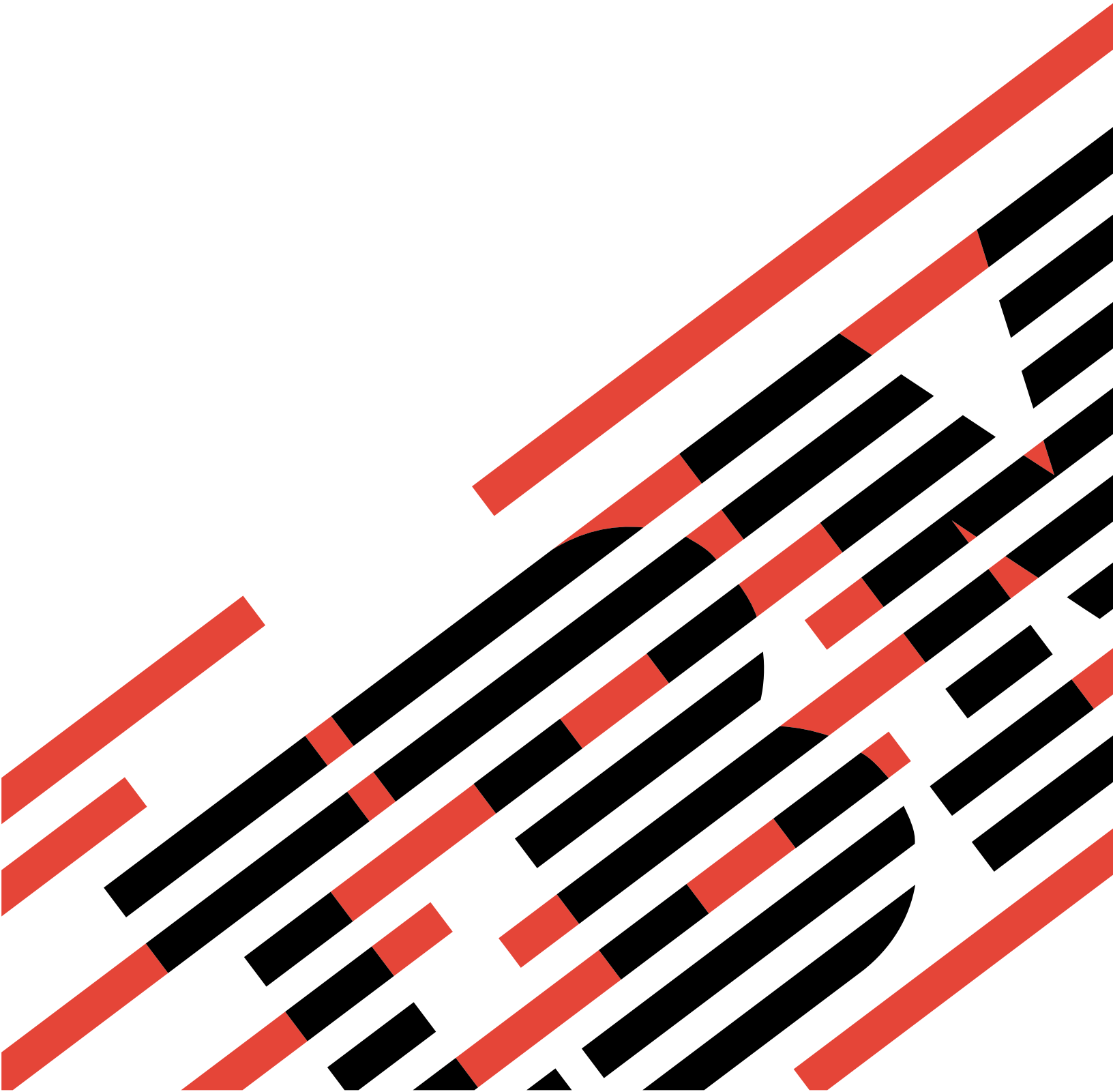
IBM

eserver

iSeries

디지털 인증 관리자



IBM

@server

iSeries

디지털 인증 관리자

목차

제 1 부 디지털 인증 관리자

디지털 인증서는 전자 상거래에서 신원 증명에 사용할 수 있는 전자 증명서입니다. 향상된 네트워크 보안 수단을 제공하기 위해 디지털 인증서를 사용하는 경우가 점차로 증가하고 있습니다. 예를 들어, 디지털 인증서는 보안 소켓층(SSL)을 구성하고 사용하는 데 필수적입니다. SSL을 사용함으로써 인터넷과 같이 신뢰할 수 없는 네트워크에서 사용자들과 서버 어플리케이션 사이의 보안 연결을 생성할 수 있습니다. SSL은 인터넷에서 사용자명 및 암호와 같은 민감한 자료를 보호하기 위한 최선의 솔루션 중 하나를 제공합니다. FTP, 텔넷, iSeries용 HTTP Server 및 다른 제품들과 마찬가지로 많은 iSeries™ 서비스 및 어플리케이션들도 현재 SSL 지원을 제공하여 자료 프라이버시를 보장합니다.

iSeries는 수 많은 보안 어플리케이션에서 디지털 인증서를 증명서로 사용할 수 있도록 확장된 디지털 인증 지원을 제공합니다. SSL을 구성하기 위해 인증서를 사용하는 것 이외에도 SSL 및 VPN(가상 사설망) 트랜잭션에서 클라이언트 인증에 대한 증명서로 인증서를 사용할 수 있습니다. 또한 오브젝트 서명에 디지털 인증서와 그와 연관된 보안 키를 사용할 수 있습니다. 오브젝트 서명은 오브젝트의 무결성을 확인하기 위해 오브젝트에 대한 서명을 확인함으로써 오브젝트의 내용에 대한 변경이나 권한이 없는 변경 처리의 가능성을 감지할 수 있게 합니다.

어플리케이션에 대한 인증서를 중앙에서 관리하기 위해 무상 iSeries 피처인 디지털 인증 관리자(DCM)를 통해 제공되는 iSeries 지원을 이용할 수 있습니다. DCM으로 인증 기관(CA)에서 받은 인증서를 관리할 수 있습니다. 또한 자사의 로컬 CA를 작성하고 운영함으로써 회사에서 사용하는 어플리케이션과 사용자들에게 개인 인증서를 발행할 수 있습니다.

적절한 계획과 평가는 추가된 보안 이점에 있어서 인증서를 효과적으로 사용할 수 있는 열쇠입니다. 인증서의 역할과 인증서를 사용하는 어플리케이션 및 인증서를 관리하기 위해 DCM을 어떻게 사용할 것인지에 관해 자세히 알려면 다음 주제를 검토하십시오.

V5R2의 새로운 사항
DCM 피처에 대한 변경사항 및 이번 릴리스에서의 변경사항에 대해 알 수 있습니다.

이 주제 인쇄
PDF 파일로 전체 내용을 인쇄하는 방법에 관해 알 수 있습니다.

이전 릴리스에서 DCM으로 마이그레이트
최신 릴리스 버전으로 기존 버전의 DCM을 마이그레이트할 때 수행해야 하는 타스크 및 기타 고려사항에 관해 알 수 있습니다.

DCM 시나리오
iSeries 보안 정책의 일부로 사용자 자신의 인증 구현을 계획할 때 도움이 되는 일반적인 인증 구현 체계를 설명하는 두 개의 시나리오가 나옵니다. 또한 시나리오마다 수행해야 하는 모든 구성 타스크를 제공합니다.

디지털 인증 개념
디지털 인증이 무엇이며 그 역할에 관해 알 수 있습니다. 기타 유형의 인증서 및 보안 정책의 일부로 이러한 인증서를 사용할 수 있는 방법에 관해서도 알 수 있습니다.

DCM 계획
사용자의 보안 목표에 맞게 디지털 인증서를 사용하는 방법과 그 시기를 결정하는 데 도움이 됩니다. DCM을 사용하기 전에 고려해야 할 기타 요구사항 뿐만 아니라 설치해야 하는 전제조건에 대해서도 알 수 있습니다.

DCM 구성
인증서 및 그 키를 관리하는 데 DCM을 사용하기 위해 필요한 모든 사항을 구성하는 방법에 관해 알 수 있습니다.

DCM 관리
인증서를 사용하는 어플리케이션과 인증서를 관리하기 위해 DCM을 사용하는 방법에 관해 알 수 있습니다. 또한 오브젝트를 디지털로 서명하는 방법과 자사의 인증 기관을 작성하여 운영하는 방법을 알 수 있습니다.

DCM 문제 해결
DCM을 사용하는 중에 발생할 수 있는 일반적인 오류를 해결하는 방법에 관해 알 수 있습니다.

DCM 관련 정보
디지털 인증서, 공용 키 인프라구조, 디지털 인증 관리자 및 기타 관련 정보에 대한 자세한 내용을 제공하는 관련 링크를 알 수 있습니다.

제 1 장 V5R2의 새로운 사항

V5R2 디지털 인증 관리자(DCM) 및 iSeries 디지털 인증 기능의 향상은 다음을 포함합니다.

- **인증서 지정 기능**
  이 새로운 DCM 타스크는 하나 이상의 어플리케이션에 좀더 빠르고 쉽게 인증서 할당을 할 수 있게 합니다. **인증서 관리** 타스크 리스트 또는 빠른 경로 페이지 **서버 및 인증에서 작업** 및 **인증에 서명하는 오브젝트에서 작업**에서 이 타스크를 액세스할 수 있습니다. *SYSTEM 및 *OBJECTSIGNING 인증서 저장소에서만 이 기능을 사용할 수 있습니다.
- **명령(*CMD) 오브젝트 서명**
  이제 DCM을 사용하여 디지털 서명의 무결성을 확인하는 수단으로 명령(*CMD) 오브젝트에서 이 서명을 작성할 수 있습니다. 또한 *CMD 오브젝트에 대한 서명의 범위를 선택할 수 있고, 전체 *CMD 오브젝트에 서명할지 또는 *CMD 오브젝트의 핵심 구성요소에만 서명할지를 선택할 수 있습니다. DCM을 사용하여 *CMD 오브젝트에서 서명을 볼 때 DCM은 서명의 범위에 대한 정보를 제공합니다.
- **DCM을 사용하지 않고 로컬 CA(인증 기관)에서 서명한 사용자 인증서를 작성하는 API**
  로컬 인증 기관(CA)에서 서명한 인증서를 비iSeries 사용자에 대해 발행하도록 사용할 수 있는 두 가지 새로운 API가 있습니다. 이 API를 사용하면 iSeries 사용자 프로파일을 사용하지 않고 사용자가 DCM을 사용하여 개별적으로 클라이언트 인증에 대한 인증서를 확보해야 할 필요 없이 사용자에게 인증서를 발행할 수 있습니다.

이 주제의 새로운 정보나 향상된 정보는 다음을 포함합니다.

- 인증서를 사용하여 보안 목표를 달성하는 최상의 방법을 판별할 수 있는 두 개의 새로운 시나리오.
- DCM을 사용해야 하는 정보를 빠르게 찾을 수 있도록 보다 쉽게 만드는 재구성된 정보.

이 릴리스의 새로운 사항이나 변경된 사항에 대한 다른 정보를 찾으려면 사용자 메모  를 참조하십시오.

제 2 장 이 주제 인쇄

PDF 버전을 보거나 다운로드하려면 디지털 인증 관리자  (파일 *크기* 약 468KB 또는 약 110 페이지)를 선택하십시오.

PDF 파일을 워크스테이션에 저장하려면 다음과 같이 하십시오.

1. 브라우저에서 PDF 파일을 여십시오(위의 링크를 클릭하십시오).
2. 브라우저 메뉴에서 **파일**을 클릭하십시오.
3. **다른 이름으로 저장...**을 클릭하십시오.
4. PDF 파일을 저장하려는 디렉토리로 이동하십시오.
5. **저장**을 클릭하십시오.

Adobe Acrobat Reader로 PDF를 보거나 인쇄하려는 경우 Adobe 웹 사이트 (www.adobe.com/prodindex/acrobat/readstep.html)  에서 사본을 다운로드할 수 있습니다.

제 3 장 이전 버전의 DCM에서 마이그레이트

V4R3 버전의 디지털 인증 관리자(DCM)에서 V5R2로 마이그레이트할 때 DCM은 기존의 로컬 인증 기관(CA) 및 시스템 인증서 키 링 파일을 자동으로 업그레이드합니다. DCM은 이름이 default.kyr인 이러한 파일들을 이름이 default.kdb인 해당 인증서 저장소 파일로 업그레이드합니다. 또한 DCM은 하이퍼텍스트 전송 프로토콜(HTTP) 및 간단한 디렉토리 액세스 프로토콜(LDAP) 서버와 연관된 키 링 파일의 유효한 모든 인증서를 마이그레이트합니다. DCM은 유효한 인증서를 *SYSTEM 인증서 저장소(default.kdb)로 마이그레이트합니다.

주: DCM의 V4R4, V4R5 또는 V5R1 버전으로부터 마이그레이트하는 경우 이러한 버전의 인증 파일은 DCM의 V5R2 버전과 호환되기 때문에 마이그레이션 타스크를 수행할 필요가 없습니다.

인증서 저장소 마이그레이션에 대한 키 링 - V4R3 마이그레이션

V5R2를 설치하는 동안 시스템은 다음의 키 링 파일을 마이그레이트합니다.

- DCM의 디폴트 키 링 파일.
- HTTP Server 구성 파일이 사용하는 키 링.
- LDAP 서버 구성 파일이 사용하는 키 링.

DCM이 자동으로 업그레이드하지 않은 .kyr 파일을 사용하는 경우 DCM에서 처음으로 이 파일에 대해 작업할 때 DCM은 이를 kyr.kdb 파일로 변환합니다. 예를 들어, DCM 사용자 인터페이스에서 처음 secure.kyr 파일을 지정하면, DCM은 이 파일을 파일명이 secure.kyr.kdb인 새로운 인증서 저장소로 변환합니다.

주: 키 링은 인증서 저장소와 다르므로 DCM 사용자 인터페이스를 통해 키 링 파일에 대해 작업하여 DCM이 자동으로 업그레이드하지 않은 키 링 파일을 변환해야 합니다. 파일명 확장자를 .kdb로 수동 변경하면, 직후에 DCM 사용자 인터페이스를 통해 이러한 파일에 대해 작업하려고 시도할 때 오류가 발생됩니다.

DCM 사용 시에 secure.kyr 파일을 삭제하려고 시도하면, DCM은 이 파일의 아카이브를 작성하고 secure.kyr.kdb 파일을 삭제합니다.

디폴트 인증서 저장소 암호

파일 /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR이 있는 경우 시스템은 이 키 링 파일과 다른 적합한 키 링 파일을 *SYSTEM 인증서 저장소로 마이그레이트합니다. /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR 파일과 연관된 원래의 암호가 *SYSTEM 인증서 저장소에 대한 암호로 사용됩니다.

파일 /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR이 없지만 다른 키 링 파일이 마이그레이트할 자격이 있는 경우(예를 들어, HTTP Server 구성 파일이 사용하는 키 링 파일), 시스템은 DEFAULT(모두 대문자) 암호를 사용하여 *SYSTEM 인증서 저장소를 작성하고 마이그레이션을 완료합니다.

파일 마이그레이션 프로세스 중에 발생할 수 있는 오류에 대한 정보와 그 해결 방법에 대한 정보는 마이그레이션 오류 및 회복 솔루션을 참조하십시오.

제 4 장 DCM 시나리오

사용자의 iSeries가 제공하는 디지털 인증 관리자 및 디지털 인증 지원은 인증서를 사용하여 다른 많은 방법으로 보안 정책을 향상시킬 수 있게 합니다. 인증서의 사용을 선택하는 방법은 사용자의 비즈니스 목표 및 보안 요구에 따라 다릅니다.

디지털 인증서를 사용하는 것은 보안을 향상시키는 데 있어서 여러 가지 방식으로 도움을 줍니다. 디지털 인증서를 통해 웹 사이트 및 기타 인터넷 서비스에 대한 보안 액세스에 보안 소켓층(SSL)을 사용할 수 있습니다. 디지털 인증서를 사용하면 VPN(가상 사설망) 연결을 구성할 수 있습니다. 또한 인증서 키를 사용하여 오브젝트에 디지털로 서명하거나 디지털 서명을 확인하여 오브젝트의 진위를 보장할 수 있습니다. 이러한 디지털 서명은 오브젝트 출처의 신뢰성을 보장하고 오브젝트의 무결성을 보호합니다.

서버와 사용자 간의 세션을 인증하고 권한을 부여하기 위해 (사용자명과 암호 대신) 디지털 인증서를 사용하여 시스템 보안을 더욱 향상시킬 수 있습니다. 또한 DCM을 사용하여 사용자의 인증서를 iSeries 사용자 프로파일과 연관시킬 수 있습니다. 그리고 나면 인증서가 연관된 프로파일과 동일한 권한 및 허가를 갖게 됩니다.

따라서 인증서의 사용 목적을 선택하는 방법이 복잡해질 수 있고 여러 가지 요소에 따라 선택 방법을 달리 할 수 있습니다. 내용 중에 제공되는 시나리오에서는 일반적인 비즈니스에 공통되는 디지털 인증 보안 목표를 설명합니다. 또한 시나리오마다 수행할 때 필요한 모든 시스템과 소프트웨어 전제조건 및 모든 구성 타스크를 설명합니다. 사용자 요구에 가장 적합한 보안 처리를 위해 어떻게 인증서를 사용할 것인지에 관해 알려면 다음 시나리오를 검토하십시오.

시나리오: 인증서를 사용하여 공용 어플리케이션 및 자원에 대한 액세스 보호
이 시나리오는 인증서를 사용하여 공용 사용자들이 공용 자원이나 엑스트라넷 자원 그리고 어플리케이션에 액세스하는 것을 어떻게 보호하고 또한 언제 제한해야 할 것인지에 관해 설명합니다.

시나리오: 인증서를 사용하여 내부 어플리케이션 및 자원에 대한 액세스 보호
이 시나리오는 인증서를 사용하여 내부 사용자가 내부 서버에서 액세스할 수 있는 자원 및 어플리케이션을 보호하고 제한하는 시기 및 방법을 설명합니다.

시나리오: 인증서를 사용하여 공용 어플리케이션 및 자원에 대한 액세스 보호

상황

보험 회사(MyCo., Inc)에 근무하며 회사의 인트라넷 및 엑스트라넷 사이트에서 서로 다른 어플리케이션을 유지보수하는 일을 담당하는 것으로 가정하십시오. 담당 어플리케이션 중에는 수 백개의 독립 에이전트들이 자신의 클라이언트에 대해 견적가를 생성할 수 있게 해 주는 이자율 연산 어플리케이션이 있습니다. 이 어플리케이션이 제공하는 정보

의 특성 상 등록된 에이전트만 이 정보를 사용할 수 있어야 합니다. 따라서 현재 사용자 이름 및 암호 메소드보다 더 안전한 어플리케이션에 사용자 액세스 메소드를 제공하려고 합니다. 신뢰할 수 없는 네트워크에서 이 정보가 전송될 때 권한이 없는 사용자가 이러한 정보를 가로채거나 다른 에이전트에서 이러한 작업에 대한 권한 없이 서로 간에 정보를 공유할 가능성을 고려해야 할 것입니다.

잠시만 시간을 내어 조사해 보더라도 디지털 인증서를 사용하는 것이 필요한 보안을 위한 훌륭한 선택임을 알게 될 것입니다. 인증서를 사용하여 보안 소켓층(SSL)을 통해 이자율 자료의 전송을 보호할 수 있습니다. 궁극적으로 모든 에이전트가 인증서를 사용하여 어플리케이션에 액세스하는 것이 목표라고 할지라도 이를 위해서는 회사 및 에이전트에 일정 시간이 필요하다는 것을 알 수 있습니다. 현재로는 전송 처리에 있어서 SSL이 이러한 민감한 자료의 프라이버시를 보호하므로 현재 사용자 이름 및 암호 인증 메소드를 계속 사용하기로 했습니다.

어플리케이션의 유형과 현재 및 향후 사용자를 위한 인증서 확인 목적에 따라 잘 알려진 인증 기관(CA)에서 발행한 공용 인증서를 사용하여 어플리케이션에 대해 SSL을 구성하기로 했습니다.

장점

이 시나리오에는 다음과 같은 이점이 있습니다.

- 이자율 연산 어플리케이션에 대한 SSL 액세스를 구성하는 데 디지털 인증서를 사용하여 서버 및 클라이언트 사이에 전송된 정보의 보호 및 프라이버시를 보장합니다.
- 클라이언트 인증을 위해 언제든지 사용할 수 있는 디지털 인증서를 통해 권한이 있는 사용자를 식별하는 데 있어서 보다 안전한 메소드를 제공합니다. 사용할 수 없는 위치에서도 사용자 이름 및 암호가 사용하는 클라이언트 인증서는 SSL 세션으로 보호를 받고, 프라이버시를 유지함으로써 이러한 민감한 자료를 보다 안전하게 교환합니다.
- *공용* 디지털 인증서를 사용하여 어플리케이션 및 자료에 대한 액세스를 제한하거나 허용하는 것은 다음의 조건이나 이와 유사한 조건 하에서 실제적인 선택이 될 수 있습니다.
  - 자료 및 어플리케이션들이 서로 다른 수준의 보안을 필요로 합니다.
  - 신뢰할 수 있는 사용자 사이에 턴오버 비율이 발생합니다.
  - 인터넷 웹 사이트 또는 엑스트라넷 어플리케이션과 같이 어플리케이션 및 자료에 공용 액세스를 제공합니다.
  - 해당 어플리케이션 및 자원 또는 관리 상의 이유로 액세스하는 사용자들이 많으므로 본인이 소유하는 인증 기관(CA)을 운영하지 않을 것입니다.
- 이 시나리오에서 공용 인증서를 사용하여 SSL에 대해 이자율 연산 어플리케이션을 구성하면 사용자가 해당 어플리케이션에 액세스를 수행해야 하는 구성 처리 작업이 감소합니다. 대부분의 클라이언트 소프트웨어에는 가장 잘 알려진 인증 기관(CA)의 CA 인증서가 포함되어 있습니다.

목표

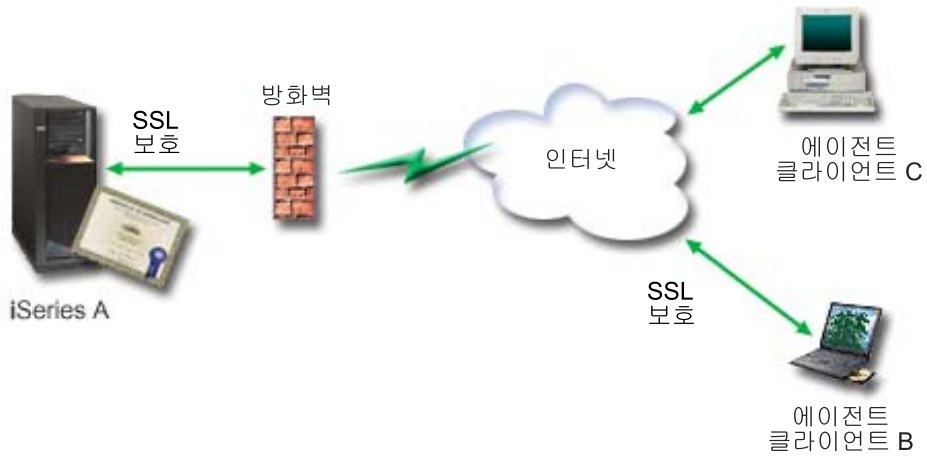
이 시나리오에서 MyCo., Inc.는 디지털 인증서를 사용하여 해당 어플리케이션이 권한이 있는 공용 사용자에게 제공하는 이자율 연산 정보를 보호하려고 합니다. 또한 이 회사는 해당 어플리케이션에 액세스를 허용하는 사용자를 좀더 안전한 메소드로 인증하려고 합니다.

이 시나리오의 목표는 다음과 같습니다.

- 회사 공용 이자율 연산 어플리케이션은 사용자에게 제공하는 자료의 프라이버시를 보호하기 위해 반드시 SSL을 사용해야 합니다.
- SSL 구성은 잘 알려진 공용 인터넷 인증 기관(CA)의 공용 인증서로 수행되어야 합니다.
- SSL 모드로 어플리케이션에 액세스하려면 권한이 있는 사용자가 유효한 사용자 이름 및 암호를 제공해야 합니다. 결국 권한이 있는 사용자가 어플리케이션에 대한 액세스 권한이 부여되는 두 개의 보안 인증 중에서 하나의 메소드를 사용할 수 있어야 합니다. 에이전트는 잘 알려진 인증 기관(CA)의 공용 디지털 인증서 또는 유효한 사용자 이름 및 암호를 제시해야 합니다.

세부사항

다음 그림은 이 시나리오에 대한 네트워크 구성을 나타냅니다.



그림은 이 시나리오의 상황에 대한 다음 정보를 설명합니다.

회사 공용 서버 - iSeries A

- iSeries A는 회사 이자율 연산 어플리케이션을 호스트하는 서버입니다.
- iSeries A는 OS/400® 버전 5 릴리스 2(V5R2)를 실행합니다.
- iSeries A에 암호 액세스 제공자(5722-AC3)가 설치되어 있습니다.
- iSeries A는 디지털 인증 관리자(OS/400 옵션 34) 및 iSeries용 IBM® HTTP Server(5722-DG1)를 설치하고 구성했습니다.

- iSeries A는 이자율 연산 어플리케이션을 실행하며 다음과 같이 구성됩니다.
  - SSL 모드가 필요합니다.
  - SSL 구성의 잘 알려진 인증 기관(CA)에서 공용 인증서를 사용합니다.
  - 사용자 이름 및 암호에 따라 사용자 인증이 필요합니다.
- iSeries A는 클라이언트 B와 C가 어플리케이션에 액세스할 때 SSL 세션을 초기화하는 해당 인증서를 제공합니다.
- SSL 세션을 초기화한 후 iSeries A는 클라이언트 B와 C가 이자율 연산 어플리케이션에 액세스를 허용하기 전에 유효한 사용자 이름 및 암호를 제공하도록 요청합니다.

에이전트 클라이언트 시스템 - 클라이언트 B 및 클라이언트 C

- 클라이언트 B 및 C는 이자율 연산 어플리케이션에 액세스하는 독립 에이전트입니다.
- 클라이언트 B 및 C는 해당 클라이언트 소프트웨어에 설치된 어플리케이션 인증서를 발행한 잘 알려진 인증 기관(CA) 인증서의 사본을 포함합니다.
- 클라이언트 B 및 C는 iSeries A의 이자율 연산 어플리케이션에 액세스하는데 이 어플리케이션은 ID를 검증하고 SSL 세션을 초기화하도록 해당 클라이언트 소프트웨어에 인증서를 제공합니다.
- 클라이언트 B 및 C의 클라이언트 소프트웨어는 iSeries A의 인증서를 승인하도록 구성되고 SSL 세션이 시작됩니다.
- SSL 세션이 시작된 후 클라이언트 B 및 C는 iSeries A가 어플리케이션에 대한 액세스 권한을 부여하기 전에 유효한 사용자 이름 및 암호를 제공해야 합니다.

전제조건 및 가정

이 시나리오는 다음 전제조건 및 가정에 따라 다릅니다.

1. iSeries A의 이자율 연산 어플리케이션은 SSL을 사용하도록 구성할 수 있는 일반 어플리케이션입니다. 많은 iSeries 어플리케이션을 포함하여 대부분의 어플리케이션은 SSL 지원을 제공합니다. SSL 구성 단계는 어플리케이션 사이에 매우 다양합니다. 따라서 이 시나리오는 SSL을 사용하도록 이자율 연산 어플리케이션을 구성하는 특정 지침을 제공하지 않습니다. 이 시나리오는 어플리케이션이 SSL을 사용하는 데 필요한 인증서를 구성하고 관리하는 데 지침을 제공합니다.
2. *선택적으로* 이자율 연산 어플리케이션은 클라이언트의 인증 확인 요청 기능을 제공합니다. 이 시나리오는 디지털 인증 관리자(DCM)를 사용하여 이러한 지원을 제공하는 어플리케이션의 인증 신뢰를 구성하는 방법에 대한 지침을 제공합니다. 클라이언트 인증에 대한 구성 단계가 어플리케이션 사이에 매우 다양하므로 이 시나리오는 이자율 연산 어플리케이션의 인증 클라이언트 확인을 구성하는 데 특정 지침을 제공하지 않습니다.
3. iSeries A는 디지털 인증 관리자(DCM)를 설치하고 사용하기 위한 요구사항과 일치합니다.
4. 누구도 이전에 iSeries A에서 DCM을 구성하거나 사용하지 않았습니다.

5. DCM을 사용하여 타스크를 수행하는 사용자는 누구나 사용자 프로파일에 대한 *SECADM 및 *ALLOBJ 특수 권한이 있어야 합니다.
6. iSeries A에는 IBM 4758-023 PCI 암호 코프로세서가 설치되어 있지 않습니다.

타스크 단계

이 시나리오를 구현하려면 iSeries A에서 이러한 타스크를 수행해야 합니다.

1. 필요한 모든 iSeries 제품을 설치하고 구성하려면 모든 전제조건 단계를 완료하십시오.
2. 서버 인증서 작성 요청은 디지털 인증 관리자(DCM)를 사용하십시오.
3. 보안 소켓층(SSL)을 사용하려면 해당 어플리케이션을 구성하십시오.
4. 해당 어플리케이션의 어플리케이션 ID에 서명된 서버 또는 클라이언트 인증서를 가져오기 또는 할당하려면 DCM을 사용하십시오.
5. 필요한 경우 SSL 모드로 어플리케이션을 시작하십시오.
6. *선택적 타스크*: 해당 지원을 제공하는 어플리케이션의 인증에 따라 클라이언트 인증서를 사용할 수 있도록 CA 신뢰 리스트 정의를 수행하려면 DCM을 사용하십시오.

   주: 이 시나리오가 설명하는 상황에서는 클라이언트 인증서를 위해 이자율 연산 어플리케이션 사용 인증서가 필요하지 않습니다. 많은 어플리케이션에서 인증 클라이언트 확인 지원을 제공합니다. 어플리케이션 사이에 이 지원을 구성하는 방법이 매우 다양합니다. 이 선택적 타스크는 DCM을 사용하여 어플리케이션의 인증 클라이언트 확인 지원을 구성하는 기초로서 클라이언트의 인증 신뢰 확인 방식을 이해하는 데 도움을 주기 위해 제공됩니다.

구성 세부사항

이 시나리오에서 설명하는 것처럼 인증서를 사용하여 어플리케이션 및 자원에 대해 보호된 공용 액세스를 구성하려면 다음 타스크 단계를 완료하십시오.

1단계: 전제조건 타스크를 완료하여 필요한 모든 iSeries 제품 설치

이 시나리오를 구현하는 데 특정 구성 타스크를 수행할 수 있으려면 먼저 모든 필요한 전제조건 타스크를 완료해야만 필요한 모든 iSeries 제품을 설치하고 구성할 수 있습니다.

2단계: 서버 또는 클라이언트 인증 요청 작성

보안 소켓층(SSL)을 사용하는 프로세스를 시작하여 이 시나리오에서 설명하는 것처럼 어플리케이션의 자료 통신을 보호하려면 먼저 공용 인증 기관(CA)에서 디지털 인증서

를 확보해야 합니다. 디지털 인증 관리자(DCM)를 사용하여 공용 인증 기관(CA)에서 인증서를 발행하는 데 필요한 정보를 작성합니다.

인증서를 확보하는 프로세스를 시작하려면 다음 단계를 완료하십시오.

1. DCM 시작.
2. DCM의 탐색 프레임에서 **새 인증서 저장소 작성**을 선택하여 안내 타스크를 시작하고 일련의 양식들을 완성하십시오. 이러한 양식들은 어플리케이션이 SSL 세션에 사용할 수 있는 인증서 저장소와 인증서를 작성하는 프로세스로 안내합니다.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
3. 작성할 인증서 저장소로 ***SYSTEM**을 선택하고 **계속**을 클릭하십시오.
4. *SYSTEM 인증서 저장소 작성의 일부로 인증서를 작성하려면 **예**를 선택하고 **계속**을 클릭하십시오.
5. 새로운 인증의 서명자로 **VeriSign 또는 기타 인터넷 인증 기관(CA)**을 선택하고 **계속**을 클릭하여 새로운 인증에 대한 식별 정보를 제공할 수 있는 양식을 표시하십시오.
6. 양식을 완성하고 **계속**을 클릭하여 확인 페이지를 표시하십시오. 이 확인 페이지는 인증서를 발행할 공용 인증 기관(CA)에 제공해야 하는 인증 요구 자료를 표시합니다. 인증 서명 요구(CSR) 자료는 공용 키와 새로운 인증에 대해 지정한 기타 정보로 구성되어 있습니다.
7. CSR 자료를 공용 CA가 인증 요구를 위해 필요로 하는 인증 어플리케이션 양식이나 별도의 파일로 복사하여 붙여넣으십시오. 새로운 인증 요구 시작 및 종료 행들을 비롯하여 모든 CSR 자료를 사용해야 합니다. 이 페이지에서 나갈 때, 이 자료는 유실되며 회복할 수 없습니다.
8. 인증서를 발행하고 서명하도록 선택한 CA로 어플리케이션 양식이나 파일을 송신하십시오.
9. 해당 시나리오의 다음 타스크 단계를 계속 진행하기 전에 인증 기관(CA)에서 서명하여 완성한 인증서가 리턴되기까지 기다리십시오.

인증 기관(CA)에서 서명하여 완성한 인증서가 리턴되면 어플리케이션을 구성하여 SSL을 사용하고, 인증서를 *SYSTEM 인증서 저장소로 가져온 후 SSL에 사용할 어플리케이션에 이 인증서를 할당할 수 있습니다.

3단계: 사용할 SSL 어플리케이션 구성

공용 인증 기관(CA)에서 다시 서명된 인증서를 수신하면 공용 어플리케이션의 보안 소켓층(SSL) 통신을 사용할 수 있게 하는 프로세스를 계속 수행할 수 있습니다. 서명된 인증에서 작업하기 전에 SSL을 사용하도록 어플리케이션을 구성해야 합니다. iSeries용 HTTP Server와 같은 일부 어플리케이션은 SSL을 사용하는 어플리케이션을 구성할 때

고유 어플리케이션 ID를 생성하고 디지털 인증 관리자(DCM)에 ID를 등록합니다. DCM을 사용하여 서명된 인증서를 여기에 할당하고 SSL 구성 프로세스를 완료할 수 있으려면 먼저 어플리케이션 ID를 알아야 합니다.

SSL을 사용할 어플리케이션을 구성하는 방법은 어플리케이션에 따라 다양합니다. MyCo., Inc.가 해당 에이전트에 이러한 어플리케이션을 제공할 수 있는 방법에는 여러 가지가 있을 수 있으므로 이 시나리오에서는 이자율 연산 어플리케이션을 위한 특정 소스를 가정하지 않습니다.

SSL을 사용할 어플리케이션을 구성하려면 어플리케이션 문서에서 제공하는 지침을 따르십시오. 또한 Information Center 주제 SSL 사용 보안 어플리케이션을 검토하여 SSL을 사용하기 위해 IBM 어플리케이션을 구성하는 것에 대해 자세히 알 수 있습니다.

4단계: 서명된 공용 인증서 가져오기 및 할당

SSL을 사용할 어플리케이션을 구성한 후 디지털 인증 관리자(DCM)를 사용하여 서명된 인증서를 가져오고 이 인증서를 어플리케이션에 할당할 수 있습니다.

인증서를 가져오고 이 인증서를 어플리케이션에 할당하여 SSL 구성 프로세스를 완료하려면 다음 단계를 따르십시오.

1. DCM 시작.
2. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
3. 인증서 저장소 및 암호 페이지가 표시되면, 인증서 저장소를 작성할 때 지정했던 암호를 제공하고 **계속**을 클릭하십시오.
4. 탐색 프레임이 화면정리된 후에 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
5. 타스크 리스트에서 **인증서 가져오기**를 선택하여 서명된 인증서를 *SYSTEM 인증서 저장소로 가져오는 프로세스를 시작하십시오.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
6. 그런 다음 현재 인증서 저장소의 인증 리스트를 표시하려면 **인증서 관리** 타스크 리스트에서 **인증서 할당**을 선택하십시오.
7. 현재 인증서 저장소에 대한 어플리케이션 정의 리스트를 표시하려면 리스트에서 인증서를 선택하고 **어플리케이션에 할당**을 클릭하십시오.
8. 리스트에서 어플리케이션을 선택하고 **계속**을 클릭하십시오. 문제가 발생한 경우 페이지에 할당 선택 또는 오류 메세지의 확인 메세지가 표시됩니다.

이러한 타스크가 완료되면 SSL 모드로 어플리케이션을 시작하고 제공하는 자료의 프라이버시를 보호할 수 있습니다.

5단계: SSL 모드로 어플리케이션 시작

어플리케이션에 인증서를 가져오고 할당하는 프로세스가 완료되면 SSL 모드로 어플리케이션을 종료했다가 재시작해야 할 수 있습니다. 어플리케이션은 실행 중 인증서 할당이 존재하는지를 판별할 수 없으므로 이런 경우에 필요합니다. 어플리케이션을 재시작해야 하는지 여부를 판별하거나 SSL 모드로 어플리케이션 시작에 대한 기타 특정 정보를 보려면 어플리케이션의 해당 문서를 검토하십시오.

(선택적) 6단계: 클라이언트의 인증 확인이 필요한 어플리케이션에 대한 인증 기관(CA) 신뢰 리스트 정의

보안 소켓층(SSL) 세션 중에 클라이언트 확인을 위한 인증 사용을 지원하는 어플리케이션은 인증서를 유효한 신원 증명으로 수락할 것인지의 여부를 판별해야 합니다. 어플리케이션이 인증 확인에 사용하는 기준 중 하나는 어플리케이션이 인증서를 발행한 인증 기관(CA)을 신뢰하는지의 여부입니다.

이 시나리오가 설명하는 상황에서는 클라이언트 인증서를 위해 이자율 연산 어플리케이션 사용 인증서가 필요 없습니다. 많은 어플리케이션에서 인증 클라이언트 확인 지원을 제공하며 그 구성 방식은 어플리케이션에 따라 다릅니다. 이 선택적 타스크는 어플리케이션을 구성하여 클라이언트의 인증 확인을 사용하는 기초로서 DCM을 사용하여 클라이언트의 인증 신뢰 확인 방식을 이해하는 데 도움을 주기 위해 제공됩니다.

어플리케이션에 대한 CA 신뢰 리스트를 정의할 수 있으려면 먼저 몇 가지 조건이 충족되어야 합니다.

- 어플리케이션이 클라이언트 확인을 위한 인증서 사용을 지원해야 합니다.
- 어플리케이션에 대한 DCM 정의가 어플리케이션이 CA 신뢰 리스트를 사용하도록 지정해야 합니다.

어플리케이션에 대한 정의가 어플리케이션이 CA 신뢰 리스트를 사용하도록 지정한 경우 어플리케이션이 인증 클라이언트 확인을 성공적으로 수행할 수 있으려면 먼저 이 리스트를 정의해야 합니다. 그러면, 어플리케이션이 신뢰하는 것으로 지정한 CA에서 이러한 인증만을 유효한 것으로 확인할 수 있습니다. 사용자나 클라이언트 어플리케이션이 CA 신뢰 리스트에서 신뢰하는 것으로 지정되지 않은 CA의 인증서를 제시하면, 어플리케이션은 유효한 확인의 기준으로 이 인증서를 수락하지 않습니다.

DCM을 사용하여 어플리케이션의 인증 기관(CA) 신뢰 리스트를 정의하려면 다음 단계를 완료하십시오.

1. DCM 시작.
2. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
3. 인증서 저장소 및 암호 페이지가 표시되면, 인증서 저장소를 작성할 때 지정했던 암호를 제공하고 **계속**을 클릭하십시오.

4. 탐색 프레임이 화면정리된 후에 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
5. 타스크 리스트에서 인증 기관(CA) 인증서의 리스트를 표시하려면 **인증 기관(CA) 상태 설정**을 선택하십시오.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
6. 인증 기관(CA) 신뢰 리스트를 사용하는 어플리케이션 리스트를 표시하려면 어플리케이션이 신뢰해야 하는 리스트에서 인증 기관(CA) 인증서를 선택하고 **사용 가능**을 누르십시오.
7. 선택된 인증 기관(CA)을 신뢰 리스트에 추가해야 하는 해당 리스트에서 어플리케이션을 선택하고 **확인**을 클릭하십시오. 페이지의 맨 위에 선택한 어플리케이션이 인증 기관(CA) 및 인증 기관이 발행하는 인증서를 신뢰함을 나타내는 메세지가 표시됩니다.

이제 클라이언트의 인증 확인이 필요한 어플리케이션을 구성할 수 있습니다. 어플리케이션에 대한 문서에서 제공한 지침을 따르십시오.

시나리오: 인증서를 사용하여 내부 어플리케이션 및 자원에 대한 액세스 보호

상황

사용자는 인사부에서 법적인 문제 및 개인 기밀과 같은 문제에 관심이 있는 회사(MyCo., Inc.)의 네트워크 관리자입니다. 회사 직원은 개인적인 이득과 의료 보험 정보 온라인에 액세스할 수 있도록 요청했습니다. 회사에서는 내부 웹 사이트를 작성하여 이 정보를 직원에게 제공함으로써 이러한 요청에 응답했습니다. 이 내부 웹 사이트를 관리하는 일을 담당합니다.

직원들이 지리적으로 분리된 사무실에 위치하고 일부 직원들은 종종 외부로 출장을 나가 있으므로 인터넷을 이용할 때 이러한 정보를 개인적으로 유지하는 데 관심을 갖습니다. 또한 일반적으로 사용자 이름 및 암호 인증서를 사용하여 회사 자료에 대한 액세스 권한을 제한합니다. 이 자료의 민감하고도 개인적인 특성 상 암호를 기반으로 자료에 대한 액세스 권한을 제한하는 것은 충분하지 않을 수 있습니다. 결국, 사람들은 암호를 공유하고, 잊고, 심지어 훔치기까지 합니다.

