igazolás kezelő (DCM) segítségével ellenőrizheti az egyedi igazolásokat, vagy az őket használó alkalmazásokat. A DCM által ellenőrzött dolgok listája egy kicsit különbözik attól függően, hogy igazolást vagy alkalmazást ellenőriz-e.

Alkalmazás ellenőrzés

Az alkalmazás definíció DCM révén történő ellenőrzésével megakadályozhatja az igazolással kapcsolatos problémákat, amikor az alkalmazás igazolást igénylő funkciókat hajt végre. Az ilyen problémák megakadályozhatják, hogy az alkalmazás sikeresen részt vegyen a Védett socket réteg (SSL) szekcióban, vagy hogy sikeresen aláírjon objektumokat.

Amikor egy alkalmazást ellenőriz, a DCM megvizsgálja az alkalmazáshoz rendelt igazolást, és megbizonyosodik arról, hogy a hozzárendelt igazolás érvényes-e. Továbbá, a DCM ellenőrzi azt, hogy az alkalmazás konfigurálva van-e a megbízható Igazolási hatóságok (CA) listájának használatára, és a lista tartalmaz-e legalább egy CA igazolást. Utána ellenőrzi, hogy az alkalmazás megbízható CA listájában szereplő CA igazolások érvényesek-e. Ha az alkalmazás definíció azt jelöli ki, hogy Igazolás visszavonási lista (CRL) feldolgozás történjen, és a CRL hely meg van adva a CA-ra vonatkozóan, a DCM ellenőrzi a CRL-t is az ellenőrzési folyamat részeként.

Igazolás ellenőrzés

Amikor egy igazolást ellenőriz, a DCM megvizsgálja az igazolásra vonatkozó adatokat, hogy megbizonyosodjon az igazolás hitelességéről és érvényességéről. Az igazolás ellenőrzése biztosítja, hogy az igazolást biztonságos kommunikációhoz vagy objektumok aláírásához használó alkalmazások ne ütközzenek hibába, amikor használják az igazolást.

Az ellenőrzési folyamat részeként a DCM ellenőrzi, hogy nem járt-e le a kiválasztott igazolás. A DCM azt is ellenőrzi, hogy nincs-e az igazolás felsorolva az Igazolás visszavonási listában (CRL), ha létezik CRL hely az igazolást kiadó CA-ra vonatkozóan. Továbbá, a DCM ellenőrzi, hogy a kiadó CA igazolása az aktuális igazolás tárolóban van-e, valamint engedélyezve van-e és ezáltal megbízható-e a CA igazolás. Ha az igazolásnak van magánkulcsa (például szerver, kliens és objektum aláíró igazolás), a DCM ellenőrzi a nyilvános - magánkulcs párt is, hogy megegyeznek-e. Másrészt, a DCM titkosítja az adatokat nyilvános kulccsal, majd ellenőrzi, hogy visszafejthetők-e magánkulccsal.

Az igazolás hozzárendelése az alkalmazásokhoz

A V5R2 változattól kezdve az új Digitális igazolás kezelő (DCM) továbbfejlesztései lehetővé teszik, hogy gyorsan és könnyedén hozzárendelje az igazolást több alkalmazáshoz is. Csak a *SYSTEM vagy az *OBJECTSIGNING igazolás tárolóból rendelhet hozzá igazolást több alkalmazáshoz.

Kövesse az alábbi lépéseket, amikor igazolásokat rendel hozzá egy vagy több alkalmazáshoz:

1. DCM indítása.

   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.
2. A navigációs kereten kattintson az **Igazolás tároló kiválasztására**, és válassza ki a megnyitandó ***OBJECTSIGNING** vagy ***SYSTEM** igazolás tárolót.
3. Írja be az igazolás tárolóra vonatkozó jelszót, és kattintson a **Folytatásra**.
4. Miután frissül a navigációs keret, válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
5. A feladatlistán válassza az **Igazolás hozzárendelése** feladatot az aktuális igazolás tárolóban lévő igazolások listájának megjelenítéséhez.
6. Válassza ki az igazolást a listából, és kattintson a **Hozzárendelés alkalmazásokhoz** feladatra, hogy megjelenítse az aktuális igazolás tárolóhoz tartozó alkalmazás definíciók listáját.
7. Válasszon ki egy vagy több 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.

CRL helyek kezelése

A Digitális igazolás kezelő (DCM) lehetővé teszi, hogy az igazolás ellenőrzési eljárás részeként meghatározza és kezelje egy adott Igazolási hatóság (CA) Igazolás visszavonási listájának (CRL) helyét. A CRL feldolgozást igénylő DCM vagy alkalmazás a CRL segítségével meghatározhatja, hogy az adott igazolást kiadó CA visszavonta-e az igazolás érvényességét. Amikor meghatározza az adott CA-ra vonatkozó CRL helyét, az alkalmazások - amelyek támogatják az igazolás használatát kliens hitelesítéshez - elérik a CRL listát.

Az olyan alkalmazások, amelyek támogatják az igazolások felhasználását kliens hitelesítéshez, végre tudják hajtani a CRL feldolgozást, ami még szigorúbb igazolás hitelesítést jelent, és amit az azonosság érvényes ellenőrzési módszerének tekintenek. Mielőtt az alkalmazás használhatná a megadott CRL listát az igazolás ellenőrzési eljárás részeként, a DCM alkalmazás definícióban meg kell követelni, hogy az alkalmazás hajtsa végre a CRL feldolgozást.

A CRL működése

Amikor a DCM segítségével ellenőrzi az igazolást vagy az alkalmazást, a DCM végrehajtja a CRL feldolgozást az ellenőrzési folyamat alapértelmezett részeként. Ha nincs megadva CRL hely az igazolást kibocsátó CA-ra vonatkozóan, a DCM nem tudja végrejhajtani a CRL ellenőrzést. Azonban a DCM megkísérli az igazolás egyéb fontos információit ellenőrizni, például, hogy az adott igazoláson lévő CA aláírás érvényes-e, vagy hogy az igazolást kiadó CA megbízható-e.

CRL hely megadása

Kövesse az alábbi lépéseket, amikor egy adott CA-ra vonatkozó CRL helyét határozza meg:

1. DCM indítása.

2. A navigációs kereten válassza a **CRL helyek kezelését** a feladatlista megjelenítéséhez.
3. Válassza ki a **CRL hely hozzáadását** a feladatlistából. Az így megjelenő űrlapon leírhatja a CRL helyét, valamint azt, hogyan érheti el a helyet a DCM vagy az alkalmazás.
4. Töltse ki az űrlapot, és kattintson az **OK** gombra. Egy egyedi nevet kell adni a CRL helynek, azonosítani kell a CRL-t befogadó LDAP szervert, és összeköttetési információkat kell biztosítani, amelyek leírják az LDAP szerver elérésének módját.

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

   Most a CRL hely definíciót kell társítani az adott CA-val.
5. A navigációs kereten válassza az **Igazolások kezelését** a feladatlista megjelenítéséhez.
6. A feladatlistából válassza a **CRL hely hozzárendelések frissítését** a CA igazolások listájának megjelenítéséhez.
7. Válassza ki azt a CA igazolást a listából, amelyhez hozzá kívánja rendelni a létrehozott CRL hely definíciót, és kattintson a **CRL hely hozzárendelés frissítésére**. Megjelenik a CRL helyek listája.
8. Válassza ki azt a CRL helyet a listából, amelyet társítani kíván a CA-val, és kattintson a **Hozzárendelés frissítésére**. A lap tetején egy üzenet tájékoztatja, hogy a CRL hely hozzárendelése megtörtént az Igazolási hatóság (CA) igazolásához.

