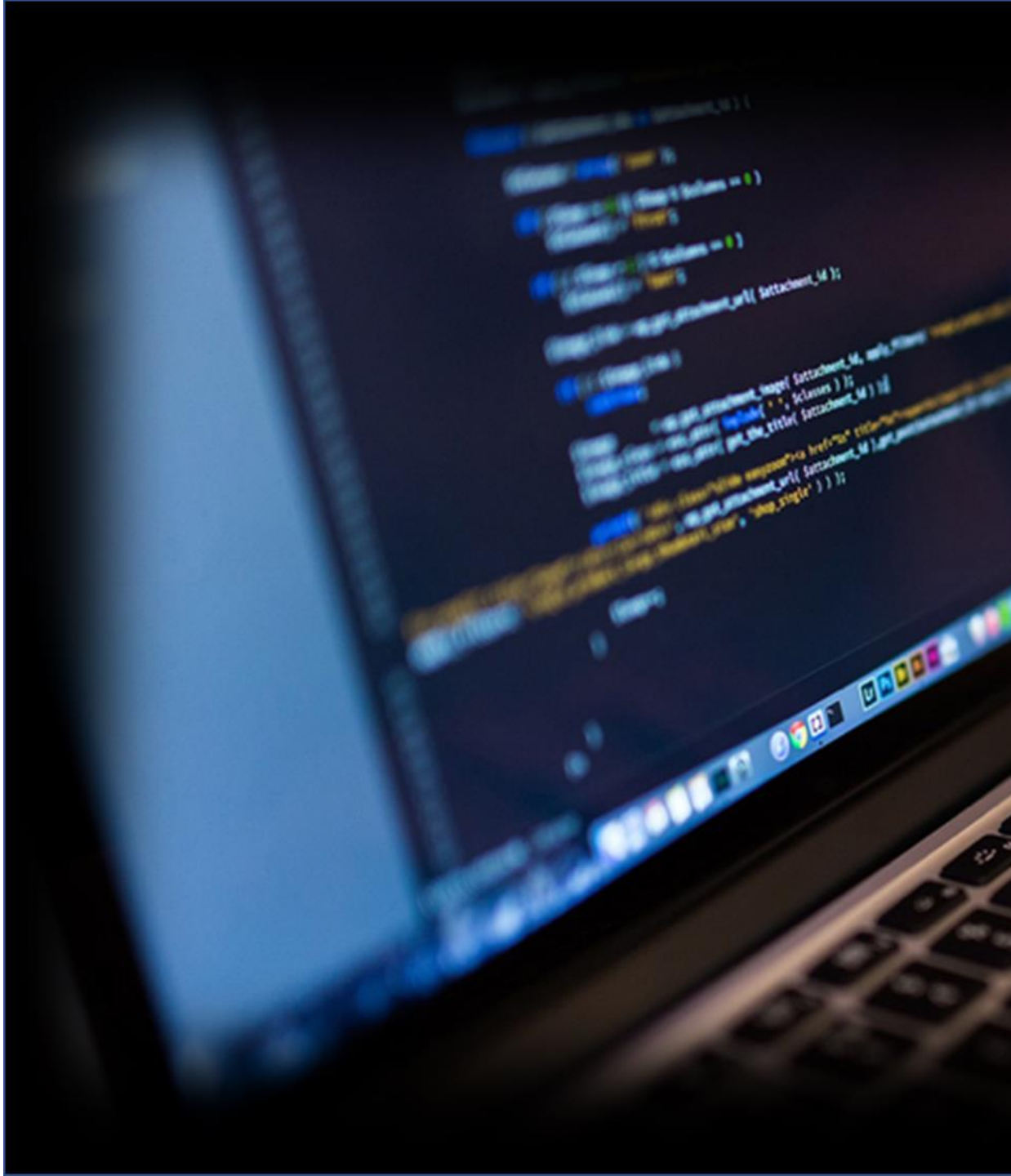
TrustSoT 개요

APT 보안 (OT8/ICS부분)

2022



목차

PanStarEnterprise

2022 © PanstarEnterprise & Sotist All rights reserved

SoTIST

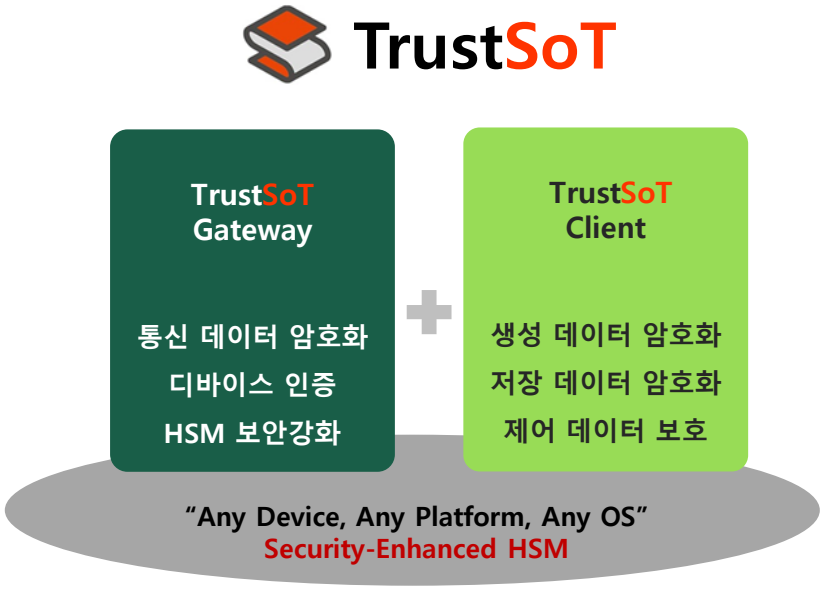
TrustSoT 소개

2022 © PanstarEnterprise & Sotist All rights reserved

최소한의 투자로 차세대 네트워크 환경에서 보안성과 통합성 실현

초경량 Cilent Library로 IoT Devices 및 센서까지 인증 및 관리
데이터와 제어신호의 쌍방향 암호화

APT주)1 공격 대응에 가장 효과적인 솔루션

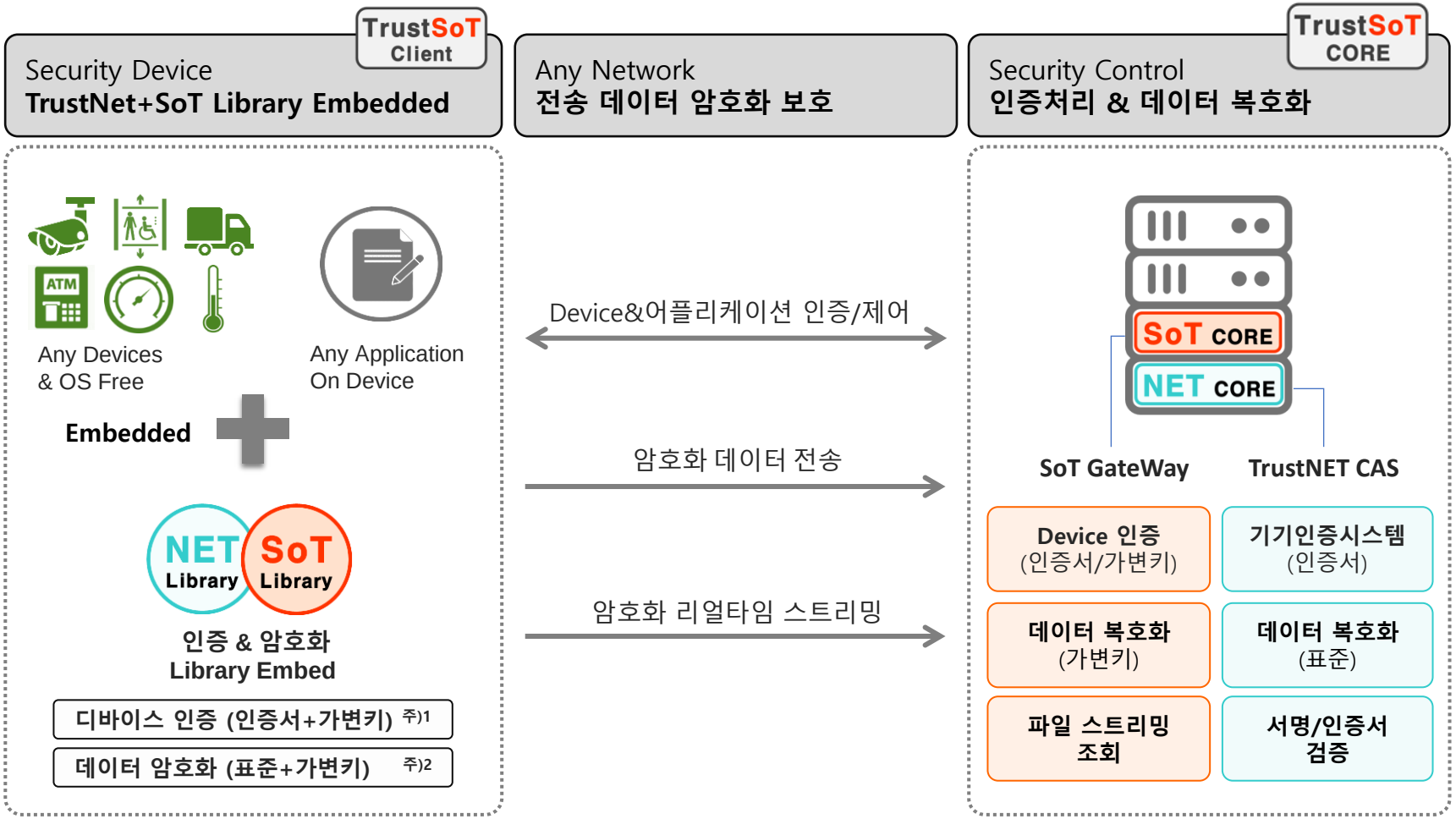


다양한 디바이스 및 네트워크 형태에서 민감한 데이터에 대한 완벽한 보호 방안을 제공

※ 주)1. APT : "Advanced Persistent Threats" 즉, "지능적이고 지속적인 위협 (Chaper 2 참조)

2022 © PanstarEnterprise & Sotist All rights reserved

인증 및 암호화

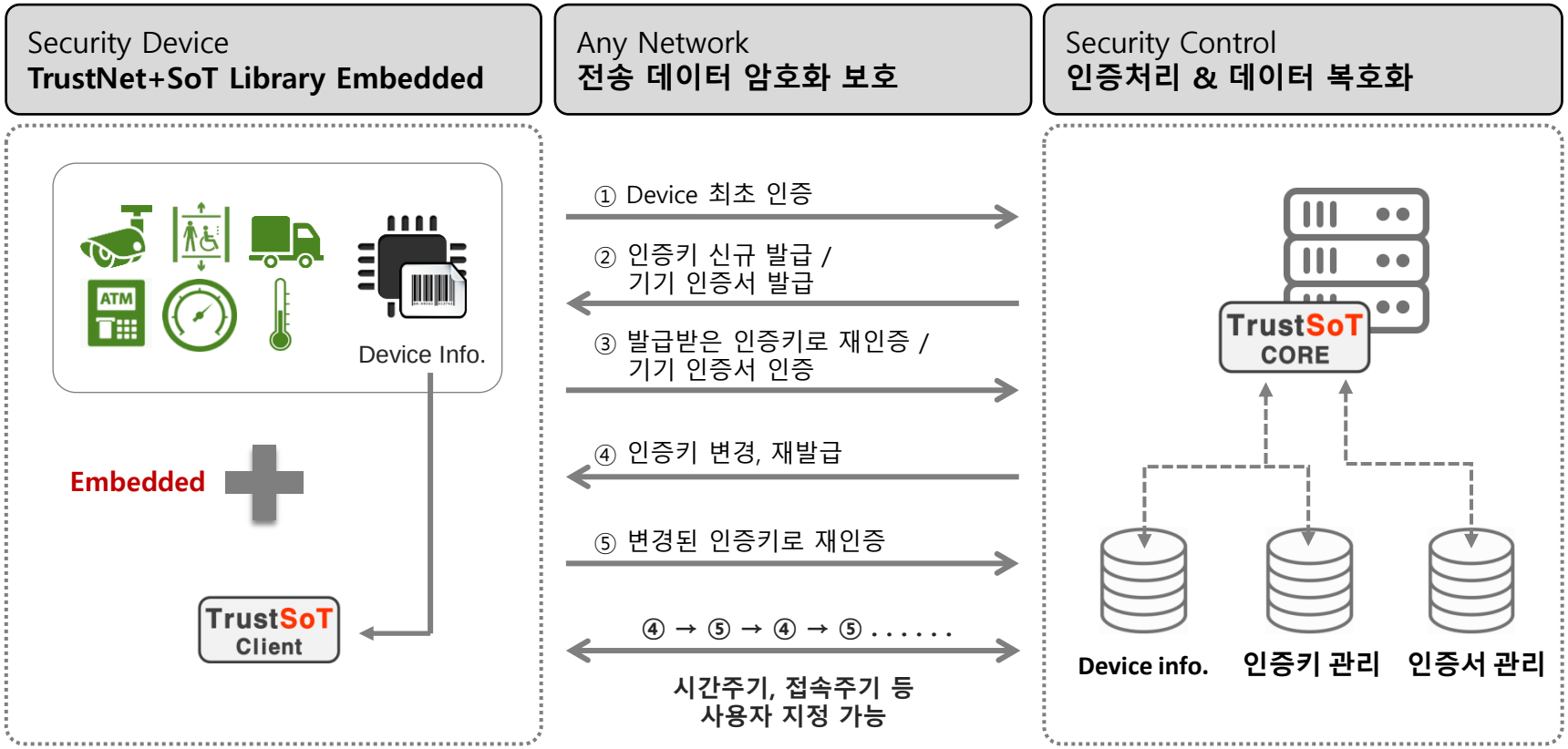


주)1 Page6 핵심기술 "**디바이스 인증**" 참조
주)2 Page7 핵심기술 "**데이터 암호화**" 참조

2022 © PanstarEnterprise & Sotist All rights reserved

핵심 기술 “디바이스 인증”