잠시만 시간을 내어 조사해 보면 디지털 인증서를 사용하는 것이 필요한 보안을 위한 훌륭한 선택임을 알게 될 것입니다. 인증서를 사용하여 보안 소켓층(SSL)을 통해 자료의 전송을 보호할 수 있습니다. 또한 암호 대신 인증서를 사용하여 보다 안전하게 사용자를 인증하고 액세스할 수 있는 인적 자원 정보를 제한할 수 있습니다.

따라서 개인 로컬 인증 기관(CA)을 설정하고 모든 사원들에게 인증서를 발행하여 사원들이 자신의 iSeries 사용자 프로파일과 인증서를 연관시키도록 결정합니다. 이러한 유형의 개인 인증서 구현을 통해 SSL을 사용하여 자료의 프라이버시를 제어할 뿐만 아니라 민감한 자료에 대한 액세스를 보다 철저하게 제어할 수 있습니다. 궁극적으로 인증서를 발행함으로써 자료의 보안을 유지하고 특정 개인만 액세스할 수 있게 했습니다.

장점

이 시나리오에는 다음과 같은 이점에 있습니다.

- 인적 자원 웹 서버에 대한 SSL 액세스를 구성하는 데 디지털 인증서를 사용하여 서버 및 클라이언트 사이에 전송된 정보의 보호 및 프라이버시를 보장합니다.
- 클라이언트 인증을 위해 언제든지 사용할 수 있는 디지털 인증서를 통해 권한이 있는 사용자를 식별하는 데 있어서 보다 안전한 메소드를 제공합니다.
- *개인* 디지털 인증서를 사용하여 어플리케이션 및 자료에 대한 액세스를 제한하거나 허용하는 것은 다음의 조건이나 이와 유사한 조건 하에서 실제적인 선택이 될 수 있습니다.
  - 특히 사용자 확인과 관련하여 높은 수준의 보안을 요구합니다.
  - 인증서를 발행하는 개인을 신뢰합니다.
  - 사용자가 어플리케이션 및 자료에 대한 액세스를 제어하기 위해 이미 iSeries 사용자 프로파일을 가지고 있습니다.
  - 사용자의 인증 기관(CA)을 운영합니다.
- 클라이언트의 개인 인증서 확인을 사용하여 인증서를 권한이 있는 사용자의 iSeries 사용자 프로파일과 좀더 쉽게 연관시킬 수 있습니다. 인증 처리 중에 사용자 프로파일과 이러한 인증서를 연관시킴으로써 HTTP Server가 인증서 소유자의 사용자 프로파일을 판별할 수 있습니다. 그리고 나면 HTTP Server가 이것을 전환하여 사용자 프로파일 아래에서 실행하거나 사용자 프로파일의 정보에 따라 사용자를 위한 조치를 수행할 수 있습니다.

목표

이 시나리오에서 MyCo., Inc.는 디지털 인증서를 사용하여 내부 인적 자원 웹 사이트가 회사 직원에게 제공하는 민감한 개인 정보를 보호하려고 합니다. 또한 회사는 이 웹 사이트에 액세스를 허용하는 사용자를 좀더 안전한 메소드로 인증하려고 합니다.

이 시나리오의 목표는 다음과 같습니다.

- 회사 내부 인적 자원 웹 사이트에서 사용자에게 제공하는 자료의 프라이버시를 보호하려면 SSL을 사용해야 합니다.
- SSL 구성은 내부 로컬 인증 기관(CA)에서 개인 인증서로 수행되어야 합니다.
- 권한이 있는 사용자는 SSL 모드로 인적 자원 웹 사이트에 액세스하려면 유효한 인증서를 제공해야 합니다.

세부사항

다음 그림은 이 시나리오에 대한 네트워크 구성 상황을 설명합니다.

그림은 이 시나리오의 상황에 대한 다음 정보를 설명합니다.

회사 인적 자원 웹 서버 - iSeries A

- iSeries A는 회사의 웹 기반 인적 자원 어플리케이션을 호스트하는 서버입니다.
- iSeries A는 OS/400 버전 5 릴리스 2(V5R2)를 실행합니다.
- iSeries A에 암호 액세스 제공자(5722-AC3)가 설치되어 있습니다.
- iSeries A는 디지털 인증 관리자(OS/400 옵션 34) 및 iSeries용 IBM HTTP Server(5722-DG1)를 설치하고 구성했습니다.
- iSeries A는 인적 자원 어플리케이션을 실행하는데 이것은 다음과 같이 구성됩니다.
  - SSL 모드가 필요합니다.
  - SSL 구성에 대해 로컬 인증 기관(CA)에서 개인 인증서를 사용합니다.
  - 클라이언트의 인증 확인이 필요합니다.
- iSeries A는 클라이언트 B, C 및 D가 어플리케이션에 액세스할 때 SSL 세션을 초기화하는 해당 인증서를 제공합니다.
- SSL 세션을 초기화한 후 iSeries A는 클라이언트 B, C 및 D가 인적 자원 어플리케이션에 액세스를 허용하기 전에 유효한 사용자 인증서를 제공합니다. 이러한 인증 교환은 클라이언트 B, C 및 D의 사용자에게 투명합니다.

직원 클라이언트 시스템 - 클라이언트 B, 클라이언트 C 및 클라이언트 D

- 클라이언트 B는 iSeries A가 위치한 MyCo의 본사에서 근무하는 직원입니다.
- 클라이언트 C는 본사에서 지리적으로 분리되어 있는 MyCo의 지사에서 근무하는 직원입니다.
- 클라이언트 D는 리모트로 근무하고 회사 업무상 종종 출장을 가는 직원으로 실제 위치에 관계 없이 인적 자원 웹 사이트에 안전하게 액세스할 수 있어야 합니다.
- 클라이언트 B, C 및 D는 인적 자원 어플리케이션에 액세스하는 회사 직원입니다.

- 클라이언트 B, C 및 D는 모두 클라이언트 소프트웨어에 설치된 어플리케이션 인증서를 발행한 로컬 CA 인증서의 사본을 소유합니다.
- 클라이언트 B, C 및 D는 iSeries A의 인적 자원 어플리케이션에 액세스하는데 이 어플리케이션은 ID를 검증하고 SSL 세션을 초기화하도록 해당 클라이언트 소프트웨어에 인증서를 제공합니다.
- 클라이언트 B, C 및 D의 클라이언트 소프트웨어는 iSeries A의 인증서를 승인하도록 구성되고 SSL 세션이 시작됩니다.
- SSL 세션이 시작된 후 클라이언트 B, D 및 D는 iSeries A가 어플리케이션 및 해당 자원에 대한 액세스 권한을 부여하기 전에 유효한 인증서를 제공해야 합니다.

전제조건 및 가정

이 시나리오는 다음 전제조건 및 가정에 따라 다릅니다.

1. iSeries용 IBM HTTP Server는 iSeries A의 인적 자원 어플리케이션을 실행합니다. 두 가지 유형의 iSeries용 HTTP Server(기본 및 Apache로 구현)가 있으며 본 정보의 공개 이후에는 많은 부분이 수정된 HTTP Server 버전을 사용할 수 있을 것입니다. 따라서 이 시나리오는 SSL을 사용하도록 HTTP Server를 구성하는 *특정* 지침을 제공하지 않습니다. 이 시나리오는 어플리케이션이 SSL을 사용하는 데 필요한 인증서를 구성하고 관리하는 데 지침을 제공합니다.
2. HTTP Server는 클라이언트의 인증 확인을 요청하는 기능을 제공합니다. 이 시나리오는 디지털 인증 관리자(DCM)를 사용하여 이 시나리오의 인증서 관리 요구사항을 구성하는 데 대한 지침을 제공합니다. 그러나 이 시나리오는 HTTP Server의 인증 클라이언트 확인을 구성하는 *특정* 구성 단계를 제공하지 않습니다.
3. iSeries A용 인적 자원 HTTP Server가 이미 암호 보호를 사용하고 있습니다.
4. iSeries A는 디지털 인증 관리자(DCM)를 설치하고 사용하기 위한 요구사항과 일치합니다.
5. 누구도 이전에 iSeries A에서 DCM을 구성하거나 사용하지 않았습니다.
6. DCM을 사용하여 타스크를 수행하는 사용자는 누구나 사용자 프로파일에 대한 *SECADM 및 *ALLOBJ 특수 권한이 있어야 합니다.
7. iSeries A에는 IBM 4758-023 PCI 암호 코프로세서가 설치되어 있지 않습니다.

타스크 단계

이 시나리오를 구현하기 위해 완료해야 하는 두 개의 타스크 집합이 있습니다. 하나의 타스크 집합은 iSeries A에서 인적 자원 어플리케이션을 설정하여 SSL을 사용하고 사용자의 인증 확인을 필요로 할 수 있습니다. 다른 타스크 집합은 클라이언트 B, C 및 D의 사용자가 인적 자원 어플리케이션의 SSL 세션에 참여하고 사용자의 인증 확인을 확보할 수 있게 합니다.

인적 자원 웹 서버 어플리케이션 타스크 단계

이 시나리오를 구현하려면 iSeries A에서 이러한 타스크를 수행해야 합니다.

1. 필요한 모든 iSeries 제품을 설치하고 구성하려면 모든 전제조건 단계를 완료하십시오.
2. SSL을 사용하고 서버 인스턴스의 어플리케이션 ID를 메모하려면 인적 자원 HTTP server를 구성하십시오.
3. 디지털 인증 관리자(DCM)를 사용하여 로컬 인증 기관(CA) 작성 및 운영 작업을 수행하고 인적 자원 HTTP Server의 인증서를 발행합니다. 또한 이 안내된 타스크는 웹 서버 어플리케이션에 인증서를 할당하고 인증 기관(CA)을 어플리케이션이 신뢰하는 인증 리스트에 추가해야 합니다.
4. 클라이언트의 인증 확인이 필요한 인적 자원 웹 서버를 구성하십시오.
5. SSL 모드로 인적 자원 HTTP Server를 시작하십시오.

클라이언트 구성 타스크 단계

이 시나리오를 구현하려면 iSeries A의 인적 자원 웹 서버에 액세스하는 각 사용자(클라이언트 B, C 및 D)가 다음 작업을 수행해야 합니다.

6. 해당 브라우저 소프트웨어에서 로컬 인증 기관(CA) 인증서의 사본 설치를 수행하십시오.
7. 로컬 인증 기관(CA)에서 인증 요청을 수행하십시오.

구성 세부사항

이 시나리오에서 설명하는 것처럼 인증서를 사용하여 내부 어플리케이션 및 자원의 보호된 액세스를 구성하려면 다음 타스크 단계를 완료하십시오.

1단계: 전제조건 타스크를 완료하여 필요한 모든 iSeries 제품 설치

이 시나리오를 구현하는 데 특정 구성 타스크를 수행할 수 있으려면 먼저 모든 필요한 전제조건 타스크를 완료해야만 필요한 모든 iSeries 제품을 설치하고 구성할 수 있습니다.

2단계: SSL을 사용하기 위한 인적 자원 HTTP Server 구성

iSeries A에서 인적 자원 HTTP Server의 보안 소켓층(SSL) 구성 단계는 원래대로 사용할지 또는 Apache 버전에 기반하여 사용할지에 따라 달라집니다.

SSL을 사용할 HTTP Server(원래)를 구성하는 데 대한 특정 정보를 보려면 HTTP Server에서 보안 서버 구성을 참조하십시오.

SSL을 사용할 HTTP Server(Apache에 기반한)를 구성하는 데 대한 특정 정보는 시나리오: JKL은 HTTP Server(Apache에 기반한)에서 보안 소켓층(SSL) 보호 가능을 참조하십시오. 이 시나리오는 가상 호스트를 작성하고 SSL을 사용할 이 호스트를 구성

하는 데 모든 타스크 단계를 제공합니다. SSL을 구성하는 특정 단계를 보려면 머리말 ″가상 호스트에 대해 SSL 작동 가능″을 참조하십시오.

iSeries용 HTTP Server의 현재 버전 및 향후 버전(기본 또는 Apache로 구현)과 관련하여 그 구성에 관한 자세한 내용은 웹 서빙 주제를 참조하십시오.

3단계: 로컬 인증 기관(CA) 작성 및 운영

보안 소켓층(SSL)을 사용할 인적 자원 HTTP Server를 구성한 후 SSL을 초기화하기 위해 서버가 사용할 인증서를 구성해야 합니다. 이 시나리오의 목표에 기초하여 로컬 인증 기관(CA)을 작성하고 운영하도록 선택하여 해당 서버에 인증서를 발행했습니다.

디지털 인증 관리자(DCM)를 사용하여 로컬 인증 기관(CA)을 작성할 때 어플리케이션에 대해 SSL이 작동될 수 있는 모든 사항이 구성되었는지 확인하는 프로세스를 수행합니다. 이것은 로컬 인증 기관(CA)이 웹 서버 어플리케이션에 발행하는 인증서 할당을 포함합니다. 또한 로컬 인증 기관(CA)을 웹 서버 어플리케이션의 인증 기관(CA) 신뢰 리스트에 추가합니다. 어플리케이션의 신뢰 리스트에 로컬 인증 기관(CA)이 있으면 어플리케이션이 로컬 인증 기관(CA)이 발행하는 인증 기관이 있는 사용자를 인식하고 인증할 수 있어야 합니다.

디지털 인증 관리자(DCM)를 사용하여 로컬 인증 기관(CA)을 작성 및 운영하고 인적 자원 서버 어플리케이션에 인증서를 발행하려면 다음 단계를 완료하십시오.

1. DCM 시작.
2. DCM의 탐색 프레임에서 **인증 기관(CA) 작성**을 선택하여 일련의 양식들을 표시하십시오. 이 양식들은 로컬 CA를 작성하고 SSL, 오브젝트 서명 및 서명 확인을 위해 디지털 인증서를 사용할 때 필요한 다른 타스크를 완료하는 프로세스로 안내합니다.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
3. 이 안내된 타스크에 대한 양식을 완료하십시오. 작업 중인 로컬 인증 기관(CA)을 설정하는 데 필요한 모든 타스크를 수행하기 위해 이러한 양식들을 사용할 때, 다음과 같이 수행하십시오.
   a. 로컬 CA에 대한 식별 정보를 제공하십시오.
   b. 소프트웨어가 로컬 CA를 인식하고 로컬 CA가 발행한 인증서를 확인할 수 있도록 로컬 CA 인증서를 PC나 브라우저에 설치하십시오.
   c. 로컬 CA에 대한 정책 자료를 선택하십시오.

      주: 로컬 인증 기관(CA)이 사용자 인증서를 발행할 수 있도록 선택해야 합니다.
   d. 새로운 로컬 CA를 사용하여 어플리케이션이 SSL 연결에 사용할 수 있는 서버 또는 클라이언트 인증서를 발행하십시오.

e. SSL 연결에 서버 또는 클라이언트 인증서를 사용할 수 있는 어플리케이션을 선택하십시오.

   주: 인적 자원 HTTP Server의 어플리케이션 ID를 선택해야 합니다.

f. 새로운 로컬 CA를 사용하여 어플리케이션이 오브젝트에 디지털로서명하는 데 사용할 수 있는 오브젝트 서명 인증서를 발행하십시오. 이 하위 타스크는 *OBJECTSIGNING 인증서 저장소를 작성하며 이것은 오브젝트 서명 인증서를 관리하는 데 사용하는 인증서 저장소입니다.

   주: 이 시나리오가 오브젝트 서명 인증서를 사용하지 않아도 이 단계를 완료해야 합니다. 현시점에서 타스크를 취소하는 경우 이 타스크가 종료되고 별도의 타스크를 수행해야만 SSL 인증서 구성을 완료할 수 있습니다.

g. 로컬 CA를 신뢰해야 하는 어플리케이션을 선택하십시오.

   주: 로컬 인증 기관(CA)을 신뢰하는 하나의 어플리케이션으로서 인적 자원 HTTP Server의 어플리케이션 ID를 선택해야 합니다.

웹 서버 어플리케이션이 SSL을 사용하는 데 필요한 인증 구성을 완료했으므로 사용자의 인증 확인이 필요한 웹 서버 어플리케이션을 구성할 수 있습니다.

4단계: 클라이언트의 인증 확인이 필요한 인적 자원 웹 서버 구성

iSeries A에서 인적 자원 HTTP Server의 클라이언트 인증 확인이 필요한 보안 소켓층(SSL) 구성 단계는 어플리케이션을 원래대로 사용할지 또는 Apache 버전에 기반하여 사용할지에 따라 달라집니다.

클라이언트의 인증 확인이 필요한 HTTP Server(원래)를 구성하는 데 대한 자세한 특정 내용은 HTTP Server(원래)의 보호 설정 작성을 참조하십시오.

클라이언트의 인증 확인을 사용하는 HTTP Server(Apache에 기반한)를 구성하는 데 대한 특정 정보는 시나리오: JKL은 HTTP Server(Apache에 기반한)에서 보안 소켓층(SSL) 보호 가능을 참조하십시오. 이 HTTP Server 시나리오는 가상 호스트를 작성하고 SSL 및 클라이언트의 인증 확인을 사용할 이 호스트를 구성하는 데 모든 타스크 단계를 제공합니다. SSL 및 클라이언트의 인증 확인을 구성하는 특정 단계를 보려면 머리글 ″가상 호스트에 대해 SSL 작동 가능″을 참조하십시오.

iSeries용 HTTP Server의 현재 및 향후 버전(기본 또는 Apache로 구현)과 관련하여 그 구성에 관한 자세한 내용은 웹 서빙 주제를 참조하십시오.

5단계: SSL 모드로 인적 자원 웹 서버 시작

HTTP Server를 중단했다가 재시작해야만 서버에서 인증서 할당이 존재하는지 판별하고 이것을 사용하여 SSL 세션을 초기화할 수 있습니다.

HTTP Server(원래)를 중단했다가 시작하려면 구성 및 관리 양식을 사용하고 다음 단계를 따르십시오.

1. **관리**를 클릭하십시오.
2. **HTTP Server 관리**를 클릭하십시오.
3. 서버를 선택하십시오.
4. 해당 양식에서 제공하는 선택적 시작 매개변수를 필드에 입력하십시오.
5. **시작**을 클릭하십시오.

주: 인증서 할당을 수행할 때 서버를 실행 중인 경우 이 서버를 중단했다가 시작해야 합니다. **재시작**을 클릭하여 항상 서버 실행 중 발생한 인증 변경사항을 판별할 수 있는 것은 아닙니다.

HTTP Server(Apache에 기반한)를 중단했다가 시작하려면 구성 및 관리 양식을 사용하고 다음 단계를 따르십시오.

1. **관리**를 클릭하십시오.
2. 왼쪽 메뉴에 있는 **일반 서버 관리**에서 **HTTP Server 관리**를 클릭하십시오.
3. 작업하려는 서버를 선택한 후 **시작** 또는 **중단**을 클릭하십시오. 시작 매개변수에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

iSeries용 HTTP Server의 현재 및 향후 버전(기본 또는 Apache로 구현)을 관리하는 것에 대한 자세한 내용은 웹 서빙 주제를 참조하십시오.

이러한 타스크가 완료되면 SSL 모드로 인적 자원 어플리케이션을 시작하고 제공하는 자료의 프라이버시를 보호할 수 있습니다.

6단계: 사용자가 해당 브라우저 소프트웨어에서 로컬 인증 기관(CA) 인증서의 사본을 설치하게 하기.

사용자가 보안 소켓층(SSL) 연결을 제공하는 서버에 액세스할 때 서버는 사용자의 클라이언트 소프트웨어에 신원 증명으로 인증서를 제시합니다. 그러면, 클라이언트 소프트웨어는 서버가 세션을 설정하기 전에 서버 인증의 유효성을 확인해야 합니다. 서버 인증의 유효성을 확인하려면, 클라이언트 소프트웨어는 서버 인증서를 발행한 인증 기관(CA)의 로컬로 저장된 인증 사본에 액세스할 수 있어야 합니다. 서버가 공용 인터넷 CA의 인증서를 제시하는 경우 브라우저나 다른 클라이언트 소프트웨어는 CA 인증서의 사본을 이미 가지고 있어야 합니다. 이 시나리오에서처럼 서버가 개인 로컬 인증 기관(CA)의 인증서를 제시하는 경우 각 사용자는 디지털 인증 관리자(DCM)를 사용해야만 로컬 인증 기관(CA)의 사본을 설치할 수 있습니다.

각 사용자(클라이언트 B, C 및 D)가 이 단계를 완료해야만 로컬 인증 기관(CA) 인증서의 사본을 확보할 수 있습니다.

1. DCM 시작.

2. 탐색 프레임에서 **PC에 로컬 CA 인증서 설치**를 선택하여 로컬 CA 인증서를 브라우저에 다운로드하거나 시스템의 파일에 저장할 수 있게 하는 페이지를 표시하십시오.
3. 인증서를 설치하려면 해당 옵션을 선택하십시오. 이 옵션은 브라우저의 신뢰 루트로 로컬 인증 기관(CA) 인증서를 다운로드합니다. 이렇게 하면 브라우저가 이 인증 기관(CA)의 인증서를 사용하는 웹 서버에서 보안 통신 세션을 설정할 수 있습니다. 브라우저는 설치 완료를 돕기 위해 일련의 창들을 표시합니다.
4. **확인**을 클릭하여 Digital Certificate Manager 홈 페이지로 가십시오.

7단계: 각 사용자가 로컬 인증 기관(CA)에서 인증 요청

이전 단계에서 사용자의 인증 확인이 필요한 인적 자원 웹 서버를 구성했습니다. 이제 사용자가 웹 서버에 액세스할 수 있으려면 먼저 로컬 인증 기관(CA)에서 유효한 인증서를 제시해야 합니다. **인증서 작성** 타스크를 사용하여 인증서를 확보하려면 각 사용자는 디지털 인증 관리자(DCM)를 사용해야 합니다. 로컬 CA에서 인증서를 확보하려면, 로컬 CA 정책이 CA가 사용자 인증서를 발행하도록 허용해야 합니다.

각 사용자(클라이언트 B, C 및 D)가 이 단계를 완료해야만 인증서를 확보할 수 있습니다.

1. DCM 시작.
2. 탐색 프레임에서 **인증서 작성**을 선택하십시오.
3. 작성할 인증 유형으로 **사용자 인증서**를 선택하십시오. 인증서에 대한 식별 정보를 제공할 수 있는 양식이 표시됩니다.
4. 이 양식을 완성하고 **계속**을 클릭하십시오.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
5. 현재로는 DCM이 인증서에 대한 개인 및 공용 키를 작성하기 위해 브라우저를 이용하여 작업합니다. 브라우저는 창을 표시하여 이 프로세스를 안내합니다. 이러한 타스크에 대한 브라우저의 지침을 따르십시오. 브라우저가 키를 생성한 후에 DCM이 인증서를 작성했음을 나타내는 확인 페이지가 표시됩니다.
6. 브라우저 소프트웨어에 새로운 인증서를 설치하십시오. 브라우저는 창을 표시하여 이 프로세스를 안내합니다. 브라우저가 이 타스크를 완료하기 위해 제공될 때 지시를 따르십시오.
7. 타스크를 완료하려면 **확인**을 클릭하십시오.

처리되는 동안 디지털 인증 관리자는 인증서와 iSeries 사용자 프로파일을 자동으로 연관시킵니다.

제 5 장 디지털 인증 개념

시스템 및 네트워크 보안 정책을 향상시키기 위해 디지털 인증서 사용을 시작하기 전에 디지털 인증서 및 디지털 인증서가 제공하는 보안 이점을 이해해야 합니다.

디지털 인증서는 인증서 소유자의 신원을 확인하는 디지털 증명서로 여권과 매우 유사합니다. 인증 기관이라고 하는 신뢰할 수 있는 상대가 사용자 및 서버 또는 클라이언트 어플리케이션에 디지털 인증서를 발행합니다. CA에 대한 신뢰는 유효한 신용장인 인증에 대해 신뢰의 기초가 됩니다.

디지털 인증 개념에 대해 자세히 알려면 다음 주제를 검토하십시오.

구별된 이름
디지털 인증의 식별 특성에 대해 자세히 알려면 이 정보를 읽어보십시오.

디지털 서명
디지털 서명이 무엇이고 오브젝트 무결성을 확인하기 위해 어떻게 작업하는지 알려면 이 정보를 읽어보십시오.

공용-개인 키 쌍
디지털 인증서와 연관된 보안 키를 자세히 알려면 이 정보를 읽어보십시오.

인증 기관(CA)
디지털 인증서를 발행하는 단체인 CA에 대해 자세히 알려면 이 정보를 읽으십시오.

CRL 위치
인증서 취소 리스트(CRL)와 이 리스트가 인증 확인 프로세스에 어떻게 사용되는지를 알려면 이 정보를 읽으십시오.

인증서 저장소
인증서 저장소와 인증서 저장소 및 여기에 들어 있는 인증에 대해 작업하기 위해 디지털 인증 관리자(DCM)를 사용하는 방법을 알려면 이 정보를 읽으십시오.

암호
암호와 보안을 제공하기 위해 디지털 인증서에서 암호를 사용하는 방법에 관해 알려면 이 정보를 읽으십시오.

보안 소켓층(SSL)
SSL에 대한 간략한 설명을 보려면 이 정보를 읽어보십시오.

구별된 이름

각 CA에는 CA가 인증서를 발행하기 위해 요구하는 식별 정보를 판별하기 위한 정책이 있습니다. 일부 공용 인터넷 인증 기관은 이름 및 전자 우편 주소와 같은 아주 적은 정보를 요구할 수 있습니다. 다른 공용 CA는 인증서를 발행하기 전에 자세한 정보를 요구하고 이 식별 정보의 보다 엄격한 증명을 요구할 수 있습니다. 예를 들어, 공용 키 인프라구조 교환(PKIX) 표준을 지원하는 CA는 인증서를 발행하기 전에 등록 기관(RA)

을 통해 리퀘스터가 신원 정보를 확인하도록 요구할 수 있습니다. 결국, 인증서를 증명서로 수락하고 사용할 계획이면, 요구사항이 보안 필요에 적합한지를 판별하기 위해 CA에 대한 식별 요구사항을 검토하십시오.

구별된 이름(DN)은 인증서 소유자의 식별 정보를 설명하는 용어이며 인증 자체의 일부분입니다. 인증서를 발행한 CA의 식별 정책에 따라 DN에는 다양한 정보가 포함될 수 있습니다. 디지털 인증 관리자(DCM)를 사용하여 개인 인증 기관을 운영하고 개인 인증서를 발행할 수 있습니다. 또한 DCM을 사용하면 사용자의 조직에 대해 공용 인터넷 CA가 발행하는 인증의 DN 정보와 키 쌍을 생성할 수 있습니다. 어느 인증 유형에나 제공할 수 있는 DN 정보는 다음과 같습니다.

- 인증서 소유자의 일반 이름
- 조직
- 조직 단위
- 나라
- 시
- 구

DCM을 사용하여 개인 인증서를 발행하는 경우 다음을 비롯하여 인증에 대한 추가 DN 정보를 제공할 수 있습니다.

- 버전 4 IP 주소
- 완전 규정 정의역명
- 전자 우편 주소

VPN(가상 사설망) 연결을 구성하기 위해 인증 사용 계획을 하는 경우 이 추가 정보가 유용합니다.

디지털 서명

전자 문서나 다른 오브젝트의 디지털 서명은 암호 형태를 사용하여 작성되며 서면 문서의 개인 서명과 동등합니다. 디지털 서명은 오브젝트의 출처에 대한 증명과 오브젝트의 무결성을 검증하는 수단을 제공합니다. 디지털 인증서 소유자는 인증서의 개인 키를 사용하여 오브젝트에 ″서명″합니다. 오브젝트의 수신자는 인증서의 해당 공용 키를 사용하여 서명을 해독함으로써 서명된 오브젝트의 무결성을 확인하고 송신자를 소스로 확인합니다.

인증 기관(CA)은 발행한 인증서에 서명합니다. 이 서명은 인증 기관의 개별 키로 암호화되는 자료 스트링으로 구성됩니다. 그러면 사용자는 서명을 해독하기 위해 인증 기관 공용 키를 사용하여 인증서에 대한 서명을 확인할 수 있습니다.

디지털 서명은 사용자나 어플리케이션이 디지털 인증서의 개인 키를 사용하여 오브젝트에 대해 작성하는 전자 서명입니다. 오브젝트의 디지털 서명은 서명자(서명 키의 소유자) ID의 고유 전자 바인딩을 오브젝트의 출처에 제공합니다. 디지털 서명을 포함하는

오브젝트에 액세스할 때 오브젝트의 서명을 검증하여 오브젝트 소스를 유효한 것으로 확인할 수 있습니다(예를 들어, 실제로 다운로드하는 어플리케이션은 IBM과 같은 권한이 있는 소스에서 기인함). 또한 이 검증 프로세스는 오브젝트가 서명된 후 권한이 없는 변경사항이 있었는지 여부를 판별할 수 있게 합니다.

디지털 서명 처리 방식의 예

한 소프트웨어 개발자가 인터넷에서 많은 고객들이 편리하게 사용할 수 있으면서 비용 대비 우수한 성능의 iSeries 어플리케이션을 작성했습니다. 그러나 합법적인 프로그램으로 가장하여 바이러스와 같이 유해한 프로그램을 유포시키는 많은 오브젝트들로 인해 고객들이 인터넷에서 프로그램을 다운로드하는 데 주저하고 있다는 것을 알고 있습니다.

따라서 그 회사에서는 어플리케이션이 합법적인 소스라는 것을 고객이 직접 검증할 수 있도록 디지털로 어플리케이션에 서명하기로 결정합니다. 어플리케이션을 서명하기 위해 잘 알려진 공용 인증 기관(CA)에서 디지털 인증서의 개인 키를 사용합니다. 그런 다음 고객이 다운로드할 수 있게 합니다. 또한 다운로드 패키지의 일부로 오브젝트 서명에 사용된 디지털 인증서의 사본을 포함시키기로 합니다. 따라서 고객이 어플리케이션 패키지를 다운로드할 때 인증서의 공용 키를 사용하여 어플리케이션의 서명을 검증할 수 있습니다. 이 프로세스를 통해 고객은 서명 후 어플리케이션 오브젝트의 내용이 변경되지 않았음을 확인할 수 있을 뿐만 아니라 어플리케이션을 식별하고 검증할 수 있습니다.

공용-개인 키 쌍

모든 디지털 인증서에는 연관된 암호 키들의 쌍이 있습니다. 이 키 쌍은 개인 키와 공용 키로 구성되어 있습니다. (서명 확인 인증서는 이러한 규칙의 예외적인 경우로서 연관된 공용 키만 가지고 있습니다.)

공용 키는 소유자의 디지털 인증서의 일부로 누구나 사용할 수 있습니다. 그러나, 개별 키는 키의 소유자만 보호하고 사용할 수 있습니다. 이러한 제한된 액세스에서는 키를 사용하는 통신에 있어서 보안을 유지할 수 있습니다.

인증서의 소유자는 이러한 키들을 사용하여 키가 제공하는 보안 피처의 이점을 활용할 수 있습니다. 예를 들어, 인증서 소유자는 인증서의 개인 키를 사용하여 ″서명″할 수 있고 메세지, 문서 및 코드 오브젝트와 같이 사용자와 서버 간에 전달된 자료를 암호화할 수 있습니다. 그런 다음 서명된 오브젝트의 수신자는 서명자의 인증서에 포함된 공용 키를 사용하여 이 서명을 해독할 수 있습니다. 이러한 디지털 서명은 오브젝트 출처의 신뢰성을 확인하고 오브젝트의 무결성을 확인하는 수단을 제공합니다.

인증 기관(CA)

인증 기관(CA)은 사용자 및 서버에게 디지털 인증서를 발행하는 신뢰할 수 있는 중앙 관리 단체입니다. CA에 대한 신뢰가 유효한 증명서인 인증서에 대한 신뢰의 기초를 이룹니다. CA는 자신의 개인 키를 사용하여 인증서의 출처를 확인하기 위해 발행한 인증서에 대해 디지털 서명을 작성합니다. 다른 사용자는 CA 인증서의 공용 키를 사용하여 CA가 발행하고 서명한 인증서의 진위를 확인할 수 있습니다.

CA는 VeriSign과 같은 공용 단체이거나 조직이 내부적으로 운영하는 개인 단체일 수 있습니다. 여러 회사에서 인터넷 사용자를 위한 인증 기관 서비스를 제공합니다. 디지털 인증 관리자(DCM)를 사용하여 공용 및 개인 CA 모두에서 제공하는 인증서를 관리할 수 있습니다.

또한 DCM을 사용하여 자사의 개인 CA를 운영하여 시스템과 사용자들에게 개인 인증서를 발행할 수 있습니다. CA가 사용자 인증서를 발행하면, DCM은 이 인증서를 사용자의 iSeries 시스템 사용자 프로파일과 자동으로 연관시킵니다. 따라서 인증서에 대한 액세스 및 인증 권한이 소유자의 사용자 프로파일과 동일한 액세스 및 인증 권한으로 유지됩니다.

신뢰할 수 있는 루트 상태

신뢰할 수 있는 루트란 인증 기관 인증서에 특별히 부여되는 것입니다. 신뢰할 수 있는 루트를 통해 브라우저나 다른 어플리케이션이 인증 기관(CA)이 발행한 인증서를 확인하고 수락할 수 있습니다.

인증 기관의 인증서를 사용자의 브라우저로 다운로드할 때 브라우저가 이것을 신뢰할 수 있는 루트로 지정할 수 있게 해줍니다. 어플리케이션이 특정 CA가 발행한 인증서를 확인하고 신뢰하기 전에 인증서 사용을 지원하는 다른 어플리케이션들도 CA를 신뢰하도록 구성해야 합니다.

DCM을 사용하여 인증서 저장소에 있는 인증 기관(CA) 인증서에 대한 신뢰 상태를 작동시키거나 작동 불가능하게 할 수 있습니다. CA 인증서를 작동시키면, 어플리케이션이 이를 사용하여 CA가 발행한 인증서를 확인하고 수락하도록 지정할 수 있습니다. CA 인증서를 작동 불가능하게 하면, 어플리케이션이 이를 사용하여 CA가 발행한 인증서를 확인하고 수락하도록 지정할 수 없습니다.

인증 기관 정책 자료

디지털 인증 관리자(DCM)에 대한 인증 기관(CA)을 작성할 때 CA에 대한 정책 자료를 지정할 수 있습니다. CA에 대한 정책 자료가 서명 권한을 설명합니다. 다음은 정책 자료에서 결정하는 사항입니다.

- CA가 사용자 인증서를 발행 및 서명할 수 있는지의 여부.
- CA가 발행하는 인증서의 유효 기간.

인증서 취소 리스트(CRL) 위치

인증서 취소 리스트(CRL)는 특정 인증 기관(CA)에 대해 유효하지 않고 취소된 모든 인증서를 나열한 파일입니다. CA는 CRL을 정기적으로 갱신하고 간단한 디렉토리 액세스 프로토콜(LDAP) 디렉토리에 다른 사용자들이 발표할 수 있도록 합니다. 핀란드의 SSH와 같은 몇몇 CA들은 직접 액세스할 수 있는 LDAP 디렉토리에 CRL을 자체적으로 발표합니다. CA가 자체의 CRL을 발표하는 경우 인증서는 URI(Uniform Resource Identifier)의 형태로 CRL 분배점 확장을 포함하여 이를 표시합니다.

디지털 인증 관리자(DCM)를 사용하여 CRL 위치 정보를 정의 및 관리함으로 다른 사용자로부터 사용하거나 수락하는 인증에 대해 보다 엄격한 증명을 보장합니다. CRL 위치 정의는 CRL을 저장하는 간단한 디렉토리 액세스 프로토콜(LDAP) 서버의 위치와 이 서버에 대한 액세스 정보를 설명합니다.

인증 확인을 수행하는 어플리케이션은 CA가 특정 인증서를 취소하지 않았음을 확인하기 위해 특정 CA에 대해 정의된 CRL 위치가 있으면 이 위치에 액세스합니다. DCM을 통해 어플리케이션이 인증 확인 중에 CRL 처리를 수행하는 데 필요한 CRL 위치 정보를 정의하고 관리할 수 있습니다. 인증 확인에 대한 CRL 처리를 수행할 수 있는 어플리케이션 및 프로세스의 예로는 VPN(가상 사설망) 인터넷 키 교환(IKE) 서버, 보안 소켓층(SSL) 사용가능 어플리케이션 및 오브젝트 서명 프로세스가 있습니다. 또한 CRL 위치를 정의하고 이를 CA 인증서과 연관시키면, DCM은 지정된 CA가 발행하는 인증에 대한 유효성 확인 프로세스의 일부로 CRL 처리를 수행합니다.

인증서 저장소

인증서 저장소는 디지털 인증 관리자(DCM)가 디지털 인증서를 저장하는 데 사용하는 특수 키 데이터베이스 파일입니다. 또한 인증서 저장소는 4758 암호 코프로세서를 사용하여 대신 키를 저장하도록 선택하지 않는 경우 인증서의 개인 키를 포함합니다. DCM을 통해 여러 가지 유형의 인증서 저장소를 작성하고 관리할 수 있습니다. DCM은 인증서 저장소를 구성하는 IFS 디렉토리의 액세스 제어 및 IFS 파일을 결합하여 암호를 통해 인증서 저장소에 대한 액세스를 제어합니다.

인증서 저장소는 여기에 들어 있는 인증의 유형에 따라 분류됩니다. 각 인증서 저장소에 대해 수행할 수 있는 관리 타스크는 인증서 저장소에 들어 있는 인증의 유형에 따라 다양합니다. DCM은 작성하고 관리할 수 있는 사전정의 인증서 저장소를 아래와 같이 제공합니다.

로컬 인증 기관(CA)
로컬 CA를 작성한 경우 DCM은 이 인증서 저장소를 사용하여 로컬 CA 인증서 및 개인 키를 저장합니다. 이 인증서 저장소의 인증서를 사용하여 로컬 CA가 발행하는 데 사용하는 인증서에 서명할 수 있습니다. 로컬 CA가 인증서를 발행하면, DCM은 확인을 목적으로 CA 인증서의 사본을 적합한 인증서 저장소(예: *SYSTEM)에 저장합니다(개인 키 없이). 어플리케이션은 CA 인증서를 사용하여 자원에 권한을 부여하기 위해 SSL 조정의 일부로 확인해야 하는 인증서의 출처를 확인합니다.

***SYSTEM**
DCM은 어플리케이션이 보안 소켓층(SSL) 통신 세션에 참여하는 데 사용하는 서버 또는 클라이언트 인증서를 관리하기 위해 이러한 인증서 저장소를 제공합니다. IBM iSeries 어플리케이션(그리고 많은 다른 소프트웨어 개발자의 어플리케이션)은 *SYSTEM 인증서 저장소에만 있는 인증서를 사용하도록 작성됩니다. DCM을 사용하여 로컬 인증 기관(CA)를 작성할 때 DCM은 프로세스의 일부로 이 인증서 저장소를 작성합니다. VeriSign과 같은 공용 인증 기관(CA)에서 인증서를 확보하도록 선택할 때 사용할 서버 또는 클라이언트 어플리케이션에 대해 이 인증서 저장소를 작성해야 합니다.

***OBJECTSIGNING**
DCM은 오브젝트에 디지털로 서명하는 데 사용하는 인증서를 관리할 수 있도록 이 인증서 저장소를 제공합니다. 또한 이 인증서 저장소의 타스크는 오브젝트의 서명을 보고 검증할 뿐만 아니라 오브젝트에 대한 디지털 서명을 작성할 수 있게 합니다. DCM을 사용하여 로컬 인증 기관(CA)을 작성할 때 DCM은 프로세스의 일부로 이 인증서 저장소를 작성합니다. VeriSign과 같은 공용 인증 기관(CA)과 같은 인증서를 확보하도록 선택할 때 이 인증서 저장소를 작성해야 합니다.

***SIGNATUREVERIFICATION**
DCM은 오브젝트에 대한 디지털 서명의 인증서를 검증하는 데 사용하는 인증서를 관리하기 위해 이 인증서 저장소를 제공합니다. 디지털 서명을 검증하려면 이 인증서 저장소에 오브젝트에 서명한 인증 사본이 있어야 합니다. 또한 인증서 저장소는 오브젝트 서명 인증서를 발행한 인증서 저장소(CA)의 인증서 저장소(CA) 인증서 사본이 있어야 합니다. 현재 시스템에 대한 오브젝트 서명 인증서를 저장소로 내보내거나 오브젝트 서명자로부터 수신한 인증서를 가져오기하여 이 인증서를 확보합니다.

기타 시스템 인증서 저장소
이 인증서 저장소는 SSL 세션에 사용하는 서버 또는 클라이언트 인증의 대체 저장 위치를 제공합니다. 기타 시스템 인증서 저장소는 SSL 인증서에 대한 사용자 정의 2차 인증서 저장소입니다. 기타 시스템 인증서 저장소 옵션을 통해 SSL_Init API를 사용하여 프로그램에 따라 액세스하고 인증서를 사용하여 SSL 세션을 설정하도록 관리자나 다른 사용자들이 작성한 어플리케이션의 인증서를 관리할 수 있습니다. 이 API를 통해 어플리케이션은 명시적으로 식별한 인증서가 아닌 인증서 저장소에 대한 디폴트 인증서를 사용할 수 있습니다. 대부분은 이전 DCM 릴리스로부터 인증서를 마이그레이트할 때에나 SSL 사용을 위한 특별한 인증 서브세트를 작성할 경우에 이 인증서 저장소를 사용합니다.

