대규모 데이터에 대한 전자서명 기술 (KIDS)

㈜ 마크애니

KIDS(Keyless Infrastructure for Digital Signature)

- 대규모 데이터 대해 서버 기반으로 무결성 검증 및 시간 증명을 수행하는 기술
- 일반적으로 널리 알려진 블록체인에 기반한 기술

01 기존 PKI에 대한 보완 또는 대체 기술

PKI를 적용하기 어려웠던
분야에도 적용 가능한 기술

02 키에 대한 관리가 필요 없음

Hash Function Cryptography
에 기반하기 때문에 별도의
키 관리가 필요 없음

03 대규모 데이터 처리

이론적으로 최대 초당 5천억개의
전자서명 처리가 가능함

04 서명 유효기간

서명 검증에 대한 유효기간
이 이용되는 해시함수의
보안강도에 기반

MarkAny

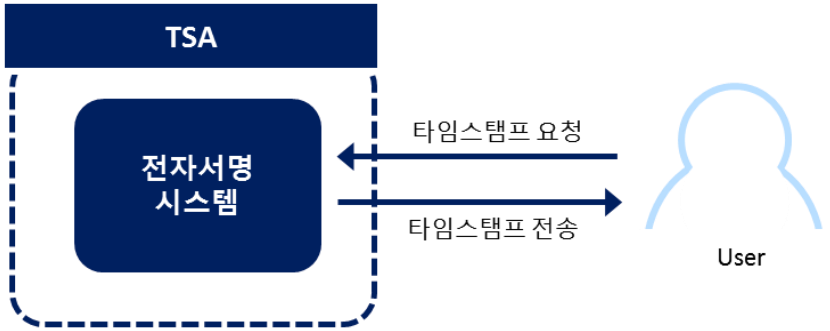
서버기반 전자서명 기술(KIDS)의 특징

- 위변조 확인 가능한 **무결성**, 법적 증빙을 위한 **부인 방지** 기능을 제공하는 서명을 서버에서 대량으로 처리하는 기술(**이론적으로 최대 초당 5천억개**)
  - ✓ **저렴한 서명 비용** : 서명에 키가 필요한 기존 기술과 달리, 저렴하게 서명 처리 가능
  - ✓ **기존 기술 대비 빠른 인증 가능** : IOT, M2M 기기들간의 통신상에서 메시지 인증을 빠르게 처리 가능
  - ✓ **디지털 포렌식 친화성** : 전자적 증거물 효력을 위해, 데이터 생성 시점 부터 증명 가능
  - ✓ **키 관리 비용 없음** : 키를 관리를 위한 기능과 갱신 위한 단말기 회수/교체가 불필요

MarkAny

기존 전자서명 기술의 한계

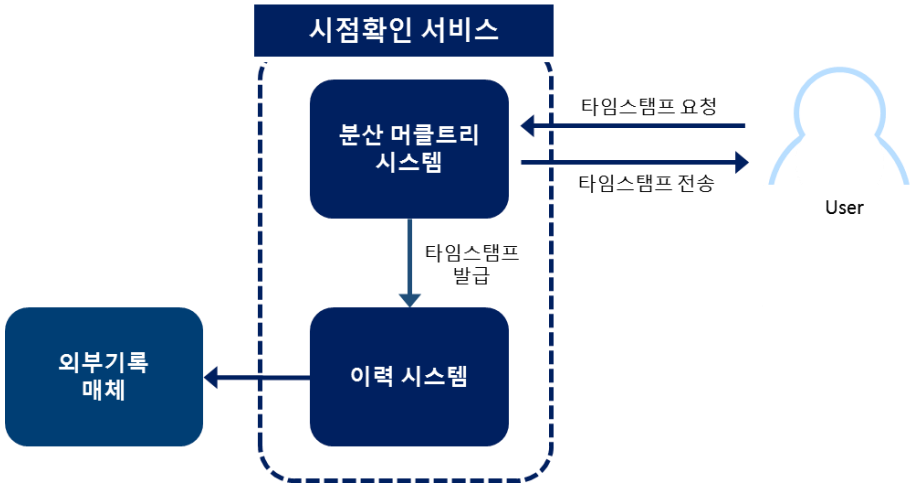
- 국가 공인의 시점확인기관(TSA) 에서 타임스탬프(전자서명)를 발급
- TSA 에서 이용되는 시계에 대한 신뢰를 기반으로 함
- 별도 인증 메커니즘을 통해 개체인증 가능
- **컴퓨팅 자원소모가 큰 비대칭 알고리즘(RSA, ECDSA 등)을 이용**
  = 빅데이터를 대상으로 이용할 수 없음



MarkAny

KIDS : 해시트리를 이용한 타임스탬프

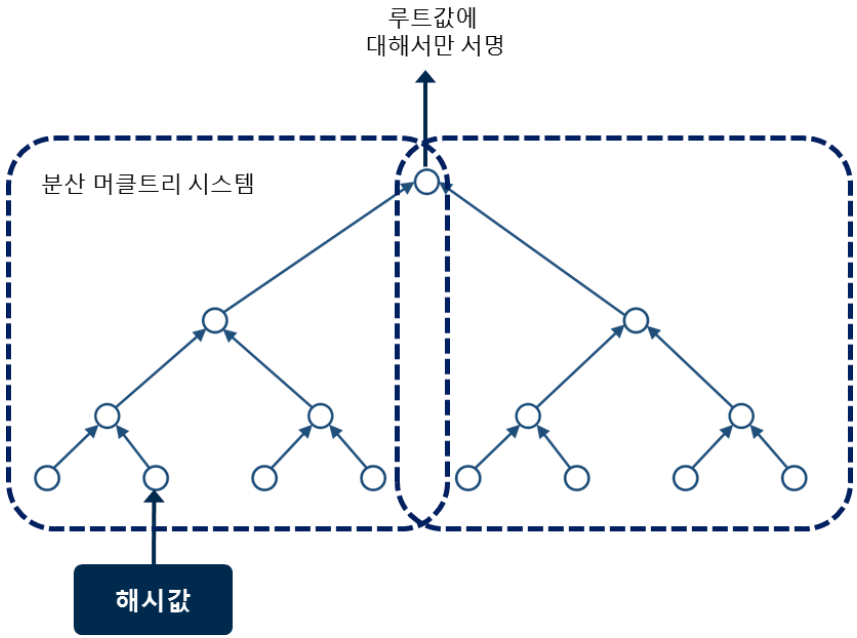
- 적은 컴퓨팅 자원소모 x 쉬운 규모 확장성
  : **대규모로 전자서명을 생성 가능**
- 외부기록 매체의 무결성에 대한 신뢰를 기반으로 함
- 별도의 인증 메커니즘을 통해
  다중 요소 인증
- 장기 보존 가능



