

디지털 신뢰와 MATTER 및 홈 기기 연결성을 위한

“DIGICERT® ONE”

나정주 지사장

Country Manager for Korea

James.nah@digicert.com

digicert®



디지털 신뢰와 적용 사례

연결된 세상의 기반이 되는 디지털 신뢰



비즈니스 중단의 위험을 감소시키는 디지털 신뢰

디지털 신뢰를 전략적 필수 요소로 설정하고 이를 구축하는 데 힘을 쏟는 기업의 경우 이에 따른 이점이 분명하게 드러나고 있습니다. **가동 시간의 안정화, 데이터 손상에 대한 위험 감소 및 사용자의 신뢰 향상** 등이 바로 그 예입니다.

- 제니퍼 글렌(Jennifer Glenn), IDC 보안 및 신뢰 그룹 연구 이사

1,100만
달러(USD)

예기치 않은 인증서
중단으로 인해 발생한
경제적 손실

1,400만
달러(USD)

실패한 감사/규정 준수에
따른 비용

940만
달러(USD)

미국의 데이터 유출 사례
건당 비용
(전 세계적으로 440만
달러(USD))

47%

신뢰를 상실하여
공급업체를 변경한
소비자의 비율

공격 표면을 보호하고 민첩성을 향상하는 디지털 신뢰

20%

중대한 유출
사례의
증가율

3X

IoT 기기의
증가

93%

해커의 공격으로 네트워크 유출이
발생할 수 있는 기업의 비율

65%

소프트웨어 공급망 공격에 따른
피해를 경험하는 기업의 비율

75%

핵심 인프라 운영을 담당하는 기기
중 심각한 취약점을 보유한 기기의
비율

새로운 전략적 필수 요소로 떠오르는 디지털 신뢰

IT 요구 사항이 증가하면서 늘어나는 중앙 집중식 디지털 신뢰 이니셔티브

위험

복잡성

민첩성

공격 표면

인프라스트럭처, 데브옵스

- 유효기간 단축
- 클라우드를 통한 민첩한 배포

신원 및 액세스 관리

- 제로 트러스트 정책
- 원격 작업

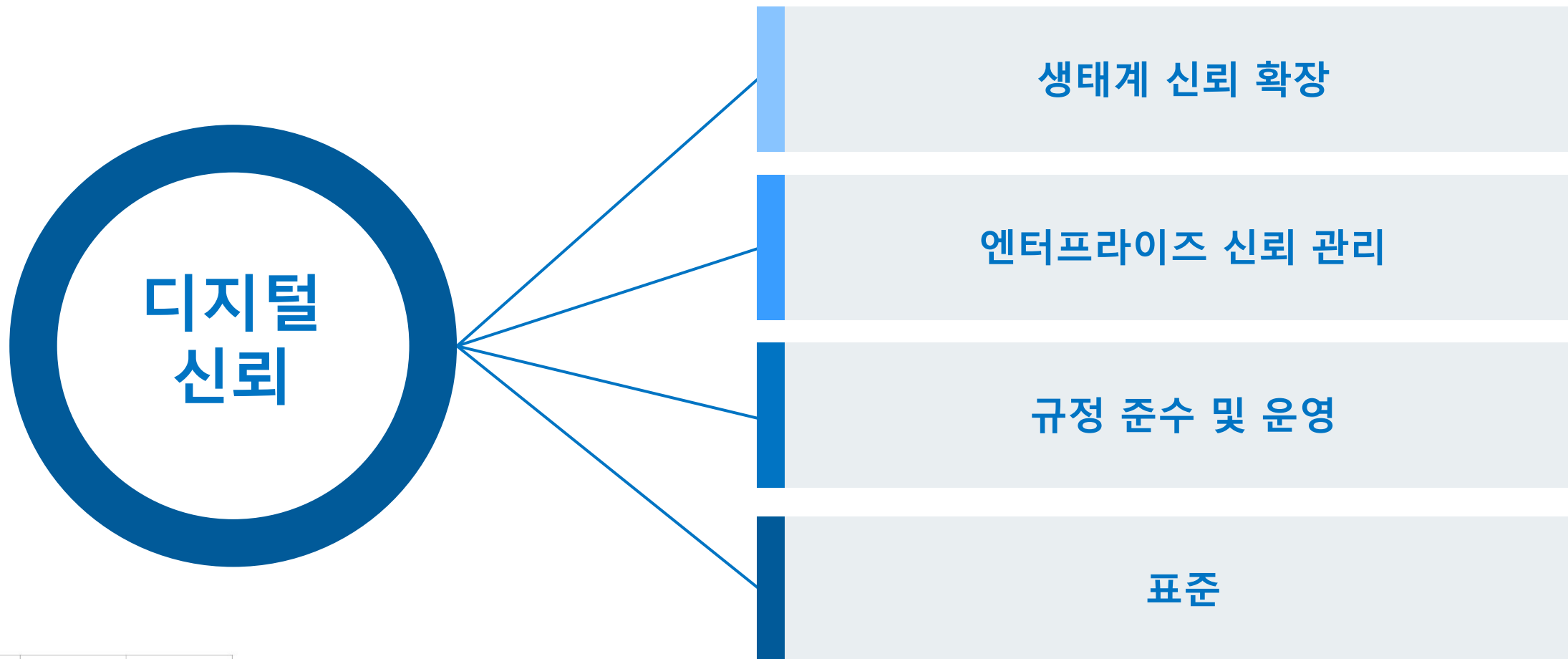
보안 운영

- 위험 증가
- 표준의 변경

IoT, 운영 기술

- 연결된 IoT 장치
- 인더스트리 4.0

디지털 신뢰의 구성 요소



디지털 신뢰의 표준을 구축한 DIGICERT

신뢰 분야의 표준 구축을 위한 투자

- 기술과 업계 표준을 선도
- 연간 25건 이상의 감사



전 세계적 범위, 현지에 적용된 서비스

- 180개 국가에 고객 보유
- 24시간 연중무휴, 세계 최고 수준의 지원



매터(MATTER): IOT 표준의 등장



- DigiCert, Matter 표준을 정립하는 과정에 크게 기여
- DigiCert, 최초로 Root CA 승인을 받은 기업
- DigiCert® IoT Trust Manager는 수백만 개의 인증서로 확장 가능
- 실리콘 임베딩부터 OTA 업데이트까지 모두 가능