Amint az adott CA megadott CRL hellyel rendelkezik, a DCM vagy a többi alkalmazás felhasználhatja a CRL feldolgozás folyamán. Azonban, mielőtt a CRL feldolgozás működne, a Címtár szolgáltató szervernek tartalmazni kell a megfelelő CRL-t. Valamint konfigurálni kell a Címtár szolgáltatási szervert és a kliens alkalmazásokat is az SSL használatához, és rendelje hozzá az igazolást az alkalmazáshoz a DCM segítségével.

Az iSeries Directory Services (LDAP) szerverről további információkat tudhat meg az alábbi Információs központbeli témakörökben:

- Directory Services (LDAP)
  A témakör minden olyan tudnivalót elmond, amit tudni kell az iSeries Directory Services (LDAP) szerver konfigurálásáról és használatáról.
- Védett socket réteg (SSL) kapcsolat LDAP címtár szerverrel
  A témakör elmagyarázza mit kell tudni az LDAP szerver konfigurálásáról, amikor SSL-t kíván használni a biztonságos kommunikáció érdekében.

Igazolás kulcsok tárolása IBM 4758 Cryptographic Coprocessor kártyán

Ha telepítette az IBM 4758–023 PCI Cryptographic Coprocessor kártyát az iSeries szerveren, a társprocesszor segítségével még biztonságosabb tárolást nyújthat az igazolások magánkulcsainak. A társprocesszor révén tárolhatja a szerver-, a kliens vagy a Helyi igazolási hatóság (CA) igazolásának magánkulcsát. Azonban nem használhatja fel a felhasználói igazolás magánkulcsának tárolására, mivel azt a felhasználó rendszerén kell tárolni. Jelenleg az objektum aláíró igazolás magánkulcsát sem tárolhatja a társprocesszor felhasználásával.

A társprocesszorral kétféleképpen tárolhatja az igazolás magánkulcsát:
- Az igazolás magánkulcsának tárolása közvetlenül a társprocesszorban magában.
- Az igazolás magánkulcsának titkosítása a társprocesszor mester kulcsával, és tárolása egy speciális kulcsfájlban.

Ezt a kulcstárolási opciót az igazolás létrehozási vagy megújítási folyamatának részeként választhatja ki. Ha társprocesszorral tárolja az igazolás magánkulcsát, megváltoztathatja a társprocesszor eszköz hozzárendelését az adott kulcsra vonatkozóan.

Ahhoz, hogy a társprocesszort magánkulcs tárolására használja, mindenképpen indítsa el (vary on) a társprocesszort a Digitális igazolás kezelő (DCM) használata előtt. Ellenkező esetben a DCM nem ajánlja fel a tárolási opció kiválaszthatóságát az igazolás létrehozási és megújítási folyamata során.

Ha létrehoz vagy megújít szerver vagy kliens igazolást, válassza ki a magánkulcs tárolására vonatkozó opciót, miután kiválasztotta az aktuális igazolást aláíró CA típusát. Ha létrehoz vagy megújít Helyi CA-t, válassza ki a magánkulcs tárolására vonatkozó opciót a folyamat első lépéseként.

Az igazolás magánkulcsának tárolása közvetlenül a társprocesszorban

Az igazolás magánkulcsához való hozzáférés még erősebb védelme érdekében választhatja azt, hogy a kulcsot közvetlenül az IBM 4758–023 PCI Cryptographic Coprocessor kártyán tárolja. Ezt a kulcstárolási opciót az igazolás létrehozásának vagy megújításának részeként választhatja ki a Digitális igazolás kezelőben (DCM).

Kövesse az alábbi lépéseket a **Kulcs tárolási hely kiválasztása** laptól kezdve, ha az igazolás magánkulcsát közvetlenül a társprocesszorban tárolja:

1. Válassza ki a **Hardvert** tárolási opcióként.
2. Kattintson a **Folytatásra**. Hatására megjelenik a **Titkosítási eszközleírás kiválasztása** lap.
3. Az eszközlistából válasszon ki egyet, amelyet az igazolás magánkulcsának tárolására kíván felhasználni.
4. Kattintson a **Folytatásra**. A DCM a végrehajtás alatt álló feladattal folytatja a lap megjelenítését, mint például a létrehozásra vagy megújításra kerülő igazolás azonosító információival.

Az igazolás magánkulcsának titkosítása a társprocesszor mester kulcsával

Az igazolás magánkulcsához való hozzáférés még erősebb védelme érdekében választhatja azt, hogy az IBM 4758–023 PCI Cryptographic Coprocessor mester kulcsával titkosítja az igazolás magánkulcsát, és eltárolja egy speciális kulcsfájlba. Ezt a kulcstárolási opciót az igazolás létrehozásának vagy megújításának részeként választhatja ki a Digitális igazolás kezelőben (DCM).

Mielőtt sikeresen használná ezt az opciót, az IBM 4758–023 PCI Cryptographic Coprocessor konfigurációs web kezelőfelületével hozza létre a megfelelő kulcstárolási fájlt. A társprocesszor konfigurációs web kezelőfelületén társítsa össze a kulcstárolási fájlt a használni kívánt társprocesszor eszközleírásával. A társprocesszor konfigurációs web kezelőfelületét az iSeries Feladatlapjáról érheti el.

Ha a rendszer egynél több telepített és elindított társprocesszor eszközzel rendelkezik, választhatja azt, hogy megosztja az igazolás magánkulcsát több eszköz között. Ahhoz, hogy a magánkulcsot megossza az eszközleírások számára, az összes eszköznek ugyanazzal a mester kulccsal kell rendelkeznie. Ugyanazon mesterkulcs több eszközhöz történő eljuttatásának folyamatát *klónozásnak* hívják. A kulcs megosztása az eszközök között lehetővé teszi, hogy használja a Védett socket réteg (SSL) terhelési kiegyensúlyozást, ami javítja a védett szekciók teljesítményét.

Kövesse az alábbi lépéseket a **Kulcs tárolási hely kiválasztása** laptól kezdve, ha a társprocesszor mesterkulcsával titkosítja az igazolás magánkulcsát, és egy speciális kulcstároló fájlban őrzi:

1. Válassza ki a **Hardver titkosítás** tárolási opcióként.

2. Kattintson a **Folytatásra**. Hatására megjelenik a **Titkosítási eszközleírás kiválasztása** lap.
3. Az eszközlistából válasszon ki egyet, amelyet az igazolás magánkulcsának titkosítására kíván felhasználni.
4. Kattintson a **Folytatásra**. Ha egynél több telepített és elindított társprocesszor eszköze van, a **További titkosítási eszközleírás kiválasztása** lap jelenik meg.

   Megjegyzés: Ha nincs több rendelkezésre álló társprocesszor eszköze, a DCM a végrehajtás alatt álló feladattal folytatja a lap megjelenítését, mint például a létrehozásra vagy megújításra kerülő igazolás azonosító információival.
5. Az eszközlistából válasszon ki egy vagy több eszközleírást, amelyek között meg kívánja osztani az igazolás magánkulcsát.

