

디바이스 DNA 기반 IoT 키보호 기술

2020. 07. 17

강유성

(youskang@etri.re.kr)

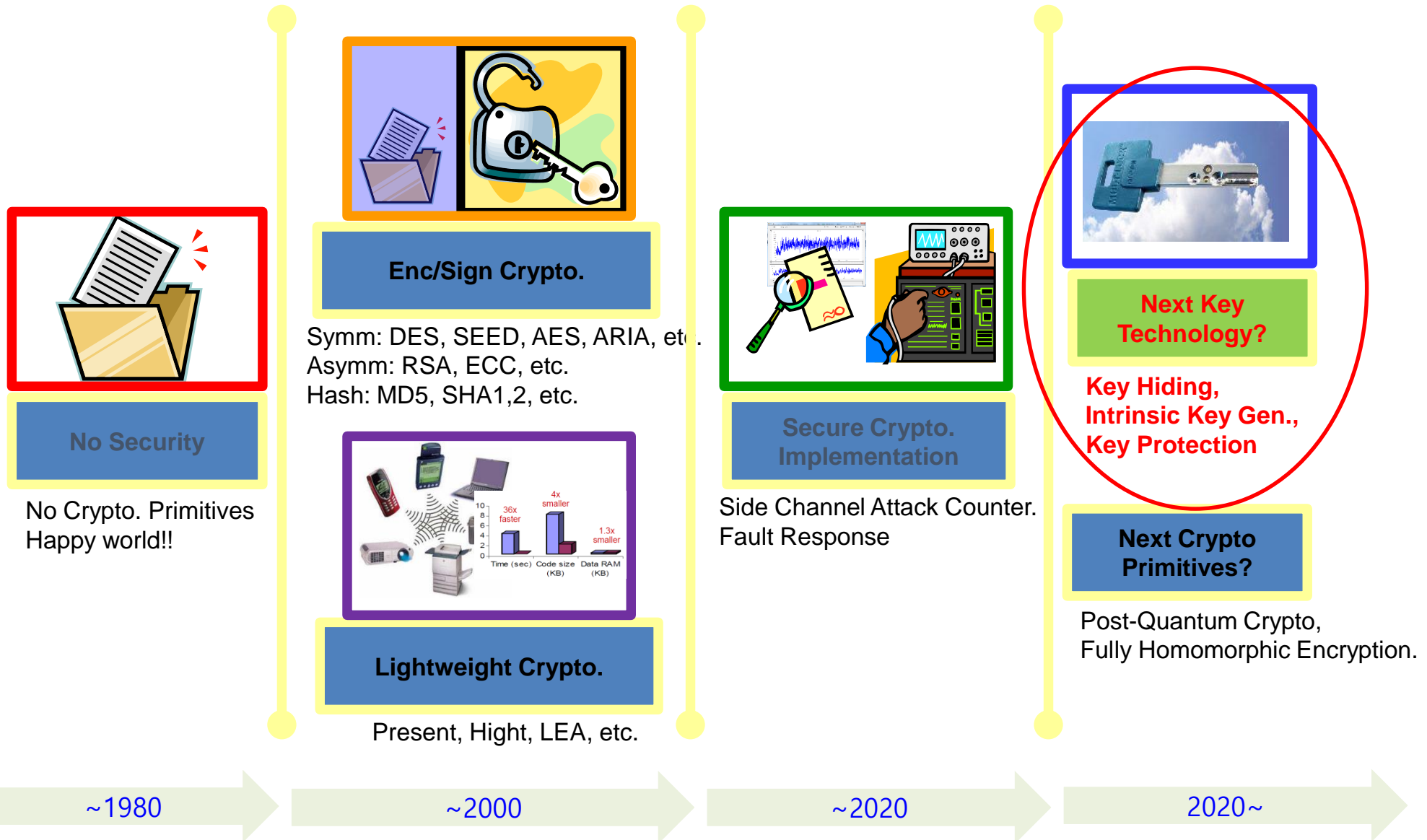
ETRI

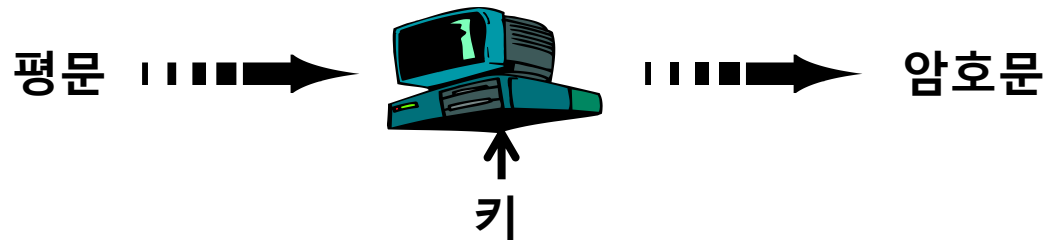




CONTENTS

1. IoT 암호키 중요성
2. IoT 디바이스 DNA
3. IoT 디바이스 DNA 활용
4. Q&A



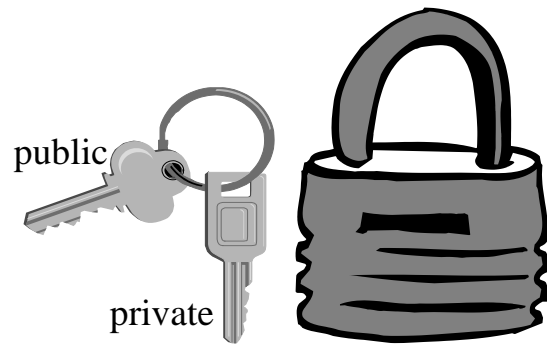


파랑:장점
빨강:단점

암호시스템 항목	대칭키 알고리즘	공개키 알고리즘
암호키의 관계	암호키=복호키	암호키≠복호키
암호화 키	비밀	공개 {비밀}
복호화 키	비밀	비밀 {공개}
암호 알고리즘	비밀, 공개	공개
대표 예	AES, ARIA, SEED, LEA	RSA, ECC
비밀키의 분배	필요	불필요
비밀키의 보유수	많음, 상대방별 키 필요	적음, 자신의 키만 비밀
암/복호화 속도	빠름	느림