Forbes

CES 2023: Matter — Unlocking The Smart Home

Bill Curtis Contributor
Moor Insights and Strategy Contributor Group © [Follow](#)

1 Jan 27, 2023, 10:47am EST

 Listen to article 13 minutes 

 **matter**

Matter MATTER

Every year, after recovering from CES, I take a step back and evaluate the most influential IoT technology trends. This year's

양자 컴퓨팅 시대의 도래

- NIST와의 협업
- PQC(Post Quantum Cryptography) 인증서
- DigiCert® Trust Lifecycle Manager가 제공하는 민첩한 암호화



실질적인 혁신을 주도하는 디지털 신뢰

정부 선거 보안

선거 관리 인력의 신원과 선거
결과의 조작을 방지하는 동시에
빠른 결과 전달

소매 데이터 기반 운영

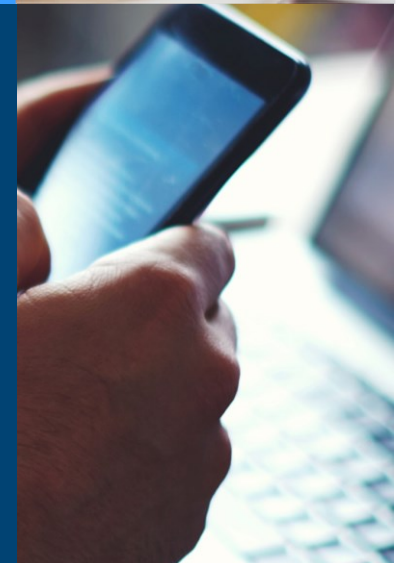
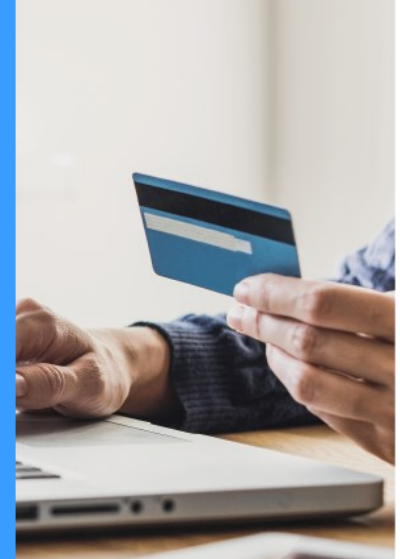
네트워크에 연결된 기기와 기기 운용
및 관리 분석을 위한 원격 측정 부문에
보안 제공

의료 환자 치료 부문의 개선

폐쇄 루프가 적용된 포도당
수치 관리 및 인슐린 전달
시스템에 보안 제공

금융 계좌의 증가

대면 신원 확인을 통한 계좌
생성을 대체하는 안전한
디지털 온보딩



디지털 신뢰를 위한 플랫폼

digicert® ONE

기업 신뢰



Public Trust
(CertCentral)

Private Trust

CLM 및 PKI 서비스
(Trust Lifecycle Manager)