   Megjegyzés: A kiválasztott eszközleírásoknak ugyanazzal a mesterkulccsal kell rendelkezniük, mint az előző lapon kiválasztott eszköznek. A 4758 Cryptographic Coprocessor konfigurációs web kezelőfelületén elérhető Mesterkulcs ellenőrzés nevű feladat segítségével ellenőrizheti, hogy azonos-e az eszközök mesterkulcsa. A társprocesszor konfigurációs web kezelőfelületét az iSeries Feladatlapjáról érheti el.
6. Kattintson a **Folytatásra**. A DCM a végrehajtás alatt álló feladattal folytatja a lap megjelenítését, mint például a létrehozásra vagy megújításra kerülő igazolás azonosító információival.

Kérési hely kezelés PKIX CA esetén

A Public Key Infrastructure for X.509 (PKIX) Igazolási hatóság (CA) egy olyan CA, amely az igazolásokat a legújabb Internet x.509 szabványok alapján adja ki, megvalósítva ezáltal a nyilvános kulcs infrastruktúráját. A PKIX szabványokat a Request For Comments (RFC) 2560 körvonalazza.

A PKIX CA szigorúbb azonosítást követel meg az igazolás kiadása előtt. Általában megköveteli a kérelmezőtől, hogy biztosítsa az azonosság ellenőrzését a Regisztrációs hatóságon (RA) keresztül. Miután a kérelmező megadja az RA által ellenőrzési célból kért adatokat, az RA hitelesíti a kérelmező kilétét. A CA által kialakított eljárástól függően vagy az RA vagy a kérelmező benyújtja a hitelesített jelentkezési lapot a megfelelő CA-nak. Ahogy ezek a szabványok egyre szélesebb körben terjednek, a PKIX előírások szerinti CA-k is egyre jobban elérhetőkké válnak. Feltétlenül vizsgálja meg a PKIX szerinti CA használatát, ha biztonsági igényei az erőforrások szigorú hozzáférés vezérlését igénylik, amelyeket az SSL kapcsolatot használó alkalmazásai nyújtanak a felhasználóknak. Például, a Lotus Domino nyújt ilyen PKIX CA-t nyilvános használatra.

Ha úgy dönt, hogy PKIX CA adja ki az igazolásokat az alkalmazások számára, a Digitális igazolás kezelővel (DCM) kezelheti az ilyen igazolásokat. A DCM segítségével URL-t konfigurálhat a PKIX CA számára. Ha így konfigurálja a Digitális igazolás kezelőt (DCM), akkor PKIX CA lesz az aláírt igazolások megszerzési módja.

Ha a DCM segítségével akarja kezelni a PKIX CA-tól származó igazolásokat, akkor az alábbi lépések útján úgy kell konfigurálni a DCM-t, hogy az használja a CA helyet:
1. DCM indítása.
2. A navigációs kereten válassza ki a **PKIX kérési hely kezelését**, hogy megjelenítse az űrlapot, amely lehetővé teszi az URL megadását a PKIX CA vagy a hozzátartozó RA számára.
3. Írja be az igazolás kéréshez használni kívánt PKIX CA teljesen megadott URL címét, például: http://www.thawte.com, és kattintson a **Hozzáadásra**. Az URL hozzáadása úgy konfigurálja a DCM-et, hogy a PKIX CA az aláírt igazolások megszerzésének egyik módja lesz.

Miután hozzáadja a PKIX CA kérési helyet, a DCM hozzáadja a PKIX CA-t a lehetséges CA típusokhoz, amelyek közül kiválaszthatja, hogy melyik adja ki az igazolást az **Igazolás létrehozása** feladatban.

Objektumok aláírása

Az objektumok aláírására három módszert használhat. Írhat egy programot, amely az Objektum aláíró API-t hívja. Használhatja a Digitális igazolás kezelőt (DCM) is az objektumok aláírásához. Végül, a V5R2 változattól kezdve az iSeries navigátor Kezelőközpont funkciójával is aláírhat objektumokat, amikor összecsomagolja őket más iSeries rendszereknek való terjesztés céljából.

A DCM-ben kezelt igazolásokkal bármilyen objektumot aláírhat, amelyet a rendszer integrált fájlrendszerében tárol, kivéve a könyvtárban tárolt objektumokat. Csak azokat az objektumokat írhatja alá, amelyeket a QSYS.LIB fájlrendszer tartalmazza: *PGM, *SRVPGM, *MODULE, *SQLPKG és *FILE (csak mentési fájl). Újdonság a V5R2 kiadásban, hogy a parancs (*CMD) objektumokat is aláírhatja. Más iSeries szervereken tárolt objektumokat nem írhat alá.

Az objektumokat aláírhatja nyilvános Internet Igazolási hatóságtól (CA) vásárolt igazolással, vagy saját helyi CA hatósággal DCM-ben létrehozott igazolással. Az igazolások aláírásának folyamata ugyanaz, függetlenül attól, hogy nyilvános vagy saját igazolást használ-e.

Objektum aláírás előfeltételei

Mielőtt használná a DCM-et (vagy az Objektum aláíró API-t) az objektumok aláírásához, győződjön meg arról, hogy eleget tesz bizonyos előfeltételeknek:

- Létre kell hozni az *OBJECTSIGNING igazolás tárolót a Helyi CA létrehozási vagy a Nyilvános Internet CA-tól származó 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.
- Az objektumok aláírásához létre kell hozni egy objektum aláíró alkalmazás definícióját.
- Hozzá kell rendelni egy igazolást az objektum aláíró alkalmazáshoz, amelyet az objektumok aláírásához kíván felhasználni.

DCM használata objektumok aláírásához

Kövesse az alábbi lépéseket, ha a DCM segítségével egy vagy több objektumot ír alá:

1. DCM indítása.

   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.
2. A navigációs kereten kattintson az **Igazolás tároló választására**, majd válassza ki a megnyitandó ***OBJECTSIGNING** igazolás tárolót.
3. Írja be az *OBJECTSIGNING igazolás tárolóra vonatkozó jelszót, és kattintson a **Folytatásra**.
4. Miután frissül a navigációs keret, válassza az **Aláírható objektumok kezelését** a feladatlista megjelenítéséhez.
5. A feladatlistán válassza az **Objektum aláírása** feladatot az objektumok aláírásához használt alkalmazás definíciók listájának megjelenítéséhez.
6. Válassza ki az alkalmazást, és kattintson az **Objektum aláírására**, melynek hatására megjelenik egy űrlap, ahol megadhatja az aláírni kívánt objektumok helyét.

Megjegyzés: Ha a kiválasztott alkalmazáshoz nincs hozzárendelve igazolás, akkor nem használhatja fel az objektum aláírására. Először az **Alkalmazások kezelése** alatt található **Igazolás hozzárendelés frissítése** feladatot kell végrehajtani, ha igazolást akar hozzárendelni az alkalmazás definícióhoz.

7. 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 ″bármilyen egyetlen karaktert jelent″. Például, az adott alkönyvtár összes objektumának aláírásához gépelje be az /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.

8. 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).

9. 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.

Objektum aláírások ellenőrzése

A Digitális igazolás kezelő (DCM) segítségével ellenőrizheti az objektumokon lévő digitális aláírások hitelességét. Amikor ellenőrzi az aláírást, győződjön meg arról, hogy az objektum adatai nem változtak meg azóta, hogy az objektum tulajdonosa aláírta az objektumot.

Az aláírás ellenőrzés előfeltételei

Mielőtt használná a DCM-et az objektumokon található aláírások ellenőrzéséhez, győződjön meg arról, hogy eleget tesz bizonyos előfeltételeknek:

- Létrehozta a *SIGNATUREVERIFICATION igazolás tárolót az aláírás ellenőrző igazolások kezeléséhez.

