# 중앙에서 관리하는 TLS/SSL 인증서 라이프 싸이클

인증서 관리와 모니터링 서비스로
원활한 프로세스 및 TLS/SSL 인증 기관 통합

ENTRUST
SECURING A WORLD IN MOTION

# 목차

# 비즈니스 및 보안 문제 해결

보안 이벤트나 업계 변화, 규제 준수 요건, 또는 비즈니스 프로세스 개선 및 비용 절감 필요성 등 다양한 이유로, TLS/SSL 인증서를 식별하고 관리하는 것은 조직의 목표를 달성하는 데 필수적인 조건입니다. 다수 웹 서버와 다양한 용도, 때로 여러 위치에 흩어져 있는 사용자들을 위한 디지털 인증서의 구매, 배포, 갱신, 만료를 관리하는 데에는 많은 시간과 비용이 소모될 수 있습니다.

인증서 관리는 종종 역동적이고 복잡한 작업입니다. 사용 중인 인증서 수가 적은 조직의 경우에도 인증서 만료와 공급업체의 규제 준수, 키 사이즈를 추적하는 것은 쉬운 일이 아닙니다. 다수 네트워크와 시스템 및 애플리케이션에 수백 개의 인증서가 배포된 대규모 조직에서는 이러한 프로세스가 극도로 복잡해집니다. 웹 기반 셀프 서비스 인증서 관리, 자동화된 배포 도구, Entrust Certificate Services(ECS)의 핵심 구성 요소인 Discovery 솔루션을 활용하는 경우, 인증서 라이프 싸이클 관리를 간소화하며 효율과 비용 통제를 획기적으로 개선할 수 있습니다. 모든 TLS/SSL 인증서를 단일 라이프 싸이클 관리 플랫폼으로 통합하는 것은 간단한 프로세스가 아닙니다. 그러나 체계적인 이전 계획을 통해 중단 없이 관리할 수 있는 프로세스입니다. 변화에 대비하는 것은 무엇보다 중요합니다.

본 백서는 ECS 및 관련 서비스로 이전하기 위한 청사진을 제공합니다. 백서 내용은 다양한 환경의 고객이 중앙 통제식 TLS/SSL 인증서 관리를 도입하는 데 도움이 되는 실제 경험을 기반으로 합니다.

## 통합 시나리오

- IT 운영 비용과 복잡성을 제거하기 위한 CIO 주도 관리 이니셔티브
- 사전 또는 사후적 규제 준수 및 보안 개선 이니셔티브
- 여러 네트워크 시스템의 통합이 필요한 인수 또는 합병
- 중앙 통제식 감독과 로컬 제어가 필요한 부서별 개편 및 비즈니스 프로세스 재설계 프로젝트
- 물리적 또는 가상의 한 위치에서 다른 위치로 인증서 배포나 이동이 필요한 데이터 센터 병합과 퍼블릭/프라이빗 클라우드 확장

# 벤더를 바꿔야 할까요, 아니면 통합해야 할까요?

벤더를 바꾸거나 통합하는 것은 자원의 낭비이고 비용 효율적이지 않다는 것이 일반적인 인식입니다. TLS/SSL 인증서 관리에 많은 비용과 시간이 소모되는 것은 대개 조직이 다수 벤더와 추적 시스템 및 수동 프로세스를 사용하고 절차와 중앙 통제에 따른 감독에 소홀해서입니다.

적절한 통합으로 이러한 복잡성, 프래그멘테이션, 중복성을 제거한다면 운영 비용은 크게 절감됩니다. 또한 단일 벤더로 구매를 통합하는 경우, 인증서 수량에 따라 대량 주문 할인 혜택을 받을 수 있습니다.

일부(자체 서비스) TLS/SSL 벤더들은 기술적인 이유로 공급업체를 변경하는 것이 어려울 수 있다고 설명합니다. 그 이유는? 새 루트를 설치하는 작업이 어렵고 시간이 많이 걸리며 오류가 발생하기 쉽기 때문입니다. 인증서 유효성 검사 절차(예: 수동으로 교체해야 하는 CRL 및 OCSP 경로)와 관련해서도 동일한 주장을 합니다.

그러나 두 주장 모두 설득력이 없습니다. TLS/SSL 인증서는 표준 기반이고 설치 절차는 벤더에 상관없이 동일하기 때문입니다. 이러한 표준화는 예상치 못한 혼란을 방지하며, 계획된 이전 작업 중에 참작될 수 있습니다.