MarkAny

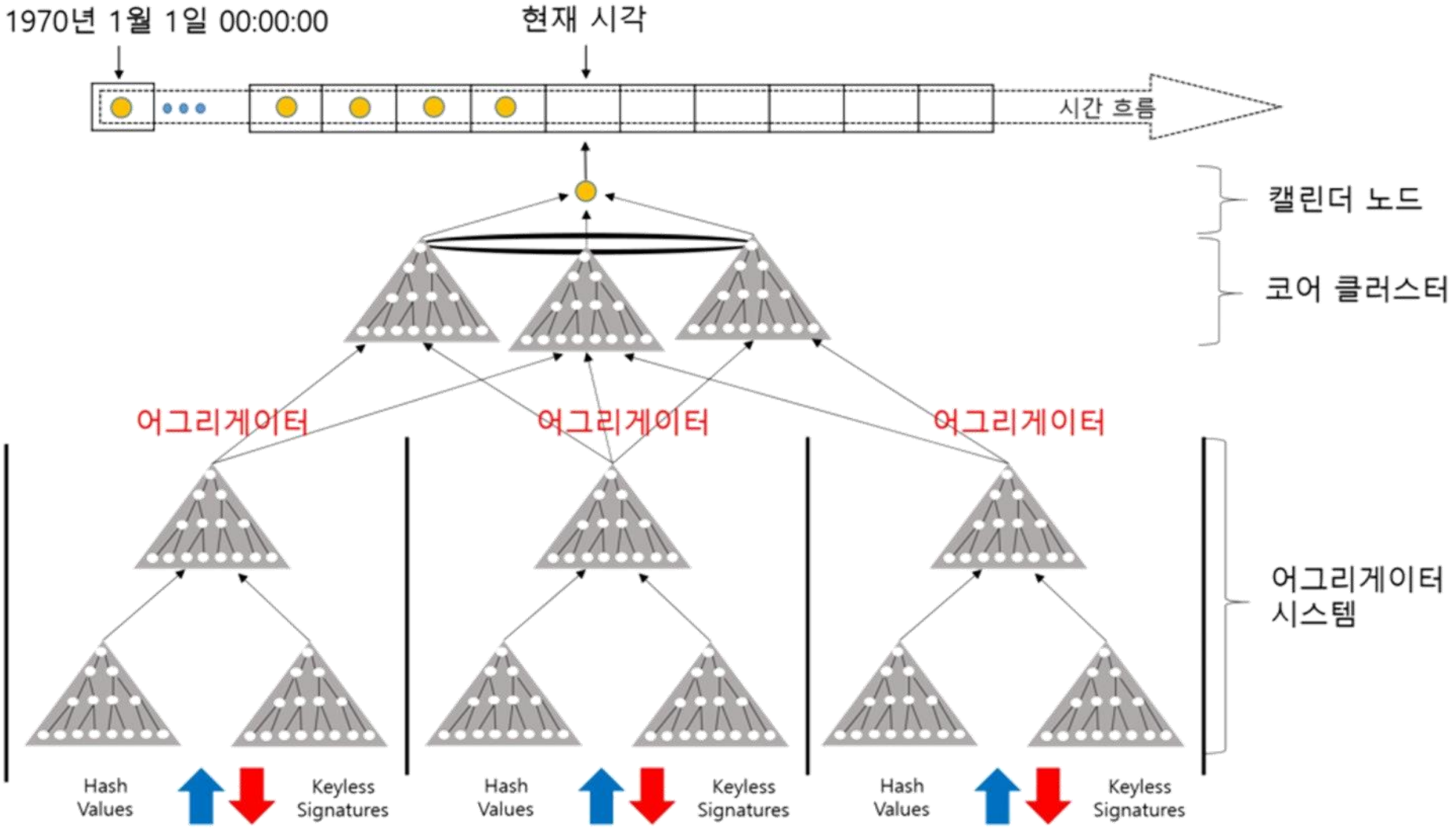
분산 머클트리 시스템

- 머클트리 : 1979년 Merkle 에 의해 고안된 해시값에 의한 이진트리
- 여러 번의 해시, 한번의 전자서명으로
  다수의 전자서명을 동시에 생성
- RSA, ECDSA 에 비해 **1000배**
  이상 빠르게 서명 생성 가능
- 트리의 분산처리가 용이하여
  대규모화가 쉽게 가능