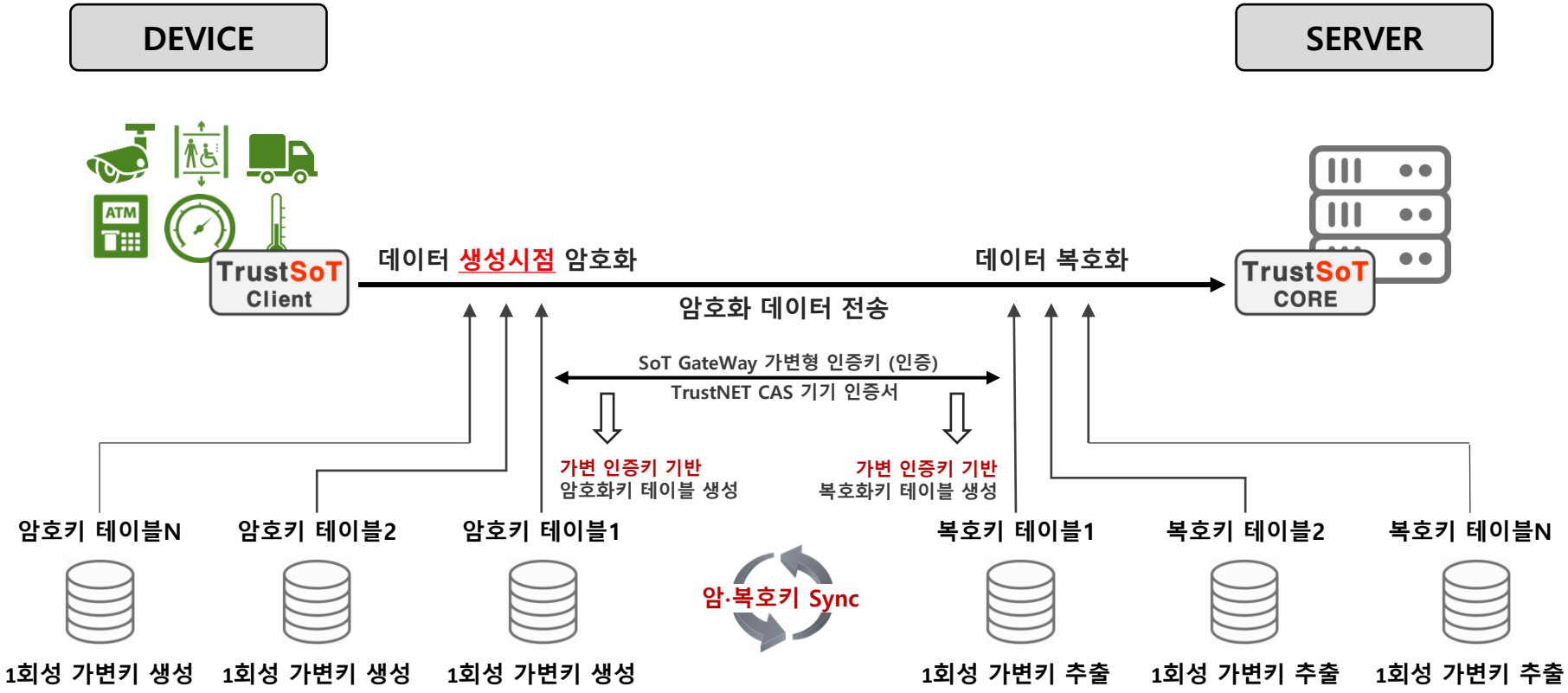
TrustNET CAS & SoT가 적용된 Device는 해당 기기의 Unique(개별) 정보 기반으로 인증되며,
초기 인증 이후부터는 시스템 연결 시 매번 신규 인증키를 갱신 받아 인증 신뢰성 극대화 (기기 인증서 지원 가능)



2022 © PanstarEnterprise & Sotist All rights reserved

핵심 기술 “데이터 암호화”

- TrustNET & SoT가 적용된 디바이스는
  데이터 생성시점부터 1회성 가변형 암호화 키를 기반으로 한 데이터 암호화를 수행하여 전송 또는
  보관 중인 모든 데이터 완벽 보호 (표준 인증 암호 모듈 및 알고리즘 지원)

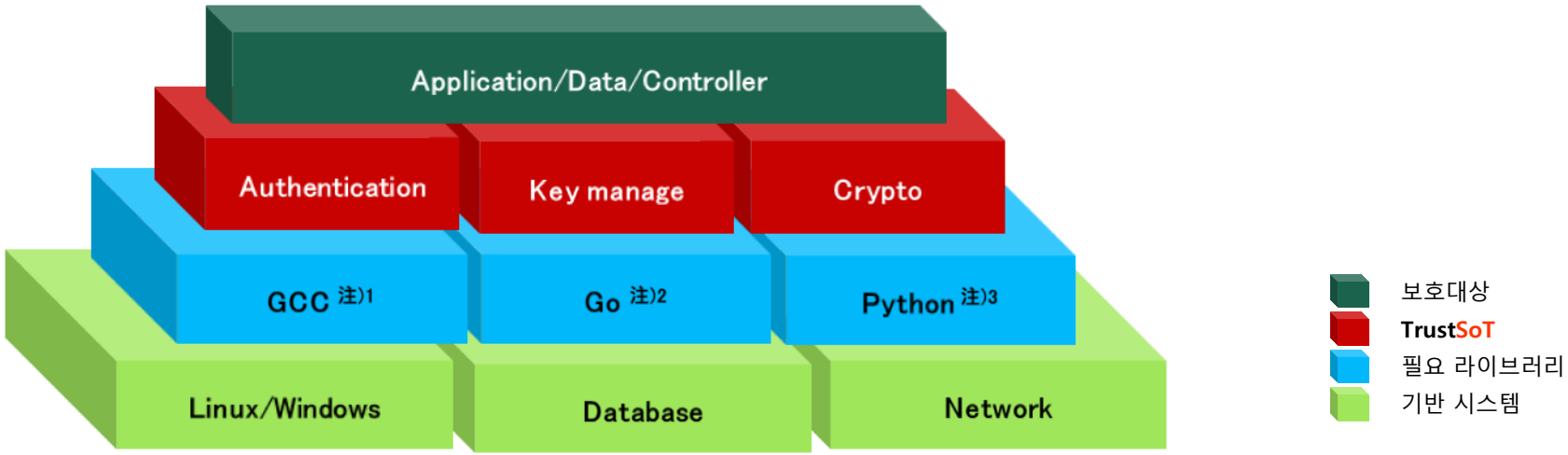


2022 © PanstarEnterprise & Sotist All rights reserved

TrustSoT S/W

100% 자체 특허를 기반으로 100% 자체 개발된 엔진과 라이브러리로 구성.

- 한국특허 : 장치인증키를 이용한 데이터 암호화 방법 및 시스템 (제10-2028151호)
- 일본특허 제 2017-563588호, 미국특허 : 16/603,339



주)1 GCC
C/C++ 언어를 위한 라이브러리로 주로 속도를 요하는 각종 데이터 처리 등을 위한 개발에 사용

주)2 Go
웹기반 사용자 화면을 위한 개발 언어 / 내부에 Web을 위한 자바스크립트나 HTML이 사용되나 핵심 운영언어는 Go 언어

주)3 Python
로그 분석 수집 과 인공지능 모듈의 적용 등을 담당 / 대부분의 로그 분석 수집 , 인공지능 모듈이 이 Python으로 제공

2022 © PanstarEnterprise & Sotist All rights reserved

S/W구성

구분	Linux	Windows
버전	Kernel 3.X 이상	7 이상
표준 배포본	Ubuntu 18.04, CentOS 7.6	Windows 7, Windows 10
구현 환경	C/C++, Python 3.X, Shell script	C/C++, Python 3.X, C#
라이브러리	GCC 7.1 이상	.NET 4.0 이상
개발 도구	대부분의 개발 도구 지원	Visual studio 2017 이상
데이터베이스	Postgressql 11 이상	Postgresql 11 이상
패키징 방식	자체 실행 및 Docker	자체 실행 및 Docker

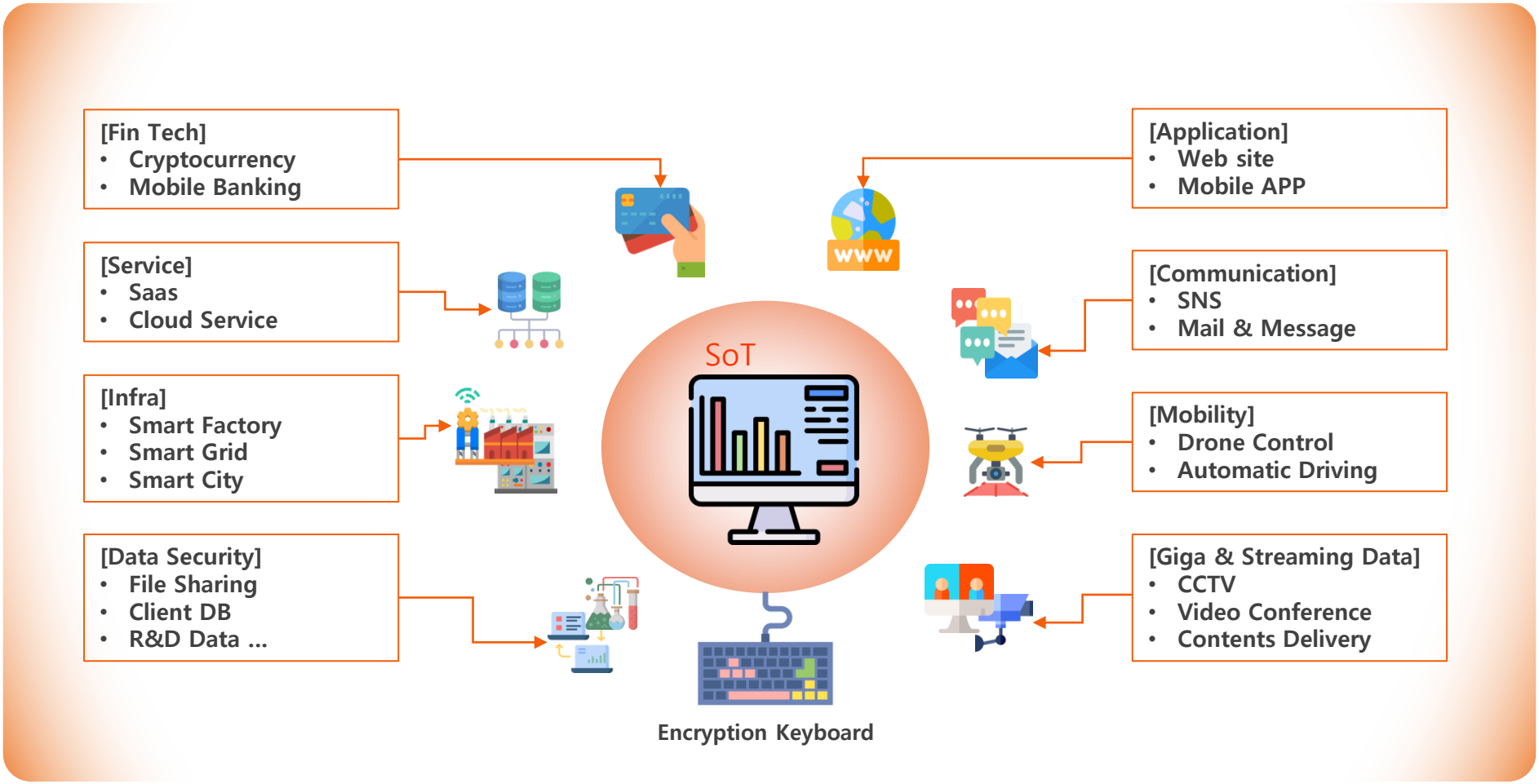
H/W구성

구분	최소사양	평균사양	최고사양
CPU	4Core	8Core	8Core
CPU architecture	Intel x86_64	Intel x86_64	Intel Xeon
Memory	8GB	16GB	32GB
SSD	256GB	1TB	1TB x 4EA(RAID)
N/W card	Ethernet 1Gbps 2개 이상	Ethernet 1Gbps 2개 이상	Ethernet 1Gbps 2개 이상
Power Supply	2EA	2EA	2EA
Interface Port	USB 3.0	USB 3.0	USB 3.0
User	less than 1,000	less than 5,000	less than 10,000

2022 © PanstarEnterprise & Sotist All rights reserved

적용분야

TrustSoT는 모든 분야에 적용 가능하며
다양한 형태의 네트워크 그리고 주요 데이터와 제어지시를 암호화하여 보호합니다.