따라서 '벤더 종속' 우려가 제기될 수도 있겠으나, 실제로는 잘 계획된 마이그레이션 및 통합으로 비용과 시간을 절약할 수 있습니다. 다음 페이지에서는 Entrust Certificate Services 플랫폼으로 이전하기 위한 4단계 프로세스를 간략하게 설명합니다.

**1단계**

# 인증서 인벤토리 생성

기업 및 기관이 확실한 인증서 관리 절차를 확립하는 데 필수적인 첫 번째 단계는 시스템 전반에 배포된 모든 인증서에 관한 최신 정보를 완벽하게 파악하는 것입니다. 인증서 위치가 파악되면 해당 속성을 검사하고 적용 가능한 정책에 따라 평가를 거쳐 담당 기관에 보고할 수 있습니다.

## 모든 소스 고려

이러한 정보의 신뢰할 수 있는 소스는 하나가 아닐 가능성이 높습니다. 따라서 인증서 사용에 관해 완전한 정보를 파악하려면 가능한 모든 소스를 고려하는 것이 최선입니다.

조직의 인벤토리는 다양한 요소를 고려하는 것을 목표로 해야 하며, 이를 통해 포괄적인 시각을 확보함으로써 평가 및 향후 계획에 효과적으로 반영할 수 있습니다.

여기에는 다음 사항이 포함되어야 합니다.

- 현재 내부 PKI와 외부 벤더가 인증서 발급을 위해 사용하고 있는 인증 기관(CA)이 총 몇 개인가?
- 현재 사용 중인 인증서의 수와 TLS/SSL 인증서를 사용하는 서버 및 애플리케이션의 수는 몇 개인가?
- 현재 TLS/SSL 인증서를 사용하는 서버와 애플리케이션의 수는 몇 개인가?
- 이러한 인증서의 만료일은 각각 언제인가?
- TLS/SSL 관리 담당자는 모두 몇 명인가?
- 현재 사용 중인 인증 솔루션이 인증서 검색 기능을 제공하는가? 마이그레이션 이전에 모든 인증서 인벤토리를 파악하고 수집할 수 있는가?

포괄적인 인증서 및 관리자 카탈로그를 개발하려면 다음의 방법과 소스를 고려하시기 바랍니다.

### 인증 기관에서 가져오기

기존 CA의 인증서에 관해 이미 알고 있는 정보를 수집합니다. 알려진 CA에서 가져오기를 통해 모든 인증서의 정확한 인벤토리가 제공될 것이라는 가정은 금물입니다. 이는 단지 하나의 소스이자 출발점에 불과하며, 반드시 인증서 검색으로 보강되어야 합니다.

### CT(Certificate Transparency) 로그에서 가져오기

CT 로그에서 구성된 도메인 목록에 발급된 인증서에 대해 쿼리를 실행하고 해당 인증서를 Entrust Certificate Services로 가져옵니다. 이 방법을 통해, 확인 가능한 환경에 설치되었거나 설치되지 않은 인증서를 찾아낼 수 있습니다.

### 관리자로부터 보고서 가져오기

네트워크 및 시스템 기반 검색에는 많은 시간이 소요될 수 있으며 모든 위치에서 수행하는 것이 불가능할 수 있습니다. 따라서 모든 관리자를 교육하고 참여시키는 것이 중요하며, 관리자들은 이미 파악된 인증서를 정기적으로 보고하고 인벤토리에 추가해야 합니다.

### 네트워크 검색 수행

네트워크 검색을 수행해 HTTPS와 같은 리스닝 포트에 존재하는 인증서를 찾아냅니다. 먼저 네트워크 주소 범위를 수집한 다음, 확인할 포트 목록을 수집합니다. 포트 443부터 확인을 시작할 수 있으나, 일반적으로 인증서는 다수의 포트에 존재합니다.

### 시스템 수준 검색 수행(옵션 기능)

TLS/SSL에서 상호 인증에 사용되는 클라이언트 측 인증서와 같이, 네트워크 포트를 통해 검색되지 않는 인증서가 다수 있습니다. 이러한 인증서를 찾아내려면 일반적으로 로컬에 설치된 스캐너를 사용해 서버 및 클라이언트 시스템에서 파일 시스템 스캔을 수행해야 합니다.

## 확인 및 수집이 필요한 주요 속성

사용 중인 인증서의 수량을 확인하는 것 외에도 다음과 같이 평가 및 마이그레이션 전략 수립에 필요한 정보를 수집하는 것이 필요합니다.

