네트워크 운여업자를 위한

IoT 보안 지침

네트워크 운여업자를 위한 IoT 보안 지침

버전 2.0

2017 년 10 월 31 일

본 문서는 GSMA 의 구속력이 없는 영구 참조 문서입니다.

보안 분류: 비기밀

본 문서의 열람과 배포는 보안 등급에서 허가된 자에게 한정됩니다. 본 문서는 협회의 기밀이며 자작권 보호 대상입니다. 본 문서는 공급된 목적에 한하여 사용해야 하며, 협회의 사전 서면 승인 없이 보안 등급에 따라 허가받은 자 이외의 사람에게 이 문서 수록된 정보의 전부 또는 일부를 공개하거나 제공해서는 안 됩니다.

저작권 고지

면책 조항

GSM 협회("협회")는 본 문서에 수록된 정보의 정확성이나 완전성, 적시성에 대해 어떠한 진술이나 보증, 약속(명시적으로나 묵시적으로나)도 하지 않고 책임도 지지 아니하며 배상할 의무도 없습니다. 본 문서에 수록된 정보는 예고 없이 변경될 수 있습니다.

독점금지 고지

본 문서에 수록된 정보는 GSM 협회의 독점금지 준수 정책에 부합합니다.

목차

1 서론

1.1 개요

본 문서에서는 IoT 서비스 업체에게 서비스를 제공하고자 하는 네트워크 사업자에게 시스템 보안과 데이터 프라이버시를 지킬 수 있는 최고 수준의 보안 기침을 제시합니다. 권고사항은 현재 배포되고 있는 것 중에서 쉽게 이용 가능한 시스템과 기술을 기반으로 하고 있습니다.

1.2 문서의 구조

본 문서는 네트워크 사업자와 IoT 서비스 업체를 대상으로 한 것입니다. 본 문서의 독자라면 GSMA 의 IoT 보안 지침서 세트 [11]에 속하는 다음 문서도 참고로 읽어 보기 바랍니다.

그림 1 GSMA IoT 보안 지침서 세트의 구조

1.3 문서의 목적과 범위

본 문서는 IoT 서비스 업체와 그 네트워크 사업자 파트너 간 공급자 계약에서 일종의 체크리스트 역할을 합니다.

본 문서의 범위는 다음과 같습니다.

- IoT 서비스와 관련된 보안 지침
- 네트워크 사업자가 제공하는 보안 서비스 관련 권고사항.
- 셀룰러 네트워크 기술

본 문서에서는 IoT 규격이나 표준의 개발을 제안하지 아니하며 현재 시중에 나와 있는 솔루션과 표준, 모범 사례만을 언급합니다.

본 문서는 또 기존 IoT 서비스의 퇴출을 촉구하려는 목적도 없습니다. 보안 확보를 고려할 때에는 네트워크 사업자의 기존 IoT 서비스와 하위 호환성을 유지해야 합니다.

본 문서는 IoT 서비스 플랫폼과 최종 사용자 또는 생태계 내 다른 엔터티 간 데이터 공유의 목적으로 (예컨대 스마트폰이나 PC 애플리케이션을 통해 최종 사용자와 데이터를 공유하기 위해) IoT 서비스 플랫폼(또는 IoT 연결 관리 플랫폼)에 구현된 인터페이스 및 API 와 관련된 보안 문제는 다루지 않습니다. 그와 같은 인터페이스와 API 는 '모범 사례' 인터넷 보안 기술과 프로토콜로 보안을 확보해야 합니다.

지역에 따라 필요한 경우 국가의 법규가 본 문서에 명시된 지침에 우선할 수도 있습니다.

1.4 대상 독자

본 문서가 지향하는 독자는 다음과 같습니다.

- IoT 서비스 업체에 서비스를 제공하는 네트워크 사업자
- 셀룰러 또는 유선 네트워크를 통해 새롭고 혁신적인 커넥티드 제품과 서비스(소위 "사물 인터넷")의 개발을 추진 중인 기업과 조직. 본 문서에서는 그와 같은 기업을 "IoT 서비스 업체"라고 칭하기로 합니다.

1.5 정의

용어	설명
장치 호스트 식별 보고	엔드포인트가 네트워크 사업자에게 호스트 정보를 보고하는 능력을 말합니다. GSMA 연결 효율 가이드라인[17] 참고
다이어미터	다이어미터는 컴퓨터 네트워크의 인증, 인가, 과금 프로토콜입니다. IETF RFC 6733 [18] 참조
엔드포인트	엔드포인트란 인터넷과 연결된 제품이나 서비스의 일부로서 기능이나 임무를 수행하는 실물 컴퓨팅 장치를 말합니다. CLP.13[29]의 3 절에 IoT 장치의 3 대 분류와 각 엔드포인트 분류별 예가 제시돼 있습니다.
게이트웨이	주로 경량 엔드포인트 장치(로컬 네트워크를 통해 연결된 것)와 장거리 네트워크를 연결하는 복잡한 엔트포인트 장치를 말합니다. 자세한 내용은 CLP.13 [29]를 참고하십시오.

용어	설명
사물 인터넷	복수의 기계와 디바이스, 어플라이언스가 조율된 형태로 복수의 네트워크를 통해 인터넷에 연결된 상태를 일컫는 말. 여기서 디바이스란 태블릿, 가전제품 외에도 통신 기능이 있어 데이터를 주고 받을 수 있는 자동차, 모니터, 센서 등 일상적인 기물을 통칭합니다.
IoT 연결기능 관리 플랫폼	보통 네트워크 사업자가 호스팅하는 시스템으로서 IoT 서비스 업체가 IoT 구독과 요금을 자체 관리할 때 이용하는 것을 말합니다.
IoT 서비스	IoT 디바이스에서 나온 데이터를 이용해 서비스를 하는 컴퓨터 프로그램을 통칭합니다.
IoT 서비스 플랫폼	IoT 서비스 업체가 호스팅하는 서비스 플랫폼으로 엔드포인트와 통신하여 IoT 서비스를 제공하는 것을 말합니다.
IoT 서비스 업체	새롭고 혁신적인 커넥티드 제품과 서비스를 개발하고자 하는 기업이나 조직을 말합니다. 네트워크 사업자도 IoT 서비스 업체가 될 수 있습니다.
경량 엔드포인트	게이트웨이 장치를 통해 IoT 서비스와 연결되는 제한된 장치(예: 센서, 액추에이터)
네트워크 사업자	IoT 엔드포인트 장치를 IoT 서비스 플랫폼과 연결하는 통신 네트워크의 운영업자를 말합니다.
UICC	ETSI TS 102 221 에 명시된 보안 요소 플랫폼으로서 암호화를 통하여 분리된 보안 도메인에서 복수의 표준화 네트워크 또는 서비스 인증 애플리케이션을 지원할 수 있는 것을 말합니다. ETSI TS 102 671 에 명시된 임베디드 폼 팩터 안에 구현될 수도 있습니다.
장거리 네트워크	지리적으로 넓은 지역까지 이어지는 이동통신 네트워크를 말합니다.

1.6 약어

용어	설명
3GPP	3 세대 프로젝트 파트너십
AKA	인증과 핵심 협약
APDU	애플리케이션 프로토콜 데이터 장치
API	응용 프로그래밍 인터페이스
APN	액세스 포인트 이름

용어	설명
BGP	경계 게이트웨이 프로토콜
CEIR	중앙 장비 식별 레지스터
CERT	컴퓨터 비상 대응팀
DNS	도메인 이름 체계
DoS	서비스 거부
DPA	데이터 처리 협약
EAB	액세스 금지 확대
EAP	확장형 인증 프로토콜
EID	eUICC ID
ETSI	유럽 전기통신표준위원회
EU	유럽연합
eUICC	임베디드 UICC
FASG	사기 및 보안 그룹
GCF	글로벌 인증 포럼
GGSN	게이트웨이 GPRS 지원 노드
GPRS	일반 패킷 무선 서비스
GRX	GPRS 로밍 익스체인지
GSM	글로벌 모바일 통신 시스템
GSMA	GSM 협회
GTP	GPRS 터널링 프로토콜
HLR	홈 위치 레지스터
HSS	홈 가입자 서버
ICCID	집적회로 카드 ID
IMEI	국제 모바일 기지국 장비 ID
IMSI	국제 모바일 가입자 ID
IoT	사물 인터넷
IP	인터넷 프로토콜

용어	설명
IPSec	인터넷 프로토콜 보안
L2TP	2 단계 터널링 프로토콜
LBO	로컬 브레이크아웃
LPWAN	저전력 장거리 네트워크
LTE	롱텀 에볼루션
M2M	머신 대 머신
MAP	모바일 애플리케이션 부품
MME	이동성 관리 엔터티
OMA	오픈 모바일 연대
OSS	운영 지원 시스템
OTA	공중
PTCRB	원래 PCS 형식 인증 검토위원회를 나타내는 약어였으나 현재 해당 없음.
RAN	무선 접속 네트워크
SAS	보안 인정 제도
SGSN	GPRS 지원 노드 서비스
SIM	구독자 ID 모듈
SMS	단문 서비스
SoR	로밍 운영
SS7	신호 시스템 7 호
UMTS	만국 모바일 전기통신 서비스
USSD	비구조 보조 서비스 데이터
VLR	방문자 위치 레지스터
VPN	가상 사설 네트워크
VoLTE	보이스 오버 LTE
WAN	장거리 네트워크