2022 © PanstarEnterprise & Sotist All rights reserved

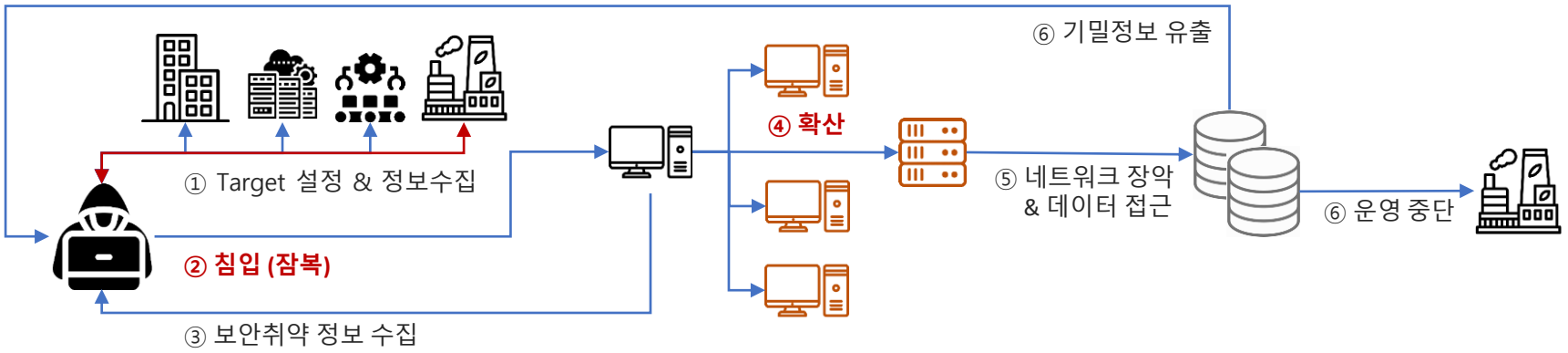
새로운 보안 환경

(APT : Advanced Persistent Threats)

2022 © PanstarEnterprise & Sotist All rights reserved

PKI(SSL/TLS), VPN등 대부분의 보안 솔루션을 무력화 하는 APT 공격

- "Advanced Persistent Threats" 즉, "**지능적인 지속 위협**"
- APT 공격은 과거의 불특정 다수를 노렸던 공격과는 달리 **하나의 대상을 목표**로 하며, 목표의 내부로 침입을 성공할 때까지 다양한 IT 기술과 공격 방식을 기반으로 여러 보안 위협을 생산하여 **공격을 지속**
- 내부로 **침입** 후, 거점을 마련하고 수집된 **보안 취약점을 이용**하여 내부의 정상적인 시스템(PC, 서버 등)까지 **확산**
- 내부 시스템 장악 후 기밀 정보 수집, 운영 중단, 시스템 마비 등 **침입 목적 수행**
- 근래 대부분의 해킹의 수단으로써, 특히 PKI, VPN의 취약점을 공략



"TrustSoT"와 "VPN"은 상호 보완제로써 APT 공격에 대한 완벽한 보안 솔루션 구현이 가능

(page23 "TrustSoT & VPN 상호 보완제로써 역할" 참조)

2022 © PanstarEnterprise & Sotist All rights reserved

APT 공격과 기존 악성코드 공격의 차이점

기존 악성코드의 공격과는 다른 APT 공격의 대표적 특징

① **Advanced** (지능적)

② **Persistent** (지속적)

③ **Motivated** (동기)

④ **Targeted** (목표)

구분	악성코드 공격	APT 공격
공격 분포	무차별 대량 살포	**치밀하고 조직화된 계획**
공격 대상	무작위 다수	**정부기관, 단체, 기업**
공격 빈도	일회성	**지속성**
공격 기술	악성코드 디자인	**고도의 지능적인 보안 위협을 동시에 이용**
탐 지 율	1개월 이내 발견 시 99% 탐지	**1개월 이내 발견되면 10%이하**
공격 결과	악성코드 감염, 개인 정보 유출	**기밀 자료 유출, 시스템 작동 불능, 사회 기반시설 마비**

2022 © PanstarEnterprise & Sotist All rights reserved

IT와 OT/ICS의 환경 차이

IT(Information Technology) : 인터넷 등 오픈 네트워크, 그를 활용한 정보통신기술
OT(Operational Technology) : 산업용 기계나 공정의 운영을 위한 기술, 과거 폐쇄망내에서 운영되었으나 점차 오픈 네트워크 영역으로 확대
ICS(Industrial Control System) : 각종 기계류와 공정을 제어하기 위한 시스템, 폐쇄망내에서 운영
전용 하드웨어/운영체제/소프트웨어 등 대부분 전용 규격을 사용하여 **보안에 대해 낮은 인식**

구분		IT	ICS
H/W	장비 구성	표준 장비 (PC, 서버)	**표준 장비, 공정 특화 장비**
	구성 변화 주기	짧음	**변화 거의 없음**
	패치 및 보수	성능 향상을 위해 자주 발생	**가용성을 이유로 거의 없음**
S/W	운영 소프트웨어(OS)	범용 OS	**제어 기기(Windows) 제어 대상 (커스터마이징 Embedded OS)**
	주 사용 소프트웨어	업무용 상용 및 자체 개발	**커스터마이징 된 상용 및 자체 개발**
	업데이트 주기	기능 오류 와 보안 패치 자주 진행	**기능 오류 외 보안 패치 없음**
보안	보안 목표	중요 데이터 유출과 서비스 중단 차단	**생산 및 공정 중단 가능성 차단**
	보안 사고 영향	유출 데이터의 중요도에 따른 피해	**생산 및 공정 중단의 직접적인 피해**
		법적 이슈 및 회사 신뢰 피해	**제품에 대한 신뢰성 피해**

2022 © PanstarEnterprise & Sotist All rights reserved

OT/ICS 에 대한 주요 APT 위협 경로

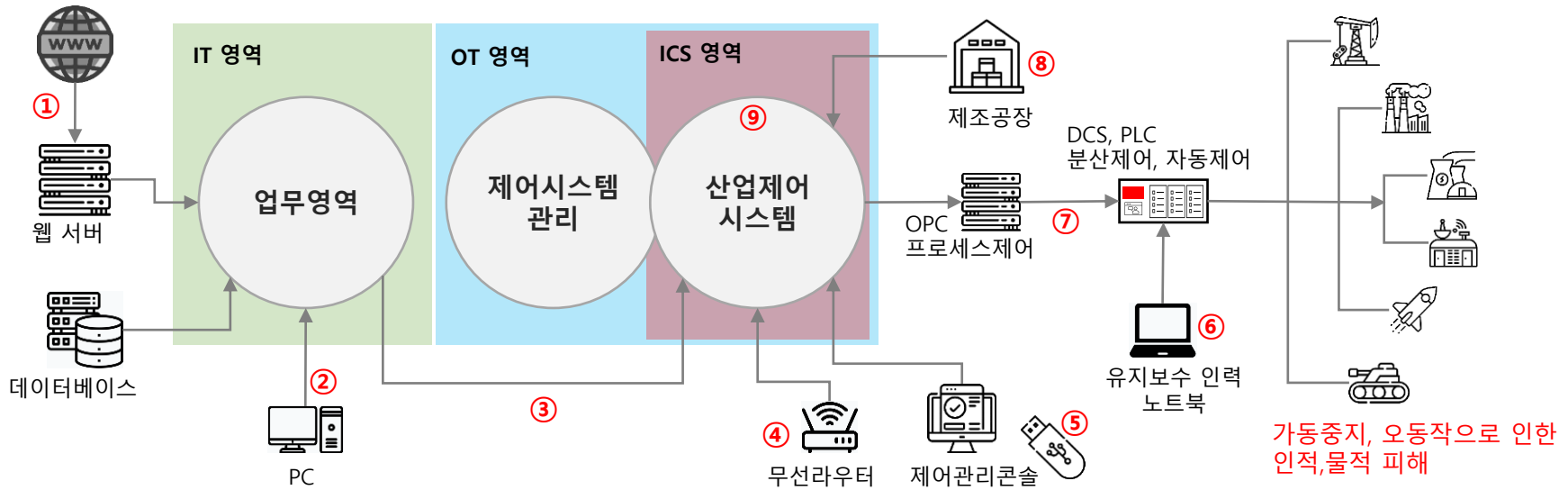
네트워크 망 영역 구분

- 임직원들이 업무를 수행하는 **IT**(업무) 영역
- 제품 생산을 위한 **OT**(제어시스템 관리) 영역
- 제조 공정을 제어하고 제품을 생산 하는 **ICS**(산업제어시스템) 영역

다양한 보안 위협

- IT보안 위협(해킹, 악성코드 감염, APT 공격)
- 업무영역에 우선 침투하여 내부 정보를 수집한 후 ICS 영역을 공격
- 불법적인 ICS영역 침입에 의한 공격

	APT 위협 경로	TrustSoT
①	해킹, APT 공격 등 IT 보안 공격	
②	악성코드 감염 후 망내 확산	○
③	업무망에서 ICS망으로 비인가 연결 악용	
④	ICS망내 무선 인증 우회 및 취약점 공격	
⑤	USB 이용, 악성코드 유포, 중요 정보 유출	○
⑥	외주/유지보수 인력의 감염된 노트북	○
⑦	제어 명령 위 변조 및 프로토콜 정보 유출	○
⑧	제조사 원격 유지보수 채널 악용	○
⑨	단일 네트워크 장애 (이중화 미적용)	



※ 대응방안 : Chapter3 "TrustSoT의 OT/ICS APT 공격 대응" 참조

PanStarEnterprise
2022 © PanstarEnterprise & Sotist All rights reserved
SoTIST

OT/ICS 분야의 APT 공격에 대한 취약점

OS 업데이트 (보안 패치) 소홀

대분분의 산업분야에서 OS 업그레이드(보안패치) 없이 운영중

- 원인1) 폐쇄망(독립망)상태에서의 장기 운영이라는 특성상 **보안 패치에 소홀**해 짐
- 원인2) 산업제어 특성상 실시간성과 무중단 운영이라는 원칙에 따라, 패치 과정의 문제 발생시 **운영 중단의 사태 우려**
  특히, **SCADA 프로그램은 Window버전**이며, **Window OS의 경우 업그레이드를 통한 보안 패치가 필수**

※ 데일리 시큐 (2021.02.14)

- 미국 플로리다 수질처리시설에 대한 사이버 공격의 세부정보가 공개
- 수질 처리장의 SCADA(스카다) 시스템에 원격으로 액세스해 상수도의 **수산화나트륨 투여량을 위험한 수준으로 늘리려는 공격**
  (다행히 현상을 발견한 담당자의 조치로 해결)
- 침입방법 : 제어 시스템에 연결된 공장의 여러 컴퓨터 중 하나에 설치된 TeamViewer 소프트웨어를 통해 SCADA(Supervisory Control and Data Acquisition) 시스템에 억세스
- 취 약 점 : 업그레이드 되지 않은 윈도우7 운영 체제의 32비트 버전을 사용 (2020년 1월 14일 이후부터 **업데이트를 중단**)
  원격 억세스를 위해 **동일한 암호를 내부 공유**
  방화벽 보호 기능이 미설치
- 해 결 책 : 소프트웨어를 포함한 컴퓨터, 장치 및 응용 프로그램을 패치 및 최신 상태로 유지
  강력한 암호로 2단계 인증 사용

※ TrustSoT의 대응 (page18~24 참조)

대응1) OS 업그레이드 무관하게 Client PC, Server(Scada)에 발생하는 모든 포트 및 패킷 감시 후 이상 징후 시 알람 또는 네트워크 차단

대응2) ID/PW 공유 또는 탈취 당하더라도 인증 받은 단말기 외의 접근 차단 (제어 명령 불가)

2022 © PanstarEnterprise & Sotist All rights reserved

APT 주요 공격 사례

☐ **3.20 전산망 장애** - 대한민국

- 백신회사 업데이트 서버 우회 침투 , 1년 이상 잠복 후 공격 개시 (북한 정찰총국)
- 부팅 영역 파괴로 전산망 마비 (PC, ATM 등 약 48000여대 시스템 파괴)
- 방송사(KBS, MBC, YTN) / 금융사(신한은행, 농협)