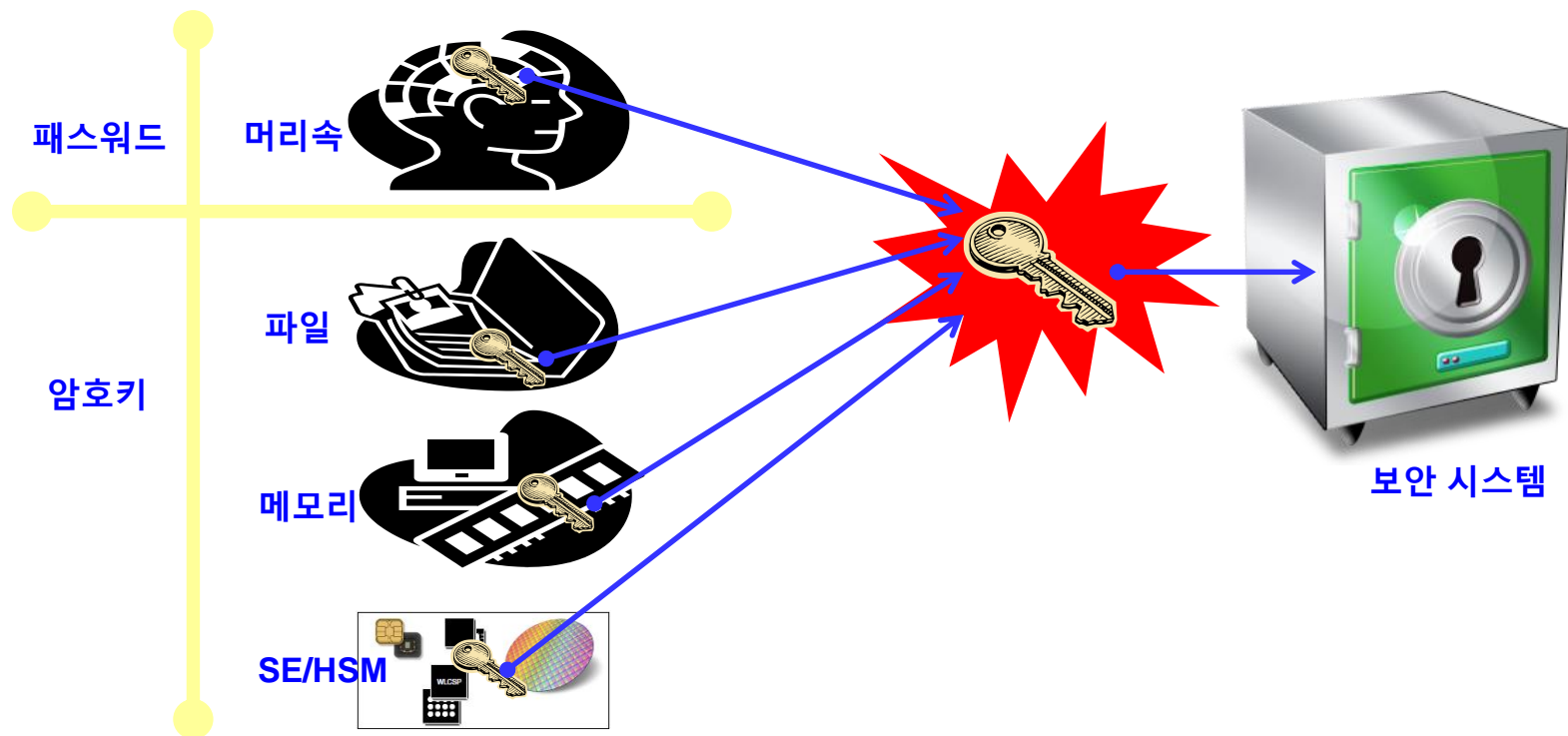


< 대칭키 암호 알고리즘 >
(Symmetric-key)



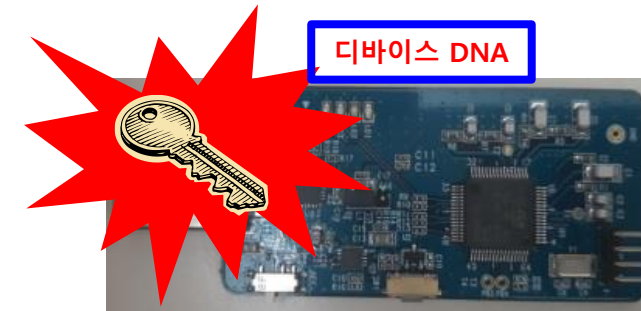
< 공개키 암호 알고리즘 >
(Asymmetric-key, Public-key)

- 기존 암호 시스템은 **암호키**(비밀키, 패스워드 등)의 주입/저장 단계가 반드시 필요함
- 암호키의 노출**은 아무리 안전한 암호 시스템이라도 손쉽게 무력화 시킬 수 있음
- 암호 및 보안 시스템 강화의 필수 기술 : **암호키 생명주기 관리** (키생성, 키은닉, 키보호 등)