1.7 참고 문서

참고	문서 번호	제목
[1]	ETSI TS 102 225	UICC 기반 애플리케이션을 위한 보안 패킷 구조(Secured packet structure for UICC based applications) www.etsi.org
[2]	ETSI TS 102 226	UICC 기반 애플리케이션을 위한 원격 APDU 구조(Remote APDU structure for UICC based applications) www.etsi.org
[3]	3GPP TS 31.102	만국 가입자 ID 모듈(USIM) 애플리케이션의 특성(Characteristics of the Universal Subscriber Identity Module (USIM) application) www.3gpp.org
[4]	해당 없음	오픈 모바일 API 규격(Open Mobile API specification) www.simalliance.org
[5]	OMA DM	OMA 장치 관리(OMA Device Management) www.openmobilealliance.org
[6]	OMA FUMO	OMA 펌웨어 업데이트 관리 객체(OMA Firmware Update Management Object) www.openmobilealliance.org
[7]	GSMA SGP.02	임베디드 UICC 기술 규격을 위한 원격 프로비저닝 아키텍처(Remote Provisioning Architecture for Embedded UICC Technical Specification) www.gsma.com
[8]	ETSI TS 102 310	UICC 에서 확장형 인증 프로토콜 지원(Extensible Authentication Protocol support in the UICC) www.etsi.org
[9]	3GPP TS 23.122	유휴 모드에서 모바일 기지국(MS)과 관련된 비접속 스트라텀(NAS)(Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode) www.3gpp.org
[10]	NISTIR 7298	주요 정보보안 용어(Glossary of Key Information Security Terms) www.nist.gov
[11]	GSMA CLP.11	IoT 보안지침 개요서(IoT Security Guidelines Overview Document) https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[12]	해당 없음	모바일 연결 개론- 디지털 인증의 새 표준(Introducing Mobile Connect – the new standard in digital authentication) https://www.gsma.com/identity/mobile-connect
[13]	3GPP TS 34.xxx	3GPP 34 시리즈 규격(3GPP 34 series specifications) www.3gpp.org/DynaReport/34-series.htm

참고	문서 번호	제목
[14]	3GPP TS 37.xxx	3GPP 37 시리즈 규격(3GPP 34 series specifications) www.3gpp.org/DynaReport/37-series.htm
[15]	3GPP TS 31.xxx	3GPP 31 시리즈 규격(3GPP 34 series specifications) www.3gpp.org/DynaReport/31-series.htm
[16]	GSMA FS.04	UICC 생산의 보안 인정 제도(Security Accreditation Scheme for UICC Production) http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
[17]	GSMA CLP.03	IoT 장치 여결 효율 가이드라인(IoT Device Connection Efficiency Guidelines) https://www.gsma.com/iot/iot-device-connection-efficiency-guidelines/
[18]	IETF RFC 6733	다이어미터 기본 프로토콜(Diameter Base Protocol) www.ietf.org
[19]	ETSI TS 102 690	머신 간 통신(Machine-to-Machine communications (M2M)); 기능 아키텍처(Functional architecture) www.etsi.org
[20]	TR-069	CPE WAN 관리 프로토콜(CPE WAN Management Protocol) www.broadband-forum.org
[21]	해당 없음	OpenID 커텍트(OpenID Connect) openid.net/connect/
[22]	해당 없음	FIDO 연대(Fast IDentity Online Alliance) fidoalliance.org/
[23]	ETSI TS 102 204	모바일 커머스, 모바일 서명 서비스, 웹 서비스 인터페이스(Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface) www.etsi.ord
[24]	해당 없음	국립표준기술원(National Institute of Standards and Technology (NIST)) www.nist.gov
[25]	해당 없음	크립토그래피 발전 유럽 네트워크(European Network of Excellence in Cryptology (ECRYPT)) www.ecrypt.eu.org
[26]	GSMA CLP.12	IoT 서비스 생태계를 위한 IoT 보안 지침(IoT Security Guidelines for IoT Service Ecosystem) https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

참고	문서 번호	제목
[27]	IETF RFC 5448	3 세대 인증 및 핵심 협약을 위한 확장성 인증 개선 프로토콜 방법(Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) tools.ietf.org/html/rfc5448)
[28]	IETF RFC 4186	GSM 구독자 ID 모듈을 위한 확장형 인증 프로토콜 방법(EAP-SIM)(Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM))tools.ietf.org/html/rfc4186
[29]	GSMA CLP.13	IoT 엔드포인트 생태계를 위한 IoT 보안 지침(IoT Security Guidelines for IoT Endpoint Ecosystem) https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[30]	해당 없음	LTE 네트워크 무선 보안(Wireless Security in LTE Networks) www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili_WirelessSecurity_121029_FINAL.pdf
[31]	해당 없음	oneM2M 사양(oneM2M Specifications) www.oneM2M.org
[32]	GSMA CLP.17	IoT 보안 평가 체크리스트(IoT Security Assessment Checklist) https://www.gsma.com/iot/iot-security-assessment/
[33]	해당 없음	LPWA 기술 보안 비교(LPWA Technology Security Comparison). Franklin Heath Ltd 의 백서 https://goo.gl/JIOlr6
[34]	CLP.28	NB-IoT 배포 가이드(NB-IoT Deployment Guide) www.gsma.com/iot
[35]	CLP.29	LTE-M 배포 가이드(LTE-M Deployment Guide) www.gsma.com/iot
[36]	3GPP TS33.163	저산출 머신형 통신(MTC) 장치를 위한 배터리 효율 보안(BEST)(Battery efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST)) www.3GPP.org

2 네트워크 사업자가 보호할 수 있는 IoT 서비스 자산

IoT 자산을 제대로 보호하기 위해 구현해야 하는 보안 기능은 서비스마다 다릅니다. 그러므로 IoT 서비스 업체는 적절한 위험 및 프라이버시 영향 평가 과정을 적용해 구체적인 보안 수요를 도출할 책임이 있습니다. 네트워크 사업자와 IoT 서비스 업체는 자산 보호를 위한 보호 요건이 유사할 때가 많으므로 둘이 보안 인프라를 중복해 (때로 불필요하게) 구현하기보다 공통의 보안 솔루션을 이용하는 편이 현명하다 하겠습니다. 또한 네트워크 사업자가 IoT 서비스 업체를 겸하는 경우도 많습니다.

네트워크 사업자가 제공하는 보안 서비스는 IoT 서비스를 제공할 때 사용되는 자산의 보안에서도 중요한 역할을 하기도 합니다. 예를 들면 다음과 같습니다.

- IoT 엔드포인트와 IoT 서비스 플랫폼 사이에 주고 받는 IoT 서비스 데이터 - 여기에는 프라이버시가 중요한 1 차 데이터(예: 최종 사용자 관련 데이터)와 2 차 프라이버시 영향이 있을 수도 있고 상업적으로 익스플로잇 가능한 데이터(예: 액추에이터 제어 데이터)가 모두 포함됩니다.
- 보안 자산(IMSI, 키세트 등)과 엔드포인트 장치(게이트웨이 장치 포함) 안에서 사용되는 네트워크 구성 설정(APN, 타이머값 등).
- IoT 서비스 업체의 사업 관련 중요 정보 - 브랜드 평판, 회사가 책임지고 있는 고객/사용자 데이터, 전략 정보, 재무 데이터, 건강 기록 등.
- IoT 서비스 업체의 사업 인프라, 서비스 플랫폼, 기업 네트워크, 기타 사설 네트워크 구성요소.
- 네트워크 사업자가 제공하고 IoT 서비스에서 이용되는 공용(즉 공유) 데이터센터 인프라. 여기에는 공용 서비스와 호스팅 기능, 가상화 인프라, 클라우드 시설 등이 포함됩니다.
- 통신 네트워크 인프라 - 무선 접속 네트워크, 코어 네트워크, 백본 네트워크, 기본 서비스 기능(DNS,BGP 등), 유선 및 무선 네트워크 접속과 취합 등.

3 네트워크 보안의 원칙

네트워크 사업자는 자사 네트워크 안에 적절하고 믿을 수 있는 보안 메커니즘을 구현해야 합니다.

이번 섹션에서는 IoT 생태계에서 네트워크가 가치를 창출하는 방안을 소개합니다.

통신 네트워크에서 제공하는 가장 기본적인 보안 메커니즘으로는 다음을 꼽을 수 있습니다.

- IoT 서비스에 관여하고 있는 엔터티들(즉 게이트웨이, 엔드포인트 장치, 홈 네트워크, 로밍 네트워크, 서비스 플랫폼)의 식별과 인증.
- IoT 서비스 생성을 위해 연결이 필요한 여러 엔터티의 접속 통제.
- 네트워크가 IoT 서비스를 위해 취급하는 정보의 보안(기밀유지, 무결성, 가용성, 진정성)과 프라이버시를 확보하기 위한 데이터 보호.
- 네트워크의 가용성을 확보하고 그것을 공격으로부터 보호하는 프로세스와 메커니즘(예: 적합한 방화벽, 침입 예방, 데이터 필터링 기술의 도입 등)

3.1 사용자와 애플리케이션, 엔드포인트 장치, 네트워크 및 서비스 플랫폼의 안전한 식별.

식별은 IoT 서비스 내 엔터티에게 고유한 식별자를 제공하고 그 전자 식별정보를 법적 구속력이 있는 현실의 신원(ID)과 연계하는 과정으로 구성됩니다.

셀룰러로 연결된 IoT 서비스 안에서 엔드포인트 장치는 IMSI 및/또는 IMEI(eUICC 가 있는 장치는 EID 도 이용 가능)로 식별됩니다. 네트워크는 네트워크 코드와 국가 코드로 식별됩니다. ID 를 제공하는 방법은 저마다 보안을 확보하는 수준이 다릅니다.

ID 는 인증 과정에서 매우 중요한 역할을 합니다. 안전한 인증은 안전한 ID 없이는 불가능하기 때문입니다. 그러므로 IoT 서비스 안에서 발급되고 사용되는 ID(IMSI, IMEI, ICCID 등)는 무단 변경이나 사칭, 도용이 일어나지 않도록 철저히 보호해야 합니다.