  Megjegyzés: Aláírás ellenőrzést hajthat végre az *OBJECTSIGNING igazolás tárolóban azokban az esetekben, amikor ugyanazon a rendszeren aláírt objektumok aláírását ellenőrzi. Az aláírások ellenőrzéséhez végrehajtott lépések (a

DCM-ben) egyformák mindegyik igazolás tároló esetén. Azonban, a *SIGNATUREVERIFICATION igazolás tárolónak léteznie kell, és tartalmaznia kell az objektumot aláíró igazolás egy példányát még akkor is, ha aláírás ellenőrzést hajt végre és az *OBJECTSIGNING igazolás tárolóban dolgozik.

- A *SIGNATUREVERIFICATION igazolás tároló tartalmazza az objektumot aláíró igazolás egy példányát.
- A *SIGNATUREVERIFICATION igazolás tároló tartalmazza a CA igazolás egy példányát, amely kiadta az objektumokat aláíró igazolást.

DCM használata objektumok aláírásának ellenőrzéséhez

Kövesse az alábbi lépéseket, ha a DCM segítségével ellenőrzi az objektum aláírásokat:

1. DCM indítása.

   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.
2. A navigációs kereten kattintson az **Igazolás tároló választása**, majd a ***SIGNATUREVERIFICATION** elemre, az igazolás tároló megnyitása céljából.
3. Írja be a *SIGNATUREVERIFICATION igazolás tárolóra vonatkozó jelszót, és kattintson a **Folytatásra**.
4. Miután frissül a navigációs keret, válassza az **Aláírható objektumok kezelését** a feladatlista megjelenítéséhez.
5. A feladatok listájából válassza ki az **Objektum aláírások ellenőrzését**, hogy megadja azoknak az objektumoknak a helyét, amelyeknél ellenőrizni kívánja az aláírásokat.
6. 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 ″bármilyen egyetlen karaktert jelent″. Például, az adott alkönyvtár összes objektumának aláírásához gépelje be az /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 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).

8. 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.

A DCM segítségével megnézheti az objektumot aláíró igazolás információit. Ez lehetővé teszi az objektum kezelése előtt annak meghatározását, hogy az objektum megbízható forrásból származik-e.

Fejezet 9. A DCM hibakeresése

Az itt található oldalak hasznos információkkal szolgálnak néhány olyan általános probléma hibakereséséről, amelyekkel a Digitális igazolás kezelő (DCM) használata során találkozhat.

Olvassa el az alábbiakat a problémákról és lehetséges megoldásaikról:

Jelszavak és általános problémák hibakeresése
Az itt leírtak segítségével megismerheti a DCM felhasználói kezelőfelület általános problémáit, és azok elhárításának lehetőségeit.

Igazolás tároló és kulcs adatbázis problémák hibakeresése
Az itt leírtak segítségével megismerheti az igazolás tároló és a kulcs adatbázis általános problémáit, és azok elhárításának lehetőségeit.

Böngésző problémák hibakeresése
Az itt leírtak segítségével megismerheti azokat az általános problémákat és elhárításuk lehetőségeit, amelyek akkor jelentkezhetnek, mikor böngészőt használ a DCM eléréséhez.

HTTP Server for iSeries problémák hibakeresése
Az itt leírtak segítségével megismerheti a HTTP szerver általános problémáit, és azok elhárításának lehetőségeit.

Áttérési hibák és helyreállítási megoldások
Az itt leírtak segítségével megismerheti azokat az általános problémákat és elhárításuk lehetőségeit, amelyek akkor jelentkezhetnek, mikor a DCM egy előző változatáról tér át.

Felhasználói igazolás hozzárendelésének hibakeresése
Az itt leírtak segítségével megismerheti azokat az általános problémákat és elhárításuk lehetőségeit, amelyek akkor jelentkezhetnek, mikor a DCM segítségével felhasználói igazolásokat regisztrál.

Jelszavak és általános problémák hibakeresése

A következő táblázat hasznos információkkal szolgál néhány jellemző jelszó probléma és egyéb általános problémák hibakereséséről, amelyekkel a Digitális igazolás kezelő (DCM) használata során találkozhat.

Probléma	Lehetséges megoldás
Nem találja a DCM további súgó részét.	A DCM-ben kattintson a ″**?**″ súgó ikonra. help icon. Keresheti az Információs központot és az Interneten lévő külső helyeket is.
NET.DATA hiba jön, amikor megpróbálja megnyitni az igazolás tárolót.	Inkább az **Igazolás tároló kiválasztása** ablakban válassza ki az egérrel a **Folytatás** gombot, mint hogy az **Enter** billentyűt használja a billentyűzeten.
A Helyi igazolási hatóságra (CA) és a *SYSTEM igazolás tárolókra vonatkozó jelszavak nem működnek.	A jelszavak kis/nagybetű érzékenyek. Győződjön meg róla, hogy a betűváltó billentyű ugyanabban a helyzetben van, mint amikor a jelszavakat megadta.
Az Igazolás tároló kiválasztása feladat használatakor a jelszó törlési kísérlete sikertelen.	A törlési funkció csak akkor következhet be, ha a DCM tárolta a jelszót. A DCM automatikusan tárolja a jelszót, amikor létrehozza az igazolás tárolót. Azonban, ha megváltoztatja (vagy törli) a jelszót, válassza ki az **Automatikus bejelentkezés** opciót, hogy a DCM továbbra is elrejtse a jelszót.

Probléma	Lehetséges megoldás
	Ha egy igazolás tárolót átvisz az egyik rendszerről egy másik rendszerre, akkor az igazolás tároló jelszavát változtassa meg az új rendszeren, hogy a DCM mindenképpen automatikusan elrejtse azt. A jelszó megváltoztatásához meg kell adni az igazolás tároló eredeti jelszavát, amikor megnyitja az új rendszeren. Nem használhatja a jelszó törlési opciót addig, amíg meg nem nyitja a tárolót az eredeti jelszóval és meg nem változtatja az elrejtés érdekében. Ha a jelszó módosítása és elrejtése nem történik meg, a DCM és az SSL nem tudja automatikusan helyreállítani a jelszót, amikor az különböző funkciókhoz kellene. Ha egy igazolás tárolót telepít át, amelyet Másik rendszer igazolás tárolójaként fog használni, válassza ki az **Automatikus bejelentkezés** opciót, amikor megváltoztatja a jelszót, hogy a DCM elrejtse az adott típusú igazolás tárolóra vonatkozó jelszót.
	Ellenőrizze a Rendszer szervizeszközök (SST) Rendszer biztonság kezelése menüpontja alatt a ″Digitális igazolások engedélyezése″ tulajdonsághoz tartozó értéket. Ha ennek a tulajdonságnak az értéke 2 (Nem), akkor az igazolás tároló jelszava nem törölhető. A tulajdonság értékét megjelenítheti és módosíthatja az STRSST parancs segítségével és a Szervizeszközök felhasználói ID és jelszó beírásával. Azután válassza a ″Rendszer biztonság kezelése″ opciót. A Szervizeszközök felhasználói azonosítója valószínűleg a QSECOFR felhasználói ID lesz.
Nem találja a CA igazolás forrását, hogy fogadja az iSeries rendszeren.	Egyes CA-k nem teszik azonnal elérhetővé CA igazolásaikat. Ha nem kapja meg a CA igazolást a CA-tól, vegye fel a kapcsolatot saját VAR részlegével, mivel lehet, hogy a VAR speciális vagy valamilyen más pénzügyi egyezséget kötött a CA-val.
Nem találja a *SYSTEM igazolás tárolót.	A *SYSTEM igazolás helye /qibm/userdata/icss/cert/server/default.kdb. Ha nem létezik az igazolás tároló, a DCM segítségével létre kell hozni. Ehhez használja az **Új igazolás tároló létrehozása** feladatot.
A DCM-től hibajelzést kapott, és a hibajelzés a hiba javítása után is fennmarad.	Törölje a böngésző gyorsítótárat. A gyorsítótár méretét állítsa 0 értékre, majd állítsa le és indítsa újra a böngészőt.
LDAP szerver hibája van, például az igazolás hozzárendelések nem láthatók, amikor a biztonságos alkalmazásokra vonatkozó információkat megjeleníti közvetlenül az igazolás hozzárendelése után. Ez a probléma a leggyakrabban akkor fordul elő, amikor az iSeries navigátort használja fel a Netscape Communications böngésző eléréséhez. A böngésző gyorsítótárra vonatkozó beállítás alapján a gyorsítótárban lévő dokumentum összehasonlításra kerül a hálózaton levővel (″Szekciónként egyszer″).	Változtassa meg ezt az alapértelmezett beállítást úgy, hogy minden alkalommal ellenőrizze a gyorsítótárat.
Amikor DCM segítségével külső CA (például Entrust) által aláírt igazolást importál, hibaüzenetet kap arról, hogy az ellenőrzési periódus nem tartalmazza a mai napot, illetve nem esik bele a kibocsátó által megadott érvényességi időtartományba.	A rendszer Általánosított időformátumot (Generalized Time) használ az érvényességi időtartamhoz. Várjon egy napot, és próbálja meg újra. Ellenőrizze azt is, hogy az iSeries helyes értékkel rendelkezik-e az UTC eltoláshoz (dspsysval qutcoffset). Ha nyári/téli időszámítást fedez fel, esetleg helytelenül van beállítva az eltolás.