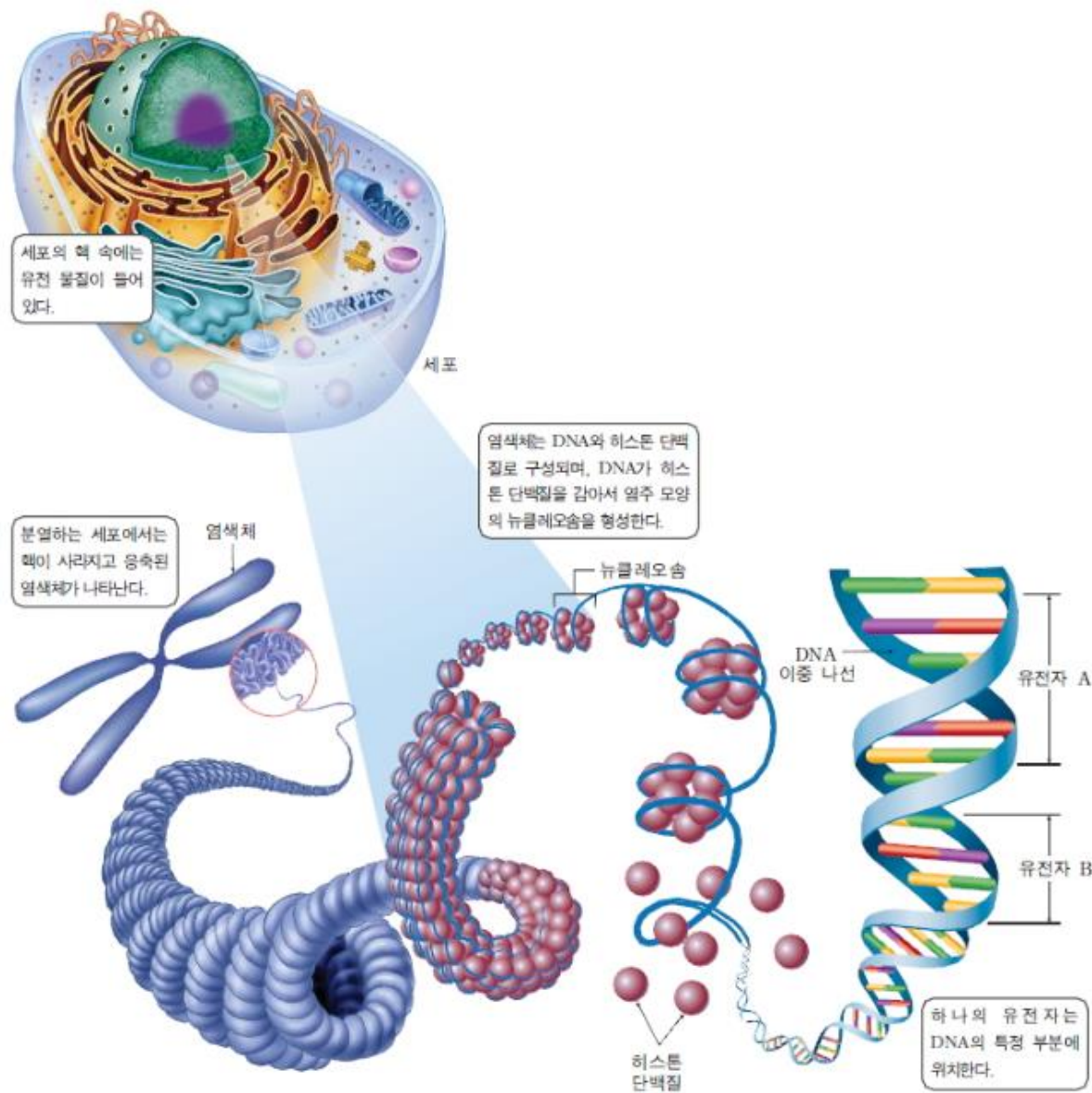




TO-BE
**Nowhere...
but, Anytime!!!**

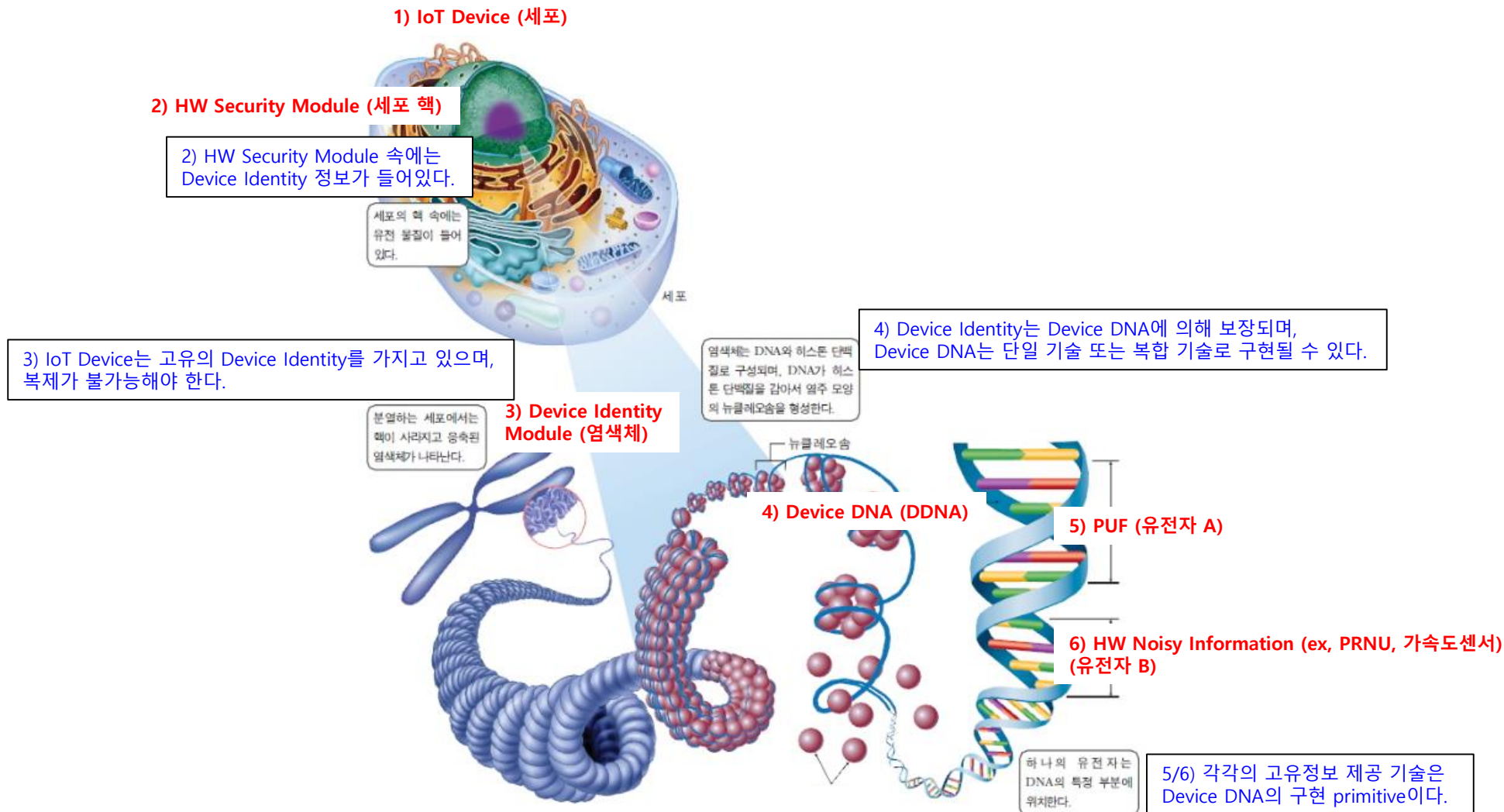


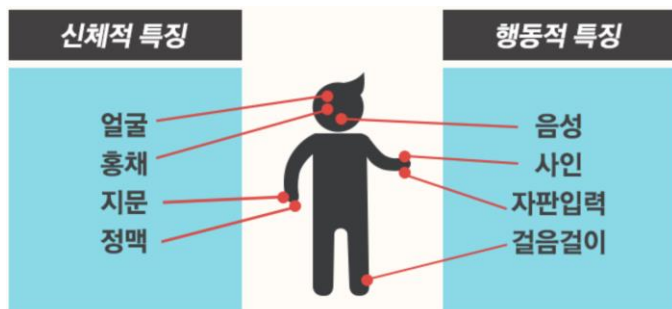
암호키 노출 위험 제거



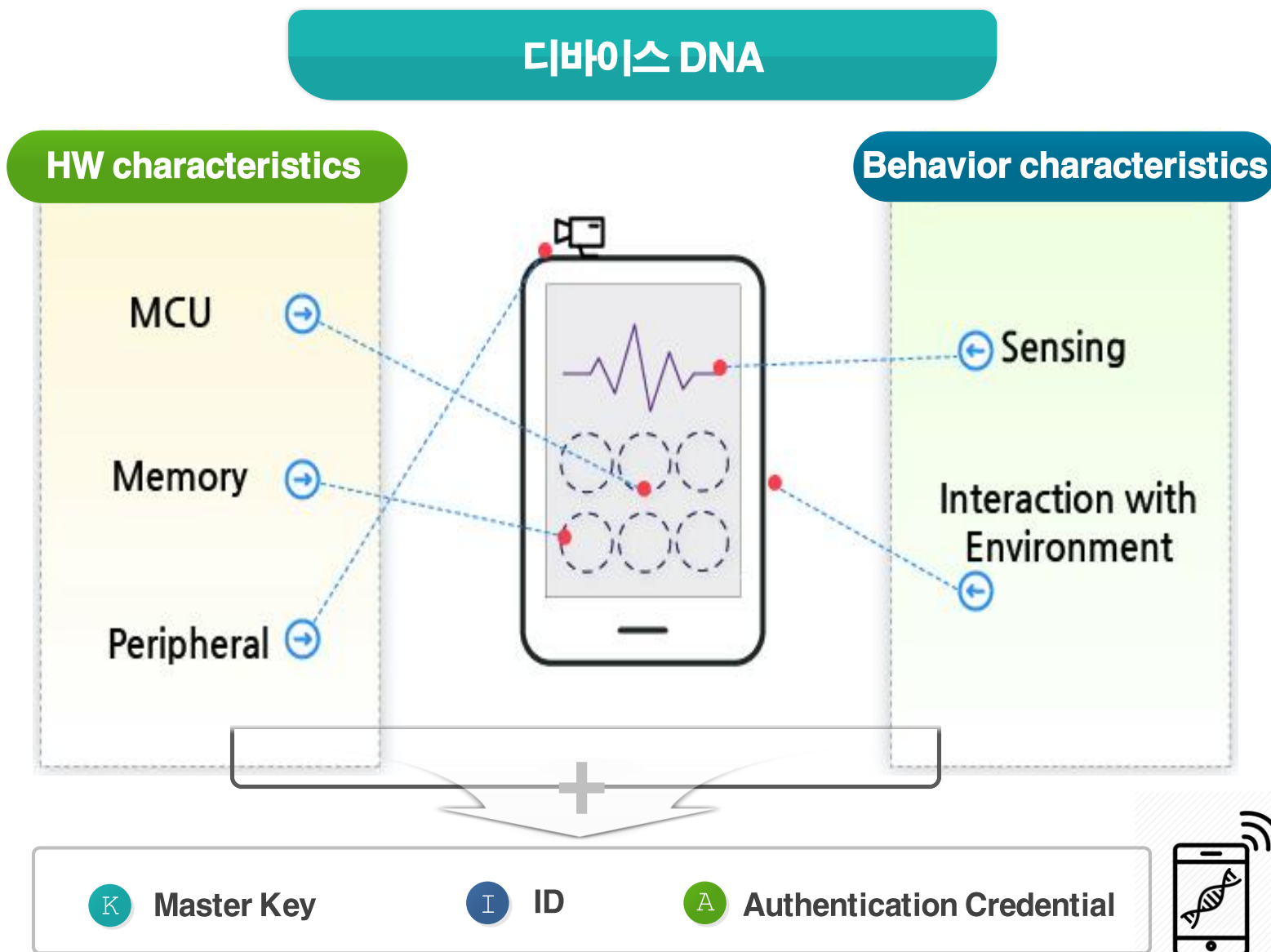
(Source: google search)

- DNA
 - **데옥시리보 핵산**(-核酸, Deoxyribonucleic acid, **DNA**, 디옥시리보핵산)는 핵산의 일종이며, 주로 세포의 핵 안에서 생물의 유전 정보를 저장하는 물질이다. **DNA의 주 기능은 장기간에 걸친 정보저장이다.**
 - 유전정보는 DNA에 기록되어 있음
- 유전자 (Gene)
 - **유전자**(遺傳子)는 유전의 기본단위이다. 지구상의 모든 생물은 유전자를 지니고 있다. 유전자에는 생물의 세포를 구성하고 유지하고, 이것들이 유기적인 관계를 이루는 데 필요한 정보가 담겨있으며 생식을 통해 자손에게 유전된다.
 - **하나의 유전자는 DNA의 특정 부분에 위치함**





바이오 인식



디바이스 DNA 정의

※ 표기 : 디바이스 DNA, Device DNA, DDNA, D²NA

- 💡 디바이스를 구성하는 하드웨어 중 특정 **하드웨어의 고유특성에 기반하여 생성할 수 있는 고유 값**
- 💡 반복성(불변성), 유일성, 복제불가성, 예측불가성, 난수성의 성질을 만족해야 함
- 💡 메모리나 파일, 칩에 주입/저장되지 않고, **필요한 시점에 사용되고 사라지는 특징**을 가짐