IoT 서비스 업체가 맞닥뜨릴 수도 있는 실질적인 문제 가운데 하나가 서비스를 위해 여러 IoT 서비스 플랫폼과 통신해야 할 때 플랫폼마다 다른 ID 를 요구하는 상황입니다. 각 IoT 서비스 플랫폼과 통신 링크를 세울 때 사용되는 ID 를 IoT 서비스에서 각각 따로 안전하게 프로비전닝해 저장하고 관리해야 하는 것입니다.

IoT 서비스에 적합하다면 네트워크 사업자는 UICC 기반의 메커니즘을 이용해 엔드포인트 장치를 안전하게 식별하는 방법을 권장합니다. 네트워크 사업자는 또 UICC 에서 제공하는 보안 저장 기능을 IoT 서비스 업체에게도 제공해 UICC 에 ID 와 관련된 추가 IoT 서비스를 저장하게 할 수도 있습니다. 이 기법은 셀룰러와 비셀룰러 엔드포인트 장치(예: EAP-AKA[27])에 모두 적용할 수 있습니다.

네트워크 사업자는 또 “단일 로그온” 서비스도 제공해 엔드포인트 장치가 ID 를 한 번 정해서 검증하면 추가로 번거로움 없이 복수의 IoT 서비스 플랫폼에 연결하게 할 수도 있습니다. 그와 같은 서비스를 이용하는 데 따르는 단점과 위험은 각 플랫폼 전체를 대상으로 검토해야 합니다.

3.2 사용자와 애플리케이션, 엔드포인트 장치, 네트워크 및 서비스 플랫폼의 안전한 인증.

NIST 에 따르면[10], "인증"이란 "사용자나 프로세스, 엔드포인트 장치의 신원을, 때로는 정보 시스템 안에 있는 리소스에 액세스하기 위한 전제조건으로서 검증하는 것"을 말합니다.

네트워크 사업자는 어떤 IoT 서비스와 관련된 사용자와 애플리케이션, 엔드포인트 장치, 네트워크, 서비스 플랫폼이 안전하게 인증을 받는 서비스를 제공할 수 있습니다.

인증에는 관련된 속성이 있습니다. 부인봉쇄(non-repudiation)가 그것입니다. NIST [10]는 부인봉쇄를 “발신자에게는 전달의 증거를 제공하고 수신자에게는 발신자 신원의 증거를 제공하여 양측 누구도 나중에 그 정보를 처리했음을 부인하지 않는다는 보장"이라고 정의하고 있습니다". 부인봉쇄는 해당 거래나 메시지의 출처를 식별할 때 진정성이 훼손되지 않았다는 주장을 기초로 합니다.

3.3 안전한 통신 채널의 제공

네트워크 사업자는 "동급 최고"의 통신 무결성과 기밀유지, 진정성을 제공하는 장거리 셀룰러 및 유선 네트워크에게 여러 가지 통신 보안 메커니즘을 제공합니다. 네트워크 사업자는 적절하다면 VPN 과 암호화 인터넷 연결을 이용해 기업 네트워크에 보안 연결을 제공하고 관리하기도 합니다.

보안 통신 채널의 목적은 이 채널을 통해 전달되는 데이터가 데이터 주체의 인지 및 동의 없이 처리되거나 사용되거나 전송되지 않게 하는 것입니다. 암호화 기술이 기밀유지와 무결성, 진정성이라는 속성을 보장함으로써 안전한 데이터 전송에서 매우 중요한 역할을 합니다.

암호화는 경량 엔드포인트 장치와 네트워크 측면(백엔드 역송 제약), 제공되는 서비스를 고려하여 구축 중인 시스템에 적합한 것이어야 합니다.

네트워크 사업자는 IoT 서비스 업체에게 데이터 암호화 서비스를 제공하여 통신의 무결성과 네트워크의 회복력을 확보하게 할 수 있습니다.

네트워크 사업자는 예로부터 공용 이동통신 인프라 또는 공용/사설 겸용 네트워크 인프라를 제공했습니다. 네트워크 사업자 중에는 공용 네트워크 인프라를 통과하는 고객/사용자 데이터에 대해 공용 네트워크를 들어오는 시점부터 나가는 시점까지 암호화를 할 수 있는 곳이 많습니다. 네트워크 사업자는 또 필요하다면 IoT 서비스 업체를 도와 자체 암호화 자격증명을 도입하거나 도출하여 자사 인프라를 통과하는 동안 IoT 데이터의 보안을 확보할 수도 있습니다.

네트워크 사업자는 어느 한 고객에게 전용 통신 채널이 제공되는 경우 자사 고객에게 사설 네트워크를 제공하여 데이터가 인터넷 등 공용 네트워크를 지나가지 못하게 할 수 있습니다. 그와 같은 사설 네트워크는 다음 방법으로 만들 수 있습니다.

그림 1 L2TP(Layer Two Tunnelling Protocol)와 같은 터널링 프로코콜과 IPsec(Internet Protocol Security)과 같은 보안 프로토콜을 이용한다

그림 2 예컨대 BEST[36]를 이용해 UE 와 애플리케이션 서버 간에 전면(end-to-end) 보안을 제공한다

그림 3 아래 보기와 같이 공유 무선 네트워크가 포함된 별도 인스턴스의 코어 네트워크를 도입하여 IoT 서비스를 위한 전용 네트워크를 만든다.

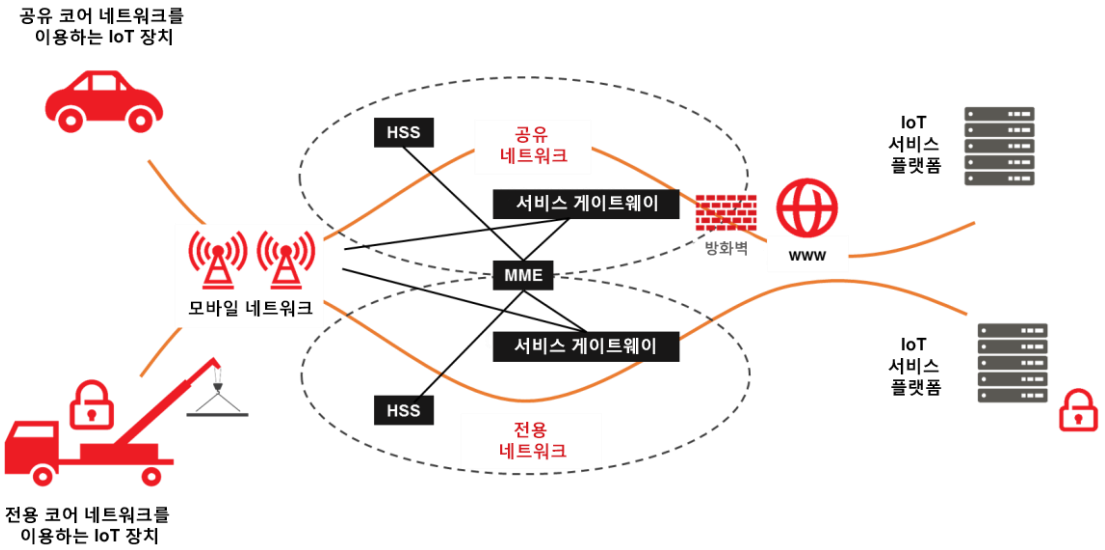

그림 2 사설 네트워크 구성의 예

3.4 통신 채널의 가용성 확보

NIST 에 따르면[10], "가용성"이란 인가 받은 엔터티가 요구하면 재산에 접속할 수 있고 이용할 수 있는 상태를 말합니다.

네트워크 사업자는 IoT 서비스 업체에게 가용한 네트워크를 제공할 수 있습니다. 네트워크 사업자가 네트워크 가용성을 확보하기 위해 제공하는 메커니즘 중에서 가장 기본이 되는 것은 다음과 같습니다.

3.4.1 라이센스 스펙트럼의 이용

GSMA 네트워크 사업자 구성원들은 각국 규제당국이 발급한 면허의 조건에 따라 허가 받은 전용 스펙트럼을 이용해 네트워크를 운영할 것입니다. 허가 받은 스펙트럼을 이용하면 다른 무선 기술의 간섭이 최소로 유지됩니다. 이 스펙트럼을 무단으로 사용하면 처벌을 받기 때문입니다. 네트워크 사업자와 규제당국은 무단 간섭을 찾아내 네트워크 가용성이 영향을 받지 않게 할 것입니다.

허가 받은 스펙트럼을 이용하면 네트워크 사업자가 자사 네트워크를 전용 무선 대역에서 운영할 수 있고 네트워크 도달 범위와 용량을 면밀하게 계획할 수 있어 고객을 위해 최대한의 네트워크 가용성을 실현할 수 있습니다.

3.4.2 표준화되고 검증된 네트워크 기술의 구현

GSMA 의 네트워크 사업자 구성원은 3GPP 와 같은 표준 기구에서 정한 GSM, UMTS, LTE 등 표준 네트워크 기술을 구현합니다. 표준 기술을 적용하면 네트워크 사업자 간에 상호호환성이 확보되며, 표준이 개발 단계에서 면밀한 검토를 받으므로 기술의 내구성이 보장됩니다.

3.4.3 시험과 인증을 마친 네트워크 기술의 구현

네트워크 사업자의 네트워크를 구성하는 부품 중에서 다수가 국제 시험 표준에 따라 시험과 인증을 받습니다. 그 안에 들어 있는 복잡한 엔드포인트 장치와 통신 모듈들은 GCF 와 PTCRB, 네트워크 사업자의 인수 시험을 통해 3GPP 시험 규격[13]의 적용을 받습니다. RAN(Radio Access Network)은 네트워크 사업자의 인수 시험을 통해 3GPP 시험 규격[14]의 적용을 받습니다. UICC 는 네트워크 사업자의 인수 시험을 통해 3GPP 시험 규격[15]의 적용을 받으며, 추가로 GSMA SAS 인증[16]을 받을 수도 있습니다.