MarkAny

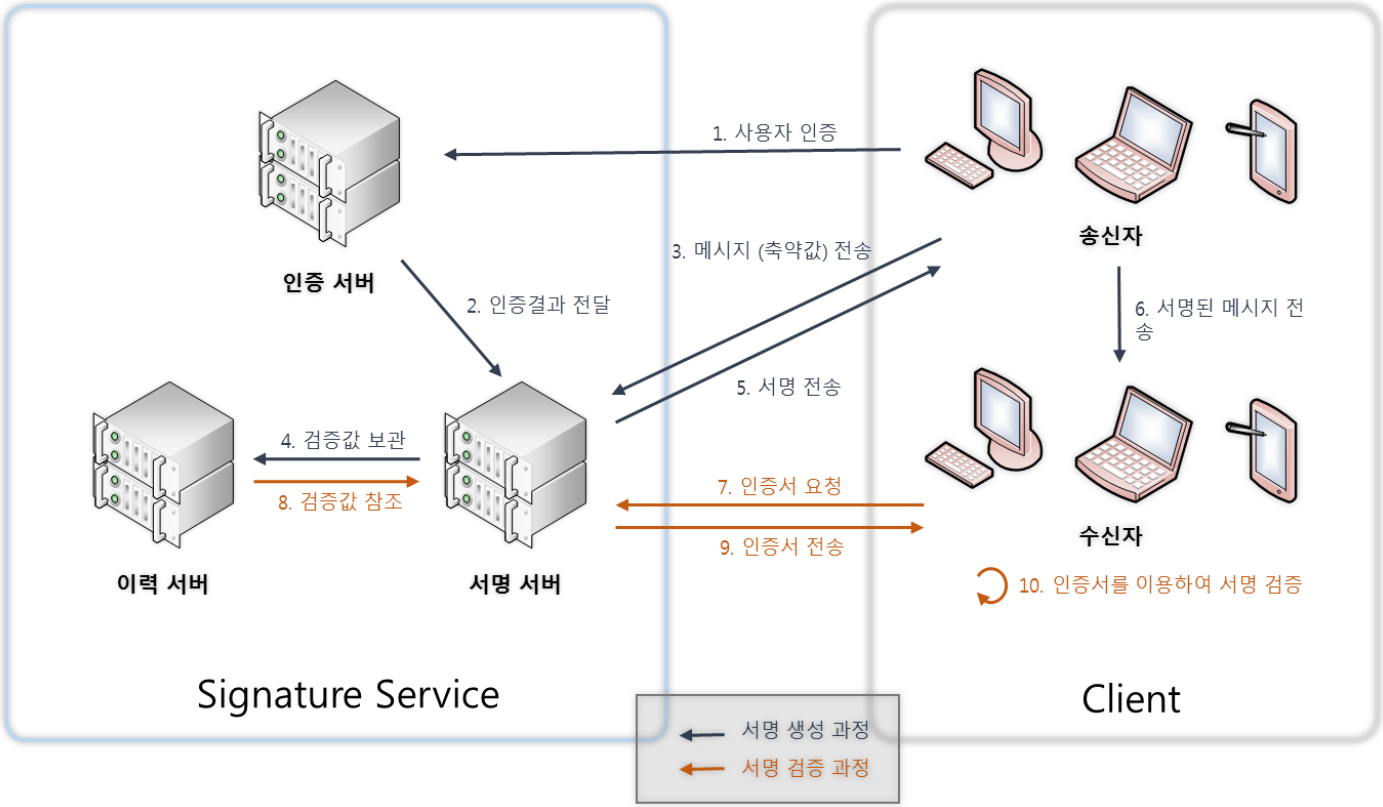
KIDS 내부 구조



MarkAny

서버 구성

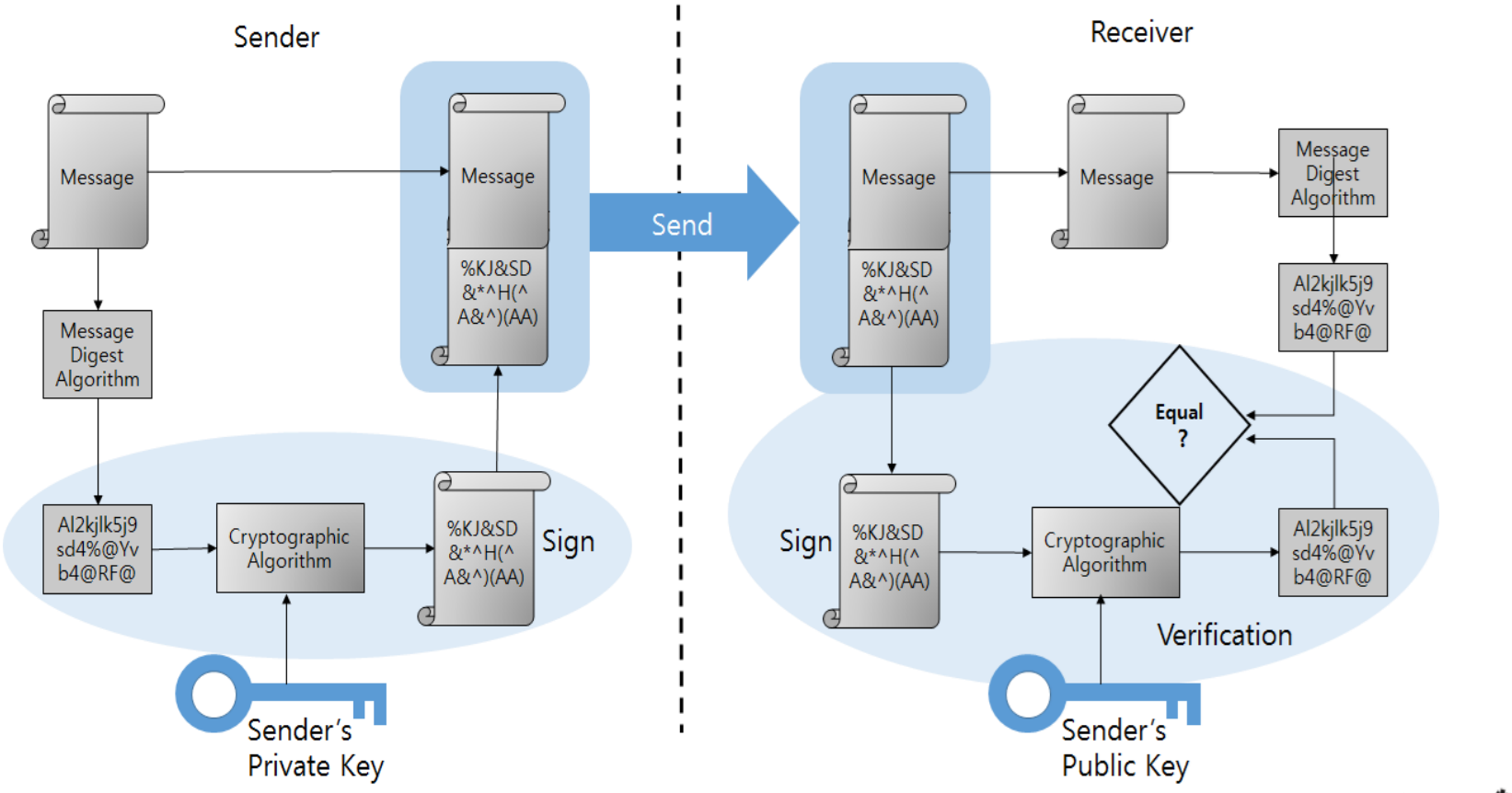
- 서명 서버와 이력 서버로 구성
  - ✓**서명 서버** : 송신자나 송신 단말에서 보낼 메시지 데이터를 서명
  - ✓**이력 서버 :** 서명된 데이터를검증 하기 위한 데이터 관리



MarkAny

전자서명 비교 – PKI 기반

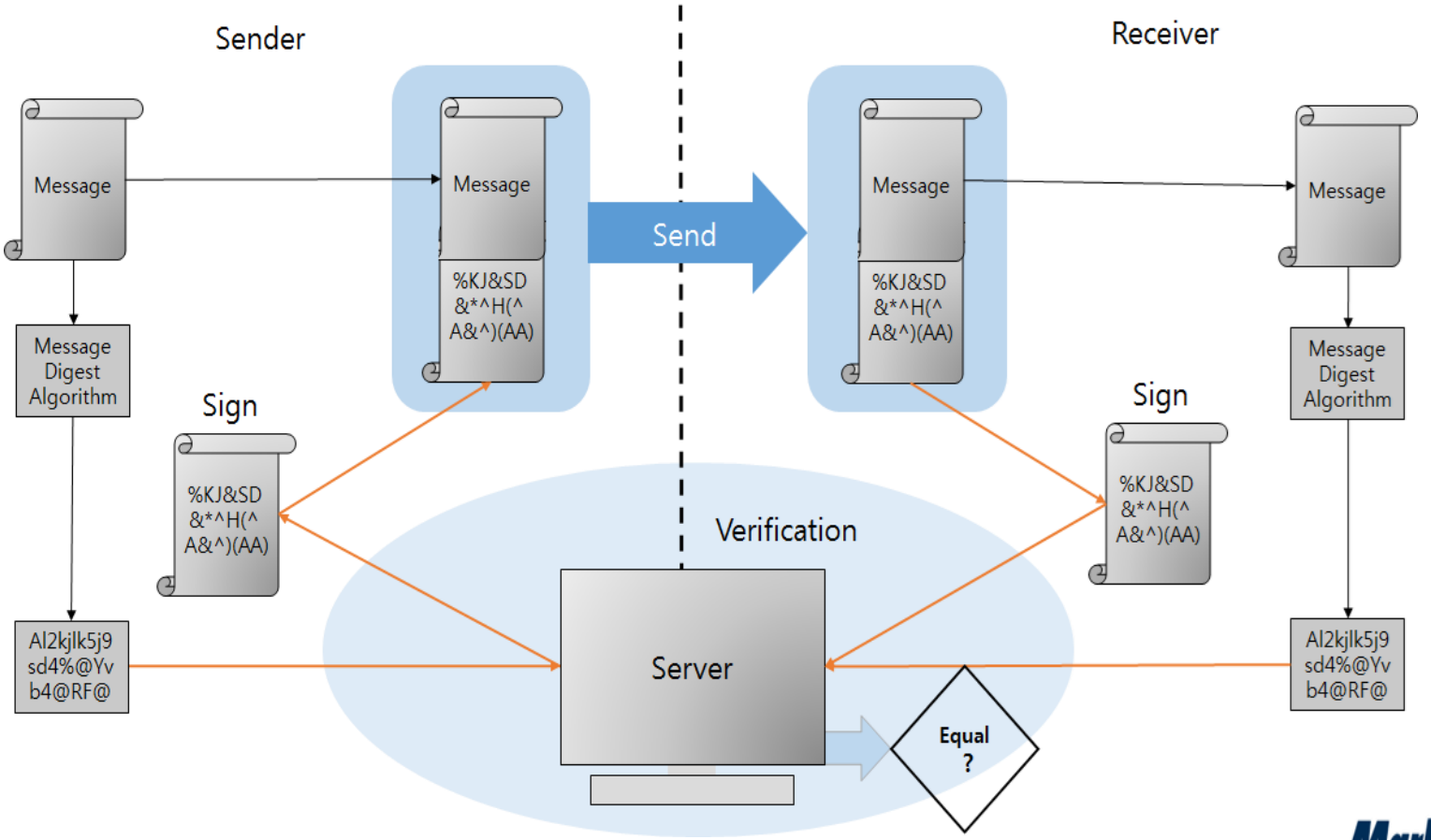
- Sender와 Receiver는 사이의 주고 받는 메시지에 대한 무결성을 확인 하기 위해서 사용하는 Key 값이 서로 다름
  - ✓**Sender의 서명 수행** : 송신자의 Private Key로 보낼 메시지 데이터를 서명
  - ✓**Receiver의 서명 검증** : 서명된 데이터를 검증 하기 위한 송신자의 Public Key를 이용