기기 신뢰

Embedded Trust
Manager

IoT Trust Manager

소프트웨어 신뢰

Software Trust
Manager

콘텐츠 신뢰

Document
Trust Manager

DNS 신뢰

DNS Trust
Manager

Performance
Monitoring

계정 서비스 - 역할, 그룹, 사용자, 정책

유효성 검사 서비스 - 조직, 도메인, 개인 ID

인증서 및 등록 기관 서비스 - 인증서 발급

플랫폼 서비스 - Kubernetes, Docker, 인증/허가, 공유 서비스

포괄적 디지털 신뢰 구조

자산 보안



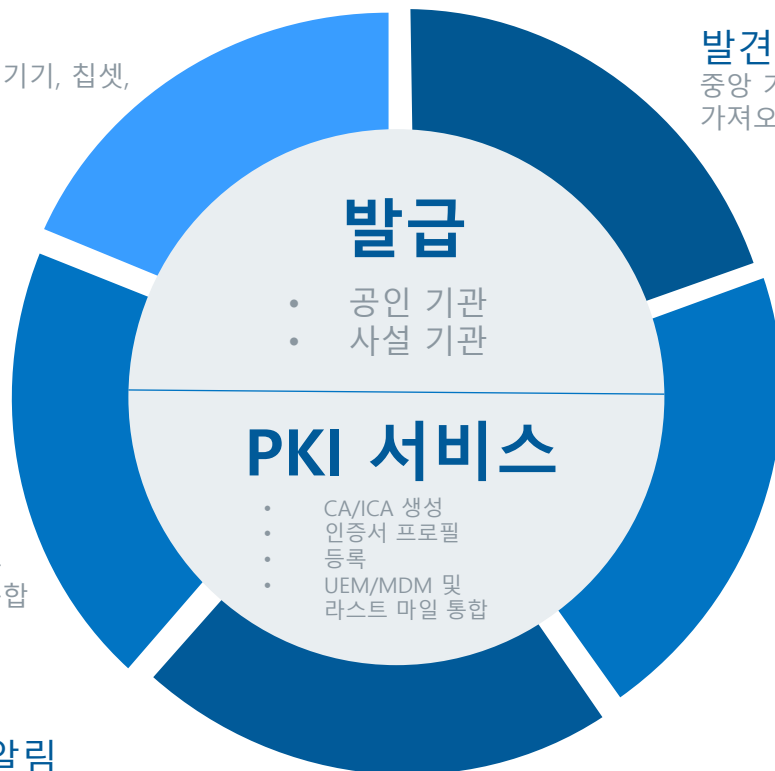
통합
CA, IT, 서버, 기기, 칩셋,
MDM/UEM

자동화
설치, 갱신
제로 터치 등록
라스트 마일 통합

알림
임계값, 에스컬레이션 경로,
에스컬레이션 방법

발견
중앙 기록부
가져오기, 스캔

관리
대시보드
그룹, 정책
필요한 조치



생태계 보안

기기 신뢰

기기 ID 관리 및 기기
운영 보안

소프트웨어 신뢰

코드 서명을 위한
보안키 보호 및
액세스 컨트롤

콘텐츠 신뢰

신뢰할 수 있는
eSignature 및
eSeal을 문서 및
콘텐츠에 적용

DNS 신뢰

트래픽 최적화 및
모니터링을 제공하는
검증된 DNS

호스팅 • 클라우드 • 온프레미스 • 하이브리드

DIGICERT 디지털 신뢰 생태계

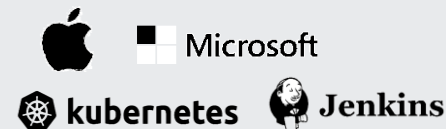
사용자



서버



데브옵스



CA



digicert® ONE

클라이언트

프로토콜

API

게이트웨이

네이티브

애플리케이션



기기



문서



IT 시스템



디지털 신뢰를 선도하는 DIGICERT



비즈니스 중단
위험 감소



공격 표면 보호
및 민첩성 향상



실제 환경을 개선하는
디지털 혁신 추진

전 세계 다양한 업계 리더의 신뢰

93%

글로벌 상위 100대
금융 서비스 기업 중
DigiCert 고객의 비율

88%

Fortune 선정 500대
기업 중
DigiCert 고객의 비율

180

DigiCert가 고객을
보유한
국가 수

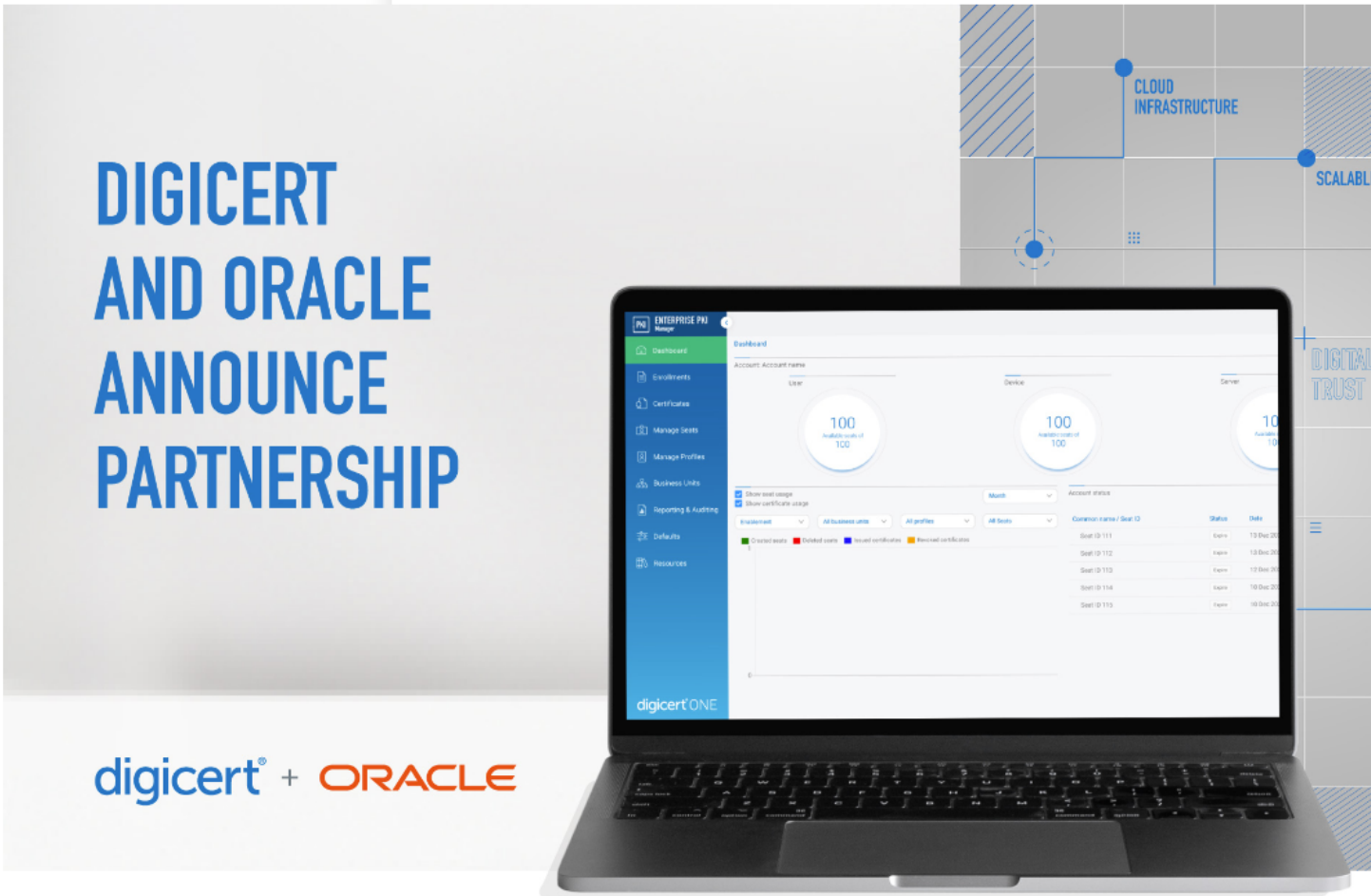


최대 규모의 사이버
보안 기업에
보안 서비스 제공



탁월한
고객 지원 서비스

오라클 OCI에서 DIGICERT ONE 제공



PRESS-RELEASE

05-24-2023

디지털트, 오라
클과 OCI에서 '디
지서트 원' 제공
위한 파트너십
체결

DIGICERT