3.4.4 견고한 네트워크 토포그래피와 구성

네트워크 사업자는 필요한 지리적 리던던시와 격리 안에서 견고한 네트워크를 구현하고 구축해 가용성은 극대화하고 유휴시간은 최소화합니다. 네트워크 구성요소는 엄격한 품질 서비스와 서비스 수준 협약에 맞춰 모두 면밀하게 구성하고 모니터링합니다.

3.4.5 실시간 모니터링과 네트워크 리소스의 관리

네트워크 사업자는 첨단 네트워크 운영 센터를 마련해 자사 네트워크의 성능을 주야 24 시간 실시간 모니터링하면서 네트워크 트래픽을 관리하고 네트워크 수요에 대응하며 고장을 수리합니다. 자세한 내용은 4.10 절에서 확인할 수 있습니다

3.4.6 위협 관리와 정보 공유

GSMA 의 사기 및 보안 그룹(FASG)에서는 네트워크 사업자 모두가 사기 및 보안 첩보, 사고 세부내용을 적기에 분별력 있게 공유할 수 있는, 열리고 믿을 수 있는 환경을 제공합니다. 이 그룹에서는 전 세계의 사기 및 보안 위협 현황을 평가하고 네트워크 사업자와 그 고객을 대신해 관련된 위협을 분석하며, 대응 조치를 지정하고 우선순위를 설정합니다.

3.4.7 로밍 서비스

네트워크 사업자는 표준 네트워크과 엔드포인트 장치 기술 및 상호연결 서비스 덕분에 네트워크 로밍 서비스를 제공하여 고객을 위한 네트워크 도달 범위와 가용성을 더욱 높이고 있습니다.

3.4.8 엔드포인트 장치 성능의 모니터링과 관리

네트워크 사업자는 자사 네트워크에 연결되는 엔드포인트 장치의 성능을 측정하여 전체 네트워크의 성능을 떨어뜨릴 만큼 무선 간섭(예: 국내 규정에 맞지 않음)이나 네트워크 신호 트래픽(예: GSMA 연결 효율 가이드라인[17]에 부합하지 않음)이 과도한 엔드포인트 장치를 격리할 수 있습니다. 이렇게 엔드포인트 장치는 비정상적 거동이 탐지됐을 때 모니터링하거나 연결을 해제하거나 펌웨어 업데이트를 할 수 있습니다.

4 사생활 보호 문제

IoT 에서 제공하는 기회를 현실로 만들기 위해서는 IoT 서비스를 제공하고 소비자 데이터를 수집하는 IoT 서비스 업체를 소비자가 믿는 것이 중요합니다. GSMA 와 그 구성원들은 사용자가 프라이버시를 제대로 존중 받고 보호 받는다고 느낄 때에만 소비자의 신뢰와 믿음이 생긴다고 믿고 있습니다.

이미 세계 각국에 데이터 보호와 프라이버시 법률이 잘 마련돼 네트워크 사업자들이 철저히 적용하고 준수하고 있습니다. 네트워크 사업자들은 기존 데이터 보호 규정과 원칙만으로도 IoT 서비스와 기술에서 프라이버시 니즈를 해결할 수 있다고 생각합니다.

그러나 IoT 서비스에서는 통상 사업자들이 IoT 서비스 업체 파트너들과 함께 업무를 진행합니다. 그러므로 IoT 서비스와 관련해서는 규정과 법제도가 명확해야 하며 프라이버시와 데이터 보호 규정은 어느 한 서비스와 기술에 치우치지 않고 IoT 서비스 업체 전체에 일관성 있게 적용되어야 합니다.

네트워크 사업자는 데이터를 처리할 때 IoT 서비스 업체와 데이터 처리 협약(DPA)을 맺어야 하는 부분이 존재하는지 알고 있어야 합니다. 특정 IoT 서비스를 위해 개발된 데이터 보호 및 보안 실무에는 개인의 프라이버시에 대한 전반적 위험과 개인에 관한 데이터가 수집, 배포, 사용되는 상황이 반영돼 있어야 합니다. 규제의 개입은 확인된 위험이 현실에 나타나 기존 조치로는 대응이 충분하지 않을 때로 한정해야 합니다. 예컨대, oneM2M(TS-0003 [31])은 사업자에게 서비스 업체를 대신한 프라이버시 관리자 역할을 허용하고 있습니다.

네트워크 사업자는 프라이버시 및 보안 문제 취급에서 쌓은 폭넓은 경험을 이용하여 IoT 서비스와 협력해 IoT 기술과 전반적인 소비자 환경에 프라이버시와 보안을 접목할 수 있습니다. 이와 같은 협업으로 IoT 서비스 업체는 제공되는 서비스와 관련해 소비자 프라이버시 침해 위험을 찾아내 대응할 수 있습니다.

더 자세한 사항은 GSMA 모바일 프라이버시 원칙 (http://www.gsma.com/publicpolicy/mobile-and-privacy/mobile-privacy-principles)을 참고하기 바랍니다

5 네트워크 사업자가 제공하는 서비스

네트워크 사업자는 IoT 서비스 업체에게 안전한 셀룰러 네트워크와 유선 장거리 네트워크(WAN)를 제공합니다.

본 절에서는 IoT 서비스를 장거리 네트워크에 연결할 때 적용할 수 있는 모범사례 권고사항을 설명합니다. 권고사항은 사용되는 기술과는 별개이나, 적절하다면 셀룰러 및 기타 네트워크 유형에서 나온 모범사례도 이용합니다.

5.1 안전한 가입자 관리 절차

본 절에서는 IoT 서비스 업체의 가입자를 네트워크 사업자가 관리하는 방식에 관해 권고사항을 제시합니다.

- 네트워크 사업자나 IoT 서비스 업체는 현재 또는 미래의 IoT 서비스(음성, 데이터, SMS 등)를 구현하는 데 필요한 네트워크 서비스를 평가해야 합니다.
- 네트워크 사업자는 이 평가 결과를 근거로 "최소 권한의 원칙"과 규정에 따라 특정 IoT 서비스에 필요한 서비스만으로 IoT 서비스 업체의 가입자를 관리해야 합니다. 예를 들면 다음과 같다.
    - 데이터 보유자만을 이용하는 IoT 서비스에 대해서는 음성과 SMS 서비스를 프로비저닝하면 안 됩니다.
    - 엔드포인트 장치가 알려져 있는 IoT 서비스 플랫폼에만 연결되는 경우, 그 장치와 관련된 가입자는 알려져 있는 IP 주소 범위(또는 도메인) 화이트리스트에만 연결이 가능해야 합니다.
    - IoT 서비스가 음성이나 SMS 를 이용하는 경우, 사전 구성된 고정 다이얼링 목록의 이용을 고려해야 합니다.
- 네트워크 사업자는 IoT 가입자를 위해 핵심적인 IoT 서비스(예컨대 주요 의료 서비스)를 구현할 수 있는 보안 가입자 관리 프로세스를 구현해야 합니다. 이들 서비스는 임의로 해제하면 안 됩니다.
- 네트워크 사업자는 IoT 서비스에 사용되는 UICC 를 종래의 서비스 제공에 사용되는 종래의 UICC 와 분리하고 IoT 서비스 업체가 요구하면 둘을 적당히 분리해야 합니다.
    - IoT 서비스에 사용되는 UICC 가 종래의 "핸드셋"에 사용되는 UICC 와 분리된다면 네트워크 사업자가 그렇지 않을 때보다 관련 가입자를 더 안전하고 효율적으로 관리할 수 있는 발판이 됩니다. 예컨대, 수명이 더 길고 UICC 를 더 오랫동안(몇 년) 지원하도록 구성하기 좋은 엔드포인트 장치를 대상으로 별도의 HLR/HSS 를 배정하는 것입니다.

5.1.1 UICC 공급과 관리

5.1.1.1 UICC 의 원격 관리(OTA)

상황에 따라 IoT 엔드포인트 장치에 물리적으로 접근하기가 불가능할 때도 있습니다. UICC 를 원격으로 변경하기 위해서는 네트워크 사업자가 UICC OTA 관리를 지원해야 합니다. UICC OTA 보안 메커니즘은 최신 ETSI[1][2]와 3GPP[3] 규격을 따르고 IoT 서비스에게 가장 적합한 수준의 보안을 적용해야 합니다.

IoT 엔드포인트는 UICC 에서 인정한 필요 APDU 명령를 지원하여 UICC OTA 의 명령 실행이 성공하게 해야 합니다.

5.1.1.2 탈착이 불가능한 UICC

네트워크 사업자는 서비스 위협 모델에서 IoT 엔드포인트 장치가 물리적 탬퍼링에 취약할 수도 있다고 경고하면 IoT 서비스에게 떼어낼 수 없는 UICC(즉 머신 폼팩터)를 제공해야 합니다.
추가로 보안 대책을 적용하여 그러한 위협을 탐지하고 대응할 수 있어야 합니다.

5.1.1.3 임베디드 UICC(eUICC)의 원격 관리

네트워크 사업자는 엔드포인트 장치가 원격 또는 닿기 힘든 곳에 위치해야 하는 IoT 서비스를 위해 탈착이 불가능한 UICC(즉 eUICC)를 안전하게 원격으로 관리해야 합니다.

예를 들면 IoT 서비스 업체가 엔드포인트 장치에 임베드되는 다수의 eUICC 를 관리해야 하는데 그 업체가 eUICC 의 소유자도 아니고 쉽게 접근할 수도 없을 때를 말합니다(예, 자동차).