디바이스 DNA 생성 및 사용

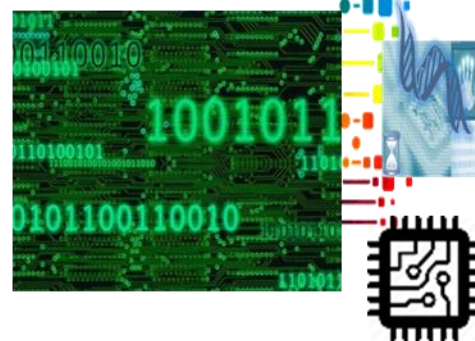
Primitives

- PC PUF
- PHY PUF
- PDRO PUF
- Flash PUF
- Image Sensor PRNU
- External Sensing Data

오류정정
및 안정화

- Error Correction Code
- Fuzzy Extractor
- Fuzzy Commitment

디바이스 DNA



Pre-master key

Pre-shared key

Key pair

ID

Password

Other credential

□ 디바이스 DNA 보안 요구사항 (ISO/IEC 20897-1 표준문서 참조)

◆ Steadiness

- 동일한 디바이스에서 동일한 디바이스 DNA 값을 출력하는 안정성(불변성, 동일성 등)
- Reliability, Reproducibility, Stability, Robustness 등이 유사한 의미로 사용 중

◆ Randomness

- 디바이스 DNA 값 자체의 난수성

◆ Uniqueness

- 동일한 설계/부품/제조공정에서 구현된 서로 다른 디바이스에서 출력되는 디바이스 DNA 값의 유일성(차별성)
- 디바이스 DNA 값의 엔트로피

◆ Tamper-resistance

- 물리적(침투 및 비침투) 공격에 의해 디바이스 DNA가 읽혀지거나 변조되지 않아야 하는 특성

◆ Mathematical unclonability

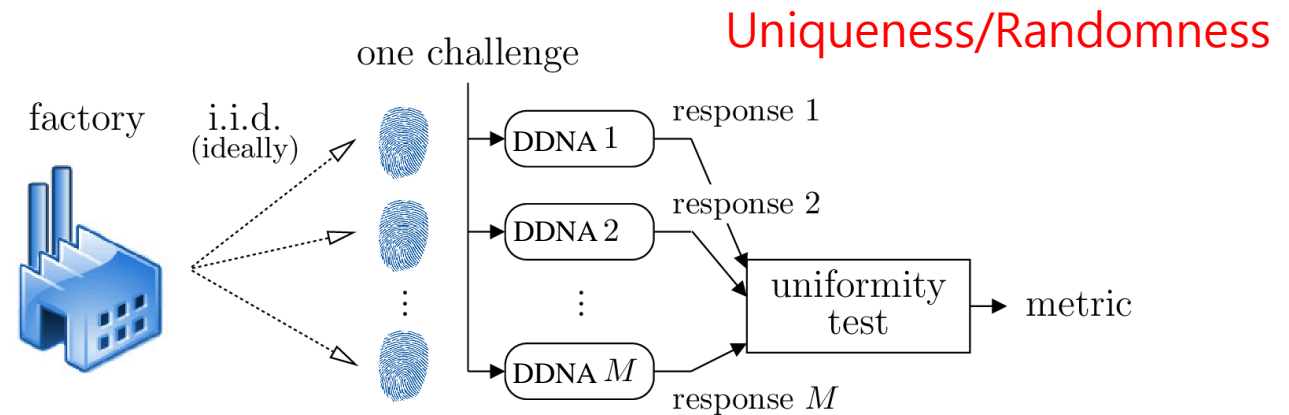
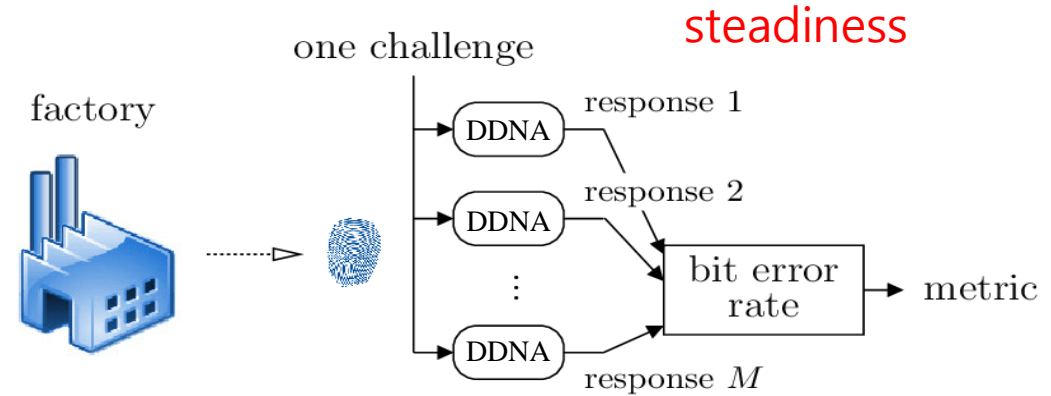
- 디바이스 DNA 값이 특정 Challenge에 특정 Response를 제공하는 경우, Challenge-Response 특성이 시뮬레이션될 수 없어야 하는 특성
- Challenge-Response 사이의 비상관성(Uncorrelated, Unbiased, Diffuseness) 및 학습공격에 대한 저항성을 의미

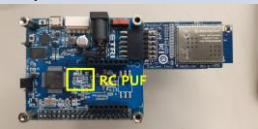
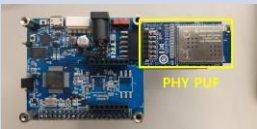

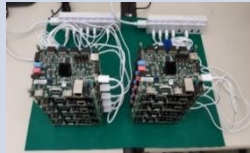

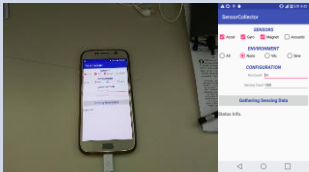
◆ Physical unclonability

- 설계나 구조, 부품, 제조공정이 알려지더라도 복제 디바이스 DNA 구현이 가능하지 않아야 하는 특성

Test using actual devices

- ◆ Test of Steadiness
 - Intra-Hamming Distance, Bit Error Rate
- ◆ Test of Randomness
 - FIPS 140-2, SP 800-22, etc
- ◆ Test of Uniqueness
 - Inter-Hamming Distance, SP 800-90B



Primitive 명칭	(1) RC PUF	(2) PHY PUF	(3) Flash PUF	(4) PDRO PUF	(5) Image Sensor PRNU	(6) External Sensing Data
대상 하드웨어	Resistor-Capacitor (저항-커패시터)	통신 칩셋 SRAM 메모리 (Wi-Fi, SUN)	Flash 메모리	링 오실레이터 (Phase detection ring oscillator)	Camera module (이미지 센서)	주변 센서류 (가속도, 자이로스코프 등)
출력 타입	Dynamic (32bits challenge)	Fixed or Restricted dynamic	Fixed or Restricted Dynamic	Dynamic	Dynamic	Dynamic
출력 사이즈	128 bits ~ 2048 bits	통신모듈 버퍼 사이즈 (256 bits 이상 가능)	Flash 메모리 사이즈 (256 bits 이상 가능)	128 bits ~ 2048 bits	학습 네트워크 모델(오토인코더의 잠재공간 노드 수에 비례)	학습 네트워크 모델(오토인코더의 잠재공간 노드 수에 비례)
개발 보드 (시험 제품)	- Kidden-Ruby 보드 (STM32F4) + RC회로	- Kidden-Ruby 보드 (STM32F4) + Pmod WiFi module	- Kidden-Ruby 보드 (STM32F4) + S25FL128S (16MB) Flash Memory	Zybo Z7-20 보드(Xilinx)의 Zynq FPGA	삼성, 로지텍, 샤오미 IP 카메라, 아이폰	스마트폰 (안드로이드), 아두이노
특징	<ul style="list-style-type: none"> 반복성, 유일성, 난수성 등 우수 3V~3.6V 범위에서 1%이하 error 특성 챔버 테스트 (-20 ~ 70 °C에서 stability 유지) 다양한 MCU에 적용 가능 	<ul style="list-style-type: none"> 반복성, 유일성, 난수성 등 우수 챔버 테스트 (-20 ~ 70 °C에서 stability 유지) Voltage variance에 강인 하드웨어 수정 불필요 	<ul style="list-style-type: none"> 반복성, 유일성, 난수성 등 우수 하드웨어 수정 불필요 온도 및 전압에 대한 신뢰성 평가 진행 예정 	<ul style="list-style-type: none"> 칩 또는 FPGA 구현을 위한 PUF IP 확보 반복성, 유일성, 난수성 등 우수 	<ul style="list-style-type: none"> 상용제품(판매중인 IP 카메라)에서 디바이스 DNA 확보 카메라 모듈 고유 노이즈(PRNU)를 학습시켜 활용 	<ul style="list-style-type: none"> 상용제품(판매중인 안드로이드/아두이노 기반 스마트폰)에서 디바이스 DNA 확보 주변 센서류의 센싱 데이터를 추출하여 활용 

* Fixed 타입 (Confined 타입): 출력이 고정되어 있는 타입

* Dynamic 타입 (Extended 타입): Challenge-Response 방식으로 동적으로 출력을 변경할 수 있음.

