방송통신정책연구

10-진흥-라-05

사물통신(Machine-to-Machine)에서의 정보보호를 위한 효율적 인증시스템 연구

(Research on Efficient Authentication System for Machine-to-Machine Communications)

2010.09.30

연 구 기 관 : 한국정보보호학회

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

방송통신정책연구

10-진흥-라-05

사물통신(Machine-to-Machine)에서의 정보보호를 위한 효율적 인증시스템 연구

(Research on Efficient Authentication System for Machine-to-Machine Communications)

2010.09.30

연 구 기 관 : 한국정보보호학회

총괄책임자 : 임종인(고려대학교)

요 약 문

1. 제목

사물통신(Machine-to-Machine)에서의 정보보호를 위한 효율적 인증시스템 연구

2. 연구의 목적 및 중요성

사물통신은 인간의 개입이 없거나 최소화된 환경에서 사물간 자동적인 통신을 의미한다. 사물통신은 현재 스마트그리드, 재난 방지를 위한 각종 환경의 측정 등 국가기반시설 등 공공 SoC 서비스, ITS, VANET 등 차량지능화 서비스, 위험 알림 서비스, 치매 노인 안심 서비스 등 스마트 안심 서비스 등에 사용될 것으로 예상되고 있다.

방송통신위원회는 2009년 '10대 미래 서비스'를 선정하고 이를 통해 GDP 4만 달러의 시대를 열어가겠다고 밝혔다. 사물통신은 4G방송, 터치DMB, 미래 인터넷 서비스 등과 함께 10대 미래 서비스로 선정되었다. 2009년 10월, 사물통신을 '사물지능통신'으로 명명하고 이를 추진하기 위한 '사물통신 기반구축 기본계획'을 발표하였다. 동 계획에서 방송통신위원회는 미래 방송통신융합 초일류 ICT 강국 실현을 비전으로 삼고, 2012년까지 세계 최고의 사물통신 기반구축을 목표로 추진할 것으로 밝히고 있다. 이를 위하여 기반구축, 서비스 활성화, 기술개발, 확산 환경 조성 등 4대 과제별 12대 세부과제를 제시하고 있다. 이 12대 세부과제에는 정보보호 체계 마련 및 도입 확산을 위한 법제도 개선이 포함되어 있다.

사물통신은 인간의 개입이 배재 혹은 최소화된 사물 간의 자동화된 통신이며, 국가 인프라, 지능형 자동차 등 안전이 가장 우선시 되는 분야에 사용이 예상되므

로 사물통신을 추진하기 위하여 정보보호의 고려는 반드시 필요하다. 기기 간 올바른 정보와 명령의 전달을 위하여 적법한 기기로부터의 적법한 메시지임을 확인할 수 있는 인증은 사물통신 정보보호 분야에 있어 가장 중요한 고려사항이다.

2012년 사물통신 기반구축 및 시범서비스 추진을 위하여 사물통신 환경의 인증기술을 연구하고 이에 대하여 규정할 필요성이 있다. 본 연구에서는 안전한 사물통신 환경 구축을 위하여 인증시스템의 분석 및 사물통신 환경에서 사용 가능한 인증기술에 대한 연구, 그리고 안전하고 효율적인 인증기술을 규정하기 위한 정책 방안의 제시를 목표로 한다.

3. 연구의 구성 및 범위

안전한 사물통신 환경 구축을 위하여 인증기술의 요구사항 분석 및 사물통신 환경에서 사용 가능한 인증기술에 대한 연구, 그리고 안전하고 효율적인 인증기술을 규정하기 위한 정책 방안의 제시 목표를 달성하기 위하여 세부과제를 도출하였다. 이 세부과제는 (1) 사물통신 기술 및 동향 연구, (2) 인증기술의 요구사항 도출 및 사물통신 환경에서 사용 가능한 인증기술의 연구, (3) 사물통신 환경에서 인증기술을 규정하기 위한 법·제도적 연구이다.

사물통신은 21세기 초에 정립된 개념으로 현재까지 사물통신의 정의, 표준 등을 규정하고 있는 문서 등이 부족한 시점이다. 현재 사물통신은 각 기관들마다 다르게 정의하고 있으며, 기술적으로는 텔레메트리(Telemetry), 센서네트워크(Ubiquitous Sensor Network, USN), IoT(Internet of Things) 등 여러 개념과 혼용되어 사용되고 있다. 본 연구에서 사물통신은 USN의 센서네트워크, Telemetry 기술 등을 통하여 정보를 수집하며 이를 인간의 개입 없이 혹은 최소화된 개입으로 게이트웨이(Gateway)를 통하여 유용한 정보로 이용할 수 있는 기술이라 정의한다. 또한 현재 방송통신위원회의 사물지능통신 추진전략에서 IoT 역시 사물통신의 한 개념으로 다루고 있으므로, 본 연구에서는 사물통신을 M2M(Machine-to-

Machine) 뿐만 아니라, IoT(Internet of Things)까지 포괄하는 개념으로 정의한다.

따라서 본 연구는 기존의 IoT와 M2M 개념을 포괄하는 인간이 개입하지 않는 사물과 사물간의 통신에서 요구되는 인증을 위한 기술과 정책을 다룬다.

4. 연구내용 및 결과

사물통신 환경의 취약점은 물리적 공격, 자격증명의 타협, 변경을 통한 공격, 프로토콜 공격, 코어네트워크에 대한 공격, 사용자 데이터 및 프라이버시에 대한 공격 등이다. 이러한 사물통신 환경의 보안 취약성은 기술적·정책적 보안 조치를 통해 예방할 수 있으며, 인증 기술은 사물통신 환경에서의 대표적인 보안 조치이다.

사물통신은 공공뿐만 아니라 민간영역에서 다양한 사업자의 제품에서, 다양한 환경과 서비스에서 사용이 예상되므로, 특정 인증기술을 사용하도록 규정하거나 통일시키는 것은 문제를 초래할 수 있다. 사물통신 환경에서 인증기술은 각 사용 환경 별 요구사항을 규정하고, 이와 같은 요구사항을 충족시키는 인증기술을 선택적으로 적용하는 것이 현실적이다. 사물통신 환경에서 인증기술의 일반적인 요구사항은 디바이스 인증, 서버 인증, 통신 내용의 암호화, 부인 방지, 기타 환경과의 호환성, 인증 기술의 효율성, 사용자 개입의 최소화 등이다.

방송통신위원회는 사물통신의 4가지 예상 사용(Use Case)환경을 예측하고 이에 따라 각 환경에 맞는 R&D 전략을 추진하고 있다. 이 4가지 예상 사용 환경은 (1) 개인맞춤형 서비스, (2) 스마트 안심 서비스, (3) 차량 지능화 서비스, (4) 공공 SoC 서비스이다. 예상 사용 환경에 따라 상이한 보안 위협과, 이에 대응하기 위한 인증기술이 갖추어야할 요구사항 역시 다를 것으로 예상된다. 개인 맞춤형 서비스는 유헬스케어의 경우 의료정보이므로 강력한 인증과 암호화가 요구되며, 서로 다른 기기들간 인증을 위한 호환성이 요구된다. 스마트안심서비스는 가용성, 그리고

경량 인증 기술이 요구된다. 차량 지능화 서비스의 경우 공격이 발생하면 바로 인명사고로 이어질 수 있어, 강력한 인증기술이 요구되며 동시에 고속주행 환경에서 지연 없이 인증이 이루어질 수 있는 인증기술이 요구된다. 또한 이동성으로 도로 환경 등으로 인증서버에 과부화가 생길 수 있음에 따라, 인증서버는 적절한 수용력이 요구된다. 공공 SoC 서비스는 국가주요기반시설임에 따라 그 어떤 환경보다 강력한 인증기술이 요구된다. 또한 스마트그리드 환경에서는 물리적 접근이 용이함에 따라, 물리적 보안 위협에도 안전한 인증기술이 요구되며, 과금이 필요한 환경에서는 부인 방지 기능이 요구된다.

사물통신 환경에서는 ID/PW 기반 인증기술, MAC 주소 기반 인증기술, 암호 프로토콜 기반 인증기술, 인증서 기반 인증기술, Identity Based Encryption을 이용한 인증기술 등이 사용이 가능할 것으로 예상된다. ID/PW 기반 인증기술은 ID/PW만 설정되면 범용적으로 어느 환경에서든 사용 가능하다는 장점이 있다. 하지만 사물통신 환경에서 새로운 기기를 추가하거나 수정을 하는 데 있어 사람의 개입이 전제되어야 하는 문제점이 있으며, 부인방지 기능을 제공하지 못한다.

MAC 주소 기반 인증기술은 비교적 간단하고 속도도 빠르다는 장점이 있다. 하지만 최근 MAC 주소 위조가 가능함에 따라 사실상 MAC Address 기반 인증은 상당히 취약하며, MAC 주소 테이블을 관리해야 하여 새로운 기기의 추가나 수정 시 관리상에 문제가 있다.

암호 프로토콜 기반 인증기술은 다양한 기반 암호기술을 선택할 수 있으며, 인증 기술이 표준으로 규정됨에 따라 안전성을 보장받을 수 있다. 하지만 기반 암호기술의 취약점이 발견될 경우 인증 역시 취약해질 수 있으며, 사물통신은 기기의 제약요건으로 인하여 많은 연산량을 요구하는 암호기술을 사용할 수 없다는 문제점이 있다.

인증서 기반 인증기술은 강력한 인증 기능을 제공하여 높은 안전성을 제공하

며, 전자서명은 본인만이 서명이 가능하기 때문에 부인방지 기능을 제공한다. 하지만 사전 키 교환이 필요하며, 인증서의 발급·갱신 등 관리가 필요하며, 폐기리스트(CRL)를 반드시 관리해야 한다는 단점이 있다. 아이디 기반 인증기술은 이메일 주소, 아이디 등 공개된 정보를 이용하여 인증하므로 사전 키 교환이 필요 없으며, 연산량이 적어 적은 연산량이 요구되는 기기에서도 사용이 가능하며, 부인방지 기능을 제공한다는 장점이 있다. 하지만 아직 상대적으로 새로운 개념과 기술로 상용화를 위한 연구가 부족하다는 단점이 있다.

사람의 개입 없이 사물들 간에 수행되는 사물통신에서는 프라이버시 침해나 가짜 사물과 같은 많은 정책적 이슈들이 존재한다. 하지만, 이러한 사물통신에서의 잠재적인 위험들은 사물은 법적 주체나 책임 귀속 주체가 될 수 없으므로 사람에게 사물통신의 모든 결과와 그 책임이 직간접적으로 귀속된다. 이러한 특성 때문에 사물통신의 신뢰성과 안전성을 보장하기 위한 핵심적인 메커니즘으로서의 인증은 사물뿐만이 아니라 사람에 대한 인증(authentication)도 함께 요구된다. 또 한편으로 사물의 안전성과 기능성에 대한 인증도 신뢰성 요건으로 요구된다. 따라서 사물통신에서의 인증은 첫째, 누구 소유인가? 혹은 누구의 통제 하에 있는가? 둘째, 누가 만든 제품인가? 셋째, 안전한 제품인가? 이 세 가지 질문에 대한 대답을 제공해줄 수 있어야 할 것으로 판단된다.

본 보고서는 단일한 인증 기술을 강제화하는 사물통신 인증정책을 제시하기보다는 다양한 사물통신 유형별로 가장 적합한 수준의 사물통신 인증기술을 적용하는 유형별 인증정책을 제시하고 있다. 즉, 사물통신을 사물정보의 민감도, 통신결과의 심각도, 서비스 기능의 중요도, 사람과의 결합도, 디바이스 환경, 조직 환경 등 통신이 발생하는 문맥에 따라 다양하게 유형화한 후, 디바이스 인증, 서버 인증, 통신내용 암호화 여부, 부인방지, 호환성, 인증기술 효율성, 사용자 개입 최소화 등의 요구사항의 수준을 정하여 해당 유형에 가장 적합한 인증시스템을 적용하는 유형별 사물통신 인증방법 수립 체계를 제시하였다.

추가적으로 이러한 사물통신 인증 정책의 효과성을 보장하기 위한 부가적인 정책으로 인증 내역 증거보존 의무화, 사물통신 인증방법 평가위원회 구성 등을 제시하였다. 또한 사물통신 인증과 관련된 국내의 법제들의 검토를 수행한 후 앞서 제시한 유형별 사물통신 인증 정책에 기반하여 사물통신 인증관련 법제가 담아야 할 원칙과 구성요소들을 제시하였다.

5. 정책적 활용내용

본 연구를 통해 달성된 사물통신의 신뢰성을 보장할 수 있는 인증기술에 대한 연구 및 법, 정책적인 환경조성을 위한 연구는 향후 사물통신 인증기술 가이드라인 작성 및 표준화 정책 추진에 있어 직접적인 도움을 제공할 수 있을 것으로 기대되며, 향후 사물통신 보안 및 인증 관련 법제 작성에 직, 간접적인 도움을 제공할 것으로 기대된다.

6. 기대효과

본 연구의 결과는 방송통신위원회의 사물통신 정책의 추진, 사물통신 인증 법안을 포함한 사물통신 관련 법제의 제·개정, 그리고 각 사업자들의 사물통신 추진에 있어 안전하고 신뢰성 있는 사물통신을 구축하는데 있어 유용한 참고자료가 될 수 있을 것으로 기대된다.

SUMMARY

1. Title

Research on Efficient Authentication System for Machine-to-Machine Communications

2. Objective and Importance of Research

Machine-to-Machine Communication(M2M) is a communication between machines without or least intervention of people. M2M is expected to be used in various areas such as public SoC service to prevent disaster and to measure various environment, intelligent vehicle service including ITS and VANET, smart safety service, and so on.

In Korea, Korea Communication Commission(KCC) selected M2M as a '10 Future Service' in 2009, and announced 'Plans to establish the foundation of M2M' on Octoer 2009. In this plan, KCC decalared to establish foundation of M2M until 2012.

As M2M is a s a communication between machines without or least intervention of people, and it is expected to be used in the sector that safety is most important, security is the first element to consider. To verify the message is came from valid device, and to verify authenticity of the message, authentication is the most important factor. In this project, we researched

authentication protocols that can be used in M2M environment, and draw the requirements of the authentication protocol in various M2M use cases. Also this paper suggests law and policy measures to regulate M2M authentication.

3. Contents and Scope of the Research

To achieve the aim of this project, we deducted 3 tasks : (1) Research on the M2M technology and trends, (2) Research on the requirement of authentication protocols in M2M environments, and authentication protocols that can be used in M2M, (3) Research on law and policy measures to regulate authentication in M2M.

4. Research Results

As the characteristics of M2M equipments, M2M equipments require to be small, able to operate unattended by humans. Also, M2M equipments are typically deployed in the field for many years, and after deployment, tend to require remote management of their functionality. These requirements introduces vulnerabilities of M2M : (1) physical attacks, (2) compromise of credentials, (3) configuration attack, (4) protocol attack, (5) attacks on the core network, (6) user data and identity privacy attack. To prevent those vulnerabilities, security measures including authentication are needed.

Requirements of authentication in M2M environments are : (1) device authentication, (2) server authentication, (3) message encryption, (4) non-repudiation, (5) compatibility, (6) efficiency, (7) minimize human intervention. Also there are other requirements by the characteristics of M2M use cases.

In M2M environment, ID/PW based authentication, MAC address based authentication, Cryptographic protocol based authentication, PKI based authentication, Authentication using Identity Based Encryption are anticipated to be used. ID/PW based authentication can be used in various M2M environments, but ID/PW list should be managed by human. MAC address based authentication is fast and easy to deploy, but MAC address can be forged by program and also MAC address list should be managed. In Cryptographic protocol based authentication, cryptographic protocol can be selected by consider the environment that M2M is used. But the safety of authentication depends on the cryptographic protocol that is used, and the possible cryptographic protocol has to be light-weight protocol due to the characteristic of M2M equipments. PKI based authentication offers strong authenticity, and also it provides non-repudiation. But the process of issuing, renewing device certificate should be managed, and the management of CRL list is critical in PKI authentication. Authentication by Identity based Encryption used public information such as ID, email address, so it does not need key distribution process. Also authentication by IBE needs less computing power than other authentication algorithms, so it is suitable for M2M environment, and provides non-repudiation. But the concept of IBE is relatively new, and research of IBE and authentication by IBE are not sufficient than other authentication protocols.

There are many policy issues such as privacy invasion and forged devices in M2M environment, a communication between machines without or least intervention of people. But the liabilities of those potential threats on M2M communications are belong to the people, because machines cannot be the legal subject. As this characteristic of M2M communication, authentications of not

only machines but also people are needed to provide safety and reliability in M2M environment. Meanwhile, authentications of machines' safety and functionality are also needed as requirements of reliabilities. Therefore, authentication of M2M should provides answers for those three questions : (1) Who owns the machine?, (2) Who made the machine? (3) Is the machine safe?.

This research does not suggests the policy of regulate one authentication technique, but suggests the policy of deploy the most adequate authentication technique to each M2M environments. In addition, this research suggest other policies to provide efficiency of M2M authentication policy, such as regulation of preserve authentication history evidences and constitute a evaluation committee of authentication techniques. Also, the research suggests principles and elements of the law that regulates M2M authentication.

5. Policy Suggestions for Practical Use

The results of this study can be used to develop guidelines and standards of efficient M2M communications authentication systems, and these guidelines and standards will guarantee the security and reliability of M2M communications systems.

6. Expectations

The results of this study is expected to be a useful reference for development of M2M communication authentication systems, development of M2M communication promotion policies, enactment of M2M Communication-related legislation including M2M Authentication laws, and formation of secure, safety and trustworthy national M2M communication systems.

목 차

Contents

표 목 차

그 림 목 차

제 1 장 연구의 개요

제 1 절 연구의 배경 및 필요성

정보통신 기술의 발전에 따라 사람과 사람을 연결하던 사람 중심의 통신은 사람과 사물, 사물과 사물을 연결하는 사물통신 환경으로 변화하고 있다. 사물통신의 확산에 따라 모든 기기들은 인터넷 등을 통해 서로 연결될 것으로 예측되며 이에 따라 모든 기기에 IP주소가 할당될 것을 대비하여 IPv6가 추진되고 있는 시점이다. 사물통신은 인간의 개입이 없거나 최소화된 환경에서 사물간 자동적인 통신을 의미한다. 사물통신은 현재 스마트그리드, 재난 방지를 위한 각종 환경의 측정 등 국가기반시설 등 공공 SoC 서비스, ITS, VANET 등 차량지능화 서비스, 위험 알림 서비스, 치매 노인 안심 서비스 등 스마트 안심 서비스 등에 사용될 것으로 예측되고 있다.

방송통신위원회는 2009년 '10대 미래 서비스'를 선정하고 이를 통해 GDP 4만 달러의 시대를 열어가겠다고 밝혔다. 사물통신은 4G방송, 터치DMB, 미래 인터넷 서비스 등과 함께 10대 미래 서비스로 선정되었다. 2009년 10월, 사물통신을 '사물지능통신'으로 명명하고 이를 추진하기 위한 '사물통신 기반구축 기본계획'을 발표하였다.[1] 동 계획에서 방송통신위원회는 미래 방송통신융합 초일류 ICT 강국 실현을 비전으로 삼고, 2012년까지 세계 최고의 사물통신 기반구축을 목표로 추진할 것으로 밝히고 있다. 이를 위하여 기반구축, 서비스 활성화, 기술개발, 확산 환경 조성 등 4대 과제별 12대 세부과제를 제시하고 있다. 이 12대 세부과제에는 정보보호 체계 마련 및 도입 확산을 위한 법제도 개선이 포함되어 있다.

사물통신은 인간의 개입이 배재 혹은 최소화된 사물 간의 자동화된 통신이며, 국가 인프라, 지능형 자동차 등 안전이 가장 우선시 되는 분야에 사용이 예상되므

1) 방송통신위원회, "사물통신 기반구축 기본계획(안) 요약", 2009.10

로 사물통신을 추진하기 위하여 정보보호의 고려는 반드시 필요하다. 기기 간 올바른 정보와 명령의 전달을 위하여 적법한 기기로부터의 적법한 메시지임을 확인할 수 있는 인증은 사물통신 정보보호 분야에 있어 가장 중요한 고려사항이다. 2012년 기반구축 및 시범서비스 추진을 위하여 사물통신의 정보보호를 고려한 효율적인 인증 기술 연구 및 이를 규정하기 위한 법·제도 개선에 관한 연구가 반드시 필요한 시점이다.

제 2 절 연구의 목표

1. 연구의 목적

본 연구는 안전한 사물통신 환경 구축을 위한 인증시스템의 분석 및 사물통신 환경에서 사용 가능한 인증기술에 대한 연구이다. 또한 사물통신 환경에서 안전한 인증을 위한 요구사항과, 이를 규정하기 위한 정책 방안의 제시를 목표로 한다.

2. 연구의 내용

본 연구에서는 사물통신의 기술 및 현황에 대하여 분석하고, 예상 위협 연구를 통하여 인증기술이 갖춰야 할 요구조건을 도출한다. 또한 사물통신은 다양한 분야에서 사용이 예상됨에 따라, 예상 사용 환경을 분석하고 각 환경의 특성에 따른 인증기술의 요구사항을 도출한다.

사물통신 환경에서 사용 가능한 인증기술로는 현재 ID/PW 기반 인증기술, MAC Address 기반 인증기술, 암호프로토콜 기반 인증기술, 인증서 기반 인증기술, ID-Based Encryption을 이용한 인증기술을 예상할 수 있으며, 각 인증기술에 대하여 연구 및 분석을 통해 각 기술들이 사물통신 환경에서 어떠한 장·단점이 있는지 분석한다.

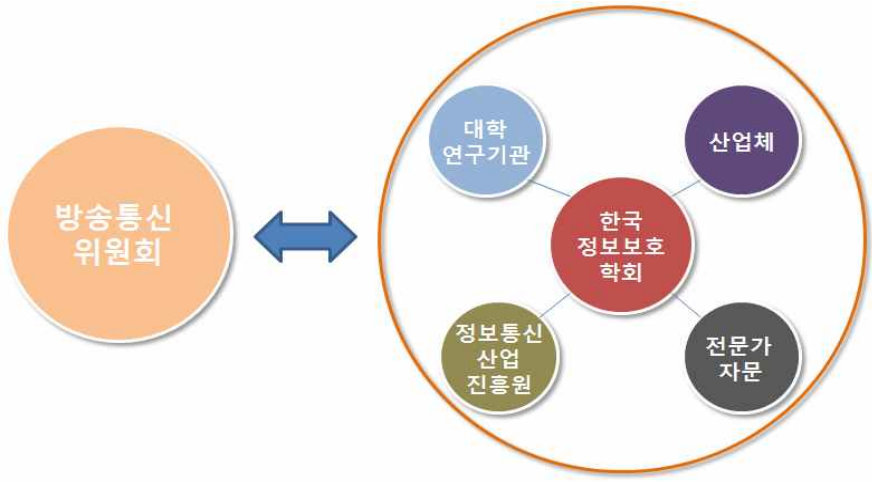
사물통신 환경에서 인증기술을 규정하기 위하여 법·정책적 논의 역시 진행되어야 한다. 개인의 자기정보 통제권 문제 등 사물통신 환경에서 발생 가능한 법정책적 문제들에 대해 식별하고 해당 문제들을 해결 가능한 적절한 인증 정책을 도출한다.

또한, 사물통신과 사물통신 인증의 법적 함의를 살펴보고, 사물통신 및 인증 관련 기존 법제들에 대한 분석을 통해 사물통신 환경에서의 기기 간 인증을 규정 및 규제하기 위한 법률의 제·개정 시 고려사항을 도출하고 가능한 법제 도입 방안을 제시한다.

제 3 절 연구 추진 체계와 방법

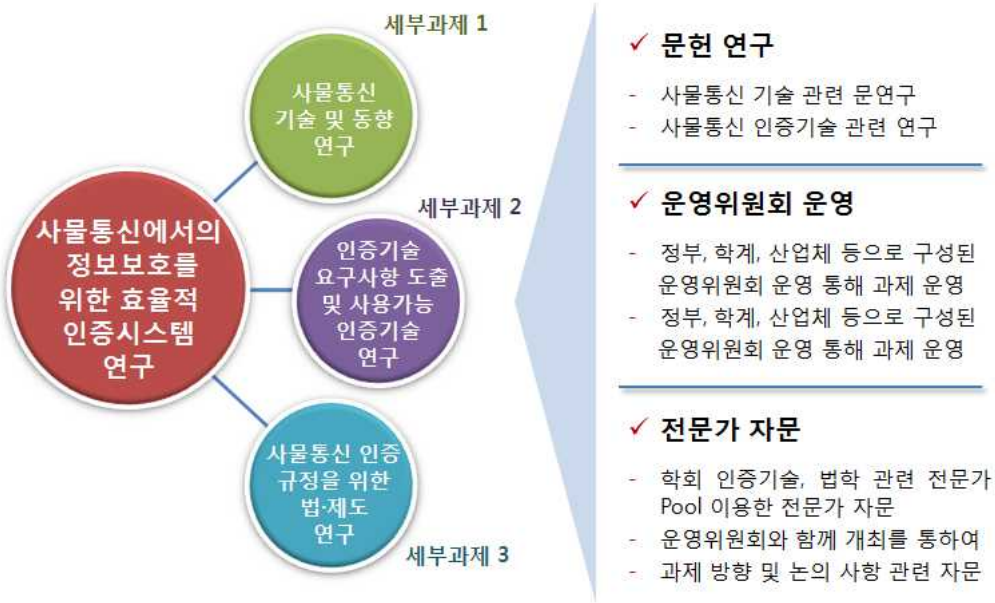
본 연구를 수행하는 한국정보보호학회는 정보보호 분야의 국내 최고의 권위를 가진 학회로서, 공공기관, 산업체 및 학계의 견고한 관계를 형성하고 있다. 한국정보보호학회는 정보보호 관련 이론, 기술, 정책, 법률 등 전반에 있어 연구 경험 및 전문가들을 보유하고 있다.

본 과제는 한국정보보호학회에서 주관하며, 주무부처인 방송통신위원회의 관리와 요구에 따라, 대학 연구기관, 산업체, 한국정보보호학회의 전문가 풀, 그리고 정보통신산업진흥원과 협력하여 과제를 수행한다.



(그림 1) 과제 추진체계

또한, 안전한 사물통신 환경 구축을 위한 인증시스템의 분석 및 사물통신 환경에서 사용 가능한 인증기술에 대한 연구, 그리고 안전하고 효율적인 인증기술을 규정하기 위한 정책 방안의 제시라는 목표를 달성하기 위하여 세부과제를 도출하였다. 이 세부과제는 (1) 사물통신 기술 및 동향 연구, (2) 인증기술의 요구사항 도출 및 사물통신 환경에서 사용 가능한 인증기술의 연구, (3) 사물통신 환경에서 인증기술을 규정하기 위한 법·제도적 연구이다. 이 세부과제들을 문헌 연구, 운영위원회 운영, 그리고 전문가 자문을 통하여 수행하였다.



(그림 2) 세부과제 및 연구 추진체계

제 2 장 사물통신기술

제 1 절 개요

1. 사물통신의 개념 및 특징

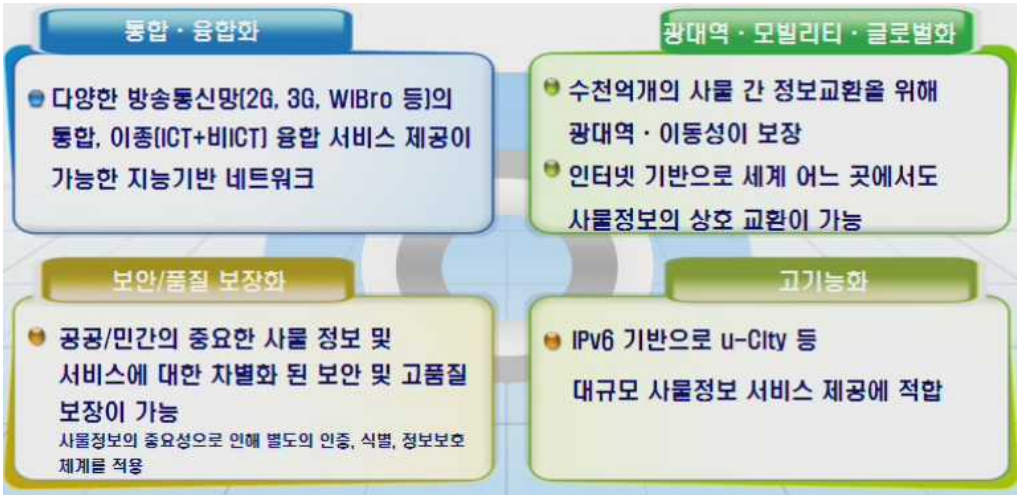
일반적으로 사물통신은 한 기기가 비슷한 다른 기기와 유선 혹은 무선으로 통신하는 기술을 지칭한다.[2] 사물통신은 기기(센서, 미터기)를 상황(온도, 재고 수준 등)을 파악하기 위하여 사용하며, 기기 간 통신을 통해 수집된 정보는 네트워크를 통하여 어플리케이션으로 전송되며 이는 유용한 정보(ex. 재고를 더욱 선적해야 함)로 변경되어 이용된다. 사물통신의 개념이 도입된 초기에는 원격조정 및 텔레메틱 정도의 개념으로 인식되어 파생되는 시장이 한정적이었으나, 최근 통신의 발전과 산업 현장에서의 자동화 등으로 인하여 사물통신의 중요성이 부각되고 있다.[3]

사물통신은 원격지의 센서 등이 데이터를 수집하고 이를 인터넷 등 네트워크를 통하여 원방으로 전송한다. 이로 인하여 사물통신은 텔레메트리(Telemetry)와 비슷한 개념으로 이해되었다. 텔레메트리 기술과 사물통신은 모두 센서 등을 통하여 수집된 정보를 통신한다는 공통점이 있다. 사물통신과 텔레메트리의 가장 근본적인 차이점은 텔레메트리는 무작위적인 라디오 시그널을 이용하여 통신하는 반면, 사물통신은 무선 네트워크 등 기존의 통신 네트워크를 이용한다는 것이다.[4] 텔레메트리 시스템은 많은 분야에서 현재까지 사용되고 있으나 전용의 주파수 통신을 하고 이를 위하여 많은 전력 및 시간 소요 등의 문제가 있다. 반면 최신의 사물통신의 경우 원격의 센서 기술은 정교하고 정확하며, 통신은 기존 무선통신 기술을 이용하여 확장에 용이하며, 전력 및 소요 시간 측면에서 훨씬 효율적이다.

---

2) Wikipedia, "Machine-to-Machine"
3) 김유창, “기기 간 통신(M2M)의 기술 동향과 전망”, 전자부품, 2009년 7월호 p.66
4) HowStuffWorks, "How Machine-to-Machine Communication Works"

사물통신의 특징으로는 통합·융합화, 광대역·모빌리티·글로벌화, 보안/품질 보장화, 고기능화라는 특징을 들 수 있다.[5] 사물통신은 CDMA, WCDMA, WiBro, ZigBee 등 다양한 통신망이 통합·융합화 되어 서비스가 제공된다는 특징이 있다. 이러한 통신네트워크는 수많은 기기들을 연결하는 광대역의 특징과 이동하는 기기들을 지원하는 모빌리티, 그리고 전세계의 기기들이 연결되는 글로벌화라는 특징을 갖는다. 또한 사물통신의 실시간 측정 및 정보수집으로 인하여 보안/품질을 보장할 수 있으며, 이러한 특징 및 기능들로 인하여 각종 영역에서 대규모로 적용이 가능하다.



(그림 3) 사물통신의 특징

출처: 김기형, "사물지능통신의 개념과 차이점", RFID/USN Online Forum 발표자료

이와 같은 사물통신의 특징에 따라 사물통신은 개인 의료 모니터링, 공급사슬의 추적 및 모니터링, 스마트그리드에서의 스마트미터기의 통신, 산업 자동화 환경에서의 통신 등에 사용이 예상되고 있다. 사물통신은 일대일의 단수 연결 구조에서 네트워크를 통하여 수많은 기기들이 연결되는 사물통신 시스템으로 변화하고 있다. 무선 네트워크의 진화는 정보가 통신되기 위하여 필요한 전력 및 시간을 단

5) 김기형, "사물지능통신의 개념과 차이점", RFID/USN Online Forum 발표자료

축함에 따라 사물통신 환경의 구축은 더욱 용이해지고 있다. 사물통신 기술의 발전과 사용의 증가로 인하여 2010년까지 20억 대의 기기들이 사물통신을 통하여 연결될 것으로 예측되며, 2020년 1000억대가 넘는 기기들이 연결될 것으로 예측하고 있다.[6)]

2. 사물통신기술의 정의 및 구성

가. 사물통신의 정의

사물통신(Machine-to-Machine Communication)은 21세기 초에 정립된 개념으로 현재까지 사물통신의 정의, 표준 등을 규정하고 있는 문서 등이 부족한 시점이다. 현재 사물통신은 각 기관들마다 다르게 정의하고 있으며, 기술적으로는 텔레메트리(Telemetry), 센서네트워크(Ubiquitous Sensor Network, USN), IoT(Internet of Things) 등 여러 개념과 혼용되어 사용되고 있다. 사물통신의 연구를 위하여 혼재되어 사용되고 있는 사물통신의 정의를 본 연구에서는 어떻게 정의할지 우선 규정해야 할 필요성이 있다.

사물통신을 선도적으로 연구하고 있는 ETSI(European Telecommunications Standards Institute)는 “사람이 개입하지 않는(혹은 최소 개입) 상태에서 Machine/Device간에 일어나는 통신”으로 정의하고 있다. ETSI는 사물통신 분과위원회인 M2M TC(Technical Committee)를 통하여 M2M의 세부적인 정의를 위한 표준문서 “DTR/M2M-00004” 작업을 2009년 5월 시작하였으며, 2011년 3월 동 문서를 공개할 예정이다.

방송통신위원회는 2009년 사물통신 기반구축 기본계획을 발표하면서 사물통신을 사물지능통신으로 명명하고, “통신·방송·인터넷 인프라를 인간 대 사물, 사물 대 사물 간 영역으로 확대, 연계하여 사물을 통해 지능적으로 정보를 수집, 가공,

6) 중앙선데이, “21세기 네트워크 혁명, 1000억 대 단말기를 연결하라”, 2009년 4월 18일자 기사

처리하여 새롭고 효율적인 서비스를 제공하는 기술”로 사물통신의 개념을 밝히고 있다. 동 계획에서 사물통신을 협의적으로는 “기계간의 통신 및 사람이 동작하는 디바이스와 기계간의 통신”으로, 광의적으로는 “통신과 ICT 기술을 결합하여 원격지의 사물정보를 확인할 수 있는 제반 솔루션”으로 정의하고 있다.

(그림 4) 사물통신 개념도

출처: 방송통신위원회, “사물통신 기반구축 기본계획” (2009)“

사물지능통신포럼은 방송통신위원회의 사물통신의 정의인 “정보의 수집·활용이 인간 對 사물(Object), 사물 對 사물로 방송통신의 대상이 확장되는 지능형 융합서비스”를 따르고 있으며, 좀 더 확장하여 IoT(Internet of Things) 역시 사물통신의 다른 한 축으로 생각하고 사물지능통신을 M2M/IoT 로 표기하고 있다.

기술적으로 사물통신은 USN, IoT, 텔레메트리(Telemetry) 등의 개념들과 혼재되어 사용되고 있다. 각 기술적 용어는 다음과 같이 정의할 수 있다.

USN(Ubiquitous Sensor Network)은 지능형 센서(Intelligent Sensor)들의 네트워크를 표현하는 용어이다.[7] 지능형 센서는 특정 입력(조도, 열, 소리, 움직임 등)이 있을 경우 이를 감지하여 미리 정해진 활동을 수행하는 센서를 의미한다. 기존 사물에 RFID 태그를 부착하여 정보를 인식, 관리하는 센서네트워크에서, ZigBee 등 WPAN(Wireless Personal Are Network), ad-hoc Network 등 무선 네트워크 기술의 발전에 따라 언제 어디서든 무선으로 통신이 가능한 유비쿼터스 네트워크로 발전함에 따라 USN 환경으로 진화하고 있다. USN의 특징은 소규모의 센서노드, 배터리 문제를 해결하기 위한 저전력 기술, 악조건 속에서도 끊김 없이 통신할 수 있는 강인함, 대규모 환경의 적용 가능성 등이 있다. USN은 센서네트워크, USN 접속 네트워크, 네트워크 기반시설, USN 미들웨어, USN 적용 플랫폼 등으로 구성된다.

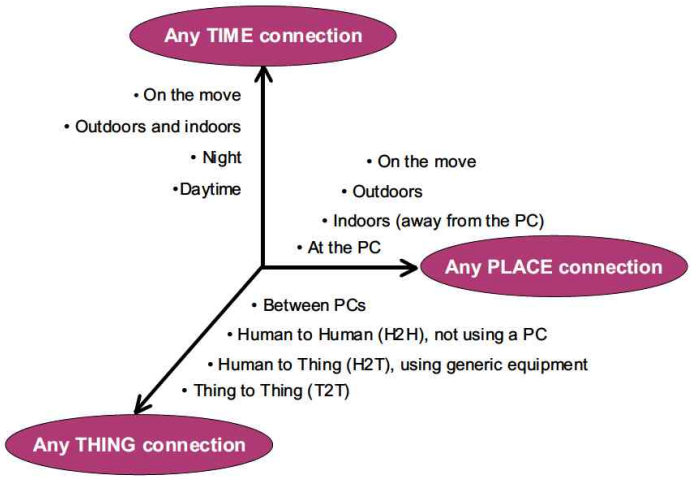
7) ITU-T, "Ubiquitous Sensor Network", Technology Watch Briefing Report (2009)

(그림 5) Ubiquitous Sensor Network의 계층별 도식도

출처: ITU-T, "Ubiquitous Sensor Network", Technology Watch Briefing Report (2009)

IoT(Internet of Things)는 2005년 11월 ITU-T World Summit on the Information Society에서 Special Report로 제안된 기술 개념이다. ITU-T는 IoT를 "정보통신기술(ICT)의 차세대 기술로, 언제 어디서든 누구에게나 연결되던 정보통신기술이 무엇에든(Anything) 연결됨으로 확장되는 기술"로 정의하였다.[8] IoT는 협의적으로는 인터넷을 통하여 사물이 연결되는 개념으로 USN(Ubiquitous Sensor Network)과 유사하게 정의할 수 있으며 광의적으로 IoT는 미래인터넷(Future Internet, FI) 분야와 유사하다고 정의할 수 있다.[9]

8) ITU-T, "The Internet of Things", 2005
url : http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf
9) 김기형, 전게발표자료

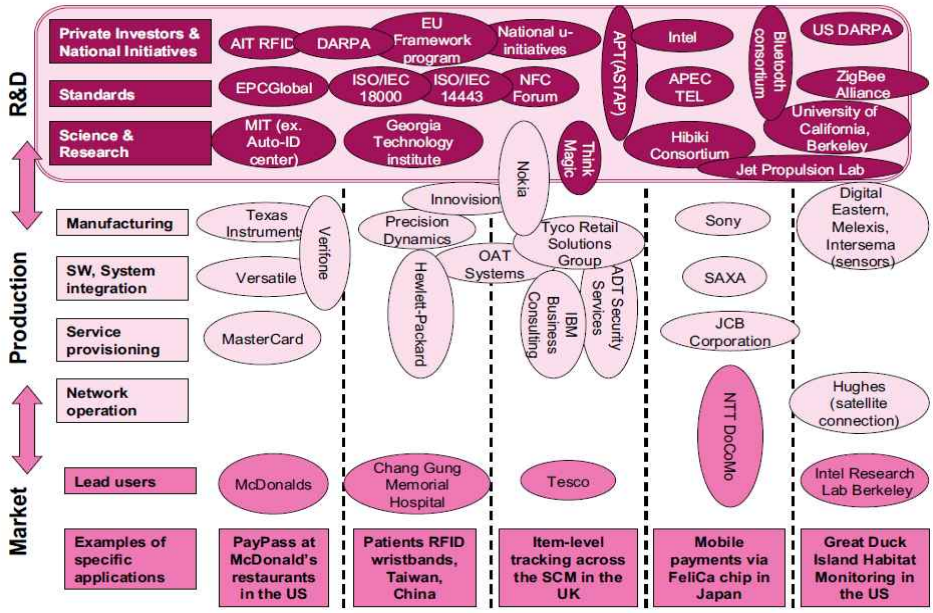


(그림 6) IoT의 개념 및 특징

출처: ITU-T, " The Internet of Things" (2005)

이와 같은 개념과 특징으로 인하여 IoT는 사물통신과 유사하다고 볼 수 있으나, 사물통신은 통신의 측면이 강하며, IoT는 식별체계에서 End Device까지 포괄하는 좀 더 광의적이고 파괴적인 개념이라는 차이점이 존재한다.[10] 이는 사물통신은 산업 환경 및 Device의 Machine-to-Machine인 측면이 강한 반면, IoT는 모든 기기를 연결하는 Thing-to-Thing인 측면이 강하다는 것이다. 이와 같은 IoT의 특징에 따라 IoT는 결제시스템, 물류시스템, 스마트홈 등 사물통신을 포함한 여러 분야에서 사용이 될 것으로 예측된다.