일반적으로 네트워크 사업자는 IoT 연결상태 관리 플랫폼을 이용해 (e)UICC 에서 IoT 장치에게 제공하는 통신 서비스를 모니터링하고 제어합니다.

네트워크 사업자는 GSMA 의 임베디드 UICC 를 위한 원격 프로비저닝 아키텍처 기술 규격[7](Remote Provisioning Architecture for Embedded UICC Technical Specification)을 지원해야 합니다.

5.1.1.4 UICC 기반 서비스

네트워크 사업자가 IoT 서비스 업체에 UICC 기반 서비스를 제공할 수도 있습니다. 그러면 IoT 서비스 업체는 자사 IoT 서비스를 대상으로 UICC 를 탬퍼링에 강하고 안전한 플랫폼으로 이용할 수 있습니다. 그와 같은 UICC 기반 서비스는 보통 JavaCard™ 로 만들며 JavaCard™ 에 부합하는

UICC 카드 간에 상호운용이 가능합니다. 그와 같은 IoT 엔드포인트 애플리케이션의 예로는 네트워크 품질의 모니터링과 보고를 들 수 있습니다. UICC 플랫폼의 탬퍼링 저항력은 공격자가 물리적으로 접근할 수 있는 IoT 엔드포인트 장치에게 매우 유용합니다. UICC 를 모든 이해관계자를 위해 공통의 보안 요소로 이용해도 보안 IoT 엔드포인트 장치의 비용 대비 효과가 높아질 수도 있습니다.

또한 IoT 서비스에서 민감한 데이터를 탬퍼링에 강한 저장장치(IoT 서비스 업체가 관리하는 보안 키)에 저장하고자 할 때에도 UICC 를 쓸 수 있습니다. ETSI TS 102 225[1]은 글로벌 플랫폼 카드 규격 중 기밀 카드 콘텐츠 관리 기능을 이용해 IoT 서비스 업체가 UICC 에서 자기 보안 영역을 독자적으로 관리할 수 있게 하고 있습니다.

IoT 서비스 업체나 네트워크 사업자는 UICC 공급업자에게 UICC 안에 그와 같은 보안 영역을 만들어 달라고 요청할 수 있습니다. UICC 의 발급자는 그것이 적절한 보안 키로 보호를 받는지, 또 IoT 엔드포인트가 그것에 액세스하기 위해 필요한 APDU 명령을 실행하는지 확인해야 합니다.

UICC 는 또 IoT 서비스의 민감한 콘텐츠를 (안전하게 저장된 키를 이용해) 암호화하여 발송하거나 Open Mobile API [4] 또는 oneM2M TS-0003 [31]과 같은 서비스를 통해 엔드포인트 장치 기반의 애플리케이션에 보안 서비스를 제공할 때에도 쓸 수 있습니다.

5.1.1.5 안전한 UICC 제조와 프로비저닝

네트워크 사업자는 GSMA 의 보안 인정 제도(SAS)[16]에 따라 제조 및 프로비저닝 공정을 인정 받은 제조사에게서 UICC 를 공급 받아야 합니다.

5.2 네트워크 인증과 암호화 알고리즘

본 섹션에서는 여러 가지 장거리 네트워크를 위한 네트워크 인증 및 링크 암호화 권고사항과 모범사례를 소개합니다.

네트워크 사업자는 IoT 서비스 업체의 엔드포인트 장치의 기대 수명에 맞는 네트워크 인증 알고리즘을 구현해야 합니다.

네트워크 사업자들은 IoT 서비스 업체를 위해 USSD, SMS, IP 데이터 연결성 등 여러 가지 통신 서비스를 제공합니다. 본 문서에서는 그 목적상 IP 데이터 연결만 소개합니다. IoT 서비스에서 가장 많이 사용하는 통신 서비스이기 때문입니다.

USSD 와 SMS 도 기존 IoT 서비스 업체에서 많이 사용하는데, 다만 IP 데이터 연결보다는 보안 지원의 폭이 좁습니다. 일반적으로 USSD 와 SMS 트래픽은 네트워크 사업자가 '처음부터 끝까지' 크립토그래픽 방식으로 보호하지 않으며, 기밀유지와 무결성 확보를 위한 크립토그래픽 보호장치가 SMS 에는 제공되지 않습니다. 통신에 USSD 나 SMS 를 이용하는 IoT 서비스 업체라면 USSD 와 SMS 와 관련된 취약성의 존재를 명심하고 가능하다면 서비스 레이어에 추가로 암호화 조치를 구현하기 바랍니다.

5.2.1 GSM/GPRS(2G) 시스템의 보안

GSM/GPRS 네트워크를 제공하는 네트워크 사업자는 다음과 같이 조치해야 합니다.

- 최소한 128 비트 A5/3 스트림 사이퍼를 이용해 IoT 엔드포인트 장치와 기지국 간 링크를 보호해야 합니다. 네트워크 사업자는 가급적 A5/1 와 A5/2 또는 암호화되지 않은 링크의 사용을 피해야 합니다.
- MILENAGE 인증 알고리즘을 이용해야 합니다. 네트워크 사업자는 COMP128-1 과 COMP128-2 를 피해야 합니다. 네트워크 사업자는 TUAK 인증 알고리즘의 지원을 고려해야 합니다
- 적절한 대책을 강구해 의사 기지국 공격(false base station attack)에 대처해야 합니다.

GSM/GPRS 시스템에서는 네트워크가 엔드포인트 장치에게 인증을 받지 않습니다. 장치만 네트워크에게 인증을 받습니다. 그러므로 GSM/GPRS 시스템을 이용할 때에는 서비스 레이어에서 전범위(end to end) 암호화를 권장합니다. IoT 서비스에서 제공되는 솔루션에 실질적 처리와 엔드포인트 제한, 네트워크 대역폭 제한도 고려해야 합니다.

GSM/GPRS 시스템에서는 GRX-네트워크를 통해 생성되는 SGSN 과 GGSN 간에 GTP 터널이 암호화되지 않습니다. 네트워크 사업자는 GRX-네트워크가 사설 네트워크로 관리되게 하여 이 링크의 보안을 확보해야 합니다.

5.2.2 UMTS(3G) 시스템의 보안

UMTS 네트워크는 상호 인증이 가능합니다. 여기서는 엔드포인트 장치가 네트워크에게 인증을 받을 뿐만 아니라 네트워크도 장치에게 인증을 받습니다.

UMTS 네트워크를 제공하는 네트워크 사업자는 MILEANAGE 인증과 키 생성 알고리즘을 지원해야 합니다. 네트워크 사업자는 Kasumi 기밀유지 및 무결성 암호화 알고리즘을 지원해야 합니다.

네트워크 사업자는 TUAK 인증 알고리즘의 지원을 고려해야 합니다

5.2.3 LTE (4G) 시스템의 보안

LTE 네트워크를 제공하는 네트워크 사업자는 MILEANAGE 인증 알고리즘을 지원해야 합니다. 네트워크 사업자는 LTE EEA1, EEA2 또는 EEA3 암호화 알고리즘을 지원해야 합니다.

네트워크 사업자는 TUAK 인증 알고리즘의 지원을 고려해야 합니다.

네트워크 사업자는 GSMA 백서 “Wireless Security in LTE Networks”[30]를 살펴보기 바랍니다.

5.2.4 저전력 장거리 네트워크의 보안

지금까지 여러 네트워크 사업자가 몇 가지 저전력 장거리(LPWA) 네트워크 기술을 도입했습니다. 지금까지 도입된 LPWA 네트워크는 GSMA 홈페이지 (www.gsma.com/iot)에서 모두 찾아볼 수 있습니다.

NB-IoT[34]와 LTE-M[35] 도입 지침도 GSMA 에서 확인할 수 있습니다. 이를 통해 네트워크와 장치 모두의 측면에서 이들 기술을 일관성 있게 도입할 수 있을 것입니다.

2017 년 5 월 정보보안 애널리스트 Franklin Heath 는 “LPWA Technology Security Comparison”[33](LPWA 기술 보안 비교)라고 하는 외부 보고서를 발표했습니다. 저자는 여기서 다섯 가지 저전력 장거리(LPWA) 네트워크 기술의 보안 특징을 스마트 농업, 스마트 가로등, 연기 탐지기, 유량계, 스마트 계량기 등 몇 가지 일반적인 IoT 활용 사례에 비춰 비교하고 대조하였습니다. 이 보고서에서는 허가 받은 스펙트럼에서 작동하는 세 가지 3GPP 표준 모바일 IoT 기술, 즉 LTE-M, NB-IoT, EC-GSM-IoT 와 허가 받지 않은 스펙트럼 기술인 LoRaWAN 과 Sigfox 의 보안 특징을 평가했습니다. 이 보고서는 https://goo.gl/JIOlr6[33]에서 다운로드 받을 수 있습니다.

이 보고서는 조직이 LPWA 솔루션을 고려할 때 비용이나 배터리 수명, 네트워크 도달 범위와 같은 요소 외에 필요한 보안 수준도 파악해야 한다고 주장합니다. 그러면서 IoT 보안 니즈가 프라이버시 및 안전 문제에 얼마나 크게 좌우되는지 설명하고 LPWA 기술을 이용하는 도입은 어느 것이든 GSMA IoT 보안평가[32]와 같은 도구를 이용해 보안 위험 평가를 받아야 한다고 강조하고 있습니다.

이 보고서에서 평가 시 검토해야 하는 중요한 네트워크 보안 요소로 꼽은 것을 몇 가지 소개하자면 다음과 같습니다.