☐ **평창올림픽 개막식 공격** – 대한민국

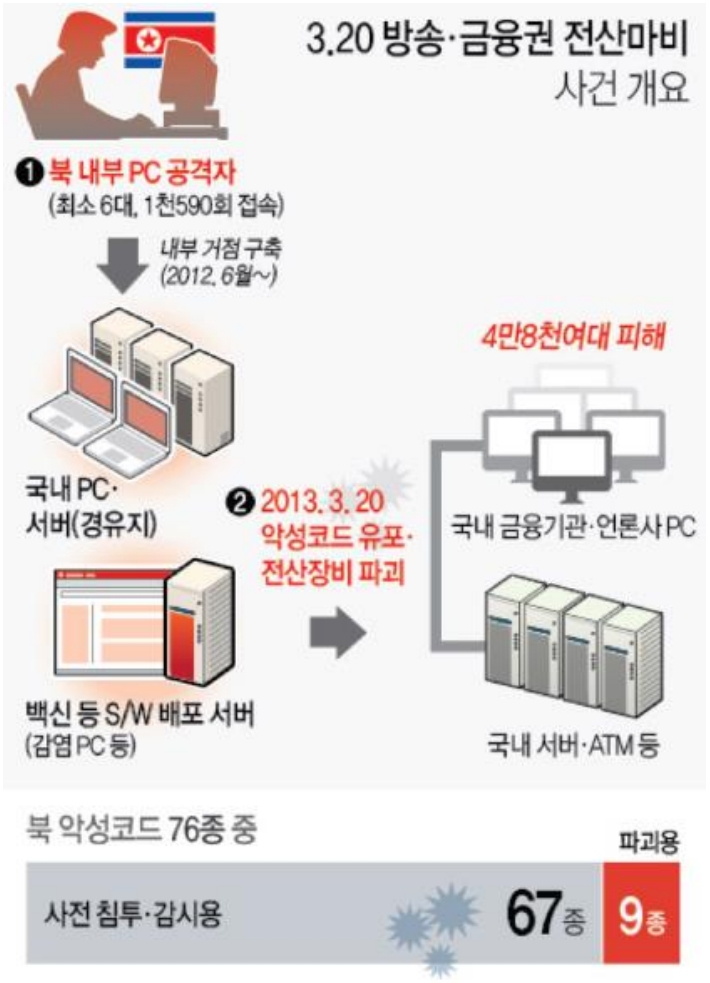
- 2018년 2월 9일 오후 8시 개막식 시간 타겟, 핵심서버 50대 파괴
  . 개막식 1개월전 올림픽 운영본부 전산실 라우터 해킹 후 PC 300대 감염,
  44개의 계정정보 탈취로 서버접근 권한 확보
- 올림픽 관련 웹사이트 마비, 올림픽 현장 와이파이 중단, 미디어센터 IPTV 중단
  8시 이후 티켓 판매 중단 (개막식 빈좌석 발생)
- 러시아 해외정찰국 (북한 소행으로 위장)

☐ **콜로니얼 파이프라인(Colonial Pipeline) 가동 중단** – 미국

- 랜섬웨어 공격, 러시아의 다크사이드(DarkSide) 추정
- 300만배럴/일 송유관 마비, 공급 차질로 유가가 5~6% 인상

☐ **스턱스넷(Stuxnet)** - 이란

- **지멘스 SCADA 시스템을 목표로 제작**된 정교하고 **군사적 수준의 악성코드**
- 원자력, 전기, 철강, 반도체, 화학 등 주요 산업 기반시설의 제어시스템의 오작동 발생
- 2010년 7월 이란원자력 발전소 작동 방해 (지멘스 SCADA 시스템)



2022 © PanstarEnterprise & Sotist All rights reserved

TrustSoT의 OT/ICS APT 공격 대응

2022 © PanstarEnterprise & Sotist All rights reserved

APT 공격에 대한 “감시 및 탐지” 및 “네트워크 차단(기술적 방어)과 위험 경고(관리적 방어)”

TrustSoT는 모든 루트의 APT 확산 경로를 **감시 및 탐지**하며, 이상 징후 발견 시 **차단 및 경고**

[감시 및 탐지]

☐ **Client**

- 행위기간 분석 : TrustSoT Agent는 외부로 부터 수신된 모든 파일에 대해
  해당 파일이 실행될 때, 이상 Process, Pattern 등의 이벤트 감시

☐ **Network**

- Port Scanning : IP와 Port에서 발생하는 이상 Service 감시
- Traffic Analysis : Traffic의 증감에 대한 이상 패턴 감시

☐ **Server**

- 보안정보/이벤트관리(SIEM) : 수집된 이상 징후 Data에 대한 분석으로 사전적 조치 시행
- Log 분석 : 시스템 로그 및 Timeline 등을 구성해 공격 감시
- 비인증 Client의 접근 감시 (ID, Password 등 사용자 정보와 무관하게 비인증 Client에 대해 차단)

[차단 및 경고]

☐ 상기 공격 대상에 대한 이상 징후를 실시간 감시 및 탐지하고, 이상 징후 발견시 해당 Client로 부터 감염 데이터 확산되지 않도록 네트워크 차단 및 감염 내용 경고

※ APT 공격에 대한 現 대응상황

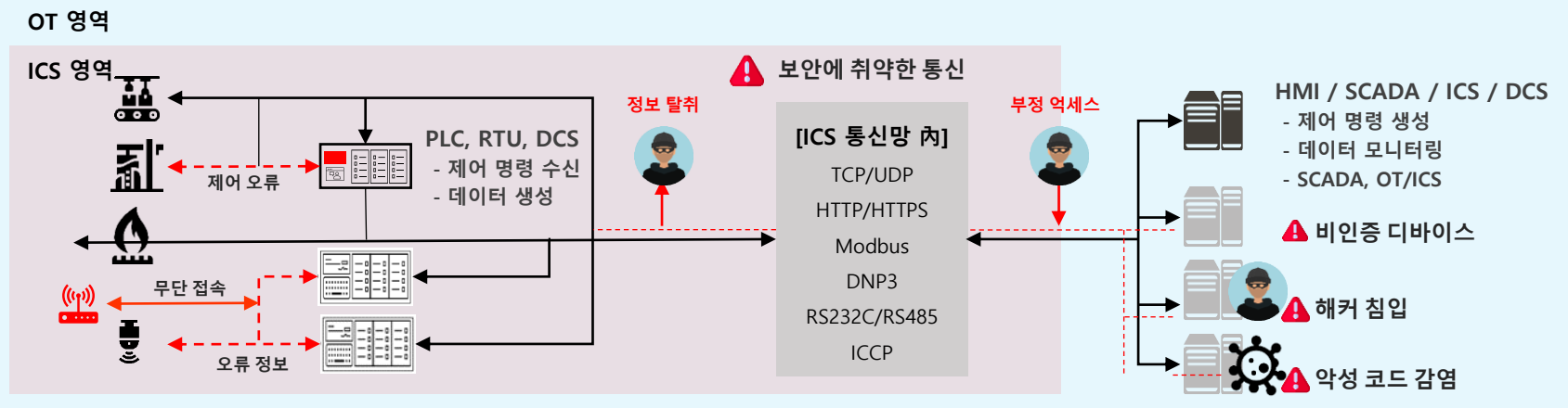
- 2019년 부터 APT 공격에 대한 경고를 계속 발동해 왔으나 현재 방어 솔루션은 이메일에 첨부된 파일을 실행할 때 경고 메시지, 감염사례 분석을 통한 백신 개발뿐인 것으로 확인됨 (KISA 한국인터넷진흥원 의견)

2022 © PanstarEnterprise & Sotist All rights reserved

OT/ICS 보안에 대한 TrustSoT

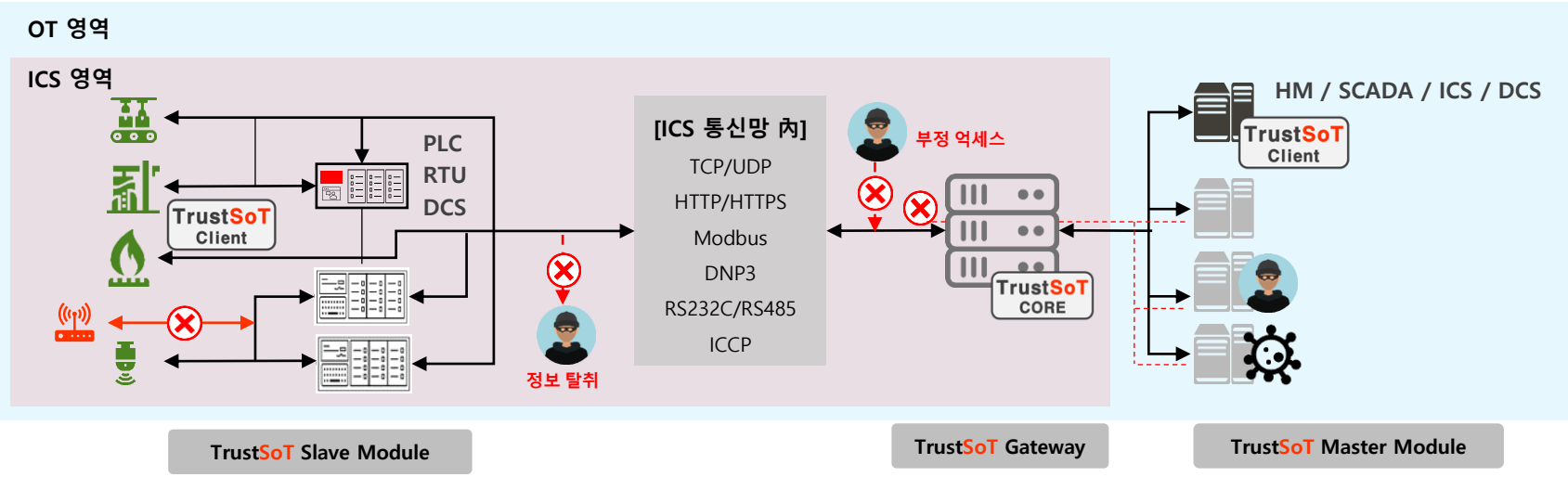
AS-IS

기존 OT/ICS(산업제어) 분야의 구성은
내부에서 진행 되는 기기 제어와 모니터링에 대한 보호 방안이 없어 각 부분별로 다양한 보호체계가 필요



TO-BE

OT/ICS(산업 제어)분야에서 발생 할 수 있는 각종 보안 문제를 해결 하기 위해
TrustSoT는 디바이스 인증, 데이터 암호화 및 이벤트 감시 등을 통한 제어 분야 보호



PanStarEnterprise
2022 © PanstarEnterprise & Sotist All rights reserved
SoTIST

Gateway 및 Module 주요 기능

TrustSoT Slave Module	TrustSoT Gateway	TrustSoT Master Module
복호화 키 요청 제어 명령 복호화 및 확인 인증서 발급/폐지 요청 데이터 생성, 인증 정보 전송 송신 데이터 생성 / 수신 데이터 분석	데이터 중개(Proxy) Master , Slave간 인증 및 접근제어 (인증, 암호화)가변키 관리 전송데이터 분석 모니터링로그수집	암호화 키 요청 제어 명령 암호화 인증서 발급/폐지 요청 데이터 인증 정보 확인 송신 데이터 생성 / 수신 데이터 분석

DEMO 기기

구분	구성
CPU	Siemens PLC 315-2 PN/DP
DI	Siemens PLC 321 (32Points)
DO	Siemens PLC 322 (32Points)
DIN Rail	Siemens DIN Rail for CPU 3xx
Power	Weidmuller 100~240V AC
Button	24V DC Input Push Button
Lamp	24V DC Output Lamp

※ Sofrware
Siemens Operation, Engineering and
TrustSoT encrypt communication library

"SIEMENS Korea" 검증 실시 : SIEMENS PLC를 활용한 "제어 데이터의 암호화" 및 "수신측의 복호화"를 통한 제어 데이터의 안전한 보호 및 정상적 제어 동작 가능 확인 (SIEMENS Korea 기술팀 및 영업팀 확인)

2022 © PanstarEnterprise & Sotist All rights reserved

주요 차이점

기존 APT 보안 솔루션이 악성코드의 **설치(침투)에 대한 방어에 집중**하는 반면
TrustSoT는 감염된 기기로 부터 **확산 방지와 중요 데이터 보호(암호화)에 집중**하여 타사 제품 대비 차별화/우위성 확보

구분	Paloalto	Symantec ATP (Advanced Threat Protection)	TrustSoT
Application 감시	○	○	○
URL 기반 악성코드 침입 방지	○	○	×
Email 악성코드 감지	○	○	×
Network 공격 방어	○	○	△ 장비 포트 감시
악성코드 감염 후 내부 확산 방지 기능	× **Application** 기반 감시 정책 수립 (허용, **차단** 등) 공개/비공개 악성코드 차단	× **Port** 기반 감시 정책 수립 (허용, **차단** 등) 공개 악성코드 차단	○ **Agent 기반 프로세서 감시** 공개/비공개 악성코드에 대한 (모든 이상 Process) **실행 경보 및 내부 확산 방지(차단)**
생성 파일 보호	×	×	○ Agent 기반 파일 실행 이벤트 감시
ICS(산업제어) 프로토콜 지원	×	×	○
기기 사용자 감시	×	×	○
파일 유출 보호	○	×	○
주요 기능	**침입 차단**	**침입 차단**	**확산 차단 데이터 암호화**

2022 © PanstarEnterprise & Sotist All rights reserved

TrustSoT & VPN 상호 보완제로써 역할

보안 Solution별 기능

Solution	기능
PKI	통신 구간의 접속과 통신 구간 암호화를 위한 솔루션
VPN	가상의 Private Network를 구현하여, 보호되고 있는 네트워크 망에 **외부에서 접속 불가능** 하도록 하는 솔루션
TrustSoT	통신 구간의 접속에 대한 제어만 가능한 PKI, VPN 과는 달리 **Application Level에서 인증과 암호화**를 통해 네트워크에 연결 하는 기기나 소프트웨어 **내부에서 부터의 보안**을 제공