10) 김기형, 전게발표자료



(그림 7) IoT의 예상 사용 환경 및 관련 업체

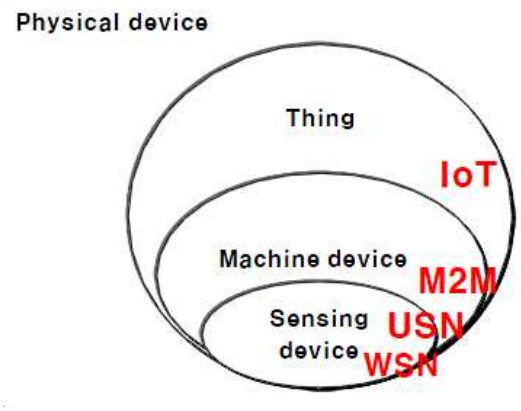
출처: ITU-T, " The Internet of Things" (2005)

텔레메트리(Telemetry)는 원격지의 정보를 측정하고 보고하는 기술이다.[11] 텔레메트리는 1845년 러시아에서 유선 텔레메트리 기술이 처음 사용되었으며, 무선 텔레메트리 역시 1930년 러시아에서 개발되었다. 현재 모터 레이싱, 농업, 수자원 관리, 국방, 에너지 모니터링, 의료 등의 분야에서 사용되고 있다. 텔레메트리 관련 표준은 CCSDS 및 IRIG의 기기 및 통신, 소프트웨어 등의 표준이 존재한다.

사물통신 기술은 이와 같이 USN, IoT, Telemetry 등 다양한 기술과 연관이 있는 기술이다. 사물통신은 USN의 센서네트워크, Telemetry 기술 등을 통하여 정보를 수집하며 이를 인간의 개입 없이 혹은 최소화된 개입으로 게이트웨이(Gateway)를 통하여 유용한 정보로 이용할 수 있는 기술이라 정의할 수 있다. IoT는 사물통신과 미래인터넷의 중간적인 개념으로 사물통신과 유사한 개념이지만 사물통신보다 확장된 개념으로 이해할 수 있다. 방송통신위원회의 사물통신 기

11) Wikipedia, "Telemetry"

반구축 기본계획에서는 IoT 역시 사물통신의 일부로 다루고 있으므로, 본 연구에서는 사물통신을 M2M(Machine-to-Machine)뿐만 아니라, IoT(Internet of Thing)까지 포괄하는 개념으로 정의한다.



(그림 8) 사물통신 관련 기술의 포괄

출처: 주성순, "M2M/IoT 기술 및 표준화". 2010 사물지능통신컨퍼런스 발표자료(2010)

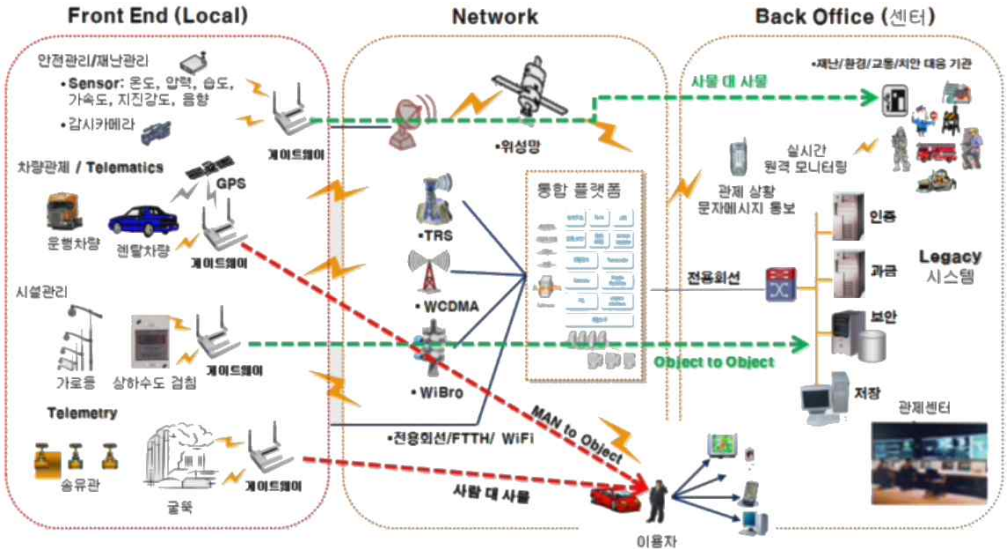
나. 사물통신의 구성요소

1) 사물통신 아키텍처[12)]

사물통신은 크게 Front End와 Network, 그리고 Back Office로 구성된다. Front End는 다양한 기능을 하는 센서들이 M2M Area Network, PAN(Personal Area Netwrok) 등 통신 기술을 이용하여 게이트웨이를 통해 Access 망에 전송되거나 직접 단말로써 사용되거나 다양한 형태로 백본네트워크인 Access Network에 접속되는 형태이다. 이 Froent End에서 수집된 정보들은 Network 기술을 통하여 Back Office의 통합플랫폼으로 전송되며, 이 Network는 현재 이동통신 기술이 사용되고 있다. 통합플랫폼은 통신사업자들이 각자 개별적으로 구축하며, 통합플랫폼을 통하여 모든 정보가 수집되어 처리된다. Back Office는 사용자 측면에 따라

12) 김기형, 전게발표자료

각 응용환경(Application)에서 사용이 된다.



(그림 9) 사물지능통신의 기술적 구성

출처: 김기형, "사물지능통신의 개념과 차이점", RFID/USN Online Forum 발표자료

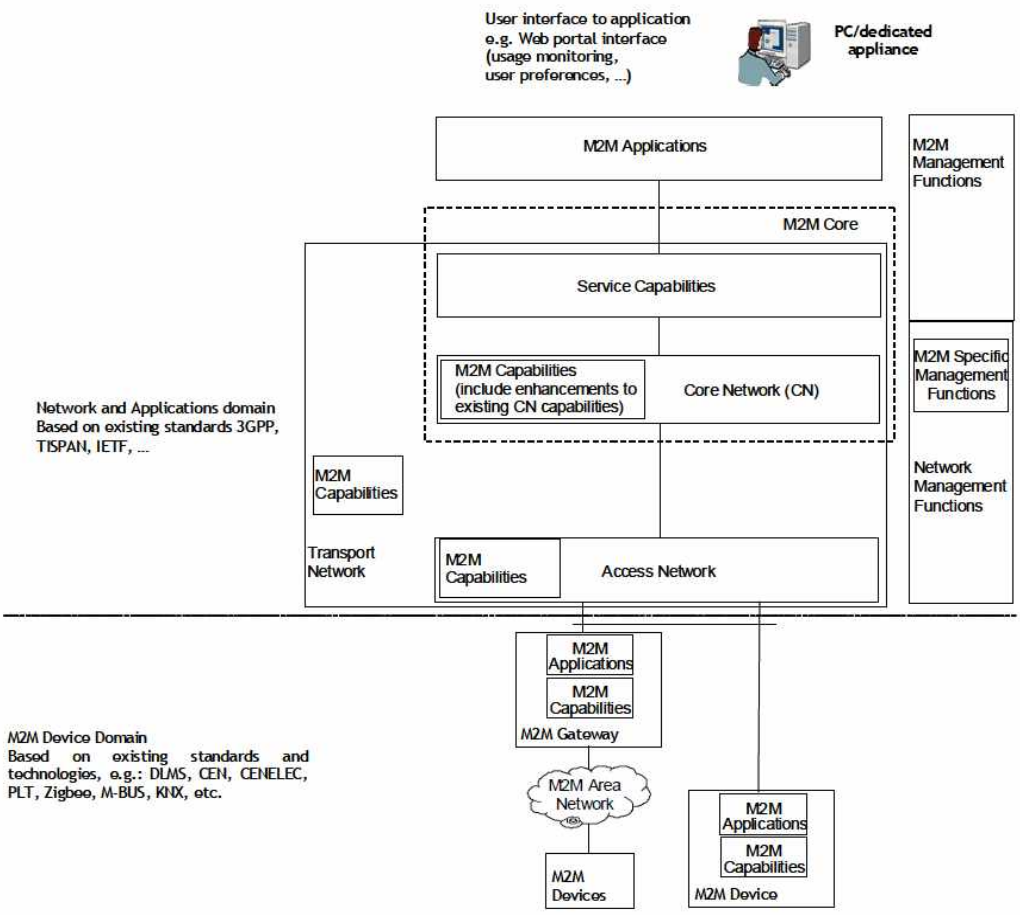
2) 사물통신 환경에서 통신 아키텍처[13]

사물통신 기술은 개념 및 정의에서 살펴본 바와 같이 대략적으로 기기들과 이 기기들간의 통신을 가능하게 하고 정보를 수집하는 게이트웨이, 그리고 이를 관리 및 사용하는 부분으로 구성된다. ETSI는 TS 102 690 "Machine-to-Machine communications(M2M) Functional Architecture"를 통해 사물통신 구조를 연구하고 있으며, 본 결과를 2010년 12월 공개할 예정이다. 동 보고서의 초안(Draft)는 현재 제한적으로 공개되어있으며, ETSI는 동보고서에서 사물통신의 아키텍처를 M2M 디바이스, M2M 디바이스 도메인, M2M 게이트웨이 도메인, 그리고 M2M 네트워크 도메인으로 분류하고 있다.[14]

---

13) 은선기 외, "안전한 M2M 통신 구축을 위한 상호인증 및 키 교환 프로토콜", 한국정보보호학회논문지, 제20권 제1호, pp.74-76, (2010)

14) "ETSI TS 102 690 v 0.06 Machine-to-Machine communications(M2M) Functional Architecture." (2009), 은선기 외, 상게논문 재인용



(그림 10) M2M 통신의 기능적 구조

출처: TTA, "[M2M] 기기간 통신(Machine to Machine Communication) 표준화 동향-유럽을 중심으로",

(가) M2M 디바이스 도메인

M2M 디바이스 도메인은 M2M 디바이스와 M2M의 집합체인 M2M 지역(Area) 네트워크로 구성된다. M2M 디바이스는 사물통신을 가능하게 할 수 있는 M2M Capability와 통신 기능을 통하여, M2M Application을 구동시키는 기기를 의미한다. M2M 지역 네트워크는 M2M 디바이스와 M2M 게이트웨이 사이의 연

결을 제공하는 네트워크로, IEEE 802.15, ZigBee, 블루투스 등의 PAN(Personal Area Network) 또는 PLC, M-BUS, Wireless M-BUS, KNX 등의 LAN(Local Area Network) 등의 기술이 사용될 수 있다.

(나) M2M 게이트웨이

M2M 게이트웨이는 M2M Application과 M2M Capabilities로 구성된다. M2M 게이트웨이는 M2M Application과 M2M Capabilities를 이용하여, M2M 디바이스들의 상호 작용을 보호하고, M2M 디바이스가 네트워크 도메인의 접속 네트워크에 접근하도록 게이트웨이 역할을 제공한다.

(다) M2M 네트워크 도메인

M2M 네트워크 도메인은 접속 네트워크(Access Network), M2M 코어(Core), 전송 네트워크(Transport Network), M2M 응용분야(Applications) M2M 관리 기능(Management Function), 네트워크 관리 기능(Network Management Function) 등으로 구성된다. 접속 네트워크는 M2M 디바이스 도메인과 M2M 코어네트워크 간 통신을 할 수 있도록 접속 네트워크를 지원한다. M2M 코어는 코어 네트워크(Core Network)와 서비스 제공기능(Service Capabilities)으로 구성되어, 사물통신의 통신에 있어 핵심적인 역할을 담당한다. M2M 응용분야는 M2M통신을 이용하여 수집된 정보를 가공하여 제공하는 인터페이스 등을 의미한다. M2M 관리 기능과 네트워크 관리 기능은 M2M 통신 구조 전반과, 네트워크 통신 기술등을 관리한다.

3. 사물통신 기술의 적용분야

사물통신의 디바이스의 연결에 따른 도입 효과 및 무선 통신 기술의 발전에 따른 도입의 용이성에 따라 사물통신은 개인 의료 모니터링, 공급사슬의 추적 및

모니터링, 스마트그리드에서의 스마트미터기의 통신, 산업 자동화 환경에서의 통신 등에 사용이 예상되고 있다. 이와 같은 다양한 분야에서 많은 사용으로 인하여 2020년 1000억대가 넘는 기기들이 연결될 것으로 예측하고 있는 시점이다.

방송통신위원회는 사물지능통신 R&D 추진 비전을 “사람과 세상을 이어주는 통신 서비스 시현 - 개인에게는 안심을, 생활에는 편익을, 사회에는 안전을”로 정하고 현재 사물지능통신의 4가지 예상 사용(Use Case)환경을 예측하고 이에 따라 각 환경에 맞는 R&D 전략을 추진하고 있다. 이 4가지 예상 사용 환경은 (1) 개인 맞춤형 서비스, (2) 스마트 안심 서비스, (3) 차량 지능화 서비스, (4) 공공 SoC 서비스 등 4가지 분야에 따라 추진하고 있으며, 2013년 개발용 테스트베드 구축 및 수도권 시범서비스 시작, 2014년 원천기술 확보, 2015년 전국 규모 시범서비스 확대 및 글로벌 시장 30% 선점을 목표로 하고 있다.[15)]

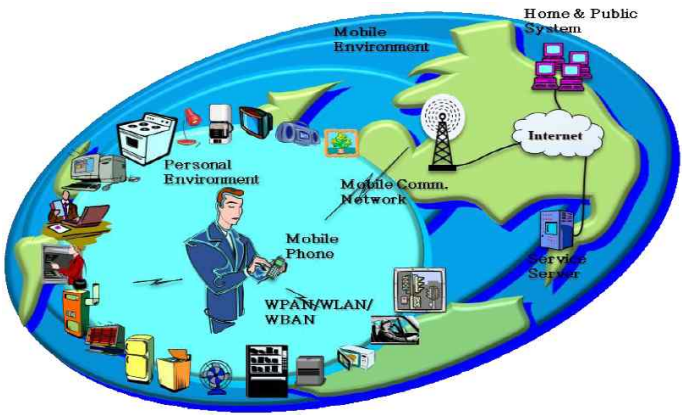
(그림 11) 방송통신위원회의 사물지능통신 예상 사용 환경

출처: 김동기, "사물지능통신 서비스 추진 전략“, 사물지능통신 컨퍼런스 발표자료, 2010

15) 김동기, "사물지능통신 서비스 추진 전략“, 사물지능통신 컨퍼런스 발표자료, 2010

가. 개인 맞춤형 서비스

개인 맞춤형 서비스는 개인의 주변 사물을 자동 제어하고 맞춤형 정보나 광고를 제공하는 서비스를 의미한다. 정보통신기술의 발전 및 스마트폰 등 개인 디바이스의 보급 및 확산에 따라 주변 사물 및 기기를 제어하고 이를 통한 서비스가 가능해지고 있다. 각 디바이스 간 통신을 위하여 Bluetooth 등 PAN(Personal Area Network) 기술의 사용이 확대되고 있는 시점이다. 사물통신은 이러한 PAN 기술 등을 이용하여 각종 디바이스의 정보를 수집하고 제어할 수 있는 서비스의 기반기술 역할을 할 것으로 기대하고 있다.



(그림 12) 개인맞춤형 서비스 도식도

출처: 김동기, "사물지능통신 서비스 추진 전략", 사물지능통신 컨퍼런스 발표자료, 2010

개인맞춤형서비스로는 유비쿼터스 도시 및 스마트홈(Smart Home) 환경에서의 가전기기 및 생활기기의 원격 관리, 각종 센서 등을 이용하여 개인의 생체정보를 수집하고 이를 통해 원격 진료 및 처방을 할 수 있는 유헬스케어(Ubiquitous Health Care) 등이 대표적인 서비스로 예상되고 있다. 또한 최근 많은 관심을 받고 있는 디지털 사이니지[16]를 통한 맞춤형 광고 및 정보 제공, Amazon의 Kindle, Apple의 iPad 등 각종 테블릿 등 모바일 기기 간의 콘텐츠 제공 등 개인 맞춤형 정보 제공 서비스 등에 사용이 예상된다.

16) Digital Signage, 정보, 광고 혹은 기타 메시지들을 표시하는 전자적 디스플레이. 최근 양방향 통신에 따른 맞춤형 서비스를 제공하도록 발전하고 있음

나. 스마트 안심 서비스

스마트안심 서비스는 증가하는 위험과 사고로부터 사물통신 기술 기반 서비스를 통하여 개인이 보호받을 수 있는 서비스이다. 최근 아동대상 성범죄 등 사회 전반적으로 사고가 증가함에 따라 안전과 관련된 서비스의 필요성이 부각되고 있다.

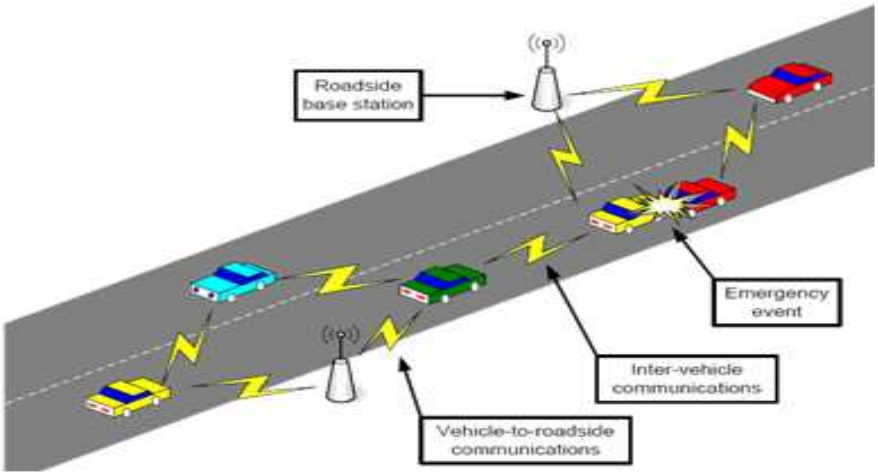
이러한 위협의 증가에 따라 사물통신 기술을 이용하여 실시간으로 센서를 통하여 정보를 수집하고 미리 설정된 이상 징후가 감지될 경우 이를 통지하거나 이에 대응하는 스마트안심서비스의 도입이 예상되고 있다. 귀가 경로를 추적하는 사이버 에스코트 서비스 및 위험 상황 발생 시, 이를 통보 및 신고해주는 위험상황 알림 서비스, 그리고 치매 및 독거노인들의 안전을 위한 노인 안심 서비스 등의 서비스가 사물통신을 이용하여 가능할 것으로 예상된다.

(그림 13) 스마트안심 서비스 도식도

출처: 김동기, "사물지능통신 서비스 추진 전략", 사물지능통신 컨퍼런스 발표자료, 2010

다. 차량 지능화 서비스

차량 지능화 서비스는 자동차에 기계, 전자, 통신, 제어, 인공지능, 감성공학, IT 기술 등을 비롯하여 각종 첨단기술을 접목시킨 지능형자동차와, 자동차의 주행 환경과 도로 인프라와 관련된 지능화 기술인 ITS(Intelligent Transport System)을 포괄하는 기술을 의미한다. 지능형자동차 기술은 예방안전, 사고회피, 충돌안전, 자율주행, 재해확대방지, 차량 정보화 기술 등으로 구성된다.[17]



(그림 14) ITS 도식도

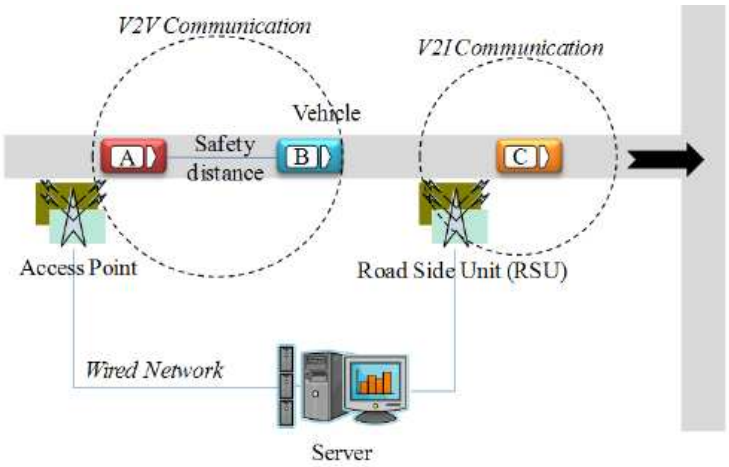
지능형 차량정보 시스템 기술은 차량과 관련된 정보화는 차량과 외부와의 정보통신을 가능케 하는 기술, 차량 내부의 제어신호와 데이터 교환을 위한 차량내부 네트워크 기술과 이 두 가지 접점에 존재하는 운전자 정보시스템 기술로 나눌 수 있다. 또한, 차량정보화기술 분야는 ITS기술과도 밀접한 관련이 있는 분야로써 텔레매틱스, 내비게이션 기술과 같은 차량 외부 통신기술뿐 아니라 전자시스템의 증가에 따른 차량배선의 감소와 기능의 증대를 위해 CAN/FlexRay와 같은 차량제어용 네트워크와 MOST와 같은 멀티미디어 네트워크 등 차량내부 네트워크 기술

17) 원윤재, “지능형 자동차 시스템 및 동향 분석”, 정보처리학회지, 2008

도 중요해지고 있다. 지능형 차량정보시스템은 차량의 기계·구조적 시스템에 전기·전자, 정보통신, 인터넷 및 소프트웨어기술 등을 결합하는 고부가가치 첨단차량 응용기술이라 할 수 있다.

지능형자동차의 핵심은 ECU를 통한 자동화된 차량 제어 및 ECU 간 통신 및 차량간, 혹은 차량 및 정보시스템과 통신을 위한 네트워크 기술이다. 차량 네트워크 기술에는 CAN(Controller Area Network), VANET(Vehicular Ad-hoc Network)가 있다. CAN은 차량 내에서의 정보전달을 위해 개발되었으며 ECU(Electronic Control Unit, 전자제어장치-제어용 컴퓨터) 사이의 통신을 이용하여 최적의 주행 상태를 유지하기 위한 차량 네트워크 시스템이다. VANET으로 알려진 차량 통신 네트워크는 차량과 무선통신망이 결합된 대표적인 자동-IT 융합기술로 차량 안전 및 진단, 텔레매틱스, ITS(Intelligent Transportation System, 지능형 교통시스템)등의 서비스 시장을 형성하며 ITS를 고도화 하는 수단이 된다.

이와 같이 지능형자동차 환경에서는 CAN을 통한 차량내 ECU간 통신, VANET에서의 차량 통신과 RSU(Road Side Unit)와의 통신에서는 통신 노드(Node)들 간의 사물통신이 핵심적인 요소이다.



(그림 15) 차량 통신 환경

출처: 최병철, 차량 통신 보안 및 프라이버시 주요 이슈

우리나라는 2003년 미래형 자동차 분야를 '차세대 성장 동력산업'으로 선정하여 국가연구개발사업인 '미래형자동차사업'을 출범시켜 국내 자동차업계는 물론 대학 및 연구소 등과 연계하여 '연료전지자동차', '하이브리드자동차', '지능형자동차' 등 3개 분야의 관련 핵심기술 개발에 박차를 가하고 있다. 지능형자동차 분야의 목표는 2012년까지 관련 핵심 부품 및 시스템 기술들을 확보하여 조기 상용화를 통한 매출증대로 국가 성장 동력의 기반을 구축하고, 지능형자동차 기술을 통해 교통사고율을 50%이상 저감하는 것을 목표로 하고 있다. 또한, 성장 동력 산업의 연구개발에 대한 체계적이고 효율적인 지원을 위해 2005년 산업자원부와 미래형자동차사업단 주관으로 미래형자동차 분야의 산업기술 로드맵을 작성하였다. 한국전자통신연구원(ETRI)에서는 VMC(Vehicle Multihop Communication) 기술 개발로 VANET의 연구가 진행되고 있다.[18] VMC 기술 개발에서는 주로 차량 안전 관련 메시지의 송수진에 대한 연구가 진행되고 있으며 V2V(Vehicle-to-Vehicle) 무선 링크 시뮬레이터 연구와 VMC 기반 기술 연구가 진행되고 있다.

사물통신은 지능형자동차의 핵심기술 요소로 지능형자동차의 개발 및 구현을 위하여 사물통신 기술이 필수적이다. 이를 위하여 방송통신위원회는 차량 원격 감시 및 관리 기술, 차량간 네트워크 기술 및 트래픽 제어 분석·제어 기술, 지능형 상황 인지 기술, 네트워크화된 스마트 네비게이션 기술, 운전 자동화를 위한 head-up 디스플레이 및 증강현실 기술, 차량 지능화 서비스를 위한 M2M 기반 무선 네트워크 기술을 핵심 요소기술로 선정하고 사물통신 R&D 전략을 추진중이다.[19]

라. 공공 SoC 서비스

공공 SoC 서비스는 사물통신 기술이 현재 사용되고 있으며 향후 사물통신이

---

18) 조선일보, 급발진 주범 논란 EUC(전자제어장치) 해부, 2010년 3월 29일자 기고
url : http://weekly1.chosun.com/site/data/html_dir/2010/03/24/2010032401264.html
19) 김동기, "사물지능통신 서비스 추진 전략", 사물지능통신 컨퍼런스 발표자료, 2010

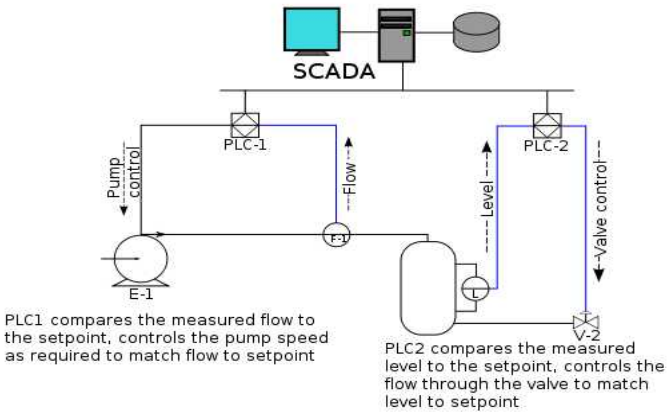
주요 요소기술로서 사용이 예상되며, 국가적으로 중요한 분야이므로 사물통신에 있어서 가장 주목해야할 분야이다. SoC(Social Overhead Capital)는 사회간접자본으로 도로, 항만, 철도 등 생산 활동에 직접적으로 사용되지는 않지만 경제활동을 원활하게 하기 위해서 꼭 필요한 사회기반시설을 의미한다. 공공 SoC 서비스는 사물통신을 통하여 공공 SoC 인프라에 대한 무인 감시·제어와 원격 검침, 환경 감시와 재난 예방 및 구호 서비스 등을 제공할 수 있다. 사물통신을 통한 공공 SoC 서비스에는 유통 및 물류 차량 실시간 모니터링 및 제어서비스, 철도·도로·교통 등 공공 시설물에 대한 안전 진단 및 모니터링 서비스, 전기·수도 시설 감시와 원격 검침 서비스, 재난 알림 서비스, 국방 및 안보 목적의 감시 서비스 등의 서비스가 예상되고 있다.[20]

공공 SoC 서비스에서 사물통신이 이미 사용되고 있으며, 앞으로도 가장 주목해야할 분야는 바로 SCADA(Supervisory Control And Data Acquisition) 시스템이다. SCADA 시스템은 주로 원방감시제어시스템으로 번역되는 기술로 '전력, 가스, 수도 등의 주요기반시설 및 산업 부문에서 원거리에 산재된 장비의 효과적인 원격 모니터링 및 제어를 위해 사용되는 시스템' 으로 정의된다. 산업 제어시스템(Industrial Control System, 이하 ICS)에서 SCADA 시스템은 생산 프로세스를 제어하고 모니터링하는 시스템으로 사용되어, ICS의 중추적인 역할을 하고 있다. ICS는 전력 시스템, 수자원 관리 시스템, 원유 및 가스의 공급 시스템, 화학 시스템, 교통 등 국가주요기반시설(Critical Infrastructure)에서 사용되고 있다. SCADA 시스템의 주요 기능은 원격 감시, 원격 측정, 원격 제어, 경보 발생, 운영자 조작 명령 등으로 공공 SoC 서비스와 유사하다.

SCADA 시스템은 원격단말장치(Remote Terminal Unit, RTU), 관리 제어 시스템(Supervisory Control System), 프로그래밍 가능 로직 제어기(Programmable Logic Controller, PLC), 통신 기술(Communication Technologies) 등으로 구성된다. RTU는 기기들과 물리적으로 연결되어 현장에서 데이터를 수집하고 전송 가

20) 김동기, "사물지능통신 서비스 추진 전략", 사물지능통신 컨퍼런스 발표자료, 2010

능한 형식으로 변환한 뒤 중앙기지국으로 송신하는 기능을 수행한다. 관리제어시스템은 RTU와 PLC의 제어 및 운영인터페이스의 구현을 위한 어플리케이션 및 장비이다. PLC는 산업 플랜트의 자동 제어 및 감시에 사용하기 위한 장치로, 미리 프로그램 된 제어순서에 의해 설비를 제어하며, 추출된 자료를 LAN을 통하여 중앙센터로 보내는 역할을 한다. 이러한 통신에 있어서 사물통신기술이 사용되며, 통신 프로토콜로는 Modbus RTU, RP-570, Profibus, Conitel와 같은 프로토콜이 사용되고 있다. 운영 인터페이스는 운영자가 SCADA 시스템의 효율적인 감시·제어를 수행하는 것을 보조하기 위해 수집된 정보를 사용하기 편한 형태로 시각화하고, 상호작용 할 수 있도록 도와주는 기능을 수행한다. SCADA 시스템은 이와 같이 RTU에서 수집하는 원격지의 기기 정보를 PLC 등에서 처리하며, 이는 운영자에게 송신되어 인터페이스를 통하여 정보를 해석하고 명령을 내리는 일련의 과정을 통해 운영된다.



(그림 16) SCADA 시스템의 개념도

출처: Wikipedia, "SCADA", http://en.wikipedia.org/wiki/SCADA

SCADA 시스템은 현재 교통, 발전, 수자원 관리 등 공공 SoC 분야의 전반적인 분야에서 사용되고 있으며, SCADA 시스템에서 사물통신은 중요한 역할을 하므로 공공 SoC 분야의 사물통신은 중추적인 역할이라고 할 수 있다.

최근 저탄소 녹색성장이라는 정부 기조에 따라 국가적으로 추진되고 있는 스

마트 그리드(Smart Grid) 역시 사물통신이 사용되는 공공 SoC 분야의 대표적인 전력 분야이다. 스마트 그리드는 효율적인 전기 에너지의 사용을 목적으로, 기존 전력망에서 전력 공급자와 소비자 간의 실시간 데이터 교환을 가능하게 하는 양방향 통신을 구축하여, 지능화된 전력 에너지의 송·배전이 가능하도록 하는 '차세대 지능형 전력망'을 의미한다.

스마트 그리드를 구성하고 있는 요소 기술은 지능형 스마트 미터기 등 AMI(Advanced Metering Infrastructure) 기술, 계통 운영 기술, 전기자동차 충전 인프라 등으로 구성된다. 계통 운영 기술은 기존의 전력 계통의 운영에 있어 시스템에 컴퓨터나 통신기술을 활용하여 전력 계통의 현장에는 직접 가지 않고도 원거리에 산재되어 있는 배전선로용 개폐기를 조작하고, 고장구간을 자동 색출할 수 있는 전력설비 원격제어 시스템과 관련된 기술이다. AMI 기술은 기존의 원격 검침기술이 한 단계 더 진보한 기술이며, 수요반응 기술은 부하를 줄이고 에너지 사용비용을 줄이기 위한 수요반응과 관련된 기술이다. 사용자영역 네트워크 기술은 사용자가 AMI 기술과 수요반응 기술 등을 사용하여 스마트 그리드 최종단의 사용자 에너지 관리 프로그램 및 네트워크상의 기기 관리·제어를 가능하게 하는 게이트웨이의 역할을 수행하는 기술이다. 신재생에너지 연계 및 충전 기술은 스마트 그리드의 일부로 구성되는 신재생에너지의 수급의 안정성을 위해 다른 에너지 시스템과 연계운용을 위한 기술로, 이 기술에는 전기 자동차의 충전과 전기자동차의 배터리를 에너지 저장소로 사용할 수 있도록 하는 기술 등이 포함된다.[21]

스마트 그리드의 기술에서 살펴볼 수 있듯이, 스마트 그리드에서는 가정 등 전력의 소비처에서 스마트 미터를 통하여 사용량과 전력의 가격 등의 정보를 전력회사, 전력 발전소 등과 통신하며, 자동으로 검침되는 양방향 통신 기술이 핵심이다. 이와 같은 AMI 환경에서는 각 기기와 스마트 미터기, 그리고 이를 관리하는 수요 반응 시스템 등이 사물통신 기술을 통하여 자동적으로 정보를 주고받는다. 이러한 환경으로 인하여 스마트 그리드의 구현을 위하여 사물통신 기술은 핵심적

21) 도윤미 외, "스마트 그리드 기술 동향: 전력망과 정보통신의 융합기술", 한국전자통신연구원 『전자통신동향분석』, 제24권 제5호, 2009

인 요소로 평가되고 있다.

(그림 17) 스마트 그리드의 주요구성요소

출처: 임종인, Smart Grid Security, 방송통신기술전망포럼 발표자료, 2010

제 2 절 사물통신 동향

1. 표준화 동향

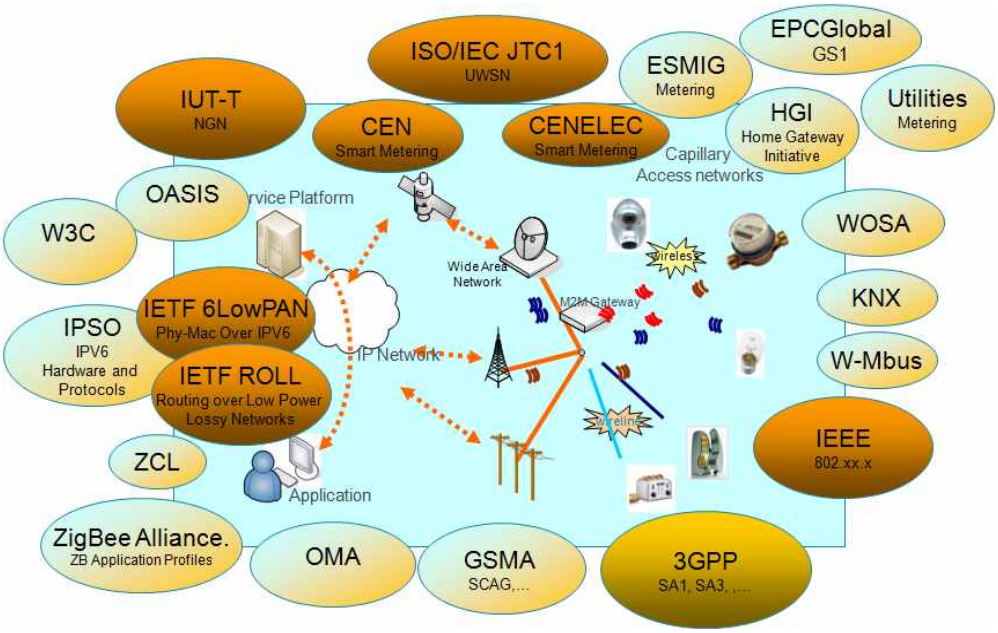
사물통신의 요소기술들은 각 기술 관련 단체들에 의하여 표준화 작업이 이루어지고 있다. 전기전자공학에 관한 주요 표준 및 연구 정책을 수행하는 미국 전기전자 학회 (Institute of Electrical and Electronics Engineers, IEEE)는 802.16.M 등 링크 및 물리계층에 대한 표준을 연구하고 있다. 유럽전기통신표준협회(European Telecommunications Standards Institute, ETSI)는 사물통신 관련 분과위원회인 M2M TC를 조직하여, 사물통신 솔루션 및 서비스 관련 표준화를 연구하고 있으며, 현재 네트워크 구조(Network function architecture), 서비스 요구사항(Service requirement), 스마트미터기 등 예상사용 환경(Use case: Smart metering) 등 표준문서를 개발하고 있다.

국제표준을 연구하는 ISO(International Organizations for Standardization)는 JTC1(Information Technology)의 WGSN(Working Group Sensor Network)을 통하여 사물통신을 기존 RFID/USN을 확장하여 새로운 통신망 기술로 정의하고 있다.[22] 국제전기통신연합(International Telecommunication Unionm ITU)은 3GPP(3rd Generation Partnership Project)를 통하여 사물통신 네트워크 최적화에 대한 표준을 연구하고 있다. 3GPP는 2005년 9월 산하 TSG SA WG1의 Facilitating Machine to Machine Communication in GSM and UMTS 보고서 등을 통하여 사물통신 연구를 시작하였으며, 이동통신 측면의 사물통신, 인간의 개입이 없는 상태의 Trusted Computing 기반 등을 연구하고 있다.[23] 또한, 사물통신에서 사용이 예상되는 ZigBee Alliance, GSMA, OMA, CEN 등 다양한 기관에서 사물통신 관련 표준화를 추진하고 있다.

---

22) 안재영, “M2M 네트워크 및 서비스 기술”, The 20th High-Speed Network Workshop, 2010

23) 안재영, 상게발표자료



(그림 18) 사물통신 구성요소별 표준화 동향

출처: David Boswarthick, “M2M Activities in ETSI”, SCS Conference 발표자료(2009)

2. 국가별 동향

유럽은 제7차 연구개발(FP7 2007~2013) 7대 과제 중 미래 네트워크 기반 과제를 선정하여 미래 네트워크 인프라가 수십억의 인구와 수조에 달하는 사물을 서로 연결할 수 있도록 대비하고 있다. 이를 위하여 미래 네트워크 2억 유로, 미래네트워크 서비스와 아키텍처 1.2억 유로 등을 투자하고 있다.

미국은 GENI(Global Environment for Network Innovation) 프로젝트를 통해 새로운 네트워크 아키텍처 등 연구, 인프라 및 서비스 아키텍처 연구로 2009년부터 2013년까지 3억 6700만 달러 배정하여 사물통신을 포함한 미래 네트워크를 연구하고 있다. 또한 국가정보위원회(National Intelligence Council, NIC)는 2025년까지 미국의 관심사에 영향을 미칠 수 있는 6대 와해성 기술(Disruptive Civil Technologies)과 관련된 보고서를 발간하였다.[24] 이 보고서에서 NIC는 6대 와해성

기술의 하나로 The Internet of Things(IoT)를 포함되어 있으며, 잠재적 영향과 예상 시나리오를 도출하고 있다.

일본은 2008년 유비쿼터스 사회를 구현하기 위하여 총무성에서 u-Japan 정책을 추진하고 있으며, 이를 위하여 중점 연구개발 방향을 UNS(Ubiquitous Network Society) 전략 II를 통하여 정립하였다. 이 UNS 전략 II는 유비쿼터스 네트워크 사회를 지향한 보편적 커뮤니케이션 기술, 차세대 네트워크 기술, ICT 안심·안전 기술 등 3개 분야에서 11대 전략을 수립하였다.[25] 이 11대 전략 중의 하나로 센싱유비쿼터스 시공 기반을 선정하여 환경·재해 등 사회문제를 사물통신을 통하여 해결하기 위하여 추진중이다.[26]

우리나라는 2004년 과거 정보통신부에서 추진하였던 IT839 전략에서 3대 인프라의 하나로 유비쿼터스 센서네트워크(Ubiquitous Sensor Network, USN)로 선정하여 개발을 추진하였다. 방송통신위원회는 2009년 사물통신 기반구축 기본계획을 발표하여 2012년까지 세계 최고의 사물통신 기반구축을 계획하고 있다. 현재 사물통신 구현은 이동통신사업자들에 의하여 서비스가 제공되고 있거나 기획 중에 있는 상태이다.

---

24) NIC, "Disruptive Civil Technologies", 2008
url : http://www.fas.org/irp/nic/disruptive.pdf
25) 한국인터넷진흥원, "일본의 정보보호 R&D 정책 현황 및 시사점", 2008
26) 방송통신위원회, "사물통신 기반구축 기본계획(안)", 2009

제 3 장 사물통신에서의 인증 기술

제 1 절 사물통신과 인증

사물통신 기술은 원격지의 기기들을 효율적으로 제어하고 정보를 수집할 수 있는 장점으로 인하여 향후 많은 사용이 예상되고 있으며, 2020년 1,000억대가 넘는 기기들이 인터넷을 통하여 연결될 것으로 예측되고 있다. 방송통신위원회의 R&D 전략에 나타난 예상 사용 환경(Use Case)과 같이 사물통신은 주변의 기기를 제어하는 개인형 서비스뿐만 아니라, 신변 보호 등을 위한 안심 서비스, 차량 간 혹은 차량과 도로간 통신하는 지능형 자동차 서비스, 사회 주요 기반시설인 SoC 등에서 사용이 예상되며, 이와 같은 분야에서는 보안이 가장 중요한 고려사항이다.