주: iSeries 서버에 4758 PCI Cryptographic Coprocessor가 설치된 경우 인증에 대해 다른 개인 키 저장 옵션을 선택할 수 있습니다(오브젝트 서명 인증서는 예외). 코프로세서 자체에 개인 키를 저장하거나 코프로세서를 사용하여 개인 키를 암호화하고 이를 인증서 저장소 대신 특수 키 파일에 저장하도록 선택할 수 있습니다.

DCM은 암호를 통해 인증서 저장소에 대한 액세스를 제어합니다. 또한 DCM은 통합 파일 시스템 디렉토리 및 인증서 저장소를 구성하는 파일들의 액세스 제어를 유지보수합니다. 로컬 인증 기관(CA), *SYSTEM, *OBJECTSIGNING 및

*SIGNATUREVERIFICATION 인증서 저장소는 통합 파일 시스템 내의 특정 경로에 위치해야 합니다. 기타 시스템 인증서 저장소는 통합 파일 시스템 내의 어디에나 위치할 수 있습니다.

암호

암호는 자료 보안을 유지하는 기술입니다. 암호를 사용하여 관련자가 아닌 다른 사람이 현재 저장되어 있는 정보나 통신에 대해 알지 못하게 하면서 상대방과 통신하거나 정보를 저장할 수 있습니다. 암호화는 이해할 수 있는 텍스트를 전혀 이해할 수 없는 자료(암호문)로 변환시킵니다. 따라서 암호 해독 처리를 통해 이해할 수 없는 자료를 이해할 수 있는 텍스트로 복원할 수 있습니다. 두 가지 프로세스 모두 수리적 공식이나 알고리즘 그리고 자료의 비밀 순서(키)가 관련됩니다.

암호 처리에는 다음과 같은 두 유형이 있습니다.

- **공유 또는 비밀 키(대칭)** 암호로서 양쪽의 통신 상대가 하나의 키를 서로의 비밀로 공유합니다. 암호화 및 해독에 모두 같은 키를 사용합니다.
- **공용 키(비대칭)** 암호로서 암호 및 암호 해독에 각각 다른 키를 사용합니다. 각각 공용 키와 개인 키로 구성되는 키 쌍을 보유합니다. 일반적으로 공용 키는 디지털 인증서 내에서 자유롭게 분산되어 있으며 개인 키는 소유자가 안전하게 보유합니다. 두 키는 수리적으로 관련되어 있으나 개별 키를 공용 키로부터 파생시키는 것은 실제적으로 불가능합니다. 누군가의 공용 키를 사용하여 암호화시킨 메세지와 같이 오브젝트는 연관된 개인 키를 사용해야만 해독할 수 있습니다. 또는 서버나 사용자가 개인 키를 사용하여 오브젝트에 "서명"할 수 있으며 오브젝트의 소스 및 무결성을 확인하기 위해 수신자가 해당 공용 키를 사용하여 디지털 서명을 해독할 수 있습니다.

보안 소켓층(SSL)

원래 Nestscape에 의해 만들어진 보안 소켓층(SSL)은 클라이언트와 서버 간의 세션 암호화를 위한 업계 표준입니다. SSL은 비대칭 또는 공용 키, 암호를 사용하여 서버와 클라이언트 사이의 세션을 암호화합니다. 클라이언트 및 서버 어플리케이션들은 디지털 인증서를 교환하는 중에 이 세션 키를 조정합니다. 이 키는 24시간이 경과하면 자동으로 만기되며 SSL 프로세스가 각 서버 연결과 각 클라이언트에 대해 다른 키를 작성합니다. 따라서, 권한이 없는 사용자가 키를 가로채서 세션 키를 해독할지라도(거의 실현 가능성은 없으나) 그 다음 세션에서 그 키를 다시 사용하여 해킹할 수 없습니다.

제 6 장 DCM 계획

디지털 인증 관리자(DCM)를 사용하여 회사의 디지털 인증서를 효과적으로 관리하려면 보안 정책의 일부로 디지털 인증서를 사용하는 방법을 전반적으로 계획해야 합니다.

DCM 사용을 계획하고 디지털 인증서를 보안 정책에 어떻게 적용할 것인지에 관해 알려면 다음 주제를 검토하십시오.

DCM 사용을 위한 요구사항
설치해야 하는 소프트웨어와 DCM을 사용하도록 시스템을 설정하는 데 필요한 다른 정보를 알려면, 이 내용을 읽으십시오.

디지털 인증서 유형
DCM을 사용하여 관리할 수 있는 여러 가지 유형의 인증서에 대해 알려면 이 정보를 사용하십시오.

공용 인증서 대 개인 인증서
제공되는 추가 보안의 이점을 활용하기 위해 인증서의 사용 방법을 결정한 후 업무에 가장 적합한 인증서의 유형을 판별하는 방법에 관해 알려면 이 정보를 사용하십시오. 공용 CA의 인증서를 사용하거나 개인 CA를 작성하고 운영하여 인증서를 발행할 수 있습니다. 인증서를 확보하는 방법은 인증서를 사용하려는 계획에 따라 다릅니다.

보안 소켓층(SSL) 통신에 대한 디지털 인증서
어플리케이션이 보안 통신 세션을 설정할 수 있도록 인증서를 사용하는 방법에 관해 알려면 이 정보를 사용하십시오.

사용자 확인에 대한 디지털 인증서
iSeries 서버 자원에 액세스하는 사용자를 보다 강력하게 확인하는 수단을 제공하는 데 인증서를 사용하는 방법을 알려면 이 정보를 사용하십시오.

VPN(가상 사설망) 연결을 인증하는 디지털 인증서
VPN 연결 구성의 일부로 인증서를 사용하는 방법을 알려면 이 정보를 사용하십시오.

오브젝트 서명을 위한 디지털 인증서
오브젝트의 무결성을 보장하거나 진위를 확인하기 위해 오브젝트에 대한 디지털 서명을 확인하기 위해 인증서를 사용하는 방법에 관해 알려면 이 정보를 사용하십시오.

오브젝트 서명 확인을 위한 디지털 인증서
인증서를 사용하여 해당 인증서를 확인하기 위해 오브젝트에 대한 디지털 서명을 확인하는 방법을 알려면 이 정보를 사용하십시오.

DCM 설치 요구사항

디지털 인증 관리자(DCM)는 어플리케이션에 대한 디지털 인증서를 중앙에서 관리할 수 있게 하는 무상 iSeries 피처입니다. DCM을 성공적으로 사용하려면 다음을 수행해야 합니다.

- 암호 액세스 제공자 사용권 프로그램 설치(5722-AC3). 이러한 암호 제품은 내보내기 및 가져오기 규칙에 따라 암호 알고리즘에 대해 허용되는 최대 키 길이를 판별합니다. 인증서를 작성할 수 있으려면 먼저 이 제품을 설치해야 합니다.
- OS/400의 옵션 34를 설치하십시오. 이 옵션은 브라우저 기본 DCM 피처입니다.

- iSeries용 IBM HTTP Server(5722-DG1)를 설치하고 *ADMIN 서버 인스턴스를 시작하십시오.
- 웹 브라우저 및 HTTP Server *ADMIN 인스턴스를 사용하여 DCM 피처에 액세스할 수 있도록 시스템에 대해 TCP가 구성되었는지 확인하십시오.

주: 필수 제품을 모두 설치하지 않으면 인증서를 작성할 수 없습니다. 필수 제품이 설치되어 있지 않으면, DCM은 누락된 구성요소를 설치하도록 지시하는 오류 메세지를 표시합니다.

디지털 인증서 유형

디지털 인증서는 몇 가지로 분류됩니다. 이러한 분류가 인증서의 사용 방식을 설명합니다. 디지털 인증 관리자(DCM)를 사용하여 다음 유형의 인증서를 관리할 수 있습니다.

인증 기관 (CA) 인증서
인증 기관 인증서는 인증서를 소유하는 인증 기관(CA)의 신원을 확인하는 디지털 증명서입니다. 인증 기관의 인증서에는 공용 키와 같은 인증 기관에 대한 식별 정보가 들어 있습니다. 다른 사용자는 CA 인증서의 공용 키를 사용하여 CA가 발행하고 서명한 인증서의 진위를 확인할 수 있습니다. 인증 기관의 인증서에는 VeriSign과 같이 다른 CA가 서명하거나 독립적 단체인 경우에는 자체적으로 서명할 수 있습니다. 디지털 인증 관리자(DCM)에서 작성하는 CA는 독립적 단체입니다. 다른 사용자는 CA 인증서의 공용 키를 사용하여 CA가 발행하고 서명한 인증서의 진위를 확인할 수 있습니다. SSL, 오브젝트 서명 또는 오브젝트 서명 확인에 대해 인증서를 사용하려면 인증서를 발행한 인증 기관(CA)의 인증 기관(CA) 인증서 사본도 있어야 합니다.

서버 또는 클라이언트 인증서
서버 또는 클라이언트 인증서는 보안 통신에 인증서를 사용하는 서버 또는 클라이언트 어플리케이션을 식별하는 디지털 증명서입니다. 서버 또는 클라이언트 인증서에는 시스템의 구별된 이름과 같이 어플리케이션을 소유하는 조직에 대한 식별 정보가 들어 있습니다. 또한 인증서에 시스템의 공용 키가 포함되어 있습니다. 서버가 보안 통신을 위해 보안 소켓층(SSL)을 이용하려면 디지털 인증서가 필요합니다. 디지털 인증서를 지원하는 어플리케이션은 클라이언트가 서버에 액세스할 때 서버의 신원을 확인하기 위해 서버의 인증서를 조사할 수 있습니다. 그런 다음, 어플리케이션은 클라이언트와 서버 사이의 SSL 암호화된 세션을 시작하기 위한 기초로 인증서를 사용할 수 있습니다. *SYSTEM 인증서 저장소에서만 이러한 유형의 인증서를 관리할 수 있습니다.

오브젝트 서명 인증
오브젝트 서명 인증서는 오브젝트에 디지털로 "서명"하는 데 사용하는 인증서입니다. 오브젝트에 서명하여 오브젝트의 무결성 및 출처 또는 소유권 모두를 확인할 수 있습니다. 인증서를 사용하여 통합 파일 시스템(IFS)의 오브젝트 대부분과 *CMD 오브젝트를 포함하여 다양한 오브젝트에 서명할 수 있습니다. 오브젝트 서명 및 서명 확인 주제에서 모든 서명 가능한 오브젝트 리스트를 찾을 수 있습니다. 오브젝트 서명 인증서의 개인 키를 사용하여 오브젝트에 서명할 때, 오브젝트의 수신자는 오브젝트 서명을 제대로 확인하기 위해 해당 서명 확인 인증서의 사본에 액세스할 수 있어야 합니다. *OBJECTSIGNING 인증서 저장소에서만 이러한 유형의 인증서를 관리할 수 있습니다.

서명 확인 인증서
서명 확인 인증서는 인증서의 개인 키를 사용하지 않는 오브젝트 서명 인증서의 사본입니다. 서명 확인 인증서의 공용 키를 사용하여 오브젝트 서명 인증서에서 작성한 디지털 서명을 인증합니다. 서명에 대한 확인을 통해 오브젝트의 출처 및 서명 이후의 변경 여부를 판별할 수 있습니다. *SIGNATUREVERIFICATION 인증서 저장소에서만 이러한 유형의 인증서를 관리할 수 있습니다.

사용자 인증서
사용자 인증서는 인증서를 소유하는 클라이언트나 사용자의 신원을 확인하닌 디지털 증명서입니다. 현재 많은 어플리케이션들은 사용자명과 암호 대신 인증서를 사용하여 자원에 대해 사용자를 확인할 수 있도록 지원을 제공합니다. 디지털 인증 관리자(DCM)는 개인 CA가 발행한 사용자 인증서를 사용자의 iSeries 사용자 프로파일과 자동으로 연관시킵니다. 또한 DCM을 사용하여 다른 인증 기관이 발행한 사용자 인증서를 사용자의 iSeries 사용자 프로파일과 연관시킬 수 있습니다.

디지털 인증 관리자(DCM)를 사용하여 인증서를 관리할 때, DCM은 인증서를 이와 같이 분류하며 인증서 및 이에 연관된 개인 키를 인증서 저장소에 저장합니다.

주: iSeries 서버에 IBM 4758 PCI Cryptographic Coprocessor가 설치된 경우 인증에 대해 다른 개인 키 저장 옵션을 선택할 수 있습니다(오브젝트 서명 인증서는 예외). 코프로세서 자체에 개인 키를 저장하도록 선택할 수 있습니다. 또는 코프로세서를 사용하여 개인 키를 암호화하고 인증서 저장소 대신 특수 키 파일에 저장할 수 있습니다. 그러나, 사용자 인증서와 그 개인 키는 사용자의 시스템에서 브라우저 소프트웨어나 다른 클라이언트 소프트웨어 패키지가 사용할 수 있도록 파일에 저장됩니다.

공용 인증서 대 개인 인증서

일단 인증서를 사용하기로 결정하면, 보안 요구에 가장 적합한 인증 구현 유형을 선택해야 합니다. 인증서를 확보하기 위해 선택할 수 있는 사항은 다음과 같습니다.

- 공용 인터넷 인증 기관(CA)에서 인증 구입.
- 사용자 및 어플리케이션에 대한 개인 인증서를 발행하기 위해 자신의 CA 운영.
- 공용 인터넷 CA의 인증과 자신의 CA를 조합하여 사용.

이러한 구현 선택사항 중에서 어느 것을 선택할 것인지는 여러 요소에 의해 결정되며 가장 중요한 것은 인증서를 사용하는 환경으로 만드는 것입니다. 다음은 현재의 비즈니스 및 보안 요구에 가장 적합한 구현 선택사항을 결정할 때 참조할 수 있는 사항입니다.

공용 인증서 사용

공용 인터넷 CA는 필요한 비용을 지불하는 사람에게 인증서를 발행합니다. 그러나, 인터넷 CA는 인증서를 발행하기 전에 여전히 신원 증명을 요구합니다. 이 증명 레벨은 CA의 식별 정책에 따라 다릅니다. CA로부터 인증서를 확보하거나 CA가 발행하는 인증서를 신뢰하도록 결정하기 전에 CA의 식별 정책의 엄격함이 사용자의 보안 필요에 적합한지를 평가해야 합니다. X.509의 공용 키 인프라구조(PKIX) 표준이 발전됨에 따라 보다 새로운 공용 인증 기관(CA)이 현재 인증서 발행에 대한 보다 엄격한 식별 표준을 제공합니다. 이러한 PKIX CA에서 인증서를 확보하기 위한 프로세스가 더욱 관련되면서, CA가 발행한 인증서는 어플리케이션에 대한 특정 사용자의 액세스를 보안시킬 수 있도록 보다 나은 보장을 제공합니다. 디지털 인증 관리자(DCM)를 통해 이러한 새로운 인증 표준을 사용하는 PKIX CA의 인증서를 사용하고 관리할 수 있습니다.

또한 인증서를 발행하기 위한 공용 CA 사용과 연관된 비용을 고려해야 합니다. 제한된 수의 서버 또는 클라이언트 어플리케이션 및 사용자에게 인증서를 발행해야 하는 경우 비용이 중요한 요소가 아닐 수도 있습니다. 그러나 클라이언트 확인에 공용 인증서가 필요한 *개인* 사용자의 수가 많으면 비용을 고려하지 않을 수 없습니다. 이러한 경우에는 공용 CA가 발행하는 특정 인증서의 서브세트만을 허용하도록 서버 어플리케이션을 구성하기 위한 관리 및 프로그래밍 처리도 고려해야 합니다.

공용 CA의 인증서를 사용하면 많은 수의 서버, 클라이언트, 사용자 어플리케이션이 대부분의 잘 알려진 공용 CA를 인식하도록 구성되므로 시간과 자원을 절약할 수 있습니다. 또한 다른 회사와 사용자들은 개인 CA가 발행한 인증서보다 잘 알려진 CA가 발행한 인증서를 인식하고 신뢰할 수 있습니다.

개인 인증서 사용

사용자가 자신의 로컬 CA를 작성하는 경우 회사 또는 조직 내에서 보다 제한된 범위 내의 시스템 및 사용자에게 인증서를 발행할 수 있습니다. 사용자 자신의 CA를 작성 및 유지 보수하여 사용자 그룹의 신뢰할 수 있는 멤버들에게만 인증서를 발행할 수 있습니다. 이것은 인증서를 갖고 자원에 액세스하는 사람을 더욱 엄중하게 제어하여 보다 나은 보안을 제공합니다. 사용자 자신의 로컬 CA를 유지보수하기 위한 잠재적 단점은 투자해야 하는 시간과 자원의 양입니다. 그러나, 디지털 인증 관리자(DCM)는 이 프로세스를 보다 쉽게 합니다.

클라이언트 인증을 위해 로컬 인증 기관(CA)을 통해 사용자에게 인증서를 발행할 때 사용자의 인증서가 iSeries 사용자 프로파일과 연관되는지 여부를 결정해야 합니다. 사용자는 해당 인증서를 iSeries 사용자 프로파일과 연관시키려는 경우 DCM을 통해 로컬 인증 기관(CA)에서 인증 확보를 수행하게 할 수 있습니다. 또한 V5R2부터는 클라이언트 인증에 개인 인증서를 사용할 때 iSeries 사용자 프로파일이 필요 없도록 API를 사용하여 프로그래밍 방식으로 비iSeries 사용자에게 인증서를 발행할 수 있습니다.

주: 인증서 발행에 어느 CA를 사용하든지 상관없이, 시스템 관리자는 자신의 시스템에서 어플리케이션이 어느 CS를 신뢰해야 하는지를 제어합니다. 잘 알려진 CA에 대한 인증 사본을 브라우저에서 찾을 수 있으면, 해당 CA에 의해 발행되었던 서버 인증서를 신뢰하도록 사용자의 브라우저를 설정할 수 있습니다. 그러나, 이 CA 인증서가 *SYSTEM 인증서 저장소에 없으면, 서버는 이 CA가 발행한 사용자 또는 클라이언트 인증서를 신뢰할 수 없습니다. CA에 의해 발행되는 사용자 인증서를 신뢰하려면 CA 인증서 사본을 CA로부터 획득하여야 합니다. 올바른 파일 형식이어야 하며 이 인증서를 DCM 인증서 저장소에 추가해야 합니다.

공용 또는 개인 인증서를 사용하는 것이 업무 및 보안 필요에 적합한지 선택하는 데 도움이 되는 공통 인증 사용 시나리오를 검토하면 도움이 될 것입니다.

관련 타스크

인증 사용 방법과 사용할 유형을 결정한 후에 계획을 실행하기 위해 디지털 인증 관리자를 사용하는 방법에 대해 자세히 알려면 다음의 프로시듀어를 검토하십시오.

- 개인 CA 작성 및 운영은 개인 인증서를 발행하기 위해 CA를 작성 및 운영해야 하는 경우에 수행해야 하는 타스크를 설명합니다.
- 공용 인터넷 CA의 인증서 관리는 PKIX CA를 비롯하여 잘 알려진 공용 CA의 인증서를 사용하기 위해 수행해야 하는 타스크를 설명합니다.
- 다른 iSeries 서버에서 로컬 CA 사용은 둘 이상의 시스템에서 개인 CA의 인증서를 사용하려는 경우에 수행해야 하는 타스크를 설명합니다.

SSL 보안 통신에 대한 디지털 인증서

디지털 인증서를 사용하여 보안 통신 세션에 보안 소켓층(SSL)을 사용하도록 어플리케이션을 구성할 수 있습니다. SSL 세션을 설정하기 위해 연결을 요구하는 클라이언트가 확인할 수 있도록 서버는 항상 인증서의 사본을 제공합니다. SSL 연결을 사용하면, 다음의 사항이 보장됩니다.

- 클라이언트 또는 일반 사용자에게 사이트가 신뢰할 수 있는 것임을 보증합니다.
- 연결을 통해 전달되는 자료의 프라이버시를 유지하기 위해 암호화된 통신 세션을 제공합니다.

서버 및 클라이언트 어플리케이션은 자료 보안을 보장하기 위해 다음과 같이 함께 작업합니다.

1. 서버 어플리케이션은 서버의 신원 증명으로 클라이언트(사용자) 어플리케이션에 인증서를 제시합니다.
2. 클라이언트 어플리케이션은 서버의 신원을 발행하는 인증 기관 인증의 사본과 비교하여 확인합니다(클라이언트 어플리케이션은 관련 CA 인증서의 로컬로 저장된 사본에 액세스할 수 있어야 합니다).
3. 서버 및 클라이언트 어플리케이션들은 암호화를 위한 대칭 키에 합의를 보고 이를 사용하여 통신 세션을 암호화합니다.
4. 선택적으로 서버는 현재 요구된 자원에 대한 액세스를 허용하기 전에 클라이언트에 신원 증명을 제공하도록 요구할 수 있습니다. 신원 증명으로 인증서를 사용하려면, 통신하는 어플리케이션들은 사용자 확인을 위한 인증 사용을 지원해야 합니다.

SSL은 SSL 핸드쉐이크 처리 중에 비대칭 키(공용 키) 알고리즘을 사용하여 특정 SSL 세션에 대한 어플리케이션 자료를 암호화 및 해독에 연속적으로 사용되는 대칭 키를 조정합니다. 이는 사용자의 서버와 클라이언트가 다른 세션 키를 사용함을 의미하며 각각의 연결에 대해 설정된 시간 후 자동으로 만기됩니다. 만일 누군가가 특정 세션 키를 가로채어 해독하는 일이 일어난다면, 이 세션 키를 사용하여 이후 키를 추론할 수 없습니다.

사용자 확인에 대한 디지털 인증서

종래에는 사용자들이 사용자명과 암호에 기초하여 어플리케이션이나 시스템으로부터 자원에 대한 액세스 권한을 받았습니다. 디지털 인증서를 사용하여(사용자명과 암호 대신) 시스템 보안을 더욱 향상시켜서 여러 서버 어플리케이션 및 사용자들 사이의 세션을 확인하고 권한을 부여할 수 있습니다. 또한 디지털 인증 관리자(DCM)를 사용하여 사용자의 인증서를 이 사용자의 iSeries 사용자 프로파일과 연관시킬 수 있습니다. 그러면, 인증서는 연관된 프로파일과 동일한 권한 및 허가를 갖게 됩니다. V5R2부터 비iSeries 사용자에게 인증서를 발행하기 위해 API 사용을 수행하여 프로그래밍 방식으로 개인 로컬 인증 기관(CA)을 사용할 수 있습니다. 사용자에게 iSeries 사용자 프로파일이 없을 때 API는 이 사용자에게 개인 인증서를 발행하는 능력을 제공합니다.

디지털 인증서는 전자 증명서의 역할을 하며 이를 제시하는 사람이 실제로 주장하는 사람인지를 확인합니다. 이런 면에서, 인증서는 패스포트와 비슷합니다. 둘 다 개인의 신원을 설정하고 식별을 위한 고유 번호가 들어 있으며 증명서를 확실한 것으로 검증하는 공인 발행 기관이 있습니다. 인증서의 경우 인증 기관(CA)은 인증서를 발행하고 이를 확실한 증명서로 검증하는 신뢰할 수 있는 제 3자로서의 역할을 합니다.

확인을 목적으로 인증서는 공용 키 및 관련 개인 키를 활용합니다. 발행하는 CA는 식별을 목적으로 이러한 키들을 인증서 소유자에 대한 다른 정보와 더불어 인증서 자체에 바인드합니다.

현재 증가하고 있는 많은 수의 어플리케이션들이 SSL 세션 중에 클라이언트 확인에 인증서를 사용할 수 있도록 지원을 제공합니다. 현재 이 iSeries 어플리케이션에서 클라이언트 확인 인증 지원을 제공합니다.

- 텔넷 서버
- IBM HTTP Server(기본 및 Apache로 구현)
- 디렉토리 서비스(LDAP) 서버
- 중앙 관리
- Client Access Express(iSeries Navigator 포함)
- FTP 서버

시간에 걸쳐서 추가 어플리케이션은 클라이언트 확인 인증 지원을 제공할 수 있고, 특정 어플리케이션의 문서를 검토하여 이 지원을 제공할지 여부를 판별할 수 있습니다.

인증서는 몇 가지 이유로 인해 사용자를 확인하는 보다 강력한 수단을 제공할 수 있습니다.

- 개인이 자신의 암호를 잊어버릴 수 있는 가능성이 있습니다. 따라서, 사용자는 사용자명과 암호를 기억할 수 있도록 암기하거나 기록해야 합니다. 결과적으로, 권한이 없는 사용자가 권한이 있는 사용자로부터 사용자명과 암호를 보다 쉽게 확보할 수 있습니다. 인증서는 파일이나 기타 전자 위치에 저장되기 때문에 클라이언트 어플리케이션(사용자가 아님)은 확인을 위해 인증에 대한 액세스 및 인증 제시를 처리합니다.

그러면, 권한이 없는 사용자가 사용자의 시스템에 액세스하지 않으면 사용자들이 권한이 없는 사용자와 인증서를 공유하지 않게 됩니다. 또한 권한이 없는 사용으로부터 이를 보호하는 추가 수단으로 인증서를 스마트 카드에 설치할 수 있습니다.

- 인증에는 식별을 위해 인증과 함께 송신된 적이 없는 개인 키가 들어 있습니다. 그 대신, 시스템은 이 키를 암호화 및 암호 해독 처리 동안 사용합니다. 다른 사용자들은 인증의 해당 공용 키를 사용하여 개인 키를 통해 서명된 오브젝트의 송신자에 대한 신원을 확인할 수 있습니다.
- 많은 시스템들은 길이가 8자 이하인 암호를 요구하므로 이러한 암호들은 외부 공격에 보다 취약하게 됩니다. 인증의 암호 키는 길이가 수백자입니다. 무작위적인 성질을 갖는 문자 자리수 때문에 암호 키가 암호보다 훨씬 추측하기 어렵습니다.
- 디지털 인증서 키는 자료 무결성 및 프라이버시와 같이 암호가 제공할 수 있는 몇 가지 잠재적인 용도를 제공합니다. 인증서 및 연관된 키를 사용하여 다음을 수행할 수 있습니다.
  - 자료에 대한 변경을 감지하여 자료 무결성을 보증합니다.
  - 특정 조치가 정말 수행되었는지 입증합니다. 이것을 비거부(nonrepudiation)라고 합니다.
  - 통신 세션을 암호화하기 위해 보안 소켓층(SSL)을 사용하여 자료 전송의 프라이버시를 보장합니다.

SSL 세션 중에 클라이언트 확인을 위해 인증서를 사용하도록 iSeries 서버 어플리케이션을 구성하는 것에 대해 자세히 알려면, SSL을 사용한 어플리케이션 보안을 참조하십시오.

VPN 연결에 대한 디지털 인증서

디지털 인증서를 iSeries VPN(가상 사설망) 연결 설정의 수단으로 사용할 수 있습니다. 동적 VPN 연결의 양쪽 종료점은 연결을 활성화하기 전에 서로 인증할 수 있어야 합니다. 종료점 인증서는 각 끝에서 인터넷 키 교환(IKE) 서버에 의해 수행됩니다. 인증이 성공된 후에 IKE 서버는 VPN 연결을 보안하는 데 사용할 암호화 방법과 알고리즘을 조정합니다.

V5R1 이전에는 IKE 서버들이 사전 공유 키의 사용을 통해서만 서로 인증할 수 있었습니다. 사전 공유 키는 VPN에 대한 다른 종료점의 관리자에게 수동으로 전달해야 하기 때문에 이 키는 보안성이 떨어집니다. 결국, 키를 전달하는 프로세스 동안에 다른 사용자에게 이 키가 노출될 가능성이 있습니다.

사전 공유 키를 사용하는 대신 디지털 인증서를 사용하여 종료점을 인증함으로 이러한 위험을 방지할 수 있습니다. IKE 서버는 서버가 연결을 보안하는 데 사용할 암호화 방법과 알고리즘을 조정하기 위해 연결을 설정할 수 있도록 다른 서버의 인증서를 확인할 수 있습니다.

디지털 인증 관리자(DCM)를 사용하여 IKE 서버가 동적 VPN 연결 설정에 사용하는 인증서를 관리할 수 있습니다. 먼저 IKE 서버에 공용 인증서 대 개인 인증서 발행을 사용할 것인지를 결정해야 합니다.

일부 VPN 구현에서는 표준 구별된 이름 정보와 함께 정의역명이나 전자 우편 주소와 같은 대체 주제명 정보가 인증에 포함될 것을 요구합니다. DCM 유틸리티의 개인 CA를 사용하여 인증서를 발행할 때, 인증에 대한 대체 주제명 정보를 지정할 수 있습니다. 이 정보를 지정하면, iSeries VPN 연결을 인증할 때 이를 요구할 수 있는 다른 VPN 구현과 호환할 수 있습니다.

VPN 연결에 대한 인증서를 관리하는 방법에 대해 자세히 알려면, 다음의 자원을 검토하십시오.

- 이전에 DCM을 사용하여 인증서를 관리한 적이 없는 경우 다음의 주제는 시작하는 데 도움이 됩니다.
  - 개인 CA, 로컬 작성 및 운영은 DCM을 사용하여 어플리케이션에 대한 개인 인증서를 발행하는 방법을 설명합니다.
  - 공용 인터넷 CA에서 제공하는 인증서 관리는 DCM을 사용하여 공용 CA에서 인증에 대해 작업하는 방법을 설명합니다.
- 현재 DCM을 사용하여 다른 어플리케이션에 대한 인증서를 관리하는 경우 어플리케이션이 기존의 인증서를 사용하도록 지정하고 어플리케이션이 수락하고 증명할 수 있는 인증서를 지정하는 방법을 알려면 다음의 자원을 검토하십시오.
  - 어플리케이션에 대한 인증서 지정 관리는 DCM을 사용하여 IKE 서버와 같이 어플리케이션에 기존의 인증서를 지정하는 방법을 설명합니다.
  - 어플리케이션에 대한 CA 신뢰 리스트 정의는 어플리케이션이 클라이언트(또는 VPN) 확인을 위해 인증서를 수락할 때 어플리케이션이 신뢰할 수 있는 CA를 지정하는 방법을 설명합니다.

오브젝트 서명을 위한 디지털 인증서

V5R1부터 OS/400은 인증서를 사용하여 오브젝트에 디지털로 ″서명″하도록 지원합니다. 오브젝트에 디지털로 서명하여 오브젝트 내용의 무결성 및 오브젝트 출처의 소스 모두를 검증하는 방법을 제공합니다. 오브젝트 서명 지원은 오브젝트를 변경할 수 있는 사람을 제어하기 위한 기존의 iSeries 시스템 툴을 향상시킨 것입니다. 기존의 제어는 오브젝트가 인터넷이나 다른 신뢰할 수 없는 네트워크에서 이동 중이거나 오브젝트가 iSeries가 아닌 다른 시스템에 저장되어 있는 동안에 권한 없는 간섭으로부터 오브젝트를 보호할 수 없었습니다. 또한 일반 제어로는 오브젝트에 대해 권한 없는 변경이 있었는지 또는 임의로 처리된 것이 있었는지 여부를 판별할 수 없습니다. 오브젝트의 디지털 서명을 사용하여 서명된 오브젝트에 대한 변경사항을 감지하는 확실한 수단을 제공합니다.

오브젝트에 대한 디지털 서명 저장은 인증서의 개인 키를 사용하여 오브젝트에 있는 자료의 암호화된 수리적 요약을 추가하는 작업으로 구성되어 있습니다. 서명은 자료를 권한이 없는 변경으로부터 보호합니다. 오브젝트와 그 내용은 디지털 서명에 의해 암호화되고 프라이버시가 보장되지 않지만 요약 자체는 암호화되어 권한이 없는 변경을 방지합니다. 오브젝트가 이동 중에 변경되지 않았으며 오브젝트가 수락된 정당한 소스로부터 기원된 것임을 확인하려는 사람은 서명된 인증서의 공용 키를 사용하여 원래의 디지털 서명을 확인할 수 있습니다. 서명이 더 이상 일치하지 않으면, 자료가 변경되었을 것입니다. 이러한 경우 해당 오브젝트를 사용하지 않고, 그 대신 서명자에게 접속하여 서명된 오브젝트의 다른 사본을 확보할 수 있습니다.

디지털 서명을 사용하는 것을 보안상의 필요와 정책에 적합한 것으로 결정했으면, 공용 인증서 대 개인 인증서 발행을 사용해야 하는지의 여부를 평가해야 합니다. 공용으로 오브젝트를 사용자에게 분배하려면 잘 알려진 공용 인증 기관(CA)의 인증서를 사용하여 오브젝트에 서명하는 작업을 고려해야 합니다. 공용 인증서를 사용하면, 분배한 오브젝트에 저장한 서명을 다른 사용자들이 쉽고 저렴하게 확인할 수 있습니다. 그러나 조직 내에서만 오브젝트를 분배하려는 경우 디지털 인증 관리자(DCM)를 사용하여 사용자 자신의 로컬 인증 기관(CA)을 운영함으로써 오브젝트에 서명시 인증서를 발행하는 것이 더 좋을 수 있습니다. 로컬 인증 기관(CA)에서 개인 인증서를 사용하여 오브젝트에 서명하는 것이 잘 알려진 공용 인증 기관(CA)의 인증서를 구입하는 것보다 더 저렴합니다.

오브젝트의 서명은 오브젝트에 서명한 시스템의 특정 사용자가 아닌 오브젝트에 서명한 시스템을 나타냅니다(그렇지만 사용자는 오브젝트에 서명하는 데 인증서를 사용하려면 적합한 권한을 가지고 있어야 합니다). 디지털 인증 관리자(DCM)를 사용하여 오브젝트에 서명하고 오브젝트 서명을 검증하는 데 사용하는 인증서를 관리합니다. 또한 DCM을 사용하여 오브젝트 서명 및 오브젝트 서명 검증을 수행할 수 있습니다.

오브젝트 서명 확인을 위한 디지털 인증서

V5R1부터 iSeries는 오브젝트에 대한 디지털 서명을 확인하기 위해 인증서 사용을 지원하고 있습니다. 오브젝트가 이동 중에 변경되지 않았으며 오브젝트가 적합한 출처에서 나온 것인지 확인하려는 경우 서명된 인증서의 공용 키를 사용하여 원래의 디지털 서명을 확인할 수 있습니다. 서명이 더 이상 일치하지 않으면, 자료가 변경되었을 것입니다. 이러한 경우 해당 오브젝트를 사용하지 않고 그 대신 서명자에게 접속하여 서명된 오브젝트의 다른 사본을 확보할 수 있습니다.

오브젝트의 서명은 오브젝트에 서명한 시스템의 특정 사용자가 아닌 오브젝트에 서명한 시스템을 나타냅니다. 디지털 서명을 확인하는 프로세스의 일부로 오브젝트 서명을 위해 신뢰하는 인증 기관과 신뢰하는 인증서를 결정해야 합니다. 하나의 CA를 신뢰하도록 선택할 때, 이 신뢰하는 CA가 발행한 인증서를 사용하여 누군가가 작성한 서명을

신뢰할 것인지의 여부를 선택할 수 있습니다. CA를 신뢰하지 않도록 결정할 경우 이 CA가 발행한 인증서나 그러한 인증서를 사용한 서명 또한 신뢰하지 않도록 결정하는 것이 됩니다.

QVFYOBJRST(오브젝트 복원 확인) 시스템 값

서명 확인을 수행하기로 결정한 경우 먼저 결정해야 하는 중요한 사항 중 하나는 시스템에 복원되는 오브젝트에 대해 서명이 얼마나 중요한 것인지를 판별하는 것입니다. 이것은 QVFYOBJRST라고 하는 시스템 값을 사용하여 제어합니다. 이 시스템 값의 디폴트 설정은 서명되지 않은 오브젝트를 복원할 수 있게 하지만 오브젝트에 유효한 서명이 있을 경우에만 서명된 오브젝트를 복원할 수 있도록 합니다. 오브젝트에 시스템이 신뢰하는 서명이 있을 경우에만 시스템은 오브젝트를 서명된 것으로 정의합니다. 시스템은 오브젝트에 대한 다른 ″신뢰하지 않는″ 서명을 무시하며 이 오브젝트를 서명되지 않은 것처럼 취급합니다.

모든 서명을 무시하는 것에서부터 시스템이 복원하는 모든 오브젝트에 대해 유효한 서명을 요구하는 것까지 QVFYOBJRST 시스템 값에 사용할 수 있는 여러 가지 값이 있습니다. 이 시스템 값은 저장 파일 또는 IFS 파일이 아닌 복원되는 실행가능한 오브젝트에만 영향을 줍니다. 이 시스템 값 및 다른 값을 사용하는 데 대해 자세히 알려면 Information Center의 시스템 값 파인더를 참조하십시오.

디지털 인증 관리자(DCM)를 사용하여 인증서 및 CA 신뢰 결정을 구현하고, 오브젝트 서명을 확인하는 데 사용하는 인증서를 관리합니다. 또한 오브젝트 서명 및 오브젝트 서명 검증에 DCM을 사용할 수 있습니다.

제 7 장 DCM 구성

디지털 인증 관리자(DCM)는 어플리케이션 및 사용자에 대한 디지털 인증서를 관리하기 위해 사용할 수 있는 브라우저 기반의 사용자 인터페이스를 제공합니다. 사용자 인터페이스는 탐색 프레임과 타스크 프레임의 두 가지 기본 프레임으로 나뉘어집니다.

탐색 프레임은 인증서를 사용하는 어플리케이션이나 인증서를 관리할 타스크를 선택하는 데 사용합니다. 일부 개별 타스크들은 기본 탐색 프레임에 직접 나타나지만 탐색 프레임에 있는 대부분의 타스크들은 범주로 구성되어 있습니다. 예를 들어, **인증서 관리**의 경우 인증서 보기, 인증서 갱신, 인증서 가져오기 등과 같은 다양한 개별 안내 타스크가 들어 있는 타스크 범주입니다. 탐색 프레임의 항목이 둘 이상의 타스크가 들어 있는 범주인 경우 화살표가 타스크의 왼쪽에 나타납니다. 화살표는 범주 링크를 선택할 때 타스크 리스트를 표시하여 사용자가 수행할 할 타스크를 선택할 수 있게 해줍니다.

빠른 경로 범주를 제외하고 탐색 프레임의 각 타스크는 빠르고 쉽게 타스크를 완료할 수 있는 일련의 단계를 제공합니다. 빠른 경로 범주는 사용 경험이 많은 DCM 사용자들이 중앙 페이지 세트에서 다양한 관련 타스크에 빠르게 액세스할 수 있게 해 주는 인증서 및 어플리케이션 관리 기능 세트를 제공합니다.

탐색 프레임에서 사용할 수 있는 타스크들은 현재 작업 중인 인증서 저장소에 따라 다릅니다. 또한 탐색 프레임에서 볼 수 있는 타스크의 범주와 수는 iSeries 사용자 프로파일이 가진 권한에 따라 다릅니다. CA 운영 및 어플리케이션이 사용하는 인증서를 관리하기 위한 모든 타스크와 기타 시스템 레벨 타스크는 iSeries 보안 담당자나 관리자만 사용할 수 있습니다. 다음과 같은 타스크를 조회하고 사용하기 위해서는 보안 담당자나 관리자에게 *SECADM 및 *ALLOBJ 특수 권한이 필요합니다. 이러한 특수 권한이 없는 사용자는 사용자 인증서 기능에만 액세할 수 있습니다.

DCM을 구성한 후 이를 통해 인증서를 관리하는 방법에 관해 알려면 다음 주제를 검토하십시오.

DCM 시작
iSeries에서 디지털 인증 관리자 피처에 액세스하는 방법을 알려면 다음 내용을 읽어보십시오.

처음으로 인증서 설정
처음으로 인증서를 사용할 때 필요한 모든 것을 설정하기 위해 DCM을 사용하는 방법에 관해 알려면 다음을 읽어보십시오. 공용 인터넷 인증 기관(CA)에서 인증서를 관리하는 방법이나 개인 로컬 CA를 작성하고 운영하여 인증서를 발행하는 방법을 알 수 있습니다.

시스템 및 네트워크 보안을 향상시키기 위해 인터넷 환경에서 디지털 인증서를 사용하는 것에 대해 보다 교육적인 정보가 필요하면 VeriSign 웹 사이트를 참조하십시오.

VeriSign 웹 사이트는 디지털 인증 주제에 대한 포괄적인 라이브러리와 함께 여러 가지 인터넷 보안 정보를 제공합니다. VeriSign Help Desk 에서 해당 라이브러리에 액세스할 수 있습니다.

디지털 인증 관리자 시작

해당 기능을 사용하려면, 먼저 디지털 인증 관리자(DCM)를 시작해야 합니다. DCM을 성공적으로 시작할 수 있도록 다음의 타스크를 완료하십시오.

1. 5722 SS1 옵션 34를 설치하십시오. 이것은 디지털 인증 관리자(DCM)입니다.

   5722 DG1을 설치하십시오. 이것은 iSeries용 IBM HTTP Server입니다.

   5722 AC3을 설치하십시오. 이 제품들은 V5R2 DCM이 인증에 대한 공용-개인 키 쌍을 생성하고, 내보낸 인증 파일을 암호화하고, 가져온 인증 파일을 해독하는 데 사용하는 암호 제품입니다.
2. HTTP Server *ADMIN 인스턴스를 시작하려면 iSeries Navigator를 사용하십시오.
   a. **iSeries Navigator**를 시작하십시오.
   b. 기본 트리 보기에서 iSeries 서버를 두 번 클릭하십시오.
   c. **네트워크**를 두 번 클릭하십시오.
   d. **서버**를 두 번 클릭하십시오.
   e. **TCP/IP**를 두 번 클릭하십시오.
   f. **HTTP 관리**를 마우스 오른쪽 버튼으로 클릭하십시오.
   g. **시작**을 클릭하십시오.
3. 웹 브라우저를 시작하십시오.
4. 브라우저를 사용하여 http://*your_system_name*:2001에서 시스템의 iSeries 타스크 페이지로 찾아 가십시오.
5. iSeries 타스크 페이지의 제품 리스트에서 **디지털 인증 관리자**를 선택하여 DCM 피처에 액세스하십시오.

