(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2016 년 1 월 28 일 (28.01.2016)

WIPO | PCT

(10) 국제공개번호
WO 2016/013846 A1

(51) 국제특허분류:
H04W 12/10 (2009.01) *H04W 4/00* (2009.01)

(21) 국제출원번호: PCT/KR2015/007546

(22) 국제출원일: 2015 년 7 월 21 일 (21.07.2015)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
62/026,704 2014 년 7 월 21 일 (21.07.2014) US
62/188,745 2015 년 7 월 6 일 (06.07.2015) US

(71) 출원인: 엘지전자 주식회사 (LG ELECTRONICS INC.) [KR/KR]; 150-721 서울시 영등포구 여의대로 128, Seoul (KR).

(72) 발명자: 김성윤 (KIM, Seongyun); 137-893 서울시 서초구 양재대로 11 길 19, LG 전자 특허센터, Seoul (KR). 박승규 (PARK, Seungkyu); 137-893 서울시 서초구 양재대로 11 길 19, LG 전자 특허센터, Seoul (KR). 안홍범 (AHN, Hongbeom); 137-893 서울시 서초구 양재대로 11 길 19, LG 전자 특허센터, Seoul (KR). 정승명 (JEONG, Seungmyeong); 137-893 서울시 서초구 양재대로 11 길 19, LG 전자 특허센터, Seoul (KR). 최희동 (CHOI, Heedong); 137-893 서울시 서초구 양재대로 11 길 19, LG 전자 특허센터, Seoul (KR).

(74) 대리인: 김용인 (KIM, Yong In) 등; 138-861 서울시 송파구 올림픽로 82, 7 층 KBK 특허법률사무소, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

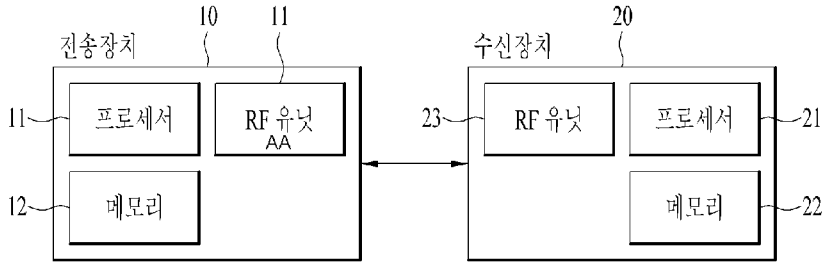
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) Title: METHOD FOR PROCESSING REQUEST MESSAGE IN WIRELESS COMMUNICATION SYSTEM AND APPARATUS THEREFOR

(54) 발명의 명칭 : 무선 통신 시스템에서 요청 메시지를 처리하기 위한 방법 및 이를 위한 장치



10 ... Transmitting device
11, 21 ... Processor
12, 22 ... Memory
20 ... Receiving device
23, AA ... RF unit

(57) Abstract: Suggested is a method for processing a request message in a wireless communication system according to one example of the present invention. The method comprises the steps of: receiving, by a first M2M entity, a request message relating to an operation for a specific resource from a second M2M entity; determining whether or not the first M2M entity has the specific resource; and if the first M2M entity does not have the specific resource, determining whether or not an integrity code is included in the request message, and if the integrity code is included in the request message, delivering the request message to a third M2M entity, or the method may comprise the steps of: if the first M2M entity has the specific resource, determining whether or not the first M2M entity has a registration relation with the second M2M entity; and if the first M2M entity has no registration relation with the second M2M entity, performing verification on the integrity code included in the request message.

(57) 요약서:

[다음 쪽 계속]

WO 2016/013846 A1

본 발명의 일 실시예에 따라 무선 통신 시스템에서 요청 메시지를 처리하기 위한 방법이 제안되며, 상기 방법은 제 1M2M 엔티티에 의해 수행되며, 제 2M2M 엔티티로부터 특정 자원에 대한 동작과 관련된 요청 메시지를 수신하는 단계, 상기 제 1M2M 엔티티가 상기 특정 자원을 가지고 있는지 여부를 판단하는 단계, 및 상기 제 1M2M 엔티티가 상기 특정 자원을 가지고 있지 않으면, 상기 요청 메시지에 무결성 코드가 포함되어 있는지 여부를 판단하는 단계, 상기 요청 메시지에 상기 무결성 코드가 포함되어 있으면, 상기 요청 메시지를 제 3M2M 엔티티로 전달하는 단계를 포함하고, 또는 상기 제 1M2M 엔티티가 상기 특정 자원을 가지고 있으면, 상기 제 1M2M 엔티티가 제 2M2M 엔티티와 등록관계가 있는지 여부를 판단하는 단계, 및 상기 제 1M2M 엔티티가 제 2M2M 엔티티와 등록관계가 없으면, 상기 요청 메시지에 포함된 무결성 코드에 대한 검증을 수행하는 단계를 포함할 수 있다.