Probléma	Lehetséges megoldás
Alap 64 hibát kap, amikor az Entrust igazolást próbálja importálni.	Az igazolás a különleges formátumú igazolások között van felsorolva (például PEM formátum). Ha a böngésző másolási funkciója nem jól működik, akkor az igazoláshoz nem tartozó extra részeket, mint például az egyes sorok elején található üres helyeket is átmásolhatja. Ha ez az eset áll fenn, az igazolás formátuma nem lesz jó, amikor megpróbálja használni az iSeries szerveren. Bizonyos weblapoknál ez problémát okoz. Más lapokat már úgy terveztek, hogy ez ne okozzon gondot. Feltétlenül hasonlítsa össze az eredeti igazolás megjelenését a másolás eredményével, mivel ezeknek egyformáknak kell lenni.
Amikor a DCM V4R3 verziójáról frissít V5R2 verzióra, a költöztetés nem tartalmazza a lejárt rendszer igazolások mozgatását.	A lejárt rendszer igazolás rossz és nem kerül a *SYSTEM igazolás tárolóba. Az áttelepítés előtt nevezze át vagy távolítsa el a régi V4R3 kulcscsomó fájlokat, hagyja figyelmen kívül az áttelepítési hiba jelzését, vagy próbálja meg újra a költöztetést.
Nem találja a mintaprogramot, amellyel igazolásokat adhat hozzá az ellenőrzési listához.	A mintaprogram még nem áll rendelkezésre.

Igazolás tároló és kulcs adatbázis problémák hibakeresése

A következő táblázat hasznos információkkal szolgál az igazolás tároló és a kulcs adatbázis néhány olyan általános problémájának hibakereséséről, amelyekkel a Digitális igazolás kezelő (DCM) használata során találkozhat.

Probléma	Lehetséges megoldás
A rendszer nem találta meg a kulcs adatbázist, illetve nem találta érvényesnek.	Ellenőrizze a jelszót és a fájl nevét gépelési hibára. Győződjön meg arról, hogy a fájlnév tartalmazza az elérési útvonalat, beleértve a kezdő ″per″ jelet (forward slash) is.
Kulcs adatbázis létrehozása sikertelen.	Ellenőrizze a fájlnév ütközést. Az ütközés lehet, hogy egy másik fájlnál áll fenn, és nem annál, amit kért.
A rendszer nem fogadja el a CA szövegfájlt, amely bináris formában egy másik rendszertől érkezett. A fájlt akkor nem fogadja el, ha American National Standard Code for Information Interchange (ASCII) kódban küldték el.	A kulcscsomók és a kulcs adatbázisok binárisak, ennek következtében eltérőek. A File Transfer Protocol (FTP) ASCII üzemmódját használja a CA szövegfájlokhoz, míg bináris üzemmódot a bináris fájlokhoz, mint például a .kdb, .kyr, .sth, .rdb, stb. kiterjesztésűekhez.
A kulcs adatbázis jelszavát nem tudja megváltoztatni. A kulcs adatbázis egyik igazolása érvénytelenné vált.	Miután ellenőrizte, hogy nem a jelszó helytelen, keresse meg és törölje az érvénytelen igazolást vagy igazolásokat az igazolás tárolóból, és próbálja meg újra a jelszó módosítását. Ha lejárt igazolások vannak az igazolás tárolóban, akkor érvényességük megszűnik. Mivel az igazolások nem érvényesek, az igazolás tároló jelszó módosítási funkciója nem engedélyezi a jelszó megváltoztatását, és a titkosítási folyamat sem titkosítja a lejárt igazolás magánkulcsait. Ez megakadályozza a jelszó módosítását, és a rendszer jelezheti, hogy az igazolás tároló emiatt sérült. Távolítsa el az érvénytelen (lejárt) igazolásokat az igazolás tárolóból.
Igazolásokat kell alkalmazni egy Internet felhasználó miatt, és ezért ellenőrzési listákat kell használni, de a DCM nem biztosítja a funkciókat az ellenőrzési listákhoz.	Az üzleti partnereknek, akik ellenőrzési listákat használó alkalmazásokat írnak, kell úgy megírniuk a programokat, hogy az ellenőrzési listák és az alkalmazások társítása az elvárásoknak megfelelő legyen. Azt is nekik kell a programban biztosítani, hogy amikor az Internet felhasználó azonossága megfelelően ellenőrzésre került, akkor az igazolás felvehető legyen az ellenőrzési (más szóval érvényesítési) listába. Olvassa el az Információs központ QsyAddVldlCertificate API című témakörét. Nézze át a Webmaster’s Guide című kiadványt, ha többet akar megtudni a biztonságos szerver konfigurálásáról ellenőrzési lista használatához.

Böngésző problémák hibakeresése

A következő táblázat hasznos információkkal szolgál a böngészővel kapcsolatos, néhány olyan általános probléma hibakereséséről, amelyekkel a Digitális igazolás kezelő (DCM) használata során találkozhat.