- 최대 다운링크 및 업링크 데이터 속도를 포함한 대역폭 - 이것은 LPWA 가 지원하거나 애플리케이션 레이어에 구현할 있는 보안 기능을 제한할 수도 있습니다.
- 일일 다운링크와 업링크 처리량 - LPWA 장치는 통상 OTA 보안 업데이트처럼 보안 기능이 영향을 받을 수도 있을 때에는 데이터를 전송하거나 받지 않습니다.
- 인증 - 장치, 가입자, 네트워크 - 안전한 네트워크 연결을 위해서는 장치, 가입자, 네트워크 사업자 등 여러 주체가 서로 자신을 인증해야 합니다. 기술은 악성 사용자가 이들 주체를 "스푸핑"하지 못하게 해야 합니다.
- 데이터 기밀유지 - 데이터가 공격자에게 탈취 당하지 않게 보호하는 방법으로 대개 암호화가 사용됩니다. 여기서 애플리케이션 레이어에 전범위 보안을 적용하면 신뢰가 커질 수 있습니다.
- 키 프로비저닝 - 인증과 기밀유지, 무결성 확보를 위한 크립토그래픽 기법은 모두 당사자끼리 안전하게 공유되는 크립토그래픽 키에 의존합니다.
- 인증 받은 장비 - 여러 나라에서 무선 송신 기능이 있는 장치에 대해 판매 전 승인 또는 인증을 의무화하고 있습니다. 이것은 보안 기능을 검증 받는 기회이기도 합니다.
- IP 네트워크 - IP 를 이용하면 장치가 인터넷을 통해 공격 받을 가능성이 있으므로 IP 보안 기능을 반드시 검토해야 합니다.

이 보고서는 LPWA 기술의 중요한 보안 기능 중에서 몇 가지는 적용이 선택적이라고 결론 내리고 있습니다. 네트워크 사업자가 직접 구현할 수도 있고, 네트워크 사업자의 선택에 따라 달라질 수 있기 때문입니다. 네트워크 사업자는 네트워크 구성의 선택에 따라 보안에 어떤 결과가 초래되는지 확인하고 선택의 내용이 고객에게 분명히 전달되게 해야 합니다. 선택사항 중 일부(예컨대 탈착 불가능한 eUICC 와 같은 요소의 포함 여부)는 장치 제조사의 관할이기도 합니다. 이 경우 그것을 고객에게 알릴 의무는 제조사에게 있습니다.

LPWA 기술을 이용할 때 고려해야 하는 대표적 보안 요소는 다음과 같습니다.

LPWA 네트워크 기술 공통

- IP 네트워크 레이어가 링크 레이어를 통해 구현되는가?
- 보안 요소가 존재하는가? 그렇다면 탈착이 가능한가?
- 데이터 보안은 어느 정도 보장되는가?
- 기술이 지원하는 알고리즘이나 키 길이는 블랙리스트 대상인가, 아니면 (GPRS 의 64 비트 암호화 키처럼) 반대해야 하는가?

3GPP LPWA 네트워크 기술(NB-IoT, LTE-M)

- 원격 SIM 프로비저닝(RSP)가 지원되는가?
- 어떤 무결성 알고리즘(EIAx/GIAx)과 기밀유지(EEAx/GEAx) 알고리즘이 구현되고 허용되는가?

LoRaWAN:

- ABP(Activation By Personalisation) 또는 OTAA(Over-The-Air Activation)가 구현되는가? OTAA 의 경우 장치 간에 AppKey 가 공유되는가?

SigFox

- SigFox 네트워크 이용 시 유료하중 암호화는 선택사항이지만 이용 가능하다는 점을 고려해야 합니다. 그러므로 Sigfox 인증을 받은 크립토 칩을 이용해 AES 128 암호화를 구현하고 OTA 에서 데이터의 기밀을 유지해야 합니다.

LPWA 장치 공통

- 어떤 보안 인증을 실시하였는가?

5.3 고정 네트워크의 보안

네트워크 사업자 또는 IoT 서비스 업체의 통제 하에서 EAP-SIM[28] 또는 EAP-AKA[27] 인증을 포함하거나 ETSI TS 102 310[8]의 UICC EAP 프레임워크에 의존할 수 있는 Wi-Fi 네트워크의 기본 구성에 대한 권고사항.

5.4 트래픽 우선순위 결정

네트워크 사업자는 제공되고 있는 IoT 서비스에 적합한 서비스 품질 수준을 제공할 수 있습니다.

5.5 백홀 보안

GSM 과 UMTS, LTE 를 지정하는 3GPP 표준은 암호화된 백홀 링크의 사용을 의무화하지 않습니다. 게다가 여러 네트워크 사업자가 RAN 과 백홀을 공유하면 보안 취약성이 늘어날 수도 있습니다.

네트워크 사업자는 최종 사용자 데이터와 신호면 데이터 트래픽 모두에 대해 GSM 과 UMTS, LTE 네트워크의 백홀 암호화를 구현해야 합니다.

5.6 로밍

네트워크 사업자는 로밍 서비스를 통해 IoT 서비스 업체에게 국제 모바일 통신을 제공할 수 있습니다.

로밍 네트워크는 홈과 로밍 네트워크의 연결에 사용되는 SS7/다이어미터 인터워킹 기능이 상대적으로 개방돼 있어 보안 침해에 취약할 수 있습니다. 이것은 로밍 네트워크에 존재하는 IoT 엔드포인트 장치의 비중이 높을 가능성 있어 IoT 서비스와 특히 관련이 있습니다. 로밍 엔드포인트 장치의 비중이 높은 이유에는 몇 가지 있습니다. 먼저, 엔드포인트 장치 중에는 한 곳에서 생산돼 전 세계로 유통되는 것이 많습니다. 그러므로 UICC 의 교체가 실용적이지 않을 때가 많으며, 임베디드 UICC 는 교체가 아예 불가능합니다. 둘째, 많은 경우에 로밍 상태가 로컬 연결보다 선호됩니다. 몇 가지 여러 로밍 네트워크가 복수로 커버할 가능성 때문입니다. 글로벌 UICC, 그리고 전용 IoT 로밍 협정과 글로벌 제휴가 형성되면서 현지 법에서 허용하는 곳에서는 영구 로밍 상황이 늘어나고 있습니다.

네트워크 사업자는 DoS 공격(의도하지 않은 DoS 공격 포함)과 비인가 소스의 요청, "로밍 스티어링" 서비스의 익스플로잇으로부터 HLR 과 VLR 을 어떻게 보호할지 고민해야 합니다.

로밍은 메인 핵심 모바일 네트워크 엔터티 사이에 주고 받는 네트워크 사업자 간 신호 프로토콜을 기반으로 합니다.

그림 1 로밍(방문) 네트워크의 VLR 또는 SGSN 과 홈 네트워크의 HLR 사이 - MAP(Mobile Application Part) 프로토콜 (CDMA 네트워크의 경우, IS41 는 MAP 와 유사).

그림 2 LTE 로밍 네트워크의 MME 와 홈 LTE 네트워크의 HSS 사이 - 다이어미터(S6a 와 같은 일부 변종) 프로토콜.

그림 3 방문 네트워크의 SGSN/S-GW 와 홈 네트워크의 GGSN/P-GW 사이 - GTP 를 이용한 로밍 데이터 전송(GPRS 터널링 프로토콜).

본 절에서는 IoT 서비스와 관련된 로밍 보안 문제에 집중합니다. 일반적인 로밍 보안 문제는 GSMA FASG(Fraud And Security Group)와 그 소그룹에서 다룹니다. 따라서, 로밍 시 이중 등록, 즉

서로 다른 나라에 위치한 두 VLR 에서 받는 상황(고전적인 로밍 사기)은 본 문서의 범위가 아닙니다.

5.6.1 로밍 신호 폭주/공격

IoT 는 모바일 네트워크에서 추가로 보안 요건이 존재합니다.엔드포인트 장치의 속성이 다르고 서비스의 치명도가 높을 가능성이 있기 때문입니다. 모바일 네트워크는 다수의 엔드포인트 장치에 서비스하는 동안 신호 폭주에 노출됩니다. 고의의 악성 DoS 공격은 그런 폭주의 한 가지 이유에 불과합니다. 서비스 중인 모바일 네트워크의 특정 지역에서 일어나는 정전이나 자연재해, 커버리지 문제는 여러 나라에서 흔하며 따라서 그런 문제를 유발할 수 있습니다. 해당 지역에 위치한 로밍 스마트 미터와 그 외 엔드포인트 장치 모두가 동시에 다른 로밍 네트워크에 로밍을 시도할 것입니다. 그와 같은 시나리오에서는 신호 폭주가 일어나며 홈 HLR/HSS 에 큰 위협이 됩니다. 3GPP TS 23.122[9]에서는 그와 같은 시나리오에 대비해 EAB(Extended Access Barring) 서비스를 규정하고 있습니다. 즉 네트워크 사업자가 보편적인 도메인별 액세스 제어 메커니즘 외에 EAN 에 맞춰 구성된 엔드포인트 장치에 대한 네트워크 액세스를 제한하는 것입니다. EAB 구성은 UICC 와 엔드포인트 장치에서 가능합니다. 네트워크 보안 게이트웨이는 의도적인 DoS 공격을 "차단"하도록 구성해야 합니다.

또한 홈 네트워크 사업자가 (IoT 서비스 업체와 함께) 우선순위가 낮은 엔드포인트 장치와 핵심 엔드포인트 장치를 구별할 필요도 있을지 모릅니다. 예컨대, 보건의료 장치는 신호 폭주와 서비스 거부 공격 상황에서 서비스를 유지해야 할 수도 있습니다. 그런가 하면 네트워크가 신호 폭주 상태에서 '낮은 우선순위' 로밍 엔드포인트 장치의 등록을 거부하고 '높은 우선순위' 엔드포인트 장치의 등록을 허용해야 할 수도 있습니다. 구현된 거부 메커니즘은 신호 폭주 후 등록 재시도 시 엔드포인트 장치를 지원하기 위해 블랙 오프 타이머를 동반할 수도 있습니다.