- **인증서 속성**

  주요 인증서 속성은 다음을 포함합니다. 대상 도메인 이름 또는 주소, 인증서가 연결된 도메인, 암호화 키 속성(알고리즘, 사이즈 및 강도 포함), 발급 기관, 인증서 품질, 취소 상태, SAN(Subject Alt Names), 만료일.

- **애플리케이션 및 서버**

  서버는 설치된 인증서가 있는 서버 및 애플리케이션의 위치를 파악하고 유형을 식별합니다. 이러한 정보는 루트 교체 및 로컬 관리 책임에 필요한 단계를 결정하는 데 필요합니다.

- **기존 관리자 및 조직 체계**

  각각의 모든 인증서에 관리 책임자가 배정되어 있습니까? 해당 관리자가 현재 조직에 소속되어 있습니까? 인벤토리 개발 작업을 수행하는 동안 인증서 관련 연락처와 오너의 상관 관계를 설정합니다. 가능한 한 개인이 아닌 그룹을 연락처로 지정해 SPOF(Single Point of Failure)를 방지합니다. 유용한 소스로 CA, 추적 스프레드시트, 구성 관리 데이터베이스(CMDB) 등이 있습니다.

- **규제 미준수 인증서**

  조직의 정책에 따라 다음과 같은 다양한 이유로 인증서의 규제 미준수가 초래될 수 있습니다. 키 강도(예: 1028비트), 해싱 알고리즘(예: SHA-1), 확인 유형(예: OV 또는 DV) 또는 기타 이유. 인벤토리 프로세스 중에 규제 미준수 인증서를 따로 분류하고 플래그를 지정하는 경우, 평가 및 마이그레이션 계획을 더 빠르게 수행할 수 있습니다.

**2단계**

# 평가 수행

## 큰 그림 보기

인벤토리 작업을 진행하는 동안 수집된 정보를 기반으로 프로젝트의 범위를 결정할 수 있습니다. 이러한 정보는 교체할 인증서의 수량과 교체 시기, 단계적으로 철수시킬 벤더의 수, 주요 관리자 연락처를 포함해야 합니다. 기존 인벤토리 외에도 인증서 수와 관리 계획에 영향을 미치게 될 오프라인 또는 온라인 작업을 고려하시기 바랍니다.

신뢰할 수 있는 CA에서 제공하는 검색 도구가 이 단계에서 도움이 될 수 있습니다. 이러한 도구를 사용하면 CT(Certificate Transparency) 로그 및 인증서를 검색해 단일 관리 플랫폼으로 가져오도록 설계된 기타 도구를 통해, 모든 디지털 인증서를 파악하고 수집할 수 있습니다.

## 통합 옵션

일단 '큰 그림'이 확보되면 모든 인증서를 한 번에 교체하거나 단계적 접근 방식을 선택할 수 있습니다. 이때 중요하게 고려해야 할 두 가지는 재정과 운영입니다. 재정은 인증서 비용에 대한 예산 책정 방식과 기존 인증서의 '매몰 비용' 범위를 기반으로 합니다. 운영 측면에서는 1회 작업에 필요한 노력의 정도, 오래된 인증서의 잔여 라이프 싸이클 중 모니터링, 직원이 불량 인증서를 배포할 가능성을 고려해야 합니다.

## 1회 작업으로 확인 및 교체

한 번의 작업으로 단기간 또는 지정된 전환일 내에 Entrust 인증서 외 기타 모든 인증서 사용을 폐지하는 것이 가능합니다. 이를 통해 대량 주문 할인 혜택을 극대화하며, 모든 관리 메뉴를 중앙 통제식으로 가장 빠르게 확인할 수 있습니다. 또한 특정 예산 주기, 프로젝트 또는 부서별 차지백(Charge-back)에 따라 인증서 구매를 조정해야 한다면 모든 인증서를 Entrust로 마이그레이션하도록 선택할 수 있습니다. 필요한 경우 인증서 만료일이 유지 관리 일정과 일치하도록 조정할 수도 있습니다. 어떤 이유로든 인증서를 취소해야 하는 경우에는 해당 인증서를 발급한 CA를 통해 취소해야 합니다. 벤더나 시스템에는 다른 CA로부터 구매한 인증서를 취소할 권한이 없기 때문입니다. 일부 인증서에 기한이 남아 있는 경우에도, 대량 주문 할인과 고객이 인증서 라이선스를 재사용하는 구독 프로그램으로 절감되는 비용은 모든 것을 한 번에 구매할 가치가 있을 만큼 충분히 큽니다.