MarkAny

전자서명 비교 – KIDS 기반

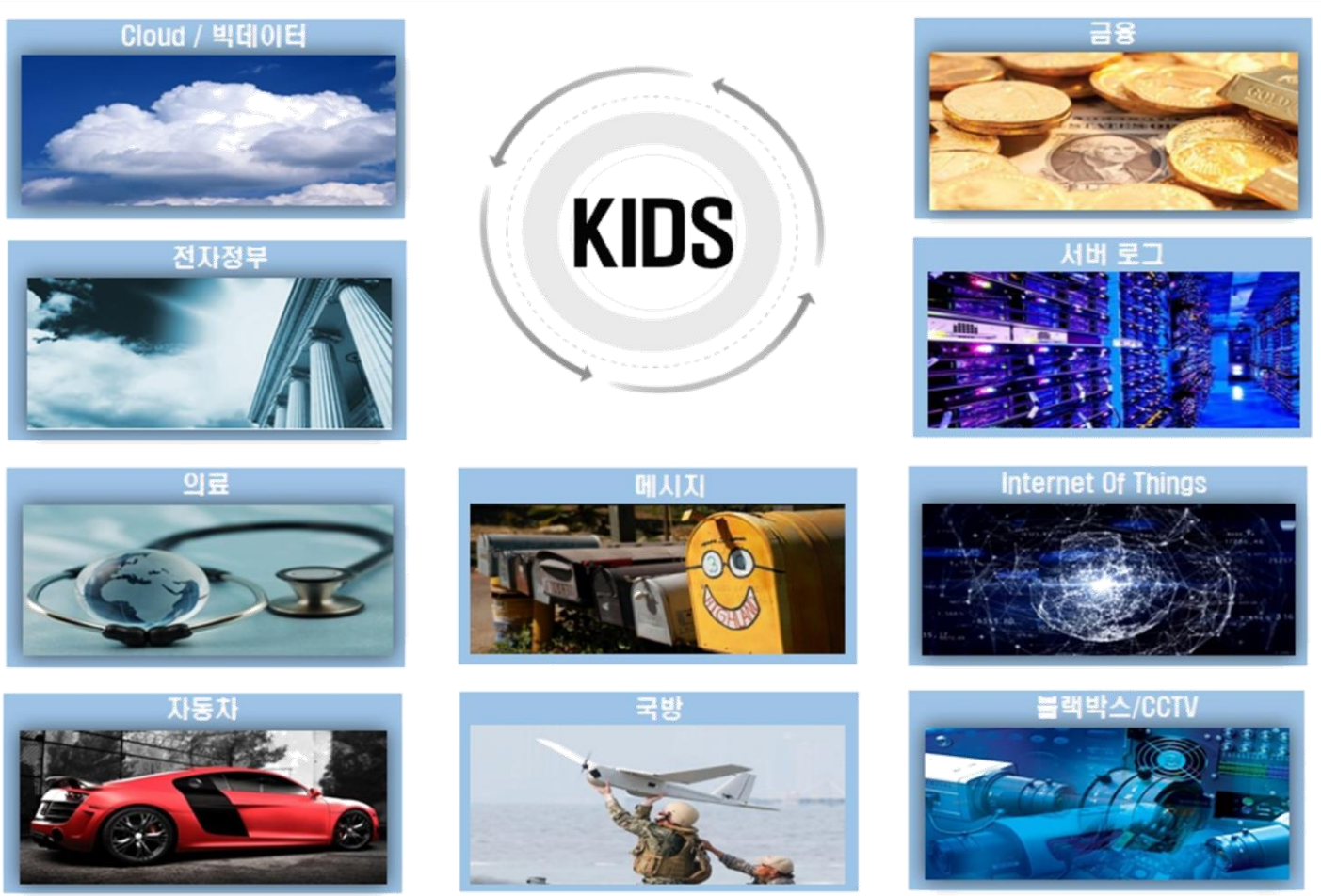
- Sender와 Receiver는 사이의 주고 받는 메시지에 대한 무결성을 확인 하기 위해서 사용하는 Key 값이 서로 다름
  - ✓**Sender의 서명 수행** : 메시지 데이터 해쉬값을 서버에 서명을 요청
  - ✓**Receiver의 서명 검증** : 송신자로 부터 받은 서명을 서버에 검증 요청



MarkAny

KIDS 활용 분야

- 데이터 처리량이 많고, 데이터의 무결성 보장이 필요한 여러 분야에 사용 가능



MarkAny

KIDS 활용분야 – IOT, 자율주행 자동차

IoT / M2M

> IoT / M2M 환경에서 사용되는 기기와 전송된 정보에 대한 KIDS 전자서명을 통하여 안전한 데이터만 기기에서 실행 가능

자동차

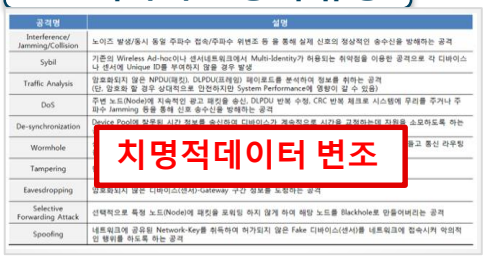
> ECU 등 자동차 제어 신호에 KIDS 전자서명을 적용하여, 제어신호의 무결성을 증명하고 이를 통해 자동차의 안전성을 보장

> 스마트카 환경에서 외부에서 입력되는 데이터에 대한 안전성 보장

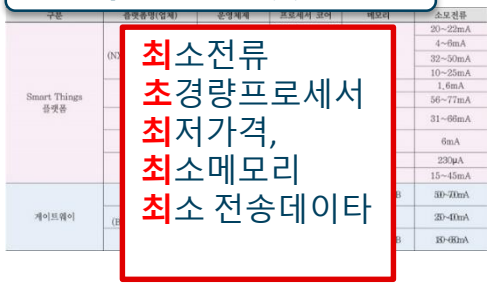
IOT 환경에서의 보안

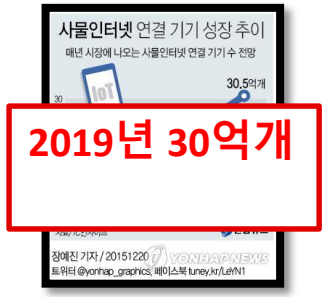
- 고의적 **데이터 위/변조 공격** 가능 : **신뢰성(생성시점, 생성개체, 무결성) 보장**이 중요
- 2019년 30억개의 **엄청난 규모와 H/W 적 한계** : **빈번하면서 대량 처리 가능한 기술 요구**