명세서

발명의 명칭: 무선 통신 시스템에서 요청 메시지를 처리하기 위한 방법 및 이를 위한 장치

기술분야

[1] 본 발명은 무선 통신 시스템에서 요청 메시지를 처리하기 위한 방법 및 이를 위한 장치에 관한 것이다.

배경기술

[2] 유비쿼터스 시대에 접어들면서 M2M(Machine to Machine) 통신 기술이 각광 받고 있다. M2M 통신 기술은 TIA, ATIS, ETSI, oneM2M 등 많은 표준화 개발 기구(SDO: Standard Development Organization)에서 연구 중에 있다. M2M환경에서는 여러 M2M관련 애플리케이션(Network Application/Gateway Application/Device Application)간의 통신이 발생하고, M2M 플랫폼 또는 프레임워크(예컨대, 공통 서비스 엔티티(Common Service Entity; CSE)과 네트워크 측 애플리케이션(예컨대, Network Application)를 운용하는 주체가 다를 수 있다.

[3] 이에, 엔티티의 다른 엔티티로의 요청 메시지의 전달이 필수적이다. 그러나, 요청 메시지를 전송하는 주체가 본래의 목적이 아닌 다른 의도, 예컨대 위장(impersonation) 공격을 위해 상기 요청 메시지를 조작하여 다른 엔티티로 전달할 수 있다.

[4] 따라서, 본 발명은 M2M 시스템에서 메시지 전달과 관련하여 위장 공격 등의 보안 관련 공격을 방지하기 위한 방안을 제안하고자 한다.

발명의 상세한 설명

기술적 과제

[5] 본 발명은 메시지 전달과 메시지의 처리를 위한 방안을 제안하고자 하며, 좀더 상세하게는, 악의의 공격을 방지하기 위한 요청 메시지의 처리 방안에 대해 제안하고자 한다.

[6] 본 발명이 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 이하의 발명의 상세한 설명으로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

[7] 본 발명의 일 실시예에 따라 무선 통신 시스템에서 요청 메시지를 처리하기 위한 방법이 제안되며, 상기 방법은 제1M2M 엔티티에 의해 수행되며, 제2M2M 엔티티로부터 특정 자원에 대한 동작과 관련된 요청 메시지를 수신하는 단계, 상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있는지 여부를 판단하는 단계, 및 상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있지 않으면, 상기 요청

메시지에 무결성 코드가 포함되어 있는지 여부를 판단하는 단계, 상기 요청 메시지에 상기 무결성 코드가 포함되어 있으면, 상기 요청 메시지를 제3M2M 엔티티로 전달하는 단계를 포함하고, 또는 상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있으면, 상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 있는지 여부를 판단하는 단계, 및 상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 없으면, 상기 요청 메시지에 포함된 무결성 코드에 대한 검증을 수행하는 단계를 포함할 수 있다.

[8] 추가적으로 또는 대안으로, 상기 제1M2M 엔티티가 제2M2M엔티티와 등록관계가 있는지 여부를 판단하는 단계는 상기 요청 메시지에 포함된 발신자의 식별자와 제 2M2M 엔티티의 식별자가 동일한지 여부를 판단하는 단계를 포함할 수 있다.

[9] 추가적으로 또는 대안으로, 상기 제1M2M 엔티티가 제2M2M엔티티와 등록관계가 있는지 여부를 판단하는 단계는 상기 제1M2M 엔티티가 가지고 있는 자원의 특정 속성에 상기 제2M2M 엔티티와 상관관계가 있는 정보가 저장되어 있는지 여부를 판단하는 단계를 포함할 수 있다.

[10] 추가적으로 또는 대안으로, 상기 무결성 코드는, 상기 요청 메시지의 발신자와 상기 특정 자원을 가지고 있는 엔티티가 등록관계가 없는 경우에, 상기 발신자에 의해 상기 요청 메시지에 포함될 수 있다.

[11] 추가적으로 또는 대안으로, 상기 무결성 코드를 생성하기 위해 사용되는 정보들은 상기 요청 메시지의 발신자와 상기 특정 자원을 가지고 있는 엔티티에 의해 사전에 공유될 수 있다.

[12] 추가적으로 또는 대안으로, 상기 무결성 코드로 보호될 정보는 상기 요청 메시지의 특정 부분을 포함할 수 있다.

[13] 추가적으로 또는 대안으로, 상기 특정 부분은 상기 요청 메시지의 발신자 정보를 포함할 수 있다.