DCM의 이전 버전으로부터 마이그레이트하는 경우 이 페이지는 시스템을 업그레이드하는 데 필요한 세부사항을 제공합니다.

처음으로 인증서 설정

디지털 인증 관리자(DCM)의 왼쪽 프레임은 타스크 탐색 프레임입니다. 이 프레임을 사용하여 인증서 및 이를 사용하는 어플리케이션을 관리할 광범위한 타스크들을 선택할 수 있습니다. 사용할 수 있는 타스크는 열어 놓은 인증서 저장소(있는 경우)와 사용자 프로파일 권한에 따라 다릅니다. 대부분의 타스크들은 *ALLOBJ 및 *SECADM 특수 권한을 가지고 있는 경우에만 사용할 수 있습니다.

처음으로 디지털 인증 관리자(DCM)를 사용하는 경우 인증서 저장소가 없습니다(이전 DCM 버전에서 마이그레이트하지 않은 경우). 결과적으로, 필요한 권한이 있을 때만 탐색 프레임에 다음의 타스크들이 표시됩니다.

- 사용자 인증서 관리.
- 새로운 인증서 저장소 작성.
- 인증 기관(CA) 작성. (주: 이 타스크를 사용하여 개인 CA를 작성한 후에는 이 타스크가 리스트에 더 이상 나타나지 않습니다.)
- CRL 위치 관리.
- PKIX 요구 위치 관리.

시스템에 인증서 저장소가 이미 있더라도(예를 들어, 이전 버전의 DCM에서 마이그레이트하는 경우) DCM이 제한된 타스크 수 또는 타스크 범주만 왼쪽 탐색 프레임에 표시합니다. 대부분의 인증서 및 어플리케이션 관리 타스크에 대한 작업을 시작하기 위해서는 먼저 적합한 인증서 저장소에 액세스해야 합니다. 특정 인증서 저장소를 열려면, 탐색 프레임에서 **인증서 저장소 선택**을 클릭하십시오.

DCM의 탐색 프레임은 또한 **보안 연결** 버튼을 제공합니다. 이 버튼을 사용하여 두 번째 브라우저 창을 표시하고 이 창에서 보안 소켓층(SSL)을 사용하여 보안 연결을 시작할 수 있습니다. 이 기능을 성공적으로 사용하려면, 먼저 SSL을 사용하여 보안 모드에서 운영하도록 iSeries용 IBM HTTP Server를 구성해야 합니다. 그런 다음, 보안 모드에서 HTTP Server를 시작해야 합니다. SSL 운영을 위해 HTTP Server를 구성 및 시작하지 않은 경우 오류 메세지가 표시되고 브라우저가 보안 세션을 시작하지 않습니다.

시작하기

인증서를 사용하여 여러 가지 보안 관련 목표를 달성할 수 있으나 맨 처음에 할 일은 인증서를 확보하는 방식에 따라 달라집니다. 즉, 처음에 DCM을 사용할 때 공용 인증서를 사용할 것인지 아니면 개인 인증서를 발행할 것인지에 따라 두 가지 경로 중 하나를 사용할 수 있습니다.

어플리케이션에 대한 인증서를 발행하기 위해 **로컬 인증 기관(CA)을 작성 및 운영**합니다.
어플리케이션이 사용할 **공용 인터넷 CA에서 제공하는 인증서를 관리**합니다.

로컬 인증 기관(CA) 작성 및 운영

보안 필요와 정책을 주의깊게 검토한 후에 어플리케이션에 대한 개인 인증서를 발행하도록 로컬 인증 기관(CA)을 운영하기로 결정했을 것입니다. 디지털 인증 관리자(DCM)를 사용하여 자신의 로컬 CA를 작성하고 운영할 수 있습니다. DCM은 CA를 작성하고 이를 사용하여 어플리케이션에 인증서를 발행하는 프로세스로 안내하는 안내 타스크 경

로를 제공합니다. 안내 타스크 경로는 SSL을 사용하도록 어플리케이션을 구성하고 오브젝트에 서명하고 오브젝트 서명을 확인하기 위해 디지털 인증서를 사용할 때 필요한 모든 것이 준비되도록 합니다.

주: iSeries용 IBM HTTP Server와 인증서를 사용하려면, DCM에 대한 작업 이전에 서명하여 완성한 인증서에 대해 작업할 수 있도록 웹 서버를 작성하고 구성해야 합니다. SSL 사용을 위해 웹 서버를 구성할 때, 서버의 어플리케이션 ID가 생성됩니다. DCM을 사용하여 이 어플리케이션이 SSL에 사용해야 하는 인증서를 지정하려면 이 어플리케이션 ID를 기록하십시오.

DCM을 사용하여 서버에 인증서를 지정할 때까지 서버를 종료하고 다시 시작하지 마십시오. 인증서를 지정하기 전에 웹 서버의 *ADMIN 인스턴스를 종료하고 다시 시작하면, 서버는 시작되지 않으며 DCM을 사용하여 서버에 인증서를 지정할 수 없게 됩니다.

DCM을 사용하여 로컬 CA를 작성 및 운영하려면, 다음의 단계를 따르십시오.

1. DCM을 시작하십시오.
2. DCM의 탐색 프레임에서 **인증 기관(CA) 작성**을 선택하여 일련의 양식들을 표시하십시오. 이 양식들은 로컬 CA를 작성하고 SSL, 오브젝트 서명 및 서명 확인을 위해 디지털 인증서를 사용할 때 필요한 다른 타스크를 완료하는 프로세스로 안내합니다.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
3. 이 안내된 타스크에 대한 모든 양식을 완료하십시오. 작업 중인 로컬 인증 기관(CA)을 설정하는 데 필요한 모든 타스크를 수행하기 위해 이러한 양식들을 사용할 때, 다음과 같이수행하십시오.
   a. 로컬 CA 인증서에 대한 개인 키 저장 방법을 선택하십시오(이 단계는 iSeries에 IBM 4758-023 PCI Cryptographic Coprocessor가 설치된 경우에만 포함됩니다. 시스템에 이 암호 코프로세서가 없는 경우 DCM은 인증과 해당 개인 키를 로컬 인증 기관(CA) 인증서 저장소에 자동으로 저장합니다).
   b. 로컬 CA에 대한 식별 정보를 제공하십시오.
   c. 소프트웨어가 로컬 CA를 인식하고 CA가 발행한 인증서를 확인할 수 있도록 로컬 CA 인증서를 PC나 브라우저에 설치하십시오.
   d. 로컬 CA에 대한 정책 자료를 선택하십시오.
   e. 새로운 로컬 CA를 사용하여 어플리케이션이 SSL 연결에 사용할 수 있는 서버 또는 클라이언트 인증서를 발행하십시오(iSeries에 IBM 4758-023 PCI 암호 코프로세서가 설치되어 있는 경우 이 단계는 서버 또는 클라이언트 인증서의 개인 키를 저장하는 방법을 선택할 수 있게 합니다. 시스템에 코프로세서가 없는 경

우 DCM은 인증과 해당 개인 키를 *SYSTEM 인증서 저장소에 자동으로 저장합니다. DCM은 이 하위 타스크의 일부로 *SYSTEM 인증서 저장소를 작성합니다).

f. SSL 연결에 서버 또는 클라이언트 인증서를 사용할 수 있는 어플리케이션을 선택하십시오.

   주: 공용 인터넷 CA에서 SSL에 대한 인증서를 관리하기 위해 이전에 DCM을 사용하여 *SYSTEM 인증서 저장소를 작성한 경우 이 단계나 이전 단계를 수행하지 마십시오.

g. 새로운 로컬 CA를 사용하여 어플리케이션이 오브젝트에 디지털로 서명하는 데 사용할 수 있는 오브젝트 서명 인증서를 발행하십시오. 이 하위 타스크는 *OBJECTSIGNING 인증서 저장소를 작성하며 이것은 오브젝트 서명 인증서를 관리하는 데 사용하는 인증서 저장소입니다.

h. 오브젝트에 대한 디지털 서명을 저장하기 위해 오브젝트 서명 인증서를 사용할 수 있는 어플리케이션을 선택하십시오.

   주: 공용 인터넷 CA에서 오브젝트 서명 인증서를 관리하기 위해 이전에 DCM을 사용하여 *OBJECTSIGNING 인증서 저장소를 작성한 경우 이 단계나 이전 단계를 수행하지 마십시오.

i. 로컬 CA를 신뢰해야 하는 어플리케이션을 선택하십시오.

안내 타스크를 완료하면, 보안 통신을 위해 SSL을 사용하도록 어플리케이션 구성을 시작하는 데 필요한 모든 것이 준비됩니다.

어플리케이션을 구성한 후 SSL 연결을 통해 어플리케이션에 액세스하는 사용자는 DCM을 사용해야만 로컬 인증 기관(CA) 인증의 사본을 확보할 수 있습니다. 사용자의 클라이언트 소프트웨어가 SSL 조정 프로세스의 일부로 서버의 신원을 확인하는 데 사용할 수 있도록 각 사용자는 인증의 사본을 가지고 있어야 합니다. 사용자는 DCM을 사용하여 로컬 CA 인증서를 파일에 복사하거나 인증서를 브라우저에 다운로드할 수 있습니다. 사용자가 로컬 CA 인증서를 저장하는 방법은 어플리케이션에 대한 SSL 연결을 설정하는 데 사용하는 클라이언트 소프트웨어에 따라 다릅니다.

또한 이 로컬 CA를 사용하여 네트워크의 다른 iSeries 시스템에 있는 어플리케이션에 인증서를 발행할 수 있습니다.

| 사용자 인증서 관리를 위한 DCM 사용 및 로컬 인증 기관(CA)이 발행하는 인증서를
| 확인하기 위해 어떻게 로컬 인증 기관(CA) 인증서의 사본을 확보할 수 있는지에 대해
| 자세히 알려면 다음 주제를 검토하십시오.

사용자 인증서 관리
사용자가 DCM을 사용하여 인증서를 확보하거나 iSeries 사용자 프로파일과 기존 인증서를 연관시킬 수 있는 방법을 알 수 있습니다.

API를 사용하여 프로그래밍 방식으로 비iSeries 사용자에 대한 인증서 발행
인증서와 iSeries 사용자 프로파일을 연관시키지 않고 로컬 인증 기관(CA)을 사용하여 사용자에게 개인 인증서를 발행하는 방법을 알 수 있습니다.

개인 CA 인증서 사본 확보
CA가 발행한 서버 인증서를 확인할 수 있도록 개인 CA 인증서의 사본을 확보하고 PC에 설치하는 방법을 알 수 있습니다.

사용자 인증서 관리

디지털 인증 관리자(DCM)를 사용하여 보안 소켓층(SSL) 세션에 참여하는 사용자에게 필요한 인증서를 관리할 수 있습니다.

사용자들이 SSL 연결을 통해 공용 서버나 내부 서버에 액세스하는 경우 서버의 인증서를 발행한 인증 기관(CA) 인증서의 사본이 필요합니다. CA 인증서 사본이 있어야 클라이언트 소프트웨어가 연결을 위해 서버 인증서의 진위를 확인할 수 있습니다. 서버가 공용 CA 인증서를 사용하는 경우 사용자의 소프트웨어에 CA 인증서의 사본이 이미 있어야 합니다. 결과적으로 DCM 관리자나 사용자 모두 SSL 세션에 참여하기 전에 어떠한 조치도 취할 필요가 없습니다. 그러나, 서버가 개인 로컬 CA 인증서를 사용하는 경우에는 서버와의 SSL 세션을 설정하기 전에 사용자에게 로컬 CA 인증서의 사본이 필요합니다.

추가로, 서버 어플리케이션이 인증서를 통해 클라이언트 확인을 지원하고 요구하는 경우 사용자는 서버가 제공하는 자원에 액세스하기 위해 수락가능한 사용자 인증서를 제시해야 합니다. 보안 필요에 따라 사용자는 공용 인터넷 CA의 인증서를 제시하거나 관리자가 운영하는 로컬 CA에서 확보한 인증서를 제시할 수 있습니다. 서버 어플리케이션이 현재 iSeries 사용자 프로파일을 가지고 있는 내부 사용자들이 자원에 액세스할 수 있도록 허용한 경우 DCM을 사용하여 사용자 프로파일에 인증서를 추가할 수 있습니다. 이러한 연관으로 인해 인증서를 제시할 때 사용자 프로파일이 부여하거나 거부하는 것과 동일하게 자원에 대한 액세스 및 제한사항을 사용자들이 가지게 됩니다.

디지털 인증 관리자(DCM)를 통해 iSeries 사용자 프로파일에 지정된 인증서를 관리할 수 있습니다. *SECADM 및 *ALLOBJ 특수 권한이 있는 사용자 프로파일을 가지고 있는 경우 관리자 자신이나 다른 사용자에 대한 사용자 프로파일 인증서 지정을 관리할 수 있습니다. 인증서 저장소가 열려 있지 않거나 로컬 인증 기관(CA) 인증서 저장소가 열려 있는 경우 탐색 프레임에서 **사용자 인증서 관리**를 선택하여 적합한 타스크에 액세스할 수 있습니다. 다른 인증서 저장소가 열려 있는 경우 사용자 인증서 타스크가 **인증서 관리** 하의 타스크에 통합됩니다.

*SECADM 및 *ALLOBJ 사용자 프로파일 특수 권한이 없는 사용자는 자신의 인증서 지정만을 관리할 수 있습니다. **사용자 인증서 관리**를 선택하여 사용자 프로파일에 연관된 인증서를 볼 수 있게 하는 타스크에 액세스하거나, 사용자 프로파일에서 인증서를 제거하거나 또는 다른 인증 기관(CA)에서 사용자 프로파일로 인증서를 할당할 수 있습

니다. 사용자 프로파일의 특수 권한에 관계 없이 사용자는 기존 탐색 프레임에서 **인증서 작성** 타스크를 선택하여 로컬 인증 기관(CA)의 사용자 인증서를 확보할 수 있습니다.

DCM을 사용하여 사용자 인증서를 관리 및 작성하는 방법에 대해 자세히 알려면, 다음의 주제를 검토하십시오.

사용자 인증서 작성
사용자가 Local 개인 CA를 사용하여 클라이언트 인증에 대한 인증서를 발행할 수 있는 방법을 알려면 이 정보를 사용하십시오.

사용자 인증서 지정
자신이 소유하는 인증서를 사용자 프로파일과 연관시키는 방법을 알려면 이 정보를 사용하십시오. 인증서는 다른 시스템에 있는 개인 로컬 인증 기관(CA)에서 발행된 것이거나 잘 알려진 인터넷 인증 기관(CA)에서 발행된 것일 수 있습니다. 사용자 프로파일에 인증서를 지정하기 전에 발행하는 CA는 서버가 신뢰하는 것이어야 하며 인증서가 아직 시스템의 사용자 프로파일과 연관된 것이 아니어야 합니다.

사용자 인증서 작성: 사용자 인증을 위해 디지털 인증서를 사용하려면 사용자에게 반드시 인증서가 있어야 합니다. 디지털 인증 관리자(DCM)를 사용하여 개인 로컬 인증 기관(CA)을 운영하는 경우 로컬 CA를 사용하여 각 사용자에게 인증서를 발행할 수 있습니다. 각 사용자는 **인증서 작성** 타스크를 사용하여 인증서를 확보하려면 DCM에 액세스해야 합니다. 로컬 CA에서 인증서를 확보하려면, CA 정책이 CA가 사용자 인증서를 발행하도록 허용해야 합니다.

로컬 CA에서 인증서를 확보하려면, 다음의 단계를 완료하십시오.

1. DCM을 시작하십시오.
2. 탐색 프레임에서 **인증서 작성**을 선택하십시오.
3. 작성할 인증 유형으로 **사용자 인증서**를 선택하십시오. 인증서에 대한 식별 정보를 제공할 수 있는 양식이 표시됩니다.
4. 이 양식을 완성하고 **계속**을 클릭하십시오.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
5. 현재, DCM은 인증에 대한 개인 및 공용 키를 작성하기 위해 브라우저에 대해 작업합니다. 브라우저는 창을 표시하여 이 프로세스를 안내합니다. 이러한 타스크에 대한 브라우저의 지침을 따르십시오. 브라우저가 키를 생성한 후에 DCM이 인증서를 작성했음을 나타내는 확인 페이지가 표시됩니다.
6. 브라우저 소프트웨어에 새로운 인증서를 설치하십시오. 브라우저는 창을 표시하여 이 프로세스를 안내합니다. 이 타스크를 완료하기 위해 브라우저의 지시를 따르십시오.
7. 타스크를 완료하려면 **확인**을 클릭하십시오.

처리되는 동안 디지털 인증 관리자는 인증과 iSeries 사용자 프로파일을 자동으로 연관시킵니다.

사용자가 클라이언트 인증으로 제시하는 다른 CA의 인증서를 자신의 사용자 프로파일과 동일한 권한을 가지도록 하려면, 사용자는 DCM을 사용하여 자신의 사용자 프로파일에 인증서를 지정할 수 있습니다.

사용자 인증서 지정: 사용자 인증에 대해 디지털 인증서를 사용하려면 사용자가 인증서를 가져야 합니다. 사용자가 공용 인터넷 인증 기관(CA)의 인증서를 제시해야 하는 경우 디지털 인증 관리자(DCM)를 사용하여 자신의 사용자 프로파일에 이러한 인증서를 지정할 수 있습니다. 그러면, 관리자와 사용자가 DCM을 사용하여 이러한 인증서를 관리할 수 있습니다.

사용자 인증서 지정 타스크를 사용하려면, 디지털 인증 관리자(DCM)에 액세스하는 것을 통해 HTTP Server와의 보안 세션을 가지고 있어야 합니다. 보안 세션의 여부는 DCM에 액세스하는 데 사용한 URL의 포트 번호로 판별됩니다. DCM에 액세스하기 위한 디폴트 포트인 포트 2001을 사용한 경우 보안 세션을 가지고 있지 않습니다. 또한 보안 세션으로 전환하기 전에 HTTP Server가 SSL을 사용하도록 구성되어야 합니다.

이 타스크를 선택하면, 새로운 브라우저 창이 표시됩니다. 보안 세션이 없으면, DCM은 **사용자 인증서 지정**을 클릭하여 시작하도록 프롬트를 표시합니다. 그러면, DCM은 브라우저와 보안 소켓층(SSL) 조정을 시작합니다.

이러한 조정의 일부로 브라우저는 HTTP Server를 식별하는 인증서를 발행한 인증 기관(CA)의 신뢰 여부에 대해 프롬트를 표시할 수 있습니다. 또한 브라우저는 서버 인증 자체의 수락 여부에 대해 프롬트를 표시할 수 있습니다.

브라우저가 CA를 신뢰하고 서버 인증서를 수락하도록 허용한 후에 서버는 클라이언트 확인을 위한 인증서를 제시하도록 요구할 수 있습니다. 브라우저의 구성 설정에 따라 브라우저는 확인을 위해 제시할 인증서를 선택하도록 프롬트를 표시할 수 있습니다. 브라우저가 시스템이 신뢰하는 것으로 수락한 CA의 인증서를 제시하면, DCM은 별도의 창에 인증 정보를 표시합니다. 수락 가능한 인증서를 제시하지 않으면, 서버는 액세스하도록 허용하기 전에 대신 확인을 위해 사용자명과 암호를 입력하도록 프롬트를 표시할 수 있습니다.

보안 세션을 설정하면, DCM은 사용자 프로파일과 연관시킬 수 있도록 브라우저에서 적합한 인증서를 검색하려고 시도합니다. DCM이 하나 이상의 인증서를 성공적으로 검색하면, 인증 정보를 보고 인증서를 사용자 프로파일과 연관시키도록 선택할 수 있습니다.

DCM이 인증의 정보를 표시하지 않는 경우 DCM이 사용자 프로파일에 지정할 수 있는 인증서를 제공할 수 없습니다. 몇 가지 사용자 인증서 문제 중 하나가 원인일 것입니다. 예를 들어, 브라우저에 포함된 인증서가 이미 사용자 프로파일과 연관되어 있을 수 있습니다.

로컬 CA를 사용하여 사용자에게 인증서를 발행하려는 경우 사용자가 대신 사용자 인증서를 작성해야 합니다.

API를 사용하여 프로그래밍 방식으로 비iSeries 사용자에 대한 인증서 발행

V5R2부터 프로그래밍 방식으로 비 iSeries 사용자에게 인증서를 발행하는 데 사용할 수 있는 두 가지 새로운 API가 있습니다. 이전 릴리스에서 로컬 인증 기관(CA)을 사용하여 사용자에게 인증서를 발행했을 때 이 인증서가 자동으로 iSeries 사용자 프로파일과 연관되었습니다. 따라서 로컬 인증 기관(CA)를 사용하여 클라이언트 인증을 위해 사용자에게 인증서를 발행하려면 iSeries 사용자 프로파일에 해당 사용자를 제공해야 합니다. 또한 사용자가 클라이언트 인증을 위해 로컬 인증 기관(CA)에서 인증서를 확보해야 할 경우 각 사용자가 디지털 인증 관리자(DCM)를 사용해야만 필요한 인증서를 작성할 수 있었습니다. 따라서 각 사용자에게 iSeries 서버로 DCM 및 유효한 사인 온을 호스트하는 iSeries 서버의 사용자 프로파일이 반드시 필요합니다.

특별히 내부 사용자에게 문제가 발생할 때 사용자 프로파일과 연관된 인증서가 있으면 그와 관련된 이점이 있습니다. 그러나 이러한 제한사항 및 요구사항으로 인해 로컬 인증 기관(CA)을 사용하여 많은 사람들에게 사용자 인증서를 발행하는 것은 특히, 해당 사용자에게 iSeries 사용자 프로파일을 소유하지 못하게 할 때 좋은 방법이 아닙니다. 특정 사용자에게 사용자 프로파일을 제공하지 않기 위해 어플리케이션에 대한 사용자 인증서를 요청할 때 사용자가 잘 알려진 인증 기관(CA)에 대해 인증 비용을 지불해야 했습니다.

이 두 가지 새로운 API는 로컬 인증 기관(CA) 인증서가 서명한 사용자 이름의 경우 사용자 인증서를 작성하기 위한 인터페이스를 제공할 수 있도록 지원합니다. 이 인증서는 사용자 프로파일과 관련이 없습니다. 사용자가 DCM을 호스트하는 iSeries 서버에 없어도 되며 DCM을 사용하여 인증서를 작성할 필요가 없습니다.

브라우저 프로그램별로 두 개의 API가 있으며 Net.Data®를 사용하여 사용자에게 인증서를 발행하는 프로그램을 작성할 때 호출할 수 있습니다. 사용자가 작성하는 어플리케이션의 경우 사용자 인증서를 작성하고 인증서에 서명하기 위해 로컬 인증 기관(CA)을 사용하는 적절한 하나의 API를 호출하는 데 있어서 반드시 GUI(Graphical User Interface) 코드를 제공해야 합니다.

이 API 사용에 대한 자세한 내용은 다음 페이지를 참조하십시오.
- 사용자 인증서 요청(QYCUGSUC) API 생성 및 서명.
- 사용자 인증서 요청(QYCUSUC) API 서명.

개인 CA 인증서 사본 확보

보안 소켓층(SSL) 연결을 사용하는 서버에 액세스할 때, 서버는 클라이언트 소프트웨어에 신원 증명으로 인증서를 제시합니다. 그러면, 클라이언트 소프트웨어는 서버가 세션을 설정하기 전에 서버 인증의 유효성을 확인해야 합니다. 서버 인증의 유효성을 확인하려면, 클라이언트 소프트웨어는 서버 인증서를 발행한 인증 기관(CA)의 로컬로 저장된 인증 사본에 액세스할 수 있어야 합니다. 서버가 공용 인터넷 CA의 인증서를 제시하는 경우 브라우저나 다른 클라이언트 소프트웨어는 CA 인증서의 사본을 이미 가지고 있어야 합니다. 그러나, 서버가 개인 로컬 CA의 인증서를 제시하면, 디지털 인증 관리자(DCM)를 사용하여 로컬 CA 인증서의 사본을 확보해야 합니다.

DCM을 사용하여 브라우저에 직접 로컬 CA 인증서를 다운로드하거나 다른 클라이언트 소프트웨어가 액세스하여 사용할 수 있도록 로컬 CA 인증서를 파일에 복사할 수 있습니다. 보안 통신에 브라우저와 다른 어플리케이션을 모두 사용하는 경우 두 가지 방법을 모두 사용하여 로컬 CA 인증서를 설치해야 합니다. 두 방법 모두 사용하는 경우 인증서를 파일에 복사하여 붙여넣기 전에 브라우저에 인증서를 설치하십시오.

서버 어플리케이션이 사용자가 로컬 CA의 인증서를 제시하여 자신을 증명하도록 요구하는 경우 로컬 CA로부터 사용자 인증서를 요구하기 전에 브라우저에 로컬 CA 인증서를 다운로드해야 합니다.

DCM을 사용하여 로컬 CA 인증서의 사본을 확보하려면, 다음의 단계를 완료하십시오.

1. DCM을 시작하십시오.
2. 탐색 프레임에서 **PC에 로컬 CA 인증서 설치**를 선택하여 로컬 CA 인증서를 브라우저에 다운로드하거나 시스템의 파일에 저장할 수 있게 하는 페이지를 표시하십시오.
3. 로컬 CA 인증서를 확보하기 위한 방법을 선택하십시오.
   a. 브라우저에 신뢰할 수 있는 루트로 로컬 CA 인증서를 다운로드하려면 **인증 설치**를 선택하십시오. 그러면, 브라우저가 이 CA의 인증서를 사용하는 서버와 보안 통신 세션을 설정할 수 있습니다. 브라우저는 설치 완료를 돕기 위해 일련의 창들을 표시합니다.
   b. 특수 코드화된 로컬 CA 인증서의 사본이 들어 있는 페이지를 표시하려면 **인증 복사 및 붙여넣기**를 선택하십시오. 페이지에 표시된 텍스트 오브젝트를 사용자의 클립보드로 복사하십시오. 이 정보를 나중에 파일로 붙여넣어야 합니다. 이 파일은 (MKKF 또는 IKEYMAN과 같은) PC 유틸리티 프로그램에 의해 사용되어 PC에서 클라이언트 프로그램이 사용할 수 있도록 인증서를 저장합니다. 클라이언트 어플리케이션이 확인을 위해 로컬 CA 인증서를 인식하고 사용하기 전에 인증서를 신뢰할 수 있는 루트로 인식하도록 어플리케이션을 구성해야 합니다. 이러한 어플리케이션이 파일 사용을 위해 제공하는 지침을 따르십시오.
4. **확인**을 클릭하여 Digital Certificate Manager 홈 페이지로 가십시오.

공용 인터넷 CA에서 제공하는 인증서 관리

보안 필요와 정책을 주의깊게 검토한 후에 VeriSign과 같은 공용 인터넷 인증 기관(CA)으로부터 인증서를 사용하기로 결정했습니다. 예를 들어, 공용 웹 사이트를 운영하고 보안 통신 세션에 보안 소켓층(SSL)을 사용하여 특정 정보 트랜잭션의 프라이버시를 보장하려고 합니다. 웹 사이트는 일반 대중들이 사용할 수 있기 때문에 대부분의 웹 브라우저가 쉽게 인식할 수 있는 인증서를 사용하려고 합니다.

또는 외부 고객을 위해 어플리케이션을 개발하고 공용 인증서를 사용하여 어플리케이션 패키지에 디지털로 서명하려고 합니다. 어플리케이션 패키지에 서명하면 고객은 패키지가 사용자의 회사로부터 온 것이고 권한이 없는 상대가 이동 중에 코드를 변경하지 않았음을 확신할 수 있습니다. 고객이 패키지의 디지털 서명을 쉽고 저렴하게 확인할 수 있도록 공용 인증서를 사용하려고 합니다. 또한 이 인증서를 사용하여 패키지를 고객에게 송신하기 전에 서명을 확인할 수도 있습니다.

디지털 인증 관리자(DCM)의 안내 타스크를 사용하여 공용 인증서와 SSL 연결 설정, 서명된 오브젝트 또는 오브젝트에 대한 디지털 서명의 진위 여부 확인을 위해 이 인증서를 사용하는 어플리케이션을 중앙 관리할 수 있습니다.

공용 인증서 관리

DCM을 사용하여 공용 인터넷 CA의 인증서를 관리하는 경우 먼저 인증서 저장소를 작성해야 합니다. 인증서 저장소는 DCM이 디지털 인증서 및 이와 연관된 개인 키를 저장하기 위해 사용하는 특수 키 데이터베이스 파일입니다. DCM을 통해 인증서 저장소에 들어 있는 인증서의 유형에 기초하여 여러 가지 유형의 인증서 저장소를 작성하고 관리할 수 있습니다.

작성하는 인증서 저장소의 유형과 인증서를 사용하는 어플리케이션 및 인증서를 관리하기 위해 수행해야 하는 후속 타스크는 인증서의 사용 계획에 따라 다릅니다. DCM을 사용하여 적합한 인증서 저장소를 작성하고 어플리케이션에 대한 공용 인터넷 인증서를 관리하는 방법을 알려면, 다음의 주제를 검토하십시오.

- SSL 통신 세션에 대한 공용 인터넷 인증서 관리
- 오브젝트 서명을 위한 공용 인터넷 인증서 관리
- 오브젝트 서명 확인을 위한 인터넷 인증서 관리

또한 DCM을 사용하면 X.509(PKIX) 인증 기관(CA)의 공용 키 인프라구조에서 받은 인증서 관리를 할 수 있습니다.

SSL 통신 세션에 대한 공용 인터넷 인증서 관리

디지털 인증 관리자(DCM)를 사용하여 어플리케이션이 보안 소켓층(SSL)과 보안 통신 세션을 설정할 수 있도록 공용 인터넷 인증서를 관리할 수 있습니다. DCM을 사용하여 자신의 로컬 인증 기관(CA)을 운영하지 않는 경우 먼저 SSL에 사용하는 공용 인증서를 관리할 적합한 인증서 저장소를 작성해야 합니다. 이는 *SYSTEM 인증서 저장소

입니다. 인증서 저장소를 작성하면, DCM은 인증서를 확보하기 위해 공용 CA에 제공해야 하는 인증 요구 정보를 작성하는 프로세스로 안내합니다.

어플리케이션이 SSL 통신 세션을 설정할 수 있도록 DCM을 사용하여 공용 인터넷 인증서를 관리하고 사용하려면, 다음의 단계를 따르십시오.

1. DCM을 시작하십시오.
2. DCM의 탐색 프레임에서 **새 인증서 저장소 작성**을 선택하여 안내 타스크를 시작하고 일련의 양식들을 완성하십시오. 이러한 양식들은 어플리케이션이 SSL 세션에 사용할 수 있는 인증서 저장소와 인증서를 작성하는 프로세스로 안내합니다.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
3. 작성할 인증서 저장소로 ***SYSTEM**을 선택하고 **계속**을 클릭하십시오.
4. *SYSTEM 인증서 저장소 작성의 일부로 인증서를 작성하려면 **예**를 선택하고 **계속**을 클릭하십시오.
5. 새로운 인증의 서명자로 **VeriSign 또는 기타 인터넷 인증 기관(CA)**을 선택하고 **계속**을 클릭하여 새로운 인증에 대한 식별 정보를 제공할 수 있는 양식을 표시하십시오.

   주: iSeries에 IBM 4758-023 PCI Cryptographic Coprocessor가 설치된 경우 DCM은 다음 타스크로 인증에 대한 개인 키를 저장하는 방법을 선택할 수 있게 합니다. 시스템에 코프로세서가 없는 경우 DCM은 *SYSTEM 인증서 저장소에 자동으로 개인 키를 저장합니다. 개인 키 저장 방법을 선택하는 데 도움이 필요한 경우 DCM에서 온라인 도움말을 참조하십시오.
6. 양식을 완성하고 **계속**을 클릭하여 확인 페이지를 표시하십시오. 이 확인 페이지는 인증서를 발행할 공용 인증 기관(CA)에 제공해야 하는 인증 요구 자료를 표시합니다. 인증 서명 요구(CSR) 자료는 공용 키와 새로운 인증에 대해 지정한 기타 정보로 구성되어 있습니다.
7. CSR 자료를 공용 CA가 인증 요구를 위해 필요로 하는 인증 어플리케이션 양식이나 별도의 파일로 복사하여 붙여넣으십시오. 새로운 인증 요구 시작 및 종료 행들을 비롯하여 모든 CSR 자료를 사용해야 합니다. 이 페이지에서 나가면, 모든 자료가 없어지며 다시 복구할 수 없습니다. 인증서를 발행하고 서명하도록 선택한 CA로 어플리케이션 양식이나 파일을 송신하십시오.

   주: 이 프로시듀어를 완료하기 전에 CA에서 서명하여 완성한 인증서가 리턴되기까지 기다려야 합니다.

   주: iSeries용 HTTP Server와 인증서를 사용하려면, DCM에 대한 작업 이전에 서명하여 완성된 인증서에 대해 작업할 수 있도록 웹 서버를 작성하고 구성해

야 합니다. SSL을 사용하기 위해 웹 서버를 구성할 때, 서버를 위한 어플리케이션 ID가 생성됩니다. 이 어플리케이션 ID를 기록했다가 이 어플리케이션이 SSL에 사용해야 하는 인증서를 지정하기 위해 DCM을 사용할 수 있습니다.

DCM을 사용하여 서명 후 완성된 인증서를 서버에 지정할 때까지 서버를 종료하고 다시 시작하지 마십시오. 인증서를 지정하기 전에 웹 서버의 *ADMIN 인스턴스를 종료하고 다시 시작하면 서버가 시작되지 않으며, DCM을 사용하여 서버에 인증서를 지정할 수 없습니다.

8. 공용 CA가 서명된 인증서를 리턴한 후에 DCM을 시작하십시오.
9. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
10. 인증서 저장소 및 암호 페이지가 표시되면, 인증서 저장소를 작성할 때 지정했던 암호를 제공하고 **계속**을 클릭하십시오.
11. 탐색 프레임이 화면정리된 후에 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
12. 타스크 리스트에서 **인증서 가져오기**를 선택하여 서명된 인증서를 *SYSTEM 인증서 저장소로 가져오는 프로세스를 시작하십시오. 인증서 가져오기를 완료한 후에 SSL 통신에 사용해야 하는 어플리케이션을 지정할 수 있습니다.
13. 탐색 프레임에서 **어플리케이션 관리**를 선택하여 타스크 리스트를 표시하십시오.
14. 타스크 리스트에서 **인증서 지정 갱신**을 선택하여 인증서를 지정할 수 있는 SSL이 사용 가능한 어플리케이션의 리스트를 표시하십시오.
15. 리스트에서 어플리케이션을 선택하고 **인증서 지정 갱신**을 클릭하십시오.
16. 가져온 인증서를 선택하고 **새 인증서 지정**을 클릭하십시오. DCM은 어플리케이션에 대한 인증 선택을 확인하기 위한 메세지를 표시합니다.

    주: 일부 SSL이 사용 가능한 어플리케이션은 인증에 기초한 클라이언트 확인을 지원합니다. 자원에 대한 액세스 권한을 제공하기 전에 이러한 지원이 있는 어플리케이션이 인증서를 확인할 수 있도록 하려면, 어플리케이션에 대한 CA 신뢰 리스트를 정의해야 합니다. 그러면, 어플리케이션이 신뢰하는 것으로 지정한 CA에서 이러한 인증만을 유효한 것으로 확인할 수 있습니다. 사용자나 클라이언트 어플리케이션이 CA 신뢰 리스트에서 신뢰하는 것으로 지정되지 않은 CA의 인증서를 제시하면, 어플리케이션은 유효한 확인의 기준으로 이 인증서를 수락하지 않습니다.

안내 타스크를 완료하면, 보안 통신을 위해 SSL을 사용하도록 어플리케이션 구성을 시작하는 데 필요한 모든 것이 준비됩니다. 사용자가 SSL 세션을 통해 이러한 어플리케이션에 액세스하기 전에, 서버 인증서를 발행한 CA에 대해 CA 인증서의 사본을 가지고 있어야 합니다. 인증서가 잘 알려진 인터넷 CA에서 발행한 것이면 사용자의 클라이

언트 소프트웨어가 이미 필요한 CA 인증서의 사본을 가지고 있을 수 있습니다. 사용자가 CA 인증서를 확보해야 하는 경우 그 CA의 웹 사이트에 액세스하여 사이트가 제공하는 지침을 따르십시오.

오브젝트 서명을 위한 공용 인터넷 인증서 관리

디지털 인증 관리자(DCM)를 사용하여 오브젝트에 디지털로 서명하도록 공용 인터넷 인증서를 관리할 수 있습니다. DCM을 사용하여 자신의 로컬 인증 기관(CA)을 운영하지 않는 경우 먼저 오브젝트 서명에 사용하는 공용 인증서를 관리할 적합한 인증서 저장소를 작성해야 합니다. 이것이 *OBJECTSIGNING 인증서 저장소입니다. 인증서 저장소를 작성하면, DCM은 인증서를 확보하기 위해 공용 인터넷 CA에 제공해야 하는 인증 요구 정보를 작성하는 프로세스로 안내합니다.

또한 인증서를 사용하여 오브젝트에 서명하려면, 어플리케이션 ID를 정의해야 합니다. 이 어플리케이션 ID는 누군가가 특정 인증서를 사용하여 오브젝트에 서명하는 데 필요한 권한의 정도를 제어하고 DCM이 제공하는 것 이상의 다른 액세스 제어 레벨을 제공합니다. 디폴트로, 어플리케이션 정의는 사용자가 어플리케이션이 오브젝트에 서명할 수 있도록 인증서를 사용하기 위해 *ALLOBJ 특수 권한을 가지고 있을 것을 요구합니다(그러나, iSeries Navigator를 사용하여 어플리케이션 ID가 요구하는 권한을 변경할 수 있습니다.)

오브젝트에 서명할 수 있도록 DCM을 사용하여 공용 인터넷 인증서를 관리하고 사용하려면 다음 타스크를 완료하십시오.

1. DCM을 시작하십시오.
2. DCM의 왼쪽 탐색 프레임에서 **새 인증서 저장소 작성**을 선택하여 안내 타스크를 시작하고 일련의 양식들을 완성하십시오. 이러한 양식들은 어플리케이션이 오브젝트 서명에 사용할 수 있는 인증서 저장소와 인증서를 작성하는 프로세스로 안내합니다.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
3. 작성할 인증서 저장소로 ***OBJECTSIGNING**을 선택하고 **계속**을 클릭하십시오.
4. 인증서 저장소 작성의 일부로 인증서를 작성하려면 **예**를 선택하고 **계속**을 클릭하십시오.
5. 새로운 인증의 서명자로 **VeriSign 또는 기타 인터넷 인증 기관(CA)**을 선택하고 **계속**을 클릭하십시오. 그러면, 새로운 인증에 대한 식별 정보를 제공할 수 있는 양식이 표시됩니다.

6. 양식을 완성하고 **계속**을 클릭하여 확인 페이지를 표시하십시오. 이 확인 페이지는 인증서를 발행할 공용 인증 기관(CA)에 제공해야 하는 인증 요구 자료를 표시합니다. 인증 서명 요구(CSR) 자료는 공용 키와 새로운 인증에 대해 지정한 기타 정보로 구성되어 있습니다.
7. CSR 자료를 공용 CA가 인증 요구를 위해 필요로 하는 인증 어플리케이션 양식이나 별도의 파일로 조심스럽게 복사하여 붙여넣으십시오. 새로운 인증 요구 시작 및 종료 행들을 비롯하여 모든 CSR 자료를 사용해야 합니다. 이 페이지에서 나갈 때, 이 자료는 유실되며 회복할 수 없습니다. 인증서를 발행하고 서명하도록 선택한 CA로 어플리케이션 양식이나 파일을 송신하십시오.

   주: 이 프로시듀어를 완료하기 전에 CA에서 서명하여 완성한 인증서가 리턴되기까지 기다려야 합니다.
8. 공용 CA가 서명된 인증서를 리턴한 후에 DCM을 시작하십시오.
9. 왼쪽 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***OBJECTSIGNING**을 선택하십시오.
10. 인증서 저장소 및 암호 페이지가 표시되면, 인증서 저장소를 작성할 때 지정했던 암호를 제공하고 **계속**을 클릭하십시오.
11. 탐색 프레임에서 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
12. 타스크 리스트에서 **인증서 가져오기**를 선택하여 서명된 인증서를 *OBJECTSIGNING 인증서 저장소로 가져오는 프로세스를 시작하십시오. 인증서 가져오기를 완료한 후에 인증서를 사용하여 오브젝트에 서명하도록 어플리케이션 정의를 작성할 수 있습니다.
13. 왼쪽 탐색 프레임이 화면정리된 후에 **어플리케이션 관리**를 선택하여 타스크 리스트를 표시하십시오.
14. 타스크 리스트에서 **어플리케이션 추가**를 선택하여 인증서를 사용하여 오브젝트에 서명하도록 오브젝트 서명 어플리케이션 정의를 작성하는 프로세스를 시작하십시오.
15. 오브젝트 서명 어플리케이션을 정의하기 위한 양식을 완성하고 **추가**를 클릭하십시오. 이 어플리케이션 정의는 실제 어플리케이션을 설명하지는 않지만 특정 인증서를 사용하여 서명하려고 계획한 오브젝트 유형을 설명합니다. 양식을 완성하는 방법을 판별하려면 온라인 도움말을 사용하십시오.
16. **확인**을 클릭하여 어플리케이션 정의 확인 메세지를 수신 확인하고 어플리케이션 관리 타스크 리스트를 표시하십시오.
17. 타스크 리스트에서 **인증서 지정 갱신**을 선택하고 **계속**을 클릭하여 인증서를 지정할 수 있는 오브젝트 서명 어플리케이션 ID의 리스트를 표시하십시오.
18. 리스트에서 어플리케이션 ID를 선택하고 **인증서 지정 갱신**을 클릭하십시오.
19. 가져온 인증서를 선택하고 **새 인증서 지정**을 클릭하십시오.