사물통신 환경에서는 데이터 기밀성, 데이터 무결성, 디바이스 무결성, 시스템 가용성, 사물통신 디바이스 인증, 사물통신 서버 인증, 그리고 접근 제어 및 인가와 같은 보안이 고려되어야 할 것으로 판단된다.[27] 사물통신환경은 사물통신 기술의 특성 상, 사람이 개입하지 않은 채 기기들 간의 상호 통신에 의하여 이루어지므로 각 기기 간 상호 인증을 하기 위한 인증기술이 반드시 필요하다. 따라서 M2M 환경에서 안전하고 효율적인 인증 기술에 대한 논의가 필요한 시점이다.

사물통신 환경에서 사용 가능한 인증 기술과 관련된 연구 및 표준화 등은 현재까지 진행되고 있지 않은 상태이다. 사물통신 환경은 USN 환경, 그리고 홈네트워크 환경 등과 유사한 환경으로, 이와 같은 환경에서는 아이디/패스워드 기반 인증 기술, MAC 주소 기반 인증기술, 암호 프로토콜을 이용한 인증 기술이 사용되고 있으며, 최근 PKI 기반 기기 인증서 기술이 이 기술들을 대체하고 있는 시점이다. 암호 프로토콜 기반 인증 기술의 경우 아이디/패스워드 혹은 PKI 기반 기기 인증서 인증 기술과 중복되는 개념이 있지만, 암호 프로토콜을 활용한 인증 기술

27) 은선기 외, “안전한 M2M 통신 구축을 위한 상호인증 및 키 교환 프로토콜”, 한국정보보호학회논문지, 제20권 제1호, (2010)

에 대한 연구가 활발히 진행되어 왔고, 현재 홈네트워크 기기 인증을 위한 국내 표준에서도 활용되고 있는 인증 기술이기 때문에 따로 분류하여 보는 견해가 있다.[28)]

사물통신 환경에서 역시 홈네트워크 환경에서의 인증기술이 사용 가능할 것으로 예상된다. 현재 사물통신 환경에서 사용이 가능할 것으로 예상되는 인증기술은 ID/PW 기반 인증기술, MAC 주소 기반 인증기술, 암호 프로토콜, 인증서 기반 인증기술, 그리고 ID 기반 암호기술(ID-Based Encryption, IBE)를 이용한 인증기술 등이다. 이와 같은 인증기술 등은 기술 특성 상, 각 인증기술 별로 장·단점을 갖고 있으며, 이 장·단점에 따라 서로 다른 환경에서 상호보완적으로 사용이 가능할 것으로 예상된다. 하지만, 안전한 사물통신 환경을 위하여 기반시설 등 보안이 중요한 시설에서는 안전한 인증기술이 사용되도록 규정해야할 필요성이 있다.

다양한 인증기술 가운데서, 사물통신 환경에서 사용가능한 인증기술을 도출하기 위해서는 사물통신 환경에서 예상되는 보안 위협 및 각 예상 사용 환경 별 인증기술의 요구사항 도출이 선행되어야 한다. 현재 사물통신 환경에서 식별되고 있는 보안위협과, 예상 사용 환경 별 인증기술의 요구사항은 다음과 같다.

1. 사물통신 환경의 보안 위협

사물통신의 특성 상, 사물통신기기는 저전력, 소규모, 저렴한 가격, WAN, WLAN 등 네트워크를 통한 통신, 그리고 사람의 개입이 없이도 운영이 가능할 수 있는 등의 특징이 요구된다. 사물통신기기는 원격지에 설치되어 오랜 기간 동안 사용이 되며, 기능 수행을 위하여 원격 관리가 필요하다. 또한 많은 예상 사용 환경(Use Case)에서 사물통신의 구축에 있어 매우 많은 사물통신기기들이 필요로 하며, 많은 경우 이동형(Mobile)이며, 각 개별 기기를 관리 혹은 제어하는 것은 비현실적이거나 불가능에 가깝다. 이와 같은 사물통신 기기들의 요구사항들로 인하

28) 한국정보통신기술협회(TTA), “홈서버 중심의 홈네트워크 사용자 인증 메커니즘”, 2005

여 사물통신 기기들은 무선 통신 등에 있어서 취약점을 갖게 된다.[29] 3GPP(Third Generation Partnership Project)의 3A3(Security WorkGroup)은 다음과 같이 사물통신의 취약점을 분석하고 있다.[30]

[표 1] 사물통신의 취약점

취약점	상세 취약점
물리적 공격	· 조작된 장치에 인가된 인증토큰을 삽입 · 조작된 소프트웨어의 설치 혹은 삽입 · 구축 전/후 부채널(Side-Channel) 공격 등
자격증명의 타협	· 토큰과 인증 알고리즘 혹은 취약한 인증기술에 대한 BruteForce공격 · 물리적 침입 · 부채널 공격 · 사물 통신 식별 모듈(Machine Communication Identity Module, MCIM)에 존재하는 인증 토큰에 대한 악의적인 복제 등
변경을 통한 공격	· 악의적인 소프트웨어의 업데이트 혹은 설정 변경 · 사물통신의 소유주, 사용자의 잘못된 설정 변경 · 접근 제어 리스트의 잘못된 구성 등
프로토콜 공격	· 최초 접속에 대한 중간자공격(Man-in-the-Middle) · 서비스거부(Denial of Service, DoS) 공격 · 활성화된 네트워크의 취약성을 이용하는 공격 등

29) Inhyok Cha et al., “Trust in M2M communication”, IEEE Vehicular Technology Magazine, 2009

30) “Feasibility study on remote management of USIM application on M2M equipment”, 3GPP Tech. Rep. 33.812

31) Rogue Device, 사물통신 네트워크에 인가받지 않은 채 연결된 사물통신 디바이스

코어 네트워크에 대한 공격	· 무선망운영업체(Mobile Network Operator, MNO)에 대한 공격 · 장치 위장을 통한 공격 · 모뎀, 라우터, 게이트웨이의 방화벽의 잘못된 구성 · 코어네트워크에 대한 서비스거부 공격 · 인가되지 않은 위치로 장비의 이동 · 로그 장비[31] 사용을 통한 공격
사용자의 데이터와 프라이버시 공격	· 사용자 혹은 장비가 전송하는 메시지의 도청 · 다른 사용자 혹은 장비로 가장하여 메시지 도청 · 사용자의 네트워크 ID 혹은 기타 기밀 정보의 누설 등

이와 같이 일반적인 사물통신 환경의 취약점은 물리적 공격, 자격증명의 타협, 변경을 통한 공격, 프로토콜 공격, 코어네트워크에 대한 공격, 사용자 데이터 및 프라이버시에 대한 공격 등이다. 이러한 사물통신 환경의 보안 취약성은 기술적·정책적 보안 조치를 통해 예방할 수 있으며, 인증 기술은 사물통신 환경에서의 대표적인 보안 조치이다.

2. 사물통신 예상 사용 환경별 보안 위협과 인증기술의 요구조건

인증기술이 가장 대표적으로 사용되고 있는 금융 분야에서는 공인인증서를 의무적으로 사용하도록 규정하고 있었으나, 스마트폰의 보급 등 환경의 변화에 따라 공인인증서 의무화 규정을 폐지하고, 다양한 인증기술 중 인증기술의 요구사항을 충족시키는 인증기술을 선택적으로 사용하도록 규정하였다. 이는 2010년 5월 31일 국무총리실, 금융위원회, 방송통신위원회 등 관계부처와 공동으로 발표한 『전자금융거래 인증방법의 안전성 가이드라인』[32]에서 규정하고 있다. 동 가이드라인에서는 전자금융거래시 적용될 인증방법이 갖춰야할 기술적 안전성 요건으로, 이용자 확인, 서버인증, 통신채널 암호화, 거래내역의 위변조 방지, 거래부인방지 기능 등을 규정하고 있다. 이와 같은 요건을 갖춘 인증기술에 대하여 금융기관 또는 전자금융업자는 공인인증서 사용하지 않고 인용자 인증, 서버인증 및 통신채널 암호화

32) 국무총리실, '전자금융거래 인증방법의 안전성 가이드라인'확정 보도자료, 2010.5.31

요건을 갖춘 경우, 인증방법평가위원회의 안전성 평가를 거쳐 다양한 전자금융 서비스 제공이 가능하도록 규정하고 있다.

사물통신 환경에서 역시 특정 인증기술을 규정하기 보다는, 각 사용환경 별 요구사항을 규정하고 이와 같은 요구사항을 충족시키는 인증기술을 선택적으로 적용하는 것이 현실적인 상황이다. 사물통신 환경에서 인증기술의 일반적인 요구사항은 다음과 같이 도출할 수 있다.

1. 디바이스 인증
사물통신 환경에서 통신 서버는 전송 및 수신하고자 하는 데이터가 정당한 M2M 디바이스 여부를 식별 및 인증할 수 있어야 한다.

2. 서버 인증
사물통신 환경에서 사물통신 디바이스 혹은 게이트웨이는 통신하고자 하는 사물통신 서버가 정당한 서버인지 등의 여부를 식별 및 인증할 수 있어야 한다.

3. 통신 내용의 암호화
사물통신 환경에 따라 이루어지는 통신 내용은 개인정보 및 유출 시 사회적으로 피해가 예상되는 데이터일 경우 반드시 암호화를 통하여 기밀성 및 무결성을 제공해야 한다.

4. 부인방지
과금 등에 있어 사물통신 인증기술은 사물통신 디바이스 사용자 등이 정당한 통신 내용을 부인할 수 없는 수단을 제공할 수 있어야 한다.

5. 기타 환경과의 호환성
사물통신 환경에서 사용되는 인증 기술은 기타 도메인 디바이스 등과 호환될 수 있어야 한다.

6. 인증기술의 효율성

사물통신 환경에서의 인증기술은 기존 디바이스에서 사용되므로 성능의 제약 및 기기의 성능의 저하 등을 고려해야 한다. 따라서 모든 디바이스에서 사용될 수 있는 경량화 된 인증기술을 고려하여야 한다.

7. 사용자 개입의 최소화

사물통신 인증기술은 사물통신 환경의 특성 상 사용자의 개입이 최소화 할 수 있는 인증기술을 사용하여야 한다.

이와 같은 일반적인 인증기술의 요구사항 외에도, 각 사용 환경의 보안의 중요성에 따라 서로 다른 보안의 요구 사항이 예상된다. 따라서 각 환경에 사물통신 기술의 도입 시, 예상 가능한 보안 위협 및 이를 방지하기 위한 인증기술의 요구사항의 도출이 필요하다. 방송통신위원회의 사물통신 예상 사용 환경에 따라 예상되는 보안 위협 및 인증기술의 요구조건은 다음과 같이 도출될 수 있다.

가. 개인 맞춤형 서비스

개인 맞춤형 서비스는 사물통신을 이용하여 주변 사물을 제어하거나 맞춤형 정보 등을 제공하는 서비스이다. 개인 맞춤형 서비스로는 PAN을 통한 주변 사물 제어, 유비쿼터스 도시 및 스마트홈 환경에서의 가전제어, 유헬스케어를 통한 원격 진료, 디지털 사이니지, 개인 콘텐츠 제공 등의 서비스가 예상된다.

개인 맞춤형 서비스에서는 개인정보에 대한 보안 위협이 가장 클 것으로 예상된다. 특히 유헬스케어 환경에서는 개인의 건강 정보, 병명 등 진료 정보의 네트워크를 통한 전송에 따라 인가된 사용자만이 해당 정보를 열람할 수 있는 강력한 인증기술이 요구된다. 또한 외부의 공격자에 의한 도청을 방지하기 위하여 암호화 기술 역시 적용되어야 한다.

스마트홈 환경에서 가전기기 제어를 위한 서비스, 주변기기를 제어하는 서비스 등에서는 서로 다른 플랫폼, 서로 다른 통신 기술 등 서로 다른 환경에서 서로 다른 기기들과의 통신을 위하여 이기종간 인증기술의 호환성이 . 스마트폰, 테블릿, 전자책 등 모바일 기기의 콘텐츠 제공 서비스, 스마트티비의 VoD(Video on Demand) 등의 서비스에서는 과금을 위하여 부인방지 기능 역시 요구될 것으로 예상된다.

나. 스마트 안심 서비스

스마트안심 서비스는 에스코트 서비스, 위험상황 알림 서비스 등 사회적 약자를 보호하기 위한 서비스이다. 센서 등을 통하여 수집되는 정보를 사물통신 플랫폼과 통신하면서, 미리 설정된 특정 상황이 발생 시 자동적으로 이를 통보하는 서비스이다.

스마트안심 서비스에서의 보안위협은 DoS(Denial of Service) 공격 등과 같은 서비스 중단이 가장 대표적이고 치명적인 위협으로 예상된다. 스마트안심 서비스는 위급 상황 발생에 대비한 서비스이기 때문에 서비스가 중단될 경우 심각한 문제가 발생할 수 있다.

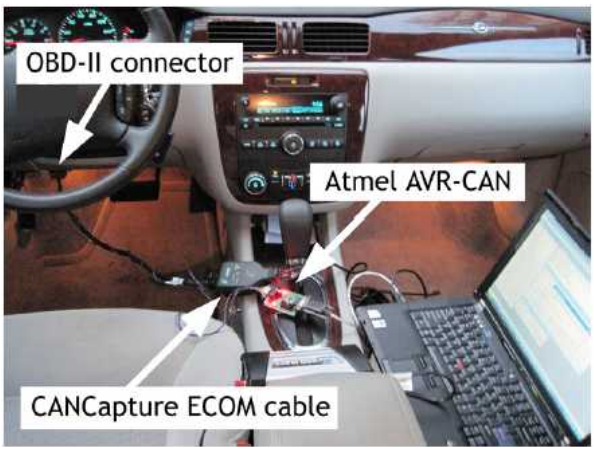
스마트안심 서비스는 위급 상황 발생에 대비한 서비스이기 때문에 스마트안심 서비스에서 인증기술이 갖추어야할 가장 중요한 요소는 바로 가용성(Availability)이다. 따라서 안정적으로 인증기술이 끊김 없이 제공될 수 있는 인증기술이 요구된다. 또한 스마트안심 서비스에 사용되는 사물통신 기기의 크기와 전력 등의 제약요건에 따라, 저전력의 낮은 연산으로도 가능한 인증기술이 사용되어야 한다.

다. 차량 지능화 서비스

차량 지능화 서비스는 자동차에 IT 기술 등을 접목시킨 지능형자동차와, 자동차의 주행 환경과 도로 인프라와 관련된 지능화 기술인 ITS(Intelligent Transport System)과 같은 기술을 의미한다. 지능형자동차 기술은 CAN(Controller Area Network)을 통한 ECU(Electronic Control Unit)간 통신으로 자동화된 차량 제어이며, ITS는 VANET(Vehicular Ad-hoc Network)을 통한 차량간 혹은 차량과 도로변 통신 스테이션 등과의 통신 등을 통하여 도로 및 주변 상황에 대한 정보를 송수신 하는 기술이다.

차량 지능화 서비스에서 보안 위협 요인은 CAN과 VANET 통신의 도청 및 메시지 변조를 통한 공격이 예상된다. CAN 환경에서 예상되는 보안위협은 2010년 5월 미국에서 실험한 자동차 해킹 실험이 대표적인 사례이다. 이 실험은 대시보드 밑에 위치한 OBD(On-Board-Diagnostics)-II Port를 통하여 통신 시스템을 설치하고, CarShark라는 CAN 내의 패킷 분석 장치를 통하여 차량을 임의적으로 제어 할 수 있다는 사실이 입증되었다. 차량 주행 시 CAN을 통해 전송되는 ECU에 대한 명령들을 가로채어 분석하거나, Fuzzing Packet[33] 등을 통하여 65km/h의 속도로 주행중인 차량을 공격자가 임의적으로 경적을 울리고 엔진을 멈추고 브레이크를 마비시킬 수 있음 확인되었다. 이처럼 CAN 환경에서 통신 시 적절한 인증이 없을 경우 공격자가 CAN에 접속이 가능하다면 정보를 분석하고, 임의적으로 제어가 가능하다는 보안위협이 있다. 자동차 환경에서 제어는 곧 생명과 직결되므로, 이는 치명적인 위협이다.

33) 랜덤한 혹은 일부만 랜덤한 패킷을 지속적으로 테스트



(그림 19) 자동차 해킹실험에 사용된 도구

출처: K. Koscher et al., Experimental Security Analysis of a Modern Automobile, The IEEE Symposium on Security and Privacy, 2010

ITS의 VANET 환경에서 역시 네트워크를 통한 여러 위협이 예상된다. 차량에게 환경과 다른 정보를 송신하여 교란함으로써 지능적 충돌 유도, 혹은 환경 정보 위조, 서비스 거부 공격 등의 공격이 예상된다. 또한 통신상에서 기록된 차량의 정보를 임의적으로 조작하거나 이를 수집하는 차량 정보 위조 및 프라이버시 추적 등이 보안위협으로 예상된다.

(그림 20) ITS 서비스의 보안 위협

차량 지능화 서비스에서는 이와 같은 보안위협이 예상됨에 따라, 통신에 있어 이 정보가 올바른 주체로부터 전송된 올바른 정보임을 확인할 수 있는 인증기술이 반드시 필요하다. 차량 지능화 서비스에서는 인증을 위한 연산 처리 시간이 지연될 경우 고속 주행되고 있는 환경에서 큰 위협이 될 수 있다. 따라서 연산에 소요되는 시간이 적으며, 올바른 사용자만이 인증을 받을 수 있는 강력한 인증기술이 요구된다.

또한 여타 사물통신 환경에 비하여, 차량 지능화 서비스는 이동성으로 인하여 교통이 혼잡하거나 이동량이 많을 경우 인증서버에 인증처리가 집중되어 과부화가 걸릴 수 있는 문제도 예상할 수 있다. 따라서 서버가 많은 인증 세션을 처리할 수 있도록 경량화된 인증기술이 역시 요구되며, 또한 인증서버는 과부하를 고려하여 적절한 수용력을 갖도록 설계하여야 한다.

라. 공공 SoC 서비스

공공 SoC 서비스는 사물통신 기술을 이용하여 도로, 항만, 철도 등 공공 SoC 인프라에 대한 무인 감시·제어와 원격 검침, 환경 감시와 재난 예방 및 구호 서비스 등을 제공하는 서비스를 의미한다. 현재 SCADA 시스템에서 원격지의 정보 수집을 위하여 사물통신이 사용되고 있으며, 스마트그리드 환경에서 사용이 예상되고 있다.

SCADA 시스템은 구조는 RTU 통하여 수집되는 원격지의 정보를 전송 가능한 형식으로 변환한 뒤 중앙기지국으로 송신하며, PLC(Programmable Logic Controller)는 미리 프로그램 된 제어순서에 의해 설비를 제어하며, 추출된 자료를 LAN을 통하여 중앙센터로 보내며, RTU와 PLC를 통해 수집된 정보를 바탕으로 자동적으로 제어하거나, 운영자가 이를 바탕으로 제어하는 방식이다. SCADA 시스템은 최근 Stuxnet에 의한 이란 부셰르 원자력발전소 마비 등 이미 사고 사례가 발생하고 있으며, 보안 위협에 대한 선행연구가 이루어진 시점이다.

가장 선도적으로 SCADA 시스템의 보안을 연구하고 있는 US-CERT의 제어시스템보안센터(Control System Security Center, CSSC)와 아이다호국립연구소(Idaho National Laboratory, INL)의 국가 SCADA 테스트베드(National SCADA Test Bed, NSTB)는 Common Control System Vulnerabilities[34] 보고서를 통하여 SCADA 시스템의 위협과 이에 대한 해결책을 제시하였다. 동 보고서에서 도출한 위협은 네트워크 정찰 및 데이터 수집, 역공학, 중간자 공격이다. US-CERT는 이 위협들에 대한 대응책(Mitigation Technique)으로 MAC Address를 통한 제한(Mac Locking), MAC 주소 관리를 위한 ARP 테이블 관리, 그리고 통신 내용의 암호화이다. 이는 곧 인증과 암호화 통신으로 SCADA 시스템의 보안을 위하여 인증이 필요하다고 제시하였다.

스마트그리드는 기존 전력망에 IT기술을 융합하여, 전력 공급자와 소비자 간의

34) US-CERT, INL, Common Control System Vulnerabilities, 2005
url : http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf

실시간 데이터 교환을 통하여, 지능화된 전력 에너지의 송·배전이 가능하도록 하는 '차세대 지능형 전력망'을 의미한다. 스마트그리드는 각 가정 각 기기와 스마트미터기, 그리고 이를 관리하는 수요 반응 시스템 등이 사물통신 기술을 통하여 자동적으로 정보를 주고받는 기술로, 이 과정에서 사물통신 기술이 사용될 것으로 예측하고 있다.

Secure Computing에서 발표한 보고서에서는 전력 기반시설을 필두로 한 중요 인프라의 보안이 취약한 주요 요인으로 센서, 디지털 계량기, 원격접속기능 등의 활용으로 인한 Access Points 수의 증가, IP 기반 네트워크의 활용, 마이크로소프트의 윈도우즈와 같이 많이 사용되는 IP 플래폼 선호, 네트워크 자동화 및 통제 시스템 업체의 보안에 대한 낮은 관심도 등을 꼽고 있다.[35]

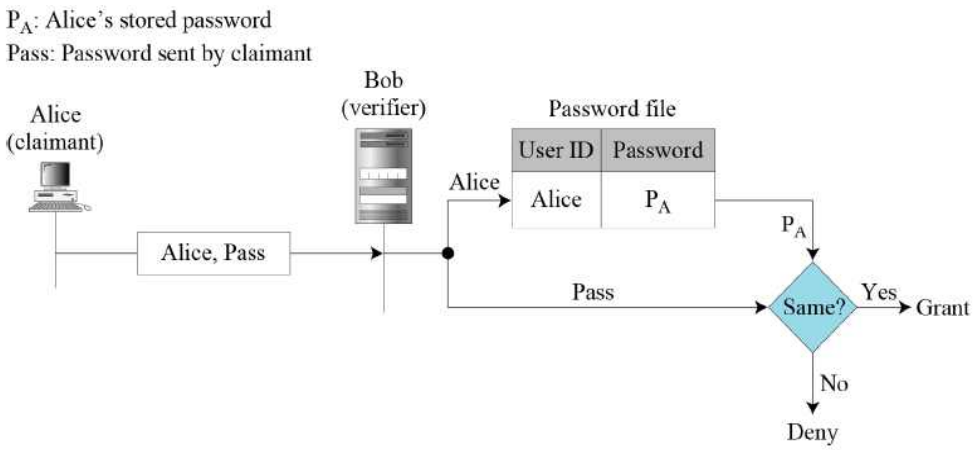
SCADA 시스템의 경우 현재 생산시설, 교통 제어, 가스, 수도 등 국가기반시설에서 사용되고 있으며, 스마트그리드의 경우 전력망으로 국민의 생활과 직결되는 주요기반시설이다. 이와 같은 SCADA 시스템과 스마트그리드 시스템에 공격자가 침투하여 임의적으로 제어를 하게 된다면 이는 국가적 재앙으로 이어질 것으로 예측됨에 따라 그 어떤 환경보다 강력한 인증이 요구된다. 스마트그리드 환경에서 스마트미터의 경우 각 가정마다 설치되며, 모니터링이 가능한 곳에 설치되기 때문에 물리적 접근이 용이하다. 따라서 스마트미터기의 경우, 물리적 보안 위협에도 안전한 인증기술이 요구된다. 또한 스마트그리드 환경에서는 과금이 중요한 요소이므로, 부인방지 기능이 요구될 것이다.

35) Žarko Sumić, "Hype Cycle for Intelligent Grid Technologies", Power Systems Engineering Research Center - Executive Forum on Smart Grid Deployment Strategies and Business Opportunities,, 2009

제 2 절 ID/PW 기반 인증

1. 기술 개요

ID/PW 기반 인증기술은 인증 기술 중 가장 기본적인 인증 방식으로 주로 서버/클라이언트 인증에서 사용되는 기술이다. 서버는 클라이언트의 최초 등록시 ID와 PW를 저장하고 있으며, 클라이언트가 접속 시도 시 해당 클라이언트 ID에 해당하는 PW가 서버가 저장하고 있는 ID의 PW와 일치하는 지 확인하는 방식의 인증이다.



(그림 21) ID/PW 인증 도식도

출처: Forouzan, Cryptography and Network Security, 2007

ID/PW 인증 기술은 서버에 패스워드 리스트가 저장되므로 서버에 저장된 클라이언트의 패스워드 리스트가 노출될 경우 인증이 무력화 될 수 있다. 따라서 이를 방지하기 위하여 서버에서 패스워드를 저장할 때 해쉬 함수[36]를 통하여 해쉬 값을 저장하며, 인증 시도가 이루어질 경우 서버는 클라이언트가 제출한 PW의 해

36) Hash Function, 입력 값에 대해 압축된 해쉬 값을 출력하는 함수로 같은 입력 값에 대해서는 일정한 값을 출력하며 입력 값이 조금이라도 변할 경우 출력 값은 전혀 다른 값을 출력하는 성질을 갖는 함수.

쉬값을 계산하여 저장된 해쉬값과 검증하는 방식을 채택하는 경우가 많다.

2. 기술 동향

현재 사용되고 있는 ID/PW 기반 인증 시스템은 “약한 인증(Weak Authentication) 시스템”이다. 약한 인증 시스템이란 제3의 공인 기관(Trusted 3rd Party)에 의존하지 않고, 사전에 교류가 없는 집단과 통신을 하는 인증 프로토콜을 의미한다.[37] 또한 약한 인증 시스템은 네트워크상에 프로토콜이 그대로 노출되거나, 패스워드를 암호화 하지 않은 채 평문으로 통신하거나 해쉬값을 통신하는 경우 역시 약한 프로토콜에 속한다.

“강한 인증 시스템”으로는 EKE(Encrypted Key Exchange) 프로토콜, DH-EKE(Diffie-Hellman Encrypted Key Exchange) 프로토콜 등이 있다. EKE 프로토콜은 패스워드의 인증 시, 대칭키 암호 방식과 공개키 암호 방식을 결합한 메커니즘을 통하여 제3의 공인 기관 없이도 안전성을 제공하며, 사전 공격에 강한 특징을 갖는다. 또한 이후 DH-EKE 프로토콜은 Diffie Hellman이 제안한 키 교환 방식에 기반한 EKE 프로토콜로, 키 교환 프로토콜에서 분배되는 패스워드로 메시지가 암호화되어 통신하는 방식의 프로토콜이다. 또한, Diffie Hellman의 키 교환에 기반하며, 세션 키(Session Key) 생성함수를 통하여 패스워드가 생성되는 SPEKE(Simple Password Exponential Key Exchange)가 등이 제안되고 있다.

ID/PW 기반 인증 시스템은 네트워크 등을 통해 연결된 각종 임베디드 환경에서 역시 사용되고 있는 추세이다. 현재 사용되고 있는 ID/PW 기반 인증 서비스들은 다음과 같다.

가. SSID(Service Set IDentifier) 숨김

37) Jari Arkko et al., Weak Authentication: How to Authenticate Unknown Principals without Trusted Parties, Lecture Notes in Computer Science, 2003

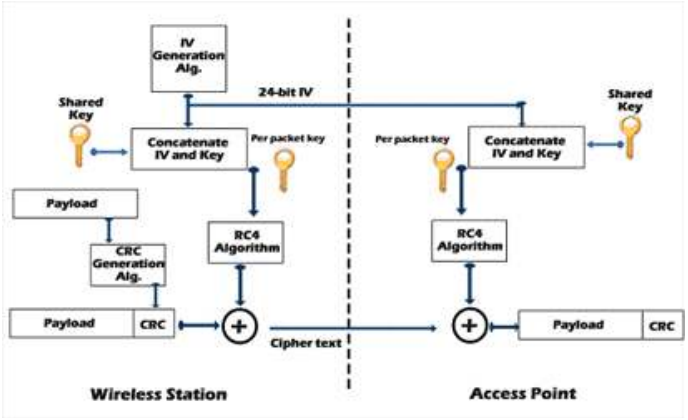
무선 네트워크 환경에서 클라이언트와 AP(Access Point) 간 통신 시, 무선 네트워크 고유 ID인 SSID(Service Set IDentifier)를 공유하여 인증하는 방식이다. 이러한 환경에서 SSID를 알 경우 인증되지 않은 클라이언트가 접속할 수 있는 문제가 있어 SSID를 숨겨주는 기능인 Secure Access를 이용하는데 이를 SSID 숨김이라고 한다. SSID 숨김의 경우 SSID의 이름을 알지 못할 경우 연결할 수 없으므로 보다 안전하다. 그러나 AP와 클라이언트간 통신이 일어나고 있는 동안은 스니핑(Sniffing)을 할 경우 SSID가 노출되는 취약성이 있어 강력한 인증이라고 할 수 없다.

나. 무선 디바이스와 AP(Access Point)간 WEP키 이용

WEP(Wired Equivalent Privacy)는 무선 인터넷 표준을 규정하고 있는 IEEE 802.11 규약에서 명시하고 있는 무선 LAN 인증 방식으로, 무선 디바이스와 AP 간 인증 시, 패스워드 방식에 기반을 두고 있는 인증방식이다. WEP 방식은 RC4 Stream Cipher를 이용한 암호프로토콜 방식이지만, WEP 키(Key)라는 비밀 정보를 공유한다는 측면에서 ID/PW 인증기술이라고 보는 견해도 있다.

WEP 키 인증 방식은 AP가 디바이스에게 Challenge 패킷을 보내고, 디바이스가 올바른 WEP 키를 보유하고 있으면 이를 통해 패스워드를 암호화하여 다시 AP로 Response를 하는 Challenge-Response 방식을 통하여 인증한다. 디바이스가 잘못된 WEP 키를 가지고 있거나 WEP 키를 가지고 있지 않다면, 적절한 Response를 생성하지 못하여 인증에 실패하게 된다.[38]

38) 김상철, 무선랜보안(Wireless LAN Security), 한국정보보호진흥원, 2002

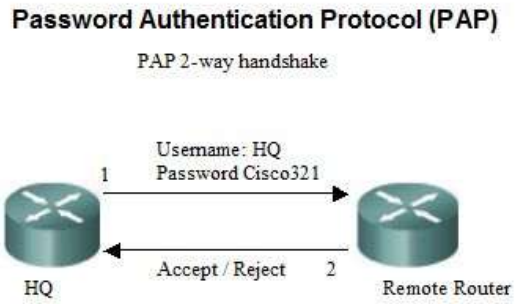


(그림 22) WEP 인증 도식도

출처: AirTight Networks WebSite

다. PAP 인증 방식

PAP(Password Authentication Protocol) 인증 방식은 단대 단 통신 규약(Point-to-Point Protocol)로, Unix 시스템에서 서버와 클라이언트간 인증 시 사용되는 프로토콜이다. PAP 프로토콜은 클라이언트에게 기존에 설정된 패스워드를 이용하여 자동으로 인증을 제공하는 기술이다. 클라이언트는 자신의 ID와 PW를 서버에 보내고, 서버와 보유하고 있는 ID/PW 정보와 비교를 통하여 인증하는 방식의 프로토콜이다.



(그림 23) PAP 인증 도식도

출처: Orbit Computer Solutions WebSite

PAP 프로토콜은 서버-클라이언트뿐만 아니라, 서버와 서버간의 인증에도 사용되고 있다. 서버-서버 간 인증 역시 서버-클라이언트 방식과 마찬가지로 Challenge-Response 방식으로 인증을 하며, 호스트네임과 PW 정보의 일치 여부를 통해 인증하는 방식이다. 홈 네트워크 환경에서 역시 PAP를 통하여 홈게이트웨이 간 상호 인증 시, 호스트네임과 PW를 통하여 상호 인증이 가능하다.

라. RFID 태그와 RFID 리더 간 인증 (EPC Global)

RFID(Radio Frequency IDentification)는 RFID 태그와 리더, 그리고 인증서버로 구성되어 있다. RFID 태그는 메모리 용량과 연산량, 그리고 전력 등의 한계로 인하여 상대적으로 계산량이 적은 인증 프로토콜을 사용해야 한다. 이로 인하여 RFID 환경에서 태그와 리더 간 인증 시에는 태그 고유의 키를 이용하여 인증한다. 이러한 RFID 인증 프로토콜에는 Hash lock, Randomized Hash lock, Hash-chain 기법 등이 있다. Hash lock 인증방식은 태그의 유일한 비밀키를 해쉬화한 metaID를 통해 이루어진다. 리더는 태그의 metaID에 해당하는 비밀키 값을 서버로부터 전달 받는다. Randomized Hash lock 인증방식은 태그에서 아이디 이외에 랜덤한 값을 선택하여 리더에게 보내어 인증하는 방식이다. Hash-chain 인증방식에서는 태그에 저장된 비밀키를 Hash-chain을 이용하여 바꾸어 주는 방식을 이용하였다. 이러한 RFID 태그-리더 간 인증 방식은 태그에 저장된 아이디 또는 패스워드 이용하여 인증을 수행하기 때문에 이 정보가 노출되지 않도록 해야 한다. 또한 태그 패스워드의 길이는 8비트이므로 공격자로 하여금 쉽게 패스워드를 추측 가능하다.[39]

3. 사물통신 환경에서 ID/PW 기반 인증 기술

39) 조희석, RFID와 개인정보보호, <IT Solutions> 칼럼, 2005

ID/PW 기반 인증기술은 서버-클라이언트 환경에서 클라이언트가 사전에 자신의 ID와 이에 해당하는 PW를 설정하고, 이에 대하여 서버가 인증을 하는 방식의 인증 프로토콜이다. ID/PW 기반 인증기술은 ID/PW만 설정이 되면 범용적으로 어느 환경과 어떤 기기에서든 사용이 가능하며, 각 기기들이 등록된 ID/PW 리스트만 관리하면 되기 때문에 관리가 쉬우며, 요구하는 자원이 크지 않다는 장점이 있다. 하지만 서버-클라이언트가 사전에 반드시 ID/PW를 공유해야 하며, 서버와 같이 여러 주체들을 인증해야 하는 경우 각 주체들의 모든 ID/PW를 저장해야 하는 단점이 있다. 이와 같은 단점으로 인하여, 대규모 환경에서 적용할 경우 관리와 저장의 문제가 있으며, 다량의 인증을 동시에 처리해야 할 경우 부하가 걸리는 문제가 예상된다.

사물통신 환경은 대규모의 기기들이 사람의 개입이 없거나 최소화된 상태에서 상호 통신하는 환경이다. 이러한 환경에서 ID/PW 방식은 서버의 관리 및 부하가 예상되며, 새로운 기기를 추가하거나 수정을 하는 데 있어 사람의 개입이 전제되어야 하는 문제점이 있다. 또한 ID/PW 인증 방식은 부인방지 기능을 제공하지 못하여 과금 서비스 혹은 강력한 보안이 필요로 하는 분야에 적용할 경우 통신 사실 등을 부인할 수 있어 인증기술로는 큰 단점이 존재한다.

제 3 절 MAC Address 기반 인증

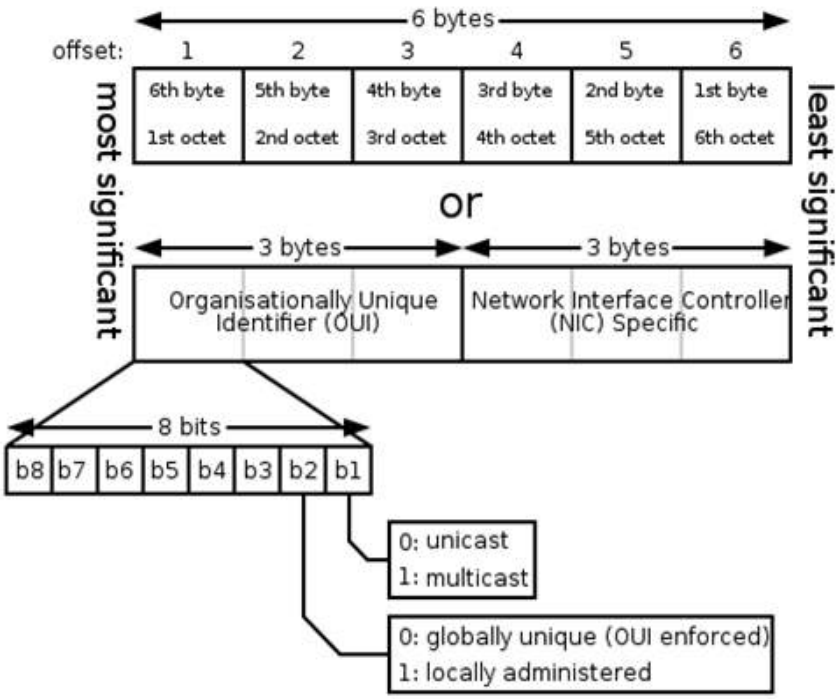
1. 기술 개요

MAC(Media Access Control) Address는 네트워크 인터페이스에 할당된 고유의 식별 주소로 OSI 모델의 Media Access Control Protocol에서 사용된다. MAC Address는 네트워크 인터페이스 카드(Network Interface Card, NIC)의 제조사에 의하여 결정되며, 하드웨어에 저보가 담기는 읽기 전용의 메모리이다. 따라서 MAC Address는 고유의 식별 주소를 부여 받음에 따라, MAC Address를 통한 인증이 가능하다.

MAC Address 기반 인증 방식은 주로 인트라넷 환경에서 네트워크 접근제어를 위하여 사용된다. MAC Address 인증 방식은 네트워크에 연결된 적합한 단말의 MAC 주소를 인증서버에 등록하여, 단말의 네트워크 접속 요청 시 이 단말의 MAC Address가 서버에 등록되어 있을 경우 연결을 승인하는 방식이다. 따라서 기기의 MAC Address를 사전에 서버에 등록해야 하며, 서버는 기기들의 MAC Address 테이블을 관리해야 한다.

2. 기술 동향

MAC Address 관련 표준화는 IEEE(Institute of Electrical and Electronics Engineers)에서 진행되고 있다. IEEE는 MAC-48을 통하여 MAC Address 할당 표준을 제정하였다. MAC-48은 각 NIC별로 01-23-45-67-89-ab와 같이 2자리의 16진수씩으로 구성된 6 블록을 통하여 MAC Address를 표기하도록 규정하였다. 최근 기기들의 증가 및 사물통신, 미래인터넷 등 사물이 인터넷에 연결될 것으로 예측됨에 따라 IPv6와 더불어 MAC-48로 MAC address를 모두 할당하기에 부족할 것으로 예측되며, 새로운 MAC address 양식을 규정해야 할 필요성이 제기되었다.



(그림 24) MAC 주소의 구성

출처: Wikipedia, MAC address

이에 따라서 최근 EUI(Extended Unique Identifier)를 새로 규정하고 EUI-48, EUI-64를 통하여 MAC address의 새로운 표준을 규정하는 것이 최근 동향이다.

3. 사물통신 환경에서의 MAC Address 기반 인증 기술

MAC Address 기반 인증 기술은 앞서 살펴본 ID/PW 인증 기술보다 비교적 간단하고 속도도 빠르다는 장점이 있다. 하지만 MAC Address 인증 방식의 인증 원리인 MAC Address가 기기 고유의 식별번호라는 특성은 최근 MAC Address를 위조가 가능함에 따라 사실상 MAC Address 기반 인증은 취약하다고 판단되는 상태이다. 또한 MAC Address 기반 인증은 서버가 MAC Address 테이블을 관리해야 함에 따라 기기를 추가하거나 수정이 있을 경우 관리상에 어려움이 있

다. 따라서 보안이 요구되며, 사람의 개입이 배재되거나 최소화된 사물 통신 환경에서 MAC Address 기반 인증 기술은 부적절하다고 판단할 수 있다.

제 4 절 암호 프로토콜 기반 인증기술

1. 기술 개요

암호 프로토콜 기반 인증기술은 공개키 기반 암호 혹은 대칭키 암호를 기반으로 개체를 인증하는 프로토콜을 의미한다. 암호 프로토콜은 주로 무선인터넷 보안 프로토콜에서 사용되고 있다. 무선인터넷의 보안 위협에 따라 IEEE와 와이파이협회(Wi-Fi Alliance)는 무선 인터넷 환경의 사용자 인증과 통신 암호화 기술을 정의한 표준 기술규격을 제정하여 이를 준수하도록 권고하고 있다.