[14] 추가적으로 또는 대안으로, 상기 방법은 상기 제2M2M 엔티티의 식별자와 보안 연계(security association)와 관련한 크리덴셜(credential)과 연계된 식별자가 상관관계가 있는지 판단하는 단계를 더 포함할 수 있다.

[15] 추가적으로 또는 대안으로, 상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있는지 여부를 판단하는 단계는 상기 제2M2M 엔티티의 식별자와 보안 연계와 관련한 크리덴셜과 연계된 식별자가 상관관계가 있다고 판단된 경우에만 수행될 수 있다.

[16] 본 발명의 또다른 일 실시예에 따라 무선 통신 시스템에서 요청 메시지를 처리하도록 구성된 M2M 장치가 개시되며, 상기 M2M 장치는 무선 주파수(radio frequency, RF) 유닛 및 상기 RF 유닛을 제어하도록 구성된 프로세서를 포함하되, 상기 프로세서는 제2M2M 엔티티로부터 특정 자원에 대한 동작과 관련된 요청 메시지를 수신하고, 상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있는지 여부를 판단하고, 상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있지 않으면,

상기 요청 메시지에 무결성 코드가 포함되어 있는지 여부를 판단하고, 상기 요청 메시지에 상기 무결성 코드가 포함되어 있으면, 상기 요청 메시지를 제3M2M 엔티티로 전달하거나, 또는 상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있으면, 상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 있는지 여부를 판단하고, 그리고 상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 없으면, 상기 요청 메시지에 포함된 무결성 코드에 대한 검증을 수행하도록 구성될 수 있다.

[17] 추가적으로 또는 대안으로, 상기 프로세서는 상기 제1M2M 엔티티가 제2M2M엔티티와 등록관계가 있는지 여부를 판단하기 위해 상기 요청 메시지에 포함된 발신자의 식별자와 제 2M2M 엔티티의 식별자가 동일한지 여부를 판단하도록 구성될 수 있다.

[18] 추가적으로 또는 대안으로, 상기 프로세서는 상기 제1M2M 엔티티가 제2M2M엔티티와 등록관계가 있는지 여부를 판단하기 위해 상기 제1M2M 엔티티가 가지고 있는 자원의 특정 속성에 상기 제2M2M 엔티티와 상관관계가 있는 정보가 저장되어 있는지 여부를 판단하도록 구성될 수 있다.

[19] 추가적으로 또는 대안으로, 상기 무결성 코드는, 상기 요청 메시지의 발신자와 상기 특정 자원을 가지고 있는 엔티티가 등록관계가 없는 경우에, 상기 발신자에 의해 상기 요청 메시지에 포함될 수 있다.

[20] 추가적으로 또는 대안으로, 상기 무결성 코드를 생성하기 위해 사용되는 정보들은 상기 요청 메시지의 발신자와 상기 특정 자원을 가지고 있는 엔티티에 의해 사전에 공유될 수 있다.

[21] 추가적으로 또는 대안으로, 상기 무결성 코드로 보호될 정보는 상기 요청 메시지의 특정 부분을 포함할 수 있다.

[22] 추가적으로 또는 대안으로, 상기 특정 부분은 상기 요청 메시지의 발신자 정보를 포함할 수 있다.

[23] 추가적으로 또는 대안으로, 상기 프로세서는 상기 제2M2M 엔티티의 식별자와 보안 연계(security association)와 관련한 크리덴셜(credential)과 연계된 식별자가 상관관계가 있는지 판단하도록 구성될 수 있다.

[24] 추가적으로 또는 대안으로, 상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있는지 여부의 판단은 상기 제2M2M 엔티티의 식별자와 보안 연계와 관련한 크리덴셜과 연계된 식별자가 상관관계가 있다고 판단된 경우에만 수행될 수 있다.

[25] 상기 과제 해결방법들은 본 발명의 실시예들 중 일부에 불과하며, 본 발명의 기술적 특징들이 반영된 다양한 실시예들이 당해 기술분야의 통상적인 지식을 가진 자에 의해 이하 상술할 본 발명의 상세한 설명을 기반으로 도출되고 이해될 수 있다.

발명의 효과

[26] 본 발명의 일 실시예에 따르면, 메시지의 전달과 관련하여 악의의 공격을 방지할 수 있다.

[27] 본 발명에 따른 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과는 이하의 발명의 상세한 설명으로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[28] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부 도면은 본 발명에 대한 실시예를 제공하고, 상세한 설명과 함께 본 발명의 기술적 사상을 설명한다.

[29] 도 1은 M2M 통신 시스템에서의 기능 구조를 도시한다.

[30] 도 2는 M2M 기능 구조에 기반하여 M2M 통신 시스템이 지원하는 구성을 도시한다.