이러한 타스크들을 완료하면 무결성 보장을 위해 오브젝트 서명을 시작하는 데 필요한 모든 것이 준비됩니다.

서명된 오브젝트들을 분배할 때, 이러한 오브젝트들을 수신하는 사용자들은 DCM의 V5R1 또는 이상 버전을 사용하여 오브젝트에 대한 서명의 유효성을 확인함으로 자료가 변경되지 않았음을 보장하고 송신자의 신원을 확인해야 합니다. 서명을 유효성을 확인하기 위해 수신자는 서명 확인 인증서의 사본을 가지고 있어야 합니다. 서명된 오브젝트 패키지의 일부로 이 인증서의 사본을 제공해야 합니다.

또한 수신자는 오브젝트에 서명하는 데 사용한 인증서를 발행한 CA에 대해 CA 인증서의 사본을 가지고 있어야 합니다. 잘 알려진 인터넷 CA의 인증서를 사용하여 오브젝트에 서명한 경우 수신자의 DCM 버전은 필요한 CA 인증서의 사본을 이미 가지고 있어야 합니다. 그러나, 수신자가 아직 사본을 가지고 있지 않을 것으로 생각되면 서명된 오브젝트와 함께 CA 인증서의 사본을 제공해야 합니다. 예를 들어, 개인 로컬 CA의 인증서를 사용하여 오브젝트에 서명한 경우 로컬 CA 인증서의 사본을 제공해야 합니다. 보안 상의 이유로 인해 별도의 패키지에 CA 인증서를 제공하거나 필요로 하는 사용자의 요구 시에 CA 인증서를 공용으로 사용할 수 있게 해야 합니다.

오브젝트 서명 확인을 위한 인증서 관리

디지털 인증 관리자(DCM)를 사용하여 오브젝트에 대한 디지털 서명의 유효성을 확인하는 데 사용하는 서명 확인 인증서를 관리할 수 있습니다. 오브젝트에 서명하려면, 인증서의 개인 키를 사용하여 서명을 작성해야 합니다. 서명된 오브젝트를 다른 사용자에게 송신할 때, 오브젝트에 서명한 인증의 사본을 포함시켜야 합니다. 이 작업은 DCM을 사용하여 서명 확인 인증서로 오브젝트 서명 인증서를 내보내어(인증서의 개인 키 없이) 수행합니다. 서명 확인 인증서를 파일로 내보내고 이를 다른 사용자들에게 분배할 수 있습니다. 또는 작성한 서명을 확인하려는 경우 서명 확인 인증서를 *SIGNATUREVERIFICATION 인증서 저장소로 내보낼 수 있습니다.

오브젝트에 대한 서명의 유효성을 확인하려면, 오브젝트에 서명한 인증의 사본이 있어야 합니다. 인증에 포함된 서명 인증의 공용 키를 사용하여 해당 개인 키로 작성된 서명을 검사하고 확인하십시오. 따라서, 오브젝트에 대한 서명을 확인하기 전에 서명된 오브젝트를 누가 제공했든지 이 제공자로부터 서명 인증의 사본을 확보해야 합니다.

또한 오브젝트에 서명한 인증서를 발행한 CA에 대해 인증 기관(CA) 인증의 사본을 가지고 있어야 합니다. CA 인증서를 사용하여 오브젝트에 서명한 인증서의 진위를 확인합니다. DCM은 가장 잘 알려진 CA의 CA 인증서 사본을 제공합니다. 그러나, 오브젝트가 다른 공용 CA 또는 개인 로컬 CA의 인증서에 의해 서명된 경우 오브젝트 서명을 확인하기 전에 CA 인증서의 사본을 확보해야 합니다.

DCM을 사용하여 오브젝트 서명을 확인하려면, 먼저 필요한 서명 확인 인증서를 관리할 적합한 인증서 저장소를 작성해야 합니다. 이것이 *SIGNATUREVERIFICATION 인증서 저장소입니다. 이 인증서 저장소를 작성하면, DCM은 여기에 잘 알려진 공용 CA 인증서의 사본들을 자동으로 수록합니다.

주: 사용자 자신의 오브젝트 서명 인증서로 작성한 서명을 확인할 수 있게 하려면, *SIGNATUREVERIFICATION 인증서 저장소를 작성하고 *OBJECTSIGNING 인증서 저장소에서 이 곳으로 인증서를 복사해야 합니다. *OBJECTSIGNING 인증서 저장소 내에서 서명 확인을 수행할 계획인 경우에도 이와 같이 복사해야 합니다.

DCM을 사용하여 서명 확인 인증서를 관리하려면 다음 타스크를 완료하십시오.

1. DCM을 시작하십시오.
2. DCM의 왼쪽 탐색 프레임에서 **새 인증서 저장소 작성**을 선택하여 안내 타스크를 시작하고 일련의 양식들을 완성하십시오.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
3. 작성할 인증서 저장소로 ***SIGNATUREVERIFICATION**을 선택하고 **계속**을 클릭하십시오.

   주: *OBJECTSIGNING 인증서 저장소가 있으면, 이 때 DCM은 오브젝트 서명 인증서를 서명 확인 인증서로 새로운 인증서 저장소에 복사할 것인지의 여부를 지정하도록 프롬트를 표시합니다. 기존의 오브젝트 서명 인증서를 사용하여 서명을 확인하려면, **예**를 선택하고 **계속**을 클릭해야 합니다. *OBJECTSIGNING 인증서 저장소로부터 인증서를 복사하려면 이 인증서 저장소의 암호를 알아야 합니다.
4. 새로운 인증서 저장소의 암호를 지정하고 **계속**을 클릭하여 인증서 저장소를 작성하십시오. 인증서 저장소가 성공적으로 작성되었음을 나타내는 확인 페이지가 표시됩니다. 이제 이 저장소를 사용하여 오브젝트 서명을 확인하기 위한 인증서를 관리하고 사용할 수 있습니다.

   주: 서명한 오브젝트의 서명을 확인하기 위해 이 저장소를 작성한 경우 중단할 수 있습니다. 새로운 오브젝트 서명 인증서를 작성할 때, *OBJECTSIGNING 인증서 저장소에서 이 인증서 저장소로 이 인증서를 내보내야 합니다. 이렇게 내보내지 않으면, 이를 사용하여 작성한 서명을 확인할 수 없습니다.

   주: 다른 소스로부터 수신한 오브젝트의 서명을 확인하기 위해 이 인증서 저장소를 작성한 경우 필요한 인증서를 인증서 저장소로 가져올 수 있도록 이 프로시듀어를 계속해야 합니다.

5. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***SIGNATUREVERIFICATION**을 선택하십시오.
6. 인증서 저장소 및 암호 페이지가 표시되면, 인증서 저장소를 작성할 때 지정했던 암호를 제공하고 **계속**을 클릭하십시오.
7. 탐색 프레임이 화면정리된 후에 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
8. 타스크 리스트에서 **인증서 가져오기**를 선택하십시오. 이 안내 타스크는 수신한 오브젝트의 서명을 확인할 수 있도록 필요한 인증서를 인증서 저장소로 가져오는 프로세스를 안내합니다.
9. 내보내려는 인증의 유형을 선택하십시오. **서명 확인**을 선택하여 서명된 오브젝트와 함께 수신한 인증서를 가져오고 가져오기 타스크를 완료하십시오.

   주: 인증서 저장소에 서명 확인 인증서를 발행한 CA에 대한 CA 인증서의 사본이 아직 들어 있지 않은 경우 *먼저* CA 인증서를 가져와야 합니다. 서명 확인 인증서를 가져오기 전에 CA 인증서를 가져오지 않으면 서명 확인 인증서를 가져올 때 오류가 수신될 수 있습니다.

이제 이러한 인증들을 사용하여 오브젝트 서명을 확인할 수 있습니다.

제 8 장 DCM 관리

디지털 인증 관리자(DCM)를 구성한 후 초과 근무를 수행해야 하는 많은 인증서 관리 타스크가 있습니다. DCM을 사용하여 디지털 인증서를 관리하는 방법을 알려면 다음 주제를 검토하십시오.

로컬 CA를 사용하여 다른 iSeries 시스템에 대한 인증서 발행
시스템에서 개인 로컬 인증 기관(CA)을 사용하여 다른 iSeries 시스템에서 사용할 인증서를 발행하는 방법을 알 수 있습니다.

DCM에서 어플리케이션 관리
DCM을 사용하여 SSL 사용가능 어플리케이션이나 오브젝트 서명 어플리케이션에 대해 정의하는 어플리케이션 작업 방법을 설명합니다. 이 주제는 어플리케이션 정의 작성 및 어플리케이션의 인증서 지정을 관리하는 방법에 대한 정보를 제공합니다. 어플리케이션이 클라이언트 인증에 대한 인증서를 수락하는 기준으로 사용하는 CA 신뢰 리스트에 대해 배울 수 있습니다.

인증서 및 어플리케이션 확인
어플리케이션이 특정 인증서를 사용하거나 허용하기 전에 이 인증서의 진위를 확인할 수 있는 방법을 알 수 있습니다.

인증서 할당
보안 기능을 위해 사용할 하나 이상의 어플리케이션을 신속하게 할당하는 방법을 알 수 있습니다.

CRL 위치 관리 어플리케이션이 허용한 인증서가 유효한 것인 지 확인하는 데 사용할 수 있는 인증서 취소 리스트(CRL) 위치를 정의하고 사용하는 방법을 알 수 있습니다.

IBM 4758 Cryptographic Coprocessor에서 인증서 키 저장
설치된 코프로세서를 사용하여 인증서의 개인 키에 보다 안전한 기억장치를 제공하는 방법을 알 수 있습니다.

PKIX CA에 대한 요구 위치 관리
DCM을 사용하여 X.509(PKIX) 표준의 공용 키 인프라구조 하에 인증서를 발행하는 공용 인터넷 인증 기관(CA)에서 확보한 인증서를 관리하는 방법을 알 수 있습니다.

오브젝트 서명
DCM을 사용하여 오브젝트의 무결성을 보장하기 위해 오브젝트에 디지털로 서명하는 데 사용하는 인증서를 관리하는 방법을 알 수 있습니다.

오브젝트 서명 확인
DCM을 사용하여 오브젝트에 있는 디지털 서명의 진위 여부를 확인하는 방법에 관해 알 수 있습니다.

로컬 CA를 사용하여 다른 iSeries 시스템에 대한 인증서 발행

네트워크에서 iSeries의 개인 로컬 인증 기관(CA)을 이미 사용하고 있을 수 있습니다. 이제, 네트워크의 다른 iSeries 시스템으로 이 로컬 CA의 사용을 연장하려고 합니다. 예를 들어, 현재 로컬 CA가 SSL 통신 서버에 사용하도록 다른 iSeries 시스템에 있는 어플리케이션에 대한 서버 또는 클라이언트 인증서를 발행하게 할 수 있습니다. 또는 한 시스템에 있는 로컬 CA의 인증서를 사용하여 다른 iSeries 서버에 저장한 오브젝트에 서명할 수 있습니다.

이러한 목표는 디지털 인증 관리자(DCM)를 사용하여 달성할 수 있습니다. 로컬 CA를 운영하는 iSeries에서 일부 타스크를 수행하고 인증서를 발행하려는 어플리케이션의 호스트인 2차 iSeries에서 다른 타스크들을 수행합니다. 이 2차 시스템을 목표 시스템이라고 합니다. 목표 시스템에서 수행해야 하는 타스크는 시스템의 릴리스 레벨에 따라 다릅니다.

주: 로컬 CA를 운영하는 iSeries 시스템이 목표 시스템보다 강력한 암호화 기능을 제공하는 암호 액세스 제공자 제품을 사용하는 경우 문제가 발생할 수 있습니다. (V5R2에 대해 사용할 수 있는 유일한 암호 액세스 제공자는 5722-AC3입니다. 이것은 사용할 수 있는 가장 강력한 제품입니다. 그러나 이전 릴리스에서 보다 낮은 레벨의 암호 기능이 제공된 보다 약한 기타 암호 액세스 제공자 제품(5722-AC1 또는 5722-AC2)을 설치할 수 있었습니다.) 인증서를 내보낼 때(개인 키와 함께), 시스템은 파일을 암호화하여 그 내용을 보호합니다. 시스템이 목표 시스템보다 강력한 암호 제품을 사용하는 경우 목표 시스템은 가져오기 프로세스 중에 파일을 해독할 수 없습니다. 결국, 가져오기가 실패하거나 인증서를 SSL 세션 설정에 사용할 수 없게 됩니다. 목표 시스템에서 암호 제품과 함께 사용하기에 적합한 새로운 인증의 키 크기를 사용하는 경우에도 마찬가지입니다.

로컬 CA를 사용하여 다른 시스템에 인증서를 발행할 수 있으며 이를 오브젝트 서명에 사용하거나 어플리케이션이 SSL 세션 설정에 사용하도록할 수 있습니다. 로컬 CA를 사용하여 다른 iSeries 시스템에서 사용할 인증서를 작성할 때, DCM이 작성하는 파일에는 로컬 CA 인증서의 사본과 더불어 많은 공용 인터넷 CA에 대한 인증의 사본도 들어 있습니다.

DCM에서 수행해야 하는 타스크는 로컬 CA가 발행하는 인증의 유형과 목표 시스템의 릴리스 레벨 및 상태에 따라 약간 다릅니다.

다른 V5R2 또는 V5R1 iSeries 시스템에서 사용할 개인 인증서 발행

로컬 CA를 사용하여 다른 V5R2 또는 V5R1 iSeries 시스템에서 사용할 인증서를 발행하려면, 로컬 CA의 호스트인 시스템에서 다른의 단계를 수행하십시오.

1. DCM을 시작하십시오.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
2. 탐색 프레임에서 **인증서 작성**을 선택하여 로컬 CA를 통해 작성할 수 있는 인증 유형 리스트를 표시하십시오.

   이 타스크를 완료하기 위해 인증서 저장소를 열 필요는 없습니다. 이러한 지침들은 특정 인증서 저장소 내에서 작업하고 있지 않거나 로컬 인증 기관(CA) 인증서 저장소 내에서 작업하고 있는 것으로 가정합니다. 이러한 타스크들을 수행하기 전에 로컬 CA가 이 시스템에 존재해야 합니다.

3. 로컬 CA가 발행하도록 하려는 인증의 유형을 선택하고 **계속**을 클릭하여 안내 타스크를 시작하고 일련의 양식들을 완성하십시오. 다른 iSeries (for SSL sessions), or an **object signing certificate for another iSeries**용(다른 시스템에서 사용하는 경우) **서버 또는 클라이언트 인증**을 작성할지 선택하십시오.

   주: 다른 시스템이 사용할 오브젝트 서명 인증서를 작성하는 경우 시스템은 인증서를 사용하려면 OS/400의 버전을 실행하고 있어야 합니다. 목표 시스템은 V5R1 이상이어야 하기 때문에 호스트 시스템의 DCM이 새로운 오브젝트 서명 인증의 목표 릴리스 형식을 선택하도록 프롬트를 표시하지 않습니다.
4. 서버 또는 클라이언트 인증서를 작성하는 경우 이 인증서를 작성할 iSeries의 릴리스 레벨을 선택하십시오. **계속**을 클릭하여 새로운 인증에 대한 식별 정보를 제공할 수 있는 양식을 표시하십시오.

   주: 선택한 릴리스 레벨이 DCM이 새로운 인증서를 작성하기 위해 사용하는 형식을 결정합니다. 양식에 있는 식별 정보의 양과 유형은 선택한 릴리스 레벨에 따라 다릅니다. 이것은 인증 파일이 인증서를 사용할 iSeries 시스템과 호환할 수 있도록 합니다.
5. 양식을 완성하고 **계속**을 클릭하여 확인 페이지를 표시하십시오.

   주: 목표 시스템에 기존의 *OBJECTSIGNING 또는 *SYSTEM 인증서 저장소가 있는 경우 반드시 고유 인증 레이블과 인증에 대한 고유 파일명을 지정하십시오. 고유 인증 레이블과 파일명을 지정하면 목표 시스템의 기존 인증서 저장소에 인증서를 쉽게 가져올 수 있습니다.

   이 확인 페이지는 목표 시스템으로 전송할 수 있도록 DCM이 작성한 파일의 이름을 표시합니다. DCM은 지정한 목표 시스템의 릴리스 레벨에 따라 이러한 파일들을 작성합니다. DCM은 로컬 CA 인증서의 사본을 이 파일들에 자동으로 저장합니다.

   주: DCM은 자체 인증서 저장소에서 새로운 인증서를 작성하고 전송할 두 개의 파일인 인증서 저장소 파일(.KDB 확장자) 및 요구 파일(.RDB 확장자)을 생성합니다.
6. 2진 파일 전송 프로토콜(FTP)이나 다른 방법을 사용하여 파일을 목표 시스템으로 전송하십시오.

V4R4 또는 V4R5 iSeries 시스템에서 사용할 개인 인증서 발행

로컬 인증 기관(CA)을 사용하여 V4R4 또는 V4R5 iSeries 시스템에서 사용할 인증서를 발행하려면 V5R2 로컬 인증 기관(CA)을 호스트하는 시스템에서 다음 단계를 수행하십시오.

1. DCM을 시작하십시오.

주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.

2. 탐색 프레임에서 **인증서 작성**을 선택하여 로컬 CA를 통해 작성할 수 있는 인증 유형 리스트를 표시하십시오.

   이 타스크를 완료하기 위해 인증서 저장소를 열 필요는 없습니다. 이러한 지침들은 특정 인증서 저장소 내에서 작업하고 있지 않거나 로컬 인증 기관(CA) 인증서 저장소 내에서 작업하고 있는 것으로 가정합니다. 이러한 타스크들을 수행하기 전에 로컬 CA가 이 시스템에 존재해야 합니다.

3. 로컬 CA가 발행하도록 하려는 인증의 유형을 선택하고 **계속**을 클릭하여 안내 타스크를 시작하고 일련의 양식들을 완성하십시오.

   주: V4R4 또는 V4R5 iSeries 시스템에서 사용할 이 인증서를 작성 중이므로 **다른 iSeries용 서버 또는 클라이언트 인증**을 선택해야 합니다. 릴리스 레벨이 V4R1 이전인 목표 시스템은 오브젝트 서명 인증서를 사용할 수 없습니다.

4. 이 인증서를 작성할 iSeries의 릴리스 레벨을 선택하십시오. **계속**을 클릭하여 새로운 인증에 대한 식별 정보를 제공할 수 있는 양식을 표시하십시오.

   주: 선택한 릴리스 레벨이 DCM이 새로운 인증서를 작성하기 위해 사용하는 형식을 결정합니다. 양식에 있는 식별 정보의 양과 유형은 선택한 릴리스 레벨에 따라 다릅니다. 이것은 인증 파일이 인증서를 사용할 iSeries 시스템과 호환할 수 있도록 합니다.

5. 양식을 완성하고 **계속**을 클릭하여 확인 페이지를 표시하십시오.

   주: 목표 시스템에 기존의 *SYSTEM 인증서 저장소가 있는 경우 반드시 고유 인증 레이블과 인증에 대한 고유 파일명을 지정하십시오. 고유 인증 레이블과 파일명을 지정하면 목표 시스템의 기존 인증서 저장소에 인증서를 쉽게 가져올 수 있습니다.

   이 확인 페이지는 목표 시스템으로 전송할 수 있도록 DCM이 작성한 파일의 이름을 표시합니다. DCM은 지정한 목표 시스템의 릴리스 레벨에 따라 이러한 파일들을 작성합니다. DCM은 로컬 CA 인증서의 사본을 이 파일들에 자동으로 저장합니다.

   주: DCM은 자체 인증서 저장소에서 새로운 인증서를 작성하고 전송할 두 개의 파일인 인증서 저장소 파일(.KDB 확장자) 및 요구 파일(.RDB 확장자)을 생성합니다.

주: 이 파일의 인증서를 V4R4 또는 V4R5 목표 시스템의 기존 *SYSTEM 인증서 저장소에서 사용할 계획인 경우 .KDB 및 .RDB 파일로부터 직접 로컬 CA 인증서를 가져올 수 없습니다. 이것은 CA 인증서가 DCM 가져오기 기능이 인식하고 사용할 수 있는 형식이 아니기 때문입니다. 그 대신, 호스트 시스템을 사용하여 로컬 CA

인증서의 사본을 별도의 파일로 내보내어 CA 인증서가 이전 릴리스의 내보내기 기능으로 작업되는 형식을 유지해야 합니다.

6. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
7. 인증서 저장소 및 암호 페이지가 표시되면, 인증서 저장소를 작성할 때 지정했던 암호를 제공하고 **계속**을 클릭하십시오.
8. 탐색 프레임에서 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
9. 타스크 리스트에서 **인증 내보내기**를 선택하십시오.
10. 내보낼 인증의 유형으로 **인증 기관(CA)**을 선택하고 **계속**을 클릭하여 CA 인증서의 리스트를 표시하십시오.
11. 인증 리스트에서 로컬 CA 인증서를 선택하십시오(예: LOCAL_CERTIFICATE_AUTHORITY). **내보내기**를 클릭하여 CA 인증서의 목적지를 선택할 수 있는 양식을 표시하십시오.
12. **파일**을 선택하고 **계속**을 클릭하십시오.
13. 내보내기 파일의 완전 규정 경로 및 파일명을 지정하고 **계속**을 클릭하십시오. DCM이 파일을 성공적으로 내보냈음을 나타내는 확인 페이지가 표시됩니다.

    주: 파일에 고유한 이름과 확장자를 제공하십시오. 예를 들어, 파일의 이름을 mycafile.exp로 지정할 수 있습니다. 파일의 이름을 지정할 때, 파일에 대해 .TXT, .KDB, .RDB 또는 .KYR 확장자 중 하나를 사용하지 마십시오. 이러한 유형의 확장자 중 하나를 사용하면 목표 시스템에서 파일을 가져올 때 문제점이 발생할 수 있습니다.
14. 2진 파일 전송 프로토콜(FTP) 또는 다른 메소드를 사용하여 V4R4 또는 V4R5 목표 시스템에 작성된 인증서 저장소 파일(.KDB 및 .RDB)을 전송하십시오. ASCII FTP 모드를 사용하여 내보낸 로컬 인증 기관(CA) 인증서를 포함하는 파일을 전송하십시오.

목표 시스템에서 전송된 파일 사용

파일을 전송한 후에 목표 시스템에서 DCM을 사용하여 전송된 인증 파일에 대해 작업하십시오. 수행해야 하는 DCM 타스크는 목표 시스템의 릴리스 레벨과 목표 시스템에 존재하는 인증서 저장소에 따라 다릅니다. 또한 호스트 시스템에서 작성한 인증의 유형이 목표 시스템에서 수행해야 하는 타스크에 영향을 줍니다. 전송된 인증 파일에 대해 작업하기 위해 목표 시스템에서 DCM을 사용하는 방법을 알려면, 다음의 주제를 검토하십시오.

- V5R2 목표 시스템에서 SSL 세션에 개인 인증서 사용.
- V5R1 목표 시스템에서 SSL 세션에 개인 인증서 사용.
- V5R2 또는 V5R1 목표 시스템에서 오브젝트 서명에 개인 인증서 사용.
- V4R5 또는 V4R4 목표 시스템에서 SSL 세션에 개인 인증서 사용.

V5R2 목표 시스템에서 SSL 세션에 개인 인증서 사용

디지털 인증 관리자(DCM)의 *SYSTEM 인증서 저장소에서 어플리케이션이 SSL 세션에 사용하는 인증서를 관리합니다. SSL에 대한 인증서를 관리하기 위해 V5R2 목표 시스템에서 DCM을 사용한 적이 없는 경우 이 인증서 저장소는 목표 시스템에 존재하지 않습니다. 로컬 인증 기관(CA) 호스트 시스템에서 작성한 전송된 인증서 저장소 파일을 사용하기 위한 타스크는 *SYSTEM 인증서 저장소의 존재 여부에 따라 다릅니다. *SYSTEM 인증서 저장소가 존재하지 않음인 경우 *SYSTEM 인증서 저장소를 작성하는 수단으로 전송된 인증 파일을 사용할 수 있습니다. V5R2 목표 시스템에 *SYSTEM 인증서 저장소가 존재하는 경우 전송된 인증 파일을 두 가지 방법 중 하나로 사용할 수 있습니다.

- 전송된 파일을 다른 시스템 인증서 저장소로 사용.
- 기존 *SYSTEM 인증서 저장소로 전송된 파일 가져오기.

*SYSTEM 인증서 저장소가 존재하지 않는 경우

전송된 인증서 저장소 파일을 사용하려는 V5R2 시스템에 *SYSTEM 인증서 저장소가 존재하지 않는 경우 전송된 인증 파일을 *SYSTEM 인증서 저장소로 사용할 수 있습니다. V5R2 목표 시스템에서 *SYSTEM 인증서 저장소를 작성하고 인증 파일을 사용하려면 다음 단계를 따르십시오.

1. 로컬 CA의 호스트인 시스템에서 작성한 인증서 저장소 파일(확장자가 .KDB인 하나의 파일과 확장자가 .RDB인 하나의 파일로 두 개의 파일)이 /QIBM/USERDATA/ICSS/CERT/SERVER 디렉토리에 있는지 확인하십시오.
2. 전송된 인증 파일이 /QIBM/USERDATA/ICSS/CERT/SERVER 디렉토리에 있으면 파일 이름을 DEFAULT.KDB 및 DEFAULT.RDB로 변경하십시오. 해당 디렉토리에서 파일 이름을 변경하여 목표 시스템의 *SYSTEM 인증서 저장소를 구성하는 구성요소를 작성합니다. 인증서 저장소 파일에는 이미 많은 공용 인터넷 CA에 대한 인증의 사본이 들어 있습니다. 이 사본들을 작성했을 때 DCM이 이 사본들을 로컬 CA 인증서의 사본과 함께 인증서 저장소 파일에 추가했습니다.

   주의: 목표 시스템이 이미 /QIBM/USERDATA/ICSS/CERT/SERVER 디렉토리에 DEFAULT.KDB 및 DEFAULT.RDB 파일을 포함하는 경우 *SYSTEM 인증서 저장소가 현재 이 목표 시스템에 존재합니다. 결국, 전송된 파일의 이름을 제안대로 변경하지 말아야 합니다. 디폴트 파일을 겹쳐쓰면, DCM, 전송된 인증서 저장소 및 그 내용을 사용할 때 문제가 발생합니다. 그 대신, 고유한 이름을 가지고 있도록 확인하고 전송된 인증서 저장소를 **기타 시스템 인증서 저장소**로 사용해야 합니다. 파일을 기타 시스템 인증서 저장소로 사용하는 경우 DCM을 사용하여 인증서를 사용해야 하는 어플리케이션을 지정할 수 없습니다.

3. DCM을 시작하십시오. 이제 전송된 파일의 이름을 변경하여 작성한 *SYSTEM 인증서 저장소의 암호를 변경해야 합니다. 암호를 변경하면, 인증서 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장할 수 있습니다.
4. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
5. 인증서 저장소 및 암호 페이지가 표시되면 V5R2 목표 시스템의 인증서를 작성할 때 인증서 저장소의 호스트 시스템에서 지정했던 암호를 제공하고 **계속**을 클릭하십시오.
6. 탐색 프레임에서 **인증서 저장소 관리**를 선택하고 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오. 암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다. 그런 다음, SSL 세션에 대한 인증서를 사용해야 하는 어플리케이션을 지정할 수 있습니다.
7. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
8. 인증서 저장소 및 암호 페이지가 표시되면 새 암호를 제공하고 **계속**을 클릭하십시오.
9. 탐색 프레임이 화면정리된 후에 탐색 프레임에서 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
10. 타스크 리스트에서 **인증서 할당**을 선택하여 현재 인증서 저장소의 인증 리스트를 표시하십시오.
11. 인증서를 할당할 수 있는 SSL 작동 가능 어플리케이션 리스트를 표시하려면 호스트 시스템에서 작성한 인증서를 선택하고 **어플리케이션에 할당**을 클릭하십시오.
12. SSL 세션에 대해 인증서를 사용해야 하는 어플리케이션을 선택하고 **계속**을 클릭하십시오. DCM은 어플리케이션에 대한 인증 선택을 확인하기 위한 메세지를 표시합니다.

    주: 일부 SSL이 사용 가능한 어플리케이션은 인증에 기초한 클라이언트 확인을 지원합니다. 이러한 지원이 있는 어플리케이션은 자원에 대한 액세스 권한을 제공하기 전에 인증서를 확인할 수 있어야 합니다. 결국, 어플리케이션에 대해 CA 신뢰 리스트를 정의해야 합니다. 그러면, 어플리케이션이 신뢰하는 것으로 지정한 CA에서 이러한 인증만을 유효한 것으로 확인할 수 있습니다. 사용자나 클라이언트 어플리케이션이 CA 신뢰 리스트에서 신뢰하는 것으로 지정되지 않은 CA의 인증서를 제시하면, 어플리케이션은 유효한 확인의 기준으로 이 인증서를 수락하지 않습니다.

이러한 타스크가 완료되면, 목표 시스템의 어플리케이션이 다른 iSeries의 로컬 CA가 발행한 인증서를 사용할 수 있습니다. 그러나, 이러한 어플리케이션에 대해 SSL 사용을 시작하기 전에 SSL을 사용하도록 어플리케이션을 구성해야 합니다.

SSL 연결을 통해 선택된 어플리케이션에 액세스할 수 있으려면 먼저 사용자는 호스트 시스템에서 로컬 인증 기관(CA) 인증서의 사본 확보를 수행하기 위해 DCM을 사용해야 합니다. 로컬 CA 인증서은 SSL이 사용 가능한 어플리케이션의 요구사항에 따라 사용자의 PC에 있는 파일로 복사시키거나 사용자의 브라우저로 다운로드시켜야 합니다.

***SYSTEM 인증서 저장소가 존재하는 경우 -- 파일을 기타 시스템 인증서 저장소로 사용**

V5R2 목표 시스템에 이미 *SYSTEM 인증서 저장소가 있는 경우 인증 파일에 대한 작업 방법을 결정해야 합니다. 전송된 인증 파일을 **기타 시스템 인증서 저장소**로 사용하도록 선택할 수 있습니다. 또는 개인 인증서 및 로컬 CA 인증서를 기존의 *SYSTEM 인증서 저장소로 가져오도록 선택할 수 있습니다.

기타 시스템 인증서 저장소는 SSL 인증서에 대한 사용자 정의 2차 인증서 저장소입니다. 이 인증서 저장소를 작성하고 사용하여 DCM 피처를 통해 어플리케이션 ID를 등록하는 데 DCM API를 사용하지 않는 사용자 작성 SSL 사용가능 어플리케이션에 대한 인증서를 제공할 수 있습니다. 기타 시스템 인증서 저장소 옵션을 통해 SSL_Init API를 사용하여 프로그램에 따라 액세스하고 인증서를 사용하여 SSL 세션을 설정하도록 관리자나 다른 사용자들이 작성한 어플리케이션의 인증서를 관리할 수 있습니다. 이 API를 통해 어플리케이션은 특별히 식별한 인증서가 아닌 인증서 저장소에 대한 디폴트 인증서를 사용할 수 있습니다.

IBM iSeries 어플리케이션(그리고 많은 다른 소프트웨어 개발자의 어플리케이션)은 *SYSTEM 인증서 저장소에만 있는 인증서를 사용하도록 작성됩니다. 전송된 파일을 기타 시스템 인증서 저장소로 사용하도록 선택한 경우 DCM을 사용하여 SSL 세션에 대한 인증서를 사용해야 하는 어플리케이션을 지정할 수 없습니다. 결국, 이 인증서를 사용하도록 표준 iSeries SSL 사용 가능 어플리케이션을 구성할 수 없습니다. iSeries 어플리케이션에 대한 인증서를 사용하려면, 전송된 인증서 저장소 파일에서 *SYSTEM 인증서 저장소로 인증서를 가져와야 합니다.

기타 시스템 인증서 저장소로서 전송된 인증 파일에 액세스하고 작업하려면, 다음의 단계를 따르십시오.

1. DCM을 시작하십시오.
2. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 **기타 시스템 인증서 저장소**를 선택하십시오.
3. 인증서 저장소 및 암호 페이지가 표시되면, 호스트 시스템으로부터 전송한 인증서 저장소파일(확장자가 .KDB인 파일)의 완전 규정 경로 및 파일명을 제공하십시오. 또한 V5R2 목표 시스템의 인증서를 작성했을 때 인증서 저장소의 호스트 시스템에서 지정한 암호를 제공하고 **계속**을 클릭하십시오.
4. 탐색 프레임에서 **인증서 저장소 관리**를 선택하고 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오.

주: 인증서 저장소의 암호를 변경할 때, 반드시 **자동 로그인** 옵션을 선택하십시오. 이 옵션을 사용하면 새로운 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장합니다.

암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다. 그런 다음, 이 저장소의 인증서를 디폴트 인증으로 사용하도록 지정할 수 있습니다.

5. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 **기타 시스템 인증서 저장소**를 선택하십시오.
6. 인증서 저장소 및 암호 페이지가 표시되면 인증서 저장소 파일의 전체 규정 경로 및 파일 이름을 제공하고 새 암호를 제공하여 **계속**을 클릭하십시오.
7. 탐색 프레임 화면정리 이후 **인증서 저장소 관리**를 선택하고 타스크 리스트에서 **디폴트 인증 설정**을 선택하십시오.

이제 기타 시스템 인증서 저장소를 작성하고 구성했으므로 SSL_Init API를 사용하는 모든 어플리케이션이 이 저장소 안의 인증서를 사용하여 SSL 세션을 설정할 수 있습니다.

*SYSTEM 인증서 저장소가 존재하는 경우 -- 기존 *SYSTEM 인증서 저장소의 인증 사용

전송된 인증서 저장소 파일의 인증서를 V5R2 시스템에 있는 기존의 *SYSTEM 인증서 저장소에서 사용할 수 있습니다. 이와 같이 하려면, 인증서 저장소 파일에서 기존의 *SYSTEM 인증서 저장소로 인증서를 가져와야 합니다. 그러나, 인증의 형식은 DCM 가져오기 기능이 인식하고 사용할 수 있는 형식이 아니기 때문에 .KDB 및 .RDB 파일에서 직접 인증서를 가져올 수 없습니다. 기존 *SYSTEM 인증서 저장소에서 전송된 인증서를 사용하려면 다른 시스템 인증서 저장소로 파일을 열고 *SYSTEM 인증서 저장소로 이 파일을 내보내야 합니다.

인증서 저장소 파일에서 *SYSTEM 인증서 저장소로 인증서를 내보내려면 V5R2 목표 시스템에서 다음 단계를 완료하십시오.

1. DCM을 시작하십시오.
2. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 **기타 시스템 인증서 저장소**를 지정하십시오.
3. 인증서 저장소 및 암호 페이지가 표시되면, 호스트 시스템으로부터 전송한 인증서 저장소파일(확장자가 .KDB인 파일)의 완전 규정 경로 및 파일명을 제공하십시오. 또한 V5R2 목표 시스템에 대해 인증서를 작성했을 때 인증서 저장소의 호스트 시스템에서 지정한 암호를 제공하고 **계속**을 클릭하십시오.
4. 탐색 프레임에서 **인증서 저장소 관리**를 선택하고 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오.

   주: 인증서 저장소의 암호를 변경할 때, 반드시 **자동 로그인** 옵션을 선택하십시오. 이 옵션을 사용하면 새로운 저장소에서 모든 DCM 인증서 관리 기능을 사용

할 수 있도록 DCM이 새로운 암호를 저장합니다. 암호를 변경하지 않고 자동 로그인 옵션을 선택하는 경우 이 저장소에서 *SYSTEM 인증서 저장소로 인증서를 내보낼 때 오류가 발생할 수 있습니다.

암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다.

5. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 **기타 시스템 인증서 저장소**를 선택하십시오.
6. 인증서 저장소 및 암호 페이지가 표시되면 인증서 저장소 파일의 전체 규정 경로 및 파일 이름을 제공하고 **계속**을 클릭하십시오.
7. 탐색 프레임이 화면정리된 후에 탐색 프레임에서 **인증서 관리**를 선택하여 타스크 리스트를 표시하고 **인증 내보내기**를 선택하십시오.
8. 내보낼 유형의 인증으로 **인증 기관(CA)**을 선택하고 **계속**을 클릭하십시오.

   주: 서버 또는 클라이언트 인증서를 인증서 저장소로 내보내기 전에 로컬 CA 인증서를 인증서 저장소로 내보내야합니다. 서버 또는 클라이언트 인증서를 먼저 내보내면, 로컬 CA 인증서가 인증서 저장소에 없기 때문에 오류가 발생할 수 있습니다.
9. 내보낼 로컬 CA 인증서를 선택하고 **내보내기**를 클릭하십시오.
10. 내보낸 인증의 목적지로 **인증서 저장소**를 선택하고 **계속**을 클릭하십시오.
11. 목표 인증서 저장소로 *SYSTEM을 입력하고, *SYSTEM 인증서 저장소의 암호를 입력하고, **계속**을 클릭하십시오. 내보내기 프로세스가 실패한 경우 인증서를 성공적으로 내보냈음을 나타내거나 오류 정보를 제공하는 메세지가 표시됩니다.
12. 이제 *SYSTEM 인증서 저장소에서 서버 또는 클라이언트 인증서를 내보낼 수 있습니다. **내보내기 인증** 타스크를 다시 선택하십시오.
13. 내보낼 인증의 유형으로 **서버 또는 클라이언트**를 선택하고 **계속**을 클릭하십시오.
14. 내보낼 해당 서버 또는 클라이언트 인증서를 선택하고 **내보내기**를 클릭하십시오.
15. 내보낸 인증의 목적지로 **인증서 저장소**를 선택하고 **계속**을 클릭하십시오.
16. 목표 인증서 저장소로 *SYSTEM을 입력하고, *SYSTEM 인증서 저장소의 암호를 입력하고, **계속**을 클릭하십시오. 내보내기 프로세스가 실패한 경우 인증서를 성공적으로 내보냈음을 나타내거나 오류 정보를 제공하는 메세지가 표시됩니다.
17. 이제 SSL에 사용할 어플리케이션에 인증서를 할당할 수 있습니다. 탐색 프레임에서 **인증서 저장소 작성**을 클릭하고 열려는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
18. 인증서 저장소 및 암호 페이지가 표시되면 *SYSTEM 인증서 저장소의 암호를 제공하고 **계속**을 클릭하십시오.
19. 탐색 프레임이 화면정리된 후에 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
20. 타스크 리스트에서 **인증서 할당**을 선택하여 현재 인증서 저장소의 인증 리스트를 표시하십시오.

21. 인증서를 할당할 수 있는 SSL 작동 가능 어플리케이션 리스트를 표시하려면 호스트 시스템에서 작성한 인증서를 선택하고 **어플리케이션에 할당**을 클릭하십시오.
22. SSL 세션에 대해 인증서를 사용해야 하는 어플리케이션을 선택하고 **계속**을 클릭하십시오. DCM은 어플리케이션에 대한 인증 선택을 확인하기 위한 메세지를 표시합니다.

    주: 일부 SSL이 사용 가능한 어플리케이션은 인증에 기초한 클라이언트 확인을 지원합니다. 이러한 지원이 있는 어플리케이션은 자원에 대한 액세스 권한을 제공하기 전에 인증서를 확인할 수 있어야 합니다. 결국, 어플리케이션에 대해 CA 신뢰 리스트를 정의해야 합니다. 그러면, 어플리케이션이 신뢰하는 것으로 지정한 CA에서 이러한 인증만을 유효한 것으로 확인할 수 있습니다. 사용자나 클라이언트 어플리케이션이 CA 신뢰 리스트에서 신뢰하는 것으로 지정되지 않은 CA의 인증서를 제시하면, 어플리케이션은 유효한 확인의 기준으로 이 인증서를 수락하지 않습니다.

이러한 타스크가 완료되면, 목표 시스템의 어플리케이션이 다른 iSeries의 로컬 CA가 발행한 인증서를 사용할 수 있습니다. 그러나, 이러한 어플리케이션에 대해 SSL 사용을 시작하기 전에 SSL을 사용하도록 어플리케이션을 구성해야 합니다.

SSL 연결을 통해 선택된 어플리케이션에 액세스할 수 있으려면 먼저 사용자는 호스트 시스템에서 로컬 인증 기관(CA) 인증서의 사본 확보를 수행하기 위해 DCM을 사용해야 합니다. 로컬 CA 인증서은 SSL이 사용 가능한 어플리케이션의 요구사항에 따라 사용자의 PC에 있는 파일로 복사시키거나 사용자의 브라우저로 다운로드시켜야 합니다.

V5R1 목표 시스템에서 SSL 세션에 개인 인증서 사용

디지털 인증 관리자(DCM)의 *SYSTEM 인증서 저장소에서 어플리케이션이 SSL 세션에 사용하는 인증서를 관리합니다. SSL에 대한 인증서를 관리하기 위해 V5R1 목표 시스템에서 DCM을 사용한 적이 없는 경우 이 인증서 저장소는 목표 시스템에 존재하지 않습니다. 로컬 인증 기관(CA) 호스트 시스템에서 작성한 전송된 인증서 저장소 파일을 사용하기 위한 타스크는 *SYSTEM 인증서 저장소의 존재 여부에 따라 다릅니다. *SYSTEM 인증서 저장소가 존재하지 않음인 경우 *SYSTEM 인증서 저장소를 작성하는 수단으로 전송된 인증 파일을 사용할 수 있습니다. V5R1 목표 시스템에 *SYSTEM 인증서가 있으면 다음 두 가지 방법 중 하나로 전송된 인증 파일을 사용할 수 있습니다.