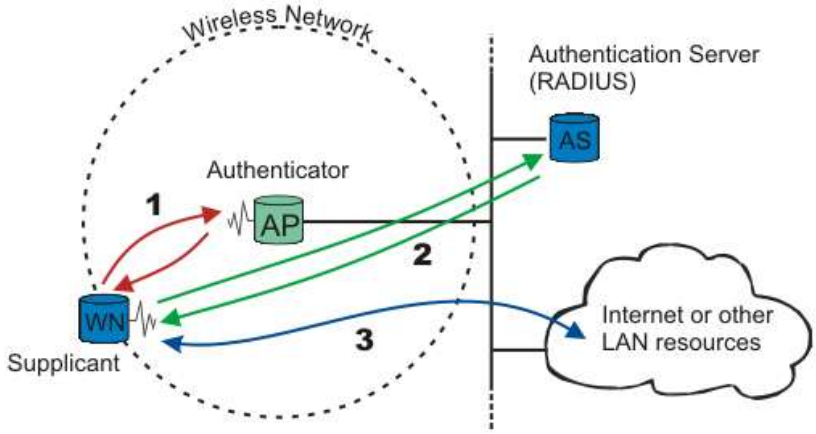
현재 모든 무선랜 솔루션은 이들이 제정한 802.1x/802.11i, WPA 표준을 지원하고 있다. 이들 표준에서 정의한 다양한 인증/암호화 기술 중에서 가장 보안성이 뛰어난 방식은 IEEE 802.1x EAP(Extensible Authentication Protocol) 사용자 인증과 WPA 버전2에 정의돼 있는 AES(Advanced Encryption Standard) 암호화 알고리즘을 이용한 CCMP(Counter mode with CBC-MAC Protocol) 기술로 알려져 있다. 이를 통해 사용자가 기업에 설치된 AP(Access Point)를 통해 사내망과 정보자산에 불법적으로 접근하거나 중간에서 키나 세션을 훔쳐 정보를 가로채려는 시도까지도 차단할 수 있다.

2. 기술 동향

가. 802.1x

802.1x의 인증 과정은 다음과 같은 일련의 과정을 통하여 이루어진다. 무선네트워크(Wireless Network, 이하 WN)이 접근하면 AP가 WN의 아이디를 요청한다. WN이 인증되기 전에는 EAP만이 가능하다. 본래 EAP는 PPP에서 사용되던 인증 기술이다. PPP에서는 아이디 패스워드를 검사하기 위해 PAP나 CHAP 인증이 사용되었다. 아이디가 전송된 뒤 인증 과정이 시작된다. WN과 AP 사이에 사

용되는 프로토콜은 EAPOL (EAP encapsulation Over Lan)다. AP는 EAP 메시지를 다시 RADIUS 방식으로 재암호화한 뒤에 인증서버(Authentication Server, AS)로 전송한다. 인증하는 동안에 AP는 단순히 WN과 AS 사이에 패킷을 전달하는 역할을 할 뿐이다. 인증이 끝나면 AS가 성공 메시지 혹은 실패 메시지를 AP에게 전송한다. 그러면 비로소 AP는 WN의 포트 접속을 허가한다.



(그림 25) 802.1x의 인증 방식 예

출처: IEEE, 802.1X-2001

802.1x에는 PAP(Password Authentication Protocol), CHAP(Challenge Handshake AP), RADIUS(Remote Authentication Dial-In User Service) - RFC2865, 그리고 WEP(Wired Equivalent Privacy) 등이 사용되고 있다.

나. 802.11i

무선랜 사용자 인증 및 암호화 국제표준은 IEEE 802.11b의 WEP, 802.11i의 WPA가 대표적이다. 1990년대 말에 지속적으로 표준화가 완성된 802.11a, b, 그리고 2003년에 802.11b의 확장 개념으로 만들어진 802.11g에 포함돼 있는 WEP 기술

은 RC4 알고리즘 기반으로 생성된 키를 간단한 처리만으로 데이터를 암호화하는 과정만 거치도록 돼 있다. 이러한 이유 때문에 충분한 전송 데이터 확보만 가능하다면 누구나 쉽게 크래킹이 가능한 보안취약점을 갖고 있다. 이러한 문제 해결을 위해 2004년에 보다 강력한 보안 방안을 담은 IEEE 802.11i를 완성했다. 하지만 당시 50% 이상의 비중을 차지하던 802.11b 장비들이 새 기술 표준을 수용하기에는 하드웨어적으로 한계가 있었다. 업계 표준화를 주도하는 Wi-Fi 협회는 802.11i 표준이 완료되기 전에 802.11b 장비와 호환이 가능한 수준의 802.11i 기술을 발췌, 2003년 2월 IEEE 802.11i Draft 3.0을 기반으로 WPA 버전1(WPA)을 해결책으로 내놓았다. 그 이후 2004년 7월 IEEE 802.11i가 완성되면서 해당 표준을 WPA2로 업그레이드했다. WPA와의 차이점은 암호 방식으로 CCMP가 추가된 것이다.

802.11x 표준에서는 공유키(Shared Key)나 PSK(Pre-Shared Keys), 802.1x EAP (Extensible Authentication Protocol) 인증과 WEP, TKIP (Temporal Key Integrity Protocol), CCMP (Counter mode with CBC-MAC Protocol) 방식의 암호화 기술을 사용한다. 가장 최신 규격인 802.11i 무선랜 보안표준에서는 Wi-Fi 협회에서 내놓은 강력한 사용자 인증, 암호화 규격인 WPA를 준수토록 하고 있다. 이러한 이유 때문에 모토로라, 시스코시스템즈, 쓰리콤, 아루바네트웍스, 콜루브리스네트웍스, 트라페즈 등이 공급하는 무선랜 솔루션에서는 WPA의 PSK, 802.1x EAP, TKIP, 암호화 알고리즘인 AES 기반의 CCMP를 지원하고 있다. 802.11i의 새 표준안은 TKIP(Temporal Key Integrity Protocol), CCMP(Counter Mode with CBC-MAC Protocol), 802.1x Port-Based Network Access Control 등으로 분류할 수 있다.

다. WPA(Wi-Fi Protected Access)

산업계가 802.11i가 완료될 때까지 기다릴 수가 없자, Wi-Fi 협회는 중간 과정의 결과를 토대로 WPA를 발표한다. 기존의 802.11 장비가 WPA에 쓰일 수 있도록 해야 했기 때문에, 기본적으로 WPA는 TKIP+802.1x 방식을 사용한다. WEP에

비해 정교한 데이터 암호화를 제공하는 것은 물론, 사용자 인증이 다소 불충분했던 WEP과는 달리 완전한 사용자 인증 기능을 제공한다. WPA는 WEP처럼 복잡하지 않은 가정용으로는 아직도 유용하지만 대량의 메시지 흐름으로 인해 암호화 키가 보다 신속하게 발견될 수 있는 기업용에는 충분치 않은 것으로 여겨진다. WPA는 802.1x와 확장 인증 프로토콜인 EAP (Extensible Authentication Protocol)을 도입해 강력한 사용자 인증을 제공한다. WPA는 각 사용자를 인증할 때 RADIUS와 같은 중앙 인증 서버를 사용한다.

3. 사물통신 환경에서의 암호 프로토콜 기반 인증 기술

암호 프로토콜 기반 인증기술은 사용하는 암호 프로토콜에 따라 아이디/패스워드 인증 기술, MAC 주소 인증 기술 그리고 인증서 기반 기기 인증서 인증 기술을 포함할 수 있다. 암호 프로토콜 기반 인증기술은 다양한 인증 방식이 존재하여 각 사용 환경에 따라 적합한 인증 방식을 선택할 수 있으며 IEEE와 Wi-Fi Alliance를 통하여 인증 기술이 표준으로써 규정됨에 따라 공식적으로 안전성을 보장받을 수 있다는 장점이 있다. 또한 인증 기술의 기반 암호 프로토콜에 따라 부인방지 기능을 제공할 수도 있다.

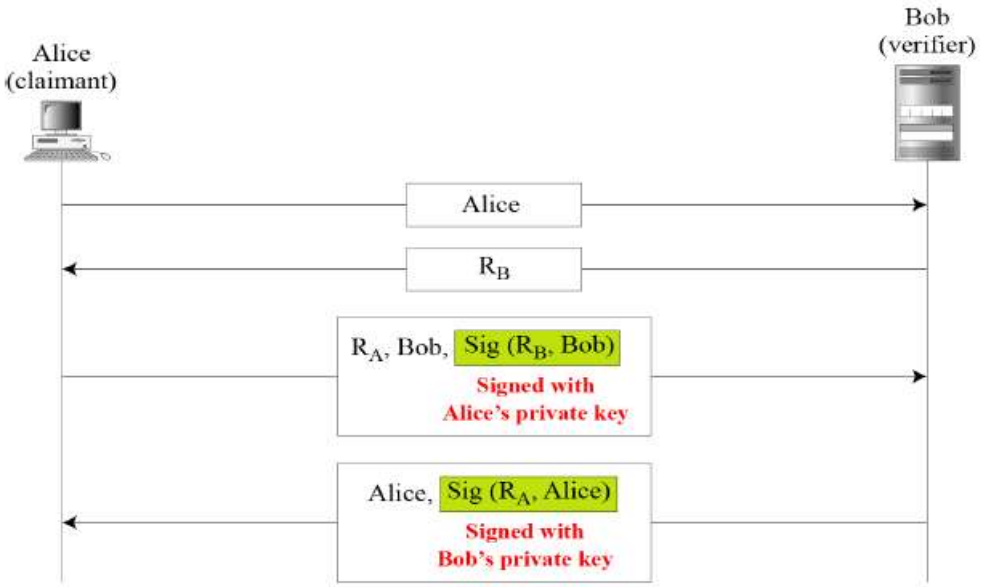
하지만 암호 프로코콜 기반 인증기술은 안전성을 기반 암호 기술에 의존하여 이 암호 기술의 취약점이 발견될 경우 이는 곧 인증기술의 취약점이 된다. WEP의 경우, 암호 알고리즘으로 RC4를 선택하였는데, RC4는 이미 1995년 깨진 암호 알고리즘으로, 정적 키 사용시 IV 헤더를 모아서 분석하면 WEP 키가 노출되는 문제가 발생하였다. 사물통신 환경에서 암호 프로토콜 기반 인증기술은 기기의 제약으로 인하여 비교적 간단한 암호 기술 기반 인증기술을 사용해야 할 것으로 예상되며, 이러한 인증기술은 도입 당시에는 안전할 수 있지만 미래에는 연산 처리 능력의 발전으로 공격이 가능할 수도 있다.

제 5 절 인증서 기반의 인증

1. 기술 개요

인증서 기반 인증기술은 공개키 기반의 암호기술을 이용하는 전자서명(Digital Signature)을 통하여 인증하는 방식의 인증기술로, 인증서에 전자서명을 위한 정보를 수록하여 이를 기반으로 인증하는 기술을 의미한다. 공개키 기반의 암호기술은 한 주체가 본인만이 알 수 있는 비밀키(Private Key)를 생성하고, 이에 대응하는 공개키(Public Key)를 생성하여 이를 공개하는 과정을 통하여 암호화 통신을 한다. 즉, 한 주체(B)가 다른 주체(A)에게 그 주체만이 알 수 있도록 암호화하여 메시지를 보내야 할 경우 이 주체(A)가 공개한 공개키를 통하여 암호화하여 전송한다. 이 주체(B)로부터 암호화된 메시지를 전달받은 주체(A)는 자신이 보유한 비밀키를 통하여 원 메시지를 복호화할 수 있다.

전자서명을 통한 인증 방식은 이 공개키 암호시스템을 이용하여 인증하는 방식이다. 즉 인증 받고자 하는 주체인 청구인(Claimant) 검증자(Verifier)에게 인증을 위한 메시지를 요청한다. 검증자는 검증메시지(Challenge Message)를 청구인에게 전송한다. 이를 수신한 청구인은 이를 자신만의 비밀키로 암호화하는 전자서명 과정을 통하여 검증 메시지를 암호화하여 다시 검증자에게 전송한다. 이 암호화된 메시지를 수신한 검증자는 사전에 청구인이 공개한 공개키로 이 메시지를 복호화하여 자신이 최초에 전송한 검증메시지와 일치하는 지 여부를 확인한다. 이 메시지가 서로 일치할 경우 검증자는 이 청구인이 적합한 청구인임을 검증할 수 있다. 이 방식이 '전자 서명'이라고 불리는 이유는 일반적인 서명과 동일한 검증을 할 수 있기 때문이다. 즉 청구인은 청구인 자신만이 유일하게 할 수 있는 서명을 하고, 이 서명은 누구나 검증할 수 있으므로 일반적인 서명과 동일한 검증 기능을 제공한다.

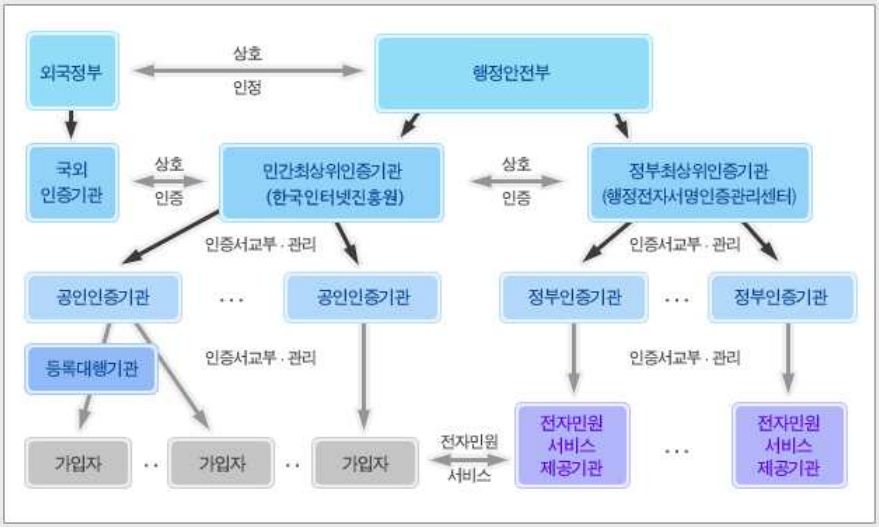


(그림 26) 전자서명을 통한 인증방식

출처: Forouzan, Cryptography and Network Security, 2007

인증서에는 전자서명을 위한 일련번호, 주체, 서명 알고리즘, 발행자, 유효기간, 공인키, 지문, 지문 생성 알고리즘 등의 정보가 포함되어 전자서명 시 인증서를 통하여 전자서명이 이루어진다.

우리나라는 1999년 전자서명법을 제정하였으며, 민간에서 사용하는 공인인증서 발급 체계 및 관리와 관련된 규정을 마련하였다. 이 체계는 최상위 인증기관인 Root CA(Certificate Authority) 하에 공인인증기관을 두고 이 기관들을 통하여 공인인증서를 발급하는 체계이다. 전자서명법 제25조에 근거하여 한국인터넷진흥원(Korea Internet & Security Agency, KISA)을 최상위 인증기관으로 지정하고, 한국정보인증(주), (주)코스콤, 금융결제원, 한국전자인증(주), 한국무역정보통신, 한국정보사회진흥원을 전자서명법 제4조의 규정에 근거한 공인인증기관으로 지정하였다. 한국정보사회진흥원은 2008년 6월 한국정보인증(주)로 이관되어 현재 5개의 공인인증기관을 통하여 인증서의 발급 및 인증이 이루어지고 있다.



(그림 27) 국내 전자서명 체계

출처: 한국인터넷진흥원 전자서명인증관리센터

전자정부 환경에서 행정관련 전자문서 송·수신 등에 있어 기관 및 공무원 신원 확인, 그리고 문서의 위·변조 등을 방지하기 위하여 행정전자서명(Government Public Key Infrastructure, GPKI)이 운영되고 있다. 전자정부법 제29조 및 전자정부법 시행령 제11조에서 제17조에 의거하여 발급 및 운영이 되고 있다. 행정안전부 산하 행정전자서명 인증관리센터가 최상위 인증기관으로 이 센터를 통하여 인증기관인 교육과학기술부, 국방부, 대검찰청, 병무청, 대법원(법원 행정처)을 통하여 행정전자서명이 발급되고 있다.

사물통신 환경에서의 인증서 기반 인증기술은 현재 국내에서 운영되고 있는 개인용 NPKI(National Public Key Infrastructure), 행정전자서명 GPKI(Government Public Key Infrastructure)와 같이 PKI(Public Key Infrastructure) 기반의 기기인증서를 통하여 인증하는 기술이다. 인증서의 대상이 개인 혹은 법인이 아닌 사물이라는 차이가 있으며, 인증서 발급 구조, 유효기간 등에서 다음 표와 같은 차이가 존재한다.

[표 2] 공인인증서와 기기인증서 비교

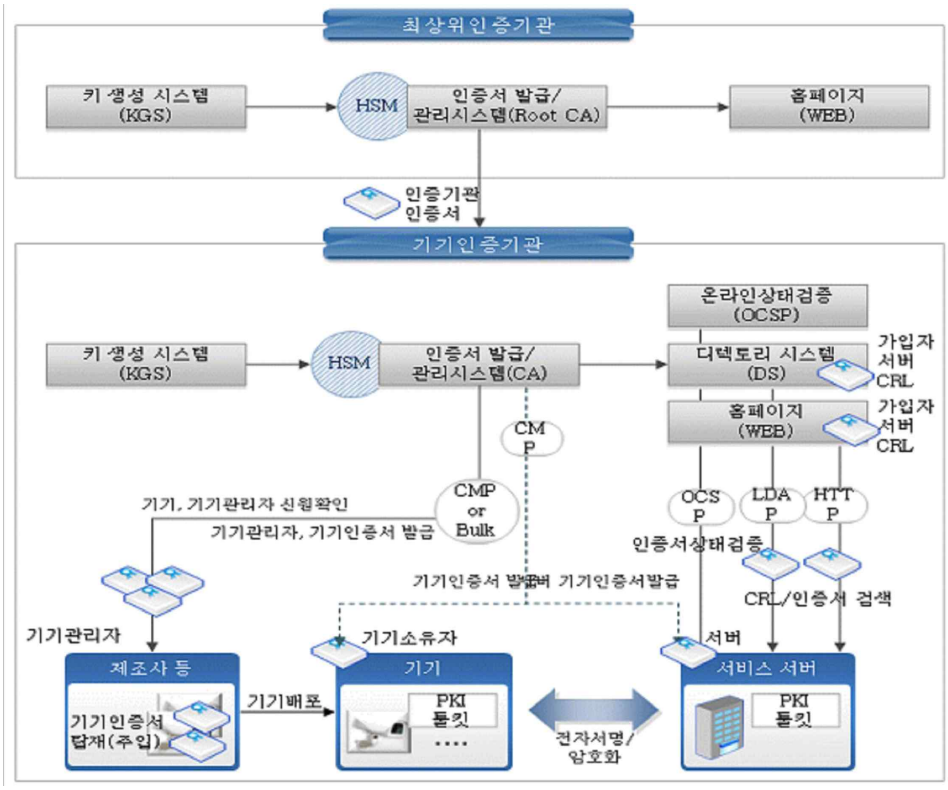
구분	공인인증서	기기인증서
서비스 대상	자연인, 법인	네트워크에 접속되는 모든 기기
서비스 내용	인터넷뱅킹 등 전자거래 시 본인확인	특정 서비스(인터넷 전화망, 케이블 TV망 등)에 접근권한 확인
인증서 사용목적	본인확인, 전자문서 무결성 등	기기식별, 암/복호화 등
이해 당사자	공인인증기관, 전자거래 서비스 업체, 가입자	기기인증기관, 네트워크 서비스 운영자, 기기 제조업체, 기기
신원확인 절차	직접대면을 통한 확인	기기 제조업체 등을 통한 기기 진위성 확인
인증서 구성	성명 등 개인정보 포함	제조업체명, 기기 식별정보(시리얼 번호, MAC Address) 등
인증서 발급	게별적으로 개인에게 발급	수천~수만 장 단위로 벌크(Bulk)로 선발급
인증서 저장	PC. USB 등에 저장	기기 제조과정 중 해당 기기에 탑재
인증서 관리	갱신, 재발급 빈번히 발생	갱신 재발급 없이 기기의 사용연한과 동일(유효기간 ↑)

출처: 강필용, 기기인증체계 현황 및 전망, 한국정보보호학회 Green-IT 융합 보안 워크샵 발표자료

현재 한국인터넷진흥원은 '기기인증관리체계를 위한 최상위인증기관 인증업무 준칙'을 제정하고 기기에 대한 인증서 정책, 인증서 발급·관리 등 기기인증관리체계 운영 등에 있어 필요한 사항을 규정하고 있다.[40] 동 준칙에서 한국인터넷진흥원은 기기인증서를 기기의 진위여부를 식별하고 기기에서 송수신되는 정보를 안전하게 전달하기 위해 공인인증기관이 발급하는 전자적 정보로 규정하고 있다. 또한 기기인증서 발급 및 운영업무를 하는 각 공인인증기관의 인증(공인인증기관 공

40) 한국인터넷진흥원, 기기인증관리체계를 위한 최상위인증기관 인증업무 준칙, 2009

인인증서) 업무에 대하여 규정하고 있다. 한국인터넷진흥원은 기기인증서의 발급 체계를 다음 도식도와 같이 예상하고 있다.



(그림 28) 기기인증 시범발급체계 예상 도식도

출처: 강필용, 기기인증체계 현황 및 전망, 한국정보보호학회 Green-IT 융합 보안 워크샵 발표자료

2. 기술 동향

인증서 기반의 사물통신 인증기술은 현재 방송, 통신, 산업/안전 분야 등에서 사용이 되고 있다. 현재 외국의 경우 VeriSign 社의 기기 인증 서비스(Device Certificate Services)를 통한 개인 디바이스 인증과 케이블모뎀 디바이스 인증, 그리고 WiMAX 산업 인증서 등을 제공하고 있다.[41] 국내의 경우 현재 충남 연기군 등의 u-City에서 네트워크카메라의 방법 서비스 등에서 시범 운영되고 있다.

가. 케이블모뎀 인증

VeriSign의 케이블모뎀 디바이스 인증은 기기인증의 대표적인 사례로 꼽히는 서비스이다. 케이블모뎀은 케이블 TV망을 이용하여 인터넷 접속 시 사용되는 장치로, 인터넷 서비스 제공자(Internet Service Provider)는 케이블모뎀을 통한 인터넷 사용 제공 시 케이블모뎀이 적합한 기기인지 인증이 필요하며, 통신 내용의 암호화가 필요하다. 이를 위하여 미국의 CableLbas와 유럽의 Excentis의 케이블 모뎀의 표준 인터페이스인 DOCSIS(Data Over Cable Service Interface Specification) 및 EURO-DOCSIS를 제정하였다. Verisign은 이 DOCSIS에서 인증서 발급 및 인증 업무 등을 담당하고 있다. VeriSign의 케이블모뎀 인증 발급 및 관리는 다음의 일련의 과정을 통하여 진행된다.[42]

① 제조사는 구매하고자 하는 인증서의 수 만큼 주문서를 발급한다. CableLab은 사전 구매송장을 제조사에 송부한다.

② 지불이 될 경우, CableLab은 VeriSign으로 하여금 구매한 수만큼 인증서를 발급하도록 인가한다.

③ 관리자는 인증기관(Certification Agency)의 웹페이지에 인증을 받는다. 이 인증을 위한 통신 시 관리자는 토큰의 키를 이용하여 암호화 및 인증이 적용된다. 관리자는 제조사가 구매한 수량의 인증서 인증기관에게 요청한다.

④ 인증기관은 CableLab이 제조사에게 인증해준 요청에 대하여 확인을 한다. 이 요청이 적합할 경우 인증기관은 인증서를 발급한다.

⑤ 요청이 완료될 경우, 인증기관은 관리자에게 Email을 통해 요청이 완료되었음을 통지한다. 인증서 파일은 제조사에게 다음의 메커니즘을 통하여 전달된다.

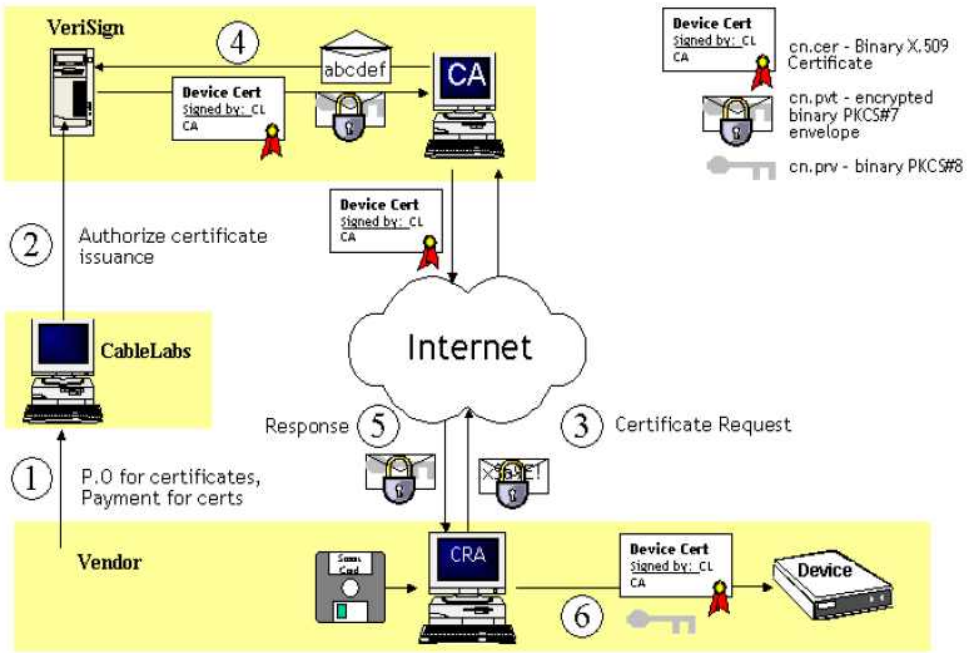
   a. 요청된 인증서는 접근이 제어되는 특정 웹사이트에 올라온다. 이 웹사이트의 접속은 클라이언트-서버 방식으로 적합한 제조사의 관리자만이

41) Verisign, Device Certificate Services
42) CableLabs, CableLabs Certificate Issuance Process, 2006

접속할 수 있도록 보호되는 URL로, 관리자는 이 URL을 통하여 인증서를 발급받는다.

b. 혹은 인증기관은 인증서를 암호화하여 CD-Rom을 통하여 제조사의 관리자에게 송부한다.

⑥ 제조사가 인증기관에게 공개키와 비밀키 키 쌍(Key Pair)을 요청했다면, 인증기관은 PKCS#7 엔벨롭(Envelop)을 통하여 이를 송부한다. 제조사는 제조사 토큰의 키를 이용하여 이 인증서를 복호화하여, 인증서를 케이블모뎀에 탑재한다.



(그림 29) 케이블모뎀의 기기인증서 발급 과정 도식도

출처: CableLabs, CableLabs Certificate Issuance Process, 2006

나. 케이블 셋톱박스

셋톱박스(Set-top Box)는 텔레비전에 연결되어 외부에서 들어오는 신호를 수신하여 변환한 후 텔레비전으로 이 신호를 디스플레이해주는 장치를 의미한다. 셋톱박스는 주로 케이블티비나 위성방송 등에서 사용되고 있다. 방송사업자는 자사의 서비스를 신청한 적합한 사용자만이 이 신호를 수신하여 영상을 시청할 수 있도록 각 셋톱박스가 정당한 기기인지 인증이 필요하다. 현재 이 과정은 셋톱박스와 이와 플러그인 되는 케이블카드(Cable Card) 간의 인증을 통하여 이루어지고 있다.

(그림 30) 케이블 셋톱박스에서 인증서 기반 인증

출처: 강필용, 기기인증체계 현황 및 전망, 한국정보보호학회 Green-IT 융합 보안 워크샵 발표자료

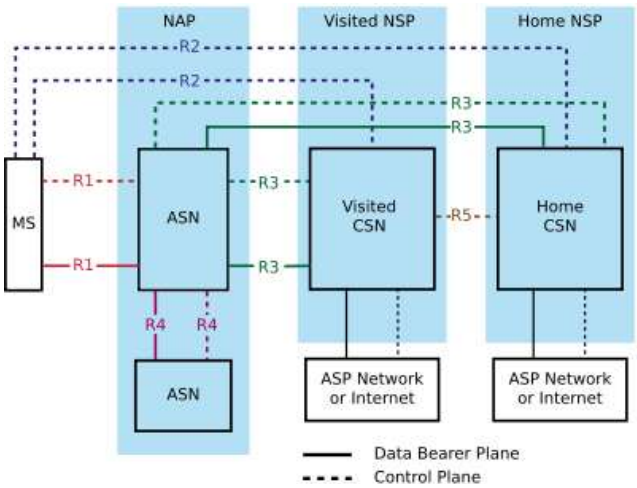
이와 같은 케이블카드를 통한 인증방식은 오픈케이블(OpenCable)에서 제시한 표준방식으로, PKI 인증서를 통하여 셋톱박스와 케이블카드간 인증을 규정하고 있다. 현재 국내에서는 한국디지털케이블연구원(Korea Digital Cable Laboratories, KLabs)이 최상위 인증기관으로서 미국 CableLab 과의 업무협력을 통해 기기인증서를 발급하고 있다.[43] 국내의 경우 독자적인 국내 케이블 인증의 필요성에 따라 2004년부터 케이블 기기 인증서 발급시스템을 구축하였다. 현재 기기인증서는 인증기관인 한국정보인증을 통하여 발급이 되고 있으며, 2010년 3월 현재 600만 건에 달하는 기기인증서가 발급된 것으로 집계되었다.[44]

43) 한국인터넷진흥원, 유비쿼터스 환경에 적합한 인증체계 구축을 위한 법제도 연구, 2008
44) 디지털데일리, 한국정보인증, 정부중앙청사 인터넷전화 기기인증 시작, 2010년 3월 11일자 기사

다. WiMAX

WiMAX(Worldwide Interoperability for Microwave Access)는 모바일 인터넷 접속을 가능하게 하는 통신 프로토콜로, IEEE 802.16 표준에 기반하고 있다. 현재 최고 40Mbit/s의 속도를 제공하고 있으며, 정지시 1Gbit/s까지 발전될 것으로 예상하고 있다. WiMAX는 이름에서 알 수 있듯이 IEEE 802.16의 상호운용성을 적용한 기술이다. 상호운용성을 위하여 WiMAX Forum의 인증서는 모든 공급자로 하여금 WiMAX 제품의 판매를 허용함에 따라, 같은 규격에 맞는 인증 제품과의 상호운용성에 대한 검증의 확인이 가능하다.[45]

WiMAX 환경에서는 CSN(Connectivity Service Network)의 AAA(Authentication , Authorization and Accounting Server)에서 인증서 기반 인증기술이 사용된다. 단말기(Subscriber Station, SS 혹은 Mobile Station, MS)가 WiMAX의 접속스테이션에 접속할 때, 단말기와 AAA 서버는 인증서 기반의 인증 기술을 통하여 접속을 요청한 사용자가 적합한 사용자임을 인증한다.



(그림 31) WiMAX 구조도

출처: Wikipedia, WiMAX

45) Wikipedia, WiMAX

라. 기타 환경

현재 VoIP(Voice over Internet Protocol)과 CCTV(Closed Circuit TV) 혹은 네트워크 감시카메라 등에 있어 기기의 인증을 위하여 인증서 기반 인증기술이 사용되고 있다. VoIP의 경우 인터넷전화 서비스를 위하여 개체 간 상호 통신 시 음성트래픽의 수집, 위·변조 방지를 위하여 VoIP단말과 PBX(Private Branch Exchange)에 인증서 기반 인증기술이 적용되고 있다. IP-PBX간 통신 시 VoIP 단말과 PBX는 인증서를 통하여 상대방이 적합한 사용자인지를 검증하고, 암호화 통신을 제공한다. CCTV 및 네트워크 감시카메라 환경에서는 IEEE 802.1x 기반의 RADIUS 프로코콜 기반 인증서 기반 인증기술이 사용된다. CCTV의 카메라는 인증서를 통해 전송하는 화상 정보에 대하여 전자서명을 생성·전송하여 적법한 개체임을 인증하고, 전송한 화상의 위·변조 여부에 대하여 원본임을 인증한다.[46]

3. 사물통신 환경에서의 인증서 기반 인증 기술

인증서 기반 인증기술은 강력한 인증 기능을 제공하여 높은 안전성을 제공한다. 또한 인증서 기반 인증 기술에서 사용되는 전자서명은 본인만이 서명이 가능하기 때문에 부인방지 기능을 제공한다. 이는 과금 및 책임소재 등에 있어 중요한 기능을 제공한다.

반면, 인증서 기반 인증기술은 반드시 사전에 키 교환이 필요하다는 단점이 있다. 또한 구현에 있어 인증서의 발급·갱신·폐기 등 인증서의 관리가 필요하다. 기기인증서의 경우 인증서 유효기간을 30년으로 늘려 이러한 불편을 최소화하고자 하는 노력이 있지만, 기본적으로 제품의 생산 시 기기인증서를 탑재하여야 하며, 폐기리스트(Certification Revocation List, CRL)를 관리해야 하는 등 여전히 관리상의 불편함이 있다. 또한 인증서의 경우 각 인증기관과의 인증 업무가 호환되지

46) 한국인터넷진흥원, 유비쿼터스 환경에 적합한 인증체계 구축을 위한 법제도 연구, 2008

않을 경우, 다른 국가 등 다른 도메인에서 사용 시 호환성의 문제가 있다. 인증서 기반 인증기술에서 사용되는 서명 알고리즘 등 기기인증서 처리 S/W 및 알고리즘은 연산 처리량이 많고 무거워 기기에 적용하기 어려운 문제점은 기기인증서의 가장 큰 단점이다.

사물통신 환경에서 인증서 기반 인증기술은 강력한 인증 및 부인방지를 제공함에 따라 높은 보안수준을 요구하는 분야에서 역시 사용이 가능하다. 또한 부인방지 기능이 요구되는 과금이 필요한 환경에서 역시 사용이 가능하다는 장점이 있다. 하지만 인증서 기반 인증기술은 높은 연산량을 요하는 단점이 있다. 사물통신 환경은 기기들의 특성상 저전력 적은 저장공간 등의 환경에서 적합한 인증기술이 필요하다. 따라서 사물통신 환경에서 인증서 기반 인증기술을 적용할 경우 사물통신 환경에 적합한 기기 인증서의 개발이 선행되어야 할 것이다. 또한 인증서 기반 인증기술은 ID/PW, MAC Address, 암호 프로토콜 기반 인증기술 들과 달리 특정 처리 소프트웨어, 발급 및 인증 체계 등이 필요하다. 사물통신 환경에서 인증서 기반 인증기술은 기기의 고장, 변경, 수리 등에 따라 잦은 변화와, 기기에서 인증서를 추출하여 위장(Masquerade)하는 공격 등을 방지하기 위한 인증서의 관리가 필요하다.

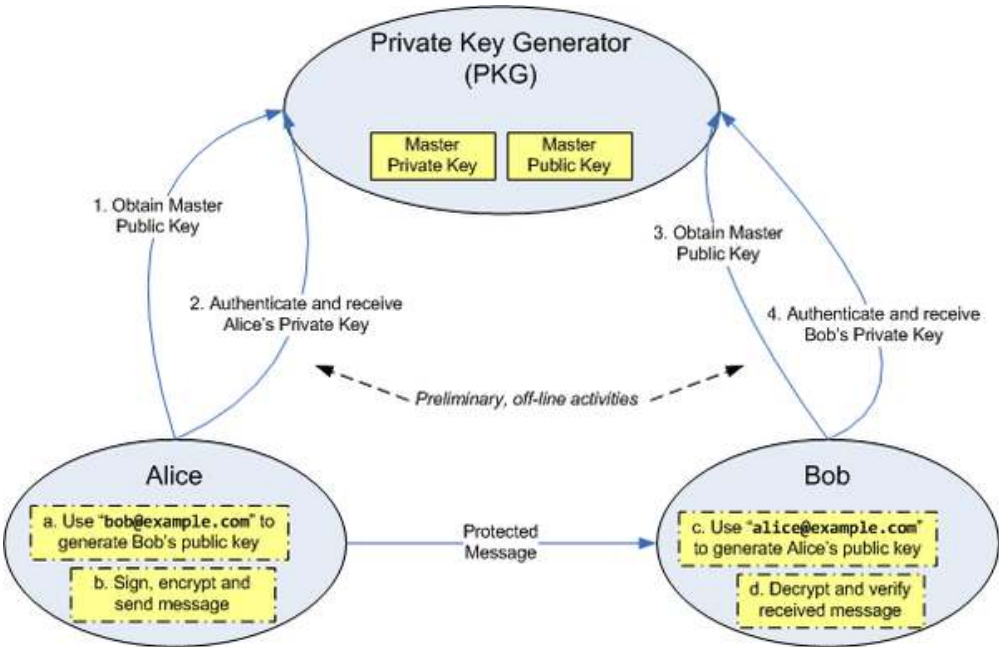
사물통신은 인간의 개입이 최소화된 상태에서 인증이 이루어져야 하기 때문에, 서로 다른 환경·서로 다른 인증기술·서로 다른 도메인 간 호환이 어려운 문제 역시 해결해야할 것이다. 이와 같은 발급체계, 인증체계 들로 인하여 인증서 기반 인증기술은 다른 인증기술에 비하여 많은 비용이 요구됨에 따라, 인증서 기반 인증기술은 일반적인 사물통신 환경보다는 높은 보안성을 요구하는 환경에서 사용할 것으로 예상할 수 있다.

제 6 절 ID-Based Encryption(IBE)을 이용한 인증

1. 기술개요

아이디 기반 인증기술(ID-based Authentication)은 ID 기반 암호기술(ID-Based Encryption, IBE)을 이용하여 서명·인증 할 수 있는 인증기술이다. 아이디 기반 암호기술은 사용자의 이메일 주소, 이름, IP주소 등 사용자의 ID를 공개키로 사용하는 방식의 공개키 암호 시스템이다. 아이디 기반 암호기술은 1984년 Adi Shamir가 제안한 암호 기술로 이메일 주소를 기반으로 PKI가 최초의 아이디 기반 암호기술의 응용이었으나 ID 기반 서명의 예시를 제시했을 뿐이었다. 이후 Boneh/Franklin의 Paring-based Encryption Scheme을 통하여 ID 기반 암호 및 인증 기술이 제시되었으며 이후 Cocks가 Quadratic Residue를 이용한 Scheme을 제시하였다.

아이디 기반 암호기술은 다음과 같은 일련의 과정을 통하여 비밀키와 공개키를 생성하고, 이 키들을 이용하여 암호화 및 복호화하는 방식의 암호기술이다. 암호 통신을 하고자 하는 두 주체는 신뢰받는 제3자(Trusted Third Party)인 PKG(Public Key Generator)에게 통신을 위한 키 생성을 요청한다. PKG는 인증을 요청하는 주체의 E-mail 주소, ID 등의 정보를 이용하여 이에 부합하는 공개키와 비밀키를 생성하며, 두 주체는 이 공개키와 비밀키를 이용하여 암호화 통신이 가능하다. 이를 위하여 PKG는 우선 마스터 공개키를 공개하며, 이에 부합하는 마스터 비밀키를 보유한다. 주어진 마스터 공개키를 통하여 사용자는 ID와 마스터 공개키를 결합하여 ID 공개키를 만들 수 있다. PKG는 마스터 비밀키를 이용하여 이 ID 공개키에 부합하는 비밀키를 사용자에게 생성하는 방식이다.



(그림 32) ID-based Encryption의 Scheme

출처: Wikipedia, ID-based Encryption

아이디 기반 인증기술에서 각 키 생성 등을 위하여 Weil Pairing 혹은 Tate Pairing과 같은 타원 곡선 기반의 알고리즘인 Elliptic Curve Cryptosystem을 이용한다. Elliptic Curve는 타원 곡선을 나타내는 수식을 통하여 가산법에 의거하여 암호화 및 복호화하는 암호시스템이다. Elliptic Curve Cryptosystem은 기존 PKI 등에서 사용되는 공개키 기반 알고리즘인 RSA 알고리즘 등의 대표적 단점인 큰 키 길이를 해결하는 알고리즘이다. 현재 안전하다고 알려진 2^{80} 수준의 안전성을 위하여 RSA는 1024비트의 키 길이를 필요로 한다. 반면 Elliptic Curve Cryptosystem은 이 안전성을 위하여 160비트의 키 길이 밖에 요구되지 않기 때문에 빠른 연산 및 키 저장 등 관리에 용이하다. 이는 특히 저장 및 연산 속도 등에 한계가 있는 모바일 기기 등 임베디드 시스템에 적합한 것으로 알려졌는데, 동일 수준의 보안성을 위한 연산 속도에서 Elliptic Curve Cryptosystem은 아래 표와 같은 연산 수행을 보였다.

[표 3] 동일 수준의 안전성에서 RSA와 ECC의 연산 속도 및 키 길이 비교

	ECC -160	RSA -1024	ECC -192	RSA -1536	ECC -224	RSA -2048
시간(ms)	3.69	8.75	3.87	27.47	5.12	56.18
Ops/sec	271.3	114.3	258.1	36.4	195.5	17.8
성능 비교	2.4 : 1		7.1 : 1		11 : 1	
키사이즈 비교	1 : 6.4		1 : 8		1 : 9.1	

출처: Forouzan, Cryptography and Network Security, 2007

아이디 기반 인증기술은 아이디 기반 암호기술을 이용하여 공개키인 자신의 ID 정보와 이에 대응하는 비밀키를 생성하여 서명 및 인증하는 방식의 인증기술이다. 두 주체의 IBE 기반의 인증기술을 이용하여 암호화 및 인증이 가능한 통신을 할 경우 다음의 일련의 과정을 통하여 가능하다.

① 통신을 위하여 메시지 송신자(A)는 메시지 수신자(B)에게 검증메시지를 요청하고, 수신자(B)는 송신자(A)에게 검증메시지를 송신한다.