보안 Solution별 보안 위협에 대한 대응 가능 여부

공격유형	비율	PKI	VPN (Network 기반)	TrustSoT (Device 기반)	TrustSoT의 대응 방법
문서기반 **악성코드 배포**	90%	×	○	○	인증 받은 기기와 사용자가 인증 받은 어플리케이션에 의해 생성된 문서인지 확인 **(감염시 확산 차단)**
악성코드에 의한 **DDos 공격**	3%	○	○	△	**인증 받은 유형의 패킷** 외 차단 (서비스 중단 방지)
백도어 기반 **불법 침임**	2%	×	○	△	**인증받은 디바이스**와 특허 암호화 기술을 통해 암호화 된 데이터만 접근 가능
파일/데이터 탈취	2%	×	○	○	파일, 데이터별 가변키 기반 인증 암호화로 각 암호화 별로 다른 정보로 암호화되어 **인증받은 기기와 사용자만 복호화 가능**
산업용 제어등 **각종 프로토콜 위/변조**	1%	×	×	○	프로토콜 생성시 데이터에 대한 암호화 및 수신처 복호화시 **인증과 프로토콜 분석 차단**

2022 © PanstarEnterprise & Sotist All rights reserved

보안 Solution별 기능

구분		기능	설명
TrustSoT	Gateway (관리 기능)	인증	사용자, 디바이스, 어플리케이션 및 데이터와 파일에 대한 인증 및 접근 제어
		암호화	사용자, 디바이스, 어플리케이션으로부터 생성되는 데이터 암호화를 위한 암호화 모듈 및 암호화 키 운영
		Client 제어	TrustSoT Agent, TrustSoT SCADA 등 전용 클라이언트의 실행, 접근제어
		로그	각종 로그 수집 및 모니터링
	Workstation (일반 업무)	암호화	지정 파일과 데이터 암호화
		프로세스 감시	디바이스의 실행 프로세스 감시, 통보 및 차단
		이벤트 감시	디바이스 OS의 발생 이벤트 감시, 통보 및 차단
		통신 감시	지정 포트 외 포트 개발 감시, 통보 및 차단
	ICS (제어네트워크)	제어 명령 보호	제어부로 부터 PLC로 전달되는 제어 명령 인증/암호화
		프로토콜 감시	지정된 프로토콜 이외의 프로토콜 송수신 차단
		접근 제어	인증된 사용자, 디바이스 및 어플리케이션 외 제어 네트워크 차단
		상태 관리	연결된 제어네트워크의 각종 장비와 OS에 대한 상태 모니터링 및 관리 정보 제공
TrustNet		PKI	공개키 기반 인증솔루션
		KMS (HMS)	S/W(H/W) 방식의 키 관리 솔루션
		공식 인증 암호화 모듈	대한민국 정부로부터 인증 받은 암호화 모듈(KCMVP)

2022 © PanstarEnterprise & Sotist All rights reserved

TrustNET

2022 © PanstarEnterprise & Sotist All rights reserved

PKI

공개키 기반구조. 인터넷상의 거래 비밀을 보장하면서도 거래 당사자들의 신분을 확인시켜 주는 보안기술
별도의 클라이언트용 프로그램 설치 없이 공개키 방식의 인증서 발급 가능

TrustNET

Public Key Infrastructure

전자상거래 시스템과 같은 정보시스템에 안전성을 부여하며,
네트워크 상에 연결된 사용자와 메시지에 대한 인증기능을
부여하기 위한 공개키 방식을 이용한 전자인증기반 기술 체계.

2022 © PanstarEnterprise & Sotist All rights reserved

제안 배경

Needs

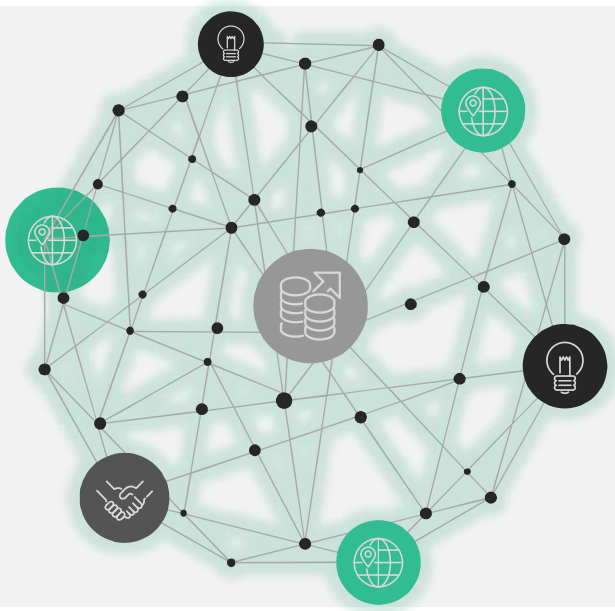
분산 시스템 환경에서의 데이터 교류를 통한 비즈니스 활성화에 따라 정보보호의 필요성이 대두되고,
다양한 통신 환경 및 단말기를 통한 정보 교류는 언제나 정보유출의 위험성을 내포하고 있음
안전한 정보교류를 통한 비즈니스 활성화를 위해 데이터 무결성 및 기밀성이 보장되어야 하고 확장성을 용이하게 할 수 있는
보안 인프라가 필요함

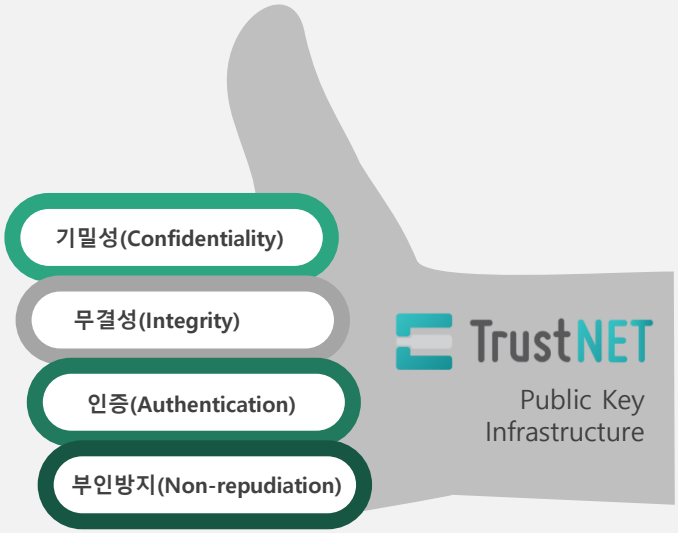
배 경

인터넷발전,
인터넷을 통한 개인신상정보,
기업 정보자산의 유통정보 증가

문제점

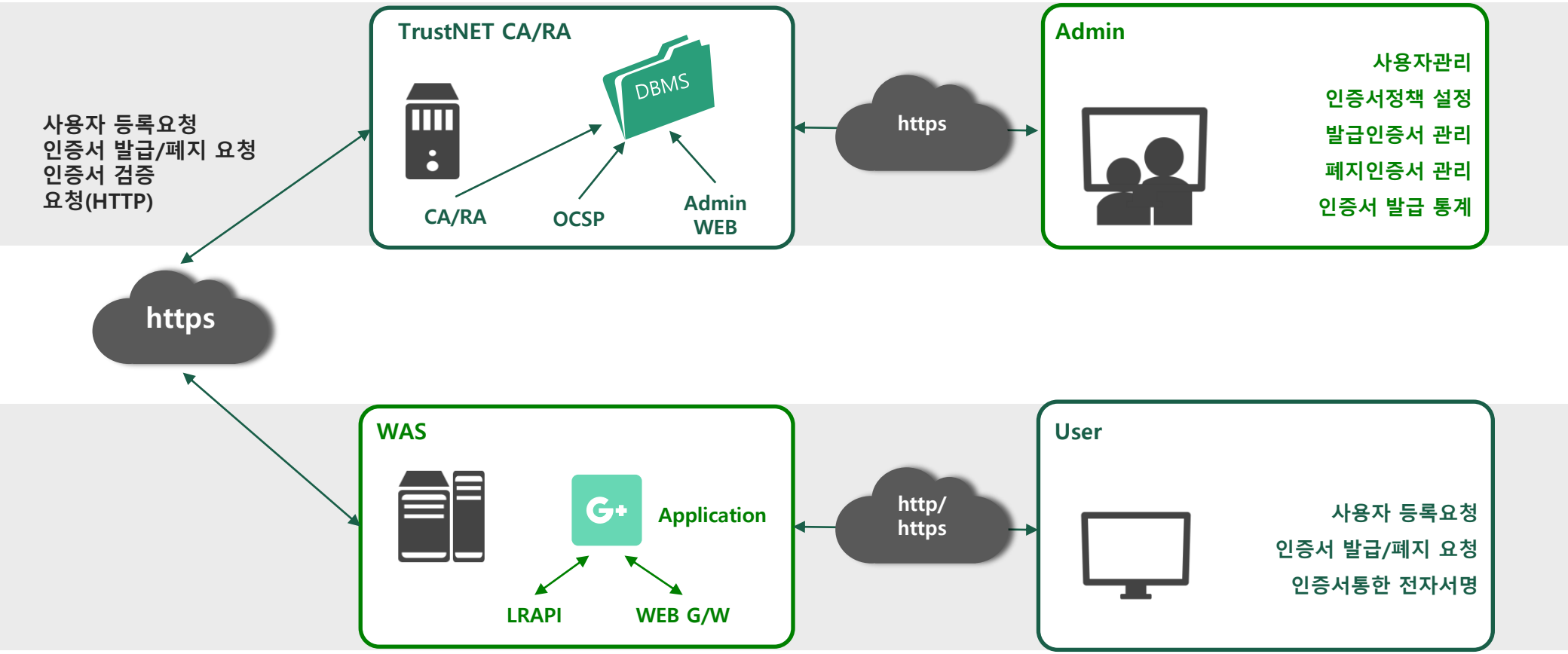
통신내용도청,
불법사용자데이터변조,
송수신사실 부인





2022 © PanstarEnterprise & Sotist All rights reserved

제품 구성도



PanStarEnterprise
2022 © PanstarEnterprise & Sotist All rights reserved
SoTIST

제품 구성 및 주요기능

구분			기능	비고
서버	**TrustNET CA/RA**		사용자정보의 등록 및 인증서의 생성, 폐지, 효력정지 기능을 수행하는 PKI 핵심 시스템	TrustNET에서는 인증서 유효성 검증을 OCSP 를 기본으로 함
	TrustNET OCSP		실시간으로 인증서 유효성을 검증하는 시스템	CA, OCSP 서버가 핸들링하는 RDB 별도 필요
	관리자 Web Console		인증서 정책 설정, 발급, 폐기 및 통계 정보 확인	CRL 사용 시 LDAP 별도 필요
응용	**TrustNET LRAPI, Web Gateway**	ActiveX client	TrustNET CA/RA 서버에 인증서 발급을 위해 사용자 등록, 사용자 삭제, 인증서 폐지 기능 수행을 위한 라이브러리	TrustNET CA client가 설치되어 있어야 함
클라이언트	**TrustNET CA-Client For PC**	ActiveX client	사용자 PC에 설치되는 컨트롤로 Windows IE 환경에서 인증서 발급 및 관리를 수행	
		Multi client	사용자 PC에 설치되는 컨트롤로 Windows, Linux, Mac 환경에서 인증서 발급 및 관리를 수행	Non Plug-in Client 사용 IE는 Active X를 사용하기도 함
	TrustNET CA-Client For Mobile	Internal Storage	내부 저장소에 인증서, 개인키를 저장하며 Application 형태로 제공되며 VPN App 또는 해당 인증서가 필요한 다른 App 에서 인증서 사용 가능	Android, iOS 환경 지원
		External Storage	외부 저장소에 인증서, 개인키를 저장하며 Library 형태로 제공되며 인증서 발급 및 관리를 수행	Android, iOS 환경 지원
	TrustNET Non-Native CA-Client		별도의 클라이언트 모듈 설치 없이 웹에서 클라이언트 기능 수행	HTML5를 지원하는 모든 웹브라우저

PanStarEnterprise
2022 © PanstarEnterprise & Sotist All rights reserved
SoTIST

TrustNET Client Toolkit

구분		기능
Toolkit	**TrustNET Toolkit for JAVA**	C/S Application 운영 환경에 적용하는 보안 라이브러리
	TrustNET Toolkit for C/S	자바통합환경에 적용하는 보안 자바 클래스
	TrustNET Toolkit for ASP	NT용 ASP 웹서버 환경에 적용하는 보안 라이브러리
	TrustNET Toolkit for .NET	.NET Application 환경에 적용하는 보안 라이브러리
	TrustNET Toolkit for PHP	PHP 기반의 웹 환경에 적용하는 보안 라이브러리