지금 Entrust 영업팀에 연락 주시면 비용 절감을 극대화하는 프로그램에 관해 자세히 알려드립니다. **HSMinfo@entrust.com**

### 단계적 이전

또는 각 인증서가 만료될 때마다 하나씩 교체하도록 선택할 수도 있습니다. 이러한 방식은 교체 작업에 소요되는 시간을 줄일 수 있으나, 교체하는 동안에도 서비스가 계속 실행되므로 단계적으로 폐기하려는 CA의 갱신을 초래할 가능성이 있습니다.

네트워크 세그먼트가 많은 조직이나 각 부서들이 서로 다른 일정과 자원 또는 예산 제약에 따라 운영되는 조직의 경우, 이러한 방식을 선호할 수 있습니다. 단계적 이전 방식에도 대량 주문 할인이 적용됩니다. Entrust는 두 가지 이전 방식을 모두 최적으로 지원합니다.

### 고려해야 할 기술적 세부 사항

인증서의 올바른 설치 및 성능을 보장하기 위해, 이전 작업 중에 고려해야 할 두 가지 중요한 기술적 세부 사항이 있습니다.

설치 작업의 한 측면은 루트 CA의 유형과 수 및 업데이트가 필요한 중간 루트와 관련됩니다.

다른 한 측면은 인증서 유효성 검사가 브라우저나 애플리케이션에서 수행되는지 확인하는 기능과 관련되며, 이는 인증서 해지 목록(CRL) 또는 온라인 인증서 상태 프로토콜(OCSP) 서버의 유지 관리를 요구합니다.

일부 벤더는 이러한 부분이 어렵거나 부담스럽다고 설명하는 경우가 있습니다. 그러나 TLS/SSL 인증서는 공통 표준(x.509)을 기반으로 하므로, 인증서 체인 구성 요소를 요청 및 설치하고 인증서 유효성 검사를 설정하는 프로세스는 각 벤더의 인증서에 정확히 동일하게 적용됩니다.

또한 Discovery+와 같은 Entrust Certificate Services 플랫폼의 표준 도구를 사용해 최소한의 작업만으로 관리가 가능합니다. 따라서 이러한 요인 중 어느 것도 벤더 교체에 장애가 되지 않으며, 새 인증서가 제대로 설치되었는지 확인하기만 하면 됩니다.

이러한 변경은 조직의 IT 인프라에 영향을 미치고 일부 조직의 경우 새 루트 CA 및 ICA의 설치 기능이나 시기에 영향을 미치는 변경 관리 정책을 보유하므로, 필요에 따라 CMDB 운영에 맞게 조정하는 것이 중요합니다.

### 고려해야 할 워크플로 및 통합

일부 기업은 API 및 기존 시스템과의 통합을 활용하는 자체 요청 프로세스, 액세스 제어 또는 결제 프로세스를 개발한 경우도 있습니다. 이는 업데이트가 필요한 지점으로 식별되어야 하지만, Entrust Certificate Services는 표준 기반 통합(예: HTTPS Post)의 사용을 지원하며 가장 일반적인 ERP 및 CMBD 시스템용 API를 지원하므로 일반적으로 장애가 되지 않습니다.

## Discovery+ 소개

Discovery+는 인증서 서비스 관리 플랫폼에서 모든 디지털 인증서 유형을 찾아내고 관리하는 여러 스캔 및 가져오기 도구를 제공합니다. 이러한 도구 모음은 중앙 대시보드에 외부 인증서 관리를 통합하는 옵션과 함께, 발급 CA에 관계없이 모든 디지털 인증서를 찾아내고 감사하는 기능을 추가합니다.

- Discovery 스캐너
- Certificate Transparency 로그 가져오기
- 수동으로 가져오기
- CAPI(Crypto API) 스캐너

## 통합 시나리오

- IT 운영 비용과 복잡성을 제거하기 위한 CIO 주도 관리 이니셔티브
- 사전 또는 사후적 규제 준수 및 보안 개선 이니셔티브
- 여러 네트워크 시스템의 통합이 필요한 인수 또는 합병
- 중앙 통제식 감독과 로컬 제어가 필요한 부서별 개편 및 비즈니스 프로세스 재설계 프로젝트
- 물리적 또는 가상의 한 위치에서 다른 위치로 인증서 배포나 이동이 필요한 데이터 센터 병합과 퍼블릭/프라이빗 클라우드 확장