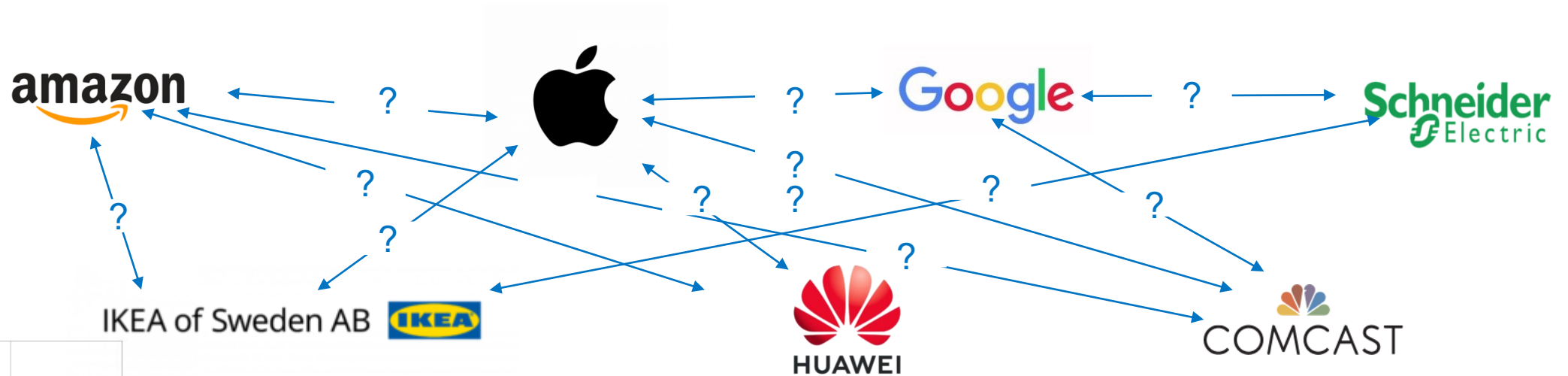


<https://www.digicert.com/kr/news/digicert-announces-partnership-with-oracle>

매터(MATTER)에 관하여

'MATTER' 선택의 이유 - 문제 상황

1. 제조업체들 간의 상호 운용성 부족
2. 보안 표준 부족
3. 수많은 제조업체들의 경쟁



'MATTER' 선택의 이유 - 탄생 배경

amazon



Google

소비자들이 여러 스마트 홈 기기를 원활하게 동시에 작동하는 데 어려움을 겪고 있다는 사실을 **Apple, Google, Amazon** 같은 업계 선두 기업들이 인식했습니다



connectivity
standards
alliance

이에 **CSA(Connectivity Standards Alliance)** 내에서 프로젝트를 만들어 새로운 표준과 인증 마크를 개발하고 이를 통해 스마트 홈 기기의 상호 운용성과 보안을 높이기로 했습니다



matter

업계를 통합하는 표준은 신뢰할 수 있고 안전한 연결을 보장해 주며 표준을 준수하는 기기의 중요한 인증 마크 역할을 합니다

'MATTER' 선택의 이유 - 솔루션



외 250개 업체

CSA(Connectivity Standards Alliance) 및 프로젝트 Matter의 지도부에서 보안과 관련된 사양의 다양한 측면을 정의하고 이를 기록하는 작업에 DigiCert의 도움을 요청했습니다

CES 2023 고객이 새 기기에서 matter 로고를 확인하면 해당 기기가 원활하고 안전하게 연결될 것이라고 신뢰할 것입니다



앞으로의 전망

H2
2022

Summer: Specification Validation Event (SVE) for first Matter capable devices
Fall: Specification 1.0 Release; Certification Program Opens

H1
2023

May 2023: Matter specification 2.0(1.1) to be updated to membership

H2
2023

November 2023: Matter specification 1.3 to be updated to membership. This may include revocation for Digital Attestation Certificates

Note: Timeline, subject to change

Revocation coming. Your Trust Chain Matters!