일반적인 권고사항은 네트워크 사업자가 홈 네트워크/로밍 파트너에게 받는 로밍 메시지를 모두 스크리닝하는 것입니다. 비인가/가짜 홈 네트워크/로밍 파트너에게서 오는 메시지를 차단하는 것 외에 엔드포인트 장치 우선순위에 따라 메시지를 필터링할 필요도 있습니다. 신호 폭주/서비스 거부 공격 상황에서는 높은 우선순위/핵심 엔드포인트 장치에서 오는 메시지를 허용하거나 핵심적이지 않은 엔드포인트 장치에서 오는 메시지를 거부할 필요가 있습니다. 거부 방법은 등록 시도나 기타 활동을 일정 기간 미루기 위해 필요합니다.

5.6.2 보안 기반 로밍 스티어링(SoR)

네트워크 사업자가 실행할 수 있는 또 다른 보안 활용 사례로는 보안을 목적으로 한 IoT 엔드포인트 장치의 로밍 스티어링(SoR)이 있습니다. 백오프 타이머가 있는 업데이트 로케이션을 거부하면 엔드포인트 장치는 재시도하며 결국에는 다른 로밍(방문) 네트워크에서 등록을 시도하게 됩니다. SoR 의 다른 방법은 OTA 를 통하는 것으로, UICC 로밍이 선호하는 목록과 그 외 UICC 에 저장된 파라미터를 이용합니다. UICC 의 OTA 업데이트 능력에 힘입어 홈 네트워크는 선호하는 로밍 목록을 업데이트할 수 있으며, 이것이 로밍 네트워크의 선택 과정에서 네트워크의 우선순위를 결정합니다. 홈 네트워크는 또 새 목록으로 엔드포인트 장치 메모리를 새로고침하고 엔드포인트 장치에게 새 네트워크 검색을 즉시 명령할 수 있습니다.

특정 방문 네트워크에서 보안 위험이 탐지될 경우, 홈 네트워크는 SoR 메커니즘을 이용해 아웃바운드 로밍 엔드포인트 장치를 다른 방문 네트워크로 바꿀 수도 있습니다. 그와 같은 엔드포인트 장치의 능동적 전환은 엔드포인트 장치의 다음 등록 시도 직후에 일어날 수도 있고 SIM OTA 서비스를 이용해 즉시 일어날 수도 있습니다. 어떤 방문 네트워크에서 로밍 중인 엔드포인트 장치 중에서 비교적 많은 수가, 또는 다른 입력장치에서 받은 정보가 어떤 문제를 보고하면 그 네트워크와 관련된 보안 문제가 탐지될 수도 있습니다.

5.6.3 데이터 로밍 DoS

DoS 공격은 이동성 신호 공간에 국한되지 않으며 데이터 로밍 역시 신호 폭주의 잠재적 무대입니다. 현재, 로밍 데이터 대부분은 방문 네트워크 SGSN(LTE 의 경우 S-GW)에서 홈 네트워크 GGSN(LTE 의 경우 P-GW)로 라우팅됩니다. 데이터가 방문 네트워크에서 인터넷으로 바로 라우팅되는 LBO(Local Breakout)는 거의 구현되지 않습니다. 이 같은 상황은 미래에 바뀔 수도 있습니다. 예컨대 유럽에서는 2014 년 7 월부터 LBO 서비스와 LTE, 특히 VoLTE(Voice over LTE)를 허용했습니다. 이에 따라 (현재 방문 네트워크에서 하는 일반적인 회로 스위치 음성 통화처럼) 로밍 네트워크에서 하는 음성 통화를 국내 P-GW 가 처리할 수 있습니다.

신호 폭주는 홈 GGSN/P-GW 에 새 데이터 세션 요청이 밀려들면 발생할 수도 있습니다. GPRS 프로토콜은 엔드포인트 장치와 GGSN 사이에 보안 터널을 만드는데, 새 세션 요청(Create-PDP-Context)이 오면 터널이 셋업되고 엔드포인트 장치에 IP 주소가 할당됩니다. IoT 엔드포인트 장치가 개인화된 방식으로 거동하지 않으면 장치들은 앞서 언급한 바와 같이 새 데이터 세션 요청을 대량으로 생성합니다. DoS 공격은 비교적 소수의 엔드포인트 장치로도 가능합니다.

복수의 새 데이터 세션 요청을 동시에 생성하는 것입니다. GGSN/P-GW 서버는 용량이 한정돼 있어 폭주가 발생하면 안 됩니다.

네트워크 사업자는 신호 폭주를 막기 위해 보안 정책에 따라 영향을 받은 장치의 통신 프로토콜을 변경하거나 네트워크 패킷 코어 안에 보안 정책을 적용하여 일부 장치가 네트워크에 연결하지 못하게 할 수도 있습니다.

핵심 엔드포인트 장치는 DoS 공격 중에도 서비스를 받게 하고 우선순위가 낮은 엔드포인트 장치는 서비스를 일정 기간 연기하는 것입니다.

5.7 엔드포인트와 게이트웨이 장치 관리

엔드포인트 장치와 게이트웨이 장치를 위한 로컬 구성 관리 콘솔을 비롯해 하드웨어와 소프트웨어 보안 대책은 본 문서의 범위가 아닙니다. 본 절에서는 네트워크와 관련된 측면만 다룹니다. 엔드포인트와 관련된 보안 지침 개요은 “CLP.11 IoT Security Guidelines Overview”[11]을 참고하기 바랍니다.

5.7.1 엔드포인트 장치 관리

네트워크 사업자는 엔드포인트 장치와 가입을 안전하게 구성하고 관리하는 기본 능력을 IoT 서비스 업체에게 제공하고 '종래의 모바일 장치 관리'에 맞춰 개발된 원칙과 기술을 일부 채택해도 됩니다. UICC 를 이용하여 등록을 하고 셀룰러 네트워크에 연결하는 IoT 엔드포인트 장치는 현재 시중에 나와 있는 연결성 관리 플랫폼과 장치 관리 플랫폼, UICC 관리 플랫폼으로 관리할 수 있습니다.

IoT 서비스 플랫폼에서는 이 기본 엔드포인트 장치 관리 기능 외에 더 복잡한 전용 엔드포인트 장치 관리 기능도 제공할 수 있습니다.

전형적인 엔드포인트 장치 관리 아키텍처의 한 예가 아래에 나와 있습니다. ETSI M2M 통신 원칙[19]에서 발췌한 것입니다.

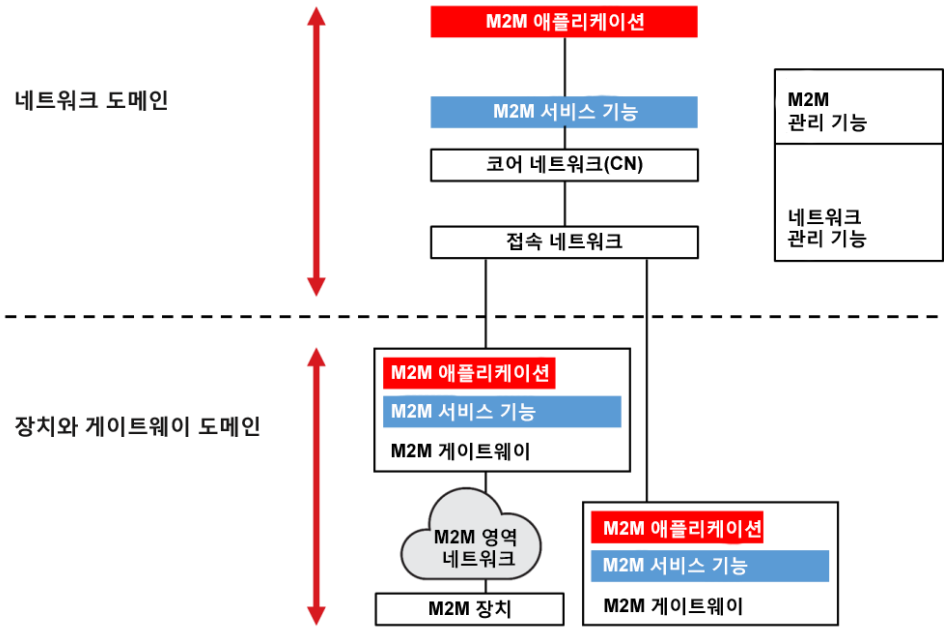

그림 3 - ETSI 의 M2M 장치 관리 고위급 아키텍처

파란색 블록은 전통적으로 네트워크 사업자의 기존 장치 관리 플랫폼에서 관리하고 있는 것을 나타내고 빨간색 블록은 IoT 서비스 플랫폼에서 관리하는 서비스 부문을 나타냅니다.

네트워크 사업자는 IoT 서비스 업체가 요청하면 빨간색으로 표시된 장치 관리 기능 가운데 일부를 수행할 수 있습니다.

5.7.2 게이트웨이 장치의 관리

게이트웨이 장치를 사용하면 IoT 서비스 업체의 장치 관리 복잡도가 한 단계 더 높아질 가능성도 있습니다. 때로는 IoT 게이트웨이 장치가 셀룰러 네트워크와 연결되는 UICC 기반의 장치가 되기도 하고 때로는 유선이 사용되기도 합니다.

게이트웨이는 관리 받는 객체여야 합니다. 모니터링을 하다가 필요할 때 새 펌웨어 또는 소프트웨어로 업데이트해야 하기 때문입니다. 안전한 펌웨어와 소프트웨어 업데이트, 안전한 소프트웨어와 시스템 통합을 제공하는 프로토콜을 사용하여 게이트웨이와 네트워크 백본의 연결에 보안을 확보해야 합니다.