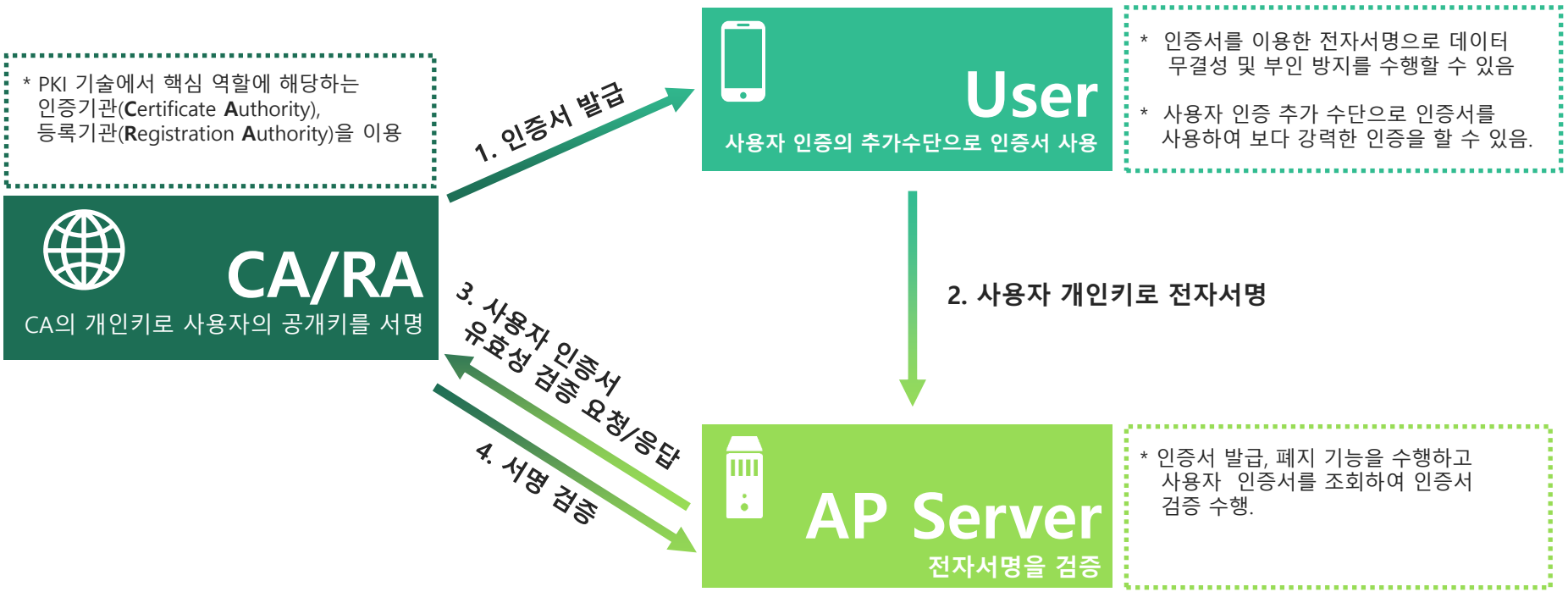
2022 © PanstarEnterprise & Sotist All rights reserved

TrustNET 구성 요소별 용도 및 기능

2022 © PanstarEnterprise & Sotist All rights reserved

용도

- 사용자의 정보 등록을 통해 사용자 DN을 부여하고 인증서 발급을 위한 참조번호, 인가코드를 발행
- 국제 표준 기술 및 최신 기술 적극 반영



PanStarEnterprise
2022 © PanstarEnterprise & Sotist All rights reserved
SoTIST

주요 기능

인증서 관리 기능

모든 인증서의 발급, 재발급, 폐지 기능
RFC 2510 CMP 를 이용한 인증서 관리 기능
DBMS 종류에 상관없이 인증서 저장 관리 기능
(별도 DBMS 를 사용하지 않을 경우 MariaDB 사용)
LDAP 서버 연동을 통한 인증서 게시 기능

인증서 정책 설정 기능

인증서 유효기간, 키길이, 키사용에 대한 설정 기능
1인 1인증서 또는 1인 다 인증서 정책 설정 기능
인증서 보존 기간에 대한 설정 기능
CRL 갱신 주기 설정 기능

CRL 생성 및 관리 지원

인증서 유효성 검증을 위해 OCSP를 기본으로 제공하고 있으나 별도 요청에 의한 CRL 생성 및 LDAP 게시 기능 제공
CRL 갱신 주기 설정에 따라 주기적으로 갱신되며,
CRL 게시 위치를 인증서에 첨부함

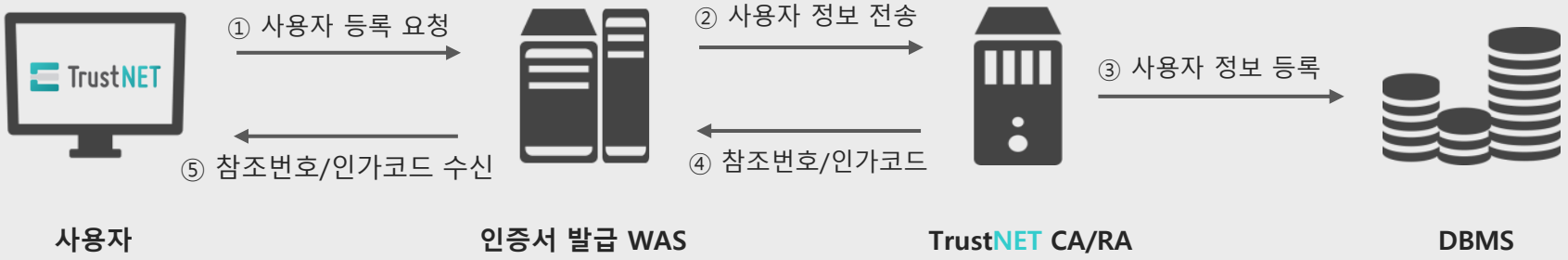
사용자 관리 및 통계

사용자를 구분하여 등록, 삭제 기능
인증서 정보(상태, SN, DN 등) 조회 및
퇴사 등으로 인한 인증서 폐지 기능 제공
월별 사용자 등록 통계 기능
월별 인증서 발급 및 폐지 통계 기능

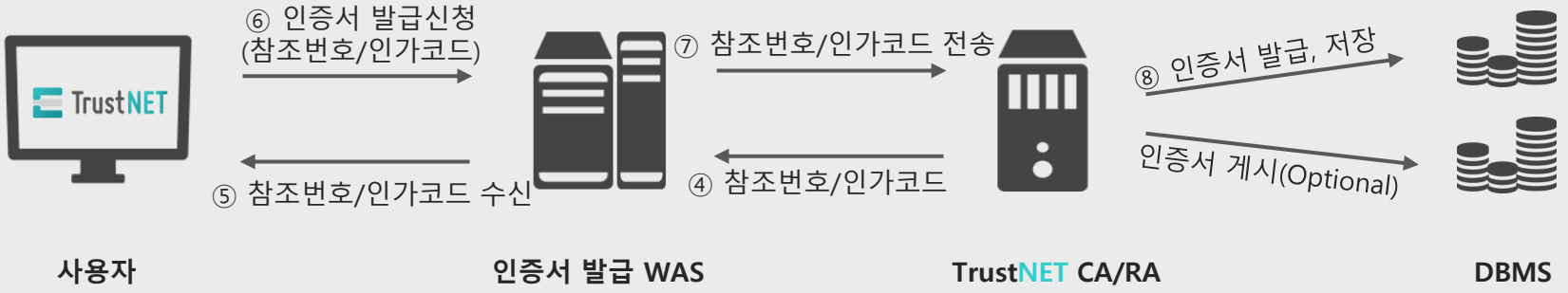
2022 © PanstarEnterprise & Sotist All rights reserved

인증서 발급 절차

사용자 등록



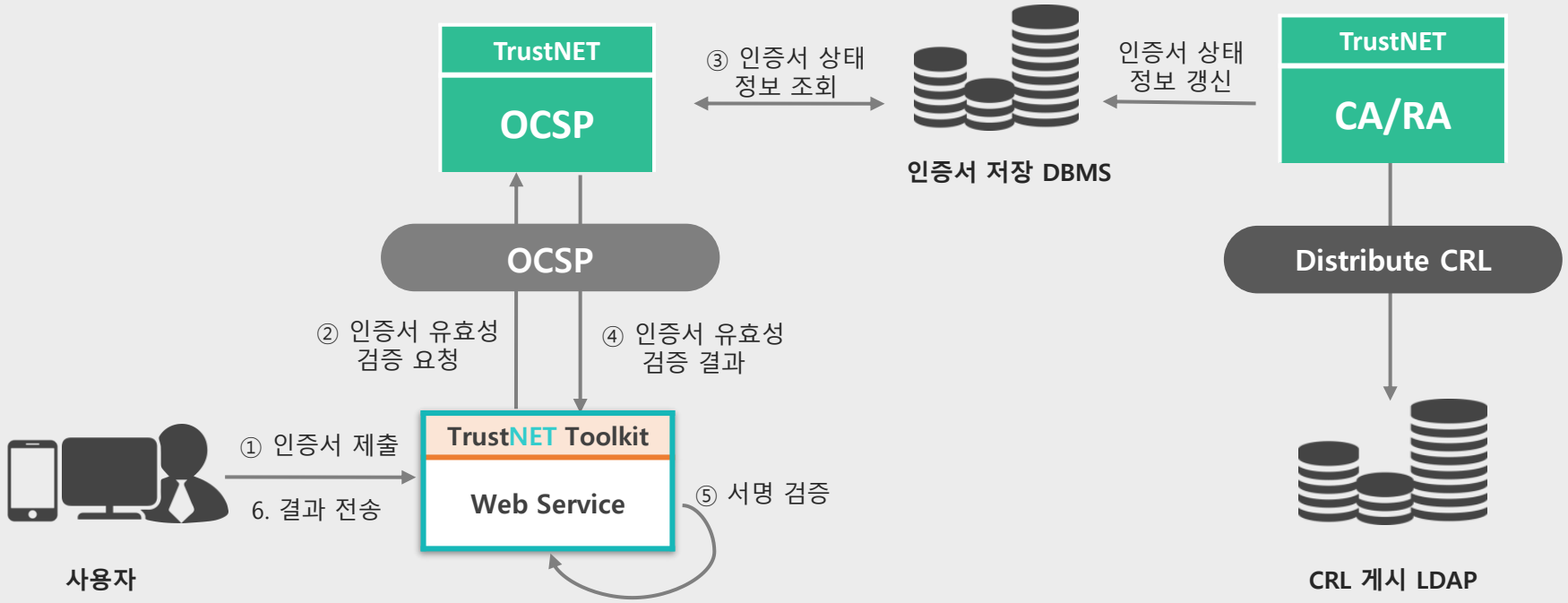
인증서 발급



2022 © PanstarEnterprise & Sotist All rights reserved

용도

- OCSP는 CRL (인증서 폐기 리스트)요청 없이 인증서의 유효성을 실시간으로 검증할 수 있는 시스템
- 고객사의 요청으로 LDAP 구성을 하여 CRL 검증을 할 수 있는 기능도 제공



2022 © PanstarEnterprise & Sotist All rights reserved

주요 기능

- 인증서의 유효성을 **실시간으로 검증** 할 수 있는 시스템

실시간 인증서 상태 확인

- ✓ OCSP 검증 요청에 대하여 검증 요청 인증서를 실시간으로 상태를 확인하는 기능
- ✓ 폐기된 인증서에 대한 폐기 일시 및 폐기 사유 정보를 구할 수 있음
- ✓ 인증서 유효성 검증 실패에 대한 인증서의 실패 원인을 로그에 기록하는 기능

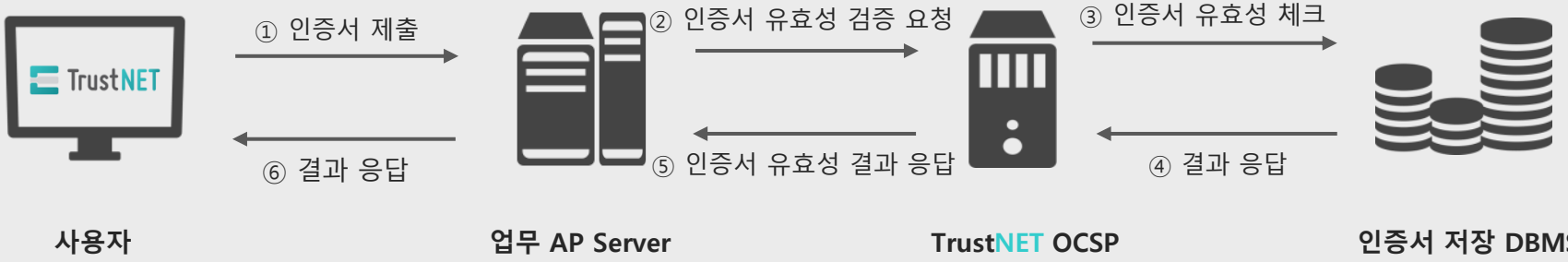
OCSP 정보 검증 기능

- ✓ OCSP 요청 정보 자체에 대한 서명 확인 기능
- ✓ OCSP 요청자의 인증서를 발급기관의 공개키로 검증하여 발급기관에서 서명한 인증서인지를 검증
- ✓ OCSP 요청자의 인증서가 유효한 인증서인지 발급기관 DB 정보와 비교해 발급자의 인증서가 종속된 인증기관의 인증서 인지 확인
- ✓ 검증할 인증서의 발급자 정보를 발급기관의 발급 인증서와 비교하여 발급기관에서 발급된 인증서인지를 검증하는 기능

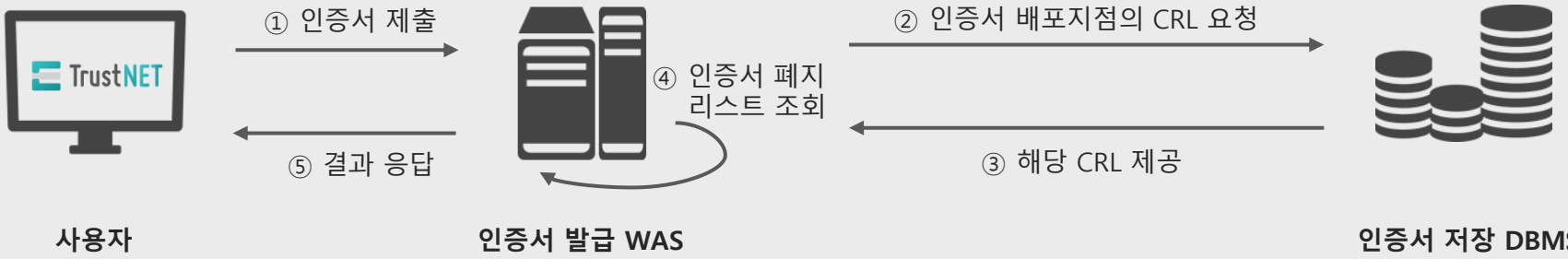
2022 © PanstarEnterprise & Sotist All rights reserved