기기에서 PKI 적용 시, 발생할 수 있는 문제

- **비공개 키 보호**

- 하드웨어 보호 구현
- 레거시 기기에 하드웨어 보호 옵션이 없을 수 있음

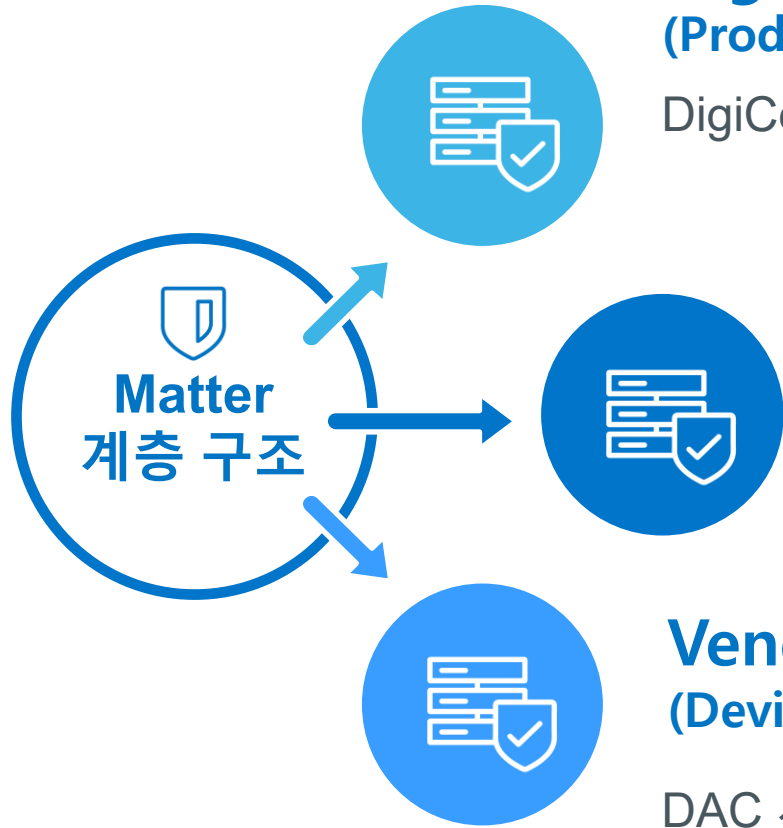
- **암호화 라이브러리 채택**

- 코드에 라이브러리를 구현할 자신감을 얻기까지 시간과 노력이 듦
- 라이브러리 선택 시 신중해야 함

- **코딩**

- 키 생성
- 등록 절차
- 갱신 절차
- 모든 새 제품에서 노력 반복
- 보안 솔루션 코딩에 익숙한 개발자 인력 유지

DIGICERT MATTER CA 계층 구조 및 서비스



DigiCert Matter PAA

(Product Attestation Authority 혹은 제품 증명 기관)

DigiCert 오프라인 루트 CA를 CSA/Matter에 제출함, 벤더 ID 미포함

Vendor PAI

(Product Attestation Intermediate 혹은 제조사 제품 증명 중재자)

DigiCert가 DigiCert의 PAA 멤버를 위한 중재자를 발행함. PAI에는 멤버의 CSA 벤더 ID가 포함됨, PAI의 제품 ID는 선택 사항임

Vendor DAC

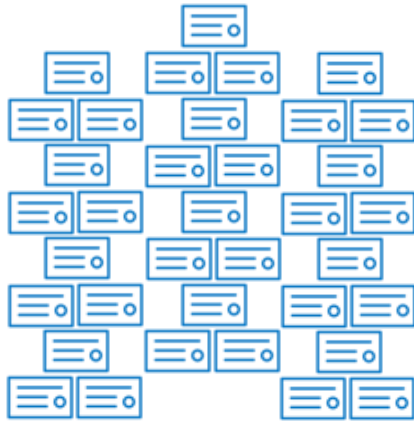
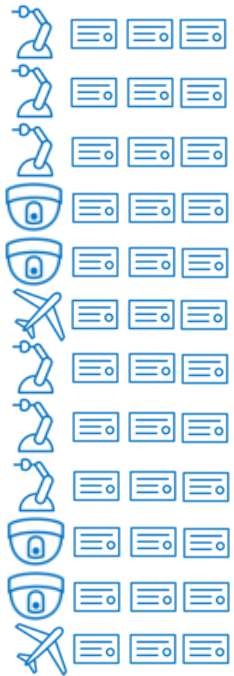
(Device Attestation Certificates 혹은 제조사 기기 증명 인증서)

DAC 서명을 위한 DigiCert 인증서 서비스. DAC에는 제품 ID 및 벤더 ID가 포함됨

IOT TRUST MANAGER 개요

DigiCert를 선택하면 현재 및 미래 제품에 필요한 유형의 인증서를 발급할 수 있습니까?

기기 기록



다양한 인증서

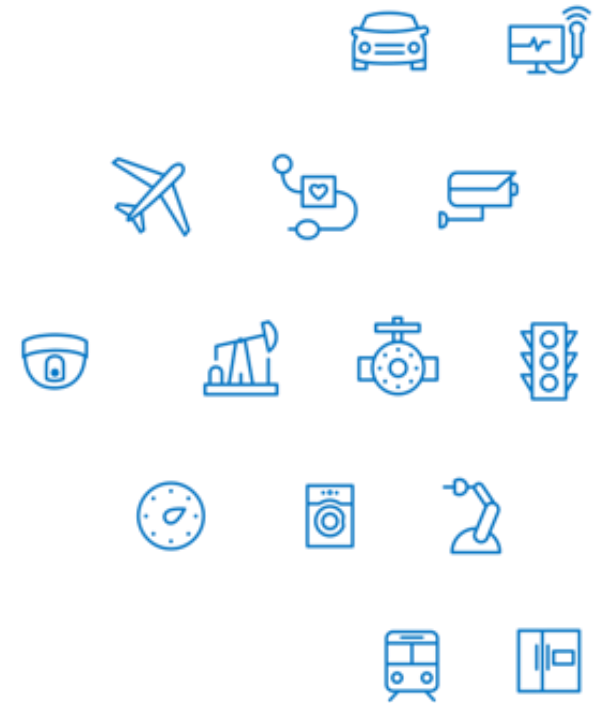
맞춤형 ECU
맞춤 정책
사용자 정의 확장
비x509
SHA2 및 SHA3

등록 방법

- EST
- CMPv2
- SCEP
- ACME
- REST API

인증 옵션

- 비밀번호
- 인증서

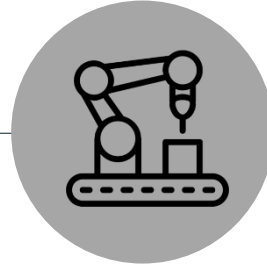
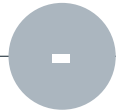


기기에 DAC(기기 증명 인증서) 프로비저닝



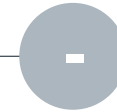
조립 전

조립 전
단계에서 부품에
프로비저닝됨



제조

제조 라인에서
기기에
프로비저닝됨



작동

기기 작동 중
프로비저닝됨

제조업에서의 요청 – ON PREM CA



안전한 로컬 키 저장 - 외부 인증서 요청(CLOUD)



인증서 발급 IoT TM에서 구성됨
배치 등록 프로필 | 등록 프로필
자격 증명

키 저장 IoT TM에서 구성됨
외부 배치 등록
프로필 | 클라우드 IoT TM
연결 정보

DIGICERT 제품 소개

DigiCert는 고객의 디지털 신뢰 과제를 어떻게 해결할까요?