Probléma	Lehetséges megoldás
A Microsoft Internet Explorer nem engedi, hogy kiválasszon egy másik igazolást, amíg el nem indít egy újabb böngésző szekciót.	Kezdjen el egy újabb Internet Explorer szekciót.
Az Internet Explorer nem jelzi ki az összes kiválasztható kliens/felhasználói igazolást a böngésző kiválasztási listájában. Az Internet Explorer csak a megbízható CA által kiadott igazolásokat mutatja, amelyeket biztonságos helyen használhat.	A CA-nak megbízhatónak kell lenni a kulcs adatbázisban és a biztonságos alkalmazás számára is. Győződjön meg arról, hogy ugyanazzal a névvel jelentkezett be a PC-n az Internet Explorer böngészőbe, mint amit a böngészőben lévő felhasználói igazolásba helyezett el. Kérjen egy másik felhasználói igazolást a rendszertől, amelyet elér. A rendszer adminisztrátor győződjön meg arról, hogy az igazolás tároló (kulcs adatbázis) számára még mindig megbízható a felhasználói és a rendszer igazolásokat aláíró CA.
Az Internet Explorer 5 fogadja a CA igazolást, de nem tudja megnyitni a fájlt, vagy nem találja a lemezt, ahova mentette az igazolást.	Ez egy új böngésző funkció azoknak az igazolásoknak, amelyeket még nem tekint az Internet Explorer böngésző megbízhatónak. A helyet kiválaszthatja a PC-n.
A böngésző figyelmeztette, hogy a rendszer neve és a rendszer igazolása nem egyezik.	Egyes böngészők eltérő módon viselkednek a rendszernevek kis- és nagybetűs egyezésekor. Ugyanazzal a kis- és nagybetűkkel írja be az URL címet, mint amit a rendszer igazolás mutat. Vagy, hozza létre a rendszer igazolást olyan betűkkel, amit a legtöbb felhasználó használ. Amíg nem biztos benne, hogy mit is tegyen, a legjobb, ha változatlanul hagyja a szerver vagy a rendszer nevét. Ellenőrizze a tartománynév szerver beállításának helyességét is.
HTTPS beállítással indította el az Internet Explorer böngészőt HTTP helyett, és figyelmeztetést kapott biztonságos és nem biztonságos szekciók keveredéséről.	Válassza az elfogadást, és hagyja figyelmen kívül a figyelmeztetést - az Internet Explorer jövőbeli változatában javítva lesz ez a hiba.
A Netscape Communicator 4.04 for Windows a hexadecimális A1 és B1 értékeket B2 és 9A értékre konvertálja lengyel kódlap esetén.	Ez böngésző hiba, ami hatással van a nemzeti nyelvű változatra. Használjon más böngészőt, vagy ugyanazt, de más platformon, például Netscape Communicator 4.04 for AIX böngészőt.
A Netscape Communicator 4.04 a felhasználói profilban helyesen mutatja az NLS nagybetűs felhasználói igazolásokat, de a kisbetűsöket helytelenül jelzi ki.	Egyes nemzeti nyelvű karakterek helyett, amelyek helyesen lettek beírva, később eltérő karakterek jelennek meg. Például, a Netscape Communicator 4.04 for Windows verzióban a hexadecimális A1 és B1 értékek B2 és 9A értékekre konvertálódtak lengyel kódlap esetén, ami azt eredményezte, hogy más NLS karakterek jelentek meg.
A böngésző folytatja annak közlését a végfelhasználó felé, hogy a CA még nem megbízható.	A DCM segítségével állítsa be a **CA állapotot**, ami engedélyezi, hogy a CA-t megbízhatónak jelölje.
Az Internet Explorer kéri a HTTPS kapcsolat visszautasítását.	Böngésző funkció vagy konfigurációs probléma. A böngésző azt választotta, hogy nem kapcsolódik olyan helyszínhez, amely saját maga által aláírt, illetve más okból kifolyólag nem érvényes rendszer igazolást használ.
A Netscape Communicator böngésző és szerver termékek cégek igazolásait alkalmazza - beleértve, de nem korlátozva erre, VeriSign - az SSL kommunikációk (különösen hitelesítés) engedélyezése céljából. Az összes ilyen igazolás lejár időnként. Egyes Netscape böngésző és szerver igazolások 1999. december 25. és 1999. december 31. között jártak le. Ha nem orvosolta a hibát 1999. december 14-én vagy előtte, akkor hibaüzenetet fog kapni.	A böngésző (Netscape Communicator 4.05 vagy korábbi) korábbi változatai rendelkeznek lejárt igazolásokkal. Frissíteni kell a böngészőt a Netscape Communicator aktuális változatára. A böngésző igazolásokról számtalan helyen olvashat, beleértve a http://home.netscape.com/security/ és a http://www.verisign.com/server/cus/rootcert/webmaster.html címeket is. A böngészőt ingyen letöltheti a http://www.netcenter.com címről.

A HTTP Server for iSeries problémák hibakeresése

A következő táblázat hasznos információkkal szolgál a HTTP Server for iSeries néhány olyan általános problémájának hibakereséséről, amelyekkel a Digitális igazolás kezelő (DCM) használata során találkozhat.

Probléma	Lehetséges megoldás
A Hypertext átviteli protokoll védelem (HTTPS) nem működik.	Győződjön meg arról, hogy a HTTP Server helyesen van konfigurálva az SSL használatára. A V5R1 vagy újabb változatokban a konfigurációs fájl az **SSLAppName**, amelyet a HTTP Server grafikus felhasználói kezelőfelületével (GUI) állíthat be. A konfiguráció tartalmazza az SSL portot használó, konfigurált virtuális gazdagépet is **SSLEnable** alatt. Két Figyelő direktíva is van, amelyek két különböző portot adnak meg - egyet az SSL kapcsolathoz, és egy másikat a nem SSL kapcsolathoz. Ellenőrizze, hogy a szerver példány létrehozása és a szerver igazolás aláírása megtörtént.
A HTTP Server példány biztonságos alkalmazásként való bejegyeztetésének folyamatát tisztázni kell.	Az iSeries rendszeren menjen a HTTP Server webes kezelőfelületére, ahol beállíthatja a HTTP Server konfigurációját. Először meg kell adni a virtuális gazdagépet az SSL engedélyezése érdekében. Ezt a Környezet kezelése képernyőn teheti meg. A virtuális gazdagépet meg kell adni a Figyelő direktívában korábban megadott SSL használatához. Azután az SSL Általános beállítások képernyőn kapcsolja be az SSL kapcsolatot az előzőleg konfigurált virtuális gazdagépen. Az összes változtatást alkalmazni kell a konfigurációs fájlnál. Ne felejtse el, hogy a példány regisztrálása nem választja ki automatikusan, mely igazolásokat kell használni a példánynak. A DCM segítségével rendelje hozzá az adott igazolást az alkalmazáshoz, mielőtt megpróbálja leállítani és újraindítani a szerver példányt.
Nehézségei támadtak, amikor a HTTP szervert állította be ellenőrzési listák és kliens hitelesítések számára.	Olvassa el a HTTP Server Webmaster's Guide című kiadványt a példány beállításáról. A könyvben leírtakat megtalálhatja az Információs központ Web kiszolgálás című témaköre alatt is.
A Netscape Communicator arra vár, hogy lejárjon a HTTP Server programban lévő konfigurációs direktíva, hogy lehetővé váljon egy másik igazolás kiválasztása.	A nagy igazolás érték nehézkessé teszi a második igazolás regisztrálását, mivel a böngésző még az elsőt használja.
Megpróbálja a böngészővel biztosíttatni az X.509 igazolást a HTTP Server számára, hogy az igazolás felhasználható legyen a QsyAddVldlCertificate API bemeneteként.	Az **SSLEnable** és az **SSLClientAuth ON** API-kat használja, hogy a HTTP szerverrel betöltesse a HTTPS_CLIENT_CERTIFICATE környezeti változót. Az API-k leírását megtalálja az Információs központ OS/400API című témakörében. Esetleg szándékában állhat a következő ellenőrzési listák vagy igazolással kapcsolatos API-k megtekintése: • QsyListVldlCertificates és QSYLSTVC • QsyRemoveVldlCertificate és QRMVVC • QsyCheckVldlCertificate és QSYCHKVC • QsyParseCertificate és QSYPARSC, stb.
Nem találja a kérés fájlt, amelyet a HTTP Server telepítésekor hozott létre. A fájlt a rendszer használja annak jelzésére, hogy érvényes kulcscsomó fájlokat talált a saját alkönyvtárában lévő konfigurációs fájlok KEYFILE direktívájában.	Olvassa el az Áttérés a DCM egy korábbi változatáról cím alatt leírtakat. HTTP Server esetén a helyes fájl a /qibm/userdata/httpsvr/keyring/keymreq.crt. LDAP esetén a helyes fájl a /qibm/userdata/os400/dirsrv/qdirsrv.crt.
A HTTP Server válaszideje túl sok, illetve időn túli, amikor a 10 000 elemet meghaladó ellenőrzési listában lévő igazolások listáját kéri le.	Hozzon létre egy kötegelt munkát, amely egy bizonyos kritérium alapján kiválogatja és törli az igazolásokat, mint például az összes lejárt igazolást, vagy egy bizonyos CA-tól származó összes igazolást.