인증서 검증 절차

OCSP 검증



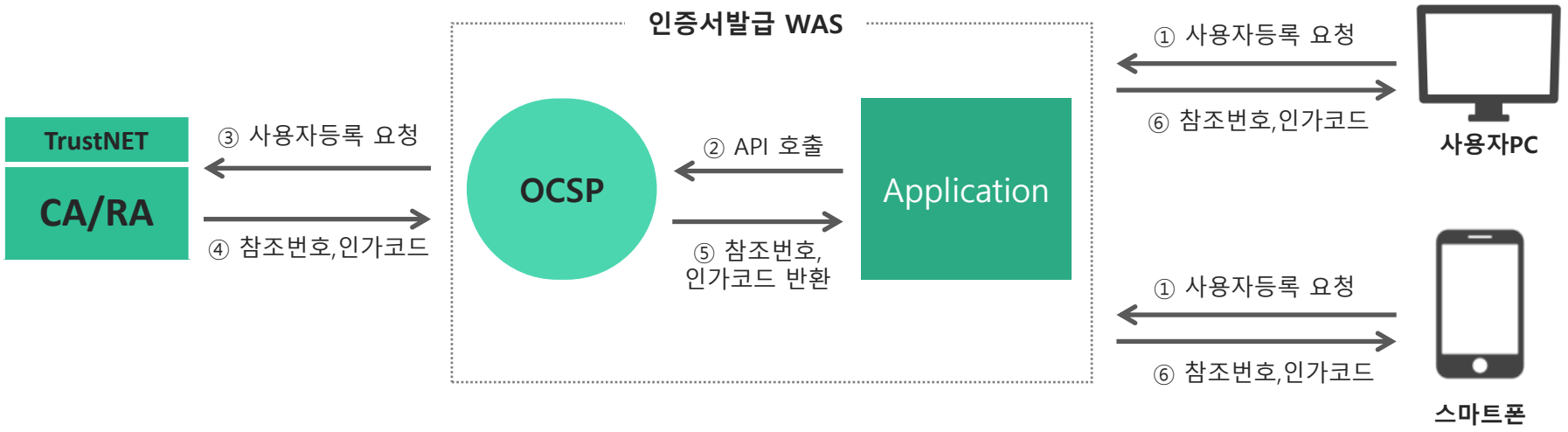
CRL 검증



2022 © PanstarEnterprise & Sotist All rights reserved

LRAPI 용도

- TrustNET CA/RA 서버에 인증서 발급을 위해 사용자 등록, 사용자 삭제, 인증서 폐지의 기능 수행을 위한 API 라이브러리 형태의 제품고객사의 요청으로 LDAP 구성을 하여 CRL 검증을 할 수 있는 기능도 제공
- 인증서 발급을 위한 웹 화면 제작 시 응용프로그램에서 각 기능에 해당하는 API를 호출하여 사용



2022 © PanstarEnterprise & Sotist All rights reserved

주요 기능

- TrustNET CA/RA 서버에서 인증서 발급을 위해 필요한 작업을 수행할 수 있도록 **API 기능 제공**

실시간 인증서 상태 확인

- ✓ TrustNET CA/RA 서버와의 암호화(https) 통신
- ✓ TrustNET CA/RA 서버에 사용자 등록/재등록, 삭제 요청
- ✓ TrustNET CA/RA 서버에 인증서 폐지 요청
- ✓ JAVA 1.3 이상의 모든 환경에서 사용 가능

OCSP 정보 검증 기능

- ✓ TrustNET CA/RA 서버와의 암호화(https) 통신
- ✓ TrustNET CA/RA 서버 응답에 대해 TrustNET CA Client 에 무결성 검증 요청
- ✓ 사용자 등록 결과값인 참조번호, 인가코드를 이용하여 인증서를 발급 및 재발급
- ✓ 클라이언트에는 CA Client 가 설치되어 동작되어야 함
- ✓ JAVA 1.3 이상의 모든 환경에서 사용 가능

2022 © PanstarEnterprise & Sotist All rights reserved

PC Client

ActiveX Client

- ✓ ActiveX 로 제작 및 배포
- ✓ Windows Internet Explore 에서만 사용가능
- ✓ 사설 인증서를 발급받아 PC내의 File 형태로 저장
- ✓ 발급받은 사설인증서의 관리 기능 지원

TrustNET CA PC Client

발급된 인증서는 로컬 디렉토리에 File 형태로 보관되며, Web Browser 또는 OS 종류에 따라 ActiveX / Non Plug-in 방식 2가지로 나뉩니다.

Windows – Internet Explore 환경에서는 ActiveX 모듈이 설치가 되며, 그 외 브라우저 (chrome, safari, opera, firefox, Edge) 또는 OS 에서는 Non Plug-in 모듈이 설치되어 동작합니다. 각 모듈이 지원하는 기능은 동일합니다.

ActiveX Non Plug-in 2 Ways

Non Plug-in Client

- ✓ Non Plug-in 방식의 모듈 제작 및 배포
- ✓ Internet Explore 환경을 포함한 브라우저와 Windows 와 타 OS (Linux, MacOS) 환경에서 사용
- ✓ 사설 인증서를 발급받아 PC내 File 형태로 저장
- ✓ 발급받은 사설인증서의 관리 기능 지원

2022 © PanstarEnterprise & Sotist All rights reserved

Mobile Client

Internal Storage Ver.

사설인증서 발급
내부 저장소에 인증서 및 개인키 저장
VPN App 또는 해당 인증서가 필요한 다른 App에서 인증서 사용 가능

TrustNET CA Mobile Client는 스마트 폰 모바일 앱에 사설인증서를 발급 및 관리를 할 수 있는 기능을 제공

발급된 인증서의 저장형태에 따라 Internal Storage / External Storage 2가지 버전으로 나뉘며,

Internal Storage는 클라이언트에서 인증서 발급 후 OS가 인식할 수 있는 내부 저장소에 저장 후 다른 App 또는 OS에서 인증서를 사용할 수 있고,

External Storage는 SD Card 또는 App 내부 자체 폴더를 생성하여 저장하여, 인증서를 사용할 수 있는 기능을 제공합니다.

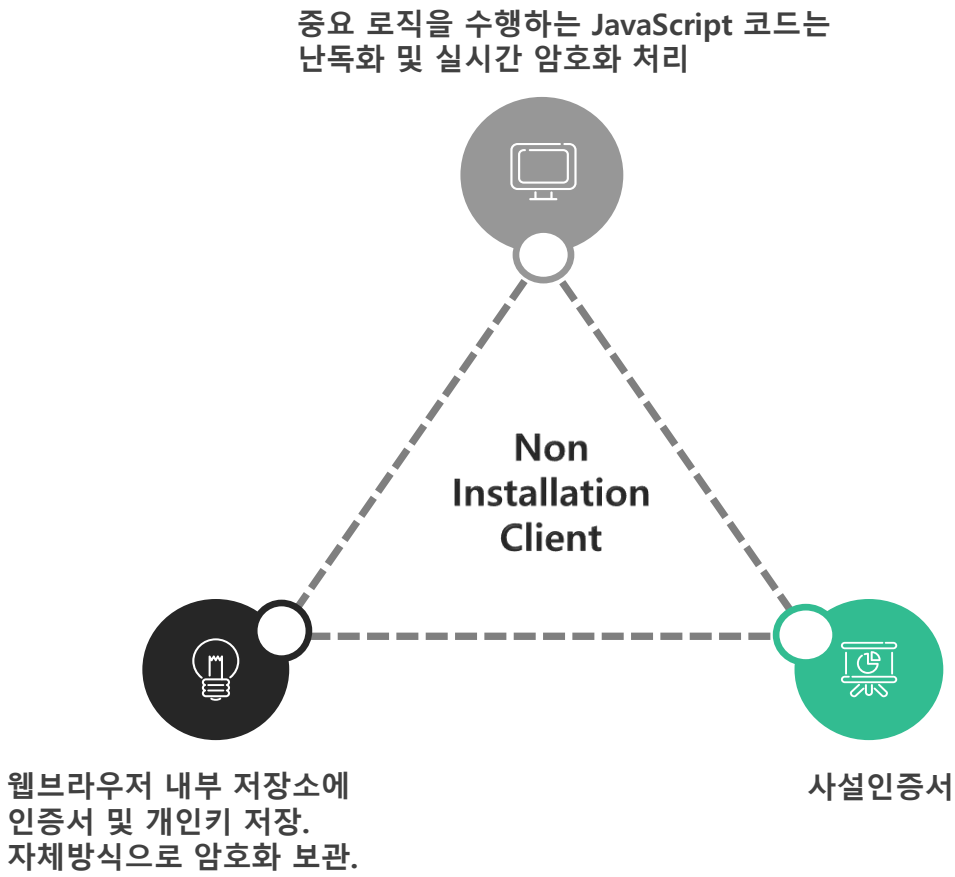
External Storage Ver.

사설인증서 발급
외부 저장소에 인증서 및 개인키 저장
개인키 패스워드 변경
키/인증서 삭제

2022 © PanstarEnterprise & Sotist All rights reserved

Non Installation Client

- JavaScript 와 HTML5 기술을 기반으로 Native 코드 없이 클라이언트 기능을 수행



- TrustNET Non-Native CA-Client는 JavaScript와 HTML5 기술을 이용하여 별도의 모듈을 설치할 필요 없이 PC, 모바일 환경에서 동일하게 사용할 수 있는 클라이언트
- 발급된 인증서는 웹브라우저 내에 저장되어 사용
- 안전하게 암호화되어 저장되므로 노출되거나 오용되거나 할 우려가 없음

2022 © PanstarEnterprise & Sotist All rights reserved

주요 기능

- TrustNET CA/RA 서버에 인증서 발급을 위해 필요한 작업을 수행할 수 있도록 API 기능 제공

PC Client

- ✓ TrustNET CA/RA 서버와의 데이트 무결성 검증 기능
- ✓ 인증서 발급에 필요한 인증서생성요청 정보 생성 및 인증서/개인키 저장 기능
- ✓ 인증서/개인키 삭제 기능, 개인키 비밀번호 변경 기능

Mobile Client

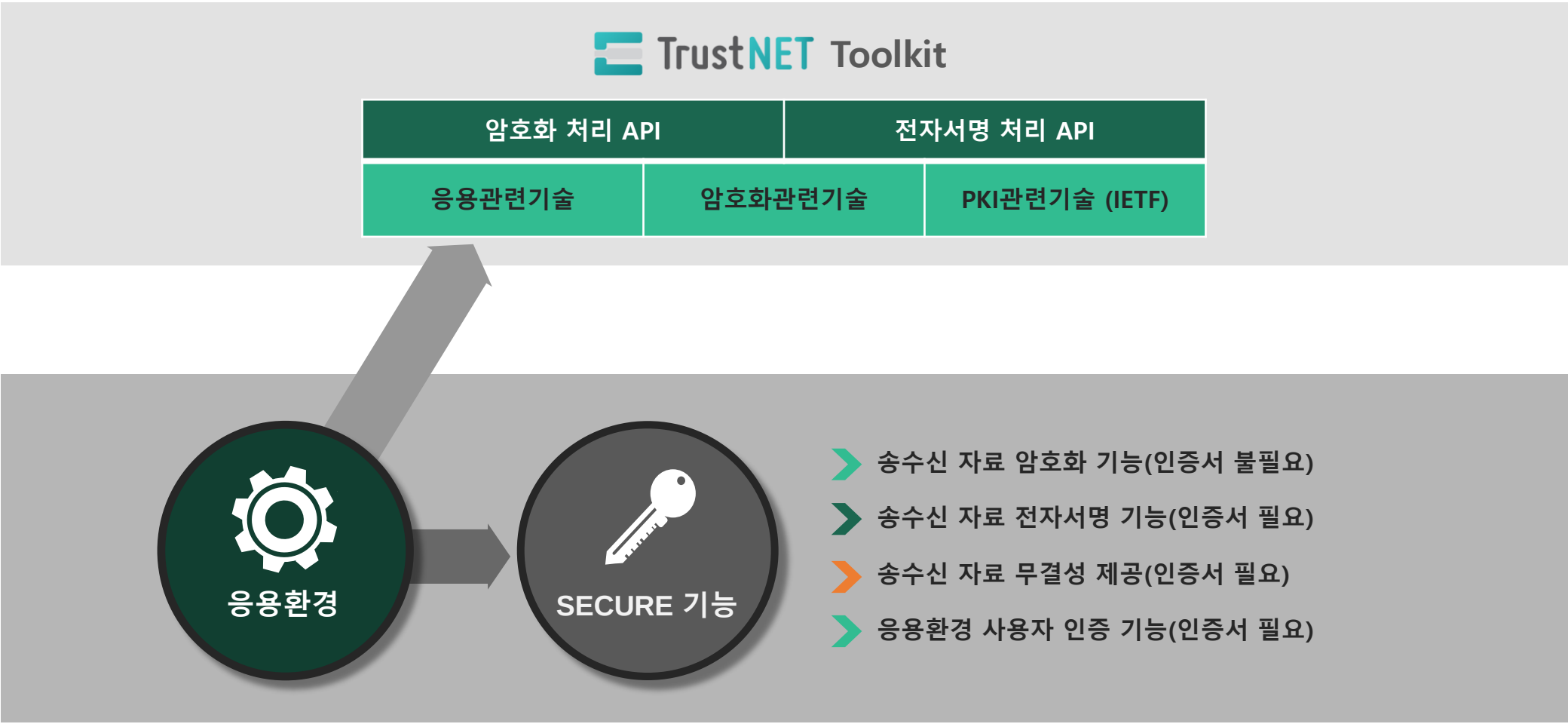
- ✓ TrustNET CA/RA 서버와의 데이트 무결성 검증 기능
- ✓ 인증서 발급에 필요한 인증서생성요청 생성 및 인증서/개인키 저장 기능
- ✓ VPN App 또는 다른 App 에서 인증서를 사용할 수 있도록 내부 저장소에 인증서세트를 저장하는 기능
- ✓ 외부 저장소에 인증서 저장 시 인증서/개인키 삭제 기능, 개인키 비밀번호 변경 기능