디지털 신뢰를 위한 플랫폼

digicert® ONE

기업 신뢰



Public Trust
(CertCentral)

Private Trust

CLM & PKI Services
(Trust Lifecycle Manager)

기기 신뢰

Embedded
Trust Manager

IoT Trust Manager

소프트웨어 신뢰

Software
Trust
Manager

콘텐츠 신뢰

Document
Trust
Manager

DNS 신뢰

DNS Trust
Manager

Performance
Monitoring

Powered by

ORACLE
Cloud

Dedicated
oracle key
management

MULTICLOUD ARCHITECTU RE

Multi-cloud services
and applications for
flexibility and
performance

DATA RESIDENCY

40-plus global
cloud regions
that support data
privacy
regulations

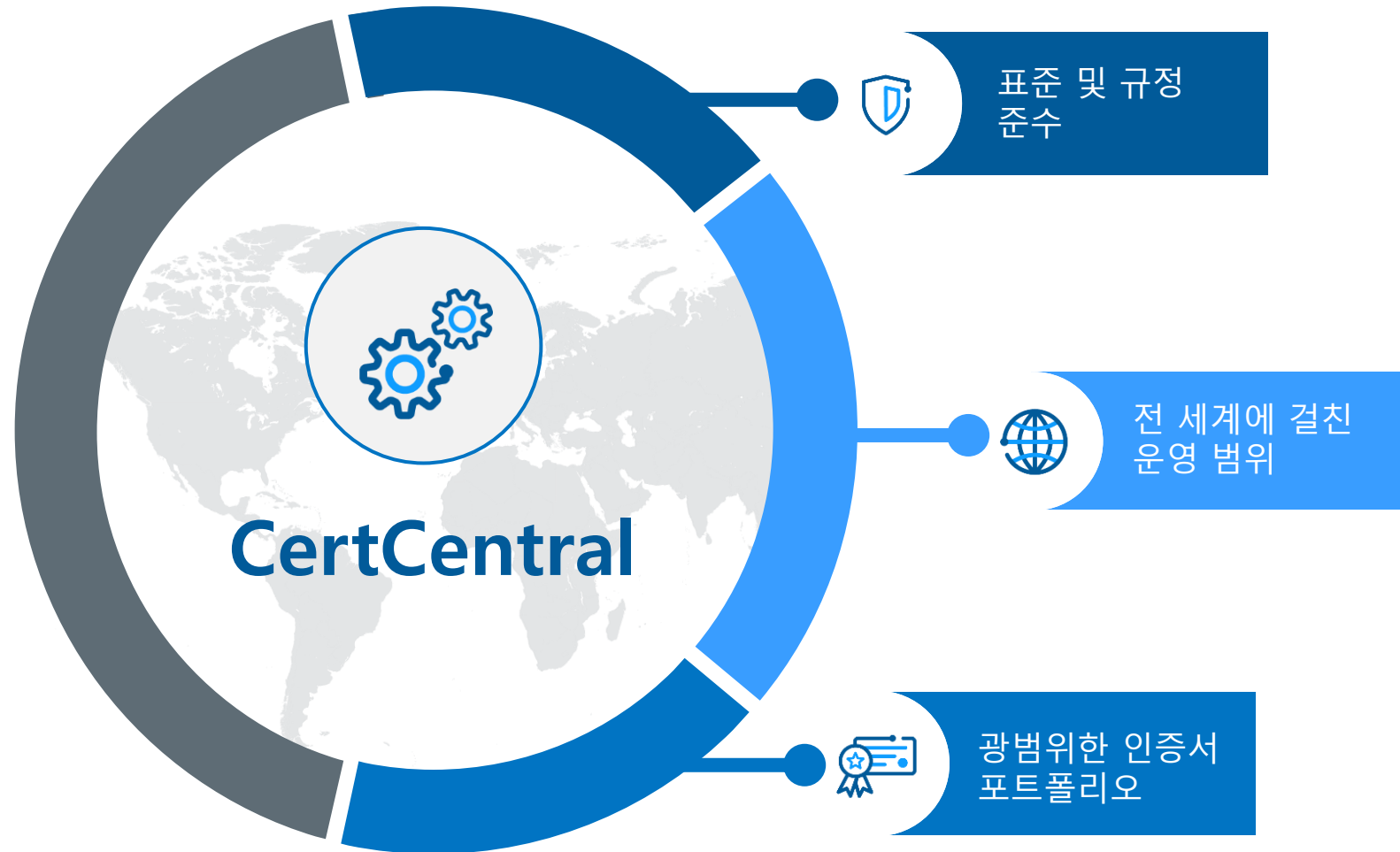
SECURITY BY DESIGN

Isolated network
virtualization &
tenancy, hardware-
based
root of trust, network
segmentation