네트워크 사업자는 IoT 서비스 업체를 대신해 안전한 게이트웨이를 제공하고 관리할 수 있습니다. 그러면 엔드포인트 장치를 안전하게 연결하고 네트워크 사업자의 장거리 네트워크 보안 메커니즘과 최적으로 통합할 수 있습니다.

고정 네트워크 연결 기능을 이용해 연결을 하는 게이트웨이는 Broadband Forum TR-069 고객 구내 장비(CPE) 장거리 네트워크(WAN) 관리 프로토콜[20]을 이용해 원격으로 관리할 수 있습니다.

셀룰러 네트워크 연결 기능을 이용해 연결하는 게이트웨이는 OMA 장치 관리(DM) 및 펌웨어 업데이트 관리 객체(FUMO) 프로토콜[5][6]을 이용해 관리할 수 있습니다.

5.7.3 IoT 엔드포인트 장치 블랙리스팅

네트워크 사업자는 IoT 엔드포인트 장치 블랙리스팅과 연결을 GSMA 중앙 장비 ID 레지스터(CEIR) 데이터베이스에 구현해야 합니다. CEIR 은 중앙 데이터베이스로 GSMA 에서 관리하며 분실 및 도난 당한 엔드포인트 장치, 네트워크 접속을 허용하면 안 되는 장치와 관련된 IMEI 를 저장하고 있습니다. 어떤 IMEI 가 CEIR 에 등록되면 그 IMEI 가 들어 있는 엔드포인트 장치는 모든 네트워크 사업자에게 블랙리스트로 인식되고, 네트워크 사업자는 그 데이터를 토대로 장비 ID 레지스터(EIR)의 활용도에 따라 로컬 블랙리스팅을 구현합니다.

네트워크 사업자는 또 로컬 장치 "그레이리스팅"을 구현해 '의심스런' 장치를 일시 중지시키고 동 장치의 성격을 조사한 후 블랙리스팅을 할 수도 있습니다. 보건의료 등 핵심 서비스에서는 IMEI 가 바람직하거나 가능하지 않을 수도 있음을 유념해야 합니다. 네트워크 사업자는 엔드포인트 장치의 진짜 애플리케이션(또는 호스트)을 알아낼 수 있을 때까지 연결된 엔드포인트 장치의 세부사항을 명확하게 파악하는 것이 중요합니다. 통신 모듈 벤더에게 발급된 IMEI 를 이용하는 엔드포인트 장치는 장치 호스트 식별 보고를 지원해야 합니다. 이것은 엔드포인트 장치가 네트워크 사업자에게 호스트 정보를 보고하도록 지원하는 기능입니다. 장치 호스트 식별 보고는 GSMA 의 연결 효율 지침[17]에 기술돼 있습니다.

5.8 그 외 보안 관련 서비스

5.8.1 클라우스 서비스 / 데이터 관리

네트워크 사업자는 호스트되는 클라우드 IoT 서비스 플랫폼을 고객에게 공급하여 IoT 서비스를 구현하게 하고 그 서비스에서 생성되는 데이터를 보관하고 관리하는 서비스도 제공할 수 있습니다.

네트워크 사업자는 IoT 서비스 업체의 요구에 따라 사설 클라우드나 공유 클라우드 인프라를 공급할 수 있습니다.

5.8.2 분석 기반 보안

네트워크 사업자는 데이터 분석과 심도 있는 패킷 검사 서비스를 제공하여 IoT 서비스에서 생성된 데이터에서 위협과 이상을 찾아낼 수 있습니다. 예를 들면 네트워크 사업자가 주기적으로 심도 있는 패킷 검사를 실시하여 사회보장번호와 GPS 좌표 같은 특정 스트링이 제대로 보호되지 않았을 가능성을 확인하고 담당 IoT 서비스 업체에게 해당 정보의 유출 가능성을 경고하는 것입니다.

이것은 IoT 에게 좋은 서비스입니다. 경량 엔드포인트 장치와 서비스는 스스로 이 기능을 제공하지 못하기 때문입니다. 네트워크 사업자는 IoT 서비스 업체에게 보안 상태의 현황과 확인된 위협과 공격, 나아가 전반적인 보안 실태를 알려줄 수 있습니다. 이와 같은 자체 점검 서비스는 "파이프 내부로" 위협이 침투하지 못하게 하는 데 매우 중요합니다. 특히 데이터 서비스가 암호화될 때 그렇습니다. 제공되는 서비스는 다음과 같습니다.

- 이상 탐지 및 머신 러닝을 통한 문제 확인
- 침입 방호 시스템을 실시간 엔드포인트 장치 진단기능 안에 구축
- 이상을 시각화해 쉽게 발견하는 대시보드 제공
- 수상한 연결을 알리고 차단하는 자동 장치 제공
- 클라우드 기반 서비스에 대해 위협 분석 제공

5.8.3 보안 네트워크 관리

네트워크 사업자는 안전하게 관리되고 유지보수되는 네트워크를 제공할 수 있습니다.

- 물리적 또는 논리적 링크 장애의 경우 백업 채널
- 보안 침해 가능성을 보여주는 링크 장애 식별
- 보안과 무결성에 영향을 미치는 로밍 정책 시행
- UICC/SIM 관리
- 보안 정보의 관리
- CERT 가입과 위협 정보 공유에 참여하여 미래의 공격에 대응하고 예방
- DoS 공격 방호
- 주기적인 보안 스캔 / 취약점 평가 실시
- 네트워크 보안과 관련된 법적 요건의 관리와 처리
- 통신 옵션을 특정 IoT 서비스에게 필요한 최소한으로 제한

5.8.4 안전한 IoT 연결능력 관리 플랫폼

네트워크 사업자들은 전용 코어 네트워크와 OSS 인프라의 사용 비중을 늘려 IoT 가입과 요금제를 더 효율적으로 관리하고 또 확대하고 있습니다. 그러한 인프라에 대한 액세스를 사업자의 기업고객(IoT 서비스 업체)이 노출하여 고객 스스로 가입자(개별 또는 집단적으로 서비스 개시, 일시중지 등)를 관리할 수 있게 하기도 합니다.

CLP 12 “IoT Security Guidelines for IoT Service Ecosystem”[26]에 수록된 서비스 플랫폼 가이드라인이 IoT 연결능력 관리 플랫폼을 지원하는 네트워크 사업자에게는 유용한 지침입니다. 이 가이드라인에는 다음과 같은 권고사항이 포함돼 있습니다.

- 네트워크 사업자는 본인이 직접 호스팅하거나 클라우드 호스팅을 통해 제공하는 IoT 연결능력 관리 플랫폼 웹사이트가 NIST[24]나 ECRYPT2[25] 등에서 발간한 최신판 업계 지침에 따라 '동급 최고'의 암호화를 통해 액세스할 수 있게 해야 합니다.
- 네트워크 사업자는 자사 IoT 연결능력 관리 플랫폼의 웹 포털에 접속할 때 비밀번호 생성과 변경, 재설정 시 표준 '모범사례' 절차를 이용하게 해야 합니다.

5.8.5 인증서 관리

네트워크 사업자는 X.509 인증서 관리 서비스를 제공할 수 있습니다.

5.8.6 다중 요소 인증

다중 요소 인증 서비스에서는 일반적으로 사용자가 ID, 비밀번호 외에 전자 토큰을 이용해 자신을 인증해야 합니다. 그러므로 다중 요소 인증은 IoT 서비스 접속 시 보호장치를 강화해 무단 사용자를 차단할 수 있습니다.

GSMA 의 Mobile Connect initiative[12]와 OpenID Connect[21], FIDO[22], ETSI MSS[23]는 모두 IoT 서비스 업체가 최종 사용자에게 추가 인증과 정보를 확보할 수 있는 다중 요소 인증 장치의 예입니다. 여기서 최종 사용자는 IOT 서비스 플랫폼에 정보를 제공하여 여러 수준의 확인이 가능한 인간을 말합니다. 예로는 PIN 번호 입력, 생체 서명 제공 등이 있습니다.

다중 요소 인증 솔루션 대부분은 현재 전통적인 "스마트폰" 서비스의 구현에 쓰이고 있지만 네트워크 연결 작업, 소프트웨어 업데이트, 하드 리셋 등 특정 작업을 위해 인체 인증을 요구하는 IoT 서비스에도 적용 가능합니다.

예컨대 다중 요소 인증을 이용해 커넥티드 자동차 안에 설치된 게이트웨이 장치 외에 추가로 모바일 ID 를 이용할 수도 있습니다. 이 활용 사례에서 다중 요소 인증 인프라는 탑승자가 차 안에서 제공되는 인포테인먼트와 결제 서비스를 이용하기 위한 추가 인가 장치 역할을 할 수도 있습니다.

부록 A 문서 관리

A.1 문서 이력

버전	날짜	변경 내용	승인권자	편집자 / 회사
1.0	2016-02-08	New PRD CLP.14	PSMC	Ian Smith GSMA
1.1	2016-11-17	GSMA IoT 보안 평가 제도에 대한 언급 추가됨. 사소한 편집 교정	PSMC	Ian Smith GSMA
2.0	2017 년 9 월 30 일	LPWA 참고문헌 다수 추가	IoT Security Group	Rob Childs GSMA

A.2 기타 정보

유형	설명
문서 담당자	GSMA IoT Programme
연락처	Rob Childs – GSMA

당 기관은 문서 품질을 중시합니다. 오류 또는 누락 발견 시 의견과 함께 연락 바랍니다.

prd@gsma.com 으로도 연락할 수 있습니다.

의견, 제언, 질문은 언제든지 환영합니다.