* Restricted Dynamic 타입: Challenge-Response 방식이나, CRP pair가 제한적이거나 하나인 경우.

PRNU: Photo Response Non Uniformity



디바이스 DNA 통합 추출 플랫폼 기술

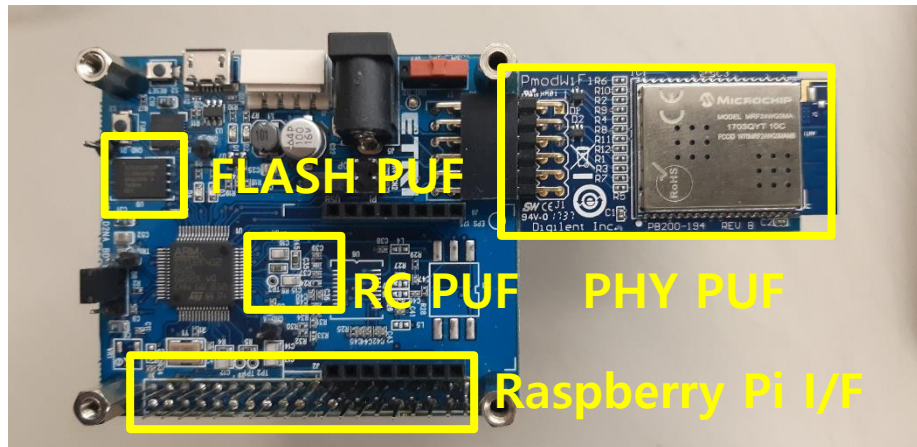
❖ 주요 기능 : RC PUF, PHY PUF, Flash PUF 및 센서 I/F 통합 내장

❖ RC PUF, PHY PUF, Flash PUF 등을 내장한 디바이스 DNA 통합 추출 플랫폼 기술

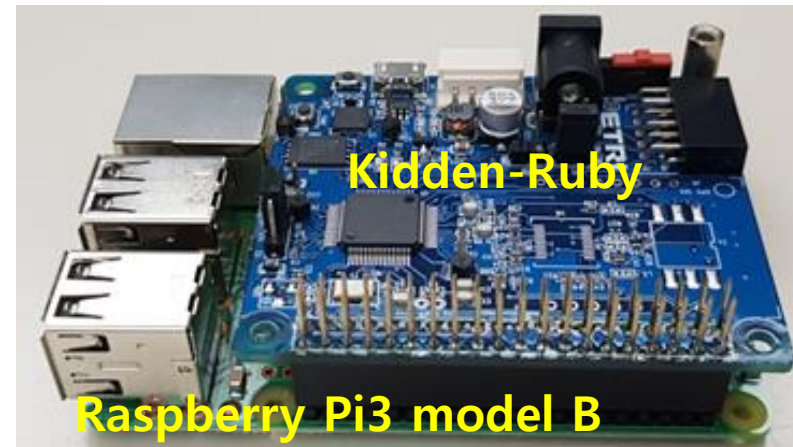
- RC PUF, PHY PUF, Flash PUF 기능 내장
- Cortex-M4 기반 STM32F412 MCU (~100MHz)
- ESP-12S Wi-Fi 모듈 내장
- 센서 인터페이스 : 가속도 센서, 지자기 센서, 자이로스코프 센서 등 각종 센서를 이용한 디바이스 DNA 추출 가능
- 라즈베리파이 보드 연동 가능
- 디바이스 DNA 생성 안정화 기술 및 디바이스 DNA 통합 추출 프로그램 개발

▪ 보드이름: Kiddren

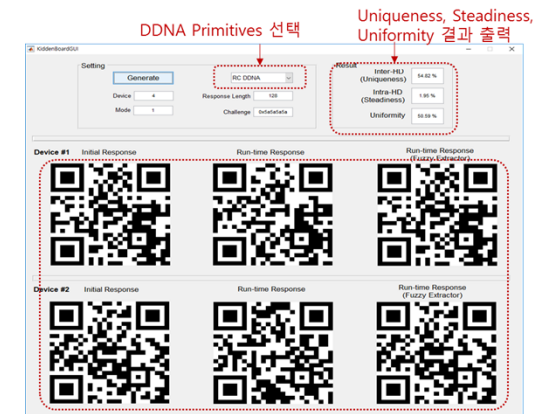
- * Key Hidden의 약자
- * 발음 '키든'은 우리말로 키가 들어있다는 의미도 가짐