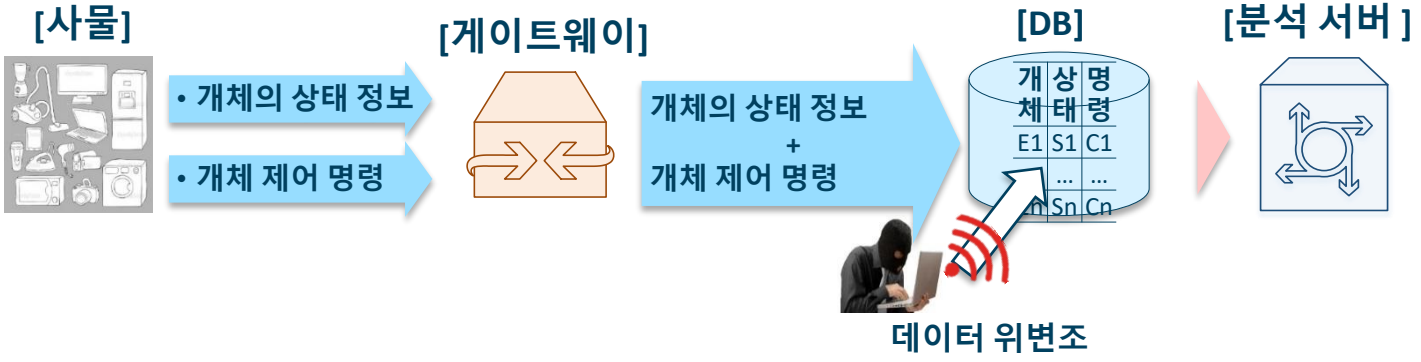
IOT 디바이스 공격 유형



IOT 디바이스 플랫폼 성능

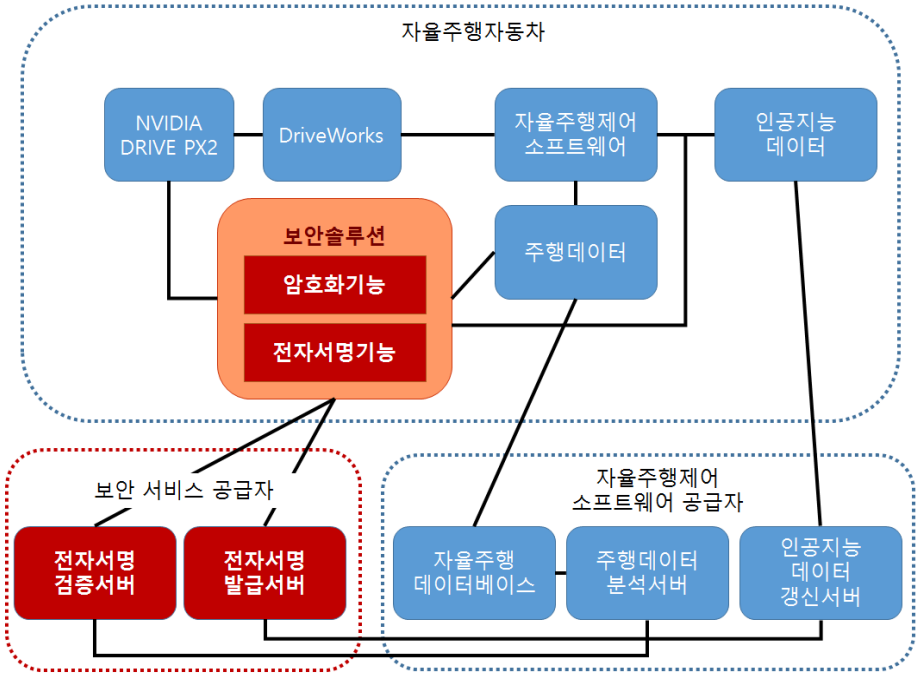






자율주행 자동차 보안

- 스마트카, 커넥티드카에서 사용되는 디지털맵, 센서 데이터, 시스템 로그, 인공지능 데이터에 전자서명을 통해 해킹 방지 : **운전자의 생명보호**



MarkAny

KIDS 활용분야 – 국방, 블랙박스/CCTV

국방

> 무인 항공기, 무선 통신 장비 등의
> 전송 데이터에 KIDS 전자서명을 적용,
> 수신 장비에서 무결성을 확인하고
> 이를 통해 안전한 전시 임무 수행 가능

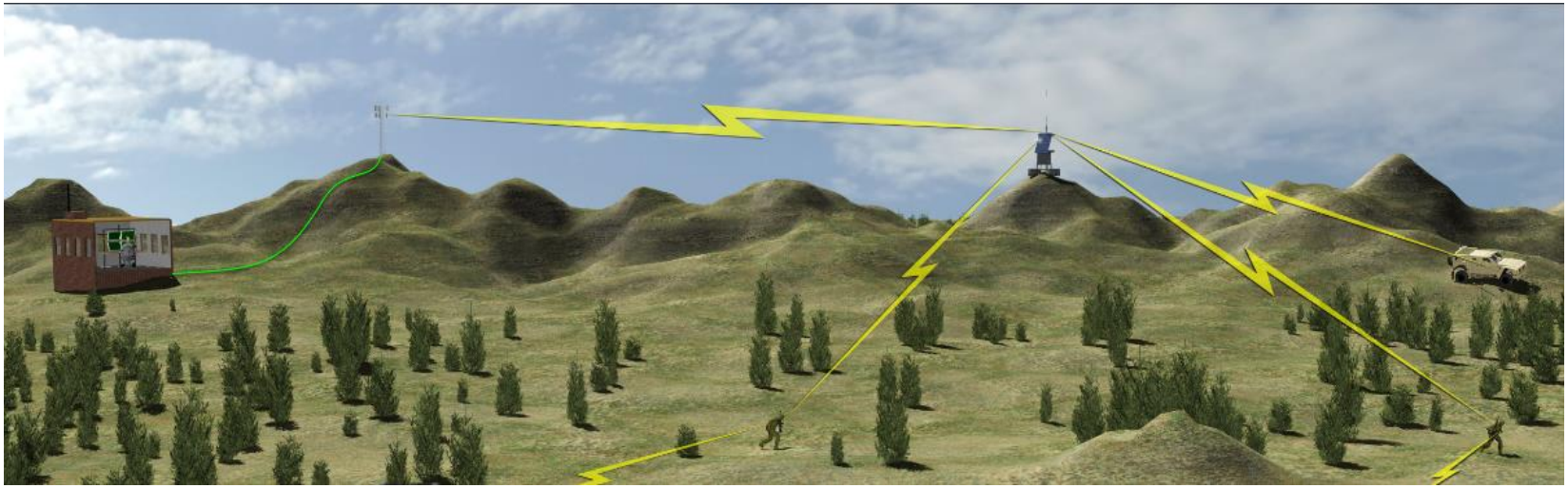
블랙박스 / CCTV

> 블랙박스 및 CCTV에 저장되는 동영상에
> KIDS 전자서명을 적용하여,
> 동영상 데이터의 조작 방지

MarkAny

국방 분야 활용

- 국방과 같은 **국가 차원의 중요 자산의 유출**이나 **내/외부자에 의한 불법적 위변조는 치명적 결과를 초래**
- **국방전투 기동 훈련 체계, 군사정보시스템(MIMS)등**의 데이터 전송/저장/활용시 무결성 보장
- **미국방성 MIMS**의 시스템과 데이터 무결성 확보를 위해 운용중
  - ✓ **DARPA(미국방성 연구개발부분) : 자능형공격(APT) 공격에 대비한 S/W, H/W 무결성 모니터링 시스템**
- **LOCKHEED MARTIN社** : 미사일, 전투기등의 설계 자산 보호