Probléma	Lehetséges megoldás
Problémát fedezett fel az igazolás tárolókkal kapcsolatban, miután a V4R3 szintre telepítette a V5R2 változatot, és létezik a /qibm/userdata/httpsvr/keyring/keymreq.crt vagy a /qibm/usedata/os400/dirsrv/qdirsrv.crt fájl. A rendszer nem tudta végrehajtani a kulcscsomó fájlok kulcs adatbázisba történő automatikus költöztetését.	A régi kulcscsomó fájlokat adja meg igazolás tárolóként, keresse meg és törölje az érvénytelen vagy a kulcscsomó fájlokból származó igazolásokat, mielőtt hívná a qicss/qyepmgrt programot az újabb költöztetési kísérlethez. Vagy mellőzze és törölje a .crt fájlt, ha a költöztetési tevékenység átvitte az összes fontos igazolást.
A HTTP Server nem indul el sikeresen **SSLEnable** beállítással, és a HTP8351 hibaüzenet jelenik meg a feladatnaplóban. Az *ADMIN szerver hibanaplója hibát mutat, amely szerint az SSL inicializálási művelet 107-es hibakóddal hiúsult meg, amikor a HTTP Server meghiúsult.	A 107-es hiba az igazolás lejártát jelenti. Ha a szerver példány az *ADMIN, akkor ideiglenesen állítsa be az **SSLDisable**-t, hogy használhassa a DCM eszközt az *ADMIN szerveren. A DCM segítségével rendeljen hozzá egy másik igazolást az alkalmazáshoz - például QIBM_HTTP_SERVER_ADMIN - ha a szerver példány az *ADMIN szerver.

Áttérési hibák és helyreállítási megoldások

Hibák és hibajavítás

A következő hibajelzők figyelmeztetnek az áttérés során előforduló hibákra:

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
A hibajelző jelenléte a 34-es opció és az 5722-DG1 sikeres telepítése után azt jelenti, hogy a kulcscsomó költöztetése, amelyet az 5722-DG1 kísérelt meg, nem sikerült. Lehet, hogy át kell költöztetni a kulcscsomót a *SYSTEM igazolás tárolóba.

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT
A hibajelző jelenléte a 34-es opció sikeres telepítése után azt jelenti, hogy a kulcscsomó költöztetése az LDAP szerver számára nem sikerült.

A jelzett hibákon túlmenően előfordulhatnak olyan áttérési hibák is, amelyeket a rendszer esetleg nem jelez. Például, amikor a rendszer olyan kulcscsomó fájlt talál, amelyet költöztetni kell a a *SYSTEM igazolás tárolóba, ami azonban konfliktust eredményezhet az integrált fájlrendszerben meglévő felhasználói adatfájlokkal. Ilyen esetben a rendszer nem feltétlenül végzi el a kulcscsomó fájl költöztetését, még akkor sem, ha egyébként a telepítést sikeresen befejezte.

Ritka forgatókönyv ugyan, de lehetősége van arra, hogy a kulcscsomó fájl átköltöztetését részleges rendszer igazolási hozzárendeléssel végezze el, mielőtt a hiba megakadályozná a költöztetés befejezését. Ez azonban hibákat eredményezhet, amikor elindítja az IBM HTTP Server *ADMIN példányát SSLMODE=ON beállítással. A lehetséges magyarázatok:

- Az átköltöztetett kulcscsomó fájl alapértelmezésként rossz rendszer igazolás készlettel rendelkezik.
- A DCM befejezte a költöztetést felhasználói adatok jelenléte miatt, amelyek egy fontos fájlban vannak.
- Előre nem látható hiba fordult elő a költöztető programban.

Elindíthatja az IBM HTTP szervert az SSLMODE bekapcsolása nélkül (ideiglenesen OFF értékre állítja az SSLMODE paramétert az *ADMIN számára), mielőtt elindítaná az *ADMIN példányt. Ez lehetővé teszi, hogy megvizsgálja az igazolás tárolókat a DCM segítségével, és megoldja a problémát az *ADMIN példány leállása előtt. Miután leállítja az *ADMIN példányt, visszaállíthatja az SSLMODE értékét ON állapotba, és az *ADMIN példány elindításával hibátlanul inicializálhatja az SSL kapcsolatot.

A 34-es opció költöztetése után hibák jelentkezhetnek az igazolás tárolókat használó szokásos DCM kérések alatt. Az ilyen hibák a böngészőben fordulnak elő. Ilyen hibákra utaló példák:

```
Adatbázis hiba
Adatbázis olvasási hiba
Adatbázis írási hiba
Adatbázis sérülés
Adatbázis tábla sérülés
```

Továbbá, a rendszerben lehet default.kdb névvel egy érvénytelen igazolás tároló ugyanabban az alkönyvtárban, mint /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR vagy /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR. Ebben az esetben végre kell hajtani a következő manuális költöztetést, mielőtt új igazolásokat hozna létre a DCM révén.

Megjegyzés: Ha úgy dönt, hogy nem költözteti a kulcscsomó fájlokat, hanem helyette új CA és rendszer igazolást hoz létre, akkor hagyja ki a következő manuális költöztetési eljárást.

- Ha telepíteni kívánja a HTTP Server for iSeries (5722-DG1) terméket, akkor most tegye ezt meg a folytatás előtt.

  Megjegyzések:

  1. Az 5722–SS1 rendszer 34-es opciójának telepítő programja nem kísérli meg újra a költöztetést a 34-es opció telepítése után. A 34-es opció ismételt telepítése egyszerűen nem segít.
  2. A megfelelő fájlok a felhasználói adatokat tartalmazó alkönyvtárakban vannak, létrehozásuk PUBLIC *EXCLUDE jogosultsággal történt. Győződjön meg róla, hogy megfelelő jogosultsággal rendelkezik.
- Nézze meg, hogy a következő fájlok léteznek-e:
  - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

  Ha igen, a WRKLNK parancs segítségével nevezze át őket, és készítsen biztonsági mentést róluk.
- Egy *ALLOBJ jogosultsággal bíró felhasználói profilt felhasználva hívja meg a QICSS/QYEPMGRT programot a parancssorból a következők szerint:

  ```
  CALL QICSS/QYEPMGRT
  ```

  Ha az eredmény sikeres, ellenőrizze, hogy a következő fájlok egyike sem létezik a rendszeren:
  - /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
  - /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

A DCM rendszerint megtartja az olyan fájlokba mentett felhasználói adatok biztonsági másolatát, amelyeknek a nevei konfliktusban vannak a DCM által használt fájlok neveivel. Ha a következő fájlok nem léteznek:

- /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
- /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR

De a következő fájlok léteznek:

- /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH
- /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH

A rendszer megkísérli átnevezni őket .OLD kiterjesztés hozzáfűzésével. Ha már ilyen fájlok is léteznek, a rendszer nem hoz létre egyetlen biztonsági másolatot sem. Helyette, egyszerűen felülírja a meglévő .STH fájlokat.