<디바이스 DNA 통합 추출 플랫폼 - Kiddren-Ruby>



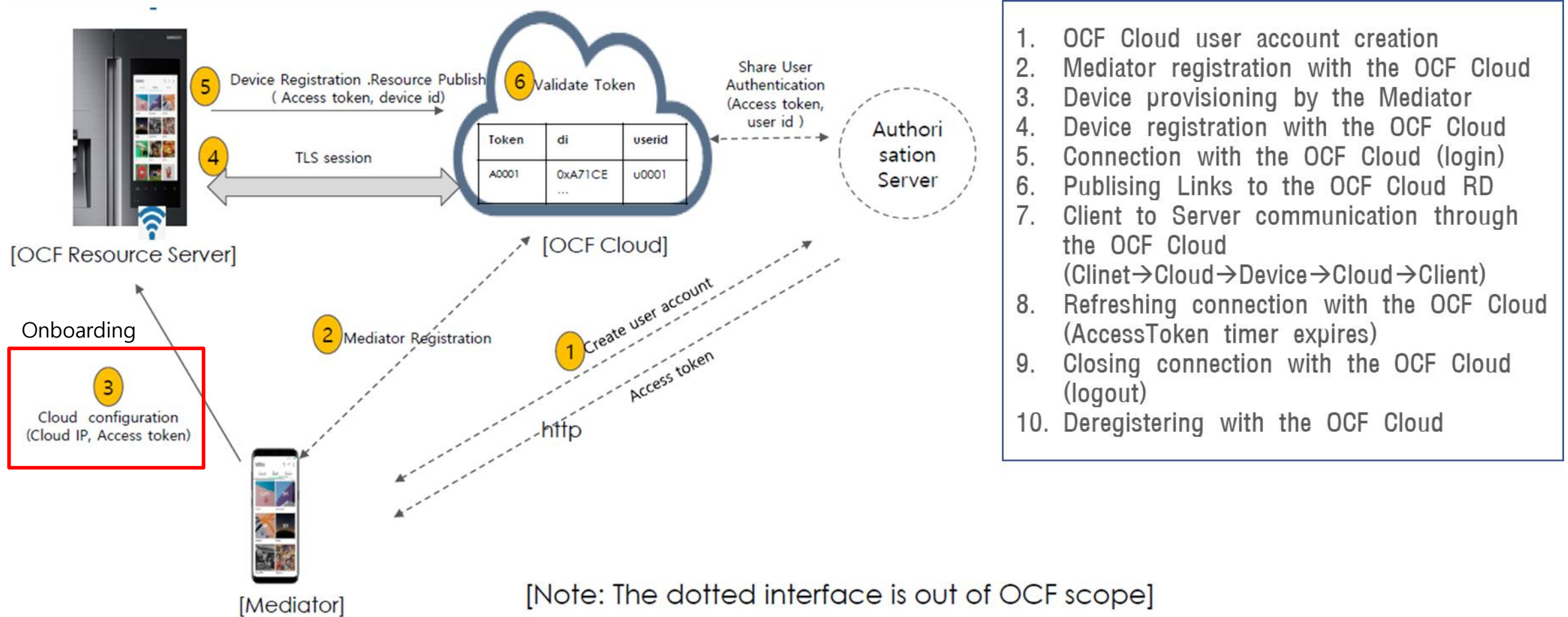
< 라즈베리파이 보드 연동 >



Device 1, 2에 대한 Initial response 및 Run-time response를 QR코드로 표시

< 디바이스 DNA 추출 프로그램 >

OCF Cloud Spec: 사용자 인증 기반의 디바이스 원격 제어 및 관리



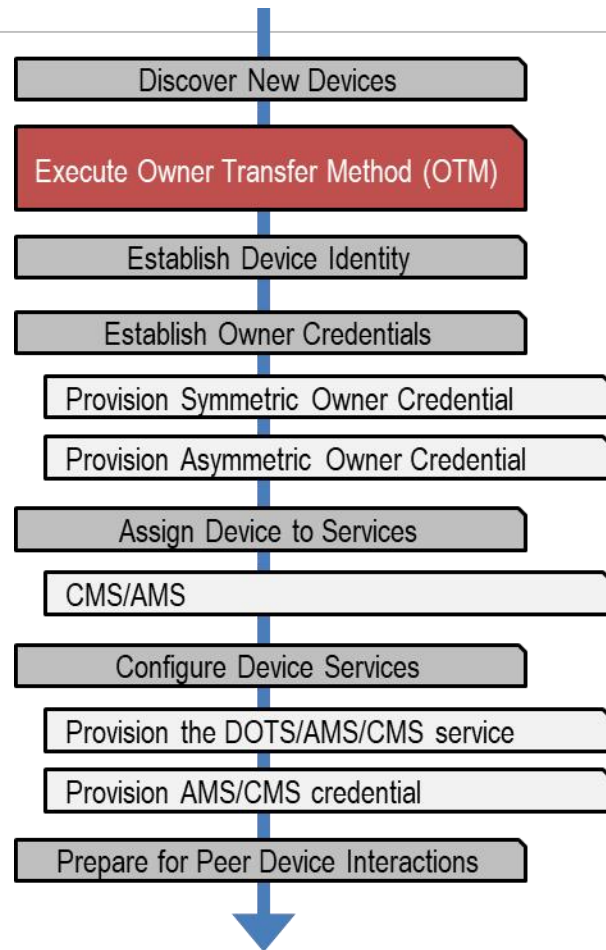
※ Mediator provisions the OCF Device with information necessary for remote service management

Onboarding: 디바이스 인터넷 연결 및 접근권한 관리



OBT를 통해 OCF 기기를 소유하고 정상 동작에 필요한 정보를 설정하는 과정

※ Device를 "Ready for Normal Operation(RFNOP)" 상태로 만들기 위한 과정



Simplified Onboarding Sequence

DOTS: Device Ownership Transfer Service
AMS: Access Management Service
CMS: Credential Management Service

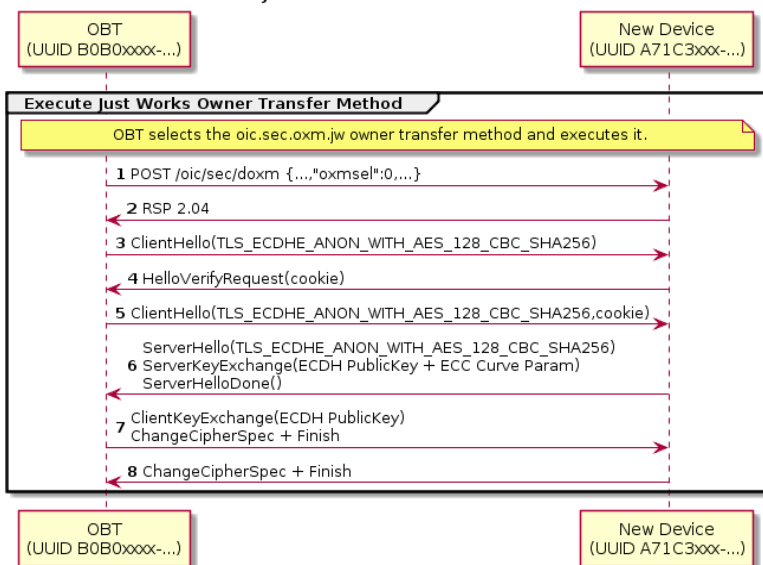
- *Unowned Device boots*
- **Discovery (unsecured):**
 - DOTS sends multicast to discover unowned devices no TLS
 - Unowned devices reply, including list of supported OTMs no TLS
- **Ownership Transfer:**
 - DOTS selects and configures this OTM to the new device no TLS
 - DOTS & unowned Device perform OTM, inc. TLS handshake TLS
 - DOTS configs SVRs to authorize itself, CMS and AMS TLS
 - *Device is now owned!*
- **Provisioning:**
 - CMS provisions credentials, AMS provisions access policies TLS
 - *Device is now provisioned and can commence normal operation*
- **Normal Operation:** TLS or no TLS
 - *Credentials and/or access policies can be updated by returning to Provisioning*

Ownership Transfer Method (OTM)

Just-Works OTM

- 단순한 형태의 가장 기본적인 방식
- 인증과정이 없는 암호화 통신 채널 제공
- Onboarding 절차에서의 MitM 공격에 취약

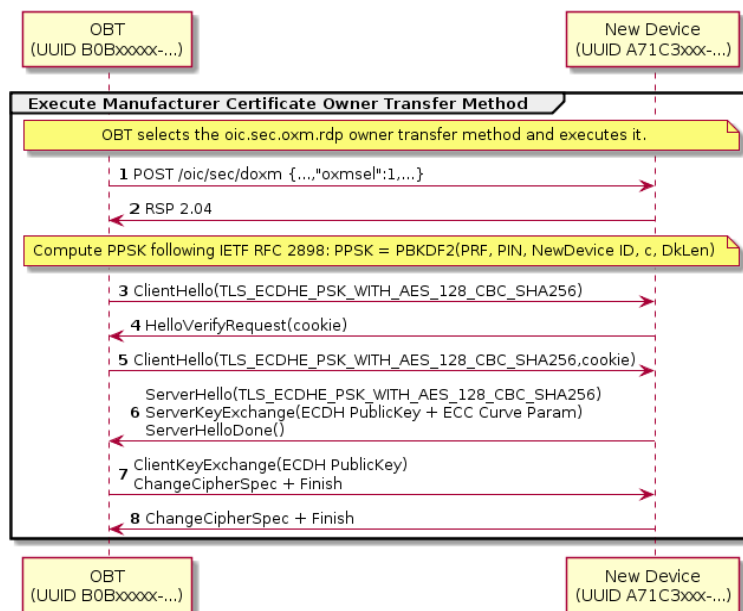
Perform Just-Works Owner Transfer Method



Random PIN based OTM

- PIN 정보에 대한 OBT(사용자) 입력 필요
→ PIN 정보를 전달하기 위한 절차 필요
- Onboarding 절차에서의 MitM 공격에 강인

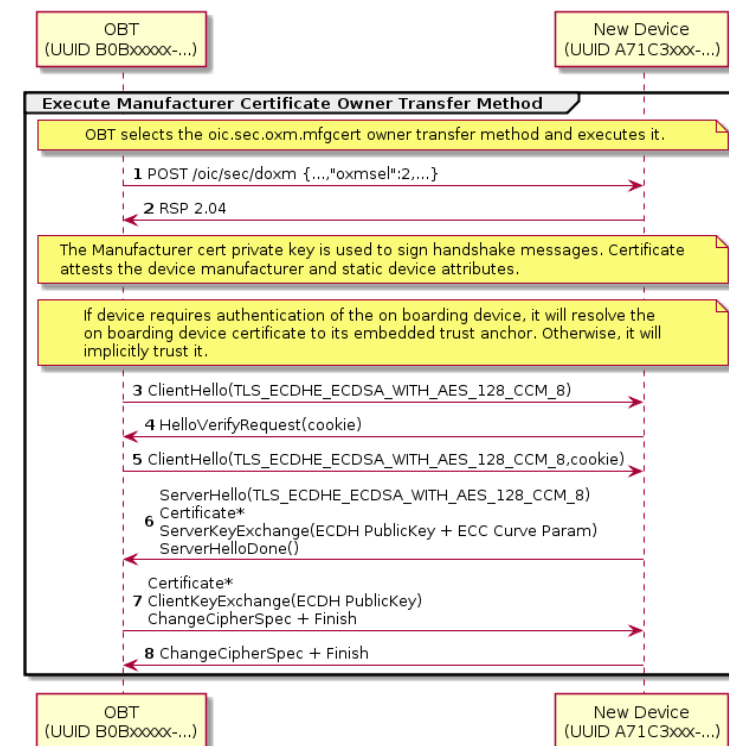
Perform Random PIN Device Owner Transfer Method