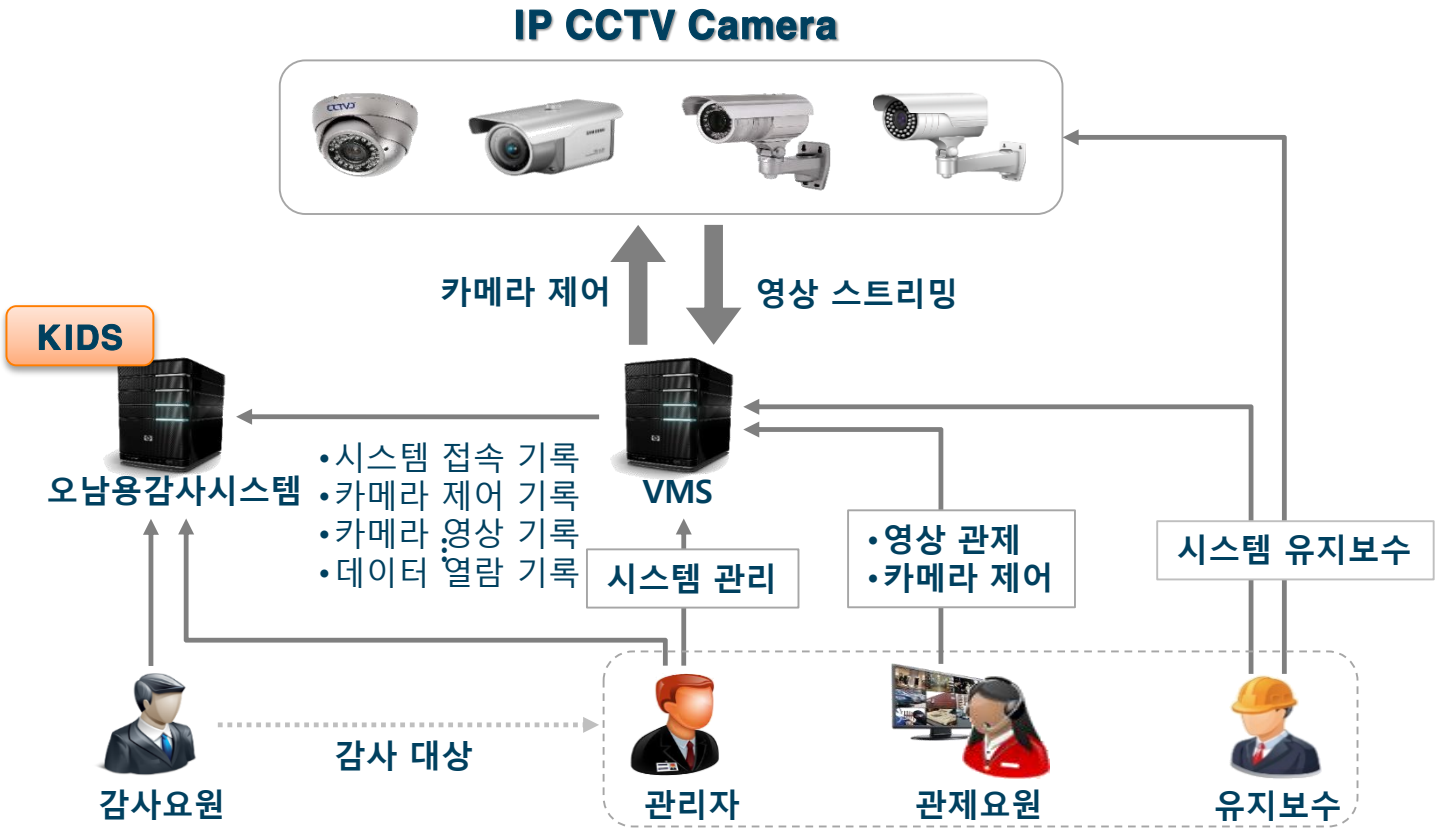


- **전투기동 훈련 체계** : 실시간으로 수집되는 전장 데이터를 분석해 추락·충돌 등의 위험을 예보하고 기종·임무 별 최적 훈련기동을 제시하는 비행훈련 위험예측 시스템
- **군사정보시스템(MIMS)** : 각종 군사정보를 빠르게 저장·분석해 산재된 정보들 간에 어떤 관련성이 있는지 신속히 찾고, 빅데이터 분석 기법을 활용해 신호·전파·영상정보를 해석하면 불확실한 전장 상황을 보다 효과적으로 가시화해 지휘관의 신속한 지휘하는 시스템

MarkAny

CCTV 분야 활용

- CCTV를 통해서 사생활에 대한 심각한 침해사고 발생할 수 있어, **정보주체가 아닌 제3자가 무단으로 CCTV 영상 열람/유출 /변조 발생 방지 요구**
- **관련 시스템상의 수집 데이터에 대한 서명과 검증을 통해 수집 원본 데이터 무결성 검증**



MarkAny

KIDS 활용분야 – 클라우드/빅데이터, 금융

클라우드 / 빅데이터

> 각 접근자가 등록한 데이터에 대한 무결성 보장 및 갱신에 대한 인증을 수행

> 등록된 데이터 사용시 KIDS 전자서명을 통하여 안전한 데이터 임을 보장

금융

> 계좌 거래내역, ATM기기의 거래 내역에 KIDS 전자서명을 적용하여, 거래 후 거래 내역이 조작되지 않았음을 보장

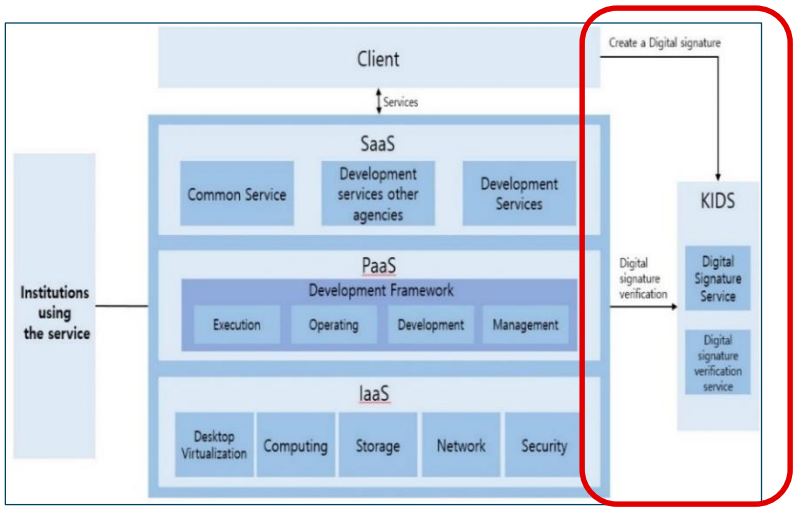
> 인터넷 뱅킹시 KIDS 전자서명을 통해 안전한 사이트인지 확인하고 거래를 함으로써 피싱 예방