- 다른 시스템 인증서 저장소로 전송된 파일 사용.
- 기존 *SYSTEM 인증서 저장소로 전송된 파일 가져오기.

***SYSTEM 인증서 저장소가 존재하지 않는 경우**

전송된 인증서 저장소 파일을 사용하려는 V5R1 시스템에 *SYSTEM 인증서 저장소가 존재하지 않는 경우 전송된 인증 파일을 *SYSTEM 인증서 저장소로 사용할 수 있습니다. V5R1 목표 시스템에서 인증 파일을 사용하려면 다음 단계를 따르십시오.

1. 로컬 CA의 호스트인 시스템에서 작성한 인증서 저장소 파일(확장자가 .KDB인 하나의 파일과 확장자가 .RDB인 하나의 파일로 두 개의 파일)이 /QIBM/USERDATA/ICSS/CERT/SERVER 디렉토리에 있는지 확인하십시오.
2. 전송된 인증 파일이 /QIBM/USERDATA/ICSS/CERT/SERVER 디렉토리에 있으면 파일 이름을 DEFAULT.KDB 및 DEFAULT.RDB로 변경하십시오. 해당 디렉토리에서 파일 이름을 변경하여 목표 시스템의 *SYSTEM 인증서 저장소를 구성하는 구성요소를 작성합니다. 인증서 저장소 파일에는 이미 많은 공용 인터넷 CA에 대한 인증의 사본이 들어 있습니다. 이 사본들을 작성했을 때 DCM이 이 사본들을 로컬 CA 인증서의 사본과 함께 인증서 저장소 파일에 추가했습니다.

   주의: 목표 시스템이 이미 /QIBM/USERDATA/ICSS/CERT/SERVER 디렉토리에 DEFAULT.KDB 및 DEFAULT.RDB 파일을 포함하는 경우 *SYSTEM 인증서 저장소가 현재 이 목표 시스템에 존재합니다. 결국, 전송된 파일의 이름을 제안대로 변경하지 말아야 합니다. 디폴트 파일을 겹쳐쓰면, DCM, 전송된 인증서 저장소 및 그 내용을 사용할 때 문제가 발생합니다. 그 대신, 고유한 이름을 가지고 있도록 확인하고 전송된 인증서 저장소를 **기타 시스템 인증서 저장소**로 사용해야 합니다. 파일을 기타 시스템 인증서 저장소로 사용하는 경우 DCM을 사용하여 인증서를 사용해야 하는 어플리케이션을 지정할 수 없습니다.
3. DCM을 시작하십시오. 이제 전송된 파일의 이름을 변경하여 작성한 *SYSTEM 인증서 저장소의 암호를 변경해야 합니다. 암호를 변경하면, 인증서 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장할 수 있습니다.
4. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
5. 인증서 저장소 및 암호 페이지가 표시되면 V5R1 목표 시스템의 인증서를 작성했을 때 호스트 시스템에서 인증서 저장소에 대해 지정한 암호를 제공하고 **계속**을 클릭하십시오.
6. 탐색 프레임에서 **인증서 저장소 관리**를 선택하고 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오. 암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다. 그런 다음, SSL 세션에 대한 인증서를 사용해야 하는 어플리케이션을 지정할 수 있습니다.
7. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
8. 인증서 저장소 및 암호 페이지가 표시되면 새 암호를 제공하고 **계속**을 클릭하십시오.

9. 탐색 프레임이 화면정리된 후에 탐색 프레임에서 **어플리케이션 관리**를 선택하여 타스크 리스트를 표시하십시오.
10. 타스크 리스트에서 **인증서 지정 갱신**을 선택하여 인증서를 지정할 수 있는 SSL이 사용 가능한 어플리케이션의 리스트를 표시하십시오.
11. 리스트에서 어플리케이션을 선택하고 **인증서 지정 갱신**을 클릭하십시오.
12. 호스트 시스템의 로컬 CA가 발행한 인증서를 선택하고 **새 인증서 지정**을 클릭하십시오. DCM은 어플리케이션에 대한 인증 선택을 확인하기 위한 메세지를 표시합니다.

    주: 일부 SSL이 사용 가능한 어플리케이션은 인증에 기초한 클라이언트 확인을 지원합니다. 이러한 지원이 있는 어플리케이션은 자원에 대한 액세스 권한을 제공하기 전에 인증서를 확인할 수 있어야 합니다. 결국, 어플리케이션에 대해 CA 신뢰 리스트를 정의해야 합니다. 그러면, 어플리케이션이 신뢰하는 것으로 지정한 CA에서 이러한 인증만을 유효한 것으로 확인할 수 있습니다. 사용자나 클라이언트 어플리케이션이 CA 신뢰 리스트에서 신뢰하는 것으로 지정되지 않은 CA의 인증서를 제시하면, 어플리케이션은 유효한 확인의 기준으로 이 인증서를 수락하지 않습니다.

이러한 타스크가 완료되면, 목표 시스템의 어플리케이션이 다른 iSeries의 로컬 CA가 발행한 인증서를 사용할 수 있습니다. 그러나, 이러한 어플리케이션에 대해 SSL 사용을 시작하기 전에 SSL을 사용하도록 어플리케이션을 구성해야 합니다.

SSL 연결을 통해 선택된 어플리케이션에 액세스할 수 있으려면 먼저 사용자는 호스트 시스템에서 로컬 인증 기관(CA) 인증서의 사본 확보를 수행하기 위해 DCM을 사용해야 합니다. CA 인증서는 SSL이 사용 가능한 어플리케이션의 요구사항에 따라 사용자의 PC에 있는 파일로 복사시키거나 사용자의 브라우저로 다운로드시켜야 합니다.

*SYSTEM 인증서 저장소가 존재하는 경우 -- 파일을 기타 시스템 인증서 저장소로 사용

V5R1 목표 시스템에 이미 *SYSTEM 인증서 저장소가 있는 경우 인증 파일에 대한 작업 방법을 결정해야 합니다. 전송된 인증 파일을 **기타 시스템 인증서 저장소**로 사용하도록 선택할 수 있습니다. 또는 개인 인증서 및 로컬 CA 인증서를 기존의 *SYSTEM 인증서 저장소로 가져오도록 선택할 수 있습니다.

기타 시스템 인증서 저장소는 SSL 인증서에 대한 사용자 정의 2차 인증서 저장소입니다. 이 인증서 저장소를 작성하고 사용하여 DCM 유틸리티를 통해 어플리케이션 ID를 등록하는 데 DCM API를 사용하지 않는 사용자 작성 SSL 사용가능 어플리케이션에 대한 인증서를 제공할 수 있습니다. 기타 시스템 인증서 저장소 옵션을 통해 SSL_Init API를 사용하여 프로그램에 따라 액세스하고 인증서를 사용하여 SSL 세션을 설정하도록 관리자나 다른 사용자들이 작성한 어플리케이션의 인증서를 관리할 수 있습니다. 이 API를 통해 어플리케이션은 특별히 식별한 인증서가 아닌 인증서 저장소에 대한 디폴트 인증서를 사용할 수 있습니다.

IBM iSeries 어플리케이션(그리고 많은 다른 소프트웨어 개발자의 어플리케이션)은 *SYSTEM 인증서 저장소에만 있는 인증서를 사용하도록 작성됩니다. 전송된 파일을 기타 시스템 인증서 저장소로 사용하도록 선택한 경우 DCM을 사용하여 SSL 세션에 대한 인증서를 사용해야 하는 어플리케이션을 지정할 수 없습니다. 결국, 이 인증서를 사용하도록 표준 iSeries SSL 사용 가능 어플리케이션을 구성할 수 없습니다. iSeries 어플리케이션에 대한 인증서를 사용하려면, 전송된 인증서 저장소 파일에서 *SYSTEM 인증서 저장소로 인증서를 가져와야 합니다.

기타 시스템 인증서 저장소로서 전송된 인증 파일에 액세스하고 작업하려면, 다음의 단계를 따르십시오.

1. DCM을 시작하십시오.
2. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 **기타 시스템 인증서 저장소**를 선택하십시오.
3. 인증서 저장소 및 암호 페이지가 표시되면, 호스트 시스템으로부터 전송한 인증서 저장소파일(확장자가 .KDB인 파일)의 완전 규정 경로 및 파일명을 제공하십시오. 또한 V5R1 목표 시스템의 인증서를 작성했을 때 호스트 시스템에서 인증서 저장소에 대해 지정한 암호를 제공하고 **계속**을 클릭하십시오.
4. 탐색 프레임에서 **인증서 저장소 관리**를 선택하고 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오.

   주: 인증서 저장소의 암호를 변경할 때, 반드시 **자동 로그인** 옵션을 선택하십시오. 이 옵션을 사용하면 새로운 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장합니다.

   암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다. 그런 다음, 이 저장소의 인증서를 디폴트 인증으로 사용하도록 지정할 수 있습니다.
5. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 **기타 시스템 인증서 저장소**를 선택하십시오.
6. 인증서 저장소 및 암호 페이지가 표시되면 인증서 저장소 파일의 전체 규정 경로 및 파일 이름을 제공하고 새 암호를 제공하여 **계속**을 클릭하십시오.
7. 탐색 프레임 화면정리 이후 **인증서 저장소 관리**를 선택하고 타스크 리스트에서 **디폴트 인증 설정**을 선택하십시오.

이제 기타 시스템 인증서 저장소를 작성하고 구성했으므로 SSL_Init API를 사용하는 모든 어플리케이션이 이 저장소 안의 인증서를 사용하여 SSL 세션을 설정할 수 있습니다.

*SYSTEM 인증서 저장소가 존재하는 경우 -- 기존 *SYSTEM 인증서 저장소의 인증 사용

전송된 인증서 저장소 파일의 인증서를 V5R1 시스템에 있는 기존의 *SYSTEM 인증서 저장소에서 사용할 수 있습니다. 이와 같이 하려면, 인증서 저장소 파일에서 기존의

*SYSTEM 인증서 저장소로 인증서를 가져와야 합니다. 그러나, 인증의 형식은 DCM 가져오기 기능이 인식하고 사용할 수 있는 형식이 아니기 때문에 .KDB 및 .RDB 파일에서 직접 인증서를 가져올 수 없습니다. 기존 *SYSTEM 인증서 저장소에서 전송된 인증서를 사용하려면 다른 시스템 인증서 저장소로 파일을 열고 *SYSTEM 인증서 저장소로 이 파일을 내보내야 합니다.

주: 이 프로시듀어는 다른 시스템 인증서 저장소를 사용하여 원래 인증서 저장소 파일에서 *SYSTEM 인증서 저장소로 인증서를 내보내는 방법을 설명합니다. 메소드를 사용하여 인증서를 *SYSTEM 인증서 저장소에 추가하면 목표 시스템이 호스트 시스템보다 약한 암호 액세스 제공자 제품(예: 5722-AC2)을 사용할 때 발생할 수 있는 문제를 방지할 수 있습니다.

인증서 저장소 파일에서 *SYSTEM 인증서 저장소로 인증서를 내보내려면 V5R1 목표 시스템에서 다음 단계를 완료하십시오.

1. DCM을 시작하십시오.
2. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 **기타 시스템 인증서 저장소**를 지정하십시오.
3. 인증서 저장소 및 암호 페이지가 표시되면, 호스트 시스템으로부터 전송한 인증서 저장소파일(확장자가 .KDB인 파일)의 완전 규정 경로 및 파일명을 제공하십시오. 또한 V5R1 목표 시스템의 인증서를 작성했을 때 호스트 시스템에서 인증서 저장소에 대해 지정한 암호를 제공하고 **계속**을 클릭하십시오.
4. 탐색 프레임에서 **인증서 저장소 관리**를 선택하고 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오.

   주: 인증서 저장소의 암호를 변경할 때, 반드시 **자동 로그인** 옵션을 선택하십시오. 이 옵션을 사용하면 새로운 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장합니다. 암호를 변경하지 않고 자동 로그인 옵션을 선택하는 경우 이 저장소에서 *SYSTEM 인증서 저장소로 인증서를 내보낼 때 오류가 발생할 수 있습니다.

   암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다.
5. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 **기타 시스템 인증서 저장소**를 선택하십시오.
6. 인증서 저장소 및 암호 페이지가 표시되면 인증서 저장소 파일의 전체 규정 경로 및 파일 이름을 제공하고 **계속**을 클릭하십시오.
7. 탐색 프레임이 화면정리된 후에 탐색 프레임에서 **인증서 관리**를 선택하여 타스크 리스트를 표시하고 **인증 내보내기**를 선택하십시오.
8. 내보낼 유형의 인증으로 **인증 기관(CA)**을 선택하고 **계속**을 클릭하십시오.

주: 서버 또는 클라이언트 인증서를 인증서 저장소로 내보내기 전에 로컬 CA 인증서를 인증서 저장소로 내보내야합니다. 서버 또는 클라이언트 인증서를 먼저 내보내면, 로컬 CA 인증서가 인증서 저장소에 없기 때문에 오류가 발생할 수 있습니다.

9. 내보낼 로컬 CA 인증서를 선택하고 **내보내기**를 클릭하십시오.
10. 내보낸 인증의 목적지로 **인증서 저장소**를 선택하고 **계속**을 클릭하십시오.
11. 목표 인증서 저장소로 *SYSTEM을 입력하고, *SYSTEM 인증서 저장소의 암호를 입력하고, **계속**을 클릭하십시오.
12. 이제 *SYSTEM 인증서 저장소에서 서버 또는 클라이언트 인증서를 내보낼 수 있습니다. **내보내기 인증** 타스크를 다시 선택하십시오.
13. 내보낼 인증의 유형으로 **서버 또는 클라이언트**를 선택하고 **계속**을 클릭하십시오.
14. 내보낼 해당 서버 또는 클라이언트 인증서를 선택하고 **내보내기**를 클릭하십시오.
15. 내보낸 인증의 목적지로 **인증서 저장소**를 선택하고 **계속**을 클릭하십시오.
16. 목표 인증서 저장소로 *SYSTEM을 입력하고, *SYSTEM 인증서 저장소의 암호를 입력하고, **계속**을 클릭하십시오. 내보내기 프로세스가 실패한 경우 인증서를 성공적으로 내보냈음을 나타내거나 오류 정보를 제공하는 메세지가 표시됩니다.
17. 이제 SSL에 사용할 어플리케이션에 인증서를 할당할 수 있습니다. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열려는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
18. 인증서 저장소 및 암호 페이지가 표시되면 *SYSTEM 인증서 저장소의 암호를 제공하고 **계속**을 클릭하십시오.
19. 탐색 프레임이 화면정리된 후에 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
20. 타스크 리스트에서 **인증서 지정 갱신**을 선택하여 인증서를 지정할 수 있는 SSL이 사용 가능한 어플리케이션의 리스트를 표시하십시오.
21. 리스트에서 어플리케이션을 선택하고 **인증서 지정 갱신**을 클릭하십시오.
22. 호스트 시스템의 로컬 CA가 발행한 인증서를 선택하고 **새 인증서 지정**을 클릭하십시오. DCM은 어플리케이션에 대한 인증 선택을 확인하기 위한 메세지를 표시합니다.

주: 일부 SSL이 사용 가능한 어플리케이션은 인증에 기초한 클라이언트 확인을 지원합니다. 이러한 지원이 있는 어플리케이션은 자원에 대한 액세스 권한을 제공하기 전에 인증서를 확인할 수 있어야 합니다. 결국, 어플리케이션에 대해 CA 신뢰 리스트를 정의해야 합니다. 그러면, 어플리케이션이 신뢰하는 것으로 지정한 CA에서 이러한 인증만을 유효한 것으로 확인할 수 있습니다. 사용자나 클라이언트 어플리케이션이 CA 신뢰 리스트에서 신뢰하는 것으로 지정되지 않은 CA의 인증서를 제시하면, 어플리케이션은 유효한 확인의 기준으로 이 인증서를 수락하지 않습니다.

이러한 타스크가 완료되면, 목표 시스템의 어플리케이션이 다른 iSeries의 로컬 CA가 발행한 인증서를 사용할 수 있습니다. 그러나, 이러한 어플리케이션에 대해 SSL 사용을 시작하기 전에 SSL을 사용하도록 어플리케이션을 구성해야 합니다.

SSL 연결을 통해 선택된 어플리케이션에 액세스할 수 있으려면 먼저 사용자는 호스트 시스템에서 로컬 인증 기관(CA) 인증서의 사본 확보를 수행하기 위해 DCM을 사용해야 합니다. CA 인증서는 SSL이 사용 가능한 어플리케이션의 요구사항에 따라 사용자의 PC에 있는 파일로 복사시키거나 사용자의 브라우저로 다운로드시켜야 합니다.

V5R2 또는 V5R1 목표 시스템에서 오브젝트 서명에 개인 인증서 사용

디지털 인증 관리자(DCM)의 *OBJECTSIGNING 인증서 저장소에서 오브젝트 서명에 사용하는 인증서를 관리합니다. 오브젝트 서명 인증서를 관리하기 위해 목표 시스템에서 DCM을 사용한 적이 없는 경우 이 인증서 저장소는 목표 시스템에 존재하지 않습니다. 로컬 CA 호스트 시스템에서 작성한 전송된 인증서 저장소 파일을 사용하기 위해 수행해야 하는 타스크는 *OBJECTSIGNING 인증서 저장소의 존재 여부에 따라 다릅니다. *OBJECTSIGNING 인증서 저장소가 존재하지 않음인 경우 *OBJECTSIGNING 인증서 저장소를 작성하는 수단으로 전송된 인증 파일을 사용할 수 있습니다. 목표 시스템에 *OBJECTSIGNING 인증서가 존재하는 경우 전송된 인증서를 여기로 가져와야 합니다.

***OBJECTSIGNING 인증서 저장소가 존재하지 않는 경우**

로컬 CA 호스트 시스템에서 작성한 인증서 저장소 파일을 사용하기 위해 수행하는 타스크는 오브젝트 서명 인증서를 관리하기 위해 목표 시스템에서 DCM을 사용한 적이 있는지에 따라 다릅니다.

*OBJECTSIGNING 인증서 저장소가 전송된 인증서 저장소 파일이 있는 V5R2 또는 V5R1 목표 시스템에 없는 경우 다음의 단계를 따르십시오.

1. 로컬 CA의 호스트인 시스템에서 작성한 인증서 저장소 파일(확장자가 .KDB인 하나의 파일과 확장자가 .RDB인 하나의 파일로 두 개의 파일)이 /QIBM/USERDATA/ICSS/CERT/SIGNING 디렉토리에 있는지 확인하십시오.
2. 전송된 인증 파일이 /QIBM/USERDATA/ICSS/CERT/SIGNING 디렉토리에 있으면 필요한 경우 인증 파일 이름을 SGNOBJ.KDB 및 SGNOBJ.RDB로 변경하십시오. 이러한 파일들의 이름을 변경하여 목표 시스템에 대한 *OBJECTSIGNING 인증서 저장소를 구성하는 구성요소를 작성합니다. 인증서 저장소 파일에는 이미 많은 공용 인터넷 CA에 대한 인증의 사본이 들어 있습니다. 이 사본들을 작성했을 때 DCM이 이 사본들을 로컬 CA 인증서의 사본과 함께 인증서 저장소 파일에 추가했습니다.

   주의: 목표 시스템이 이미 /QIBM/USERDATA/ICSS/CERT/SIGNING 디렉토리에 SGNOBJ.KDB 및 SGNOBJ.RDB 파일을 포함하는 경우 *OBJECTSIGNING

인증서 저장소가 현재 이 목표 시스템에 존재합니다. 결국, 전송된 파일의 이름을 제안대로 변경하지 말아야 합니다. 디폴트 오브젝트 서명 파일을 겹쳐 쓰면, DCM, 전송된 인증서 저장소 및 그 내용을 사용할 때 문제가 발생합니다. 두 가지 방법 중 한 방법으로 이러한 파일에서 기존의 *OBJECTSIGNING 인증서 저장소로 인증서를 가져올 수 있습니다. 이 파일의 인증서를 플랫 파일 세트로 내보내어 여기에서 인증서를 기존의 *OBJECTSIGNING 인증서 저장소로 가져올 수 있습니다. 또는 이 자료에 자세하게 설명된 대로 전송된 파일을 기타 시스템 인증서 저장소로 열고 인증서를 *OBJECTSIGNING 인증서 저장소에 직접 내보낼 수 있습니다. 어느 경우에나 이 프로시듀어가 설명하는 것과 같이 인증서를 사용하는 어플리케이션을 관리할 수 있으려면 *OBJECTSIGNING 인증서 저장소로 인증서를 가져와야 합니다.

3. DCM을 시작하십시오. 이제 *OBJECTSIGNING 인증서 저장소의 암호를 변경해야 합니다. 암호를 변경하면, 인증서 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장할 수 있습니다.
4. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***OBJECTSIGNING**를 선택하십시오.
5. 암호 페이지가 표시되면, 호스트 시스템에서 인증서 저장소를 작성할 때 지정했던 암호를 제공하고 **계속**을 클릭하십시오.
6. 탐색 프레임에서 **인증서 저장소 관리**를 선택하고 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오. 암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다. 그런 다음, 오브젝트에 서명하는 데 인증서를 사용할 수 있도록 어플리케이션 정의를 작성할 수 있습니다.
7. 인증서 저장소를 다시 연 후에 탐색 프레임에서 **어플리케이션 관리**를 선택하여 타스크 리스트를 표시하십시오.
8. 타스크 리스트에서 **어플리케이션 추가**를 선택하여 인증서를 사용하여 오브젝트에 서명하도록 오브젝트 서명 어플리케이션 정의를 작성하는 프로세스를 시작하십시오.
9. 오브젝트 서명 어플리케이션을 정의하기 위한 양식을 완성하고 **추가**를 클릭하십시오. 이 어플리케이션 정의는 실제 어플리케이션을 설명하지는 않지만 특정 인증서를 사용하여 서명하려고 계획한 오브젝트 유형을 설명합니다. 양식을 완성하는 방법을 판별하려면 온라인 도움말을 사용하십시오.
10. **확인**을 클릭하여 어플리케이션 정의 확인 메세지를 수신 확인하고 **어플리케이션 관리** 타스크 리스트를 표시하십시오.
11. 타스크 리스트에서 **인증서 지정 갱신**을 선택하고 인증서를 지정할 수 있는 오브젝트 서명 어플리케이션 ID의 리스트를 표시하십시오.
12. 리스트에서 어플리케이션 ID를 선택하고 **인증서 지정 갱신**을 클릭하십시오.
13. 호스트 시스템의 로컬 CA가 작성한 인증서를 선택하고 **새 인증서 지정**을 클릭하십시오.

이러한 타스크들을 완료하면 무결성 보장을 위해 오브젝트 서명을 시작하는 데 필요한 모든 것이 준비됩니다.

서명된 오브젝트들을 분배할 때, 이러한 오브젝트들을 수신하는 사용자들은 DCM의 V5R2 또는 V5R1 버전을 사용하여 오브젝트에 대한 서명을 확인함으로 자료가 변경되지 않았음을 보장하고 송신자의 신원을 확인해야 합니다. 서명을 유효성을 확인하기 위해 수신자는 서명 확인 인증서의 사본을 가지고 있어야 합니다. 서명된 오브젝트 패키지의 일부로 이 인증서의 사본을 제공해야 합니다.

또한 수신자는 오브젝트에 서명하는 데 사용한 인증서를 발행한 CA에 대해 CA 인증서의 사본을 가지고 있어야 합니다. 잘 알려진 인터넷 CA의 인증서를 사용하여 오브젝트에 서명한 경우 수신자의 DCM 버전은 필요한 CA 인증서의 사본을 이미 가지고 있어야 합니다. 그러나, 필요하면 서명된 오브젝트와 함께 별도의 패키지에 CA 인증서의 사본을 제공해야 합니다. 예를 들어, 로컬 CA의 인증서를 사용하여 오브젝트에 서명한 경우 로컬 CA 인증서의 사본을 제공해야 합니다. 보안 상의 이유로 인해 별도의 패키지에 CA 인증서를 제공하거나 필요로 하는 사용자의 요구 시에 CA 인증서를 공용으로 사용할 수 있게 해야 합니다.

*OBJECTSIGNING 인증서 저장소가 존재하는 경우

전송된 인증서 저장소 파일의 인증서를 V5R2 또는 V5R1 시스템에 있는 기존의 *OBJECTSIGNING 인증서 저장소에서 사용할 수 있습니다. 이와 같이 하려면, 인증서 저장소 파일에서 기존의 *OBJECTSIGNING 인증서 저장소로 인증서를 가져와야 합니다. 그러나, 인증의 형식은 DCM 가져오기 기능이 인식하고 사용할 수 있는 형식이 아니기 때문에 .KDB 및 .RDB 파일에서 직접 인증서를 가져올 수 없습니다. V5R2 또는 V5R1 목표 시스템에서 전송된 파일을 기타 시스템 인증서 저장소로 열어서 기존의 *OBJECTSIGNING 인증서 저장소로 인증서를 추가할 수 있습니다. 그런 다음, 인증서를 *OBJECTSIGNING 인증서 저장소로 직접 내보낼 수 있습니다. 전송된 파일에서 로컬 인증 자체와 로컬 CA 인증서 둘 다의 사본을 내보내야 합니다.

인증서 저장소 파일로부터 *OBJECTSIGNING 인증서 저장소로 인증서를 내보내려면, V5R2 또는 V5R1 목표 시스템에서 다음의 단계를 완료하십시오.

1. DCM을 시작하십시오.
2. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 **기타 시스템 인증서 저장소**를 지정하십시오.
3. 인증서 저장소 및 암호 페이지가 표시되면 인증서 저장소 파일의 전체 규정 경로 및 파일 이름을 제공하십시오. 또한 호스트 시스템에서 인증서 저장소를 작성했을 때 사용한 암호를 제공하고 **계속**을 클릭하십시오.
4. 탐색 프레임에서 **인증서 저장소 관리**를 선택하고 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오.

주: 인증서 저장소의 암호를 변경할 때, 반드시 **자동 로그인** 옵션을 선택하십시오. 이 옵션을 사용하면 새로운 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장합니다. 암호를 변경하지 않고 자동 로그인 옵션을 선택하는 경우 이 저장소에서 *OBJECTSIGNING 인증서 저장소로 인증서를 내보낼 때 오류가 발생할 수 있습니다.

암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다.

5. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 **기타 시스템 인증서 저장소**를 선택하십시오.
6. 인증서 저장소 및 암호 페이지가 표시되면 인증서 저장소 파일의 전체 규정 경로 및 파일 이름을 제공하고 **계속**을 클릭하십시오.
7. 탐색 프레임이 화면정리된 후에 탐색 프레임에서 **인증서 관리**를 선택하여 타스크 리스트를 표시하고 **인증 내보내기**를 선택하십시오.
8. 내보낼 인증의 유형으로 **인증 기관(CA)**을 선택하고 **계속**을 클릭하십시오.

   주: 이 타스크에 대한 용어는 기타 시스템 인증서 저장소에 대해 작업할 때, 서버 또는 클라이언트 인증에 대해 작업하고 있는 것으로 가정합니다. 이것은 이러한 유형의 인증서 저장소는 *SYSTEM 인증서 저장소에 대한 2차 인증서 저장소로 사용하기 위한 것이기 때문입니다. 그러나, 이 인증서 저장소에서 내보내기 타스크를 사용하는 것이 전송된 파일에서 기존의 *OBJECTSIGNING 인증서 저장소로 인증서를 내보내는 가장 쉬운 방법입니다.
9. 내보낼 로컬 CA 인증서를 선택하고 **내보내기**를 클릭하십시오.

   주: 오브젝트 서명 인증서를 인증서 저장소로 내보내기 전에 로컬 CA 인증서를 인증서 저장소로 내보내야 합니다. 오브젝트 서명 인증서를 먼저 내보내면, 로컬 CA 인증서가 인증서 저장소에 없기 때문에 오류가 발생할 수 있습니다.
10. 내보낸 인증의 목적지로 **인증서 저장소**를 선택하고 **계속**을 클릭하십시오.
11. 목표 인증서 저장소로 *OBJECTSIGNING을 입력하고, 이 인증서 저장소의 암호를 입력하고, **계속**을 클릭하십시오.
12. 이제 오브젝트 서명 인증서를 *OBJECTSIGNING 인증서 저장소로 내보낼 수 있습니다. **내보내기 인증** 타스크를 다시 선택하십시오.
13. 내보낼 인증의 유형으로 **서버 또는 클라이언트**를 선택하고 **계속**을 클릭하십시오.
14. 내보낼 해당 인증서를 선택하고 **내보내기**를 클릭하십시오.
15. 내보낸 인증의 목적지로 **인증서 저장소**를 선택하고 **계속**을 클릭하십시오.
16. 목표 인증서 저장소로 *OBJECTSIGNING을 입력하고, *OBJECTSIGNING 인증서 저장소의 암호를 입력하고, **계속**을 클릭하십시오. 내보내기 프로세스가 실패한 경우 인증서를 성공적으로 내보냈음을 나타내거나 오류 정보를 제공하는 메세지가 표시됩니다.

    주: 이 인증서를 사용하여 오브젝트에 서명하려면 이제 오브젝트 서명 어플리케이션에 인증서 할당을 해야 합니다.

V4R5 또는 V4R4 목표 시스템에서 SSL 세션에 개인 인증서 사용

디지털 인증 관리자(DCM)의 *SYSTEM 인증서 저장소에서 어플리케이션이 SSL 세션에 사용하는 인증서를 관리합니다. SSL에 대한 인증서를 관리하기 위해 V4R5 또는 V4R4 목표 시스템에서 DCM을 사용한 적이 없는 경우 이 인증서 저장소는 목표 시스템에 존재하지 않습니다. 로컬 인증 기관(CA) 호스트 시스템에서 작성한 전송된 인증서 저장소 파일에 두 개의 인증서가 포함됩니다. 이 파일은 작성된 서버나 클라이언트 인증서 및 서명에 사용된 개인 로컬 인증 기관(CA) 인증서입니다.

전송된 인증서 저장소 파일을 사용하기 위해 수행해야 하는 타스크는 *SYSTEM 인증서 저장소의 존재 여부에 따라 다릅니다. *SYSTEM 인증서 저장소가 존재하지 않음인 경우 *SYSTEM 인증서 저장소를 작성하는 수단으로 전송된 인증서 파일을 사용할 수 있습니다. 목표 시스템에 *SYSTEM 인증서가 없으면 다음 방법 중 하나로 전송된 인증서 파일을 사용할 수 있습니다.

- 다른 시스템 인증서 저장소로 전송된 파일 사용.
- 기존 *SYSTEM 인증서 저장소로 전송된 파일 가져오기.

*SYSTEM 인증서 저장소가 존재하지 않는 경우

전송된 인증서 저장소 파일을 사용하려는 V4R5 또는 V4R4 시스템에 *SYSTEM 인증서 저장소가 존재하지 않는 경우 다음의 단계를 따르십시오.

1. 로컬 CA의 호스트인 시스템에서 작성한 인증서 저장소 파일(확장자가 .KDB인 하나의 파일과 확장자가 .RDB인 하나의 파일로 두 개의 파일)이 /QIBM/USERDATA/ICSS/CERT/SERVER 디렉토리에 있는지 확인하십시오.
2. 전송된 인증 파일이 /QIBM/USERDATA/ICSS/CERT/SERVER 디렉토리에 있으면 파일 이름을 DEFAULT.KDB 및 DEFAULT.RDB로 변경하십시오. 해당 디렉토리에서 파일 이름을 변경하여 목표 시스템의 *SYSTEM 인증서 저장소를 구성하는 구성요소를 작성합니다. 인증서 저장소 파일에는 이미 많은 공용 인터넷 CA에 대한 인증의 사본이 들어 있습니다. 이 사본들을 작성했을 때 DCM이 이 사본들을 로컬 CA 인증서의 사본과 함께 인증서 저장소 파일에 추가했습니다.

   주의: 목표 시스템이 이미 /QIBM/USERDATA/ICSS/CERT/SERVER 디렉토리에 DEFAULT.KDB 및 DEFAULT.RDB 파일을 포함하는 경우 *SYSTEM 인증서 저장소가 현재 이 목표 시스템에 존재합니다. 결국, 전송된 파일의 이름을 제안대로 변경하지 말아야 합니다. 디폴트 파일을 겹쳐쓰면, DCM, 전송된 인증서 저장소 및 그 내용을 사용할 때 문제가 발생합니다. 그 대신, 고유한 이름을 가지고 있도록 확인하고 전송된 인증서 저장소 파일을 **기타** 인증서 저장소로 사용해야 합니다. 다른 인증서 저장소로 파일을 사용하는 경우 DCM을 사용하여 인증서를 사용해야 하는 어플리케이션을 지정할 수 없습니다.

3. DCM을 시작하십시오. 이제 *SYSTEM 인증서 저장소의 암호를 변경해야 합니다. 암호를 변경하면, 인증서 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장할 수 있습니다.
4. 탐색 프레임에서 *SYSTEM이 드롭 다운 리스트 상자에 인증서 저장소로 표시되는지 확인하고 **시스템 인증**을 선택하여 사용할 수 있는 타스크의 리스트를 표시하십시오. **인증서 저장소 및 암호** 창이 표시됩니다.
5. 적합한 필드에 열고자 하는 인증서 저장소로 *SYSTEM을 입력하고 호스트 시스템에서 로컬 CA를 사용하여 파일을 작성할 때 사용했던 암호를 입력하십시오. 이제 인증서 저장소의 암호를 변경할 수 있습니다.
6. 탐색 프레임의 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오. 암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다.
7. *SYSTEM 인증서 저장소를 다시 연 후에 타스크 리스트에서 **보안 어플리케이션에 대한 작업**을 선택하여 특정 어플리케이션과 연관된 인증서를 관리할 수 있는 페이지를 표시하십시오.
8. 어플리케이션 리스트에서 SSL 세션에 전송된 개인 인증서를 사용해야 하는 어플리케이션을 선택하십시오.
9. **시스템 인증에 대한 작업**을 클릭하고 호스트 시스템의 로컬 CA가 발행한 인증서를 선택하십시오.
10. **새 인증서 지정**을 클릭하여 지정된 어플리케이션이 선택된 인증서를 사용하게 하십시오.

    주: 일부 SSL이 사용 가능한 어플리케이션은 인증에 기초한 클라이언트 확인을 지원합니다. 클라이언트 확인에 인증서를 사용하면 어플리케이션이 제어하는 자원에 대한 액세스를 허용하기 전에 어플리케이션이 유효한 인증서를 수신하게 됩니다. 이러한 지원이 있는 어플리케이션은 특정 CA가 발행한 인증서를 확인하기 전에 CA를 신뢰하도록 설정해야 합니다. **인증 기관(CA)에 대한 작업** 페이지를 사용하여 인증 기관(CA) 인증서가 인증서 저장소의 상태를 신뢰하도록 보장하십시오. 그런 다음 **보안 어플리케이션에 대한 작업** 페이지를 사용하여 인증서를 사용하는 어플리케이션이 그 인증서를 발행한 로컬 인증 기관(CA)을 신뢰하도록 보장하십시오. 그러면, 어플리케이션이 신뢰하는 것으로 지정한 CA에서 이러한 인증만을 유효한 것으로 확인할 수 있습니다. 사용자나 클라이언트 어플리케이션이 신뢰하는 것으로 지정되지 않은 CA의 인증서를 제시하면, 어플리케이션은 유효한 확인의 기준으로 이 인증서를 수락하지 않습니다.

이러한 타스크가 완료되면, V4R5 또는 V4R4 목표 시스템의 어플리케이션이 다른 iSeries의 V5R2 로컬 CA가 발행한 인증서를 사용할 수 있습니다. 그러나, 이러한 어플리케이션에 대해 SSL 사용을 시작하기 전에 SSL을 사용하도록 어플리케이션을 구성해야 합니다.

SSL 연결을 통해 선택된 어플리케이션에 액세스할 수 있으려면 먼저 사용자는 호스트 시스템에서 로컬 인증 기관(CA) 인증서의 사본 확보를 수행하기 위해 DCM을 사용해야 합니다. CA 인증서는 SSL이 사용 가능한 어플리케이션의 요구사항에 따라 사용자의 PC에 있는 파일로 복사시키거나 사용자의 브라우저로 다운로드시켜야 합니다.

***SYSTEM 인증서 저장소가 존재하는 경우 -- 파일을 기타 시스템 인증서 저장소로 사용**

V4R5 또는 V4R4 목표 시스템에 이미 *SYSTEM 인증서 저장소가 있는 경우 인증 파일에 대한 작업 방법을 결정해야 합니다. 전송된 인증서 저장소 파일에는 두 개의 인증 즉, 작성한 서버 또는 클라이언트 인증과 서명하는 데 사용한 개인 로컬 CA 인증서가 들어 있습니다. 전송된 인증 파일을 **기타** 시스템 인증서 저장소로 사용하도록 선택할 수 있습니다. 또는 개인 인증서 및 해당 CA 인증서를 기존의 *SYSTEM 인증서 저장소로 가져오도록 선택할 수 있습니다.

전송된 파일을 **기타** 시스템 인증서 저장소로 사용하도록 선택한 경우 DCM을 사용하여 SSL 세션에 대한 인증서를 사용해야 하는 어플리케이션을 지정할 수 없습니다. 그러나, 이 인증서 저장소에서 인증서 저장소에 대한 디폴트 인증으로 인증서를 지정할 수 있습니다. 기타 시스템 인증서 저장소 옵션을 통해 SSL_Init API를 사용하여 프로그램에 따라 액세스하고 인증서를 사용하여 SSL 세션을 설정하도록 관리자나 다른 사용자들이 작성한 어플리케이션의 인증서를 관리할 수 있습니다. 이 API를 통해 어플리케이션은 특정 인증서가 아닌 인증서 저장소에 대한 디폴트 인증서를 사용할 수 있습니다.

전송된 인증서 저장소 파일을 사용하려는 V4R5 또는 V4R4 시스템에 *SYSTEM 인증서 저장소가 존재하는 경우 다음 단계를 따르십시오.

1. DCM을 시작하십시오. 이제 전송된 인증서 저장소의 암호를 변경해야 합니다. 암호를 변경하면, 인증서 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장할 수 있습니다.
2. 탐색 프레임에서 OTHER이 드롭 다운 리스트 상자에 인증서 저장소로 표시되는지 확인하고 **시스템 인증**을 선택하여 사용할 수 있는 타스크의 리스트를 표시하십시오. **인증서 저장소 및 암호** 창이 표시됩니다.
3. 적합한 필드에 로컬 CA 호스트 시스템으로부터 전송한 인증서 저장소의 완전 규정 경로 및 파일명(.KDB 확장자)을 입력하십시오. 호스트 시스템에서 파일을 작성할 때 사용된 암호를 입력하십시오. 이제 인증서 저장소의 암호를 변경할 수 있습니다.
4. 탐색 프레임의 시스템 인증 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오.

   주: 인증서 저장소의 암호를 변경할 때, 반드시 **자동 로그인** 옵션을 선택하십시오. 이 옵션을 사용하면 새로운 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장합니다.

암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다. 그런 다음, 이 저장소의 인증서를 디폴트 인증으로 사용하도록 지정할 수 있습니다.

5. 탐색 프레임에서 **인증에 대한 작업**을 선택하여 여러 가지 인증서 관리 타스크를 수행할 수 있는 페이지를 표시하십시오.
6. 인증 리스트에서 현재 저장소의 디폴트 인증으로 사용하려는 인증서를 선택하고 **디폴트 설정**을 클릭하십시오.

이제 기타 시스템 인증서 저장소를 작성하고 구성했으므로 SSL_Init API를 사용하는 모든 어플리케이션이 이 저장소 안의 인증서를 사용하여 SSL 세션을 설정할 수 있습니다.

***SYSTEM 인증서 저장소가 존재하는 경우 -- 기존 *SYSTEM 인증서 저장소에 파일 가져오기**

V4R5 또는 V4R4 목표 시스템의 *SYSTEM으로 인증서를 가져오기 전에 먼저 인증서 저장소에서 다른 파일 형식으로 작성한 인증서를 내보내야 합니다. 그런 다음, 새로운 파일로부터 *SYSTEM 인증서 저장소로 인증서를 가져올 수 있습니다. 전송된 인증서 저장소 파일에는 두 개의 인증 즉, 작성한 서버 또는 클라이언트 인증과 서명하는 데 사용한 개인 로컬 CA 인증서가 들어 있습니다. 작성한 서버 또는 클라이언트 인증과 개인 로컬 CA 인증서를 모두 *SYSTEM 인증서 저장소로 가져와야 합니다.

주: V4R5 및 V4R4에 대해 DCM에서 사용할 수 있는 내보내기 기능은 V5R2에서처럼 잘 개발되지 않았으며 목표 시스템을 사용하여 개인 로컬 CA 인증서를 내보내면 문제가 발생할 수 있습니다. 결국, V4R4 또는 V4R5 목표 시스템을 사용하여 내보내지 않고 V5R2 호스트 시스템을 사용하여 로컬 CA 인증서의 *추가* 사본을 별도의 파일로 내보내야 합니다. V5R2 호스트 시스템에서 CA 인증서를 내보낸 후에 로컬 CA 인증서 내보내기 파일을 V4R4 또는 V4R5 목표 시스템으로 수동 전송하고 이 프로시듀어에서 계속 제공되는 단계를 따라 로컬 CA 인증서를 *SYSTEM 인증서 저장소로 가져올 수 있습니다. 로컬 CA 인증서를 사용하여 작성한 개인 인증서를 가져오기 *전*에 이 로컬 CA 인증서를 가져와야 합니다. 개인 인증서를 먼저 가져오면, 로컬 CA 인증서가 인증서 저장소에 없기 때문에 오류가 발생할 수 있습니다.

인증서 저장소 파일에서 인증서를 내보내려면, V4R4 또는 V4R5 목표 시스템에서 다음의 단계를 완료하십시오.