Manufacturer Certificate based OTM

- Cert meta-data를 이용한 최상의 인증 방식
- OBT로의 Certificate 제공
→ Root Cert를 포함한 확실한 방식 필요

Perform Manufacturer Certificate Owner Transfer Method

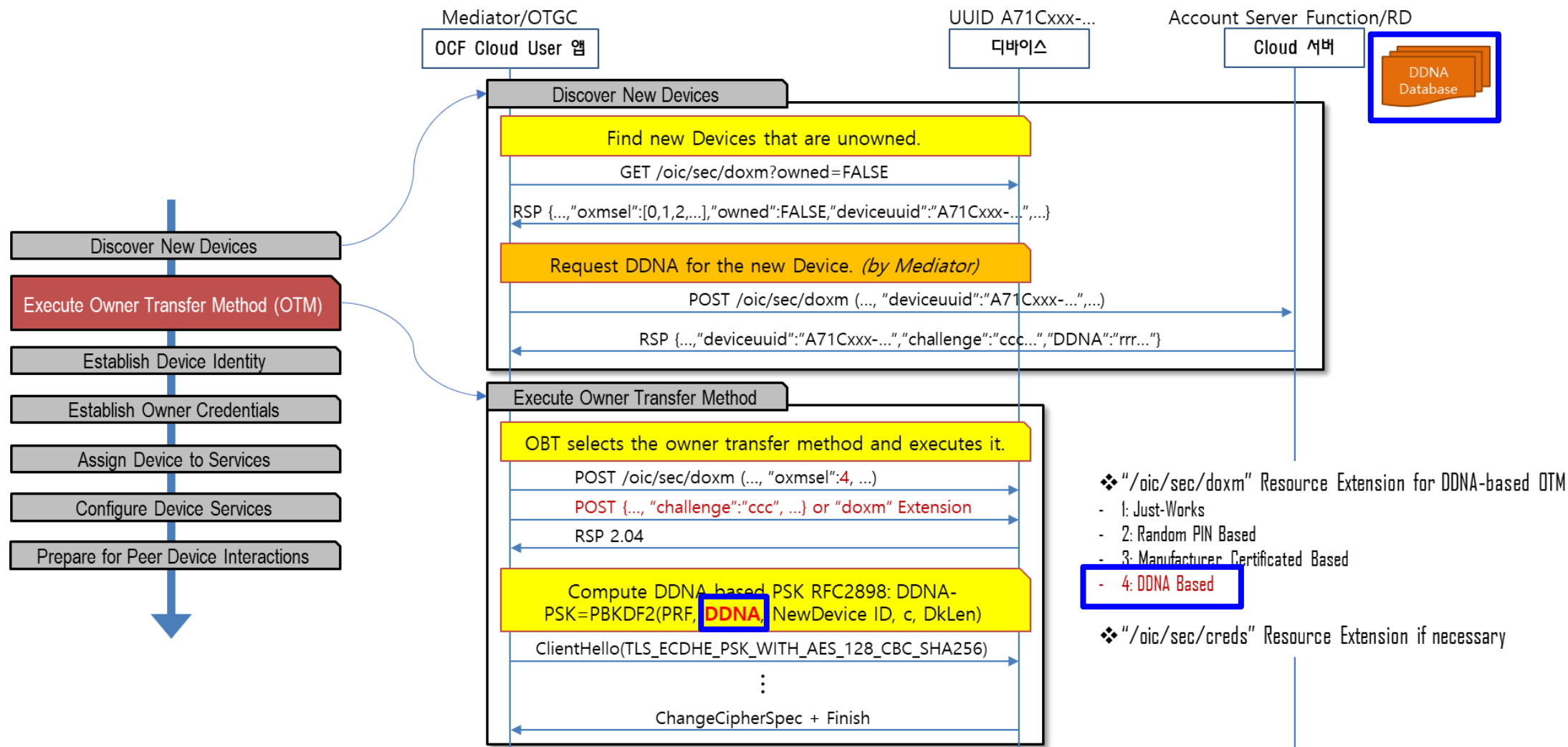


Authentication Algorithm Strength Mode

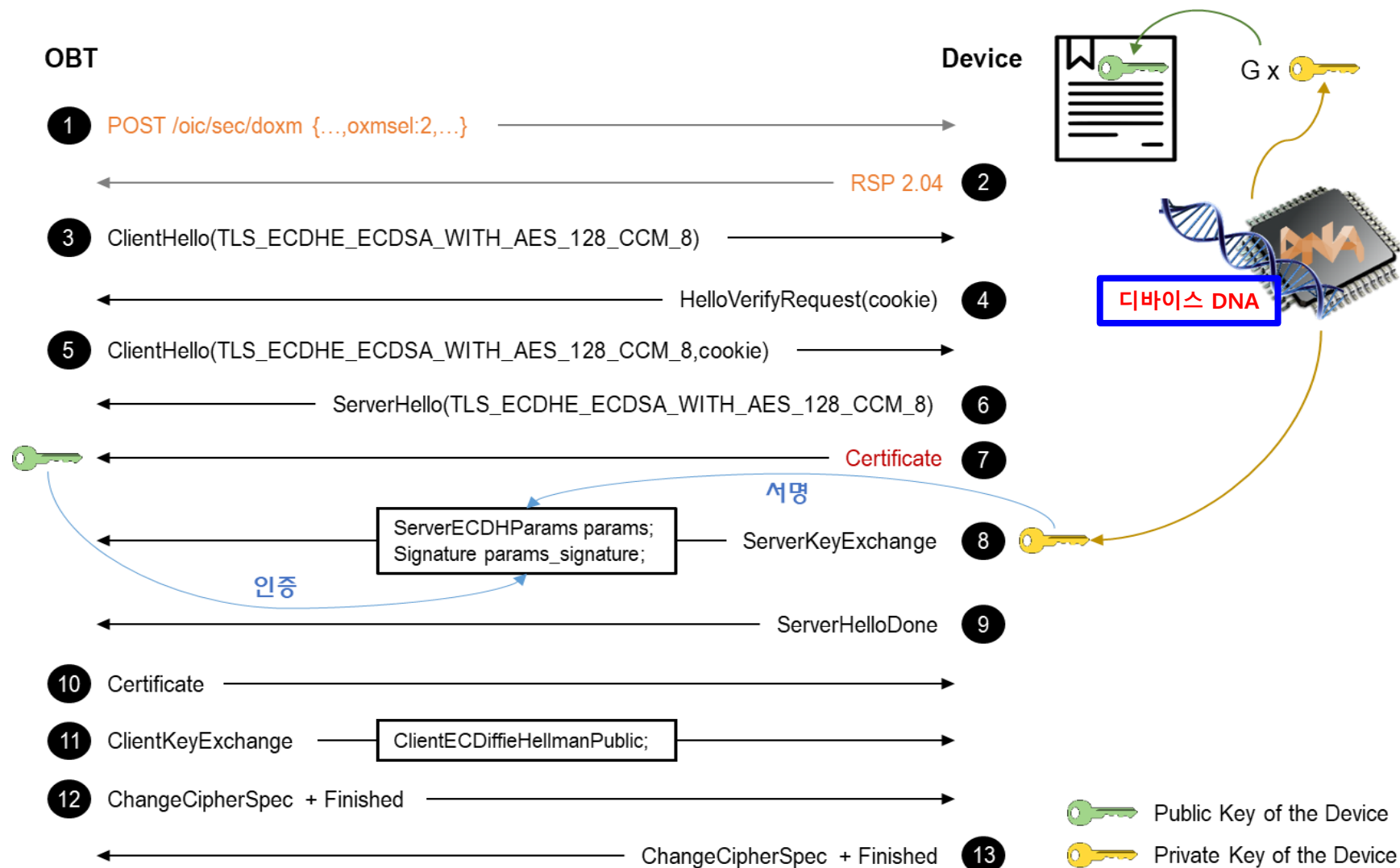
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Key exchange Cipher MAC or PRF