3단계

# 갱신 플랜 개발

## 오너 및 역할 할당

마이그레이션 방식을 결정한 다음에는 소유권을 할당하고 절차와 책임을 전달합니다. 인증서 연락처 정보의 유지 관리에 관해 명확한 책임을 정의합니다. 정책 감독(조직의 인증서 관리 권한이 부여된 개인) 외에도 모든 인증서 속성을 다루는 전사적 수준의 정책이 있어야 합니다. 최고 관리자, 관리자 요청자, 승인자 및 조직에 필요한 기타 역할을 정의합니다. 이를 통해 견제와 균형으로 작동하는 관리 프로세스를 쉽게 배치하고, 필요한 제어 및 책임 수준에 맞게 시스템 액세스 권한을 위임할 수 있습니다. 신뢰할 수 있는 보고서를 작성하고 배포할 수 있다면, 정책 위반을 식별하고 해결하는 것은 간단합니다. 중단이 임박한 경우 신속한 해결을 위해 시스템 가용성 유지 관리를 담당하는 책임자에게 경고가 전송됩니다.

## 갱신에 기존 인증서 매핑

인증서 교체 경로를 매핑합니다. 동등한 인증서(예: 유효 기간, 암호화 수준, 유효성 검사 유형 등)로 교체합니까? 아니면 업그레이드 시 인증서 유형을 변경합니까?

## 규제 미준수 인증서

규제 미준수 인증서의 경우, 프라이빗 키를 삭제할 수 있으며 발급 기관에서 이를 취소하도록 요청할 수 있습니다. 승인되지 않은 기관에서 발급한 인증서가 발견된 경우에는 신속하게 시정 조치를 취할 수 있습니다. 마찬가지로 약한 키가 발견된 경우에도 적절한 강도의 키를 신속하게 발행해 대체할 수 있습니다.

## 통합 플랜 문서화 및 전달

가장 중요한 우선 순위는 인증서 관리와 관련해 누가 업무를 담당하고, 책임을 지며, 조치를 취할 권한이 있는지를 명확하게 확인하는 것입니다. 기본 관리 계정이 있는 경우, 발급에서 폐기까지 전체 라이프 싸이클 프로세스를 감독하고 관리 시스템 내에서 이러한 통제를 실행하기 위해 누가 승인된 관리자 역할을 할지 설정해야 합니다.

감독 및 통제 정책에 관한 조직 전반의 관리 프로세스 규정을 문서화하는 작업은 액세스가 필요한 모든 사람이 사용할 수 있는 저장소에서 개발 및 유지 관리가 이루어져야 합니다. 또한 필요한 경우 변경 사항을 알리는 메커니즘도 포함해야 합니다.

등록 및 프로비저닝에 관한 표준 관행은  안정성과 반복성을 최대화하고 보안과 규제 준수를 보장하며 관리자의 업무 부담을 최소화하는 방식으로 수립해야 합니다. 인증서 발급 또는 갱신은 일반적으로 20개 이상의 단계로 진행됩니다. 이러한 단계는 항상 정책에 따라 표준화되고 구현되어야 합니다.

3단계

# Entrust Certificate Services로 통합하기

검증된 Entrust 플랫폼을 사용하는 경우, 다음을 포함해 인증서 작업을 통합하는 데 필요한 모든 주요 기능을 수행할 수 있습니다.

- 기존 인증서 벤더에서 Entrust로의 원활한 통합
- 모든 비 Entrust 인증서 정보를 관리 포털로 가져오기 및 경고 플래그 지정
- 조치 실행을 보장하는 에스컬레이션 경로로 만료 라우팅 할당
- 관리 그룹 및 위치에 할당
- 인증서 관리 및 모니터링을 위한 맞춤형 워크플로 설정

### Discovery+ (인벤토리 확인 및 수집)

Discovery+는 안전한 환경에 즉시 배포할 수 있으며, 별도의 프로젝트 리소스 보안, 하드웨어 구매 또는 설치 작업이 필요하지 않습니다.

- 모든 소스에서 디지털 인증서를 찾아내고 자동으로 가져옵니다.
- 다른 CA에서 발급한 디지털 인증서와 내부 PKI에서 발급한 인증서를 관리합니다.
- 비용 효율적인 비즈니스 모델로, 외국 인증서에 대한 관리 라이선스만 필요합니다.
- 모범 사례에 기반해 알림 및 경고, 만료, 정책, 보고, 엔드포인트 규제 준수 테스트를 위한 단일 대시보드의 보안을 강화하며, 사용자 지정 가능한 필드로 추가 데이터를 추적하는 기능을 제공합니다.
- 단일 통합 플랫폼에서 인증서 관리를 간소화합니다.