CONTINUOUS PROTECTION

Always-on
encryption and
monitoring of user
behavior

기업 신뢰: CERTCENTRAL - 업계 최고 수준의 공인된 신뢰 발급



가장 광범위한 인증서

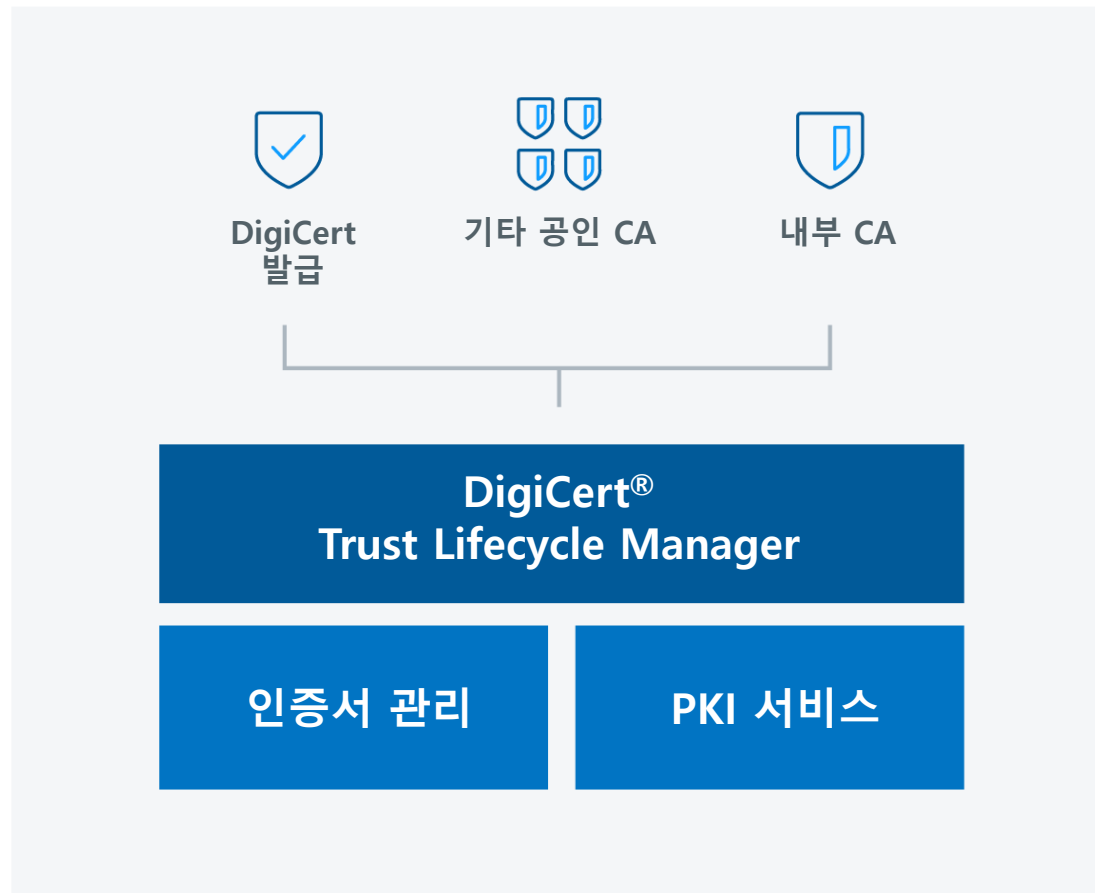


가장 광범위한
유효성 검사 방법



업계 최고 수준의
지원

기업 신뢰: DIGICERT® TLM (TRUST LIFECYCLE MANAGER)



Trust Lifecycle Manager는 다음을 통합합니다.

- 인증서 검색, 관리, 알림, 자동화 및 통합으로 IT 운영을 간소화하는 **인증서 수명 주기 관리**
- ICA 생성과 사용자, 기기, 서버, 기타 IT 리소스를 위한 사설 인증서 발급을 통해 ID 및 인증을 간소화하는 **PKI 서비스**

DigiCert가 제공하는 업계 최고 수준의 공인된 신뢰를 통해 CA에 구매받지 않는 **인증서 수명 주기 관리** 및 **PKI 서비스**를 긴밀하게 결합할 수 있습니다.



중앙 집중식 디지털 신뢰

IBM - DigiCert 이니셔티브

- 사용자 및 기기 Wi-Fi 및 VPN 인증
- 이메일 암호화 및 서명을 위한 공용 S/MIME
- 일반화된 내부 CA에서 전문화된 내부 CA로 전환
- TLS 서버 인증서
- 중앙 집중식 코드 서명 서비스
- IBM 클라우드 카탈로그

향후 계획

- TLS 구매 통합 및 단순화
- 인벤토리 중앙 집중화, 갱신 실패 및 중단 방지, 다양한 클라우드/CA에서 인증서 관리
- IoT - IP 전화, Webex 보드, Apple TV 등
- 멀티 클라우드 - VPC, K8S, Istio 등

1

전 세계 규모

10,000,000+
digiCert® 지금까지 발행된 증명서

2

자산 확보 현황



사용자



기기



코드



서버



이메일

3

통합

- MaaS360(모바일)
- Intune(PC)
- JAMF(Mac)
- BigFix(Linux)
- 디렉토리 서비스

소프트웨어 신뢰: STM (SOFTWARE TRUST MANAGER)

Software Trust Manager는
소프트웨어 공급망 전반에 걸쳐
소프트웨어의 무결성을 보호하는
디지털 신뢰 솔루션으로 코드 손상
위험을 줄이고 기업 및 규제 정책을
시행하며 세분된 키 사용 및 액세스
제어를 제공합니다.



소프트웨어
공급망
무결성을
위한 디지털
신뢰

- 코드 무결성
- 무결성 구축
- 프로세스 무결성 구축
- 소프트웨어 무결성
- 퍼블리싱 무결성

기기 신뢰: ITM (IOT TRUST MANAGER)

기업이 연결된 기기와 운영 시스템에서 디지털 신뢰를 적용할 수 있도록 지원합니다.