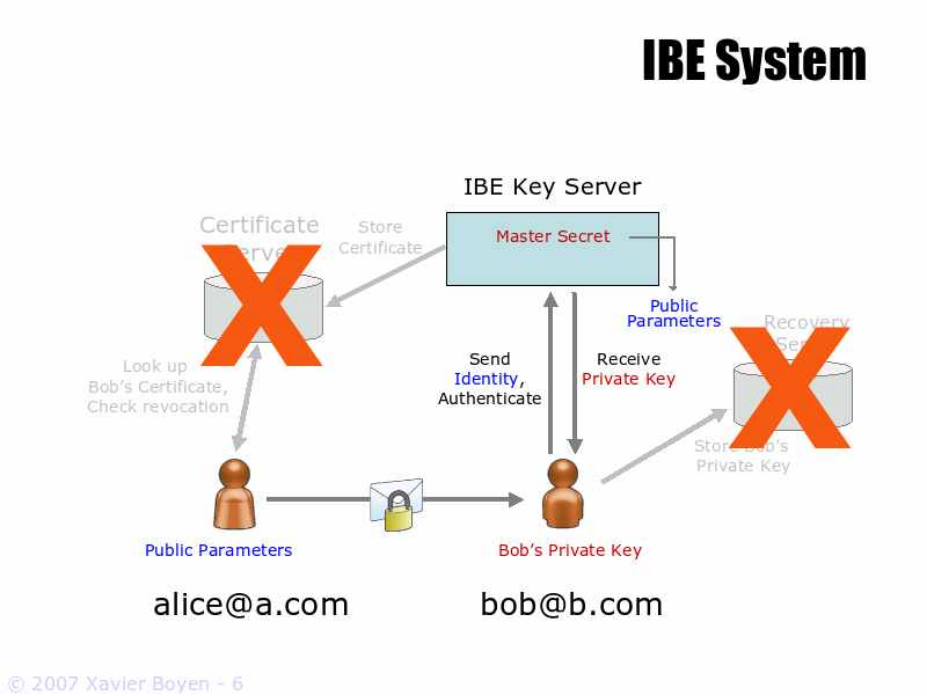
② 인증을 받고자 하는 주체인 송신자(A)는 검증메시지를 수신한 후, IBE 키 서버에 비밀키를 요청한다.

③ IBE 키 서버는 인증을 요청한 주체가 적법한 주체인지 확인하고 적법한 주체일 경우, 그 주체(A)의 ID에 해당하는 비밀키를 생성한다.

④ 자신의 비밀키를 수신한 인증 받으려는 주체(A)는 최초에 수신자(B)가 송신한 검증메시지를 이 비밀키를 이용하여 암호화 한 후 암호화 된 검증메시지를 수신자(B)에게 전송한다.

⑤ 암호화된 검증메시지를 수신한 수신자(B)는 송신자(A)의 ID를 이용하여 이 메시지를 복호화 한다. 복호화 된 메시지가 자신이 최초에 송신자(A)에게

송신한 검증메시지와 일치할 경우, 수신자(B)는 송신자가 적법한 송신자임을 확인할 수 있다.



(그림 33) IBE를 이용한 객체 인증 도식도

출처: Xavier Boyen, An Introduction to IDentity-Based Encryption, ICE-EM RNSA 2007

2. 기술 동향

아이디 기반 암호기술 및 2000년대 초반에 정립된 이론 및 기술로, 다른 인증 기술에 비하여 상대적으로 최신의 기술이다. 아이디 기반 암호기술을 이용한 인증 기술은 이에 따라 최근 Hess's Algorithm(Single Domain), Lynn's Algorithm(Signcryption Scheme, Single Domain), Gentry and Silverberg's Algorithm(Hierarchical Domain), Chow's Algorithm(Signcryption Scheme, Hierarchical Domain) 등 IBE를 이용하는 인증 Scheme이 등장하고 있다.[47]

47) Patil and Willis, Identity based authentication in SIP, 2008

현재 다음과 같은 분야에서 아이디 기반 암호기술을 이용한 인증기술이 사용되고 있거나 사용이 예상되고 있다.

가. BlackBerry의 이메일 인증기술 논의

BlackBerry는 캐나다의 통신기기 제조 업체인 RIM(Research In Motion)의 스마트폰으로, 이메일 푸쉬 등에 강점을 보이는 비즈니스 스마트폰이다. BlackBerry는 BlackBerry Enterprise Server(BES)를 통하여 암호화하여 전송되는데, 이 BES를 통하지 않으면 암호화가 되지 않아 기업 기밀 보호 등에서 문제가 발생할 수 있다. 특히 문제가 된 것은 국경을 넘는(Cross-Border) 정보의 보안 문제였다. 이러한 보안에 대한 우려로 인하여 캐나다와 미국은 공동연구 기관인 공공안전기술 프로그램(Public Safety Technical Program, PSTP)을 통하여 BlackBerry의 보안성 강화를 위한 연구를 진행하였으며, 이 프로그램에는 캐나다의 국방연구개발부(Defence Research and Development), 그리고 미국의 국토안보부(Department of Homeland Security, DHS) 등이 참여하였다.

BlacyBerry의 보안 요구사항으로 PKI를 사용하고 있는 S/MIME(Secure Multi-Purpose Internet Mail Extention)의 보안성평가, 그리고 이를 대체할 기술에 대한 연구를 진행하였다. 이 PKI기반 인증을 대체할 수 있으면서, 사용에 지장이 없고, 보안 요구사항을 충족시키면서, 사법 집행 등에 문제가 없는 기술로 아이디 기반 암호기술을 이용한 인증기술이 선정되었다. 이로 인하여 향후 블랙베리의 인증 관리 등에 있어 IBE 기반 인증기술이 사용될 것으로 예측되고 있다.[48]

나. 헬스케어 정보의 전송

미국의 경우 의료기관 간의 의료정보 전송, 의료기관과 보험회사간의 의료정보 전송시 HIPAA(Health Insurance Portability and Accountability Act)의 Security

48) Government Purchase Guide, Case Study : Security-Enhanced BlackBerry Trial, 2007

Rule과 Privacy Rule에 의하여 암호화 등의 조치가 필요하다. 현재 California의 HCS(Health Care Services), 북미 최대의 건강보험업체인 KAISER Permanente, 그리고 HealthSouth 등이 의료정보 전송시 아이디 기반 암호기술을 이용한 인증기술을 통하여 인증을 하고 있다.

3. 사물통신 환경에서의 ID-Based Encryption 기반 인증 기술

아이디 기반 인증기술은 사전 키 분배가 필요치 않으며, 연산량이 적고 키 길이가 상대적으로 짧다는 장점, 그리고 또한 부인방지 기능을 제공하는 장점이 있다. 그러나 아이디 기반 인증기술은 공개된 정보인 ID를 사용함에 따라 ID 위장한 공격에 취약점이 있다는 단점이 있다. 또한 아직까지 기타 인증기술에 비하여 상대적으로 새로운 개념과 기술로 아직까지 많은 연구가 부족한 시점이다.

사물통신 환경의 제약요건으로 인하여, IBE를 이용한 인증기술의 적은 연산량과 짧은 키길이, 사전 키 분배의 불필요 등의 특징은 사물통신 환경에서 큰 장점이 될 것으로 예상된다. 또한 IBE를 이용한 인증기술은 다른 인증기술과의 호환성이 높아, 변화하는 환경에서도 문제없이 사용될 수 있을 것으로 예상되며, 부인방지 기능을 제공하기 때문에 과금되는 환경에서 역시 사용이 가능할 것으로 예상된다.

제 7 절 소 결

1. 사물통신 환경에서 인증기술의 요구사항

사물통신 환경에서는 물리적 공격, 자격증명의 타협, 변경을 통한 공격, 프로토콜 공격, 코어네트워크에 대한 공격, 사용자 데이터 및 프라이버시에 대한 공격과 같은 취약점이 예상된다. 따라서 이와 같은 보안 위협으로부터 사물통신을 안전하게 보호하기 위하여 기술적·정책적 보안 조치가 필요하며, 인증 기술은 사물통신 환경에서 대표적인 보안 조치라고 할 수 있다.

사물통신은 공공뿐만 아니라 민간영역에서 다양한 사업자의 제품에서, 다양한 환경과 서비스에서 사용이 예상되므로, 특정 인증기술을 사용하도록 규정하거나 통일시키는 것은 문제를 초래할 수 있다. 사물통신 환경에서 인증기술은 각 사용 환경 별 요구사항을 규정하고, 이와 같은 요구사항을 충족시키는 인증기술을 선택적으로 적용하는 것이 현실적이다. 사물통신 환경에서 인증기술의 일반적인 요구사항은 디바이스 인증, 서버 인증, 통신 내용의 암호화, 부인 방지, 기타 환경과의 호환성, 인증 기술의 효율성, 사용자 개입의 최소화 등이다. 또한 예상 사용 환경에 따라 상이한 보안 위협과, 이에 대응하기 위한 인증기술이 갖추어야할 요구사항 역시 다를 것으로 예상되며 이는 다음과 같다.

[표 4] 예상 사용 환경별 인증기술의 요구사항

예상사용환경	인증기술의 요구사항
개인 맞춤형 서비스	· 유헬스케어 등 프라이버 침해의 우려가 있는 환경의 경우 인가된 사용자만이 해당 정보를 열람할 수 있는 강력한 인증 및 암호화 · 서로 다른 환경에서 서로 다른 기기들 간 인증이 가능하도록 인증기술의 호환성

스마트 안심 서비스	· 스마트 안심 서비스는 위협 상황에 대비하는 서비스이므로 언제 어디서든 인증이 가능한 가용성 · 저전력, 낮은 연산 등 사물통신의 제약에서도 사용가능한 경량화된 인증기술
차량 지능화 서비스	· 차량 지능화 서비스에서 보안 위협은 곧 인명 사고로 이어질 수 있어, 강력한 인증기술이 필요 · 고속 주행 환경을 고려하여 인증을 위한 연산 처리 시 지연이 최소화되는 인증기술 · 이동성으로 인하여 인증서버에 과부화가 생길 수 있으므로, 인증서버는 적절한 수용력이 요구됨
공공 SoC 서비스	· 주요기반시설에 대한 공격은 국가적 재앙으로 이어질 수 있음에 따라, 그 어떤 환경보다 강력한 인증기술이 요구됨 · 스마트그리드 환경에서는 물리적 접근이 용이함에 따라, 물리적 보안 위협에도 안전한 인증기술이 요구됨 · 과금 환경에서 부인 방지 기능이 요구됨

2. 각 인증기술의 비교분석

사물통신 환경에서 사용이 가능할 것으로 예상되는 인증기술은 앞에서 살펴본 바와 같이 ID/PW 기반 인증기술, MAC 주소 기반 인증기술, 암호 프로토콜 기반 인증기술, 인증서 기반 인증기술, Identity Based Encryption을 이용한 인증기술 등이다. 각 인증기술은 기술의 특성에 따라 다음과 같은 장·단점을 갖으며, 이는 다음 표와 같이 정리할 수 있다.

[표 5] 사물통신 환경에서 사용 가능한 인증 기술의 장·단점

가능한 인증기술	각 인증기술별 장 · 단점	
ID/PW 기반 인증기술	장점	- ID/PW가 사전 공유될 경우 어느 기기를 사용하여도 쉽게 인증이 허가될 수 있음
	단점	- ID/PW 접속을 위한 별도의 어플리케이션이나 프로토콜이 필요함 - ID/PW 정보가 노출되었을 경우 합법적인 기기 이외의 기기 또한 인증이 허가됨 - 부인방지 기능 제공 못함
MAC 주소 기반 인증기술	장 점	- 접속이 용이. 추가적인 어플리케이션이나 프로토콜이 필요하지 않음 - 추가적인 연산이나 지연이 요구되지 않음
	단 점	- 기기가 바뀌면 MAC 주소를 재등록해야 함 - 새로운 사용자가 추가/탈퇴될 때마다 MAC 주소를 새로이 추가/삭제해야 함. 즉 다수의 사용자를 관리하기가 어려움 - 항상 사용자 본인의 기기만을 사용하여 접속해야 함 - 등록된 MAC 주소가 유출되었을 경우 레지스트리에 의한 MAC 주소 변경만으로 쉽게 인증이 허가됨 - 부인방지 불가능
암호 프로토콜 기반 인증기술	장 점	- 다양한 인증 방식 존재하여 각 어플리케이션 환경에 적합한 인증 방식을 선택할 수 있음 - 예를 들어 인증서가 존재하는 어플리케이션 환경에서는 EAP-TLS, EAP-TTLS, PEAP 등을 선택할 수 있으며, 인증서가 존재하지 않는 환경에서는 EAP-TTLS, FAST, LEAP을 선택하여 적용할 수 있음 - 802.1x의 EAP, WAP2 등 이미 표준화가 진행된 인증 방식을 적용한다면 공식적으로 안정성을 보장받을 수 있음

		- 설계된 프로토콜에 의존하여 부인방지 가능
	단 점	- 암호 프로토콜의 안정성이 암호 프로토콜이 채용한 암호 및 인증 알고리즘의 안정성에 의존함 - WEP의 경우, 암호 알고리즘으로 RC4를 선택하였는데, RC4는 이미 1995년 깨진 암호 알고리즘임. 정적 키 사용시 IV 헤더를 모아서 분석하면 WEP 키가 노출됨. 따라서 WEP는 이와 같은 취약성으로 안정성이 매우 낮음 - LEAP의 경우도 초기에는 Cisco 호환 확장 프로그램을 통해 여러 관련업체가 LEAP을 사용하였으나, 취약점이 밝혀지면서 LEAP 내에서 보다 강력한 암호 알고리즘을 사용할 것을 권고함 - 높은 안전성을 보장하는 암호 프로토콜이라도 표준이 아닌 암호 프로토콜들은 지원되는 플랫폼이 제한적임. 예를 들어 EAP-TTLS, PEAP는 정식 표준이 아니어서 지원되는 플랫폼이 적음 - 암호 프로토콜이 아이디/패스워드를 사용하는지 또는 인증서를 사용하는지에 따라 각 인증 기술이 가지고 있는 장·단점을 계승함
PKI 기반 인증기술	장 점	- 매우 높은 안정성 - 아이디 패스워드 노출의 위험성이 줄어듬 - 확실한 기기 식별 가능 - 부인 방지 가능
	단점	- 인증서 관리 필요 (인증서 발급, 갱신, 폐기) - CRL 리스트 관리 필요 - 많은 계산량에 의한 처리 시간 지연
아이디 기반 인증기술	장 점	- 사전 키 분배가 필요 없음 - 연산량이 적고 키 길이가 짧아 저전력 소형 기기 등에서 사용이 가능 - 부인방지 기능
	단 점	- 공개된 정보인 ID를 사용함에 따라 ID를 위장한 공격에 취약

3. 인증기술에 대한 고려사항

가. 인증기술 의무화에 있어 고려사항

현재 대표적으로 인증기술이 사용되고 있는 금융분야에서는 각 인증기술별로 보안 등급을 분류하고 이 보안등급에 따라 서비스 범위를 규정하고 있다.[49] 금융감독원은 전자금융의 발전과 보안사고의 발생, 그리고 OTP(One-Time Password)라는 새로운 인증기술의 도입에 따라 각 인증기술의 사용에 대하여 보안등급을 3등급으로 분류하고, 이에 따라 거래한도를 10배까지 차등하도록 규정하였다.

[표 6] 거래이용수단에 따른 보안등급

거래이용수단	보안등급
OTP발생기 + 공인인증서	1등급
HSM 방식 공인인증서 + 보안카드	
보안카드 + 공인인증서 + 2Channel 인증	
보안카드 + 휴대폰 SMS(거래내역통보) + 공인인증서	2등급
보안카드 + 공인인증서	3등급

[표 7] 보안등급별 이체한도 (단위 : 천만원)

구 분		이체한도	보안등급		
			1등급	2등급	3등급
인터넷 뱅킹	개인	1회	10	5	1
		1일	50	25	5
	법인	1회	100		
		1일	500		
텔레 뱅킹	개인	1회	5	2	1
		1일	25	10	5
	법인	1회	10	2	1
		1일	50	10	5

49) 금융감독원, 전자금융감독규정 개정, 2008

또한 2009년, 전자금융거래시 반드시 공인인증서를 사용하도록 하는 의무화 규정이 스마트폰 환경 등 기존 PC 환경 외의 다른 환경에서 사용의 문제 등으로 인하여 논란이 되었다. 이에 대하여 2010년 5월 31일 국무총리실, 방송통신위원회, 금융위원회 등 관계부처들은 공동으로 '전자금융거래 인증방법의 안전성 가이드라인'을 발표하여 다음의 기준에서 공인인증서와 동등한 수준의 인증수단이 가능할 경우 공인인증서를 의무적으로 사용하도록 하는 기존의 규정을 사실상 폐지하였다.[50]

① (이용자 인증) 금융기관 또는 전자금융업자는 전자금융거래 제공시 정당한 이용자 여부를 식별 및 인증할 수 있어야 함

② (서버 인증) 금융기관 또는 전자금융업자는 이용자가 서버(정보처리시스템)에 접속한 경우 정당한 금융기관 등의 여부를 이용자가 식별 및 인증할 수 있도록 하여야 함

③ (통신채널의 암호화) 금융기관 또는 전자금융업자는 이용자와 서버간의 전자금융거래내역 등 중요정보가 유출되지 않도록 암호화를 통한 비밀성·무결성을 제공하여야 함

④ (거래내역의 무결성) 금융기관 또는 전자금융업자는 해당 전자금융거래내역의 위조·변조 여부를 확인할 수 있어야 함

⑤ (거래내역의 부인방지) 금융기관 또는 전자금융업자는 정당한 전자금융거래 사실을 이용자 및 금융기관이 부인할 수 없는 수단을 제공할 수 있어야 함

금융 환경에서의 인증기술의 사례에서 살펴볼 수 있듯이, 다양한 인증기술에 대하여 보안성을 평가하여 사용 환경 혹은 요구되는 보안의 수준에 따라서 차등적으로 적용이 필요할 것이다. 또한 특정 기술의 의무 사용은 미래 환경의 변화, 그리고 다른 기술들과의 호환성 등에 있어 문제가 발생할 소지가 있다. '전자금융거래 인증방법의 안전성 가이드라인'과 같이 각 인증기술의 안전성을 평가할 기준

50) 국무총리실, 총리실, '전자금융거래 인증방법의 안전성 가이드라인' 확정, 2010년 5월 31일자 보도자료

을 마련하고, 각 사용 환경의 특성과 요구되는 보안 안전성에 따라 선택적으로 인증 기술을 적용하도록 규정하거나 가이드라인을 제시하는 것이 사물통신 환경에서도 필요할 것이다.

나. 기기 및 인증기술의 예상 사용 기간에 따른 안전성

사물통신 환경에서는 사물통신기기(M2ME)가 원격지 등에 설치가 될 경우 오랜 기간 동안 사용이 될 것으로 예상되고 있다. 따라서 최초에 인증기술을 적용시에 연산 처리 능력(Computation Power)의 발전에 따라 향후에도 안전한 인증과 암호화를 위하여 알고리즘 및 키 길이(Key Length)에 대한 고려 역시 필요할 것이다.

미 표준과학원(National Institute of Standards and Technology, NIST)은 2007년 키 관리의 권유 사항이라는 보고서를 통하여 알고리즘의 보안 라이프타임에 따른 요구되는 알고리즘 및 키 길이를 규정하고 있다.[51]

[표 8] 알고리즘의 보안 라이트타임별 요구되는 알고리즘 및 키 길이

알고리즘의 보안 라이프타임	대칭키 알고리즘 (암호, MAC[52] 등)	Finite Field Cryptography (DSA, 등)	Integer Factorization Cryptography (RSA 등)	Eliptic Curve Cryptosystem (IBE 등)
2010년 까지 (최소 80비트 이상의 강인성)	2TDEA 3TDEA AES-128비트 AES-192비트 AES-256비트	최소 L=1024 N=160 이상	최소 k=1024 이상	최소 f=160 이상

51) NIST, Recommendation for Key Management - Part1 : General(Revised), 2007
52) Message Authentication Code

2030년 까지 (최소 112비트 이상의 강인성)	3TDEA AES-128비트 AES-192비트 AES-256비트	최소 L=2048 N=224 이상	최소 k=2048 이상	최소 f=224 이상
2030년 이후 (최소 128비트 이상의 강인성)	AES-128비트 AES-192비트 AES-256비트	최소 L=3072 N=256 이상	최소 k=3072 이상	최소 f=256 이상

NIST, Recommendation for Key Management - Part1 : General(Revised), 2007

제 4 장 사물통신 인증 기술에 대한 정책적 논의

본 장에서는 사물통신에 대해 다시금 정의해보고, 사물통신 및 사물통신 인증과 관련된 법정책적 이슈들을 살펴본다. 또한 사물통신 인증 전반을 규율할 수 있는 법제 개발과 관련된 논의를 진행하고자 한다. 이를 통해 사물통신 인증 관련 법제 개발을 위한 방안들과 요구사항을 도출해본다.

특별히 본 장의 내용들은 기존의 대표적인 사물통신이라고 할 수 있는 RFID와 CCTV, 자동 에이전트에 의한 계약 등을 통해 법적 이슈들에 대한 검토와 법전문가들과 기술전문가가 모여 진행된 법정책 전문가 회의의 논의 결과를 바탕으로 논의과정을 거쳐 인증기술관련 정책적 이슈들을 도출해내고 관련 법제정을 위한 요구사항들을 도출하였다.

제 1 절 사물통신 개념

1. 사물통신 개념

사물통신은 인간의 개입 없이 이루어지는 사물과 사물간의 통신을 일컫는데, 다양한 방식으로 개념화되고 있다. 국내 방송통신위원회는 통신, 방송, 인터넷 인프라를 인간 대 사물, 사물 대 사물 간 영역으로 확대, 연계하여 사물을 통해 지능적으로 정보를 수집, 가공, 처리하여 새롭고 효율적인 서비스를 제공하는 기술을 사물지능통신으로 정의하고 있으며, 3GPP/ETSI는 M2M(Machine-to-Machine)을 사람이 개입하지 않는 상태에서 기계(machine) 혹은 기기(device)간 일어나는 통신으로 정의하고 있다.

특히 M2M은 협의적으로 기계간의 통신 및 사람이 동작하는 기기와 기계간의 통신을 말하며, 광의적으로는 통신과 ICT 기술을 결합하여 원격지 사물의 상태정

보를 전달하거나 제어할 수 있는 서비스와 솔루션을 말한다. 유럽의 경우 M2M이라는 이름으로 논의가 진행된다기 보다는 RFID를 필두로 하여 사물들의 인터넷(IoT: Internet of Things)라는 이름으로 주로 논의가 진행되고 있는 상황이며, 사물들의 웹(WoT: Web of Things) 개념도 등장하고 있다. 사물 통신은 이처럼 다양하게 개념화되고 있지만, 그 기본적인 특징들을 추출하여 사물통신을 정의해보면 메시지와 명령의 송신과 수신과정에서 인간이 개입하지 않은 기계나 기기간의 통신이라고 정의할 수 있다.

2. 사물정보 개념

국내 방송통신위원회의 사물지능통신의 정의는 통신, 방송, 인터넷 인프라를 인간 대 사물, 사물 대 사물 간 영역으로 확대, 연계하여 사물을 통해 지능적으로 정보를 수집, 가공, 처리하여 새롭고 효율적인 서비스를 제공하는 기술이라는 정의에서 나와 있는 것처럼, 사물정보를 전제로 하고 있다. 사물정보란 사물을 이용하여 특정한 목적을 위해 광 또는 전자적 방식으로 처리되어 부호, 문자, 음성, 음향 및 영상으로 표현된 모든 종류의 자료 또는 지식을 말한다. 혹은 사물 자체를 표시하고 있는 정보 또한 사물정보라고 할 수 있다.

3. 법정책적 관점의 사물통신 개념

사물통신은 위에서 살펴본 대로 메시지와 명령의 송신과 수신과정에서 인간이 개입하지 않은 기계나 기기간의 통신이라고 정의할 수 있지만, 법정책적 차원에서의 사물통신 개념은 이러한 일반화된 개념만으로는 충분하지 못하다. 또한 기존의 정의에 포괄되는 모든 사물통신이 법정책적 차원에서 의미 있는 사물통신으로 포괄될 수 있는 것은 아니다.

통신(communications)이란 주체의 의사를 반영하고 전달하여 상대방에게 어떤 행동이나 영향을 유도하기 위한 상호간의 행위라고 할 수 있다. 의사 전달로서의

통신이란 결국 의사 주체와 그 상대방을 전제로 한다. 지능을 가진 사물이 통신을 한다는 것의 법적 의미는 직접적으로는 인간이 개입하고 있지 않지만 결국 통신 행위가 인간의 의사에 의해 이루어지고, 인간에게 영향을 주게 된다는 것이다. 즉, 법적으로 의미가 있는 통신은 인간에 의하는 것이냐, 인간에게 향하는 것이냐가 핵심적인 문제가 된다. 그렇지 않은 사물들의 통신행위는 동물들끼리의 통신행위처럼 인간에게는 어떠한 법적 의미도 갖지 못한다. 강아지끼리의 자율적인 의사소통행위는 전혀 인간에게 법적으로 의미가 없다.

법률적으로 법적 주체나 의사의 주체가 될 수 있는 존재는 자연인과 법인을 포함한 인간이므로 통신에서 법률행위의 주체가 될 수 있는 것은 사물이나 동물이 아닌 인간뿐이다. 따라서 지능을 가진 사물이나 동물이 해당 지능의 범위 하에서 신호를 주고받는 통신행위가 인간이 만들어 놓은 법적 규율 대상이 되는가가 법적인 관점의 사물통신의 의의이다.

인간의 훈련에 의해 길들여진 동물들이 인간과 인간의 통신에 사용되는 경우, 예를 들어 비둘기가 통신행위에 이용되는 경우 등은 단순히 인간의 통신에 이용되는 통신수단일 뿐이다. 이처럼 법적으로 유의미한 통신이 이루어지기 위해서는 사물통신의 원래 의미와는 다르게 법적으로 유의미한 사물통신은 그 과정에 사람이 개입해야 한다.

하지만 사람의 개입은 실제 통신 과정인 송신과 수신 사이에는 사람이 개입하지 않아야 한다. 송신과 수신 과정에서 개입한다면 엄밀히 말해 사물통신이라고 할 수 없다. 사물과 사물 간의 송, 수신 과정에서는 사람이 개입해서는 안되지만, 송신 이전과 수신 이후에는 어떤 식으로든 인간이 연관되어야 법적 의미를 갖는 통신행위가 될 수 있다. 결국 사물통신이 법적으로 유의미하기 위해서는 해당 사물통신이 인간의 의사에 지배되고 있거나, 해당 통신이 타인의 권리 또는 의무에 직, 간접적인 영향을 끼쳐야 한다.

법적 관점에서 사물통신을 파악하는데 있어 가장 중요한 점은 사물통신을 어떻게 어떤 범위로 정의할 것인가에 달려있다. 일반적으로 통신행위를 상호통신의 주체를 중심으로 구분해보면 다음과 같다.

① 사람-사람 통신

(그림 34) 사람-사람 통신

가장 전형적인 통신 유형으로 법적 의미를 갖고, 일반적으로 법적 규율체계가 규정되어 있다.

② 사람-사물 통신

(그림 35) 사람-사물 통신

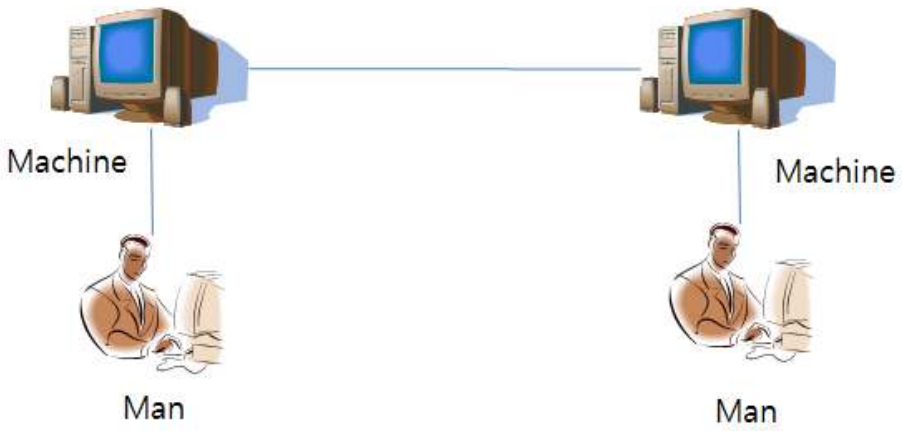
사람의 의사가 반영되고 통신의 결과가 사람에게 직,간접적으로 영향을 주게 되므로 법적 의미를 갖는 통신이라고 할 수 있다.

③ 순수한 사물간의 통신으로서의 사물-사물 통신

(그림 36) 사물-사물 통신

사람의 의사가 반영되지 않고, 통신의 결과가 사람에게 법적인 의미나 법적인 차원의 영향을 주지 않는 사물-사물 통신이 존재할 수 있다.

④ 사람간의 통신으로서의 사물-사물 통신



(그림 37) 사람-사물-사물-사람 통신

사람의 의사를 주고받는 도구로서 사물이 이용되는 경우 사물에 의해 이루어지기는 하지만 매번 통신이 사람의 의사에 의해서 이루어지고 사람에게 직접적인 영향을 주게 되므로 결국 사람 간의 통신으로 규율된다.

⑤ 사물-사물 통신

(그림 38) (사람)-사물-사물-(사람) 통신

매번 통신 과정이 사람에게 인지되지는 않지만 본질적으로 사람의 의사가 반영되고 사람에게 직,간접적으로 영향을 주는 통신으로 전형적인 법적 의미를 갖는 사물통신이라고 할 수 있다.

사물통신은 이러한 관점에서 사람을 대신하여 자동적으로 수행되는 사물간의 계약행위에서부터 사물을 이용한 공무원의 법률 집행과 같은 엄격한 법률행위에서부터 단순한 텔레메트리에 이르기까지 다양한 수준의 통신행위를 포괄한다. 이러한 다양한 수준의 사물통신 중에서 통신행위의 결과 상 법률관계가 발생할 수 있고, 국민에게 심각한 피해가 발생할 수 있으며, 전반적인 사물통신의 신뢰성을 해칠 수 있는 사물통신 유형의 경우에는 이를 법으로써 엄격히 규율하는 것이 필요하다.

결국 중요한 것은 모든 사물통신이 법적인 규제 대상은 아니라는 것이다. 법적으로 규제할 필요할 수 있는 사물통신을 명확하게 규정하게 규율함으로써 사물통신에서 발생할 수 있는 위험을 최소화하기 위한 효과적이고 효율적인 법적 규제를 마련하는 일이 가장 중요하다고 할 수 있다. 즉, 본 장에서는 사물간의 통신 자체가 문제가 아니라 사물간의 통신이 법적 규제 대상이 될 때가 문제이다.

동물간의 통신과 행위가 법적 규율 대상이 아니듯, 사물간의 통신 행위 자체가 법적 규율 대상은 아니다. 결국은 사물간의 통신행위의 결과가 사람, 재산, 환경

등에 해를 끼침으로써 현행법을 위반하는 효과를 낳았거나 불법행위에 해당될 경우에 법적 규제 대상이 되는 것이다. 따라서 사물간의 통신행위가 어떠한 위법적인 효과를 낳지 않고 사람의 건강, 재산, 환경에 영향을 미치지 않는다면 해당 통신에 대해서는 법에서 규제할 필요가 전혀 없게 된다. 예를 들어 홈 디지털 기기간의 블루투스 통신, 혹은 Zigbee 통신의 경우 별도의 법조항을 규정함으로써 심각하게 규제할 필요는 없다. 하지만 공공시설물에 대한 통제 혹은 공공집행행위가 기기에 의해서 자동적으로 수행되는 경우나 자동적으로 기계에 의해서 계약이 수립되는 경우 등은 법률적인 권한을 가져야 하므로 법에서 그 권한과 책임관계를 명확히 규정해야 할 필요가 존재한다.

따라서 법정책적인 차원에서의 사물통신은 다음과 같이 새롭게 정의될 필요가 있다. 즉, 법적인 의미에서 사물통신은 송신의 개시와 수신의 완료 간에는 사람의 개입 없이 이루어지지만 사람의 의사가 반영되고 사람에게 직,간접적인 영향을 주는 사물간의 통신이라고 정의할 수 있을 것이다.

제 2 절 사물통신의 정책적 이슈

위에서 살펴본 것처럼 인간의 의사를 반영하고 인간에게 직간접적인 영향을 주는 사물통신만이 법정책적 차원에서 의미를 가지게 된다. 또한 사물통신에서 법정책적 차원에서 사회적 이슈들이 존재하는 경우에는 인간에게 직간접적으로 우려될만한 영향을 준다고 할 수 있으므로, 이러한 사물통신 관련 법정책적 이슈들을 살펴봄으로써 법적 의미를 갖는 사물통신의 범위를 짚어보도록 하겠다. 이를 위해 전통적인 사물통신이라고 할 수 있는 RFID, CCTV 등과 최근 유럽의 IoT 이슈와 국내의 사물통신망 추진단계의 이슈들을 짚어보도록 하겠다. 또 마지막으로 앞서 살펴본 사물정보를 둘러싼 법적 이슈도 살펴보도록 하겠다.

1. RFID와 프라이버시 침해

RFID 기술은 사물의 식별정보 등을 극소형 태그에 저장하여 사물에 부착하고, 당해 사물 및 주변 환경 정보를 무선주파수를 통해 안테나가 장착된 리더 및 네트워크로 전송하여 필요한 정보처리를 하는 비접촉형 자동식별 기술을 말한다. 사물에 부착된 태그와 리더와 같은 기기들 간의 통신을 통해 수행되므로 사물통신의 대표적인 예라고 할 수 있다. RFID 기술은 유통, 물류, 자동차 등 다양한 분야에서 응용될 수 있는 장점이 있는 반면 사용자 정보의 접근이 용이해짐에 따라 프라이버시 침해 등의 역기능 문제가 대두되고 있으며, 전세계적으로 RFID에서의 프라이버시 이슈가 심각하게 논의된 바 있으며, 관련된 이러한 프라이버시 위험을 최소화하기 위한 RFID 프라이버시 가이드라인과 법제들이 만들어진 바 있다. 일반적으로 알려진 RFID 기술의 프라이버시 취약점은 다음과 같다.

[표 9] RFID와 프라이버시 이슈

정보유출 (데이터보안 문제)	RFID 태그 내부에 저장된 사용자의 비밀정보가 공개되어 프라이버시 침해가 발생될 수 있다.
추적 가능성 (위치 프라이버시 문제)	RFID 태그에 저장된 정보의 내용이 노출되지 않는 경우라도 RFID 태그가 가지는 고유한 값을 통한 사용자의 위치추적이 문제될 수 있다.
전방향 프라이버시 문제 (Forward Privacy)	일시적으로 공격자에게 태그의 비밀 정보가 노출되었다고 하더라도 그로 인하여 그 태그와 관련된 사용자에 대한 이전의 모든 행적이 다 노출될 수 있다.

2. 네트워크 CCTV와 프라이버시 침해

건물 외벽 등 CCTV, 웹 카메라를 설치하는 경우 촬영 범위 또는 카메라의 각도에 따라 주변 아파트나 주택 등이 촬영되어 타인의 사생활이 침해될 우려가 있으며, 도로변에 설치된 CCTV의 경우 개인의 얼굴 등의 식별정보가 노출될 수 있는 위험이 존재한다.

특히 네트워크 기반 CCTV는 영상센서가 달려있는 카메라를 통해 자동적으로 수집된 영상 사물정보를 네트워크를 통해 서버로 실시간 전송하는 것을 말한다. 일반 CCTV와 마찬가지로 개인의 얼굴이나 사적인 행위 등이 기록될 수 있는 위험이 존재하나 오프라인 장소에 기록, 저장되는 일반 CCTV와 달리, 통신 선로 상에서 가로채기 등에 의해 유출될 수 있고 손쉬운 복제 등으로 인해 유출범위가 넓다는 더욱 심각한 위험이 존재한다.

네트워크 CCTV는 원격센서에서 수집한 사물정보를 원격기기에 전송하는 일종의 텔레메트리 방식의 사물통신의 대표적인 예라고 할 수 있으며, 이러한 텔레메트리 방식의 사물통신은 센서의 대상이 인간의 민감한 개인정보를 포함했을 경우 해당 통신에서 전송되는 정보에 대한 심각한 프라이버시 이슈가 대두될 수 있다.

3. 유럽에서의 IoT 프라이버시 및 보안 이슈

IoT(Internet of Things)는 2005년 11월 ITU-T 국제정상회의에서 제안된 기술 개념으로 “정보통신기술(ICT)의 차세대 기술로, 언제 어디서든 누구에게나 연결되던 정보통신기술이 모든 사물과의 연결로 확장되는 기술”을 말한다. IoT는 RFID나 센서 네트워크와 같은 기술들을 기반으로 하고 있으며, 이러한 대표적인 기반 기술에서 다양한 보안 및 프라이버시 이슈들이 제기되고 있다. 특히 유럽의 경우 유럽의회는 이러한 사물들의 인터넷 문제의 심각성에 대해 인식하고 2010년 6월 다음과 같은 사물 인터넷 문제의 해결을 위한 정책을 통과시켰다. 유럽의 국민들이 IoT로 인한 혜택을 누리기 위해서는 다음과 같은 항목들이 우선적으로 고려되어야 한다. 아래 항목들에서 보이는 것처럼, 보안, 데이터 보호 및 프라이버시가 사물들의 인터넷에서 매우 중요함을 알 수 있다[53].

- 프라이버시와 개인정보의 보호
- 인프라의 보안 문제와 네트워크 정체 문제 해결
- IoT의 문화적 윤리적 측면 고려
- 인간이 개입하지 않는 조용한 불간섭 기술
- 보안 강화
- 엄청난 양의 데이터
- 소비자 신뢰의 확보
- 비용 감소
- 최신 인터넷 기술의 발전의 반영
- 경제 발전 잠재력
- 주파수 조율
- 사회적 논의 강화

또한 유럽은 사물들의 인터넷에서의 이러한 문제점들에 대한 대응 방법으로 다음과 같은 14가지 기술들을 제시하고 있다.

53) European Parliament, Internet of things Procedure file, INI/2009/2224, 2010

- 거버넌스
- 지속적인 프라이버시 모니터링
- 기술의 조용한 불간섭 기술
- 잠재적인 위험의 식별
- 경제와 사회의 핵심 자원으로서의 IoT 인식
- 강제적인 표준
- 연구 개발
- 민간-정부의 파트너십
- 혁신과 파일럿 프로젝트
- 제도적인 인식
- 국제적인 논의
- RFID 라이프사이클 고려
- 관련 공동체 정책의 효과성과 경제와 사회에 미칠 영향 평가
- 진화수준의 평가

4. 국내에서의 사물통신망 추진 시 이슈

국내의 사물지능통신법 해설서에 따르면 KT는 사물통신망 추진 과정에서 다음과 같은 문제점들에 대한 이슈를 제기하고 있다. 우선 사물통신과 관련된 단말기가 불법적으로 사용될 수 있지만, 이에 대한 책임 소재를 파악할 수 있는 명확한 기준이 존재하지 않는 상황이다. 즉, 장애 및 오작동에 대한 기술적 오류와 책임소재의 문제가 발생할 수 있으며, 악용의 소지가 존재한다는 점이다. 따라서 장애, 사고 발생 시에 대한 사물통신 사업자의 역할과 의무 및 책임의 범위를 법규로 명시할 필요가 있으며, 각종 정보의 공개 및 노출에 대한 이용자와 사업자의 책임 범위를 명확하게 할 필요가 존재한다고 밝히고 있다.

5. 사물정보의 프라이버시 이슈

사물정보란 앞서 살펴보았던 대로 센서네트워크와 텔레메트리 등의 기술에서

사물을 이용하여 특정한 목적을 위해 광 또는 전자적 방식으로 처리되어 부호, 문자, 음성, 음향 및 영상으로 표현된 모든 종류의 자료 또는 지식을 말한다.

사물정보는 단순한 사물식별정보를 넘어 사람과 연계를 맺고 사람에 대한 정보를 포함하는 한 개인정보와의 관련성에 따른 프라이버시 문제가 발생할 수 있다. 따라서 사물정보를 정확하게 개념화하기 위한 작업이 필요하며, 이러한 유무선 통신망을 활용한 사물원시정보의 수집과 수집된 사물정보의 원활하고 안전한 공동이용을 위한 법제 정비가 필요한 시점이다.

사물정보는 다음과 같이 다양한 차원에서 프라이버시와 결부될 수 있다.

첫째, 사물과 사람의 결합도가 높아지면서 사물의 인증정보 자체가 사람에 대한 개인정보가 되어버림으로써 이러한 인증정보의 유출이 개인정보유출의 효과를 갖게 되는 경우이다. 이런 차원에서 사물의 식별과 인증에 사용되는 정보는 개인정보로서 보호되어야 하며, 개인의 자기정보결정권이 보장되어야 한다.

둘째, 사물이 센서 등을 통해 수집하는 정보 중에 민감한 개인정보가 포함되게 되는 경우이다. 앞서 CCTV나 RFID 기술에서 보인바와 같이 심각한 프라이버시 침해 이슈가 발생된다.