Entrust Discovery Scanner는 모든 Microsoft® Windows® 시스템에 설치 가능하며, 정의된 네트워크 세그먼트의 식별된 IP 주소 범위에서 발급 기관(예: 상용 CA 또는 내부 PKI)에 관계없이 모든 인증서를 찾아낼 수 있습니다.

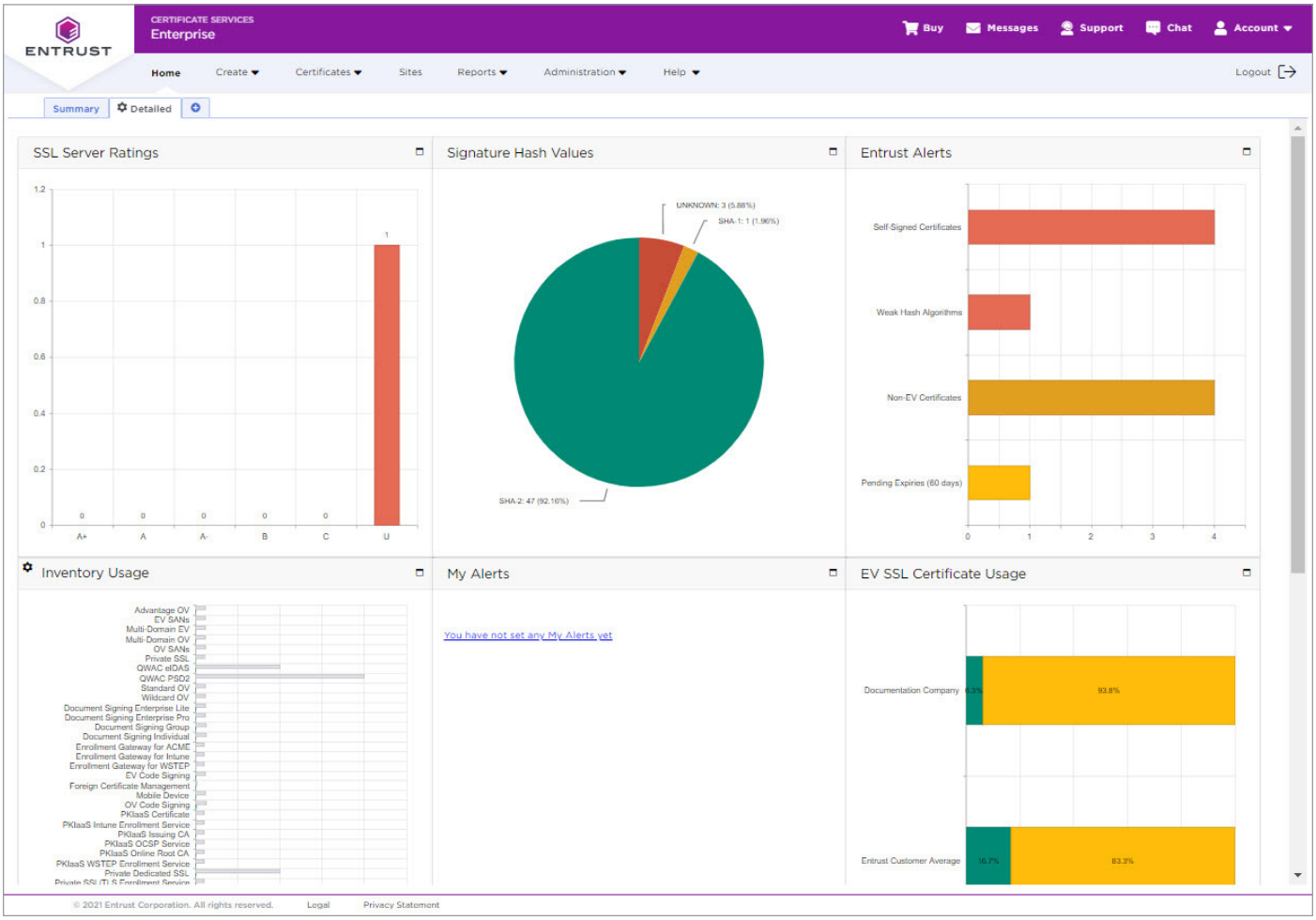



표1: ECS Discovery+ 보고서

### 도메인 및 회사명 검증

온디맨드 가용성 및 발급 기능을 제공하기 위해, Entrust는 모든 조직의 회사명과 자회사를 검증합니다.