Egyebek

Ha a CA és a rendszer igazolás létrehozására irányuló kísérletei meghiúsulnak fájlnév ütközések miatt, a következők egyikével találkozhat:

- **Eltérő fájlnév ütközés** – A DCM kísérletet tesz az általa alkönyvtárakban létrehozott felhasználói adatok védelmére, még akkor is, ha ezek a fájlok megakadályozzák, hogy a DCM sikeresen létrehozhassa a számára szükséges fájlokat. Ennek megoldására, másolja át az ütközést okozó fájlokat egy másik alkönyvtárba, és lehetőség szerint törölje az egyező fájlokat a DCM funkciók segítségével. Ha nem használhatja a DCM funkciókat ennek végrehajtásához, akkor manuálisan törölje a fájlokat az integrált fájlrendszer eredeti alkönyvtárából, ahol az ütközés jelentkezett. Feltétlenül jegyezze fel, hogy pontosan melyik fájlt mozgatta és hová. A másolatok lehetővé teszik a fájlok helyreállítását, ha úgy találja, hogy még szükség van rájuk. Új CA-t kell létrehozni a következő fájlok mozgatása után:

  ```
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.KDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.RDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH .OLD
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POL
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.BAK
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STHBAK
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.STH
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TXT
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.BAK
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TMP
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLTMP
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLBAK
  /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CACRT
  /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CATMP
  /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CABAK
  /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CLIENT/*.USRCRT
  ```

  Új *SYSTEM igazolás tárolót és rendszer igazolást kell létrehozni a következő fájlok mozgatása után:

  ```
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.BAK
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.RDB
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH.OLD
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STHBAK
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TMP
  /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TEMP.STH
  /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TMP
  /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.BAK
  /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TXT
  /QIBM/USERDATA/ICSS/CERT/SERVER/SRV.SGN
  /QIBM/USERDATA/ICSS/CERT/SERVER/SGN.TMP
  /QIBM/USERDATA/ICSS/CERT/SERVER/SGN.BAK
  /QIBM/USERDATA/ICSS/CERT/SERVER/EXPSRV.TMP
  /QIBM/USERDATA/ICSS/CERT/SERVER/EXPSGN.TMP
  ```

- **Hiányzó előfeltételek** – Győződjön meg arról, hogy hibátlanul telepítette az előzetes követelményként meghatározott licencprogramokat (LPP).
- **Programhiba** – Lépjen kapcsolatba a szerviz képviselőjével.

Felhasználói igazolás hozzárendelésének hibakeresése

A **Felhasználói igazolás hozzárendelése** feladat használatakor a Digitális igazolás kezelő (DCM) megjeleníti az igazolás információit, hogy jóváhagyja azokat az igazolás regisztrálása előtt. Ha a DCM nem tudja megjeleníteni az igazolást, a problémát az alábbi esetek egyike okozhatja:

1. A böngésző nem kérte, hogy válasszon ki egy igazolást a szervernek való bemutatásra. Ez akkor fordulhat elő, ha a böngésző gyorsítótárában az előző igazolás van (egy másik szerver eléréséből). Próbálja meg törölni a böngésző gyorsítótárát, és ismételje meg a feladatot. A böngészőnek kérni kell a felhasználótól az igazolás kiválasztását.
2. A regisztráltatni kívánt igazolást már regisztráltatta a DCM segítségével.
3. Az Igazolási hatóság, amely kiadta az igazolást, nincs kijelölve megbízható gyökérnek a rendszeren. Ennek következtében, az igazolás, amit bemutat, nem érvényes. Keresse meg a rendszeradminisztrátort, hogy meghatározza, az igazolást kiadó CA helyes-e. Ha a CA helyes, a rendszeradminisztrátornak esetleg **importálni** kell a CA igazolást a *SYSTEM igazolás tárolóba. Vagy a **CA igazolások kezelése** feladat végrehajtásával az adminisztrátor engedélyezheti, hogy a CA megbízható gyökér legyen a rendszeren, így korrigálva a problémát.
4. Nincs igazolás a regisztráltatáshoz. Ellenőrizheti a felhasználói igazolásokat a böngészőben, hogy ez okozza-e a problémát.
5. Az igazolás, amit regisztráltatni próbál, lejárt vagy nem komplett. Vagy meg kell újítani az igazolást, vagy lépjen kapcsolatba a kiadó CA-val a probléma megoldása érdekében.
6. Az IBM HTTP Server for iSeries helytelenül van beállítva az igazolás regisztrálásához, amelyet SSL és kliens hitelesítés segítségével a biztonságos *ADMIN szerver példányon végez. Ha az eddigi hibakeresési tanácsok nem segítenek, keresse meg a rendszeradminisztrátort a probléma jelentése céljából.

A **felhasználói igazolás hozzárendeléséhez** SSL szekcióval kell csatlakozni a Digitális igazolás kezelőhöz (DCM). Ha nem használ SSL protokollt, amikor a **Felhasználói igazolás hozzárendelése** feladatot választja ki, a DCM egy üzenetet ad ki arról, hogy SSL protokollt kell használnia. Az üzenet egy gombot tartalmaz, amely révén SSL protokollal csatlakozhat a DCM-hez. Ha az üzenet gomb nélkül jelenik meg, jelezze a problémát a rendszeradminisztrátornak. A webszervert lehet, hogy újra kell indítani ahhoz, hogy az SSL használatára vonatkozó konfigurációs direktívák aktivizálva legyenek.

Fejezet 10. A DCM-hez kapcsolódó információk

Ahogy egyre elterjedtebbé vált a digitális igazolások használata, a rendelkezésre álló információforrások száma is úgy változott. Az alábbiakban az egyéb források kisebb listáját találja, amelyek révén tovább tanulmányozhatja a digitális igazolásokat, és segítségükkel javíthatja az iSeries biztonsági jellemzőit:

- **VeriSign Help Desk webhely**
  A VeriSign webhely terjedelmes könyvtárral rendelkezik a digitális igazolások témaköréből, valamint számos egyéb Internet biztonsággal kapcsolatos tárgykörből.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Ez az IBM piros 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.
- **AS/400 Internet Security: Developing a Digital Certificate (SG24-5659)**
  Ez a piros könyv ismerteti, hogy mit tehet a digitális igazolásokkal az iSeries szerveren. Elmagyarázza a különféle szerverek és kliensek beállítását az igazolások használatához. Továbbá tájékoztatást és minta programot nyújt annak megismeréséhez, hogyan használhatja az OS/400 API-kat a digitális igazolások kezeléséhez és használatához a felhasználói alkalmazásokban.
- **RFC Index Search**
  Ez a webhely a Request for Comments (RFC) kereshető tárolóhelye. Az RFC-k leírják a digitális igazolások használatához kapcsolódó Internet protokollok - mint például SSL, PKIX és mások - szabványait.

Nyomtatva Dániában