셋째, 사물의 위치정보가 프라이버시 침해로 이어지게 되는 경우이다. 사물의 이동성이 증가하고 사물과 사람의 결합도가 높아지면서 사물의 위치가 개인의 위치정보를 유출시킴으로써 프라이버시를 침해하게 된다.

각각의 경우에 발생할 수 있는 이슈들을 하나씩 살펴보도록 하겠다.

1) 개인정보로서의 사물식별정보

첫 번째 사례는 사물을 식별하기 위해 내부에 저장해놓은 식별정보가 개인정보에 해당되는 경우이다. 예를 들어 네트워크 장치마다 부여된 IP/MAC주소 정보를 들 수 있다. IP주소나 MAC주소는 직접적으로 사람에게 부여된 것이 아니라 기계들에 부여되는 일종의 사물정보라고 할 수 있다.

이러한 사물정보가 개인정보가 될 수 있는 근거는 정보통신망법의 개인정보 정의이다. 정보통신망법은 개인정보를 해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우로 한정함으로써 IP주소정보와 MAC주소정보가 개인정보로의 조건을 갖추도록 하고 있다. 기본적으로 개인정보로서의 IP주소정보와 MAC주소정보는 정통망법에 의해서는 무단 제3자 제공 및 무단 수집, 이용을 금지하고 있다.

제2조 (개인정보의 "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.

제24조의2 (개인정보의 제공 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

제22조 (개인정보의 수집·이용 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호 어느 하나의 사항을 변경하려는 경우에도 또한 같다.
1. 개인정보의 수집·이용 목적
2. 수집하는 개인정보의 항목
3. 개인정보의 보유·이용 기간

또한 통신비밀보호법은 IP주소를 정확히 명시하고 있지는 않지만 컴퓨터 통신 또는 인터넷 로그 자료의 일부로서 통신사실확인자료에 포함시켜 통신사실확인자료를 취득하려면 통신사실확인자료 제공요청 허가를 필하도록 하고 있다.

> 제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
> 11. "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다.
> 마. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료
>
> 제13조 (범죄수사를 위한 통신사실 확인자료제공의 절차) ①검사 또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자(이하 "전기통신사업자"라 한다)에게 통신사실 확인자료의 열람이나 제출(이하 "통신사실 확인자료제공"이라 한다)을 요청할 수 있다.
> ②제1항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다. 이하 같다) 또는 지원의 허가를 받아야 한다. 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체 없이 그 허가를 받아 전기통신사업자에게 송부하여야 한다.

많은 개인정보보호 관련 보고서들과 정보보호진흥원의 매뉴얼에는 개인정보의 예시항목에서 기타 부분에 전화통화내역, IP주소, 웹사이트접속내역, 이메일, 전화메시지, GPS 등에 의한 개인위치정보를 들고 있다. 또한 현재 많은 기업들은 자사 홈페이지의 개인정보보호정책에서 수집하는 개인정보 중의 하나로 IP주소 정보를 명시하고 있는 상황이다.

1. 수집하는 개인정보의 항목 및 수집방법

가. 수집하는 개인정보의 항목

첫째, 회사는 회원가입, 원활한 고객상담, 각종 서비스의 제공을 위해 최초 회원가입 당시 아래와 같은 개인정보를 수집하고 있습니다.

- 필수항목 : 성명, 주민등록번호, 외국인등록번호 또는 여권번호(외국인에 한함), 아이디, 비밀번호, 본인확인문답, 이메일 주소, 만 14세 미만인 경우 법정 대리인 정보
- 선택사항 : 휴대폰 번호

둘째, 서비스 이용과정이나 사업처리 과정에서 아래와 같은 정보들이 자동으로 생성되어 수집될 수 있습니다.

- IP Address, 쿠키, 방문 일시, 서비스 이용 기록, 불량 이용 기록

IP주소의 개인정보성격에 대해서는 국내외적으로 많은 논란이 존재해왔고, 해외도 제각각인 판결을 내리고 있는 상황이다. 독일의 경우 최근 IP가 개인정보가 아니라는 판결을 내린 바 있고, 스위스의 경우 올해 IP주소도 개인정보이므로 IP주소를 무단으로 수집하거나 제3자에게 공개해서는 안된다고 판결한 바 있다. 프랑스의 경우 2007년과 2009년에 IP주소가 개인정보보호의 대상이 아니라는 판결이 내려진 바 있지만, 2010년 개인정보보호법 개정안에서는 '통신 네트워크 연결의 단말 장치를 판별하는 모든 주소나 번호를 개인정보로 규정한다'고 명시하고 있다. 미국에서도 주에 따라서 저작권 침해자 식별목적의 미국 음반협회(RIAA)의 IP주소 수집행위에 대해 합법 및 불법 결정이 엇갈리고 있는 상황이다.

국내에서는 2004년 통신비밀보호법 개정안 논의 당시 진보네트워크센터는 IP주소가 개인정보라는 온라인 캠페인을 벌여 사회적인 논란을 일으킨 적이 있다. 이때 이후 대부분 IP주소는 개인정보로 사회적으로 인정되어 오고 있다. 2009년 1월 미네르바 사건 당시 다음커뮤니케이션이 미네르바의 신상정보와 IP 기록을 검찰에 제공했다며 인터넷기자협회를 비롯한 시민단체들이 규탄성명을 발표한 바 있다.

IP주소가 개인정보가 되지 않는다는 의견으로는 IP주소의 유동성과 관련된 것과 IP주소가 기기에 제공되는 것일 뿐 개인에게 제공되는 주소가 아니라는 것, 따라서 IP주소를 통해 개인을 식별할 수 없다는 것이다. 또한 보통 공공장소나 가정의 PC들도 개인 1인이 이용하는 것이 아니라 여러 사람이 이용할 수 있는 가능성이 존재하므로 개인 1인을 특정하는 것이 어렵다는 특징이 존재하기 때문에, IP정보 자체만으로는 개인정보가 되지 않는다는 것이다.

이에 대한 반론은 IP 정보는 그 자체 단독으로는 개인을 식별할 수 있는 정보는 아니지만 다른 정보와 결합하면 개인을 식별할 수 있는 정보라는 점이다. A은행의 고객 성명, 주민등록번호, 이메일주소 누출사례에서도 법원은 이메일 주소에 대해 당해 정보만으로는 특정 개인을 알아볼 수 없지만 다른 정보와 용이하게 결합할 경우 당해 개인을 알아볼 수 있는 정보라고 할 수 있으므로 앞서 설명했던 정보통신망법 제2조 소정의 개인정보에 해당한다고 판결을 내리고 있다. 이를 통해 보더라도 다른 정보와 용이하게 결합할 경우 당해 개인을 알아볼 수 있는 정보이므로 IP주소도 개인정보에 해당한다는 것이다. 또한 IP 주소를 숨기기 위한 익명화도구들이 존재한다는 사실은 IP주소가 자신의 신원을 식별당할 수 있는 핵심적인 개인정보의 하나라는 사실을 반증하고 있다.

IP주소를 포함한 통신사실 확인자료 항목의 민감성과 중요성 때문에 통신비밀보호법에서 규정하고 있는 것이다. 또한 미국음반협회 등 저작권 단체들이 IP주소를 근거로 하여 저작권 침해자들을 식별하여 책임을 묻고 있다는 점에서도 IP주소가 개인을 식별하는 핵심적인 정보의 하나로 사용되고 있음을 알 수 있다. 2010년 5월 야후는 90일이 지나면 개인정보로서의 IP주소를 식별할 수 없도록 보관중인 IP주소 정보 중 일부 항목을 삭제할 방침이라고 한다.

MAC 주소의 경우 IP와 달리 하나의 컴퓨터에 고유하게 부여되는 고유식별번호이다. MAC주소는 랜카드-이더넷 카드의 고유주소로 해당 카드 생산 시에 최초 부여되어 유일하게 가지고 있는 정보이다. 절대 동일한 MAC주소는 존재하지 않

으며, IP와 함께 수집하여 매핑을 하면 특정 컴퓨터가 어디에 위치하고 있는지에 대해 확인할 수 있다. 따라서 해당 기기를 소유하거나 통제권을 가지고 있는 개인을 특정하기에는 더없이 좋은 정보라고 할 수 있다. MAC주소에 대해 개인정보성을 부정하고 있는 사람들은 MAC주소는 기기에 부여된 주소일 뿐이며, 랜카드를 교체하면 MAC주소가 틀려지고 MAC주소에 대한 위조 공격 또한 가능하므로 개인과 랜카드를 매칭할 수 없기 때문에 개인정보에 해당하지 않는다고 주장하고 있다. 하지만, 일반적으로 MAC 주소 또한 다른 정보와 결합하면 개인을 식별할 수 있는 정보가 될 수 있으므로 많은 사람들은 MAC주소를 개인정보의 일종으로 보고 있으며, 특히 개인을 특정하는데는 유동적인 IP주소보다 더 확실한 정보라고 인정되고 있다. 2010년 7월, 국내 싸이월드의 경우 피싱을 막기 위해 MAC주소와 컴퓨터 이름을 추가적으로 수집하겠다고 밝힌 이후 회원들의 반발을 산후 자진 철회한 바 있다. 구글 또한 MAC주소를 수집한다는 의심을 받아오고 있다.

국내에서 IP주소와 MAC주소는 사람이 아닌 기계에 부여되는 식별자로서 사물정보라고 할 수 있지만, 다른 정보와 결합하면 개인을 식별할 수 있는 정보에 해당하므로 정보통신망법 제2조의 정의에 근거하여 개인정보에 해당한다고 할 수 있다. 사업자측과 국민들 또한 개인정보로 받아들이고 있고, 해당 정보의 무단 수집 및 제3자 제공에 대해 민감하게 반응하고 있는 상황이다. 따라서 이처럼 다른 정보와 결합됨으로써 개인정보가 될 수 있는 사물정보들의 경우 개인정보로 취급하여 법적으로 규율할 필요가 있다. 이러한 사물정보들을 주고받는 사물통신의 경우 일반적으로 개인정보보호법이 존재하는 국가에서는 개인정보에 준하여 보호해야 하며, 일반법이 존재하지 않는 경우에도 특별법을 통해 해당 사물정보에 대해 보호하고 있다.

2) 개인정보로서의 사물위치정보

위치추적은 대표적인 기기 간 통신이라고 할 수 있다. 위치정보는 일종의 사물정보라고 할 수 있다. 사람의 몸에 직접 부착되지 않거나 사람이 이상 사물의 위

치라고 할 수 있지만, 개인이 지니고 다니는 한 개인과 센서의 연관관계가 유지되는 한 개인정보라고 할 수 있다. 국내의 위치정보보호법에서는 위치정보와 개인위치정보를 다음과 같이 정의하고 있다.

> 제2조(정의)
> 1. “위치정보”라 함은 이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 전기통신기본법 제2조 제2호 및 제3호의 규정에 따른 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것을 말한다.
> 2. “개인위치정보”라 함은 특정개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다.)를 말한다.

사물에 부착된 장치에 의해 기록되는 위치 정보는 사람과 결합될 때 민감한 개인정보가 될 수 있으므로 사물에 부착된 장치와 위치 정보 서버간의 사물 통신은 개인정보보호법이나 위치정보보호법에 의해 규제된다. 특히 재난 사고와 관련된 스마트 안심 서비스의 경우 이러한 특징의 사물위치정보가 이용된다.

3) 감청대상으로서의 사물통신

사람과 사람간의 통신에서 통신프라이버시를 보호하기 위한 온라인 감청 규제는 보호할만한 대상을 보호한다는 원칙이 존재한다. 하지만, 앞서 살펴보았던 것처럼 사람과 사람의 통신이 아닌 사물과 사물의 통신에 대한 감청에도 감청영장이 요구되는가의 이슈가 존재한다. 즉, 사물과 사물의 통신이 보호할만한 대상이 되는지에 따라 판단되어야 한다. 프라이버시에 대한 민감도 때문에 스마트그리드 시스템에서 스마트 미터기 정보의 실시간 데이터 전송에 대한 무단 지득행위의 위법성이나 앞서 살펴보았던 개인정보로서의 사물정보가 실시간으로 전송되는 사물통신로상에서의 감청을 어떻게 바라볼 것인가에 대한 이슈가 존재한다.

제 3 절 사물통신에서의 법적 책임 귀속

앞 절에서 사물통신을 둘러싼 다양한 이슈들을 살펴보았다. 위의 이슈들은 주로 사물정보의 개인정보성이나 이에 따른 사물통신에서의 프라이버시 침해와 관련된 이슈들을 살펴보았다. 사물통신과정에서 인증을 요구하는 이유는 어떠한 방식으로든 사물통신 과정이 인간의 의사나 인간의 삶에 영향을 주기 때문이다. 인증이란 것 자체가 어떤 행위가 인간의 삶에 영향을 끼칠 것으로 예상될 때 이에 대한 의사결정의 오류를 줄이고 문제 발생 시 책임을 규율하기 위한 방식으로 가장 고전적으로 많이 사용되는 방식이라고 할 수 있다.

법적 규제 대상으로서의 사물지능통신의 전제조건 중의 하나가 인간의 의도를 반영해야 하고, 인간에게 영향을 미쳐야 한다는 것이라는 점을 살펴보았다. 따라서 사물지능통신에서 가장 중요한 것은 송신자로서의 인간의 의도를 정확하게 반영해야 하고, 수신자로서의 인간에게 악영향을 미치지 않아야 한다는 것이다. 따라서 사물지능통신은 이용주체의 보호 혹은 소비자 보호 측면에서 고려되고 통제될 필요가 있다.

본 절에서는 사물통신 과정에서 발생할 수 있는 프라이버시나 보안 관련 사고와 같은 이슈들이 발생했을 경우의 사물통신의 책임 문제에 대해 논하고자 한다. 사물통신에서의 책임귀속 문제는 자동 에이전트에 의한 계약 문제에서 드러났던 논의들을 중심으로 살펴보도록 하겠다.

1. 계약주체로서의 전자에이전트

계약주체로서의 전자 에이전트의 문제는 사물통신 개념이 등장하기 이전에 이미 사물통신의 특성들을 보여주고 있으며 사물통신 문제의 법정책적 해결을 위한 노력의 단초를 제공하고 있다.

에이전트(agent)라는 용어는 서로 다른 과학 영역에서 다양한 내포와 정의들을 가지고 있다. 경제학에서의 대리인(representative) 개념이 존재하고, 컴퓨터 과학 영역에서 특정 방식으로 업무를 수행하는 컴퓨터 시스템을 가리키기도 한다. 일반적으로 컴퓨터 과학에서의 에이전트의 정의는 특정 환경에 위치하여 설계 목표를 달성하기 위해 이러한 환경에서 자율적인 행위를 할 수 있는 능력을 갖춘 컴퓨터 시스템을 말한다. 일반적으로 경제학적 관점에서의 대리인과 구분하기 위해 전자 에이전트(electronic agent)라는 용어를 사용한다.

자치 혹은 자율성 개념은 중개인 개념을 이해하는데 매우 중요하다. 컴퓨터 시스템이 자율적이라는 것은 만약 인간이나 다른 시스템의 개입 없이 행동할 수 있고, 일정 정도 범위 내에서 자신의 행위를 통제할 수 있다는 것을 말한다. 팀 스미더에 따르면 자동화된 시스템이란 자율 규제적인 시스템을 말하며, 자율적인 시스템이란 그들이 스스로 자신의 행위를 규제하기 위한 법칙과 전략들을 개발할 수 있다는 의미를 포함한다. 즉, 자율에 있어 가장 핵심적인 요소는 학습능력이다. 만약 시스템이 설계 시에 정해진 대로만 어떤 사건에 대해 반응 할 수 있다면 순수하게 자동화된 시스템이라고만 할 수 있다. 많은 경우 전자 에이전트는 외부 개입 없이 자율적으로 행동하는 능력을 갖춘 시스템으로 인식된다.

현실에서 사용되는 전자 에이전트는 매우 다양하다. 흔히 정보검색이나 전자상거래에서 많이 사용된다. 특히 전자상거래에서 에이전트가 사용되는 경우에는 거래비용을 줄일 수 있다는 장점이 존재한다. 전자 에이전트를 통한 거래는 인간에 의해 수행되는 것에 비해 더 빠르고 저렴하게 이루어질 수 있고, 좀 더 복잡한 거래도 가능하다는 장점이 존재한다. 이처럼 지능형 시스템인 자동 에이전트에 의한 계약은 온라인 환경의 비즈니스 활성화를 위한 필수적인 시스템으로 기업들과 소비자들에게 편이성을 포함한 많은 혜택들을 제공해준다.

방통위가 사물지능통신 R&D 핵심 4대 분야 중 하나로 꼽은 개인맞춤형 서비스는 특히 이러한 전자 에이전트 혹은 자동 에이전트에 의한 계약문제가 직접적

으로 결부되는 분야라고 할 수 있다. 개인맞춤형 서비스의 경우 개인이 자신이 원하는 수준의 서비스를 받기 위해 서비스를 제공하는 컴퓨터와 개인정보 노출 수준과 관련한 협상을 수행하고 계약을 수행하는 것이라고 할 수 있다. 따라서 개인장치와 서버와의 협상과 계약과정에서의 법적 효과의 문제는 직접적으로 사물통신과 관련이 있다고 할 수 있다.

전자상거래에서 전자 중개자의 이용은 이미 일상화가 되었고, 더욱 그 비중은 증가하게 될 것으로 예상된다. 전자 에이전트의 자율성에도 불구하고 그들에 의해 수행되는 계약의 결과는 이용자들에게 귀속된다. 일반적으로 전자 에이전트들을 법적 주체로 간주하는 것은 이치에 맞지 않는 것으로 인정된다.

현재도 많은 경우들이 존재하지만, 향후 전자상거래는 시맨틱 웹 등을 이용한 전자 에이전트나 "Know-bots"에 의해 인간의 개입 없이 컴퓨터 상호간에 이루어질 것이며, 이러한 인간의 개입의 결여는 인간 상호간의 계약과정을 필수적으로 요구하고 있는 Uniform Commercial Code(통합상거래법)에서 말하는 것과 같은 계약법의 근본적인 가정과 충돌하고 있다.

한편으로 전형적인 일반법 국가들에 적용되는 동의의 객관주의 이론은 외화된 결과물(external appearance)에 강조점을 두는 것이다. 즉, 개인의 실제 의도가 무엇인든 상관없이, 개인이 행한 계약행위는 사람들이 합리적으로 생각하기에 상대편 당사자가 제안한 계약조건에 대해 동의하는 것으로 믿어진다. 객관주의 이론에 따르면 외화된 의도는 법정은 사람의 심리학적인 내부 심리상태는 별로 중요하게 생각하지 않는다. 단지 계약서 상의 결과물만이 중요하다.

계약 수립을 목적으로 전자 에이전트를 이용하는 행위는 자신의 동의 행위를 표시한 것으로 받아들여진다. 객관주의 이론은 자동화된 에이전트가 수행한 계약행위의 적법성을 보증해줄 수 있는 이론으로 받아들여진다. 자동화된 전자 에이전트에 의한 계약의 법적 효과와 관련된 다양한 법들이 해외에 이미 존재한다.

1) EU Electronic Commerce Directive

유럽의 전자상거래지침은 전자적인 방식의 계약 행위를 장려하고 있으며, 제안서에 따르면 회원국들은 전자시스템을 지능화된 전자 에이전트로 이용하는 행위를 막지 않는다고 적고 있다.

2) UNICITRAL Model Law on Electronic Commerce (1996)

2(c) : 메시지 발송자에는 본인 혹은 대리인이 포함된다. 13(2)(b) : 데이터 메시지를 발송한 사람은 전자장비를 운용할 수 있다.

3) U.S. Uniform Electronic Transaction Act 1999

2(6) : 전자 에이전트는 개인에 의한 검토나 행위 없이 전체 혹은 부분적으로 전자기록이나 수행에 대응하기 위한 행위를 시작하기 위해 독자적으로 이용되는 컴퓨터 프로그램 혹은 전자 및 다른 자동화된 수단을 의미한다. 14 : 인간이 전자 에이전트의 행위와 동의행위를 인지하거나 검토하지 못했더라도 계약은 전자 에이전트들간의 상호작용에 의해 성립될 수 있다. 또한 계약은 전자 에이전트와 개인 간의 상호작용에 의해서도 성립된다.

4) UETA 입안자의 주석 중

지금의 전자 에이전트는 사전에 프로그래밍된 기술적인 능력의 범위안에서 행동할 수 있을 뿐이다. 하지만 향후에는 전자 에이전트는 단지 자동적으로 수행될 뿐 아니라 자율적으로 행동할 수 있는 능력이 부여될 수 있다. 인공지능 기술의

발전으로 컴퓨터는 경험을 통해 배울 수도 있으며, 스스로의 프로그램에서의 명령을 수정할 수 있고, 새로운 명령을 고안해낼 수도 있다. 만약 이러한 발전이 가능해진다면, 법원은 새롭게 등장하는 가능성들에 따라 전자 에이전트의 정의를 새롭게 해야 할 것이다.

5) U.S. Uniform Computer Information Transactions Act, 1999 (UCITA)

UCITA는 206조에서 계약은 전자 에이전트의 작동에 의해 체결될 수 있다고 규정함으로써 사람이 아닌 컴퓨터의 작동에 의해서도 계약이 체결될 수 있음을 명시하였다. 또한 전자계약에서 컴퓨터 작동의 인간에의 귀속에 대해서 컴퓨터 작동의 위험귀속까지 규율하고 있다. 전자 에이전트의 작동은 인간의 포괄적 지시에 따른 기계적 작동에 불과하고 원인을 규명하기 힘든 오류발생의 가능성이 상존한다는 점에서 인간의 의사표시나 행위와 동가치한 것으로 다루기 어려운 문제를 입법적으로 해결하고 있다.

UCITA는 청약에 대한 승낙이라고 할 수 있는 상황에서 작동하는 전자 에이전트의 작동에 의해서 계약이 체결되지만, 그 작동이 사기나 전자적 오류에 기인한 경우에는 법원이 적절한 구제수단을 부여할 수 있음을 원칙으로 하고 있다. 그러나 전자적 오류에 관해서는 별도의 조문을 두고 있다. (213,214조)

전자대리인을 통한 계약체결이 인정되지만 그 방법은 반드시 의사표시를 전자 에이전트가 행하는 것뿐만 아니라 전자대리인으로 하여금 이행하게 하거나 이익을 제공하게 하거나 청약자가 계약의 목적인 사용이나 정보의 접속을 할 수 있게끔 컴퓨터를 조작하는 것도 계약체결의 구체적인 방법으로 인정된다.

전자 에이전트는 배후의 사람이 프로그래밍 등의 방법으로 반응할 수 있는 범위를 제한하는 것이 일반적이다. 예를 들어 청약으로 하는 사이트를 만들어 청약을 받는 경우에, 프로그래머가 기입을 할 수 있도록 프로그래밍한 내용이나 사항

만을 기재할 수 있도록 하고 있어서 그 외의 사항에 대해서 기재를 하더라도 컴퓨터가 그 사항을 인식하지 못할 것이라는 것을 알면서도 당사자가 그러한 행동을 취하는 경우에는 승낙이 있는 것으로 다루고 있다.

전자 에이전트는 개인에 의한 검토나 행위 없이 전자기록이나 수행에 대응하기 위한 행위를 시작하기 위해 독자적으로 이용되는 컴퓨터 프로그램 혹은 전자 및 다른 자동화된 수단을 의미한다.

107(d) : 전자 에이전트를 이용하여 동의의 의사표시를 선택한 사람은 에이전트의 수행결과에 종속된다.

동의의 표시 : 동의의 표시는 다음과 같이 수행될 수 있다.

행위에 의한 동의 : 개인이 의도적으로 행위에 참여하거나 계약서를 작성함으로써 상대방측과 전자 에이전트가 해당 기록과 조건에 동의한다는 행위나 계약서로부터 유추할 수 있다는 것을 알고 행동이나 계약에 참여하는 행위를 말한다.
전자 에이전트에 의한 동의 : 만약 전자 에이전트가 기록이나 조건을 검토하고 해당 기록과 조건을 받아들일 환경인지를 확인할 기회가 제공된 이후에 동의가 이루어질 수 있다. 전자 에이전트는 비록 합리적으로 전자 에이전트를 기록이나 조건에 반응할 수 있도록 설정할 수 있는 방식으로 가능할 때에만 기록과 조건을 검토할 기회를 갖는 것으로 간주된다.

해당 조항들은 너무 복잡하다는 평가를 받는다. 많은 이들은 행위에 의한 동의만으로 충분하다고 여기고 있다. 계약이 성립될 수 있는 상황과 관련된 조항들로는 다음과 같다.

(1) 에이전트의 상호작용에 의한 경우

(2) 에이전트와 개인의 상호작용에 의한 경우

(1)과 관련해서 “전자적인 실수(electronic mistake)” 개념이 존재하나, (2)에는 존재하지 않는다.

5) 캐나다의 Uniform Electronic Commerce Act

전자 에이전트의 정의는 전자 에이전트는 개인에 의한 검토나 행위 없이 전체 혹은 부분적으로 전자기록이나 수행에 대응하기 위한 행위를 시작하기 위해 독자적으로 이용되는 컴퓨터 프로그램 혹은 전자 및 다른 자동화된 수단을 의미한다.

전자에이전트와 자연인 혹은 전자에이전트 상호간의 상호작용에 의해 계약이 성립할 수 있다. 비록 계약 당사자들이 다른 방식으로 동의하였더라도, 청약이나 청약에 대한 수락 혹은 계약 성립에 중요한 다른 문제들은 표현될 수 있다.

(a) 전자문서의 방식으로 표현될 수 있다.

(b) 컴퓨터 스크린 상에 위치한 적절하게 지정된 아이콘에 대한 클릭과 터치 등 전자양식에 대한 행위나 청약, 수락 등을 표현하기 위해 고안된 기타 전자적 통신수단을 통해, 표현될 수 있다.

독일법에서는 전자에이전트의 법적 문제를 연소자의 제한된 계약능력의 특성과의 상호 비교 하에 정의를 내리기도 했다. 또 한편으로는 전자적 인간(ePerson) 개념을 창출함으로써 전자 에이전트가 자연인이나 법인에 대한 대안으로서 제시하기도 했다. 전자적 인간 개념을 제안한 이들은 전자적 인간이 새로운 유형의 법적 주체로 기업이 등록을 하는 것처럼 에이전트들도 등록부를 만들어야 한다고 주장하고 있다.

민법 상 계약 능력을 갖춘 계약의 주체는 자연인과 법인을 포함하여 오직 사람(person)만이 될 수 있다. 하지만 계약 능력이 없는 사람들도 존재하므로, 무조건 계약능력이 부재가 인격의 부재와 동일시되는 것은 아니다. 계약은 청약과 동의 혹은 수락과정으로 이루어진다. 일반적으로 계약능력을 가진 인간의 능력은 동의 혹은 수락과정과 관련이 된다. 자동 에이전트를 이용한 계약의 법적 문제는 기계가 동의의 능력을 갖느냐, 기계의 동의행위가 법적 효과를 낳을 수 있는가가 문제가 된다. 법적으로 동의(consent)는 개인의 자유의지에 의해 수행되어야 한다.

전자 에이전트에 있어서의 문제점은 계약을 위한 동의가 자유의지에 의해 이루어졌다는 것을 증명할 수 있는가의 문제이다. 문제는 에이전트가 수행하는 계약행위의 자동성(automation)이 아니라 자율성(autonomy)의 문제이다. 즉, 계약이 자동적으로 수행되었는가가 아니라 계약자의 자유의지에 따라 자율적으로 이루어졌는가의 문제이다.

기계는 아무리 지능적인 기계, 혹은 지능적인 에이전트(Intelligent Agent)라고 하더라도 법적 주체(legal person)가 못되므로 이러한 문제가 발생한다. 기계가 법적 주체는 될 수 없다는 것은 명확하다면 그 다음의 문제는 기계를 대리인으로 상정한 대리인법의 문제로 넘어간다. 즉, 권한의 위임과 관련된 문제이다. 대리인은 타인의 법률관계를 변화시킬 권한을 가지고 있는 사람을 말한다. 민법에서도 대리인은 법에 의해서 어떤 사람으로부터 법적 권한을 이전받은 사람을 말한다. 대리인은 위임받은 한계 내에서 계약능력을 가지게 되지만, 권한이 아예 없는 것이 아니며, 이러한 권한 유무는 인간성의 부재와는 직접적인 관련이 없다.

전자 에이전트가 대리인으로 인정될 경우 전자 에이전트의 책임은 없고, 에이전트 이용자와 계약 상대방 간에 위험의 적절한 배분만이 문제가 된다. 자치와 학습능력의 증가로 인해, 중개자의 이용에 따른 위험의 배분은 더욱 더 중대한 이슈가 되고 있다. 다양한 논문에서 말하고 있는 것처럼 전자 에이전트를 대리인으로 간주하는 접근방법이 가장 적절한 것으로 인정되고 있다. 일반적으로 에이전트는 자신의 실수에 책임을 질 수 없으므로, 기술적이고 법적 해결책들에 의해 전자 에이전트에 의한 계약문제의 해결책이 모색될 필요가 있다.

에이전트의 권한은 전자서명에 의해 정의될 수 있다. 이 전자권한으로서의 전자서명은 신분인증과 함께 권한인증, 속성인증까지 다 포함해야 한다. 만일 중개자가 자신의 권한 범위 안에서 행동하는 한, 그 이용자는 해당 계약 결과물에 종속된다. 그렇지 않으면, 계약 상대방은 위험을 안게 된다. 반면, 그러한 규제가 양자간의 균형을 충분히 유지할 수 있는지는 명확하지 않다. 예를 들어 전자 중개인의

사기나 조작 사건을 처리하기 위한 추가적인 규제들이 필요하게 될 수 있다.

전자 에이전트 방식의 계약의 문제점은 다음과 같다. 계약 상대편은 에이전트가 제대로 작동하지 않았고, 결함이 있다고 주장함으로써 전자계약의 의무 이행을 거부하려는 경우가 발생할 수 있다. 또한 이러한 위험이 발생할 경우에 위험에 누구에게 어떻게 할당되는가의 문제도 발생할 수 있다. 예를 들어 프로그래머에게 그 책임이 주어지는가? 아니면 이용자에게 그 위험에 대한 책임을 물어야 하는가? 의 문제가 존재한다.

보통법상에서 실수나 무의식 원칙 혹은 오류나 악의의 원칙이 적용될 수 있다. 예를 들어 전신의 전송도중의 오류에 의해 야기된 실수의 유비를 들 수 있다. 이 경우 합리적이지 못한 인간에 의해 그러한 변화가 야기되었을 경우, 제공받은 자가 변화가 만들어졌음을 알 수 있을만한 근거가 없는 경우 등을 들 수 있다. 이 경우 판단은 갈리게 되는데, 코빈은 실수의 위험이 보낸 사람이 책임을 져야 한다고 보고 있다.

이러한 문제들 때문에 전자 에이전트들이 충분한 보안과 적절한 기능, 그리고 신뢰성을 제공하는지에 대한 요구사항이 발생한다. 또한 가장 기본적인 문제 중의 하나는 이러한 자동 에이전트에 의한 계약행위들이 많은 경우 이용자들이 언제 어떻게 이루어지고 있는지 알 수 없다는 것이다. 이 때문에 이용자들은 걱정과 불안감을 갖게 된다. 이러한 걱정과 불안감을 해소시키고 신뢰감을 높이기 위한 다양한 수단들이 존재하는데, 이러한 대책들로는 에이전트들을 위한 인증시스템(Certification System)과 보안검증(Security Verification), Lerouge가 제안한 레이블링 시스템(Labeling System) 등을 들 수 있다.

이중에서 인증 시스템이란 Karnow가 제안한 것으로 에이전트를 위한 인증시스템을 도입하여 인증을 받은 에이전트들만 사용될 수 있도록 하는 시스템을 말한다. 보안 검증 (Security Verification)이란 보안 표준에 대한 레퍼런스를 통한

보안 분류와 전자 에이전트의 인증을 개발하는 것을 말한다. 따라서 전자 에이전트의 보안 특성에 대한 독립적인 검증 테스트 시스템을 개발하는 것을 목표로 한다.

지금까지 사물통신의 응용 중 하나로 살펴본 자동 에이전트에 의한 계약행위의 문제를 통해 사물통신에서 발생할 수 있는 법률관계의 일면을 살펴볼 수 있었다. 즉, 사물 간에 이루어지는 통신이지만, 결국 그 결과의 영향이 사람에게 미치게 되며 사물들은 단순히 인간의 의사를 반영하여 대리하는 대리자에 불과하며 사물통신의 책임을 직접 지게 되는 경우가 발생한다는 것이다.

이처럼 자동 에이전트의 통신은 사물통신에서도 높은 수준의 법적 효과가 요구되는, 또한 높은 수준의 책임성이 요구되는 부문이라고 할 수 있다. 따라서 필수적으로 인증기술은 높은 수준의 인증이 요구되며, 자동 에이전트의 계약행위와 관련된 제반 행위에 대하여 부인방지 기능을 제공해야 할 필요가 있다.

2. 사물통신에서의 책임 귀속의 문제

사물통신 인증의 특수성은 인증 대상과 인증 효과 면에서 그 특수성이 존재한다. 즉, 기기 자체에 대한 인증인가, 아니면 소유하는 사람에 대한 인증인가 여부와 인증의 효과가 누구에게 어느 정도로 미치는가에 대해 사람 통신에서의 인증과 확연히 구분된다.

앞서 전자 에이전트의 예를 통해 살펴본 것처럼, 현실적으로 전자 에이전트가 사물통신을 통해 대리인으로서 수행된 계약 등의 능력은 인정되고 있지만 그 결과와 영향은 사람에게 귀속되며, 그 책임 또한 사람에게 귀속됨을 알 수 있다. 비단 계약이 아니더라도 사람의 의사가 반영되는 자동화된 지능형 사물들의 통신의 결과가 사람에 귀속되고 그 행위의 책임이 사람에게 귀속되게 된다.

사물통신 인증에 있어서도 법적 효과가 나타나지 않고 법적 책임을 물을 수 없다면 입법화를 고려할 필요가 없다. 사물은 법의 대상이 되지 않기 때문이다. 오로지 인간과 관련되는 한해서 사물은 법의 대상이 되지만 법적 주체는 되지 못한다. 동물 또한 사물에 준하여 취급되며 따라서 법의 대상이 되지 않는다. 법은 사물의 소유주, 사물의 관리권자, 동물의 소유주와 동물의 관리권자를 관리소홀 등의 이유로 처벌하지 사물 그 자체를 처벌하지 않는다.

또 한편으로 계약관계는 존재하지 않더라도 자신의 소유 및 통제하의 장치가 타인에게 불법행위를 구성할 경우 누구에게 책임을 물을 수 있는가의 문제가 존재한다. 앞서 설명했던 사물은 동물과 마찬가지로 법률 주체가 될 수 없으므로 책임 귀속의 주체가 될 수 없다. 따라서 동물이 타인에게 침해를 입히고 불법행위를 저질렀을 경우, 동물의 주인이 그 불법행위나 피해의 책임을 대신 관리자의 입장에서 지게 되는 것처럼 사물의 주인이 그 불법행위나 피해의 책임을 져야 하는 것이다. 즉, 개를 키우는 사람에게 개가 사람을 물어 죽였을 경우에 미치는 귀속 문제라고 할 수 있다. 예를 들어 최근 판례에서 애완견 관리 소홀로 사람에게 피해를 입히게 한 애완견 주인들에게 형사상 책임(벌금 5백만 원)과 민사상 책임(치료비와 위자료 7백50만 원)을 물어 공동생활의 질서 유지의 책임을 지운 바 있다. 즉, 이처럼 기기에 의한 피해에 대한 관리책임을 어느 정도까지 주인에게 물릴 수 있는가의 문제가 존재한다. 원격진료 사고 발생 시의 책임 귀속 문제는 매우 심각하고 중요한 문제이다.

따라서 인증의 목적이 통신의 기밀성과 신뢰성을 보장하는 한편 문제 발생 시 책임을 추적할 수 있는 목적이라고 할 수 있다면, 법적 책임의 주체가 될 수 없는 사물의 식별이 아닌 법적 책임을 질 수 있는 책임자에 대한 식별과 인증이 가장 중요하게 된다. 따라서 사물의 인증은 사물 자체에 대한 인증 보다는 사물 관리 책임을 지게 될 혹은 계약 주체인 사람을 인증하는 것이 되어야 한다.

어쨌든 중요한 것은 이러한 의사결정을 하는 것, 인증할 것인지 말 것인지, 인

증이 되었다면 그에 근거하여 어떠한 일을 할 것인지를 결정하는 주체가 인간이 아니라 기계라는 점이다. 인증에 의한 의사결정이 인간의 인식이 배제된 기계의 내부 알고리즘에 의해 의사 결정되고 처리된다면 그렇게 인간의 인식이 배제된 결정 행위로 인해 발생한 문제에 대하여 소유주 혹은 통제권자가 책임을 져야 하는가의 문제가 존재한다. 따라서 알고리즘을 만든 제조사 측의 책임과 소유주의 책임간의 책임귀속 문제는 뜨거워 질 수 있다.

또한 사물의 소유주 및 관리자는 합리적인 수준의 관리조치를 취했는데 사고가 발생했을 경우의 과실 책임과 사물 자체의 본질적 문제 때문에 과실이 발생했을 경우의 책임 문제도 존재한다. 이럴 경우는 누구에게 책임을 둘 것인가? 사물 자체는 책임주체가 될 수 없기 때문에 원인에 따라 하드웨어 개발업체, 소프트웨어 개발업자, 서비스 업자 등이 제조물 책임법 등에 의거하여 책임을 질 수 있다.

특히 지능형 사물의 성격과 수준이 계속 진화하면서 특정 디지털 디바이스의 작동결과가 인간에 귀속되어야 하는 법리가 새로운 차원으로 논의되어야 할 것으로 보인다. 어느 정도 수준에서 어느 주체로 귀속이 되어야 하는 것인가의 문제이다. 예를 들어 인공지능의 수준이 지속적으로 발달하면서 인간의 의사나 판단이 최소화되고 있는 상황에서 그들의 인공지능을 통한 판단 및 행위의 결과물에 대해 인간에게 귀속할 수 있는지에 문제는 향후에도 지속적으로 나오게 될 것이다.

지능형 사물의 판단 및 행위의 결과물의 인간으로의 귀속 문제는 어떤 주체에게 귀속되어야 하는가의 문제가 존재하는데, 이러한 귀속주체가 될 수 있는 주체들은 다음과 같다.

- 하드웨어 제조업체
- 소프트웨어 제조업체
- 소유주
- 관리자
- 실제 행위에 대한 결과물을 가져가는 기타 주체

또 하나의 문제점은 공무원과 같은 인간이 배제된 공공 디바이스들의 인증과 판단으로 인해 발생한 행위들을 공무에 준하는 법적 행위로 볼 수 있는가의 이슈가 존재한다. 즉, 공공 디바이스에 의해 자동으로 수행되는 공무행위들을 공무원의 적법한 권한에 의해 수행되는 것으로 볼 수 있는가 하는 문제이다. 또한 이러한 권한에 의해 수행되는 공공 디바이스의 수행 결과물에 대한 책임을 관리 공무원이 질 것인가의 문제가 존재한다. 예를 들어 공공 디바이스의 오작동으로 인해 교통체계가 마비되고 교통사고를 야기하게 되었다면 그 책임이 관리 공무원에게 존재하게 되는가 하는 문제이다. 즉, 공공 디바이스의 행위성의 문제와 책임성 문제는 사물통신 문제의 핵심적인 문제 중의 하나라고 할 수 있다.

결국 사물통신에서 사물은 법적 주체가 될 수 없고, 책임귀속 주체도 될 수 없으므로, 사람이 사물통신의 결과에 대한 책임을 지게 된다. 먼저 계약관계를 발생시키는 유형의 사물통신의 경우 사람의 의사가 반영된 계약서의 내용만큼의 직접적인 책임을 지게 되며, 이외의 사물통신에서 발생하는 고의적이지 않은 불의의 피해나 불법행위의 책임은 사람이 관리소홀의 책임을 지게 된다. 결국 사물통신은 사람의 의사가 반영되고 사람에게 영향을 주는 한 사람에게 그 책임이 전가된다.

제 4 절 사물통신에서의 정보보호와 인증

사물통신에서의 프라이버시 문제나 보안 문제와 같은 위험들을 최소화하고 이런 위험 발생 시에 적절하게 책임 귀속 문제를 처리하여 사물통신의 신뢰성과 안전성을 보장함으로써 사물통신의 지속가능한 발전을 보장할 수 있어야 한다. 따라서 사물통신 기반망 혹은 사물통신 과정에서의 정보보호에 대한 요구가 높아지고 있다.

정보보호는 조직이 가지고 있는 자산의 기밀성, 무결성, 가용성을 보장하는 것으로 정보보호의 가장 기본적인 메커니즘은 접근통제라고 할 수 있다. 접근통제는 특정 주체의 접근으로부터 객체의 기밀성, 무결성, 가용성을 보장하기 위한 것이다. 일반적으로 접근통제는 해당 주체를 식별(identification), 인증(authentication), 권한을 부여(authorization)하는 일련의 행위라고 할 수 있다. 식별-인증-권한부여는 동일한 과정으로 보이지만 엄격히 논리적으로 분리된다.