인벤토리 및 향후 요건에 따라, 사전 검증을 위해 회사명 및 자회사와 함께 조직에서 관리하는 도메인 목록을 Entrust에 제공할 수 있습니다. Entrust는 즉각적인 인증서 발급이 가능하도록 도메인 및 회사명을 검증합니다.

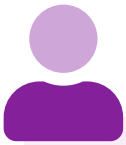
### 관리자 설정 및 위임

기업 및 기관은 Entrust에 사용자 및 역할 목록을 제공할 수 있습니다. 회사 계정 관리자는 지정된 회사 승인 담당자의 승인을 받아야 하며, 다양한 사용자 역할을 할당할 수 있습니다(표2 참고).

- 최고 관리자
- 하위 관리자
- 요청자
- 읽기 전용
- '서명자' 사용자
- REST API 사용자

**최고 관리자**

모든 조치 | 모든 데이터



**요청자**
웹 양식을 통해 인증서를 요청할 수 있는 비시스템 사용자

클라이언트/조직 1

**하위 관리자**
보기, 생성, 승인, 재사용/취소, 보고
데이터 서브 세트에 한함

**읽기 전용**
인증서 보기/도메인 보기/ 클라이언트 요청 인증서/도메인
데이터 서브 세트에 한함

클라이언트/조직 2

**하위 관리자**
보기, 생성, 승인, 재사용/취소, 보고
데이터 서브 세트에 한함

**읽기 전용**
인증서 보기/도메인 보기/ 클라이언트 요청 인증서/도메인
데이터 서브 세트에 한함

**표2: 샘플 구성**

### 인증서 관리 워크플로 정의

현재 보유하고 있는 절차가 있는 경우, 그 절차에 따라 인증서 요청/승인 및 취소/승인 프로세스를 정의하는 인증서 라이프 싸이클 관리 워크플로를 정의합니다.

이미 워크플로가 확립되어 있는 경우, 기존의 워크플로를 모방하거나 필요에 따라 세분화하거나 유연하게 조정합니다. 또는 새로운 워크플로를 처음부터 구축할 수 있습니다.

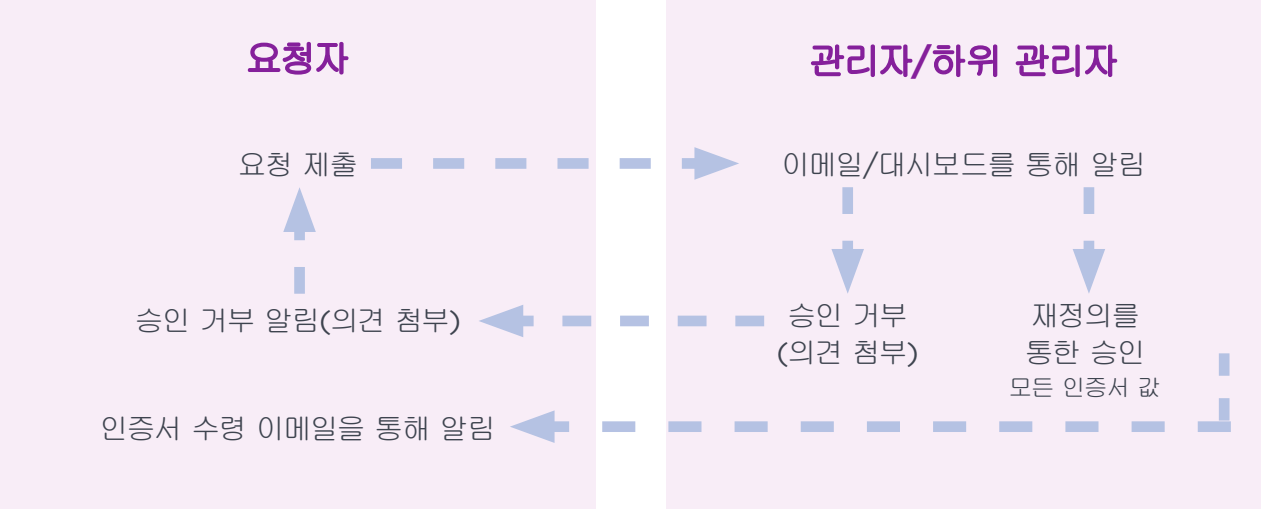



**표3: 샘플 인증서 관리 워크플로**

### 만료 시 Entrust로 인증서 갱신

일회성 업데이트를 수행하든, 단계적 방식을 추진하든, 중앙 통제식 플랫폼을 사용해 다른 벤더의 만료 인증서 갱신을 관리할 수 있습니다.