디바이스 DNA를 활용한 PSK 기반 Onboarding → Random PIN based OTM 수정 적용



디바이스 DNA를 활용한 인증서 기반 Onboarding → Device as Server로의 동작 적용



Device Authentication 기술

**D2D (Device as Client to Device as Server)**

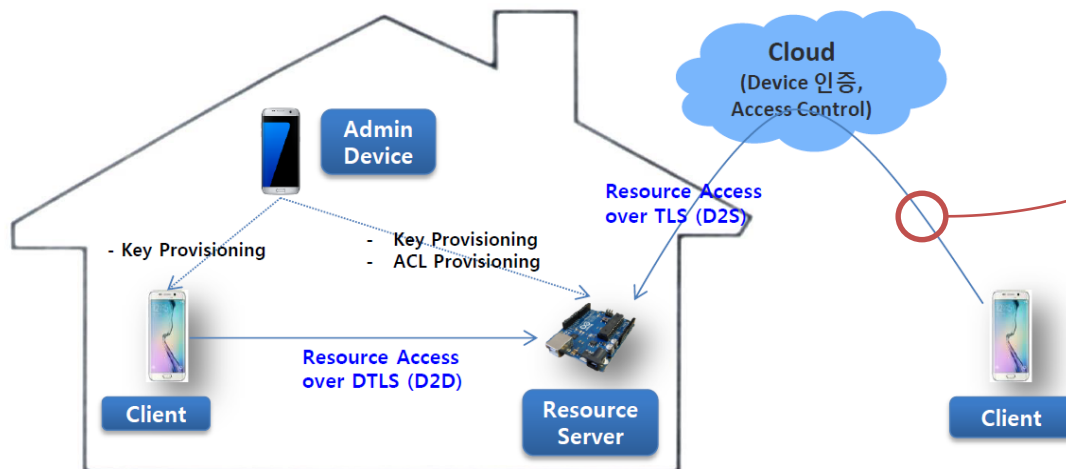
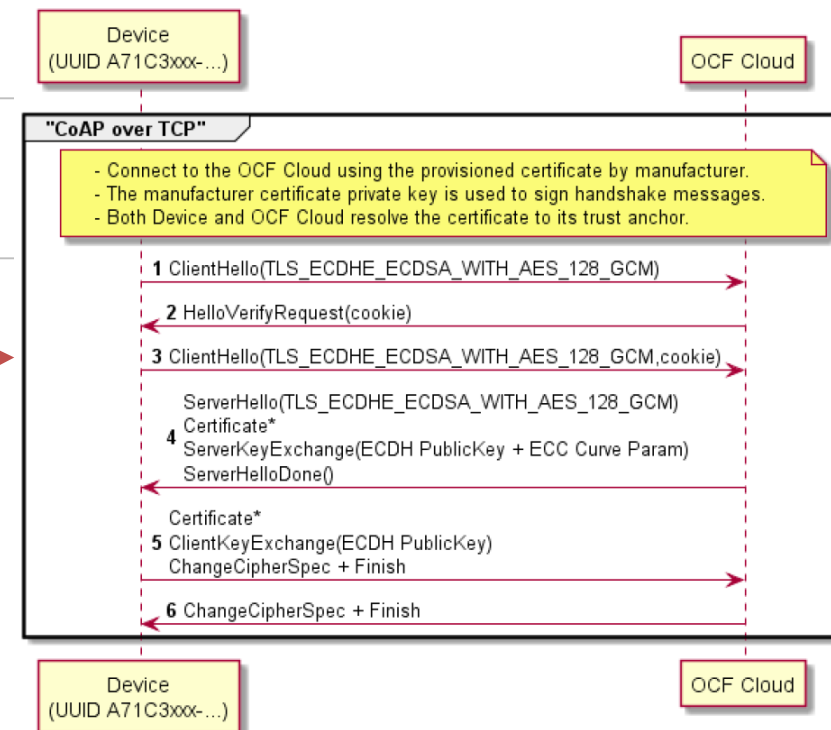
- ※ Symmetric Key를 이용한 기기 인증 (PSK)
- ※ Raw Asymmetric Key를 이용한 기기 인증 (without Certificate)
- ※ Certificate를 이용한 기기 인증 → RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile

**D2C (Device as Client to OCF Cloud)**

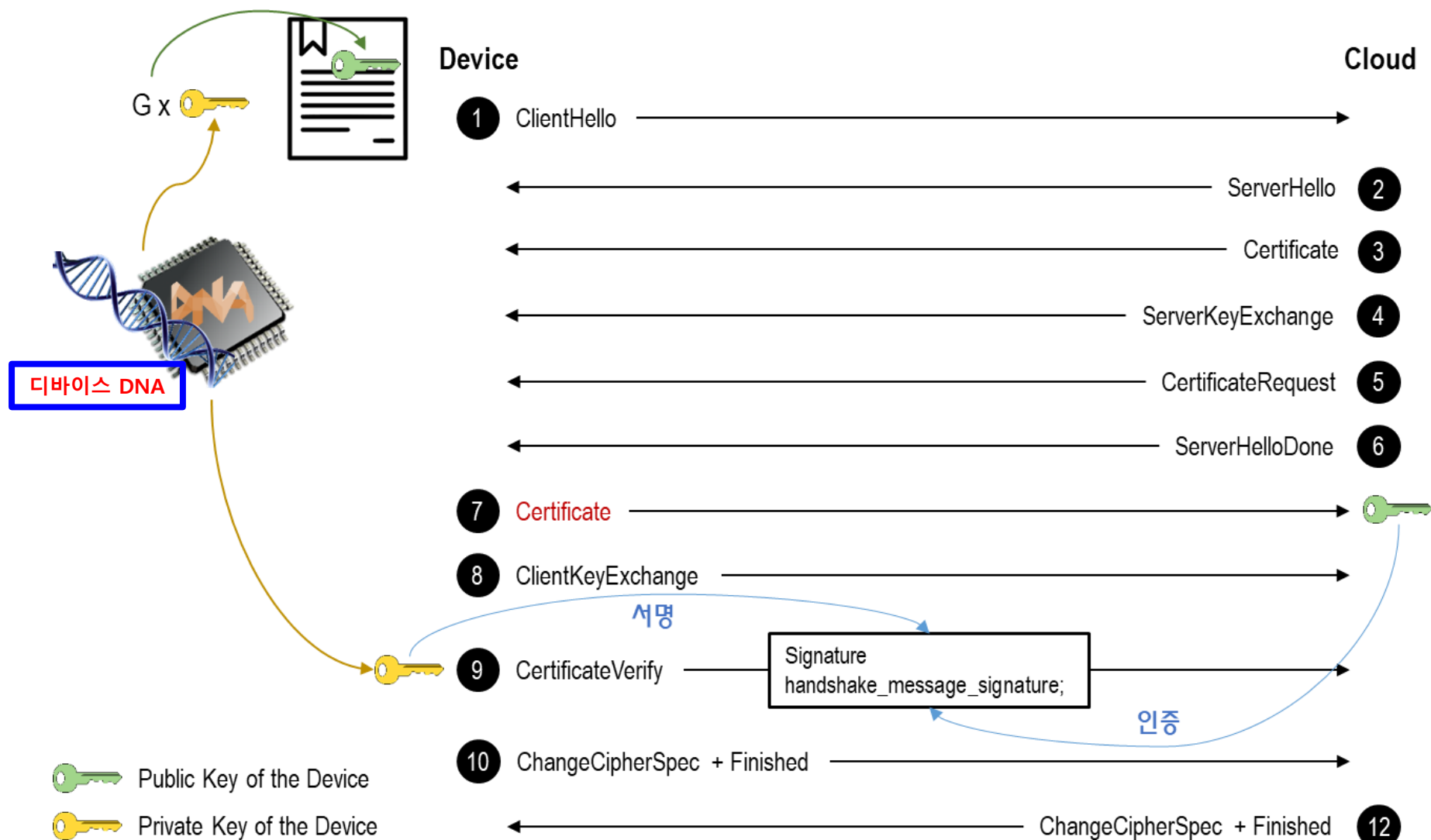
- ※ Certificate를 이용한 기기 인증
→ RFC 8323 CoAP(Constrained Application Protocol) over TCP, TLS, and WebSockets
- ※ 표준 규격 ver. 2.0 이후 추가

**새로운 기기 간 인증 방식을 정의하기보다는 기존의 인증 기법 활용**

- ※ 기존의 인증서, 대칭 키 기반의 인증 기법 등을 이용 → TLS/DTLS 보안 프로토콜

**Device Connection with OCF Cloud**

Device to OCF Cloud 사이의 디바이스 인증 → Device as Client로의 동작 적용





Thank you!