식별(identification)이란 사용자가 시스템에 유일한 식별자로서 자신의 신분을 제시하는 과정을 말한다. 책임추적성이란 사용자의 시스템 내에서의 행동을 기록하는 것으로 식별자를 이용하여 기록이 수행된다. 인증이란 사용자가 식별과정을 통해 제시한 신분이 타당한가 여부를 확인하는 과정이라고 할 수 있다.

인증(Authentication)이란 어떤 사람이나 사물이 실제로 신고된 바로 그 사람(또는 바로 그 것)인지를 판단하는 과정이다. 개별 또는 인터넷을 포함한 공공 네트웍에서의 인증은 대개 로그온시 암호의 사용을 통해 이루어진다. 암호를 알고 있는 사람은 일단 믿을만한 사용자라고 간주된다. 모든 사용자는 처음에 자신이 원하는 암호를 등록하고, 이후 계속 사용할 때마다, 사용자는 이전에 신고된 암호를 잊지 않고 사용해야만 한다. 그러나, 자금 교환 등이 수반되는 중요한 거래에서 이 시스템의 약점은, 암호가 종종 도난 당하거나, 우연히 알려지거나 또는 잊혀질 수 있다는데 있다. 이러한 이유 때문에, 인터넷 비즈니스와 많은 다른 거래들에서

는 좀더 엄중한 인증 과정을 필요로 하는 것이다. 공개키 기반구조의 일부인 인증기관에 의해 발급되고 검증된 디지털 증명의 사용은 인터넷 상에서 인증을 수행하는 표준적인 방법이 되어가고 있다. 필연적으로, 인증은 권한부여에 우선한다[54].

권한부여(Authorization)는 누구에게 무엇을 할 수 있거나, 가질 수 있는 권한을 부여하는 과정이다. 다중 사용자 컴퓨터 시스템에서, 시스템 관리자는 어떤 사용자가 그 시스템을 액세스할 수 있는지, 그리고 부여된 사용권한은 어디까지인지(파일 디렉토리의 접근 범위, 허용된 액세스 시간, 할당된 저장 공간의 크기 등)를 그 시스템을 위해 정의한다. 어떤 사람이 컴퓨터 운영체계나 응용프로그램에 로그온 했을 때, 그 시스템이나 응용프로그램은 그 세션 동안 그 사용자에게 어떤 자원의 이용을 허락해야하는지 확인한다. 그러므로, 권한부여는 때로 시스템 관리자에 의해 미리 설정되는 권한들과 사용자가 액세스를 해 왔을 때 미리 설정된 권한을 실제로 확인하는 일 모두를 지칭하기도 한다[55].

특별히 전자서명법 상의 인증의 개념은 전자서명을 생성하기 위하여 이용하는 전자적 정보인 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말한다. 인증서는 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 전자적 정보를 말하며, 이러한 전자적 정보를 공인인증기관이 발급할 경우 공인인증서라고 한다. 즉, 공인인증서는 제3의 기관이 통신 당사자들의 신원을 보증해주는 시스템이라고 할 수 있다.

사람 대 사람의 통신과정에서의 정보보호와 신뢰성과 관련된 법률로는 이미 정보통신망 이용촉진 및 정보보호에 관한 법률이 존재하는데 반해, 사물통신에서의 신뢰성과 안전에 관해서는 규율하고 있는 법률이 없는 상황이다.

---

54) http://www.terms.co.kr/authentication
55) http://www.terms.co.kr/authorization.htm

1. 사물통신에서의 인증정책

사물통신이 가능해진 것은 사물의 지능화와 사물의 네트워크화 때문에 발생한다. 따라서 사물지능통신이라는 발생하게 된 것이다. 사물이 네트워크화 되면서 사물과 사물 간에 상호작용해야 하는 일이 발생하기 때문이다. 따라서 또한 사물통신망에서 대한 정보보호와 책임귀속 해결을 위한 핵심적인 메커니즘으로 효과적인 인증 기술이 요구되고 있다. 사물들 간의 상호작용을 위해서는 서로를 식별하고 인증하는 과정을 통해 신뢰할 수 있는 대상으로 인정한다면 권한부여 과정을 통해 지정된 수준만큼의 정보를 주고받는 일련의 과정을 수행하게 된다.

사물통신 인증에서 인증은 두 가지 관점에서 가능하다. 첫째, 정보보호 관점의 개체 식별과 관련된 인증과 둘째, 특정 자격을 가지고 있음을 검증하고 확인해주는 인증의 의미를 동시에 가지고 있다. 첫 번째 것은 통신 대상인 지능형 사물의 신원에 대한 인증(authentication)을 말한다. 즉, 상대방 사물이 내가 통신하려고 하는 대상이 맞는지 인증하는 것을 말한다. 또 하나는 상대방 사물이 문제가 없는 정상적인 통신 대상인지를 인증(certification)하는 것을 말한다. 즉 상대방 사물 제품이 규격이나 기술 기준에 의한 인증과 서비스에 대한 인증을 통과하였는지 여부를 파악하는 것이다. 제품과 서비스에 대한 형식승인과 품질인증이 이러한 인증에 해당된다.

앞서 살펴본 것처럼 사람 통신의 경우 통신참여자가 직접 법적 책임을 지기 때문에 향후 문제발생 시에 책임 귀속이 확실한 반면 사물통신에서는 사물 자체는 책임을 질 수 없기 때문에 책임을 질 수 있는 주체들을 식별할 수 있도록 하는 것이 중요하며, 단순히 주체들을 식별뿐만 아니라 이들의 신뢰성을 확보하게 하는 것이 중요하다.

이러한 신뢰성 확보 방식으로는 서비스 및 제품의 보안성 검토 등 여러 가지 방식이 존재할 수 있을 것이다. 즉, 내가 접근하려고 하는 사물이 과연 그 사물이 맞는지와 관련된 동일시의 문제와 그 사물이 과연 신뢰할 수 있는지에 대한 것이

다. 따라서 부인방지와 권리, 의무 귀속과 같은 법적 효력적 인증을 핵심대상으로 하는 인증과 정보보호 분야의 핵심적 기술 및 서비스표준 인증 및 품질인증과 같은 인증을 모두 포괄하여 논의될 필요가 있다.

사물통신 인증정책이 사물통신 시스템의 신뢰성을 진정으로 보장해주기 위해서는 따라서 다음과 같은 세 가지에 대한 인증이 수행되어야 할 것으로 생각된다.

첫째, 누구 소유인가? 혹은 누구의 통제 하에 있는가?

이는 통신내용에 누구의 의사가 반영되는가에 대한 내용으로 책임을 부여하기 위한 핵심적인 요소라고 할 수 있다. 즉, 사물 인증이지만 사람에 대한 인증요소도 필요하게 될 수 있다.

둘째, 누가 만든 제품인가?

사물통신의 신뢰성을 보장해줄 수 있는 하나의 요소이자, 제조물 책임법이나 기타 제품 자체의 오류로 인한 법률적 책임을 묻기 위한 핵심 요소라고 할 수 있다.

셋째, 안전한 제품인가?

이는 기존의 인간이 개입한 통신에서는 그다지 보장할 필요가 없는 인증요소라고 할 수 있다. 이러한 신뢰성과 안전성을 확인하는 과정이 인증과정에서 수행되어야 하는지, 통신을 위한 협상(negotiation) 과정에서 수행되어야 하는지는 확실하지 않지만, 인증과정 뒤의 권한부여를 위해서는 선행되어야 할 과정이라고 할 수 있으므로, 이러한 협상 과정 또한 인증과정의 일부로 포함시킬 수 있을 것이다.

사물통신에서의 인증과정은 위와 같은 모든 정보들이 정확하다는 사실을 신뢰

하는 과정이라고 할 수 있다. 즉, 위와 같은 사실들을 모두 믿을 수 있고 내가 통신할 만한 대상임을 확인했으니 이제 통신을 시작하기 위한 준비가 완료가 되었다는 것이다. 이제 내부적으로 기존의 룰셋이나 협상 과정을 거쳐 원하는 수준의 통신을 수행하면 된다.

예를 들어 개인정보보호 관점에서 사물통신의 인증의 문제는 개인정보자기통제권 부여의 문제이다. 일반적으로 사물통신은 개인정보 협상과 관련한 룰셋을 세팅함으로써 개인이 원하는 수준 내에서는 개인정보를 가져갈 수 있도록 제공할 것으로 동의(consent)했다는 것을 전제로 한다. 이러한 동의를 전제로 하여 자동에이전트에 의한 개인정보 제공 협상을 인정하고 적법하게 제공하기 위한 근거를 마련하고 있다.

하지만, 근본적으로 사물통신 과정과 협상의 시작과 진행과정을 개인이 인지할 수 없기 때문에 적절하게 개인이 자기정보통제권을 확보할 수 없다는 문제점이 존재한다. 따라서 사물통신과정에서 개인의 자기정보통제권을 어떻게 확보할 것인지에 대한 대책이 마련될 필요가 있다.

2. 사물통신 신분인증 정책

사물 간 통신의 인증에서 가장 중요한 것은 바로 가짜 사물(Rogue Machine)을 없애는 것이라고 할 수 있다. 서버와 클라이언트 혹은 P2P 상황에서 서버가 클라이언트를 클라이언트가 서버를 기기가 기기를 인증하는 상황에서 악의적인 가짜 머신을 걸러내는 것이 인증의 가장 큰 목표가 되어야 한다. 악의적인 머신의 문제점은 사물과 사물간의 통신행위에 있어서 법적 책임을 물을 수 없는 상황이 된다는 점에서 특히 중요하다. 악의적인 머신이 존재하지 않는 상황이라면 정당한 머신들이 자신을 서로에게 확인시키며 그에 기반한 통신을 진행하면 충분하다. 가짜 머신들에 의한 악의적인 통신 및 행위가 발생할 경우가 문제가 발생하게 된다.

따라서 사물통신에 참여하는 일방의 인증이 아닌 사물통신 참여 기기 상호간의 인증이 기본적으로 전제가 되어야 한다. 즉, 기기 상호간, 기기와 서버 간 통신을 위한 인증은 상호간에 인증할 수 있어야 한다. 이러한 쌍방향 인증은 일반적으로 서버와 클라이언트 간의 통신에 있어 클라이언트가 서버를 인증하고, 서버가 클라이언트를 인증하는 것을 전제로 하고 있다.

현상적으로는 법률관계를 내포하고 있지 않지만 실제 통신과정에서 혹은 해당 시스템들 중 일방에서 문제가 발생했을 경우 이러한 피해에 대하여 원인을 분석하고 책임귀속 주체를 찾는 목적으로 사용될 수 있기 때문에 결국은 법적 행위로서의 일면을 가지고 있다고 할 수 있다.

인증의 목적의 또 다른 한 측면은 바로 접근통제를 위한 것이다. 적절한 사람에 의해 접근되고 있는지, 적절한 사람이 자신의 권한에 맞는 행위를 하고 있는지를 검사하는 것이다. 또하나는 클라이언트의 입장에서 서버를 인증하는 것이다. 지금까지 금융서비스 등에서 요구해왔던 것은 대부분의 경우 서버의 클라이언트 인증에 한정이 되어 있었다. 하지만, 실제 피싱 등의 Rogue Server를 이용한 공격들이 늘어나면서 이러한 가짜 서버들에 대응하기 위한 클라이언트의 서버 인증의 중요성이 높아지고 있다. 즉, 내가 특정 서비스를 받기 위해 접근한 서버가 과연 내가 접근하려고 하는 바로 그 서버가 맞는지를 인증하는 것을 말한다.

3. 사물통신 성능 및 자격 인증 정책

방송통신위원회는 사물지능통신을 향후 미래 정보화의 핵심 기술 기반으로 규정하고 있으며, 사물지능통신을 진흥적 규율의 대상으로 삼고 있다. 이 때문에 사물지능통신에서는 표준화, 상호운용성 확보, 기반망 구축, 응용서비스 확산과 같은 진흥적 목표들이 핵심과제로 제시되고 있는 상황이다. 따라서 사물지능통신의 기반망 및 사물지능통신용 기기들에 대한 품질인증과 형식승인이 필수적으로 요구되고 있는 상황이라고 할 수 있다.

기존의 대면성을 기초로 한 식별과 인증, 신뢰획득 과정은 철저한 비대면성과 비인간성을 특징으로 하는 사물통신에서는 적용될 수 없으므로, 사물통신에서의 인증과정은 유적특징과 개별성을 기반으로 하여 누구 소유의 어느 사 제품인지, 또한 이 제품은 충분한 안전성과 신뢰성을 보장하고 있는지에 대해서도 함께 인증시켜줄 필요가 있을 것이다.

사물통신의 인증과정의 특수성은 기기와 기기의 인증을 위해서는 사람-기기, 기기-기기, 기기-사람 인증을 해야 한다는 점이다. 즉, 인증과정이 한번 더 요구되는 셈이다. 또한 사물 속성 그 자체로는 신뢰할 수 없기 때문에 사물을 둘러싼 제반 정보들을 통해 신뢰를 보여야 하다. 따라서 많은 경우 기기와 기기간의 인증 또한 상호간의 인증만으로는 부족하고 인증정보의 신뢰성을 보증할 수 있기 위한 제3자의 인증이 요구된다고 할 수 있다.

이러한 제3자의 인증에는 공인인증기관에 의한 신분인증은 물론 전파인증이나 전자제품인증과 같은 제품인증, 그리고 보안기능과 관련된 신뢰성 인증 등이 모두 포괄될 수 있다. 결국 인증은 기기의 인증이지만 최종적으로는 책임을 질 수 있는 사람의 인증이 될 수밖에 없다. 기기는 책임의 주체가 될 수 없으며, 기기에게 책임을 물을 수는 없기 때문이다.

1) 정보통신기기인증규칙

제2조 (정의) 2. "정보통신기기"라 함은 「전기통신기본법」 제2조제6호의 규정에 의한 전기통신기자재, 「전파법」 제2조제5호의 규정에 의한 무선설비의 기기와 「전파법」 제57조의 규정에 의한 전자파장해기기 및 전자파로부터 영향을 받는 기기를 말한다.

2) 전기통신기본법

제33조 (형식승인) ① 방송통신위원회가 관계행정기관의 장과 협의하여 정하는 전기통신기자재를 제조 또는 판매하거나 수입하고자 하는 자는 그 전기통신기자재의 형식에 관하여 방송통신위원회의 승인을 얻어야 한다. 다만, 시험·연구 또는 수출용 전기통신기자재 등 대통령령이 정하는 전기통신기자재의 경우에는 그러하지 아니하다.

3) 전파법

제46조 (형식검정 및 형식등록 등) ① 무선설비의 기기를 제작하거나 수입하려는 자는 방송통신위원회가 수행하는 형식검정을 받거나 형식등록을 하여야 한다. 다만, 시험·연구 또는 수출용 무선설비의 기기 등 방송통신위원회 고시로 정하는 무선설비 기기의 경우에는 그러하지 아니하다.

제57조 (전자파적합등록) ① 전자파장해기기 또는 전자파로부터 영향을 받는 기기를 제작하거나 수입하려는 자는 그 기기에 대하여 방송통신위원회에 전자파적합등록을 하여야 한다. 다만, 시험·연구 또는 수출용 무선설비의 기기 등 방송통신위원회 고시로 정하는 기기와 다음 각 호의 어느 하나에 해당하는 기기로서 관계 법령에 따라 이 법에 따른 전자파적합등록에 준하는 전자파장해 및 전자파로부터의 보호에 관한 검정 등을 받은 기기는 그러하지 아니하다.

후자의 인증에 해당하는 인증정책 및 관련 법제들을 살펴보면 다음과 같다.

- 전기통신기본법 상의 형식 승인
- 전파법 상의 전자파적합등록 및 적합 인증
- 건설기술, 교통기술, 전기기술, 환경기술 등 위험물 관련 분야의 법체계 등 유사입법
- 공간정보산업법, ITS법 등 정보분야의 표준인증 및 품질인증
- 국가표준기본법 및 산업표준화법 등의 제품인증 및 품질인증 관련 기본법
- 부품, 소재전문기업 등의 육성에 관한 특별 조치법 : 신뢰성 인증 관련 법률

4. 사물통신 인증 지원 정책

사물통신의 인증은 사물통신의 신뢰성과 안전성 보장을 통한 지속가능한 사물통신 산업의 발전을 보장해줄 수 있는 중요한 기술이다. 이러한 인증 기술 및 인증 정책의 효과를 배가시켜 신뢰성을 더욱 강화하기 위해서는 효과적인 사물통신 인증 지원 정책이 제시될 필요가 있다. 또한 이러한 정책은 사물통신 인증 관련 법제에서 의무화함으로써 그 효과를 보장할 필요가 있다.

이러한 효과적인 사물통신 인증 지원 정책으로는 인증내역 증거보존 의무화, 사물통신 인증 방법 평가위원회 구성, 사물통신 인증방법 수립 정책 기준 마련 등을 들 수 있다.

가. 인증 내역 증거보존 의무화

실제 책임여부를 확정하기 위해서는 인간이 개입하지 않은 사물통신에서의 증거 보존이 핵심적이다. 즉, 인간은 통신이 이루어진 사실이나 통신 내용에 대해 인지할 수 없으므로, 통신상에서 문제가 있었는지 여부도 인지할 수 없으며, 단지 그 영향을 받게 될 뿐이다.

따라서 사후적으로 자신이 어떠한 문제로 그러한 영향을 받게 되었는지 증명하기가 쉽지 않다. 때문에 인증 내역이 기록, 보존되고 계약적 성격을 갖는 민감하고 심각한 통신의 경우에는 통신 내역을 기록하고 보존하도록 요구하는 것이 좋을 것이다. 이를 통해서 신뢰할 수 있는 사물통신망을 구축할 수 있을 것이다.

또한 기술적인 대안으로서의 디지털 포렌식 기술, 인증내역 아카이빙 기술 및 소형기기용 경량형 블랙박스 기술에 대한 연구도 함께 진행될 필요가 있을 것이다.

나. 사물통신 인증방법 평가위원회 구성

새롭게 등장하는 사물통신 인증기술들에 대하여 특정 유형의 사물통신에 적합한 수준의 안전한 인증방법인지를 테스트하고 평가할 수 있는 공신력 있는 평가위원회가 구성되어 운영될 필요가 있다. 인증방법 평가위원회는 인증기술들의 보안성 수준을 분류하여 해당 수준에 맞는 평가항목들을 개발할 필요가 있으며, 이러한 인증방법 평가위원회를 통과하여 인증필을 받은 인증기술들만이 해당 장비의 수준에 맞추어 사용될 수 있도록 해야 한다.

다. 사물통신 인증방법 수립 정책 기준 마련

앞서 설명했던 대로 사물통신의 인증은 한 가지 방법을 강제하는 것이 아니라 사물통신 인증 수준은 해당 통신이 어떤 컨텍스트에서 사용되는가에 따라 다르게 규정될 필요가 있다. 사물통신 인증에서 중요한 것은 보호받아야 할 통신과 보호가 필요 없는 통신을 명확히 구분하여 적절한 수준의 인증기술을 제안하는 것이 필요하다는 점이다. 사물통신 인증 방법의 수준을 분류하는 기준은 다음과 같다. 사물통신 인증방법을 결정할 때에는 아래와 같은 기준들을 검토한 후 그 수준을 결정할 필요가 있다.

(그림 39) 사물통신 인증방법 수립 기준

사물통신 인증방법 기준은 위의 그림과 같이 왼쪽의 기준들을 통하여 사물통신에 대한 구분을 한 후 해당 특성에 맞게끔 오른쪽의 사물통신 인증요구사항의 구현 수준을 정함으로써 이루어질 수 있다. 특히 사물통신 구분기준에 따라 사물정보의 민감도가 높거나 생명, 건강에 피해를 주는 경우, 법적 권리가 심각하게 침해되거나 경제적인 손해가 심한 경우 등에는 오른쪽의 인증 수준이 전반적으로 높게 요구될 것임을 알 수 있다.

1) 사물통신 구분 기준

가) 사물정보의 민감도

취급하는 정보가 개인정보에 해당되는가, 혹은 기밀정보인가에 따라 해당 사물통신의 의미는 달라진다. 따라서 사물정보가 사람의 민감한 정보를 포함하는가, 사람과 결합되어 개인정보로서 인정되어 법적으로 보호받는가에 따라 인증방법의

수준은 달라져야 한다.

나) 통신 결과의 심각도

사물통신의 결과가 사람에게 어떤 영향을 미치게 될 경우, 그 결과의 영향이 어떠한 성격이며, 어느 정도의 심각도가 예상되는가에 따라 인증방법의 수준은 달라져야 한다. 예를 들어 사람의 생명이나 건강에 영향을 주거나, 계약이나 법집행 등 사람의 권리와 의무에 영향을 주게 될 경우, 또한 과금서비스 등 사람에게 경제적인 피해를 주게 되어 경제시스템의 불신을 야기할 것이라고 기대될 경우에는 높은 수준의 책임성과 인증을 요구할 필요가 있다.

① 생명이나 건강에의 영향

사물통신의 결과 및 효과가 개인의 생명이나 건강에 영향을 미칠 정도로 심각하다면 당연히 높은 수준의 책임성과 그에 준하는 높은 수준의 인증이 요구된다고 할 수 있다. 예를 들어 원격진료법이 만들어지고 원격진료가 본격화되면서 의료 분야에서 에이전트 사용이 본격화되면, 원격의료를 위한 디바이스와 병원 서버 간 통신과정에서 오류가 발생하게 되는 경우 환자의 인명과 건강에 심각한 위험을 가할 수 있게 된다는 문제가 발생한다. 따라서 이러한 경우에는 책임성이 핵심적인 요소이며, 이를 보장할 수 있는 인증이 요구된다.

② 법적 권리에 미치는 영향

개인의 프라이버시 침해나 재산권 침해, 업무 방해, 그 외의 기타 타인의 법적 권리를 침해하게 되는 경우를 말한다. 이러한 불법행위의 책임은 사람이 의도하지 않았던 의도하지 않았던 통제권한이나 소유권이 있는 사람이 책임을 지게 되므로 이러한 책임관계를 명확하게 규명하기 위해서는 높은 수준의 인증이 요구된다고 할 수 있다.

③ 과금 서비스 존재 유무

과금 서비스가 존재하거나 텔레메트리로 전송되는 사물정보가 전력사용량처럼 돈과 관련되어 있는 것이라면 다는 것은 해당 사물통신의 결과는 개인의 재산권에 영향을 미칠 수 있다. 이러한 부분은 사람에게 심각한 영향을 미칠 수 있는 민감한 요소이므로, 과금 서비스나 경제적인 부분과 연관되는 부분들은 이에 걸맞는 인증이 요구된다고 할 수 있다.

다) 서비스/기능의 중요도 : 정보통신기반시설 지정 여부 등

많은 경우 사물통신이 적극적으로 사용되는 영역 중의 하나는 SCADA 시스템으로 알려져 있는 제어시스템의 통신네트워크이다. 이러한 제어시스템이 주로 활용되는 국가정보통신기반시설에 해당되는 제어시스템과 관련된 보안은 행정안전부의 통신기반보호법에 의해 높은 수준으로 보호되어야 하므로, 이 법에서 준하는 보호와 인증수단이 제공될 필요가 있다. 또한 사회나 해당 조직에서 가용성과 기능이 핵심적인 역할을 차지하고 있는 기능이나 서비스인 경우에는 높은 수준의 인증이 요구된다.

라) 사람과의 결합도 : 사람 의사 반영도

계약이나 사람들 간의 통신에서 중요한 것은 사람의 의사를 제대로 반영하는 것이다. 이러한 유형의 통신에서는 통신의 내용 및 그 계약 결과물이 그대로 그 의사표명한 개인에게 귀속이 되므로 통신의 정확성과 신뢰성은 매우 중요하게 된다. 따라서 이 경우에도 높은 수준의 인증이 요구된다.

마) 디바이스 환경 : 컴퓨팅 파워와 저장공간

컴퓨팅 파워와 저장 공간의 크기와 같은 지능형 사물의 디바이스 환경과 능력은 인증기술의 효율성을 규정하는데 중요한 요인이다. 이동성이 강조되는 사물통신 환경에서는 컴퓨팅 파워와 저장 공간이 부족한 경우도 많으므로, 이에 적합한 수준의 효율적인 경량의 인증방식을 요구하게 되는 경우가 많다.

바) 조직 환경 : 민간, 공공 여부

또한 공공기관의 CCTV의 경우 폐쇄적인 사물지능통신망을 이용하고 있다는 점에서 법규율의 문제는 민간망에서의 사물통신과 다른 양상을 띠고 있다. 공공부문의 경우 행정 소송 등에 대비하여 엄격한 부인방지 및 책임추적성을 제공해야 하고, 기기에 대한 소유관계 및 통제 관계가 확실하므로 공인인증서 방식이 가장 적당하다고 할 수 있다. 하지만, 이 경우도 엄격하게 공무용으로 사용되는 것으로 한정될 필요가 있으며, 공공기관에서 사용되는 것이라도 대국민 대상의 법률관계를 형성하지 못하거나 조직의 보안문제와 관련이 없는 기기의 활용의 경우에는 공인인증서 방식을 강제화할 필요는 없을 것으로 생각된다.

2) 사물통신 인증 요구사항

사물통신 인증기술이 일반적으로 담보해야 할 특성과 기능 요구사항들은 앞서 살펴본 바와 같다.

가) 디바이스 인증

사물통신 환경에서 통신 서버는 전송 및 수신하고자 하는 데이터가 정당한 사물통신 디바이스 여부를 식별 및 인증할 수 있어야 한다.

나) 서버 인증

사물통신 환경에서 사물통신 디바이스 혹은 게이트웨이는 통신하고자 하는 사물통신 서버가 정당한 서버인지 등의 여부를 식별 및 인증할 수 있어야 한다.

다) 통신 내용의 암호화

사물통신 환경에 따라 이루어지는 통신 내용은 개인정보 및 유출 시 사회적으로 피해가 예상되는 데이터일 경우 반드시 암호화를 통하여 기밀성 및 무결성을 제공해야 한다.

라) 부인방지

과금 등에 있어 사물통신 인증기술은 사물통신 디바이스 사용자 등이 정당한 통신내용을 부인할 수 없는 수단을 제공할 수 있어야 한다. 특히 인증기술 결정에 있어 핵심적으로 고려해야 할 부분 중의 하나가 바로 부인방지 기능을 제공하게 할 것인가 말 것인가 이다.

마) 기타 환경과의 호환성

사물통신 환경에서 사용되는 인증 기술은 기타 도메인 디바이스 등과 호환될 수 있어야 한다.

바) 인증기술의 효율성

사물통신 환경에서의 인증기술은 기존 디바이스에서 사용되므로 성능의 제약 및 기기의 성능의 저하 등을 고려해야 한다. 따라서 모든 디바이스에서 사용될 수 있는 경량화 된 인증기술을 고려하여야 한다.

사) 사용자 개입의 최소화

사물통신 인증기술은 사물통신 환경의 특성 상 사용자의 개입이 최소화 할 수 있는 인증기술을 사용하여야 한다.

제 5 절 사물통신 인증 관련 법률

본 절은 사물통신의 신뢰성과 안전성을 보장하기 위한 핵심적인 메커니즘으로서의 사물통신 인증과 관련된 내용을 규제할 수 있는 사물통신 인증 관련 법률 대안을 모색해보도록 한다. 먼저 사물통신 인증 관련 법률들에 대해 살펴보고, 앞서의 사물통신의 특성과 책임을 중심으로 사물통신 인증 관련 법률의 요구사항들을 살펴봄으로써 향후 사물통신 인증 관련 규율 법제를 만드는데 도움을 제공하고자 한다.

먼저 사물통신 인증 관련 법률들은 크게 전기통신 및 정보통신을 포함한 (사물)통신과 관련된 법률, 직접 사물통신과 관련된 법률, 정보보호를 위한 법률, 신분 인증과 관련된 법률, 성능 및 자격 인증과 관련된 법률 등을 들 수 있다.

1. (사물)통신 및 (사물)통신기반 지원 관련 법률

본 법들은 명확히 사물통신과 관련된 법률들은 아니지만, 사물통신을 운용하거나 통신기반을 운용하는데 있어 기본이 될 수 있는 법률들이라고 할 수 있다. 특히 사물통신은 전기통신망 뿐만 아니라 정보통신망, 유선망, 무선망 등 다양한 수준의 망들을 다 포괄하므로, 이러한 다양한 통신망과 통신과 관련된 법제에 대한 기본적인 이해가 필요하다고 할 수 있다.

가. 국가정보화 기본법

국가정보화와 국가 네트워크 구축에 관한 기본적인 사항을 선언적 의미로 규정한 국가 정보통신망에 대한 가장 기본적인 법률로 국가정보화의 기본 방향과 관련 정책의 수립·추진에 필요한 사항을 규정함으로써 지속가능한 지식정보사회의 실현에 이바지하고 국민의 삶의 질을 높이는 것을 목적으로 한다.

나. 정보통신망 이용촉진 및 정보보호에 관한 법률

정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다. 정보통신망법은 방송통신망을 포함한 정보통신네트워크에 관한 기본적인 사항을 규정하고 있지만, 기본적으로 사람 중심의 통신을 다루고 있다. 즉, 기본적으로 사람과 사람 사이의 통신에 정보통신망이 이루어지는 경우, 이러한 정보통신망에서의 신뢰성과 안전성을 어떻게 보장하는지에 초점을 맞추고 있다.

다. 전기통신기본법

전기통신에 관한 기본적인 사항을 정하여 전기통신을 효율적으로 관리하고 그 발전을 촉진함으로써 공공복리의 증진에 이바지함을 목적으로 한다.

라. 전기통신사업법

전기통신사업의 운영을 적정하게 하여 전기통신사업의 건전한 발전을 기하고 이용자의 편의를 도모함으로써 공공복리의 증진에 이바지함을 목적으로 한다.

마. 전파법

전파의 효율적인 이용 및 관리에 관한 사항을 정하여 전파이용과 전파에 관한 기술의 개발을 촉진함으로써 전파 관련분야의 진흥과 공공복리의 증진에 이바지함을 목적으로 한다.

바. 정보통신공사업법

정보통신공사의 조사・설계・시공・감리(감리)・유지관리・기술관리 등에 관한

기본적인 사항과 정보통신공사업의 등록 및 정보통신공사의 도급(도급) 등에 필요한 사항을 규정함으로써 정보통신공사의 적절한 시공과 공사업의 건전한 발전을 도모함을 목적으로 한다.

사. 인터넷멀티미디어방송사업법

방송과 통신이 융합되어가는 환경에서 인터넷 멀티미디어 등을 이용한 방송사업의 운영을 적정하게 함으로써 이용자의 권익보호, 관련 기술과 산업의 발전, 방송의 공익성 보호 및 국민문화의 향상을 기하고 나아가 국가경제의 발전과 공공복리의 증진에 이바지하는 것을 목적으로 한다.

아. 인터넷주소자원에 관한 법률

인터넷주소자원의 개발·이용을 촉진하고 인터넷주소자원의 안정적인 관리체계를 구축함으로써 인터넷 이용자의 편익을 증진하고 국가사회의 정보화에 이바지함을 목적으로 한다.

자. 공간정보산업진흥법

공간정보산업의 경쟁력을 강화하고 그 진흥을 도모하여 국민경제의 발전과 국민의 삶의 질 향상에 이바지함을 목적으로 한다.

차. 국가공간정보에 관한 법률

국가공간정보체계의 효율적인 구축과 종합적 활용 및 관리에 관한 사항을 규정함으로써 국토 및 자원을 합리적으로 이용하여 국민경제의 발전에 이바지함을 목적으로 한다.

카. 전기사업법

전기사업에 관한 기본제도를 확립하고 전기사업의 경쟁을 촉진함으로써 전기사업의 건전한 발전을 도모하고 전기사용자의 이익을 보호하여 국민경제의 발전에 이바지함을 목적으로 한다.

2. 사물통신망 관련 법률

전용 사물통신망이라고 부를 수 있는 망으로는 센서망, 측정망, 관측망 등을 들 수 있다. <사물통신기반 구축 및 사물정보 이용 활성화에 관한 법률(안)>에서는 특별히 사물통신에 사용될 수 있는 망들로 센서망, 측정망, 관측망 등을 포괄하는 것으로 규정하고 있다.

가. 센서망에 관한 법률

사물통신망의 하나인 국내의 센서 망과 관련된 법률은 유비쿼터스 센서 망에 대한 규율을 담고 있는 유비쿼터스 도시의 건설 등에 관한 법률 시행령 제3조를 들 수 있다. 유비쿼터스 도시의 건설 등에 관한 법률은 유비쿼터스 도시의 효율적인 건설 및 관리 등에 관한 사항을 규정하여 도시의 경쟁력을 향상시키고 지속가능한 발전을 촉진함으로써 국민의 삶의 질 향상과 국가 균형발전에 이바지함을 목적으로 한다. 사물통신기반의 구축과 이용의 촉진은 이러한 유비쿼터스 도시 건설에 필수적인 요인이라고 할 수 있다.

나. 측정망에 관한 법률

사물통신망의 하나인 국내의 측정망과 관련된 법률은 다음과 같다.

- 대기환경보전법 제3조 대기오염 등의 상시측정망
- 소음·진동규제법 제3조 소음·진동의 상시측정망

- 수질 및 수생태계 보전에 관한 법률 제9조 하천·호소 등의 수질 및 수생태계의 상시측정망
- 잔류성 유기오염물질 관리법 제11조 측정망의 설치·운영
- 지하수법 제17조 지하수의 관측 및 조사 등
- 토양환경보전법 제5조 토양오염도 측정 등
- 한국수자원공사법 제26조의2 수질오염도의 측정 등
- 해양환경관리법 제9조 해양환경측정망

다. 관측망에 관한 법률

사물통신망의 하나인 국내의 관측망 관련된 법률은 다음과 같다.

- 기상관측표준화법 제8조 기상관측망
- 기상법 제7조 기상관측망
- 해양수산발전기본법 제17조 해양과학조사 및 기술개발 등

3. 사물통신 서비스 관련 법률

실제 사물통신망이나 사물통신을 이용한 서비스들과 관련된 규제 및 진흥 법안들은 다음과 같은 법안들이 존재한다. 이러한 법들이 통과된다면 사물통신 서비스의 활성화에 큰 기여를 할 수 있을 것으로 기대된다. 대표적인 사물통신 서비스 관련 법안으로는 원격진료 허용을 포함하는 의료법 개정안과 스마트그리드 촉진법 등을 들 수 있다. 두 법안은 차세대 주력 사물통신 서비스라고 할 수 있는 스마트그리드와 U-헬스케어 서비스의 활성화를 위해 만들어진 것들이다.

가. 원격진료법안 및 건강관리서비스법안

의료인-환자 간 원격의료를 허용함으로써 의료인 및 의료기관에 대한 불필요한 규제를 완화하고 의료서비스 산업의 경쟁력을 제고하기 위해 제안된 의료법

개정안이다. 원격진료의 기반에 사물통신이 자리 잡고 있기 때문에 사물통신의 활성화에도 크게 기여할 것으로 보인다.

나. 스마트그리드 촉진법 (지능형전력망의 구축 및 이용 촉진에 관한 법률)

본 법은 스마트그리드 사업을 안정적이고 체계적으로 구축하는 것과 이용촉진, 관련 산업을 육성키 위한 제도적 기반을 마련하기 위해 제안된 법안으로 에너지 이용 효율을 극대화하는 종합적이면서도 체계적인 방안이 담겨있다. 스마트그리드 촉진법은 국가 단위의 스마트그리드를 구축하기 위해 관계 부처가 합동으로 '지능형전력망 기본 계획'을 수립할 것을 요구하고 있다.

다. 위치정보의 보호 및 이용에 관한 법률

위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하여 위치정보의 이용을 활성화함으로써 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.

4. 통신망 정보보호 관련 법률

통신망의 정보보호와 관련된 법률로는 기본법이라고 할 수 있는 국가정보화기본법을 필두로 정보통신망 이용촉진 및 정보보호에 관한 법률과 같은 보안과 프라이버시를 전문으로 하는 법률들도 존재한다. 또한 유비쿼터스 도시 관련 법률이나 스마트그리드 촉진법에서도 일부 해당 센서망과 통신망에서의 정보보호의 요구조항들을 포함하고 있다.

가. 국가정보화기본법

국가정보화기본법은 정보이용의 신뢰성과 안전성 보장이라는 절을 통해 정부의 국가정보통신망에 대한 정보보호 및 국민들의 프라이버시 보호 조치를 의무화하고 있다.

제37조(정보보호 시책의 마련) ① 국가기관과 지방자치단체는 정보를 처리하는 모든 과정에서 정보의 안전한 유통을 위하여 정보보호를 위한 시책을 마련하여야 한다.
② 정부는 암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치를 마련하여야 한다.

제38조(정보보호시스템에 관한 기준 고시 등) ① 행정안전부장관은 관계 기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호시스템을 제조하거나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있다.
② 행정안전부장관은 유통 중인 정보보호시스템이 제1항에 따른 기준에 미치지 못할 경우에 정보보호시스템의 보완 및 그 밖에 필요한 사항을 권고할 수 있다.
③ 제1항에 따른 기준을 정하기 위한 절차와 제2항에 따른 권고에 관한 사항 및 그 밖에 필요한 사항은 대통령령으로 정한다.

제39조(개인정보 보호 시책의 마련) 국가기관과 지방자치단체는 국가정보화를 추진할 때 인간의 존엄과 가치가 보장될 수 있도록 개인정보 보호를 위한 시책을 마련하여야 한다.

나. 정보통신망 이용 촉진 및 정보보호에 관한 법률

정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성함으로써 국민생활의 향상과 공공복리의 증진에 이바지하는데 그 목적이 있다. 기본적으로 사람간의 통신에 대한 규율을 목적으로 하지만, 사물통신에 대한 보호에도 직, 간접적으로 연관되어 있다고 할 수 있다.

다. 정보통신기반보호법

전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다. 특히 스마트그리드와 같은 국가기반시설에서는 제어시스템 등에서 사물통신이 흔하게 이루어지게 되므로, 국가기반시설에서의 사물통신에 대한 보안과 관련이 있다.

라. 위치정보의 보호 및 이용에 관한 법률

위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하여 위치정보의 이용을 활성화함으로써 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다. 개인정보로서의 사물위치정보의 보호와 관련된 내용을 규율할 수 있다.

마. 스마트그리드 촉진법 (지능형전력망의 구축 및 이용 촉진에 관한 법률)

스마트그리드 촉진법도 스마트그리드 환경에서의 잠재적 위험에 대한 인식에 근거하여 보안과 프라이버시 보호와 관련된 내용을 포함하고 있다. 본 법에는 사이버 테러, 정보 유출 등 사생활 침해 사고에 대비해 스마트그리드와 관련된 정보를 철저히 보호할 수 있도록 각종 보호지침을 갖출 것을 요구하고 있다. 특히 스마트그리드와 관련된 개인 정보를 정보 주체의 동의 없이 수집 및 처리할 수 없고 사업자는 정보 수집 및 활용을 위한 표준 약관을 제정해야 하며, 사업자는 또 정보보호 시스템을 설치 및 운영하고 정보의 불법 유출을 막을 수 있는 각종 보호 조치를 취할 것이 요구된다.

바. 유비쿼터스 도시의 건설 등에 관한 법률

유비쿼터스 도시 건설법에서도 유비쿼터스 도시 관리를 위해 사물간의 통신을 통해 이용되는 개인정보에 대한 보호와 기반 시설에 대한 보안 요구사항들을 포함하고 있다. 본 법에 나와 있는 프라이버시 보호 및 요안 요구사항은 다음과 같다.

> 제21조 (개인정보 보호) 유비쿼터스도시의 관리 및 유비쿼터스도시서비스의 제공과정에서 개인의 정보가 수집, 이용, 제공, 보유, 관리 및 파기(이하 "취급"이라 한다)되는 경우에는 관계 법령에 따라 필요한 목적의 범위에서 적법하고 안전하게 취급되어야 한다.
> 제22조 (유비쿼터스도시기반시설의 보호) ① 행정안전부장관은 「정보통신기반 보호법」 제8조에 따른 기준 및 절차 등에 따라 해당 지방자치단체의 장과 협의하여 유비쿼터스도시기반시설 중 대통령령으로 정하는 시설을 주요 정보통신기반시설로 지정하여야 한다.
> ② 제12조제1항제1호부터 제3호까지에 해당하지 아니하는 민간사업자는 유비쿼터스도시기반시설에 대하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항에 따른 인증을 받을 수 있다.

5. 사물지능통신 관련 법률

위와 같이 많은 법들과 직, 간접적으로 연관이 존재하지만 사물지능통신을 포괄하는 기본적인 내용들을 담고 있는 것은 아니다. 최근 준비 중인 사물통신기반 구축 및 사물정보 이용활성화에 관한 법률은 최초로 사물통신 및 사물정보의 이용과 관련된 일반적인 내용을 담고 있는 법률안이라고 할 수 있다.