1. DCM을 시작하십시오.
2. 탐색 프레임에서 OTHER이 드롭 다운 리스트 상자에 인증서 저장소로 표시되는지 확인하고 **시스템 인증**을 선택하여 사용할 수 있는 타스크의 리스트를 표시하십시오. **인증서 저장소 및 암호** 창이 표시됩니다.

3. 전송된 인증서 저장소 파일의 완전 규정 경로 및 파일명을 지정하고, 호스트 시스템에서 이 파일을 작성할 때 사용했던 암호를 제공하고, **확인**을 클릭하십시오. 이제 인증서 저장소의 암호를 변경할 수 있습니다.
4. 탐색 프레임의 시스템 인증 타스크 리스트에서 **암호 변경**을 선택하십시오. 인증서 저장소의 암호를 변경하기 위한 양식을 완성하십시오.

   주: 인증서 저장소의 암호를 변경할 때, 반드시 **자동 로그인** 옵션을 선택하십시오. 이 옵션을 사용하면 새로운 저장소에서 모든 DCM 인증서 관리 기능을 사용할 수 있도록 DCM이 새로운 암호를 저장합니다. 암호를 변경하지 않고 자동 로그인 옵션을 선택하는 경우 이 저장소에서 인증서를 내보낼 때 오류가 발생할 수 있습니다.

   암호를 변경한 후에 인증서 저장소 안의 인증에 대해 작업하기 전에 인증서 저장소를 다시 열어야 합니다.
5. 탐색 프레임에서 **인증에 대한 작업**을 선택하여 인증 리스트를 표시하십시오.
6. 리스트에서 개인 인증서를 선택하고 **내보내기**를 클릭하여 인증 내보내기 페이지를 표시하십시오.
7. 인증 내보내기 양식을 완성하십시오.

   주: 파일에 고유한 이름과 확장자를 제공하십시오. 예를 들어, 파일의 이름을 `myfile.exp`로 지정할 수 있습니다. 파일 이름을 지정할 때 `.TXT`, `.KDB`, `.RDB` 또는 `.KYR`의 확장자 중 하나를 사용하면 파일에서 인증서를 가져올 때 오류가 발생할 수 있으므로 파일에 이러한 확장자는 사용하지 마십시오. 이 인증서를 사용할 목표 시스템에 적합한 릴리스 레벨을 선택하십시오. 선택하는 릴리스 레벨은 내보낸 인증의 형식에 영향을 줍니다.
8. **확인**을 클릭하십시오. DCM이 지정된 파일로 인증서를 내보냈음을 나타내는 메세지가 페이지의 맨 위에 표시됩니다.

이 때, 로컬 CA 인증서의 추가 사본을 내보내기 위해 원래의 V5R2 호스트 시스템에서 DCM을 사용하고 V4R4 또는 V4R5 목표 시스템에 수동으로 이를 전송했어야 합니다. 또한 이 목표 시스템에서 DCM을 사용했어야만 개인 서버 또는 클라이언트 인증서를 파일로 내보낼 수 있었습니다. 이제 이러한 인증서를 *SYSTEM 인증서 저장소에 가져올 준비가 되었습니다. 로컬 CA 인증서를 사용하여 작성한 개인 인증서를 가져오기 전에 이 로컬 CA 인증서를 가져와야 합니다. 개인 인증서를 먼저 가져오면, 로컬 CA 인증서가 인증서 저장소에 없기 때문에 오류가 발생할 수 있습니다.

이러한 내보내기 파일에서 인증서를 가져오고 SSL 사용가능 어플리케이션이 이를 사용하도록 지정하려면, V4R4 또는 V4R5 목표 시스템에서 다음의 단계를 완료하십시오.

1. DCM을 시작하십시오.

2. 탐색 프레임에서 *SYSTEM이 드롭 다운 리스트 상자에 인증서 저장소로 표시되는지 확인하고 **시스템 인증**을 선택하여 사용할 수 있는 타스크의 리스트를 표시하십시오. **인증서 저장소 및 암호** 창이 표시됩니다.
3. 열고자 하는 인증서 저장소로 *SYSTEM을 지정하고, 암호를 제공하고, **계속**을 클릭하십시오.
4. 이제 V5R2 호스트 시스템에서 작성한 내보내기 파일에서 로컬 CA 인증서를 가져와야 합니다. 탐색 프레임에서 **CA 인증서 수신**을 선택하여 양식을 표시하십시오.
5. 양식을 완성하고 **확인**을 클릭하여 인증 수신 성공 페이지를 표시하십시오.
   *SYSTEM 인증서 저장소에서 작업하고 있는 경우 이 페이지는 가져온 CA 인증서를 신뢰하도록 설정할 수 있는 어플리케이션의 리스트를 표시합니다.

   주: 일부 SSL이 사용 가능한 어플리케이션은 인증에 기초한 클라이언트 확인을 지원합니다. 클라이언트 확인에 인증서를 사용하면 어플리케이션이 제어하는 자원에 대한 액세스를 허용하기 전에 어플리케이션이 유효한 인증서를 수신하게 됩니다. 이러한 지원이 있는 어플리케이션은 특정 CA가 발행한 인증서를 확인하기 전에 CA를 신뢰하도록 설정해야 합니다. 그러면, 어플리케이션이 신뢰하는 것으로 지정한 CA에서 이러한 인증만을 유효한 것으로 확인할 수 있습니다. 사용자나 클라이언트 어플리케이션이 신뢰하는 것으로 지정되지 않은 CA의 인증서를 제시하면, 어플리케이션은 유효한 확인의 기준으로 이 인증서를 수락하지 않습니다.
6. CA 인증서를 신뢰해야 하는 어플리케이션을 선택하고 **확인**을 클릭하십시오. 어플리케이션 보안 상태 페이지는 신규 인증서를 신뢰하도록 선택한 어플리케이션이 설정되도록 확정하기 위해 표시됩니다.
7. 이제 서버 인증서를 가져올 수 있습니다. 탐색 프레임에서 **인증에 대한 작업**을 선택하여 인증 리스트를 표시하십시오.
8. **가져오기**를 클릭하여 인증서 가져오기 페이지를 표시하십시오.
9. 인증서 가져오기 양식을 완성하고 **확인**을 클릭하여 인증에 대한 작업 페이지로 되돌아가십시오. 내보낸 서버 또는 클라이언트 인증서를 포함하는 파일 이름을 제공하고 이전에 인증서를 내보낼 때 지정한 목표 릴리스와 일치하는 릴리스를 지정해야 합니다. DCM이 현재 저장소에 인증서를 추가했음을 나타내는 메세지가 페이지의 맨 위에 표시됩니다. 또한 가져오기 처리한 인증서가 인증서 리스트에 표시되어야 합니다.
10. 이제 SSL에 대해 가져온 개인 인증서를 사용해야 하는 어플리케이션을 지정해야 합니다. 탐색 프레임에서 **보안 어플리케이션에 대한 작업**을 선택하여 지정된 어플리케이션과 연관된 인증서를 관리할 수 있는 페이지를 표시하십시오.
11. 리스트에서 어플리케이션을 선택하고 **시스템 인증에 대한 작업**을 클릭하여 SSL 세션 설정에 대한 선택된 어플리케이션 사용에 지정할 수 있는 인증의 리스트를 표시하십시오.

12. 리스트에서 인증서를 선택하고 지정된 어플리케이션에 선택된 인증서를 지정하도록 **새 인증서 지정**을 클릭하십시오. 인증 선택을 나타내는 확인 메세지가 페이지의 맨 위에 표시됩니다.

이러한 타스크가 완료되면, V4R4 또는 V4R5 목표 시스템의 어플리케이션이 다른 iSeries의 로컬 CA가 발행한 인증서를 사용할 수 있습니다. 그러나, 이러한 어플리케이션에 대해 SSL 사용을 시작하기 전에 SSL을 사용하도록 어플리케이션을 구성해야 합니다.

SSL 연결을 통해 선택된 어플리케이션에 액세스할 수 있으려면 먼저 사용자는 호스트 시스템에서 로컬 인증 기관(CA) 인증서의 사본 확보를 수행하기 위해 DCM을 사용해야 합니다. CA 인증서은 SSL이 사용 가능한 어플리케이션의 요구사항에 따라 사용자의 PC에 있는 파일로 복사시키거나 사용자의 브라우저로 다운로드시켜야 합니다.

DCM에서 어플리케이션 관리

디지털 인증 관리자(DCM)를 사용하여 SSL이 사용 가능한 어플리케이션 및 오브젝트 서명 어플리케이션에 대한 다양한 관리 타스크들을 수행할 수 있습니다. 예를 들어, 어플리케이션이 보안 소켓층(SSL) 통신 세션에 사용하는 인증서를 관리할 수 있습니다. 수행할 수 있는 어플리케이션 관리 타스크는 어플리케이션의 유형과 작업하고 있는 인증서 저장소에 따라 다양합니다. *SYSTEM 또는 *OBJECTSIGNING 인증서 저장소에서만 어플리케이션을 관리할 수 있습니다.

DCM이 제공하는 대부분의 어플리케이션 관리 타스크들은 이해하기 쉽지만 몇몇 타스크에 익숙하지 않을 수도 있습니다. 이러한 타스크에 대한 자세한 내용은 다음의 주제를 검토하십시오.

어플리케이션 정의 작성은 정의하고 작업할 수 있는 어플리케이션의 유형을 설명합니다.

인증서 지정 관리는 어플리케이션이 SSL 세션을 설정하거나 오브젝트에 서명하는 데 사용하는 인증서를 지정하거나 변경하는 방법을 설명합니다.

CA 신뢰 리스트 정의는 어플리케이션이 인증의 유효성을 검증하고 수락하기 위해 신뢰할 수 있는 인증 기관을 정의할 수 있고 정의해야 하는 시기를 설명합니다.

온라인 도움말에서 다른 DCM 타스크에 대한 정보를 찾을 수 있습니다.

어플리케이션 정의 작성

DCM에서 작업할 수 있는 어플리케이션 정의에는 두 가지 유형이 있는데, SSL을 사용하는 서버 및 클라이언트 어플리케이션에 대한 어플리케이션 정의와 오브젝트 서명에 사용하는 어플리케이션 정의가 있습니다.

DCM을 사용하여 SSL 어플리케이션 정의 및 그 인증에 대해 작업하려면, 어플리케이션은 먼저 DCM을 사용하여 어플리케이션 정의로 등록하여 고유한 어플리케이션 ID를 가져야 합니다. 어플리케이션 개발자는 DCM에서 자동으로 어플리케이션 ID를 작성하

기 위해 API(QSYRGAP, QsyRegisterAppForCertUse)를 사용하여 SSL이 사용 가능한 어플리케이션을 등록합니다. 모든 IBM iSeries SSL이 사용 가능한 어플리케이션은 DCM을 사용하여 등록되므로 이러한 어플리케이션이 SSL 세션을 설정할 수 있도록 어플리케이션에 인증서를 지정하는 데 쉽게 DCM을 사용할 수 있습니다. 또한 직접 작성했거나 구입한 어플리케이션의 경우 어플리케이션 정의를 정의하고 DCM 자체 내에서 이에 대한 어플리케이션 ID를 작성할 수 있습니다. 클라이언트 어플리케이션이나 서버 어플리케이션에 대한 SSL 어플리케이션 정의를 작성하려면 *SYSTEM 인증서 저장소에서 작업하고 있어야 합니다.

인증서를 사용하여 오브젝트에 서명하려면, 먼저 사용할 인증에 대한 어플리케이션을 정의해야 합니다. SSL 어플리케이션 정의와 달리, 오브젝트 서명 어플리케이션은 실제 어플리케이션을 설명하지 않습니다. 그 대신, 작성한 어플리케이션 정의는 서명하려고 하는 오브젝트의 유형이나 그룹을 설명해야 합니다. 오브젝트 서명 어플리케이션 정의를 작성하려면 *OBJECTSIGNING 인증서 저장소에서 작업하고 있어야 합니다.

어플리케이션 정의를 작성하려면, 다음의 단계를 따르십시오.

1. DCM을 시작하십시오.
2. **인증서 저장소 작성**을 클릭하고 적합한 인증서 저장소를 선택하십시오(작성하는 어플리케이션 정의의 유형에 따라 *SYSTEM 인증서 저장소이거나 *OBJECTSIGNING 인증서 저장소임).

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
3. 인증서 저장소 및 암호 페이지가 표시되면, 인증서 저장소를 작성할 때 지정했던 암호를 제공하고 **계속**을 클릭하십시오.
4. 탐색 프레임에서 **어플리케이션 관리**를 선택하여 타스크 리스트를 표시하십시오.
5. 타스크 리스트에서 **어플리케이션 추가**를 선택하여 어플리케이션을 정의하기 위한 양식을 표시하십시오.

   주: *SYSTEM 인증서 저장소에서 작업하고 있는 경우 DCM은 서버 어플리케이션 정의를 추가할 것인지 아니면 클라이언트 어플리케이션 정의를 추가할 것인지를 선택하도록 프롬트를 표시합니다.
6. 이 양식을 완성하고 **추가**를 클릭하십시오. 어플리케이션 정의에 대해 지정할 수 있는 정보는 정의하는 어플리케이션의 유형에 따라 다릅니다. 서버 어플리케이션을 정의하는 경우 어플리케이션이 인증서를 클라이언트 확인에 사용할 수 있으며 클라이언트 확인을 요구해야 하는지를 지정할 수도 있습니다. 어플리케이션이 CA 신뢰 리스트를 사용하여 인증서를 확인하도록 지정할 수도 있습니다.

어플리케이션에 대한 인증서 지정 관리

어플리케이션이 보안 소켓층(SSL) 세션 설정이나 오브젝트 서명과 같은 보안 기능을 수행할 수 있으려면 디지털 인증 관리자(DCM)를 사용하여 어플리케이션에 인증서를 지정해야 합니다. 어플리케이션에 인증서를 지정하거나 어플리케이션에 대한 인증서 지정을 변경하려면, 다음의 단계를 따르십시오.

1. DCM을 시작하십시오.
2. **인증서 저장소 작성**을 클릭하고 적합한 인증서 저장소를 선택하십시오(인증서를 지정받을 어플리케이션의 유형에 따라 *SYSTEM 인증서 저장소이거나 *OBJECTSIGNING 인증서 저장소임).

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
3. 인증서 저장소 및 암호 페이지가 표시되면, 인증서 저장소를 작성할 때 지정했던 암호를 제공하고 **계속**을 클릭하십시오.
4. 탐색 프레임에서 **어플리케이션 관리**를 선택하여 타스크 리스트를 표시하십시오.
5. *SYSTEM 인증서 저장소에 있는 경우 관리할 어플리케이션 유형을 선택하십시오. (적절하게 **서버** 또는 **클라이언트** 어플리케이션을 선택하십시오.)
6. 타스크 리스트에서 **인증서 지정 갱신**을 선택하여 인증서를 지정할 수 있는 어플리케이션의 리스트를 표시하십시오.
7. 리스트에서 어플리케이션을 선택하고 **인증서 지정 갱신**을 클릭하여 어플리케이션에 지정할 수 있는 인증의 리스트를 표시하십시오.
8. 리스트에서 인증서를 선택하고 **새 인증서 지정**을 클릭하십시오. DCM은 어플리케이션에 대한 인증 선택을 확인하기 위한 메세지를 표시합니다.

   주: 클라이언트 확인을 위한 인증 사용을 지원하는 SSL이 사용 가능한 어플리케이션에 인증서를 지정하는 경우 어플리케이션에 대해 CA 신뢰 리스트를 정의해야 합니다. 그러면, 어플리케이션이 신뢰하는 것으로 지정한 CA에서 이러한 인증만을 유효한 것으로 확인할 수 있습니다. 사용자나 클라이언트 어플리케이션이 CA 신뢰 리스트에서 신뢰하는 것으로 지정되지 않은 CA의 인증서를 제시하면, 어플리케이션은 유효한 확인의 기준으로 이 인증서를 수락하지 않습니다.

어플리케이션에 대한 인증서를 변경 또는 제거할 때 어플리케이션이 인증서 지정 변경 시에 실행 중이라면 어플리케이션이 변경을 인식하거나 인식할 수 없습니다. 예를 들어, Client Access Express 서버는 사용자가 변경한 인증 변경사항을 자동으로 적용합니다. 그러나, 이러한 어플리케이션이 인증 변경사항을 적용할 수 있으려면 먼저 텔넷 서버, iSeries용 IBM HTTP Server 또는 기타 어플리케이션을 중단하고 시작해야 합니다.

V5R2부터 인증서를 한번에 여러 어플리케이션에 할당하려고 할 때 인증서 할당 타스크를 사용할 수 있습니다.

어플리케이션에 대한 CA 신뢰 리스트 정의

보안 소켓층(SSL) 세션 중에 클라이언트 확인을 위한 인증 사용을 지원하는 어플리케이션은 인증서를 유효한 신원 증명으로 수락할 것인지의 여부를 판별해야 합니다. 어플리케이션이 인증 확인에 사용하는 기준 중 하나는 어플리케이션이 인증서를 발행한 인증 기관(CA)을 신뢰하는지의 여부입니다.

디지털 인증 관리자(DCM)를 사용하여 인증에 대한 클라이언트 확인을 수행할 때 어플리케이션이 신뢰할 수 있는 CA를 정의할 수 있습니다. 어플리케이션이 신뢰하는 CA는 CA 신뢰 리스트를 통해 관리합니다.

어플리케이션에 대한 CA 신뢰 리스트를 정의할 수 있으려면 먼저 몇 가지 조건이 충족되어야 합니다.

- 어플리케이션이 클라이언트 확인을 위한 인증 사용을 지원해야 합니다.
- 어플리케이션에 대한 정의가 어플리케이션이 CA 신뢰 리스트를 사용하도록 지정해야 합니다.

어플리케이션에 대한 정의가 어플리케이션이 CA 신뢰 리스트를 사용하도록 지정한 경우 어플리케이션이 인증 클라이언트 확인을 성공적으로 수행할 수 있으려면 먼저 이 리스트를 정의해야 합니다. 그러면, 어플리케이션이 신뢰하는 것으로 지정한 CA에서 이러한 인증만을 유효한 것으로 확인할 수 있습니다. 사용자나 클라이언트 어플리케이션이 CA 신뢰 리스트에서 신뢰하는 것으로 지정되지 않은 CA의 인증서를 제시하면, 어플리케이션은 유효한 확인의 기준으로 이 인증서를 수락하지 않습니다.

어플리케이션에 대한 신뢰 리스트에 CA를 추가할 때, 이 CA가 사용 가능한지도 확인해야 합니다.

어플리케이션에 대한 CA 신뢰 리스트를 정의하려면, 다음의 단계를 따르십시오.

1. DCM을 시작하십시오.
2. **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 *SYSTEM을 선택하십시오.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.
3. 인증서 저장소 및 암호 페이지가 표시되면, 인증서 저장소를 작성할 때 지정했던 암호를 제공하고 **계속**을 클릭하십시오.
4. 탐색 프레임에서 **어플리케이션 관리**를 선택하여 타스크 리스트를 표시하십시오.
5. 타스크 리스트에서 **CA 신뢰 리스트 정의**를 선택하십시오.
6. 리스트를 정의하려는 어플리케이션의 유형(서버 또는 클라이언트)을 선택하고 **계속**을 클릭하십시오.
7. 리스트에서 어플리케이션을 선택하고 **계속**을 클릭하여 신뢰 리스트 정의에 사용하는 CA 인증서의 리스트를 표시하십시오.

8. 어플리케이션이 신뢰해야 하는 CA를 선택하고 **확인**을 클릭하십시오. DCM은 신뢰 리스트 선택을 확인하기 위한 메세지를 표시합니다.

   주: 리스트에서 개별 CA들을 선택하거나 어플리케이션이 리스트의 CA를 모두 신뢰하거나 모두 신뢰하지 않도록 지정할 수 있습니다. 또한 신뢰 리스트에 CA 인증서를 추가하기 전에 CA 인증서를 보거나 유효성을 확인할 수 있습니다.

인증서 및 어플리케이션 확인

디지털 인증 관리자(DCM)를 사용하여 각 인증서나 이들을 사용하는 어플리케이션의 유효성을 확인할 수 있습니다. DCM이 검사하는 것들의 리스트는 인증의 유효성을 확인하는지 아니면 어플리케이션의 유효성을 확인하는지에 따라 약간 다릅니다.

어플리케이션 유효성 확인

DCM을 사용하여 어플리케이션 정의의 유효성을 확인하면 인증서를 요구하는 기능을 수행할 때 어플리케이션에 대한 인증 문제를 방지하는 데 도움이 됩니다. 이러한 문제는 어플리케이션이 보안 소켓층(SSL) 세션에 성공적으로 참여하거나 오브젝트에 성공적으로 서명하지 못하도록 방해할 수 있습니다.

어플리케이션의 유효성을 확인할 때, DCM은 어플리케이션에 대한 인증서 지정이 있는지 확인하고 지정된 인증서가 유효한지를 확인합니다. 추가적으로, DCM은 어플리케이션이 인증 기관(CA) 신뢰 리스트를 사용하도록 구성된 경우 신뢰 리스트에 최소한 하나의 CA 인증서가 있는지 확인합니다. 그런 다음, DCM은 어플리케이션 CA 신뢰 리스트의 CA 인증서들이 유효한지 확인합니다. 또한 어플리케이션 정의가 인증서 취소 리스트(CRL) 처리가 발생되며 CA에 대해 정의된 CRL 위치가 있다고 지정하면, DCM은 유효성 확인 프로세스의 일부로 CRL을 검사합니다.

인증 유효성 확인

인증서의 유효성을 확인할 때, DCM은 인증의 진위와 유효성을 확인하기 위해 인증서에 속한 여러 가지 항목들을 확인합니다. 인증서의 유효성을 확인할 경우 보안 통신이나 오브젝트 서명에 인증서를 사용하는 어플리케이션에 있어서 인증서를 사용할 때 문제가 발생할 가능성이 거의 없습니다.

유효성 확인 프로세스의 일부로 DCM은 선택된 인증서가 만기되지 않았는지 검사합니다. 또한 인증서를 발행한 CA에 대해 CRL 위치가 존재하는 경우 DCM은 인증서가 인증서 취소 리스트(CRL)에 취소된 것으로 나열되지 않는지 검사합니다. 그외에 DCM은 발행하는 CA에 대한 CA 인증서가 현재 인증서 저장소에 있으며 CA 인증서를 사용할 수 있으며 신뢰할 수 있는 것인지에 대해 검사합니다. 인증서에 개인 키(예: 서버, 클라이언트 및 오브젝트 서명 인증)가 있는 경우 DCM은 공용-개인 키 쌍이 일치하도록 공용-개인 키 쌍의 유효성도 확인합니다. 다시 말해서, DCM은 공용 키를 사용하여 자료를 암호화한 다음, 이 자료를 개인 키를 사용하여 해독할 수 있도록 합니다.

어플리케이션에 인증서 할당

V5R2부터 새로운 디지털 인증 관리자(DCM)의 향상된 기능을 통해 인증서를 여러 어플리케이션에 빠르고 쉽게 할당할 수 있습니다. *SYSTEM 또는 *OBJECTSIGNING 인증서 저장소에서만 인증서를 여러 어플리케이션으로 할당할 수 있습니다.

하나 이상의 어플리케이션에 대해 인증서를 할당하려면 다음 단계를 따르십시오.

1. DCM을 시작하십시오.

   주: DCM을 사용하는 동안 특정 양식을 완료하는 방법에 대해 알려면, 페이지의 맨 위에 있는 의문 부호(**?**)를 선택하여 온라인 도움말에 액세스하십시오.
2. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열고자 하는 인증서 저장소로 ***SYSTEM**을 선택하십시오.
3. 인증서 저장소의 암호를 입력하고 **계속**을 클릭하십시오.
4. 탐색 프레임이 화면정리된 후에 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
5. 타스크 리스트에서 현재 인증서 저장소의 인증 리스트를 표시하려면 **인증서 할당**을 선택하십시오.
6. 현재 인증서 저장소의 어플리케이션 정의 리스트를 표시하려면 리스트에서 인증서를 선택하고 **어플리케이션에 할당**을 클릭하십시오.
7. 리스트에서 하나 이상의 어플리케이션을 선택하고 **계속**을 클릭하십시오. 문제가 발생한 경우 페이지에 할당 선택의 확인 메세지 또는 오류 메세지가 표시됩니다.

CRL 위치 관리

디지털 인증 관리자(DCM)를 통해 인증 유효성 확인 프로세스의 일부로 사용할 인증 기관(CA)에 대한 인증서 취소 리스트(CRL) 위치 정보를 정의하고 관리할 수 있습니다. DCM이나 CRL 처리를 요구하는 어플리케이션은 CRL을 사용하여 특정 인증서를 발행한 CA가 인증서를 취소하지 않았음을 판별할 수 있습니다. 특정 CA에 대한 CRL 위치를 정의할 때, 클라이언트 확인을 위한 인증 사용을 지원하는 어플리케이션은 CRL에 액세스할 수 있습니다.

클라이언트 확인을 위한 인증 사용을 지원하는 어플리케이션은 CRL 처리를 수행하여 유효한 신원 증명으로 수용한 인증에 대해 보다 엄격한 증명을 보장할 수 있습니다. 어플리케이션이 정의된 CRL을 인증 유효성 확인 프로세스의 일부로 사용하기 전에 DCM 어플리케이션 정의는 어플리케이션이 CRL 처리를 수행하도록 요구해야 합니다.

CRL 작업 방식

DCM을 사용하여 인증서나 어플리케이션의 유효성을 확인할 때, DCM은 디폴트로 유효성 확인 프로세스의 일부로 CRL 처리를 수행합니다. 유효성을 확인할 인증서를 발행한 CA에 대해 정의된 CRL 위치가 없는 경우 DCM은 CRL 검사를 수행할 수 없

습니다. 그러나 DCM은 특정 인증의 인증 기관(CA) 서명이 유효한지, 인증서를 발행한 인증 기관(CA)이 신뢰할 수 있는 CA인지와 같이 인증에 대한 기타 중요한 정보를 확인하려고 할 수 있습니다.

CRL 위치 정의

특정 CA에 대한 CRL 위치를 정의하려면, 다음의 단계를 따르십시오.

1. DCM을 시작하십시오.
2. 탐색 프레임에서 **CRL 위치 관리**를 선택하여 타스크 리스트를 표시하십시오.
3. 타스크 리스트에서 **CRL 위치 추가**를 선택하여 CRL 위치와 DCM 또는 어플리케이션이 이 위치에 액세스하기 위해 사용해야 하는 방법을 설명하는 데 사용할 수 있는 양식을 표시하십시오.
4. 이 양식을 완성하고 **확인**을 클릭하십시오. CRL 위치에 고유 이름을 제공하고, CRL을 호스트하는 LDAP 서버를 식별하고, LDAP 서버에 액세스하는 방법을 설명하는 연결 정보를 제공해야 합니다.

   주: 이 안내 타스크에서 특정 양식을 완성하는 방법에 대해 의문 사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**) 버튼을 선택하여 온라인 도움말에 액세스하십시오.

   이제 특정 인증 기관(CA)과 CRL 위치 정의를 연결시켜야 합니다.
5. 탐색 프레임에서 **인증서 관리**를 선택하여 타스크 리스트를 표시하십시오.
6. 인증 기관(CA) 리스트를 표시하려면 타스크 리스트에서 **CRL 위치 할당 갱신**을 선택하십시오.
7. 작성한 CRL 위치 정의를 할당하려는 리스트에서 인증 기관(CA)을 선택하고 **CRL 위치 할당 갱신**을 클릭하십시오. CRL 위치 리스트가 표시됩니다.
8. 리스트에서 인증 기관(CA)과 연관시키려는 CRL 위치를 선택하고 **할당 갱신**을 클릭하십시오. 페이지의 맨 위에 인증 기관(CA) 인증서에 할당한 CRL 위치를 나타내는 메세지가 표시됩니다.

특정 CA에 대한 CRL의 위치를 정의했으면, DCM 또는 기타 어플리케이션은 CRL 처리를 수행할 때 이를 사용할 수 있습니다. 그러나, CRL 처리가 적용되기 전에 디렉토리 서비스 서버에 적합한 CRL이 포함되어야 합니다. 또한 SSL을 사용하도록 디렉토리 서비스 서버 및 클라이언트 어플리케이션을 둘 다 구성해야 하며 DCM의 어플리케이션에 인증서를 지정해야 합니다.

iSeries 디렉토리 서비스(LDAP) 서버 구성 및 사용에 대해 자세히 알려면, 다음의 Information Center 주제를 검토하십시오.

- 디렉토리 서비스(LDAP)
  이 주제는 iSeries 디렉토리 서비스(LDAP) 서버의 구성 및 사용에 대해 알아야 하는 모든 사항을 알려줍니다.

- LDAP 디렉토리 서버와 함께 보안 소켓층(SSL) 사용
  이 주제는 보안 통신에 SSL을 사용하도록 LDAP 서버를 구성하기 위해 수행해야 하는 작업을 설명합니다.

IBM 4758 Cryptographic Coprocessor에서 인증서 키 저장

iSeries에 IBM 4758-023 PCI Cryptographic Coprocessor가 설치되어 있는 경우 코프로세서를 사용하여 인증서의 개인 키에 보다 안전한 기억장치를 제공할 수 있습니다. 이 코프로세서를 사용하면 서버 인증, 클라이언트 인증 또는 로컬 인증 기관(CA) 인증에 대한 개인 키를 저장할 수 있습니다. 그러나, 사용자 인증서 개인 키는 사용자의 시스템에 저장해야 하기 때문에 이 키를 저장할 때에는 코프로세서를 사용할 수 없습니다. 또한 현재로는 오브젝트 서명 인증서에 대한 개인 키를 저장하는 경우에 코프로세서를 사용할 수 없습니다.

다음의 두 가지 방법 중 하나로 인증서의 개인 키를 저장할 때 코프로세서를 사용할 수 있습니다.
- 자체적으로 코프로세서에서 직접 인증서 개인 키 저장.
- 특수 키 파일에 저장하도록 인증서 개인 키의 암호화에 코프로세서 마스터 키 사용.

인증서 작성 또는 갱신 프로세스의 일부로 이 키 저장 옵션을 선택할 수 있습니다. 또한 코프로세서를 사용하여 인증서의 개인 키를 저장하는 경우 이 키에 대한 코프로세서 장치 할당을 변경할 수 있습니다.

개인 키 저장에 코프로세서를 사용하려면, 디지털 인증 관리자(DCM)를 사용하기 전에 코프로세서가 연결변환되었는지 확인해야 합니다. 그렇지 않으면, DCM은 인증서 작성 또는 갱신 프로세스의 일부로 저장 옵션을 선택할 수 있는 페이지를 제공하지 않습니다.

서버 또는 클라이언트 인증서를 작성하거나 갱신하는 경우 현재 인증에 서명하는 CA의 유형을 선택한 후에 개인 키 저장 옵션을 선택합니다. 로컬 CA를 작성하거나 갱신하는 경우 프로세스에서 첫 번째 단계로 개인 키 저장 옵션을 선택합니다.

코프로세서에서 직접 인증 개인 키 저장

인증서의 개인 키에 대한 액세스와 사용을 보다 강력하게 보호하기 위해 IBM 4758-023 PCI Cryptographic Coprocessor에서 직접 키를 저장하도록 선택할 수 있습니다. 디지털 인증 관리자(DCM)에서 인증서 작성 또는 갱신의 일부로 이 키 저장 옵션을 선택할 수 있습니다.

코프로세서에서 직접 인증서의 개인 키를 저장하려면 **키 저장 위치 선택** 페이지에서 다음의 단계를 따르십시오.
1. 저장 옵션으로 **하드웨어**를 선택하십시오.
2. **계속**을 클릭하십시오. 그러면, **암호 장치 설명 선택** 페이지가 표시됩니다.

3. 장치 리스트에서 인증서의 개인 키 저장에 사용하려는 것을 선택하십시오.
4. **계속**을 클릭하십시오. DCM은 작성하거나 갱신할 인증의 식별 정보와 같이 완료할 타스크에 대한 페이지들을 계속해서 표시합니다.

인증 개인 키의 암호화를 위해 코프로세서 마스터 키 사용

인증서의 개인 키에 대한 액세스와 사용을 보다 강력하게 보호하기 위해 IBM 4758-023 PCI Cryptographic Coprocessor의 마스터 키를 사용하여 개인 키를 암호화하고 특수 키 파일에 이 키를 저장할 수 있습니다. 디지털 인증 관리자(DCM)에서 인증서 작성 또는 갱신의 일부로 이 키 저장 옵션을 선택할 수 있습니다.

이 옵션을 성공적으로 사용하려면 먼저 IBM 4758-023 PCI Cryptographic Coprocessor 구성 웹 인터페이스를 사용하여 적합한 키 저장 파일을 작성해야 합니다. 또한 코프로세서 구성 웹 인터페이스를 사용하여 키 저장 파일을 사용하려는 코프로세서 장치 설명과 연관시켜야 합니다. iSeries 타스크 페이지에서 코프로세서 구성 웹 인터페이스에 액세스할 수 있습니다.

시스템에 둘 이상의 코프로세서 장치가 설치되어 연결변환된 경우 여러 장치들이 인증서의 개인 키를 공유하도록 선택할 수 있습니다. 장치 설명들이 개인 키를 공유하려면 모든 장치들이 동일한 마스터 키를 가지고 있어야 합니다. 동일한 마스터 키를 여러 장치들에 분배하는 프로세스를 *복제*라고 합니다. 장치들이 키를 공유하면 보안 소켓층(SSL) 로드 균형을 사용할 수 있으며 보안 세션의 성능이 향상됩니다.

코프로세서 마스터 키를 사용하여 인증으 개인 키를 암호화하고 이를 특수 키 저장 파일에 저장하려면 **키 저장 위치 선택** 페이지에서 다음의 단계를 따르십시오.
1. 저장 옵션으로 **하드웨어 암호화**를 선택하십시오.
2. **계속**을 클릭하십시오. 그러면, **암호 장치 설명 선택** 페이지가 표시됩니다.
3. 장치 리스트에서 인증서의 개인 키 암호화에 사용하려는 것을 선택하십시오.
4. **계속**을 클릭하십시오. 둘 이상의 코프로세서 장치가 설치되어 연결변환된 경우 **추가 암호 장치 설명 선택** 페이지가 표시됩니다.

   주: 여러 코프로세서 장치들이 사용가능하지 않은 경우 DCM은 작성하거나 갱신할 인증의 식별 정보와 같이 완료할 타스크에 대한 페이지들을 계속해서 표시합니다.
5. 장치 리스트에서 인증서의 개인 키를 공유하려는 하나 이상의 장치 설명들의 이름을 선택하십시오.

   주: 선택한 장치 설명은 이전 페이지에서 선택한 장치와 동일한 마스터 키를 가지고 있어야 합니다. 마스터 키가 여러 장치들에서 동일한지 확인하려면, 4758 Cryptographic Coprocessor 구성 웹 인터페이스에서 마스터 키 확인 타스크를 사용하십시오. iSeries 타스크 페이지에서 코프로세서 구성 웹 인터페이스에 액세스할 수 있습니다.

6. **계속**을 클릭하십시오. DCM은 작성하거나 갱신할 인증의 식별 정보와 같이 완료할 타스크에 대한 페이지들을 계속해서 표시합니다.

PKIX CA에 대한 요구 위치 관리

공용 공개 인프라 구조 X.509(PKIX) 인증 기관(CA)은 공용 키 인프라 구조 구현을 위한 최신 인터넷 x.509 표준에 기초하여 인증서를 발행하는 CA입니다. PKIX 표준은 의견 요청(RFC) 2560에 요약되어 있습니다.

PKIX CA는 인증서를 발행하기 전에 보다 엄격한 식별을 요구합니다. 대개 신청자가 등록 기관(RA)을 통해 신원 증명을 제공하도록 요구합니다. 신청자가 RA가 요구한 신원 증명을 제공한 후에 RA는 신청자의 신원을 보증합니다. RA 또는 신청자는 CA의 설정된 프로시듀어에 따라 보증된 어플리케이션을 연관된 CA에 제출합니다. 이러한 표준은 보다 널리 채택되기 때문에 PKIX를 준수하는 CAs는 보다 널리 사용할 수 있게 됩니다. PKIX를 준수하는 CA를 사용하여 SSL 사용가능 어플리케이션이 사용자에게 제공하는 자원에 대한 엄격한 액세스 제어를 요구하는 보안 필요성이 있는지 조사해야 합니다. 예를 들어, Lotus® Domino™는 공용 PKIX 인증 기관(CA)을 제공합니다.

어플리케이션들이 사용할 인증서를 PKIX CA가 발행하도록 선택한 경우 디지털 인증 관리자(DCM)를 사용하여 이러한 인증서를 관리할 수 있습니다. DCM을 사용하여 PKIX CA에 대한 URL을 구성합니다. 이와 같이 하면 서명된 인증서를 확보하기 위한 옵션으로 PKIX CA를 제공하도록 디지털 인증 관리자(DCM)가 구성됩니다.

DMC를 사용하여 PKIX CA에서 인증서를 관리하려면, 다음의 단계에 따라 CA에 대한 위치를 사용하도록 DCM을 구성해야 합니다.

1. DCM을 시작하십시오.
2. 탐색 프레임에서 **PKIX 요구 위치 관리**를 선택하여 PKIX CA 또는 연관된 RA에 대한 URL을 지정할 수 있는 양식을 표시하십시오.
3. 인증 요구에 사용하려는 PKIX CA의 완전 규정 URL(예: `http://www.thawte.com`)을 입력하고 **추가**를 클릭하십시오. URL을 추가하면 서명된 인증서를 확보하기 위한 옵션으로 PKIX CA를 추가하도록 DCM이 구성됩니다.

PKIX CA 요구 위치를 추가한 후에 DCM은 **인증서 작성** 타스크 사용 시에 인증서를 발행하도록 선택할 수 있는 CA의 유형을 지정하기 위한 옵션으로 PKIX CA를 추가합니다.

오브젝트 서명

오브젝트 서명에 사용할 수 있는 세 가지 방법이 있습니다. 오브젝트 API 서명을 호출하는 프로그램을 기록할 수 있습니다. 오브젝트에 서명할 디지털 인증 관리자(DCM)를 사용할 수 있습니다. 또는 V5R2부터 다른 iSeries 시스템에 분배할 오브젝트를 패키지할 때 iSeries Navigator의 오브젝트에 서명할 중앙 관리 피처를 사용할 수 있습니다.

라이브러리에 저장된 오브젝트를 제외하고는 DCM에서 관리하는 인증서를 사용하여 시스템의 통합 파일 시스템에 저장한 오브젝트에 서명할 수 있습니다. QSYS.LIB 파일 시스템에 저장된 *PGM, *SRVPGM, *MODULE, *SQLPKG 및 *FILE(저장 파일만) 오브젝트에만 서명할 수 있습니다. V5R2에서 새로운 사항은 또한 명령(*CMD) 오브젝트에 서명할 수 있다는 것입니다. 다른 iSeries 서버에 저장된 오브젝트에는 서명할 수 없습니다.

공용 인터넷 인증 기관(CA)에서 구입했거나 DCM에서 개인 로컬 CA를 통해 작성한 인증서를 사용하여 오브젝트에 서명할 수 있습니다. 인증 서명 프로세스는 공용 인증서를 사용하든지 아니면 개인 인증서를 사용하든지 상관없이 동일합니다.

오브젝트 서명 전제조건

DCM(또는 오브젝트 서명 API)을 사용하여 오브젝트에 서명하기 전에 특정 전제조건이 충족되었는지 확인해야 합니다.

- 로컬 CA 작성 프로세스의 일부 또는 공용 인터넷 CA에서 오브젝트 서명 인증서 관리 프로세스의 일부로 *OBJECTSIGNING 인증서 저장소를 작성했어야 합니다.
- *OBJECTSIGNING 인증에는 로컬 CA를 사용하여 작성한 인증서나 공용 인터넷 CA에서 확보한 인증서 중에서 최소한 하나의 인증서가 있어야 합니다.
- 오브젝트 서명에 사용할 오브젝트 서명 어플리케이션 정의 작성을 수행했어야만 합니다.
- 오브젝트 서명에 사용할 계획인 오브젝트 서명 어플리케이션에 인증서 할당을 수행했어야만 합니다.

DCM을 사용한 오브젝트 서명

DCM을 사용하여 하나 이상의 오브젝트에 서명하려면 다음 단계를 수행하십시오.

1. DCM을 시작하십시오.

   주: DCM을 사용하는 동안 특정 양식을 완료하는 방법에 대해 의문사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**)를 선택하여 온라인 도움말에 액세스하십시오.
2. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열려는 인증서 저장소로 ***OBJECTSIGNING**을 선택하십시오.
3. *OBJECTSIGNING 인증서 저장소의 암호를 입력하고 **계속**을 클릭하십시오.
4. 탐색 프레임이 화면정리된 후에 **서명가능한 오브젝트 관리**를 선택하여 타스크 리스트를 표시하십시오.
5. 타스크 리스트에서 **오브젝트 서명**을 선택하여 오브젝트 서명에 사용할 수 있는 어플리케이션 정의 리스트를 표시하십시오.
6. 어플리케이션을 선택하고 **오브젝트 서명**을 클릭하여 서명하려는 오브젝트의 위치를 지정할 수 있는 양식을 보십시오.

주: 선택한 어플리케이션에 지정된 인증서 없는 경우 이 어플리케이션을 사용하여 오브젝트에 서명할 수 없습니다. 먼저 **어플리케이션 관리**에서 **인증서 지정 갱신**을 사용하여 어플리케이션 정의에 인증서를 지정해야 합니다.

7. 제공된 필드에 오브젝트의 완전 규정된 경로 및 파일명이나 서명하려는 오브젝트의 디렉토리를 입력하고 **계속**을 클릭하십시오. 또는 디렉토리 위치를 입력하고 **찾아보기**를 클릭하여 서명할 오브젝트를 선택하기 위해 디렉토리 내용을 보십시오.