Entrust 인증서 서비스를 사용하는 경우, 이러한 인증서가 만료될 때 알림이 전송됩니다. 만료 알림을 받으면 Entrust로 인증서를 갱신하고 정책에 따라 이전 인증서를 폐기하시기 바랍니다.

앞서 언급한 바와 같이, TLS/SSL 인증서는 공통 표준(x.509)을 기반으로 하므로, 인증서 체인 구성 요소를 요청하고 설치하는 프로세스는 각 벤더의 인증서에 정확히 동일하게 적용됩니다.

Certificate Services는 설치 확인 도구를 제공해 인증서의 적절한 구성과 간편하고 원활한 사용을 지원합니다.

### 지속적인 검색 및 모니터링 활성화

악성 인증서가 배포될 수 있는 위험은 지속적으로 존재합니다. 누군가가 대역 외 테스트 또는 개발 환경에서 합법적으로 인증서를 조달할 수도 있고, 외부 벤더가 인증서를 배포하거나 악의적인 행위자가 자신의 이익을 위해 인증서를 설치할 수도 있습니다.

프로세스의 무결성을 보장하고 중단 및 보안 위험을 방지하기 위해서는 시스템 환경을 지속적으로 모니터링하고 검사해야 합니다. 또한 규제 및 기타 정책에 따라 현재 관행을 검토해야 합니다.

## 결론

위의 권장 사항 및 절차에 따라 많은 Entrust 고객이 원활한 마이그레이션 작업을 완료했습니다. 이 방식을 통해 TLS/SSL 인증서 관리의 비용과 복잡성을 대폭 줄일 수 있습니다.

TLS/SSL 서비스 플랫폼에 포함된 다수 가이드와 자가 진단 모듈 외에도, 수상 이력을 보유한 Entrust 고객 지원팀이 이전 작업에 필요한 지원을 제공합니다.

### 지금 바로 이전하세요

질문이 있으신가요? 지금 Entrust TLS/SSL 인증서 전문가에게 문의하세요.

02-2088-4691 | HSMinfo@entrust.com으로 연락 주시면 전체 과정을 안내해 드립니다. 지금 시작하세요.

# 마이그레이션 체크리스트

| 조치 | 완료 여부 | 날짜 | Entrust | 고객 |
|---|---|---|---|---|
| ECS 계정 등록 | | | | ✓ |
| 제품 인벤토리 추가 | | | | ✓ |
| 도메인 목록 제공 | | | | ✓ |
| 회사명 목록 제공 | | | | ✓ |
| 도메인 검증 | | | ✓ | |
| 회사명 검증 | | | ✓ | |
| 관리자 및 역할 목록 제공 | | | | ✓ |
| 관리자 검증 | | | ✓ | |
| 위임 설정 | | | ✓ | ✓ |
| 인증서 요청 및 승인을 위한 맞춤형 워크플로 설정 | | | ✓ | ✓ |

자세한 정보

**02-2088-4691**
**HSMinfo@entrust.com**
**entrust.com/ko**

## ENTRUST CORPORATION 소개

Entrust는 안전한 디지털 세상을 위해 신뢰할 수 있는 신원 인증과 결제 및 데이터 보안을 구현합니다. 국경 간 이동과 구매 활동, 전자정부 서비스 접속, 회사 네트워크 로그인까지, 오늘날 원활하고 안전한 경험에 대한 요구는 그 어느 때보다 높아졌습니다. Entrust는 이러한 모든 상호작용의 중심에서 탁월한 범용성을 갖춘 디지털 보안 및 자격 증명 발급 솔루션을 제공하며, 150개 이상의 국가에서 2,500명 이상의 직원과 글로벌 파트너 네트워크 및 고객을 보유하고 있습니다. 전 세계 가장 신뢰받는 여러 기관이 Entrust를 신뢰하는 것은 당연한 결과입니다.

**자세한 정보:**
**entrust.com/ko**


SL21Q4-establish-your-blueprint-for-centralized-ssl-certificate-lifecycle-management-wp

ENTRUST

대한민국 서울특별시 강남구 삼성동 159-1
KWTC 트레이드타워 2503호 135-729
전화: 02-2088-4691
**HSMinfo@entrust.com**