MarkAny

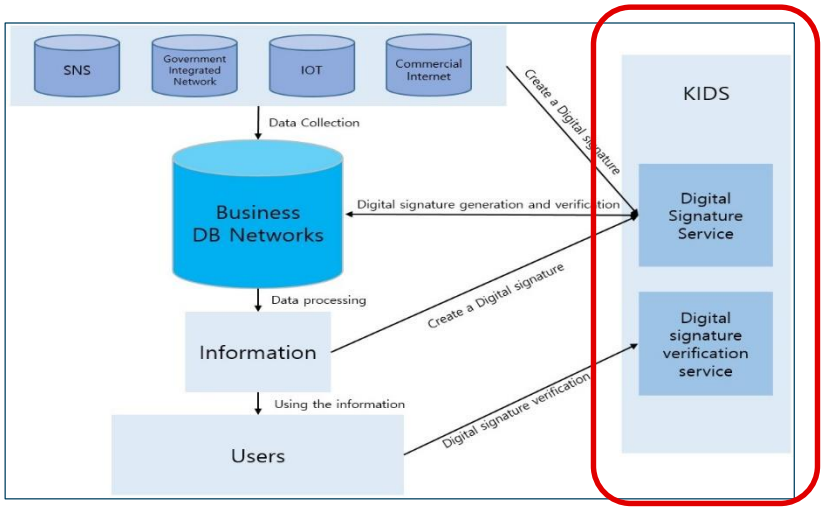
클라우드 및 빅데이터 활용

- 클라우드 시스템과 빅데이터 처리상에, 파일에 대한 무결성과 파일 갱신자에 대한 인증을 통한 **데이터 무결성 보장 기술**로 사용
- 美국방성과 CIA에서 AWS를 Private 클라우드로 쓰고 있는데 이 체계 전반에 적용

클라우드



빅데이터



MarkAny

클라우드 - 의료-헬스케어 산업

- 의료기관 내부에서만 보관·관리하던 전자의무기록을 의료기관 외부장소에서도 관리가 가능 ***의료분야 클라우드 규제개선(보건복지부고시_제2016-140호)**
- '개인 의료정보 공유 클라우드 포털 구축' 이 진행 中
- 에스토니아에서는 블록체인 기술로 헬스케어 클라우드의 데이터 무결성을 보장

Estonia partners with Guardtime to secure 1 million health records with blockchain technology - 2016년 3월

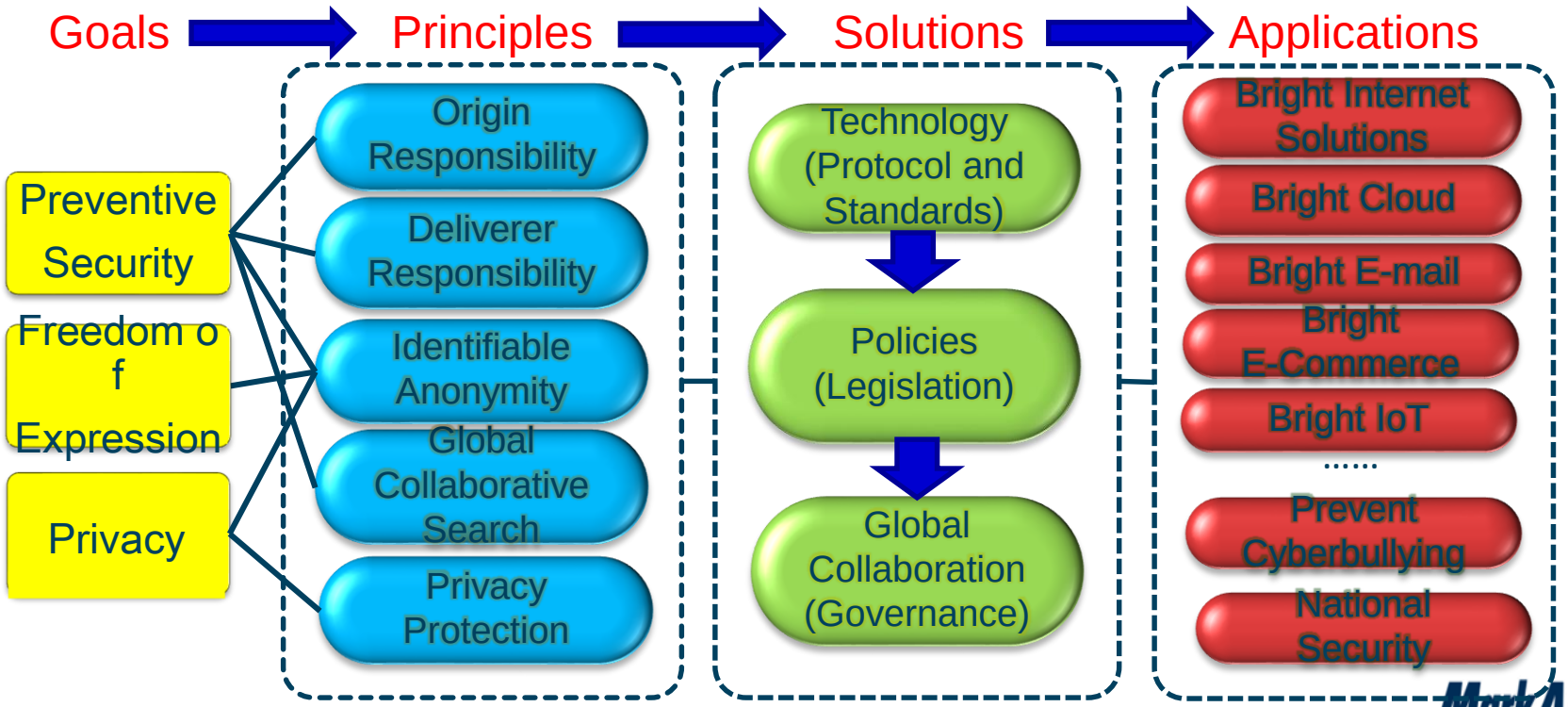
MarkAny

Bright Internet - Goal Driven Principles & Prescriptive Design

- **밝은 인터넷은 익명의 범죄자들에 의해 악용돼 범죄와 테러의 온상이 되고 있는 유·무선 인터넷의 문제를 근본적으로 해결하기 위한 기술과 제도, 국제 협약**
- **'4대 원칙**