   주: 오브젝트명은 슬래시(/)로 시작해야 하며 그렇지 않으면 오류가 발생됩니다. 특정 와일드카드 문자를 사용하여 서명하려는 디렉토리 부분을 설명할 수도 있습니다. 이러한 와일드카드 문자로는 "수에 상관없이 문자"를 지정하는 별표(*****)와 "단일 문자"를 지정하는 의문 부호(**?**)가 있습니다. 예를 들어, 특정 디렉토리의 모든 오브젝트에 서명하려면, `/mydirectory/*`를 입력할 수 있고 특정 라이브러리의 모든 프로그램에 서명하려면, `/QSYS.LIB/QGPL.LIB/*.PGM`을 입력할 수 있습니다. 이러한 와일드카드는 경로명의 마지막 부분에서만 사용할 수 있습니다. 예를 들어, `/mydirectory*/filename`은 오류 메세지를 표시합니다. 찾아보기 기능을 사용하여 라이브러리 리스트나 디레토리 내용을 보려면, **찾아보기**를 클릭하기 전에 경로명의 일부로 와일드카드를 입력해야 합니다.

8. 선택된 오브젝트(들)의 서명에 사용하려는 처리 옵션을 선택하고 **계속**을 클릭하십시오.

   주: 작업 결과를 기다리도록 선택한 경우 결과 파일이 브라우저에 직접 표시됩니다. 현재 작업에 대한 결과는 결과 파일의 끝에 첨부됩니다. 결국, 파일에는 현재 작업의 결과와 함께 이전 작업의 결과가 포함될 수 있습니다. 파일의 날짜 필드를 사용하여 현재 작업에 적용되는 파일의 행을 판별할 수 있습니다. 날짜 필드의 형식은 YYYYMMDD입니다. 파일의 첫 번째 필드는 메세지 ID(오브젝트 처리 중 오류가 발생한 경우)이거나 날짜 필드(작업이 처리된 날짜 표시)일 수 있습니다.

9. 오브젝트 서명 조작에 대한 작업 결과를 저장하는 데 사용할 완전 규정된 경로 및 파일명을 지정하고 **계속**을 클릭하십시오. 또는 디렉토리 위치를 입력하고 **찾아보기**를 클릭하여 작업 결과를 저장할 파일을 선택하기 위해 디렉토리의 내용을 보십시오. 오브젝트에 서명하기 위한 작업이 제출되었음을 나타내는 메세지가 표시됩니다. 작업 결과를 보려면, 작업 기록부에서 작업 **QOBJSGNBAT**를 보십시오.

오브젝트 서명 확인

디지털 인증 관리자(DCM)를 사용하여 오브젝트에 있는 디지털 서명의 진위 여부를 확인할 수 있습니다. 서명을 확인할 때, 오브젝트의 자료가 오브젝트 소유자가 오브젝트에 서명한 이후로 변경되지 않았는지 확인하십시오.

서명 확인 전제조건

DCM을 사용하여 오브젝트에 있는 서명을 확인하기 전에 특정 전제조건이 충족되었는지 확인해야 합니다.

- 서명 확인 인증서를 관리할 *SIGNATUREVERIFICATION 인증서 저장소를 작성했어야 합니다.

  주: 동일한 시스템에서 서명된 오브젝트에 대한 서명을 확인하는 경우에 *OBJECTSIGNING 인증서 저장소 내에서 작업하는 동안 서명 확인을 수행할 수 있습니다. DCM에서 서명을 확인하기 위해 수행하는 단계는 어느 인증서 저장소에서나 동일합니다. 그러나, *OBJECTSIGNING 인증서 저장소 내에서 작업하는 동안 서명 확인을 수행하는 경우에도 *SIGNATUREVERIFICATION 인증서 저장소가 존재해야 하며 오브젝트에 서명한 인증의 사본이 들어 있어야 합니다.

- *SIGNATUREVERIFICATION 인증서 저장소에는 오브젝트에 서명한 인증의 사본이 들어 있어야 합니다.
- *SIGNATUREVERIFICATION 인증서 저장소에는 오브젝트에 서명한 인증서를 발행한 CA 인증서의 사본이 들어 있어야 합니다.

DCM을 사용한 오브젝트 서명 확인

DCM을 사용하여 오브젝트 서명을 확인하려면, 다음의 단계를 따르십시오.

1. DCM을 시작하십시오.

   주: DCM을 사용하는 동안 특정 양식을 완료하는 방법에 대해 의문사항이 있는 경우 페이지의 맨 위에 있는 의문 부호(**?**)를 선택하여 온라인 도움말에 액세스하십시오.
2. 탐색 프레임에서 **인증서 저장소 선택**을 클릭하고 열려는 인증서 저장소로 ***SIGNATUREVERIFICATION**을 선택하십시오.
3. *SIGNATUREVERIFICATION 인증서 저장소의 암호를 입력하고 **계속**을 클릭하십시오.
4. 탐색 프레임이 화면정리된 후에 **서명가능한 오브젝트 관리**를 선택하여 타스크 리스트를 표시하십시오.
5. 타스크 리스트에서 **오브젝트 서명 확인**을 선택하여 서명을 확인하려는 오브젝트의 위치를 지정하십시오.
6. 제공된 필드에 오브젝트의 완전 규정된 경로 및 파일명이나 서명을 확인하려는 오브젝트의 디렉토리를 입력하고 **계속**을 클릭하십시오. 또는 디렉토리 위치를 입력하고 **찾아보기**를 클릭하여 서명을 확인할 오브젝트를 선택하기 위해 디렉토리 내용을 보십시오.

   주: 특정 와일드카드 문자를 사용하여 확인하려는 디렉토리 부분을 설명할 수도 있습니다. 이러한 와일드카드 문자로는 "수에 상관없이 문자"를 지정하는 별표(*****)와 "단일 문자"를 지정하는 의문 부호(**?**)가 있습니다. 예를 들어, 특정 디렉토리의

모든 오브젝트에 서명하려면, /mydirectory/*를 입력할 수 있고 특정 라이브러리의 모든 프로그램에 서명하려면, /QSYS.LIB/QGPL.LIB/*.PGM을 입력할 수 있습니다. 이러한 와일드카드는 경로명의 마지막 부분에서만 사용할 수 있습니다. 예를 들어, /mydirectory*/filename은 오류 메세지를 표시합니다. 찾아보기 기능을 사용하여 라이브러리 리스트나 디레토리 내용을 보려면, **찾아보기**를 클릭하기 전에 경로명의 일부로 와일드카드를 입력해야 합니다.

7. 선택된 오브젝트(들)에 있는 서명을 확인하는 데 사용하려는 처리 옵션을 선택하고 **계속**을 클릭하십시오.

   주: 작업 결과를 기다리도록 선택한 경우 결과 파일이 브라우저에 직접 표시됩니다. 현재 작업에 대한 결과는 결과 파일의 끝에 첨부됩니다. 결국, 파일에는 현재 작업의 결과와 함께 이전 작업의 결과가 포함될 수 있습니다. 파일의 날짜 필드를 사용하여 현재 작업에 적용되는 파일의 행을 판별할 수 있습니다. 날짜 필드의 형식은 YYYYMMDD입니다. 파일의 첫 번째 필드는 메세지 ID(오브젝트 처리 중 오류가 발생한 경우)이거나 날짜 필드(작업이 처리된 날짜 표시)일 수 있습니다.

8. 서명 확인 조작에 대한 작업 결과를 저장하는 데 사용할 완전 규정된 경로 및 파일명을 지정하고 **계속**을 클릭하십시오. 또는 디렉토리 위치를 입력하고 **찾아보기**를 클릭하여 작업 결과를 저장할 파일을 선택하기 위해 디렉토리의 내용을 보십시오. 오브젝트 서명을 확인하기 위한 작업이 제출되었음을 나타내는 메세지가 표시됩니다. 작업 결과를 보려면, 작업 기록부에서 작업 **QOBJSGNBAT**를 보십시오.

DCM을 사용하여 오브젝트에 서명한 인증에 대한 정보도 볼 수 있습니다. 이 정보에서 오브젝트에 대해 작업하기 전에 오브젝트가 신뢰하는 소스로부터 비롯된 것인지를 판별할 수 있습니다.

제 9 장 DCM 문제 해결

다음 페이지를 사용하여 디지털 인증 관리자(DCM)에서 작업하는 중 발생할 수 있는 일부 공통적인 문제를 해결하는 데 도움이 되는 유용한 정보를 찾을 수 있습니다.

문제 및 그 가능한 솔루션에 대한 정보는 다음 페이지를 검토하십시오.

암호 및 일반 문제 해결
발생할 수 있는 공통 DCM 사용자 인터페이스 문제와 이 문제를 정정할 수 있는 방법에 대해 알려면 이 정보를 사용하십시오.

인증서 저장소 및 키 데이터베이스 문제 해결
발생할 수 있는 공통 인증서 저장소 및 키 데이터베이스 문제와 이 문제를 정정할 수 있는 방법에 대해 알려면 이 정보를 사용하십시오.

브라우저 문제 해결
브라우저를 사용하여 DCM에 액세스할 때 발생할 수 있는 공통 문제와 이 문제를 정정할 수 있는 방법에 대해 알려면 이 정보를 사용하십시오.

iSeries 문제 해결 HTTP Server
발생할 수 있는 공통 HTTP Server 문제와 이 문제를 정정할 수 있는 방법에 대해 알려면 이 정보를 사용하십시오.

마이그레이션 오류 및 회복 솔루션
이전 릴리스로부터 DCM을 마이그레이트할 때 발생할 수 있는 공통 문제와 이 문제를 정정할 수 있는 방법에 대해 알려면 이 정보를 사용하십시오.

사용자 인증서 지정에 대한 문제 해결
DCM을 사용하여 사용자 인증서를 등록할 때 발생할 수 있는 공통 문제와 이 문제를 정정할 수 있는 방법에 대해 알려면 이 정보를 사용하십시오.

암호 및 일반 문제 해결

다음 표를 사용하여 디지털 인증 관리자(DCM)에서 작업하는 중 발생할 수 있는 보다 공통적인 일부 암호 및 기타 일반 문제를 해결하는 데 도움이 되는 정보를 찾을 수 있습니다.

문제	가능한 솔루션
DCM에 대한 추가 도움말을 찾을 수 없습니다.	DCM에서, "**?**" 도움말 아이콘을 클릭하십시오. 또한 Information Center 및 외부 인터넷 사이트를 탐색할 수 있습니다.
인증서 저장소를 열려고 시도하면 NET.DATA 오류를 수신합니다.	**인증서 저장소를 선택**할 때, 키보드에서 **Enter** 키를 사용하지 말고 **계속** 버튼을 선택하십시오.
로컬 인증 기관(CA)에 대한 암호와 *SYSTEM 인증서 저장소가 적용되지 않습니다.	암호는 대소문자를 구분합니다. caps Lock 키가 암호를 지정했을 당시와 동일한지 확인하십시오.
인증서 저장소 선택 타스크 사용 시에 실패한 암호를 재설정하려고 시도합니다.	재설정 기능은 DCM이 암호를 저장한 경우에만 작동됩니다. DCM은 인증서 저장소를 작성할 때 자동으로 암호를 저장합니다. 그러나 다른 시스템 인증서 저장소의 암호를 변경하거나 재설정하는 경우 DCM이 암호를 계속 은닉하도록 **자동 로그인** 옵션을 선택해야 합니다.

문제	가능한 솔루션
	또한 하나의 시스템에서 다른 시스템으로 인증서 저장소를 이동하는 경우 새 시스템에서 인증서 저장소의 암호를 변경해야만 DCM이 자동으로 암호를 은닉하는 것을 보장할 수 있습니다. 암호를 변경하려면 새 시스템에서 저장소를 열 때 인증서 저장소 암호의 원래 암호를 제공해야 합니다. 원래 암호로 저장소를 열고 암호를 변경하여 은닉하기 전에는 재설정 암호를 사용할 수 없습니다. 암호를 변경하고 은닉하지 않는 경우 암호가 다양한 기능에 필요할 때 DCM 및 SSL은 이 암호를 자동으로 회복할 수 없습니다. 다른 시스템 인증서 저장소로 사용할 인증서 저장소를 이동하는 경우 암호를 변경할 때 **자동 로그인**옵션을 선택하여 DCM이 이러한 유형의 인증서 저장소에 대해 새 암호를 은닉하는 것을 보장합니다.
	시스템 서비스 툴(SST)의 시스템 보안에 대한 작업 옵션에서 ″Allow new digital certificates″ 속성에 할당된 값을 확인하십시오. 이 속성을 값 2(아니오)로 설정한 경우 인증서 저장소 암호는 재설정할 수 없습니다. STRSST 명령을 사용하고 서비스 툴 사용자 ID 및 암호를 입력하여 이 속성의 값을 보거나 변경할 수 있습니다. 그런 다음 ″시스템 보안에 대한 작업″ 옵션을 선택하십시오. 서비스 툴 사용자 ID는 QSECOFR 사용자 ID일 수 있습니다.
iSeries 시스템에 수신할 CA 인증서의 소스를 찾을 수 없습니다.	일부 CA는 자신의 CA 인증서를 쉽게 사용할 수 없게 합니다. CA로부터 CA 인증서를 얻을 수 없는 경우에는 VAR이 특수하거나 금전적인 CA 배열을 수행했을 수 있으므로 VAR에게 문의하십시오.
*SYSTEM 인증서 저장소를 찾을 수 없습니다.	*SYSTEM 인증의 파일 위치는 `/qibm/userdata/icss/cert/server/default.kdb`이어야 합니다. 해당 인증서 저장소가 없는 경우에는 DCM을 사용하여 인증서 저장소를 작성해야 합니다. **새로운 인증서 저장소 작성** 타스크를 사용하십시오.
DCM으로부터 수신된 오류를 수정한 후에도 계속 오류가 나타납니다.	브라우저 캐시를 지우십시오. 캐시 크기를 0으로 설정하고 브라우저를 종료한 다음 다시 시작하십시오.
인증서를 할당한 후 보안 어플리케이션에 대한 정보가 표시될 때 표시되지 않은 인증서 할당이 표시되지 않는 등의 LDAP 서버 문제가 발생합니다. 이러한 문제는 iSeries Navigator를 사용하여 Netscape Communications 브라우저를 열 때 더욱 자주 발생합니다. 브라우저 캐시의 기본설정이 네트워크 ″Once per session″의 문서에 캐시의 문서를 비교하도록 설정합니다.	디폴트 기본설정을 변경하여 매 시간마다 캐싱을 체크하십시오.
DCM을 사용하여 Entrust와 같은 외부 인증 기관(CA)에서 서명한 인증서를 가져올 때 유효 기간이 당일을 포함하지 않거나 발행자의 유효 기간 내에 있지 않다는 오류 메세지를 수신합니다.	시스템은 일반화된 시간 형식을 유효성 기간에 사용하고 있습니다. 하루 동안 대기한 후 다시 시도하십시오. 또한 iSeries의 UTC 오프셋 값(`dspsysval qutcoffset`)이 올바른지를 확인하십시오. 일광 절약 시간이 표시되는 경우에는 오프셋이 올바르지 않게 설정되어 있을 수 있습니다.
Entrust 인증서를 가져오려고 시도할 때 기본 64 오류를 수신했습니다.	인증서는 PEM 형식과 같은 특정 형식으로 나열됩니다. 브라우저의 복사 기능이 제대로 작동되지 않는 경우 각 행 앞의 공백 간격과 같이 인증에 속하지 않는 추가 자료를 복사할 수 있습니다. 이러한 경우 iSeries에서 이를 사용하려고 시도할 때 인증의 형식이 올바르지 않습니다. 이런 문제를 일으키는 웹 페이지가 일부 있습니다. 다른 웹 페이지는 이러한 문제가 발생하지 않도록 설계됩니다. 붙여넣은 정보의 모양이 동일해야 하므로 원본 인증의 모양을 붙여넣기의 결과와 비교하십시오.

문제	가능한 솔루션
DCM의 V4R3 버전에서 V5R2 버전으로 마이그레이트할 때 마이그레이션은 만기된 시스템 인증서를 수용하지 않습니다.	만료된 시스템 인증서는 사용할 수 없고 *SYSTEM 인증서 저장소에 넣을 수 없습니다. 마이그레이트하기 전에 이전 키 링 파일을 V4R3에서 제거 또는 이름 변경하거나 마이그레이션 실패 인디케이터를 무시하거나 마이그레이션을 다시 시도하십시오.
인증서를 유효성 리스트에 추가하기 위한 샘플 코드를 찾을 수 없습니다.	샘플 코드는 아직 사용할 수 없습니다.

인증서 저장소 및 키 데이터베이스 문제 해결

다음의 표를 사용하여 디지털 인증 관리자(DCM)에서 작업하는 중 발생할 수 있는 보다 공통적인 일부 인증서 저장소 및 키 데이터베이스 문제를 해결하는 데 도움이 되는 정보를 찾을 수 있습니다.

문제	가능한 솔루션
키 데이터베이스를 찾을 수 없거나 유효하지 않은 키 데이터베이스입니다.	암호 및 파일명의 입력 오류가 있는지 검사하십시오. 맨 앞에 슬래시(/)를 포함하는 파일명이 경로에 있어야 합니다.
키 데이터베이스를 작성할 수 없습니다.	파일명이 충돌하는지 검사하십시오. 요구한 파일이 아닌 다른 파일에서 충돌이 발생할 수 있습니다.
해당 시스템은 다른 시스템에서 2진 모드로 전송된 인증 기관(CA) 텍스트 파일을 허용하지 않습니다. V4R3 시스템은 미국 표준 정보 교환 코드(ASCII) 형식으로 전송되는 파일을 허용합니다.	키 링 및 키 데이터베이스는 2진이므로 서로 다릅니다. CA 텍스트 파일의 경우에는 ASCII 모드로 파일 전송 프로토콜(FTP)을 사용해야 하며 확장자가 .kdb, .kyr, .sth, .rdb 등인 파일과 같은 2진 파일의 경우에는 2진 모드로 FTP를 사용해야 합니다.
키 데이터베이스의 암호를 변경할 수 없습니다. 키 데이터베이스에 있는 인증서가 더 이상 유효하지 않습니다.	올바르지 않은 암호가 문제가 아닌지 확인한 후 인증서 저장소에서 유효하지 않은 인증서를 찾아 삭제한 후 암호 변경을 시도하십시오. 인증서 저장소에 만기된 인증서가 있으면 만기된 인증서는 더 이상 유효하지 않습니다. 인증서가 유효하지 않기 때문에, 인증서 저장소에 대해 암호 변경 기능을 사용하더라도 암호가 변경되지 않고 암호화 프로세스가 만료된 인증서의 개인용 키를 암호화하지 못합니다. 이것은 암호 변경을 방해하며 시스템은 인증서 저장소의 훼손을 그 이유 중 하나로 보고할 것입니다. 인증서 저장소에 있는 유효하지 않은(만료된) 인증서를 제거해야 합니다.
인터넷 사용자에 대해 인증서를 사용해야 하므로 유효성 확인 리스트를 사용해야 하지만, DCM은 유효성 확인 리스트의 기능을 제공하지 않습니다.	유효성 리스트를 사용하기 위해 어플리케이션을 기록 중인 비즈니스 상대는 유효성 리스트를 해당 어플리케이션에 연관시키는 코드를 기록해야 합니다. 또한 인증서가 유효성 리스트에 추가될 수 있도록 인터넷 사용자의 신원이 적절하게 확인되는 시기를 판별하는 코드를 기록해야 합니다. QsyAddVldlCertificate API에 대한 Information Center 주제를 검토하십시오. 유효성 리스트를 사용하기 위한 보안 서버 인스턴스 구성에 대한 도움말은 웹마스터 안내서를 참조하십시오.

브라우저 문제 해결

다음의 표를 사용하여 디지털 인증 관리자(DCM)에서 작업하는 중 발생할 수 있는 보다 공통적인 일부 브라우저 관련 문제를 해결하는 데 도움을 줍니다.

문제	가능한 솔루션
Microsoft® Internet Explorer는 새로운 브라우저 세션을 시작할 때까지 다른 인증서를 선택할 수 있도록 허용하지 않습니다.	Internet Explorer에 대해 새로운 브라우저 세션을 시작하십시오.
Internet Explorer는 브라우저의 선택 리스트에 선택할 수 있는 모든 클라이언트/사용자 인증서를 표시하지 않습니다. Internet Explorer는 보안 사이트에서 사용할 수 있는, 신뢰하는 CA에서 발행한 인증만을 표시합니다.	CA는 보안 어플리케이션뿐만 아니라 키 데이터베이스에서도 신뢰되어야 합니다. 사용자 인증서를 브라우저에 저장할 때와 동일한 사용자명을 사용하여 Internet Explorer 브라우저의 PC에 사인 온했는지 확인하십시오. 액세스하는 시스템으로부터 다른 사용자 인증서를 얻으십시오. 시스템 관리자는 사용자 및 시스템 인증에 서명한 CA를 인증서 저장소(키 데이터베이스)가 여전히 신뢰하는지를 확인해야 합니다.
Internet Explorer 5는 CA 인증서를 수신하지만 파일을 열 수 없거나 인증서를 저장한 디스크를 찾을 수 없습니다.	아직 Internet Explorer 브라우저가 신뢰하지 않는 인증에 대한 새로운 브라우저 피처입니다. PC에서 위치를 선택할 수 있습니다.
시스템명 및 시스템 인증서가 일치하지 않음을 알리는 브라우저 경고를 수신했습니다.	일부 브라우저는 시스템명의 대소문자를 서로 다르게 인식합니다. 시스템 인증서가 표시하는 것과 동일한 대소문자를 사용하여 URL을 입력하십시오. 또는 대부분의 사용자가 사용하는 것과 일치하는 대소문자를 사용하여 시스템 인증서를 작성하십시오. 무엇을 수행 중인지를 알 수 없는 경우에는 서버명 또는 시스템명을 그대로 남겨두는 것이 가장 좋습니다. 또한 정의역명 서버가 올바르게 설정되어 있는지를 검사해야 합니다.
HTTP 대신 HTTPS를 사용하여 Internet Explorer를 시작했으며 보안과 비보안의 세션 혼합을 알리는 경로를 수신했습니다.	이 경고를 수락하거나 무시하도록 선택하십시오. Internet Explorer의 추후 릴리스에서는 이 문제를 수정합니다.
Windows®용 Netscape Communicator 4.04가 폴란드어 코드 페이지에서 16진 값 A1과 B1을 B2와 9A로 변환했습니다.	이는 NLS에 영향을 미치는 브라우저 결함입니다. 다른 브라우저를 사용하거나 AIX®용 Netscape Communicator 4.04와 같이 다른 플랫폼에서 이 브라우저와 동일한 버전을 사용하십시오.
사용자 프로파일에서, Netscape Communicator 4.04가 대문자의 사용자 인증서 NLS 문자는 올바로 표시하지만 소문자는 올바로 표시하지 못했습니다.	한 문자로 맞게 입력된 일부 자국어 문자들이 서로 다른 문자로 표시되었습니다. 예를 들어, Netscape Communicator 4.04의 Windows 버전에서, 폴란드어 코드 페이지의 16진 값 A1과 B1이 B2와 9A로 변환되어서 다른 NLS 문자가 표시되었습니다.
브라우저가 CA를 아직도 신뢰할 수 없음을 일반 사용자에게 표시합니다.	DCM을 사용하여 **CA 상태**를 사용가능으로 설정하여 CA를 신뢰할 수 있는 것으로 표시하십시오.
Internet Explorer 요구가 HTTPS 연결을 거부합니다.	이는 브라우저 기능 또는 그 구성에 대한 문제입니다. 자체 서명되었거나 일부 다른 이유로 인해 유효하지 않을 수도 있는 시스템 인증서를 사용 중인 사이트에 연결하지 않도록 브라우저가 선택했습니다.
Netscape Communicator 브라우저 및 서버 제품은 SSL 통신의 사용가능 피처로(특히 확인 피처) VeriSign을 포함하지만 이에 국한되지 않는 회사들로부터 루트 인증서를 채택합니다. 모든 루트 인증서는 정기적으로 만기됩니다. 일부 Netscape 브라우저 및 서버 루트 인증서는 1999년 12월 25일과 1999년 12월 31일 사이에 만기되었습니다. 1999년 12월 14일 당일과 그 전에 이 문제를 수정하지 않은 경우 오류 메세지를 수신하게 됩니다.	이전 브라우저 버전(Netscape Communicator 4.05 이전)에 만기되는 인증서가 있습니다. 브라우저를 현재 Netscape Communicator 버전으로 업그레이드해야 합니다. 브라우저 루트 인증서에 대한 정보는 `http://home.netscape.com/security/` 및 `http://www.verisign.com/server/cus/rootcert/webmaster.html`을 비롯한 많은 사이트에서 구할 수 있습니다. 무상 브라우저 다운로드는 `http://www.netcenter.com`에서 구할 수 있습니다.

iSeries용 HTTP Server 문제 해결

다음의 표를 사용하여 디지털 인증 관리자(DCM)에서 작업하는 중 발생할 수 있는 보다 공통적인 일부 iSeries용 HTTP Server의 문제를 해결하는 데 도움이 되는 정보를 찾을 수 있습니다.

문제	가능한 솔루션
HTTPS(하이퍼텍스트 전송 프로토콜 보안)는 작동되지 않습니다.	SSL 사용을 위해 HTTP Server가 올바로 설정되게 하십시오. V5R1 이상의 버전에서 구성 파일은 HTTP Server의 그래픽 사용자 인터페이스(GUI)를 사용하여 **SSLAppName**을 설정해야 합니다. 또한 구성은 가상 호스트 내부에 **SSLEnable**로 SSL 포트를 사용하는 구성된 가상 호스트가 있어야 합니다. 또한 하나는 SSL용이고 다른 하나는 SSL용이 아닌 두 개의 다른 포트를 지정해주는 두 개의 Listen 지시문이 있습니다. 서버 인스턴스가 작성되고 서버 인증서가 서명되어 있는지를 확인하십시오.
HTTP Server 인스턴스를 보안 어플리케이션으로 등록하는 프로세스에 대한 확인이 필요합니다.	iSeries 시스템에서 HTTP Server의 웹 인터페이스로 이동하여 HTTP Server의 구성을 설정하십시오. 먼저 SSL 작동 가능한 가상 호스트를 정의해야 합니다. 이 작업은 문맥 관리 화면에서 수행됩니다. 가상 호스트는 이전에 Listen 지시문에서 정의한 SSL 포트를 사용하도록 정의해야 합니다. 그런 다음 SSL 일반 설정 화면을 사용해야만 이전에 구성한 가상 호스트에서 SSL을 작동할 수 있습니다. 모든 변경사항을 구성 파일에 적용해야 합니다. 인스턴스를 등록해도 인스턴스가 사용해야 하는 인증서가 자동으로 선택되지 않습니다. 서버 인스턴스를 종료했다가 다시 시작하기 전에 어플리케이션에 특정 인증서를 할당하려면 DCM을 사용해야 합니다.
유효성 리스트 및 선택적 클라이언트 인증서를 위해 HTTP Server를 구성하는 데 문제가 발생했습니다.	인스턴스 설정 옵션은 HTTP Server 웹마스터 안내서를 참조하십시오. 또한 Information Center의 웹 서빙 주제에도 그 내용이 나옵니다.
Netscape Communicator는 다른 인증서를 선택할 수 있기 전에 HTTP Server 코드의 구성 지시문이 만료될 때까지 기다립니다.	브라우저가 계속 처음 인증서를 사용하고 있기 때문에 큰 인증 값은 두 번째 인증서를 등록하기 어렵게 합니다.
QsyAddVldlCertificate API에 대한 입력으로 사용할 수 있도록 브라우저가 X.509 인증서를 HTTP Server에 제시하도록 시도하고 있습니다.	**SSLEnable** 및 **SSLClientAuth ON**을 사용해야만 HTTPS_CLIENT_CERTIFICATE 환경 변수를 로드하는 HTTP Server를 확보할 수 있습니다. Information Center의 OS/400 API 주제에서 이 API를 찾을 수 있습니다. 또한 다음의 유효성 확인 리스트나 인증 관련 API를 볼 수 있습니다. • QsyListVldlCertificates 및 QSYLSTVC • QsyRemoveVldlCertificate 및 QRMVVC • QsyCheckVldlCertificate 및 QSYCHKVC • QsyParseCertificate 및 QSYPARSC 등
HTTP Server가 설치될 때 작성되는 요구 파일을 찾을 수 없습니다. 시스템은 이 파일을 사용하여 디렉토리의 구성 파일에 있는 KEYFILE 지시문에서 발견된 유효한 키 링 파일을 표시합니다.	자세한 내용은 이전 버전에서 DCM으로 마이그레이트를 참조하십시오. HTTP Server의 경우 올바른 파일은 `/qibm/userdata/httpsvr/keyring/keymreq.crt`입니다. LDAP의 경우에 올바른 파일은 `/qibm/userdata/os400/dirsrv/qdirsrv.crt`입니다.
10,000개 이상의 항목이 있는 유효성 확인 리스트에서 인증 리스트를 요구하는 경우 HTTP Server가 리턴하는 데 시간이 너무 오래 걸리거나 시간 종료됩니다.	일정한 기준에 일치하는 인증(만료된 모든 인증 또는 특정 CA의 인증)을 찾아 삭제하는 일괄처리 작업을 작성하십시오.

문제	가능한 솔루션
V4R3 릴리스 위에 V5R2를 설치한 후 인증서 저장소에서 문제를 발견했고 /qibm/userdata/httpsvr/keyring/keymreq.crt 또는 /qibm/usedata/os400/dirsrv/qdirsrv.crt 파일이 현재 존재합니다. 시스템이 키 데이터베이스에 대한 키 링 자동 마이그레이션을 완료할 수 없습니다.	인증서 저장소로 이전 키 링 파일을 지정하고, qicss/qyepmgrt를 호출하여 마이그레이션을 다시 시도하기 전에 키 링 파일에서 유효하지 않은 인증(들)을 찾아서 삭제하십시오. 또는 마이그레이션 활동이 중요한 모든 인증서를 이동시킨 경우 .crt 파일을 무시하거나 삭제하십시오.
HTTP Server는 **SSLEnable** 세트에서 성공적으로 시작하지 않고 오류 메세지 HTP8351이 작업 기록부에 나타납니다. *ADMIN 서버의 오류 로그는 HTTP Server 실패시 SSL 초기화 작업이 107의 리턴 코드 오류로 실패한 오류임을 표시합니다.	오류 107은 인증서가 만기되었음을 의미합니다. 서버 인스턴스가 *ADMIN 서버인 경우 *ADMIN 서버에서 DCM을 사용할 수 있도록 **SSLDisable**을 임시로 설정하십시오. DCM을 사용하여 어플리케이션에 다른 인증서를 할당하십시오(예: 서버 인스턴스가 *ADMIN 서버인 경우 QIBM_HTTP_SERVER_ADMIN).

마이그레이션 오류 및 회복 솔루션

오류 및 오류 회복

다음 인디케이터는 마이그레이션 중에 발생할 수 있는 오류에 대해 경고합니다.

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT

옵션 34 및 5722-DG1 모두를 성공적으로 설치한 후에 이 인디케이터가 표시되면 5722-DG1이 시도한 키 링 마이그레이션이 성공하지 않았음을 의미합니다. 키 링을 *SYSTEM 인증서 저장소로 마이그레이트해야 합니다.

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

34 옵션을 성공적으로 설치한 후 이 인디케이터가 표시되면 LDAP 서버가 시도한 키 링 마이그레이션이 수행되지 않았음을 의미합니다.

표시된 오류뿐만 아니라, 시스템이 표시하지 않은 마이그레이션 오류도 있을 수 있습니다. 예를 들어, 시스템이 *SYSTEM 인증서 저장소로 마이그레이트하는 데 필요한 키 링 파일을 찾을 때, 기존 통합 파일 시스템 자료 파일과의 충돌이 발견될 수도 있습니다. 이러한 경우 설치를 성공적으로 완료했더라도 시스템이 키 링 파일 마이그레이션을 완료할 수 없습니다.

드문 경우지만, 오류가 마이그레이션의 완료를 방해하기 전에 부분적 시스템 인증서 할당을 통해 키 링 파일 마이그레이션을 완료하는 것도 가능합니다. SSLMONE가 ON이면 IBM HTTP Server *ADMIN 인스턴스를 시작할 때 이로 인해 오류가 발생할 수 있습니다. 가능한 설명은 다음과 같습니다.

- 마이그레이트된 키 링 파일의 디폴트 시스템 인증서가 틀리게 설정되었습니다.
- DCM이 해당 파일명에 이미 존재하는 사용자 자료를 보존하기 위해 마이그레이션을 종료하였습니다.
- 예측하지 못한 오류가 마이그레이션 코드에서 발생했습니다.

*ADMIN 인스턴스를 시작하기 전에 *ADMIN 인스턴스에 대해 SSLMOCE를 일시적으로 OFF로 설정하면 SSLMODE를 ON으로 설정하지 않고서도 IBM HTTP Server

를 시작할 수 있습니다. 이것을 사용하여 *ADMIN 인스턴스를 종료하기 전에 DCM으로 인증서 저장소를 조사하여 문제를 해결할 수 있습니다. *ADMIN 인스턴스를 종료한 후에는 SSLMODE를 다시 ON으로 설정한 다음 *ADMIN 인스턴스를 시작하여 SSL을 올바르게 초기화할 수 있습니다.

옵션 34의 마이그레이션 후 DCM이 정상적인 인증서 저장소 사용을 요구하는 동안 오류가 발생할 수 있습니다. 이와 같은 오류는 브라우저에서 발생합니다. 이러한 오류의 예는 다음과 같습니다.

```
데이터베이스 오류
데이터베이스 읽기 오류
데이터베이스 쓰기 오류
데이터베이스 손상
데이터베이스 표 손상
```

또한 /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR 또는 /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR과 동일한 디렉토리에 이름이 default.kdb인 유효한 인증서 저장소가 없는 파일이 시스템에 있을 수 있습니다. 이러한 경우에는 DCM을 사용하여 새로운 인증서를 작성하기 전에 다음의 수동 마이그레이션을 완료해야 합니다.

주: 키 링 파일을 마이그레이트하지 않고 대신 새로운 CA와 시스템 인증서를 작성하도록 선택한 경우 다음의 수동 마이그레이션 프로시듀어를 생략하십시오.

- iSeries용 HTTP Server(5722-DG1)를 설치할 계획인 경우 작업을 계속 진행하기 전에 이것을 설치하십시오.

  주:

  1. 5722-SS1 옵션 34 설치 코드는 옵션 34를 설치한 후에 다시 마이그레이션을 시도하지 않습니다. 단순히 옵션 34를 재설치하더라도 도움이 되지 않습니다.
  2. 적절한 파일이 PUBLIC *EXCLUDE 권한으로 작성된 사용자 자료 디렉토리에 위치해 있습니다. 파일에 대해 올바르게 권한이 부여되도록 하십시오.

- 다음 파일이 있는지 검사하십시오.
  - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

  위의 파일이 있으면, WRKLNK 명령을 사용하여 이름을 변경하고 백업을 작성하십시오.

- *ALLOBJ 권한이 있는 사용자 프로파일로부터, 다음과 같이 명령행에서 프로그램 QICSS/QYEPMGRT를 호출하십시오.

  ```
  CALL QICSS/QYEPMGRT
  ```

  결과가 성공적인 경우 시스템에 다음의 파일이 존재하지 않음을 확인하십시오.
  - /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
  - /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

일반적으로, DCM은 DCM이 사용하는 파일명과 충돌하는 이름을 가진 파일에 저장되는 사용자 자료의 백업 사본을 보유합니다. 한 예로, 다음 파일이 없을 수 있습니다.

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

그러나 다음 파일이 있을 수 있습니다.

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

이 경우 시스템은 .OLD 확장자를 추가하여 이름을 변경하려고 시도합니다. 위의 파일이 이미 존재하면, 시스템은 백업 사본을 작성하지 않습니다. 그 대신, 기존의 .STH 파일을 간단하게 겹쳐씁니다.

기타

파일명 충돌로 인해 CA 및 시스템 인증서 작성을 계속할 수 없는 경우 다음 중 하나가 발생한 것입니다.

- **서로 다른 파일명 충돌** - DCM은 필요할 때 파일을 작성할 수 없더라도 DCM이 작성하는 디렉토리에 있는 사용자 자료를 보호하려고 시도합니다. 이를 해결하려면 모든 충돌하는 파일을 다른 디렉토리로 복사하고 가능한 경우 DCM 기능을 사용하여 해당 파일을 삭제하십시오. DCM을 사용하여 이를 수행할 수 없는 경우 DCM과 충돌되었던 원래의 통합 파일 시스템에서 파일을 수동으로 삭제하십시오. 이동 파일 및 이동 위치를 정확하게 기록해야 합니다. 필요한 경우 사본으로 파일을 회복할 수 있습니다. 다음 파일을 이동시킨 후에는 신규 CA를 작성해야 합니다.

  ```
  /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
  ```

  다음의 파일을 이동시킨 후에 새로운 *SYSTEM 인증서 저장소 및 시스템 인증서를 작성해야 합니다.

```
/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
```

- **전제조건 누락** - 필수 사용권 프로그램(LPP)을 올바로 설치했는지 확인하십시오.
- **코드 문제점** - 서비스 담당자에게 문의하십시오.

사용자 인증서 지정 문제 해결

사용자 인증서 지정 타스크를 사용할 때, 디지털 인증 관리자(DCM)는 인증서를 등록하기 전에 승인할 수 있도록 인증 정보를 표시합니다. DCM이 인증서를 표시할 수 없는 경우 다음 상태 중의 하나에 의해 문제가 야기될 수 있습니다.

1. 브라우저가 서버로 제공하기 위한 인증서를 선택할 것을 요구하지 않았습니다. 이것은 (다른 서버에 액세스하여) 브라우저가 이전 인증서를 캐시하는 경우 발생할 수 있습니다. 브라우저 캐시를 지우고 다시 타스크를 시도하십시오. 사용자가 인증서를 선택하도록 브라우저에서 프롬트할 것입니다.
2. 등록하려는 인증서가 이미 DCM을 사용하여 등록되어 있습니다.
3. 인증서를 발행한 인증 기관이 시스템에 대해 신뢰할 수 있는 루트로서 지정되어 있지 않습니다. 그러므로, 사용자가 제출하는 인증서가 유효하지 않습니다. 사용자의 인증서를 발행한 CA가 올바른 CA인지 판별하려면 시스템 관리자에게 문의하십시오. 올바른 CA이면, 시스템 관리자가 CA 인증서를 *SYSTEM 인증서 저장소로 **가져오기** 해야 할 것입니다. 또는 관리자가 **CA 인증서에 대한 작업** 타스크를 사용하여 문제를 정정하기 위해 시스템에 대해 신뢰할 수 있는 루트로서 CA를 지정해야 할 수 있습니다.
4. 등록할 인증서가 없습니다. 이것이 문제인지를 알기 위해 사용자의 브라우저에서 사용자 인증서를 확인할 수 있습니다.
5. 등록하려는 인증서가 만기되었거나 불완전합니다. 문제를 해결하기 위해서는 인증서를 갱신하거나 인증서를 발행한 CA에 문의하여야 합니다.
6. iSeries용 IBM HTTP Server가 보안 *ADMIN 서버 인스턴스에 대해 SSL 및 클라이언트 인증서를 사용하여 인증 등록을 수행하도록 제대로 설정되지 않았습니다. 앞에 나오는 문제 해결 추가 정보로 해결할 수 없으면 시스템 관리자에게 문제를 알리십시오.

사용자 인증서를 지정하려면, SSL 세션을 사용하여 디지털 인증 관리자(DCM)에 연결해야 합니다. **사용자 인증서 지정** 타스크를 선택할 때 SSL을 사용하지 않으면, DCM은 SSL을 사용해야 함을 나타내는 메세지를 표시합니다. 메세지에 버튼이 들어 있어 SSL을 사용하여 DCM에 연결할 수 있습니다. 버튼이 없이 메세지가 표시된다면, 문제의 시스템 관리자에게 알리십시오. 웹 서버는 SSL 사용에 대한 구성 지시문이 활성화되도록 재시작시킬 필요가 있습니다.

제 10 장 DCM 관련 정보

디지털 인증의 사용이 많이 보급됨에 따라 보다 많은 정보 자원을 사용할 수 있게 되었습니다. 다음은 디지털 인증서와 이를 사용하여 iSeries 보안 정책을 향상시키는 방법에 대해 알 수 있는 기타 자원들의 리스트입니다.

- **VeriSign Help Desk 웹 사이트**
  VeriSign 웹 사이트는 디지털 인증에 대한 포괄적인 라이브러리와 함께 여러 가지 다른 인터넷 보안 주제도 제공합니다.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  이 IBM 레드북은 V5R1 네트워크 보안 확장 기능을 중점적으로 다룹니다. 이 레드북은 iSeries 오브젝트 서명 기능, 디지털 인증 관리자(DCM), SSL의 4758 Cryptographic Coprocessor 지원 등을 사용하는 방법을 포함하는 다양한 주제를 다룹니다.
- **AS/400® Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)**
  이 레드북은 iSeries 서버에서 디지털 인증서를 사용하여 수행할 수 있는 작업을 설명합니다. 인증서를 사용하기 위해 다양한 서버 및 클라이언트를 설정하는 방법을 설명합니다. 또한 사용자 어플리케이션에서 디지털 인증서를 관리하고 사용하기 위해 OS/400 API를 사용하는 방법에 대한 정보와 샘플 코드를 제공합니다.
- **RFC Index Search**
  이 웹 사이트는 의견 요청(RFC)의 탐색 가능한 저장소를 제공합니다. RFC는 SSL, PKIX 및 기타 디지털 인증서의 사용과 관련된 인터넷 프로토콜에 대한 표준을 설명합니다.

Printed in U.S.A