개별 산업 부문에서 별도로 추진되고 있는 사물지능통신과 관련된 구체적인 사항을 종합적으로 규정하는 법이 미비하고 u-City법, 위치정보법, 스마트그리드법, 도로법 등 개별 산업 분야에서 필요한 내용들이 산재해 있는 상황이기 때문에 종합적으로 사물통신의 내용을 규율할 수 있는 사물지능통신법이 요구되고 있다.

가. 사물통신기반 구축 및 사물정보 이용활성화에 관한 법률안[56)]

방송통신위원회는 2009년 말 사물통신기반 구축 및 사물정보이용에 관한 사항을 정하여 사물통신기반 투자의 효율성을 제고하고 사물정보이용을 활성화함으로써 사물통신 관련 산업의 진흥과 공공복리의 증진에 이바지함을 목적으로 <사물통신기반 구축 및 사물정보 이용 활성화에 관한 법률(안)>을 발표한 바 있다.

본 법의 설명 자료를 보면 사물통신기반과 관련된 새로운 법을 제안한 이유는 사물통신기반이라는 개념 자체가 복합적, 융합적 개념으로 기존의 개별 단일법으로는 정의가 불가능하고 사물통신 기반 자체가 관련법 상의 망, 설비 등을 모두 포함한 복합적인 요소를 혼합하여 구축한 새로운 차원의 체계이므로 기존의 법으로만 규율이 어렵기 때문이라고 한다. 즉, 사물통신이라는 개념 자체가 사물통신기반을 전제로 하면서도 통신개념에 부가적인 새로운 현상을 접목시킨 것으로 기존의 전기통신사업법 등 개별적 규범으로는 규제가 어려운 경우가 발생하게 된다.

본 법에서는 사물통신을 환경, 교통, 해양, 기상, 에너지, 건물 등 사물의 상태나 상황정보를 지능화된 기기 간에 송신하거나 수신하는 것으로 정의하고 있다. 본 법은 사물에 감지장치 또는 장비를 부착/설치하고, 이러한 방법으로 정보를 수집하기 위한 원시적 상태를 가정한다. 기술적 측면에서는 환경 등 자연물 자체가 사물이라기보다는 정보수집을 위해 선택/채택된 실체에 센서 등이 부착/설치된 상태를 지능형 사물이라고 부른다. 사물통신망 체계는 사물로부터 수집된 내용(원시정보)를 유무선을 통해 지능화, 융합화된 통신망으로 송수신하는 것을 말하며, 소규모 혹은 개인의 내부적인 통신은 이 법의 대상에서 제외된다. 즉, 국가적 차원에서 규율할 필요가 있는 사물정보의 흐름만을 본 법의 규율대상으로 한다고 규정하고 있다.

---

56) 한국정보화진흥원, 사물통신기반 구축 및 사물정보이용 활성화에 관한 법률(안) 설명자료, 2009.11

또한 사물통신을 위하여 계통적, 유기적으로 연결, 구성된 전기통신설비의 집합체인 사물통신망을 정의하면서 사물통신 공공망, 사물통신 공중망, 사물통신 선도망으로 구분하고 있다. 또한 그 적용대상을 관측망, 센서망, 측정망 등의 사물통신망으로 규정하고 있다. 이러한 망에는 공유수면관리법, 공유수면매립법, 기상관측표준화법, 기상법 등 개별 법률들에서 규정하고 있는 기상관측망, 상시측정망 등을 포괄한다. 따라서 이 법에서 규정하고 있는 규제 대상으로서의 사물통신망은 공공에서 운영하고 있는 공공영역의 사물통신망으로 한정된다는 한계가 존재한다. 따라서 민간영역의 사물통신에 대해서는 여전히 규제할 수 있는 법적 방안이 존재하지 않는다.

사물통신 기반구축 기본계획(안)에는 확산 환경 조성 과제로서 식별 및 정보자원 관리 체계 구축과 정보보호 관리체계 개발, 법제도 개선, 협력체계 및 전문인력 양성과 같은 과제들을 제시하고 있다. 특별히 식별 및 정보자원 관리 체계 구축 과제로는 식별체계 수립은 물론 식별체계 가이드라인 보급 및 사물정보자원 관리체계 마련, 사물정보자원 관리시스템 운영 등의 세부 과제들을 제시하고 있으며, 정보보호관리체계 개발 과제에서는 2009년 정보보호관리체계 수립, 2010년 2단계에는 정보보호 검증체계 구축 및 정보보호 가이드라인 개발, 보급, 2012년 3단계 과제로 정보보호 체계 보급 및 확산 과제를 세부과제로 제시하고 있다.

법제도 개선에서는 사물통신 기반 구축 및 사물정보 이용활성화에 관한 법률 제정을 목표로 전용 요금제도와 SLA제도의 마련 등의 세부 과제를 제시하고 있다. 또한 기술 개발 과제에서는 사물통신핵심기술 개발이라는 과제 하에 사물정보 보안, 인프라보호, 서비스 보안등의 핵심 기술 개발과 개방형 서비스 통합 플랫폼 기술 개발등을 2010년부터 추진할 계획이다. 세부적으로 살펴보면 식별체계 도입 및 정보자원 관리체계의 구축은 IP6기반의 안전하고 효율적인 사물통신 서비스를 제공하기 위한 식별체계를 도입하고 사물정보 자원 관리 시스템을 구축 및 운영하여야 한다.

사물통신에서의 인증서비스는 이러한 플랫폼 기술 및 보안 기술의 일환으로 추진될 것으로 보이며, 식별체계의 기반 하에 정보보호 관리체계안에 인증체계 마련을 위한 과제가 추진될 것으로 보인다. 또한 이러한 사물통신 기반구축을 위한 법제도의 한편으로 사물통신에서의 인증과 같은 정보보호 관련 법제의 수립에 대해서도 논의가 될 필요가 있을 것으로 보이며, 사물통신기반 인증과 관련된 일반적인 근거법규를 확보하는 일이 요구된다.

하지만 본 법은 활성화와 동시에 보안 문제를 고려되어야 함에도 이러한 고려가 미약해 보이고 전반적으로 진흥과 활성화에 대한 내용이 주축을 이루고 있다. 많은 새로운 서비스와 관련된 법률들이 진흥뿐만 아니라 보호에도 높은 비중을 두고 있는데 비해 보안에 대한 내용 특히 인증 관련된 내용은 전혀 포함되어 있지 않다.

하지만 본 법은 방송통신위원회로 하여금 사물통신 기본 계획을 수립하고 공고할 것을 의무화하면서 사물통신망의 안전성 및 신뢰성 제고 및 사물정보 이용의 촉진 및 보호와 관련된 내용을 포괄할 것을 포함시키고 있다. 따라서 해당 법률의 규제 대상 통신에서의 인증정책 및 인증기술에 대한 내용 또한 사물통신 기본 계획에 포함시킬 수 있을 것이다.

제5조 (사물통신 기본계획의 수립) ① 방송통신위원회는 사물통신기반의 효율적인 구축과 사물정보의 원활한 공동이용촉진 및 사물정보이용의 활성화를 위하여 다음 각 호의 사항이 포함된 사물통신 기본계획(이하 “기본계획”이라 한다)을 수립하고 이를 공고하여야 한다. 기본계획 중 대통령령으로 정하는 중요한 사항을 변경한 경우에도 또한 같다.
1. 사물통신 시책의 기본방향
2. 사물통신망의 구축을 위한 기본방향
3. 사물정보이용의 활성화를 위한 기본방향
4. 사물통신기반의 확보 및 합리적·경제적 사용
5. 사물통신망에 관련된 기술의 개발·보급·확산 활용
6. 사물통신망의 이용촉진을 위한 식별체계의 표준화
7. 사물통신망을 위한 주파수의 확보

8. 사물통신망의 안전성 및 신뢰성 제고
9. 사물정보이용의 촉진 및 보호
10. 사물정보의 수요조사와 시범사업의 발굴 및 이용촉진
11. 사물정보이용과 관련된 기술개발 및 표준화
12. 사물정보이용의 지원 및 육성
13. 사물통신에 관한 전문 인력의 양성
14. 사물통신과 관련된 재원의 조달 및 운용
15. 사물통신과 관련된 국제협력의 활성화
16. 사물통신산업의 발전과 해외시장 진출의 지원
17. 그 밖에 사물통신 관련 분야의 진흥을 위하여 필요한 사항

② 방송통신위원회는 제1항에 따른 기본계획을 시행하기 위하여 필요한 경우에는 연도별 시행계획(이하 “시행계획”이라 한다)을 수립하고 시행할 수 있다.

③ 방송통신위원회는 관계 중앙행정기관의 장 또는 지방자치단체의 장에게 제1항에 따른 기본계획과 제2항에 따른 시행계획의 수립에 필요한 자료를 요청할 수 있으며, 중앙행정기관의 장 또는 지방자치단체의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.

④ 제3항에 따른 관계 중앙행정기관의 장 및 지방자치단체의 장은 사물통신에 관한 소관 주요정책의 수립과 그 집행에 있어서 기본계획을 우선적으로 고려하여야 한다.

⑤ 그 밖에 기본계획 및 시행계획의 수립·시행 등에 필요한 사항은 대통령령으로 정한다.

6. 온라인 인증 관련 법률

온라인 환경에서 신뢰성과 안전성을 보장하기 위한 핵심적인 기반 기술로서 전자적인 방식의 인증을 요구하는 기존의 법률들이 존재한다. 대표적인 법률들로는 전자서명법, 전자정부법, 공증인법 등을 들 수 있으며, 이외에도 각종 인터넷 규제법 상의 실명인증과 본인확인 등을 들 수 있다.

가. 전자서명법

전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 한다. 특히 본 법은 인증의 방식으로 공인인인증기관으로부터 발급받은 공인인증서를 사용하는 것에 대한 법적 효력과 공인인증기관의 요건 등을 법으로 규정하고 있다. 또한 전자서명법은 전자서명에 의한 부인방지 기능의 제공을 명시하고 있다.

나. 전자정부법

행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법 등을 규정함으로써 전자정부를 효율적으로 구현하고, 행정의 생산성, 투명성 및 민주성을 높여 국민의 삶의 질을 향상시키는 것을 목적으로 한다. 전자정부법은 행정전자서명의 인증 항목을 통해 인증요구사항을 명시하고 있다.

> 제29조(행정전자서명의 인증) ① 행정기관이 작성하는 전자문서에는 행정전자서명을 사용한다. 다만, 행정기관은 「전자거래기본법」 제2조제5호에 따른 전자거래를 효율적으로 운영하기 위하여 공인전자서명을 사용할 수 있다.
> ② 중앙사무관장기관의 장은 행정전자서명에 대한 인증업무를 수행한다.
> ③ 중앙사무관장기관의 장은 제2항의 인증업무를 수행할 때 공인전자서명과의 호환성을 높이기 위하여 행정안전부장관과 협의하여 행정전자서명에 대한 기술표준을 마련하고, 행정전자서명과 공인전자서명이 서로 연계될 수 있는 방안을 마련하여야 한다.
> ④ 제2항에 따라 인증 받은 행정전자서명이 있는 경우에는 그 행정전자서명을 전자문서에 표시된 행정기관 및 공공기관의 관인·공인 또는 해당 기관에서 직접 업무를 담당하는 사람의 서명이 있는 것으로 보며, 그 전자문서는 행정전자서명이 된 후에 그 내용이 변경되지 아니하였다고 추정한다.
> ⑤ 행정전자서명의 인증업무에 관하여 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회 규칙 및 대통령령으로 정한다.

다. 공증인법

공증이란 우리의 법률생활에서 생기는 여러 상황을 공적으로 증명하는 것으로서 중요한 거래에 관하여 증거를 보전하고 권리자의 권리 실행을 용이하게 하기 위하여 사실을 증명하여 주는 제도로서, 이를 이용하면 여러 가지 거래나 분쟁을 예방하거나 분쟁 발생 시 유력한 증거로 활용할 수 있고 나아가 재판절차를 거치지 않고 간편하게 권리를 실행할 수도 있는 장점을 제공하는 제도라고 할 수 있다. 본 법은 공증업무를 수행할 권한을 갖는 공증인(公證人)의 지위와 그 직무에 관한 사항을 규율하여 공증사무의 적절성과 공정성을 확보함을 목적으로 한다. 또한 전자문서의 공증에 대한 요구사항을 담고 있다.

제66조의5 (전자문서의 인증) ① 전자문서에 대한 인증은 다음 각 호의 어느 하나에 해당하는 방법으로 한다.
1. 촉탁인으로 하여금 대통령령으로 정하는 바에 따라 전자문서에 전자서명을 하게 하는 방법
2. 전자문서의 전자서명을 촉탁인이나 그 대리인으로 하여금 확인하게 한 후 그 사실을 적은 정보를 전자문서에 전자적 방식으로 첨부하는 방법
② 지정공증인은 전자문서를 인증할 때에 촉탁인이 그 앞에서 전자문서의 내용이 진실함을 선서하고 이에 전자서명을 하거나 전자서명을 확인한 경우에는 그 선서사실을 적은 정보를 전자문서에 전자적 방식으로 첨부하여야 한다.
③ 제1항에 따른 인증에 관하여는 제25조부터 제33조까지의 규정을 준용한다.
④ 제2항에 따른 선서인증에 관하여는 제25조부터 제29조까지, 제32조, 제33조 및 제57조의2제2항·제3항·제5항을 준용한다.

제66조의6 (전자화문서의 인증) ① 지정공증인은 전자화문서와 전자화대상문서를 대조하여 서로 일치하는 경우에는 전자화문서에 대하여 제57조제2항의 인증을 부여할 수 있다.
② 전자화문서의 인증에 관하여는 제25조부터 제33조까지의 규정을 준용한다.

제66조의7 (지정공증인의 전자서명) 지정공증인은 제66조의5제1항·제2항 및 제66조의6제1항에 따라 전자문서등에 인증을 부여하는 경우에는 해당 전자문서등에 수록된 정보 및 이에 첨부한 정보에 대하여 전자서명을 하고, 이를 확인할 수 있는 정보를 해당 전자문서등에 전자적 방식으로 첨부하여야 한다.

지금까지 사물통신의 신뢰성과 안전성을 보장하기 위한 핵심적인 메커니즘으로서의 사물통신 인증과 관련된 내용을 규제할 수 있는 사물통신 인증 관련 법률 대안을 모색하기 위해 전기통신 및 정보통신을 포함한 (사물)통신과 관련된 법률, 직접 사물통신과 관련된 법률, 정보보호를 위한 법률, 신분 인증과 관련된 법률, 성능 및 자격 인증과 관련된 법률 등을 살펴봄으로써 향후 사물통신 인증 관련 규율 법제를 만드는데 필요한 요소들을 검토해보았다.

기존의 많은 법률들은 일정부분 사물통신 인증과 관련된 내용을 담고 있긴 하지만, 엄격하게 법적 규율 대상으로서의 사물통신을 다루고 효과적인 인증을 보장하고 규제의 공백을 메울 수 있는 법률들은 부재한 상황이다. 다음 장에서는 구체적으로 현재까지 논의되고 있는 사물통신 인증 관련 법률 제정 방안에 대해 살펴보고, 사물통신 인증 법안이 담아야 될 요소와 원칙들에 대해 살펴보도록 하겠다.

제 6 절 사물통신 인증 관련 법안 제정방안

사물 지능 통신의 일반화가 예상되는 고도 정보화 환경에 대비하여 이에 대한 기술적, 규범적 통제가 요구되고 있으며, 이에 대한 규제 방안에 대한 논의가 진행되고 있는 상황이다. 이러한 통제방안의 한 영역으로 사물통신 과정에서의 정보보호 및 보안을 위한 인증방안에 대한 논의도 시작되고 있다. 본 절에서는 이러한 사물통신에서의 신뢰성과 안전성을 보장하기 위한 핵심적인 메커니즘인 사물통신 인증 관련 법안을 제정하기 위한 방안을 모색해보도록 한다. 우선 사물통신 인증의 특수성을 살펴봄으로써 사물통신 인증 법안 제정 시 고려해야 될 사항들을 추출해낸다. 또한 본 절에서는 사물통신 인증을 위한 구체적인 법안을 제시하지 않고 이러한 법안이 담아야 할 구성요소와 구체적인 법안 작성 방안을 위한 기초 논의들을 이끌어내도록 한다.

1. 사물통신 인증 법안 제정 방안

앞서 살펴본 대로 사물통신 관련 총체적인 규율 및 진흥 법률안은 현재 만들어지고 있는 상황이지만, 아직까지 사물통신의 신뢰성과 안전성과 관련된 내용을 규제하는 법률은 존재하지 않는 상황이다. 앞서 살펴본 대로 사물통신 과정에서 발생할 수 있는 프라이버시 침해나 보안 사고의 문제, 또한 이러한 사고에 대한 법적 책임의 귀속 문제를 해결함으로써 사물통신의 신뢰성과 안전성을 보장해줄 수 있는 법률이 요구되고 있다.

사물통신은 다양하고 이질적인 요소들 간의 복합적이고 융합적인 통신 환경을 전제하고 있으므로, 기존의 법률로는 사물통신의 보안이나 프라이버시 문제, 그리고 신뢰성 보장을 위한 인증과 관련된 부분을 모두 포괄할 수 있는 법률은 아직까지는 존재하지 않는 상황이다. 사물통신법안 설명 자료에도 사물통신은 복합적/융합적 개념이므로 지금까지의 개별 단일법으로는 정의가 불가능한 상황이며, 사물통신기반 자체가 관련법상의 망, 설비 등을 포함한 여러 가지 요소를 혼합하여

구축한 새로운 차원의 체계이므로 기존의 법으로는 규율하기 어렵기 때문에 별도의 법으로 규율해야 한다고 밝히고 있다.

따라서 새롭게 등장한 사물통신 개념을 통한 사업은 기존의 법규로는 규제하기 어려운 상황이므로, 사물통신 관련 인프라와 사물통신의 정보 등을 종합적으로 구축하고 이를 운영할 수 있는 별도의 법률의 필요성을 강조하고 있다. 또한 사물통신은 사람간의 통신과는 다른 특수성을 가지고 있으므로, 이러한 특수성에 기반한 사물통신 보안 및 책임 귀속과 관련된 법률이 특수하게 요구된다.

현재 사물통신 인증관련 법률들을 현존하는 다양한 법률에 포함시키는 방안과 새로 제정되는 사물통신 관련법에 인증관련 조항을 포함시키는 방안 등이 논의가 되고 있다. 일반적으로 논의되고 있는 사물통신 인증관련 법제화 논의들은 다음과 같다.

가. 정보통신망 이용촉진 및 정보보호에 관한 법률에 포함시키는 방식

사물통신기반은 정보통신망과 기존의 전기통신망 및 자가 설비의 연결이 자동화/지능화되는 것을 일부 요소로 포괄하므로 정보통신망에 대한 규율을 담고 있는 정보통신망 이용촉진 및 정보보호에 관한 법률에서도 일부 규율할 수 있다. 또한 사람 간의 통신에서 하지만, 사물지능통신은 많은 경우 공중정보통신망이 아닌 통신망을 통해 이루어지는 부분도 많기 때문에 모든 부문을 규율하지는 못하는 한계를 가지고 있다.

나. 전자서명법의 적용대상을 확장하는 방식

사물지능통신의 인증방식을 공인인증서 방식으로 의무화시킴으로써 공인인증서를 통한 법적 효과를 활용할 수 있다. 공인인증서는 전자서명을 통해 부인방지를 할 수 있는 강력한 기술적 인증방안을 제공한다. 지금까지의 전자서명법의 대

상인 사람통신에서의 공인인증서를 통해 사람의 신분을 인증하는 것을 넘어 사물통신으로 그 대상 범위를 확장하여 기기인증서 시스템을 구축하도록 하는 방안이 제시되고 있다. 하지만, 앞서 살펴보았듯, 사물지능통신은 다양한 수준이 존재하며, 다양한 수준의 인증방법을 요구한다. 굳이 부인방지나 강력한 수준의 인증이 필요하지 않고 사람에게 심각한 법적, 신체적 영향을 미치지도 않는 통신에 비싼 구축 및 운영비용이 드는 기기인증서 시스템만을 요구하는 것은 합리적이지 못한 것으로 생각된다.

다. 사물통신지원법에서 인증 및 정보보호 부분을 추가하는 방식

앞서 살펴보았던 것처럼 사물통신과 관련된 법률안이 준비 중지만, 사물통신의 정보보호 부분에 대해서는 간단한 원칙만 언급이 되어있을 뿐이고, 구체적인 보안과 관련된 조항들은 두고 있지 않다. 단순히 정보보호에 관한 사항이 사물통신 기본계획에 포함되어 있어야 한다는 요구사항을 두고 있을 뿐이다. 사물지능통신은 앞서 살펴보았던 것처럼 인간이 개입하는 통신과는 달리 부가적으로 인간의 개입이 존재하지 않는 상황에서 이루어지는 사물통신만의 심각한 보안위험이 존재한다. 따라서 사물통신 지원법에서 사물통신진흥 및 보호에 관한 법률로 개편하고, 사물통신 인증 및 정보보호에 관련된 내용을 포괄하자는 의견이 존재한다.

하지만, 지금 추진 중인 사물통신지원법은 그 대상이 공공기반으로 엄격히 제한되어있다는 한계가 존재하므로, 향후 민간의 개별적인 사람들에게 영향을 미치게 될 다양한 사물통신들을 모두 포괄하지 못하는 한계가 존재하는 것으로 판단된다.

라. 전자인증법을 신설하는 방식

기존의 전자서명법은 공인인증서라는 특정 유형의 인증방식만을 규정하고 있다는 한계가 존재한다. 따라서 본격적인 사물통신의 시대에 맞추어 사람 및 사물통신을 모두 포괄하여 공인인증을 포함한 전자인증과 관련된 일반화된 내용을 담

고, 그에 근거한 다양한 인증체계들의 이용의 진흥을 도모할 수 있는 일반법 수준의 인증관련 법제의 마련이 필요하다는 의견도 존재한다.

지금까지 네 가지 방식의 사물통신 인증 관련 법제화 방안에 대해 살펴보았다. 네 가지 방식은 각각 장단점을 가지고 있으므로 본 보고서에서는 특정한 방식의 법제화를 지정하기 보다는 사물통신 인증 관련 법제가 담아야 할 내용들을 재안하도록 하겠다.

2. 한국인터넷 진흥원의 기기인증 제도화

사람통신에 사용되는 공인인증서와 유사하게 공인인증기관이 배포하는 기기인증서를 이용하여 기기인증서비스를 시행할 경우 제도적 요구사항은 다음과 같다. 먼저 기기인증서비스에 대한 법적 근거를 마련하는 것과 제3자 인증방식을 채택할 경우 기기인증서 발급절차의 신뢰성을 확보하는 것, 또 한편으로 기기인증기관 관리 및 감독체계를 마련하는 것이라고 할 수 있다.

한국인터넷진흥원은 위와 같은 기기인증 제도화 방안으로 기기인증서비스의 신뢰성 확보를 위한 기기인증서 공인화를 추진하고 있다. 또한 이의 구체적인 법제화 방안으로 전자서명법 개정을 통한 제도화를 추진할 계획을 밝힌 바 있다. 한국인터넷진흥원에 따르면 기기인증 제도화의 구체적인 방안으로는 기기인증서의 정의 및 발급 관련 규정, 기기인증서의 법적 효력, 기기인증서 발급 이용 시 지켜야 할 기준들이 법에 포함되어야 한다고 밝히고 있다.

한국인터넷진흥원이 말하고 있는 기기인증 관리체계란 VoIP, CCTV 등 다양한 네트워크 기기에 기기인증서를 탑재하여 기기의 식별 및 권한 확인, 데이터 암호화를 수행하는 기기인증체계를 수립하는 것을 골자로 한 기기인증서 발급 및 이용 등 공인인증서에 준하는 기기인증 관리체계를 말한다. 또한 이미 유비쿼터스 도시 사업과 연계하여 2009년에 기기인증 시범 사업을 추진했으며, 2009년 12월에

는 기기인증서 발급을 위한 기기인증체계도 구축한 바 있다.

기기인증서는 기기제조과정 중에 해당 기기에 탑재하게 되며, 갱신 및 재발급 과정과 같은 번거로운 작업 없이도 기기의 사용연한과 동일하게 유지된다. 기기인증서는 제조업체명, 기기식별정보(시리얼번호, MAC 주소) 등을 포함하며, 기기 제조업체 등을 통해 기기의 진위성을 확인하게 된다.

공인인증서를 기기인증에 사용하도록 법제화하는 경우 공인인증서 방식의 사물통신의 가장 큰 한계라고 할 수 있는 공인인증서 발급, 재발급, 파기와 같은 번거로운 추가 관리 작업이 여전히 필요하다는 한계가 존재할 수 있다. 이러한 문제를 어떻게 사물통신의 환경에 맞추어 조정할 것인가가 논의되어야 한다. 예를 들어 사물통신의 특성상 유효기간을 기기들의 평균 수명에 맞추어 늘린다고 하더라도 이는 인간들의 통신에서와 마찬가지로 공인인증서 유출에 따른 위조의 위험이 높고, 기간이 길어지면 기존의 암호화 방식이 안전하지 않게 되는 일이 발생하여 어차피 업데이트를 해야 하는 번거로운 일이 생길 수도 있다는 점이 고려될 필요가 있다.

또한 기기 인증서의 경우 기기 인증서의 발급 및 관리책임을 누구에게 둘 것인가의 문제가 발생한다. 기기인증서의 경우 수천~수만장 단위로 벌크로 선발급되는 방식으로 발급이 되므로, 이러한 발급된 인증서를 관리하고 안전하게 보존하는 문제는 쉽지 않을 것이다. 결국 기기 업체들이 인증서 확인 및 신뢰성을 유지할 책임을 지게 된다. 이는 기기업체들에게는 과다한 부담을 지우는 것이 될 수도 있다. 즉, 기기의 소유권 및 통제 주체가 변경될 때마다 기존의 기기인증서를 없애고 새로 발급받아야 하는가의 문제가 발생한다. 또한 기기인증서의 경우 인증서 시스템의 신뢰성을 보장하기 위하여 사용이 중지된 혹은 망가진 기기들이 기존에 가지고 있던 인증서가 부정한 목적으로 재활용될 가능성을 막기 위한 목적으로 파기할 수 있는가의 문제가 존재한다.

높은 수준의 보호가 요구되고 엄격한 업무분장과 책임성이 존재하고 엄격하게 기기 관리자 지정 및 엄격한 파기 및 반납 과정과 같은 종합적인 관리가 가능한 공공의 환경에서는 기기인증서 방식이 가장 최선의 대안이 될 수 있을 것이다. 기존의 공인인증서 시스템이 국가적인 차원으로 구축된 국내 환경에서는 초기비용을 줄일 수 있다는 장점도 존재할 것이다.

또한 기기인증서의 경우 기기 시리얼 번호나 MAC 주소 정보만을 담고 있으며, 실제 법적 주체인 사람에 대한 인증은 하고 있지 않으므로 그 효과에 있어 매우 제한적으로 수행될 수 있다는 점을 알 수 있다.

이처럼 공공의 경우에는 충분히 가능한 대안이 될 수 있지만, 소유자가 지속적으로 변할 수 있는 민간영역의 모든 수준의 사물통신에 대한 인증에 의무적으로 적용될 필요는 없으며, 실제 적용되기도 쉽지 않아 보인다.

3. 특정 인증방법 강제의무화 이슈와 유형별 적용 원칙

다양한 유형의 사물통신의 인증방법을 한 가지 방식으로 의무화하고 하는 것은 많은 무리수가 존재한다. 전자금융서비스의 경우에도 공인인증방식의 의무화에 의해 다양한 문제점들이 발생했었다. 사물통신에서도 또한 다양한 목적과 다양한 수준의 통신방법이 존재할 수 있다. 현재 공인인증서 기술을 기반으로 한 기기인증서 시스템을 구축하여 운영하는 것으로 사물통신의 인증문제를 잡아가고 있는 것으로 보인다. 사물통신의 인증수단으로 공인인증서 시스템을 이용하는 것은 일부 문맥에서는 매우 유의미할 수 있지만, 그렇지 않은 경우에는 구축 및 관리 등에 있어 관리인력 및 시스템 자원의 낭비가 될 수 있다.

자원의 낭비를 막고 최적화된 인증방법을 제공하기 위해서 가장 중요한 것은 사물통신을 유형별로 분류하는 것이다. 사물통신은 단순히 센서 등을 이용하여 기계의 정보나 환경정보를 수집하여 전송하는 행위 이상을 포함할 수 있기 때문이

다. 고차원적인 법률행위들인 계약과 명령행위를 포괄할 수 있으며, 인간의 생명을 위협하는 심각한 행위나 정보를 포괄하기도 한다.

이처럼 유의미한 사물통신 인증방법들을 구분하기 위해서는 사물통신을 통해 수집되는 정보의 유형별로 구분하는 것과, 제공하는 서비스의 유형별, 통신영역별, 그리고 통신기기의 유형별로 구분하는 방식이 존재한다. 또한 이러한 통신기기들이 통신을 수행하는 다양한 문맥에 따른 유형 분류도 가능할 것이다. 어쨌든 이러한 다른 맥락과 유형 별로 각각 적절한 수준의 인증기술을 사용하도록 하는 것이 가장 관건이 될 것이다. 사물통신 인증을 선택하는데 영향을 줄 수 있는 요소들에는 다음과 같은 것들이 존재할 수 있다.

- 해당 통신사물 기기의 컴퓨팅 파워와 저장 공간
- 해당 통신사물 기기가 다루는 정보의 민감도 (개인정보, 기밀정보)
- 해당 통신사물 기기 서비스의 중요성과 법적 맥락
- 해당 통신사물 기기가 다루는 정보의 법적 맥락 (계약 여부)
- 해당 통신사물 기기의 통신 행위가 사회 혹은 사람에 미칠 수 있는 영향의 심각도

앞서 본 보고서는 이러한 맥락들을 중심으로 사물통신의 유형 분류 방법을 제안한 바 있다. 따라서 사물통신 인증법제는 사람들의 인증도 사용되는 서비스에 따라 다른 인증을 사용할 수 있도록 하고, 특별히 금융거래와 같이 특수한 부분만 따로 규율을 하는 것처럼 각 유형별로 세분화하여 적용할 필요가 있다.

4. 사물통신 인증 법안 구성요소

사물통신에서의 인증관련 법제에 포함되어야 할 내용은 다음과 같다. 앞서 살펴보았듯 사물통신에서 중요한 것은 해당 법의 규제대상이 되는 사물지능통신의 범위를 확정하는 것과 인증행위의 법적 능력을 부여하는 것, 그리고 이러한 정상적인 인증행위를 우회하거나 인증을 오용하는 행위에 대한 처벌을 통해 인증시스템의 효과성을 보장하는 것이라고 할 수 있다.

또한 앞서 살펴보았던 것처럼 법안에는 단일한 인증 시스템을 의무화하는 것은 적절하지 않아 보이며, 사물통신을 그 성격과 영향력에 따라 구분하고 적절한 수준의 안전한 인증시스템이 다양하게 개발 및 적용될 수 있도록 개발을 촉진하고 인증평가를 수행하여 관리하는 시스템을 구축하는 방안을 법제화하는 것이 필요할 것으로 생각된다.

- 사물통신의 명확한 정의
- 법적 규제대상이 되는 사물통신의 범위
- 사물통신에서의 인증의 의미와 정의
- 사물통신에서의 인증행위의 법적 능력
- 사물인증과 사람인증의 관계
- 사물통신의 유형 분류
- 사물통신 인증기술의 분류
- 사물통신 인증기술평가위원회 필요성과 구성
- 사물통신 가짜 인증, 인증 우회 행위에 대한 처벌 규정

제 7 절 소 결

사람의 개입 없이 사물들 간에 수행되는 사물통신에서는 프라이버시 침해나 가짜 사물과 같은 많은 정책적 이슈들이 존재한다. 하지만, 이러한 사물통신에서의 잠재적인 위험들은 사물은 법적 주체나 책임 귀속 주체가 될 수 없으므로 사람에게 사물통신의 모든 결과와 그 책임이 귀속된다. 이러한 특성 때문에 사물통신의 신뢰성을 보장하기 위한 핵심적인 메커니즘으로서의 인증은 사물뿐만이 아니라 사람에 대한 인증(authentication)도 함께 요구된다. 또 한편으로 사물의 안전성과 기능성에 대한 인증도 신뢰성 요건으로 요구된다. 따라서 사물통신에서의 인증은 첫째, 누구 소유인가? 혹은 누구의 통제 하에 있는가? 둘째, 누가 만든 제품인가? 셋째, 안전한 제품인가? 이 세 가지 질문에 대한 대답을 제공해줄 수 있어야 할 것으로 판단된다.

사물통신은 단일한 유형의 통신이 아니라 다양한 유형의 통신 방법과 구체적인 서비스 구현들이 존재하므로, 사물정보의 민감도, 통신결과의 심각도, 서비스 기능의 중요도, 사람과의 결합도, 디바이스 환경, 조직 환경 등 통신이 발생하는 문맥에 따라 다양하게 분류될 수 있다. 따라서 단일한 사물통신 인증정책을 제시하기 보다는 다양한 사물통신 유형별로 디바이스 인증, 서버 인증, 통신내용 암호화 여부, 부인방지, 호환성, 인증기술 효율성, 사용자 개입 최소화 등의 요구사항의 수준을 정하여 해당 유형에 가장 적합한 인증시스템을 적용하는 정책을 마련하는 것이 중요하다. 따라서 본 연구에서는 이를 위해 사물통신 유형별 사물통신 인증 방법 수립 방법론을 제시하였다.

또한 이러한 사물통신 인증 정책의 효과성을 보장하기 위한 부가적인 정책으로 인증 내역 증거보존 의무화, 사물통신 인증방법 평가위원회 구성, 사물통신 인증방법 수립 정책 기준 마련 등을 제시하였고, 앞서 제시한 사물통신 인증 정책에 기반하여 사물통신 인증관련 법제가 담아야 할 원칙과 구성요소들을 제시하는 것으로 마무리 지었다.

제 5 장 결 론

인간이 개입하지 않고 인간의 검토나 확인 없이 사물 간에 수행되는 사물통신은 인간의 개입이 없거나, 최소화된 상태에서 기기 간 자동적으로 이루어지는 통신으로, 국가주요기반시설, 지능형자동차 등 새로운 제품 및 서비스를 위한 핵심적인 기반기술이라고 할 수 있다.

사물통신은 그 통신의 결과가 인간의 삶에 직간접적으로 심각한 영향을 줄 수 있다는 점에서, 사물통신에 인간의 의사가 정확히 반영이 되었는지, 통신내용의 기밀성, 무결성, 가용성이 충분히 보장되는지가 매우 중요하다고 할 수 있다. 사물통신에서의 신뢰성은 사물통신의 이용한 다양한 서비스들의 성공과 활성화를 보장할 수 있는 핵심적인 요소라고 할 수 있으며 그 중에서 사물통신 인증은 신뢰성 보장을 위한 핵심적이고 기본적인 요소라고 할 수 있다.

따라서 사물통신을 추진하는 데 있어 정보보호에 대한 고려가 필수적이며, 사물통신의 정보보호는 적법한 기기로부터 적법한 메시지임을 확인할 수 있는 인증기술이 가장 중요할 것으로 예상된다. 본 연구에서는 사물통신이 갖추어야 할 요구조건, 사물통신 환경에서 사용될 것으로 예상되는 인증기술 분석 및 연구, 그리고 이를 규정하기 위한 법 정책을 제시했다.

본 보고서에서는 우선 사물통신에서 활용될 수 있는 사물통신인증기술들을 살펴보았다. 본 보고서에서는 다양한 사물통신인증기술들 중에서 가장 적합한 인증기술 하나를 선택하기 보다는 사물통신의 목적과 성격이 단일하지 않고 이질적이기 때문에 사물통신의 목적과 성격, 그리고 그 결과의 영향력에 따라 해당 사물통신인증 요구수준을 구분하여 적절한 수준의 인증기술을 적용하는 방식이 가장 적절하다고 제안하였다. 이를 위해 본 보고서에서는 다양한 사물통신을 분류하기 위한 기준들을 제시하였고, 그러한 분류에 기초하여 적합한 사물통신 요구사항들을 도출해내었다.

본 연구를 통해 달성된 사물통신의 신뢰성을 보장할 수 있는 인증기술에 대한 연구 및 법, 정책적인 환경조성을 위한 연구는 향후 사물통신 인증기술 가이드라인 작성 및 표준화 정책 추진에 있어 직접적인 도움을 제공할 수 있을 것으로 기대되며, 향후 사물통신 보안 및 인증 관련 법제 작성에 직, 간접적인 도움을 제공할 것으로 기대된다.

향후에는 본 보고서에서 제시한 사물통신 분류를 기반으로 구체적인 유형별 사물통신 인증 가이드라인을 만드는 작업을 수행하고 본 사물인증 기술 및 정책 연구의 결과를 기반으로 사물통신에서의 효과적인 인증 목표를 달성할 수 있는 사물인증 관련 법률의 조항을 만들어 제안하는 작업이 진행되어야 할 것으로 생각된다.

참 고 문 헌

[1] 강필용, 기기인증체계 현황 및 전망, 한국정보보호학회 Green-IT 융합 보안 워크샵 발표자료

[2] 국무총리실, '전자금융거래 인증방법의 안전성 가이드라인'확정 보도자료, 2010.5.31.

[3] 국무총리실, 총리실, '전자금융거래 인증방법의 안전성 가이드라인'확정, 2010년 5월 31일자 보도자료

[4] 금융감독원, 전자금융감독규정 개정, 2008

[5] 김기형, "사물지능통신의 개념과 차이점", RFID/USN Online Forum 발표자료

[6] 김동기, "사물지능통신 서비스 추진 전략", 사물지능통신 컨퍼런스 발표자료, 2010

[7] 김상철, 무선랜보안(Wireless LAN Security), 한국정보보호진흥원, 2002

[8] 김유창, "기기 간 통신(M2M)의 기술 동향과 전망", 전자부품, 2009년 7월호

[9] 도윤미 외, "스마트 그리드 기술 동향: 전력망과 정보통신의 융합기술", 한국전자통신연구원『전자통신동향분석』, 제24권 제5호, 2009

[10] 방송통신위원회, "사물통신 기반구축 기본계획(안)", 2009

[11] 사물통신 법제도TFT, 사물통신기반 구축 및 사물정보이용 활성화에 관한 법률(안) 설명자료

[12] 안재영, "M2M 네트워크 및 서비스 기술", The 20th High-Speed Network Workshop, 2010

[13] 오병철, 디지털정보계약법, 법문사, 2007

[14] 원윤재, "지능형 자동차 시스템 및 동향 분석", 정보처리학회지, 2008

[15] 은선기 외, "안전한 M2M 통신 구축을 위한 상호인증 및 키 교환 프로토콜", 한국정보보호학회논문지, 제20권 제1호, pp.74-76, 2010

[16] 조희석, RFID와 개인정보보호, <IT Solutions> 칼럼, 2005

[17] 중앙선데이, "21세기 네트워크 혁명, 1000억 대 단말기를 연결하라", 2009년 4월 18일자 기사

[18] 한국인터넷진흥원, 기기인증관리체계를 위한 최상위인증기관 인증업무 준칙, 2009

[19] 한국인터넷진흥원, 유비쿼터스 환경에 적합한 인증체계 구축을 위한 법제도 연구, 2008

[20] 한국인터넷진흥원, "일본의 정보보호 R&D 정책 현황 및 시사점", 2008

[21] 한국정보통신기술협회(TTA), “홈서버 중심의 홈네트워크 사용자 인증 메커니즘”, 2005
[22] 한국정보화진흥원, 사물통신기반 구축 및 사물정보이용 활성화에 관한 법률(안) 설명자료, 2009.11
[23] TTA, "[M2M] 기기간 통신(Machine to Machine Communication) 표준화 동향-유럽을 중심으로"
[24] CableLabs, CableLabs Certificate Issuance Process, 2006
[25] Cristoph Sorge, Conclusion of Contracts by electronic agents, ICAIL 05, June 6-11, Bologna, Italy, 2005
[26] European Parliament, Internet of things Procedure file, INI/2009/2224
[27] Government Purchase Guide, Case Study : Security-Enhanced BlackBerry Trial, 2007
[28] HowStuffWorks, "How Machine-to-Machine Communication Works"
[29] Inhyok Cha et al., “Trust in M2M communication”, IEEE Vehicular Technology Magazine, 2009
[30] Irene Kafeza et al., Legal Issues in Agents for Electronic Contracting
[31] ITU-T, “Ubiquitous Sensor Network", Technology Watch Briefing Report (2009)
[32] ITU-T, "The Internet of Things", 2005
[33] Jari Arkko et al., Weak Authentication: How to Authenticate Unknown Principals without Trusted Parties, Lecture Notes in Computer Science, 2003
[34] NIC, "Disruptive Civil Technologies", 2008
[35] NIST, Recommendation for Key Management - Part1 : General(Revised), 2007
[36] Patil and Willis, Identity based authentication in SIP, 2008
[37] US-CERT, INL, Common Control System Vulnerabilities, 2005
[38] Verisign, Device Certificate Services
[39] Žrko Sumić “Hype Cycle for Intelligent Grid Technologies”, Power Systems Engineering Research Center - Executive Forum on Smart Grid Deployment Strategies and Business Opportunities,, 2009