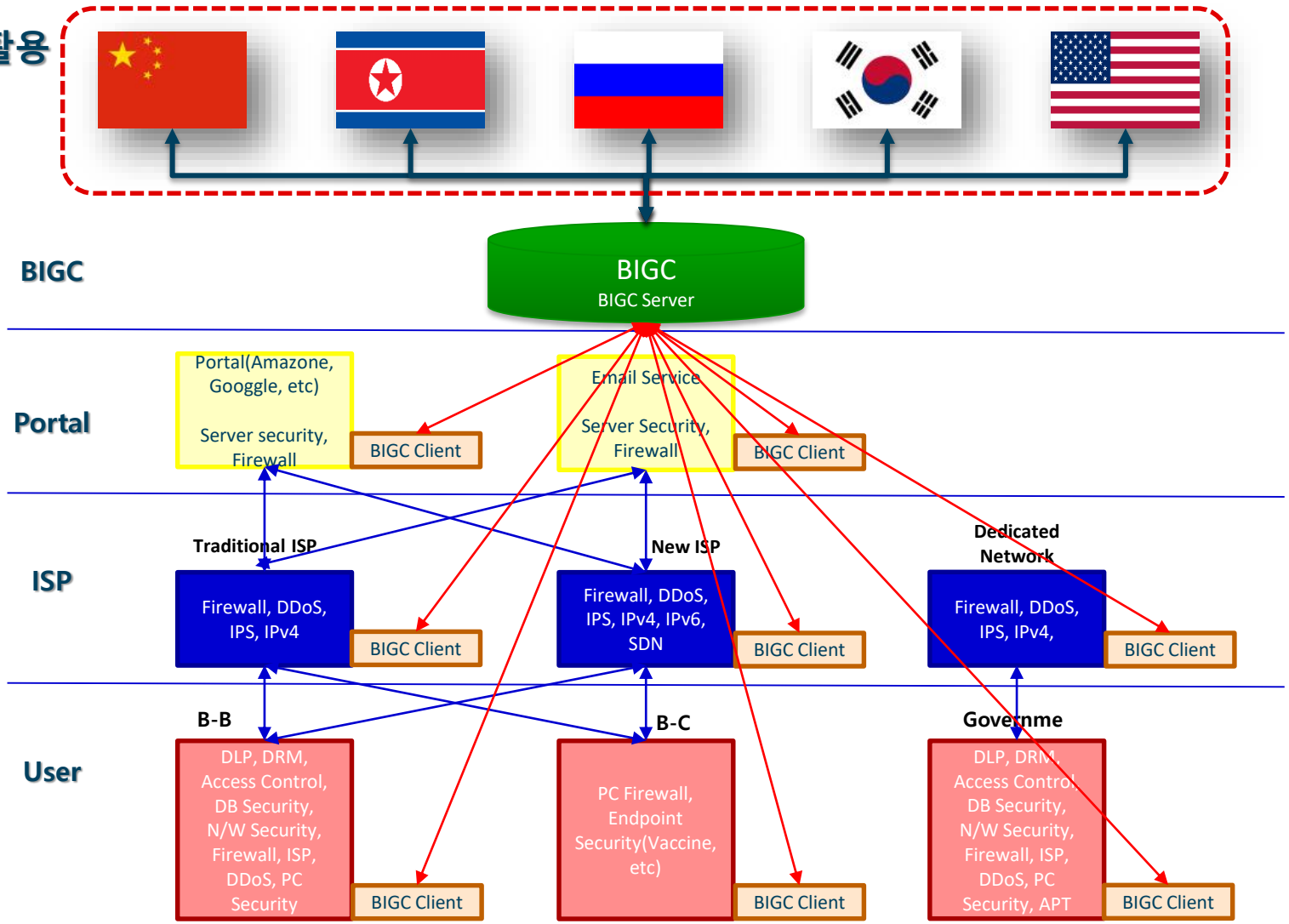
  ▷발송자 책임의 원칙 ▷배달자 책임의 원칙 ▷디지털 영장의 원칙 ▷추적 가능한 익명성의 원칙 등'을 제시했다.

  발송자 책임의 원칙은 문제의 발송자를 추적하고 책임을 묻도록 하는 것이고 발송자에만 그치지 않고 배달자 또한 책임을 지도록 해 근본적인 문제를 해결하겠다는 것이 '배달자 책임의 원칙'



Bright Internet 에서의 블록체인을 통한 국가간 신뢰성 확보

분산 원장 기술 활용 하여 국가간 신뢰 구축



New Network Architecture 예상

MarkAny

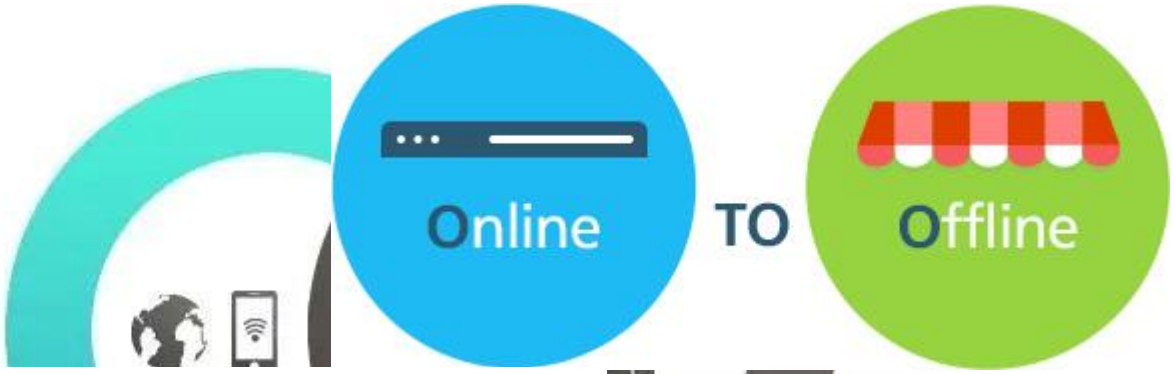
서명 등록과 확인을 통한 전송 데이터 무결성 확인

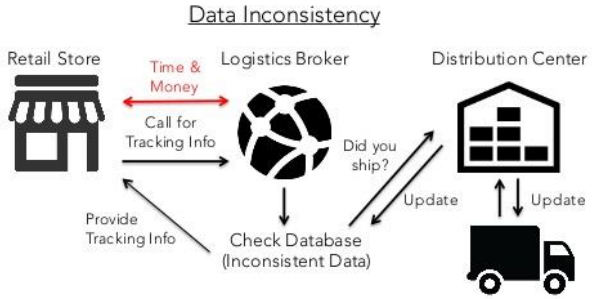
- **수신자에게 전송 데이터나 파일의 무결성 보장 하여, 신뢰성 확보**
- 데이터와 파일을 통해 전파되는 램섬웨어(ransomware), 멀웨어(malware), 고도화된 지능형 공격인 APT 공격을 방지하거나 억지 가능
- 국제적인 피해에도, Sender와 Deliverer의 책임을 위한 법적 증빙(**부인 방지)** 기능 제공

Bright Internet
서명 확인 서비스 시스템

MarkAny

O2O 서비스에서의 활용





"Increased risk of error due to multiple systems trying to work together which opens the door to data inconsistency issues between parties."

MarkAny

해외 적용 사례

도입사	도입 내용
Government of the Republic of Estonia	Estonian Succession Registry 에 보관중인 전자문서에 대한 인증 및 지속적 무결성 관리 시스템 (전자주민증)
SEB Bank (스웨덴 은행)	전자 뱅킹 로그/모바일 결제 로그/ATM 거래 로그에 대한 인증 및 무결성 검증 시스템
Parity Energy Inc.	통화기록에 대한 인증 및 무결성 검증 시스템
Sichuan CA	Sichuan 지역 eGovernment 시스템상의 보관자료에 대한 무결성 관리 시스템
China Telecom / Crew Systems	인터넷에 연결된 차량용 블랙박스에서 촬영된 영상에 대한 인증 및 시계열 무결성 검증 시스템
China Telecom	CCTV 넷웍 전체에 대하여 모든 촬영영상에 대한 인증 및 시계열 무결성 검증 시스템
Tianhe China LifeScienceCloudAlliance	생명 과학/의학 데이터의 클라우드 서버를 위한 시계열 무결성 검증 시스템
Lifeline Medical Systems	Teleradiology 의 데이터인 x-ray 이미지와 같은 환자 진단 자료들에 대한 인증 및 무결성 검증 시스템
Ericsson / Estonian Energy	Smart Grid 에서 전력 생산자/소비자의 계측 데이터에 대한 인증 및 시계열 무결성 검증 시스템
Japan Drones	무인항공기에 전달하는 명령에 대한 실시간 인증 및 무결성 검증 시스템
Scrive / Avanza Bank (the largest online stock broker in Sweden)	전자화된 고객 서명에 대한 인증 및 무결성 검증 시스템

MarkAny

Q&A

Your Security Partner MarkAny

MarkAny