기기 관리/
운영



Embedded
Trust Manager

TrustEdge

TrustEdge Client를 통해 기기에
신뢰할 수 있는 ID 프로비저닝
기기에 OTA(over-the-air) 업데이트

인증서 등록



IoT Trust
Manager

신뢰할 수 있는 ID(예: EST,
CMPv2, SCEP, 일괄 발급)를
생성하는 IoT에 국한된 등록
워크플로

인증서 발급



CertCentral

공인된
신뢰

DigiCert ONE
CA

사설
신뢰

기타 CA

기기 신뢰

Software Trust
Manager

서명 관련 정책
사용 및 시행

신뢰할 수 있는 포도당 수치 모니터링

목표

- 기기 및 데이터에 디지털 신뢰 구축

요구 사항

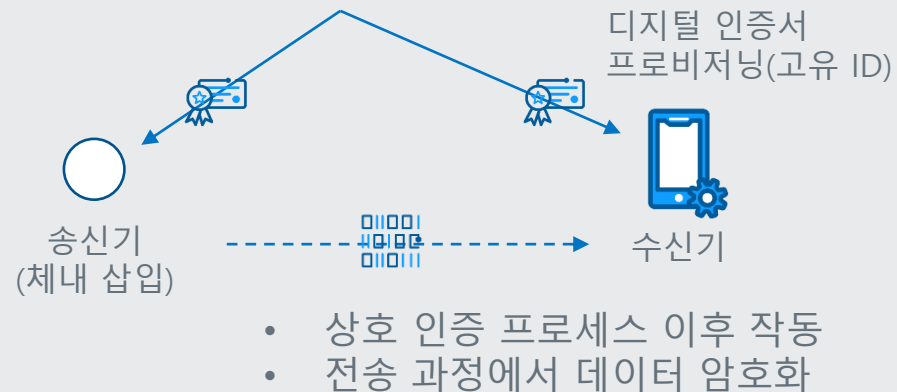
- 기기 인증 보장
- 환자 데이터 보호

결과

- 위조 및 데이터 도난 방지
- 실시간 인슐린 전달 체계를 위한 조작이 불가능한 폐쇄 루프 시스템

1

IoT Trust Manager



2

안전한 폐쇄 루프 시스템을 구축하기 위해 인슐린 펌프 기기 제공 업체에 보안 모델을 확장



운영 기술(OT) 보안

목표

- 5천 개 이상의 스토어에서 네트워크에 연결된 OT 기기를 보호하고 원격 측정에 관한 운영 분석을 실시

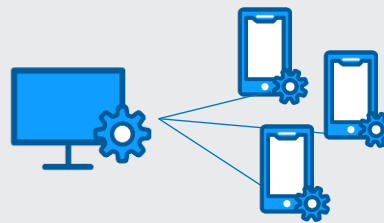
요구 사항

- 조작이 불가능하도록 기기 개선
- 네트워크 통신 보호
- ID 프로비저닝 자동화
- 펌웨어 업데이트 보장
- 클라우드 서비스로 통합

결과

- 조작이 불가능한 기기 및 운영 의사 결정을 위해 클라우드 환경에 원격 측정 데이터 제공

1



OT 기기의 **TrustEdge** 클라이언트가 통신을 보호하고 소매 지점에서 Wi-Fi에 인증

2



OEM 클라우드

Embedded Trust Manager
키 및 인증서 수명 주기 관리

+

기기 OEM을 통한 기기 ID
프로비저닝 자동화

3

Software Trust Manager가 펌웨어
업데이트 승인



Embedded Trust Manager가 현장에
있는 기기에 안전한 펌웨어 업데이트를 전달

4



IoT
게이트웨이



클라우드 서비스

Embedded Trust Manager가 운영 및 유지 보수를 전달하는
원격 측정 분석을 위해 클라우드 서비스에 기기 등록을 자동화

콘텐츠 신뢰: DTM (DOCUMENT TRUST MANAGER)

전송

서명

추적

사용

DocuSign®

 Adobe Acrobat Sign

 Signing Hub

SealSign 2.0

API 통합

 CLOUD
SIGNATURE
CONSORTIUM

Document Trust
Manager

서명 워크플로

ID 검증


서명 엔진

키 관리

인증서 발급



NIST

 Approved Trust List
MEMBER

IDnow.

영상 통화

RIV

등록 기관

공증인

DigiCert 사무실

F2F

선거 보안

목표

- 선거 결과의 유효성에 대한 신뢰 개선

요구 사항

- 안전한 시스템 액세스를 위한 선거 인력 신원 검증
- 선거 결과 문서의 디지털 서명
- 전자 문서의 안전한 전송 및 저장

결과

- 선거 관리 인력 신원 검증을 통해 선거 조작 방지

① 원격 ID 유효성 검사/ID 증명



선거 관리 인력 등록
및 신원 검증

②



선거 관리 인력이 **Document Trust Manager**를 사용해 선거 결과 PDF에 서명하고 업로드

디지털 서명이 검증하는 대상

- 서명자의 신원
- 서명 시간
- 문서 내용의 무결성

③

정부 관계자가 디지털 서명이 포함되어 클라우드에 안전하게 업로드된 선거 결과를 검토



DNS 신뢰: DIGICERT® DNS TRUST MANAGER

업계 최고의 가용성, 성능 및 모니터링 기능을 갖춘 공신력 있는 DNS 서비스

- 관리형 DNS
- 트래픽 최적화
- 모니터링 및 분석

12년이 넘는 기간 동안
100% 가용성 제공



업계 최고 수준의 가용성

12년이 넘는 기간 동안 100% 가용성을 제공하고 있으며 고장을 방지하고 복원력이 뛰어난 공신력 있는 DNS 네트워크



고성능

일부 시장의 1등 서비스



고급 트래픽 최적화

지리, 대기 시간, 가동 시간을 고려한 라우팅, 다중 CDN 관리 지원



DNS 모니터링

실시간 이상 탐지를 통한 네트워크 리소스 모니터링, 업계 대표 서비스

감사합니다.

digicert®