Non-Native Client

- ✓ TrustNET CA/RA 서버와의 데이트 무결성 검증 기능
- ✓ 인증서 발급에 필요한 인증서생성요청 생성 및 인증서/개인키 저장 기능
- ✓ 인증서/개인키 삭제 기능, 개인키 비밀번호 변경 기능
- ✓ 인증서 내보내기/들여오기 기능 제공

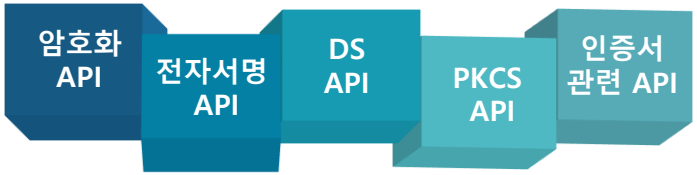
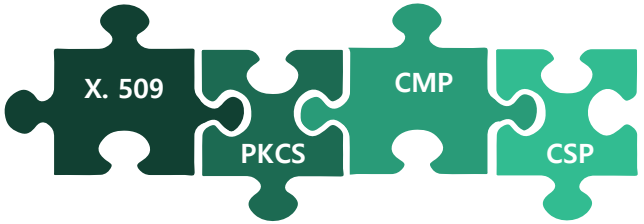
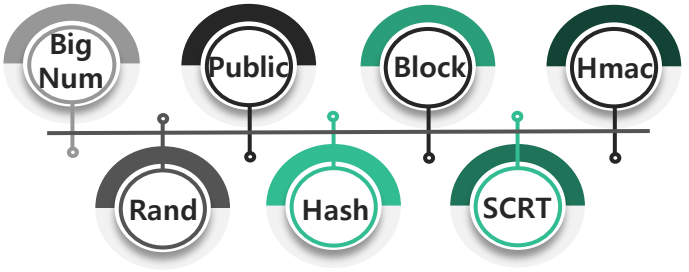
2022 © PanstarEnterprise & Sotist All rights reserved

용도



2022 © PanstarEnterprise & Sotist All rights reserved

제품 구성

구분	Linux	Windows
Toolkit(API)		■ 각종 암호화 알고리즘 제공 (암호,전자서명, 해쉬, 랜덤넘버생성등..)
Cert Library		■ 인증서(X509) 검증,경로검색 기능 ■ 암호문구 처리 기능 ■ 인증서 요청/폐지등 CA인터페이 기능 ■ 암복호자료 인코딩/디코딩
Crypto Library		■ 서버 응용프로그램에서 암복호화 및 ■ 전자서명/검증 등에 대한 기능제공 ■ 레지스터리 및 스마트카드 인터페이스 지원

2022 © PanstarEnterprise & Sotist All rights reserved

주요 기능

구분	기능	특징
암복호화 기능	대칭키 알고리즘 및 공개키 알고리즘을 사용하여 특정 자료를 암호화/복호화 할 수 있는 기능	▪ 특정 자료 및 임의의 자료에 대한 암/복호화 가능 ▪ 첨부화일에 대한 암복호화 기능
전자서명 기능	특정 자료에 대해 전자 서명값을 생성하고 서명값을 검증하는 기능	▪ 첨부화일에 대한 전자서명 기능
암호화 키 생성 및 키 교환 기능	암복호화에 사용되는 세션 키(암호화키)를 안전하게 생성하여 교환(공유)할 수 있는 기능 제공	▪ SSL V3와 TLS V1.1에서의 키 공유 기능과 동일 방식
인증서 I/O 기능	인증서 및 개인 키를 레지스터리, 하드디스크, 스마트카드, USB포트등에 백업 및 복구할 수 있는 기능	▪ 다양한 형식의 저장형식 제공 (PKCS#12, PEM, DER인코딩,디코딩 기능) ▪ PKCS#8형태의 비밀키 관리
PKCS#7 메시지 (전자봉투) 기능	RSA의 표준 형식의 암복호화 및 전자서명 메시지 생성/복구 기능 지원	▪ 보안 메일, XML등에 대한 확장성 제공
인증서 검증기능	각종 인증기관에서 발급한 인증서에 대한 유효성 검증(경로검증) 기능 제공	
전자서명인증센터 인증서 연동 기능	사내 사설인증서 및 전자서명인증센터 인증서를 통합하여 인터페이스 할 수 있는 기능 제공	▪ 6대 전자서명인증센터 발행 인증서 및 전자서명인증센터 상호연동 인증서 처리

2022 © PanstarEnterprise & Sotist All rights reserved

주요 기능

구분	기능	특징
인증서 관리 기능	인증서 발급요청 프로토콜인 CMP주)1 방식에 의한 인증서 발급 신청 및 인증서 폐지, 인증서 갱신, 인증서 비밀번호 변경, 인증서 내보내기, 드려오기 등에 대한 기능 제공	▪ CMP 표준을 따르는 인증기관(전자서명인증센터 포함)은 모두 인터페이스 가능 ▪ 스마트 카드 및 USB 포트 등과의 인터페이스 제공
인증서 GUI(사용자 인터페이스) 기능	저장매체 별 인증서 선택 및 개인키 획득 등을 위한 편리한 화면 인터페이스 기능 제공	▪ 전자서명인증센터 인증서 처리 ▪ 인증서 자동선택 기능 제공
다양한 형태의 클라이언트 제공	ActiveX, 모바일, Non-Native 환경등 다양한 환경에 사용할 수 있는 클라이언트 제품을 제공 가능	▪ PC, 모바일 환경에서 사용되는 거의 모든 환경을 지원 가능 ▪ Non-Native 지원 클라이언트는 HTML5 기능을 지원하는 웹브라우저이어야 함.

주)1 CMP : Certificate Management Protocol

2022 © PanstarEnterprise & Sotist All rights reserved

특징 및 장점

맞춤형 툴킷제공

툴킷 구조가 3계층으로 구조화 되어 있으므로
고객이 원하는 기능만으로 가볍게 재구성 할 수 있음

관련 표준 완벽한 지원

국내 표준 알고리즘 지원, 기타 공개키 알고리즘 및
암호학적 표준의 완벽한 준수

공용 인증서 처리

현재 5개의 전자서명인증센터용 인증서 처리
(암복호화, 전자서명, 인터페이스, 스마트카드 지원)

속도 및 안정성 확보

멀티 쓰레드 환경을 고려한 설계에 따른 안전성 및
처리속도 보장(K전자서명/검증 시 약 0.03초)

다양한 환경 지원

웹To브라우저, 클라이언트To서버, 서버To서버 등
다양한 구조와 응용 환경 지원

다양한 구축 경험

제품사의 다양한 PKI 구축경험
(공용 및 대규모 인증센터구축, 다양한 전자서명인증센터 연동)

2022 © PanstarEnterprise & Sotist All rights reserved

TrustNET 주요 제원

2022 © PanstarEnterprise & Sotist All rights reserved

관련 표준

구분	기술요소	표준안 근거	기술설명
인증	인증서 규격	**X.509 v3, RFC3280**	적용된 기술은 인터넷 표준안인 RFC 2459 의 인증서 규격을 채택하여 다른 PKI 영역과의 연동을 위한 최소한의 기능을 갖춤
	인증서 폐기목록규격	**X.509 v2, RFC3280**	인증서와 같이 인터넷 표준안인 RFC 2459 가 적용되어 업체간 연동을 갖춤
	인증서 관리절차	**RFC 2510, RFC 2511 draft-ietf-pkix-cmp-transport-protocols-01**	인증서 발급/폐기/갱신을 위한 상호 메시지 부분에서 인터넷 표준안인 RFC 2510과 실제 메시지의 전송부분의 인터넷 표준안인 draft-ietf-pkix-cmp-transport-protocols-01 를 적용하여 종단간 연동성을 갖춤
	인증서 검증	**RFC 3280**	인증서의 유효성 검증을 위한 경로인증부분은 인터넷 표준안인 RFC 2459를 준용하여 상호 인증 시에 인증서의 검증에 대한 연동성을 갖춤
	인증서 분배	**RFC 2559, RFC 2585, RFC2587**	발급된 인증서를 배분하기 위해 표준화된 디렉토리 구조를 통한 LDAP 지원 및 HTTP 나 FTP 기타 네트워크 프로토콜을 통한 접근자를 위해 RFC 2585를 적용하여 분배 편의를 도모함
통신프로토콜	CRMF	**RFC 2511**	Certificate Request
	CMP	**RFC 2510**	Internal messaging cross certification
	SSL	**RFC 6101**	Secure Socket Layer
	X.509 PKI-OCSP	**RFC 2560**	Online Certificate Status Protocol
	CMS	**RFC 2630**	Cryptographic Message Syntax
	LDAP	**LDAP**	Communication LDAP
	SQL	**SQL**	Internal Communication
	HTML5	**World Wide Web Consortium**	HTML5

PanStarEnterprise
2022 © PanstarEnterprise & Sotist All rights reserved
SoTIST

관련 표준

구분	기술요소	표준안 근거	기술설명
기술	RSA 암호화	**PKCS #1**	RSA 알고리즘을 이용한 데이터 암호화 및 전자서명 생성과 관련된 업계 표준을 지원
	패스워드 기반 데이터 암호화	**PKCS #5 v2.0**	패스워드 기반의 암호화를 위한 키 유도 함수 PBKDF2 및 8바이트 이상의 블록 암호 키를 이용한 PBES2 를 지원
	인증서 확장 구조	**PKCS #6**	확장된 인증서 구조를 지원하기 위한 업계 표준으로 서명 메시지 등에서 첨부 기능 지원
	전자서명 및 암호데이터	**PKCS #7, RFC 2630, RFC 2634**	공개키 암호화 방식을 이용해 전자서명 메시지 및 암호메시지, 다이제스트 메시지 등의 전자 문서 표준을 지원
	개인키 구조	**PKCS #8**	개인키의 보관 및 이동을 위한 메시지 형식 및 암호화된 개인키 표준을 지원
	인증서 요구 양식	**PKCS #10, RFC 2511**	인증서 발급 요구서 메시지의 표준 구조로 PKCS #10 에 비해 POP 및 구조가 개선된 RFC 2511 추가 지원
	사용자 정보 교환	**PKCS #12**	사용자 개인키 및 인증서 기타 보안자료들의 이동 보관 및 전달 양식 표준으로 PC 에서의 인증서 이동수단을 위해 지원

2022 © PanstarEnterprise & Sotist All rights reserved

지원 환경

제품			지원 환경
서버	TrustNET CA/RA TrustNET OCSP 관리자 Web Console		JAVA 1.7 이상의 모든 OS 환경 지원 DBMS : Oracle, MS-SQL, MySQL, MariaDB, TiberoDB 지원 (그 외 DBMS 는 포팅하여 지원 가능)
응용	TrustNET LRAPI, Web Gateway	ActiveX client	JAVA 1.3 이상의 모든 OS 환경 지원
클라이언트	TrustNET CA-Client For PC	ActiveX client	Browser : Internet Explorer OS : Windows (Windows 8.1 tile UI 제외)
		Multi client	Browser : Chrome, Safari, Opera, Firefox, Edge OS : Windows, Mac, Linux
	TrustNET CA-Client For Mobile	iOS	iOS 6.0 이상
		Android	Android 4.0 (Ice Cream Sandwich) 이상 (Internal Storage Version 기준)
	TrustNET JavaScript CA-Client		HTML5 를 지원하는 모든 OS및 웹브라우저 수정

2022 © PanstarEnterprise & Sotist All rights reserved

주요 공급 실적

PanStarEnterprise
2022 © PanstarEnterprise & Sotist All rights reserved
SoTIST

주요 공급 실적

삼성전자	삼성중공업	삼성SDS	삼성코닝정밀소재
삼성화재	삼성생명	삼성인력개발원	삼성전자서비스
삼성증권	삼성물산	삼성디스플레이	삼성코닝어드밴스드글라스

하나은행	하나캐피탈	하나금융투자
하나카드	하나저축은행	하나금융지주
하나생명	하나자산신탁	하나멤버스

중앙보훈병원	대전보훈병원	한국보훈복지의료공단
인천보훈병원	광주보훈병원	
부산보훈병원	대구보훈병원	

2022 © PanstarEnterprise & Sotist All rights reserved