[31] 도 3은 M2M 통신 시스템에서 제공되는 공통 서비스 기능을 도시한다.

[32] 도 4는 M2M 애플리케이션 서비스 노드와 M2M 인프라스트럭쳐 노드에 존재하는 리소스 구조를 도시한다.

[33] 도 5는 M2M 애플리케이션 서비스 노드(예컨대, M2M 디바이스)와 M2M 인프라스트럭쳐 노드에 존재하는 리소스 구조를 도시한다.

[34] 도 6은 M2M 통신 시스템에서 사용하는 요청 및 응답 메시지를 주고받는 절차를 도시한다.

[35] 도 7은 <accessControlPolicy> 리소스의 구조를 도시한다.

[36] 도 8은 M2M 통신 시스템에서 등록 절차를 도시한다.

[37] 도 9는 본 발명의 일 실시예에 따른 위장 공격 방지를 위한 절차를 도시한다.

[38] 도 10은 본 발명의 일 실시예에 따른 위장 공격 방지를 위한 절차를 도시한다.

[39] 도 11은 본 발명의 일 실시예에 따른 위장 공격 방지를 위한 절차를 도시한다.

[40] 도 12는 본 발명의 일 실시예에 따른 위장 공격 방지를 위한 절차를 도시한다.

[41] 도 13은 본 발명의 일 실시예에 따른 위장 공격 방지를 위한 절차를 도시한다.

[42] 도 14은 본 발명의 일 실시예에 따른 위장 공격 방지를 위한 절차를 도시한다.

[43] 도 15는 본 발명의 실시예(들)을 수행하도록 구성된 장치의 블록도를 도시한다.

발명의 실시를 위한 최선의 형태

[44] 이하, 본 발명에 따른 바람직한 실시 형태를 첨부된 도면을 참조하여 상세하게 설명한다. 첨부된 도면과 함께 이하에 개시될 상세한 설명은 본 발명의 예시적인 실시형태를 설명하고자 하는 것이며, 본 발명이 실시될 수 있는 유일한 실시형태를 나타내고자 하는 것이 아니다. 이하의 상세한 설명은 본 발명의 완전한 이해를 제공하기 위해서 구체적 세부사항을 포함한다. 그러나, 당업자는 본 발명이 이러한 구체적 세부사항 없이도 실시될 수 있음을 안다.

[45] 몇몇 경우, 본 발명의 개념이 모호해지는 것을 피하기 위하여 공지의 구조 및 장치는 생략되거나, 각 구조 및 장치의 핵심기능을 중심으로 한 블록도 형식으로

도시될 수 있다. 또한, 본 명세서 전체에서 동일한 구성요소에 대해서는 동일한 도면 부호를 사용하여 설명한다.

[46] 본 발명에 있어서, 기기간 통신을 위한 디바이스 즉, M2M 디바이스는 고정되거나 이동성을 가질 수 있으며, 기기간 통신을 위한 서버 즉, M2M 서버와 통신하여 사용자데이터 및/또는 각종 제어정보를 송수신하는 각종 기기들이 이에 속한다. 상기 M2M 디바이스는 단말(Terminal Equipment), MS(Mobile Station), MT(Mobile Terminal), UT(User Terminal), SS(Subscribe Station), 무선기기(wireless device), PDA(Personal Digital Assistant), 무선 모뎀(wireless modem), 휴대기기(handheld device) 등으로 불릴 수 있다. 또한, 본 발명에 있어서, M2M 서버는 일반적으로 M2M 디바이스들 및/또는 다른 M2M 서버와 통신하는 고정된 지점(fixed station)을 말하며, M2M 디바이스들 및/또는 다른 M2M 서버와 통신하여 각종 데이터 및 제어정보를 교환한다.

[47] 이하에서는 본 발명과 관련된 기술에 대해 설명한다.

[48] M2M 애플리케이션

[49] 서비스 로직을 실행하고 개방 인터페이스를 통해 접근 가능한(accessible) 공통 서비스 엔티티(Common Service Entity; CSE)를 사용하는 애플리케이션. M2M 애플리케이션은 M2M 디바이스, M2M 게이트웨이 또는 M2M 서버에 설치 또는 탑재될 수 있다.

[50] M2M 공통 서비스

[51] 표준화된 인터페이스들을 통해 M2M CSE가 이용가능하게 하는 기능들의 집합

[52] oneM2M은 다양한 M2M 애플리케이션(또는 애플리케이션 엔티티(Application Entity; AE)) 들을 위한 공통 M2M 서비스 프레임워크(또는 서비스 플랫폼, 공통 서비스 엔티티(CSE) 등)를 정의한다. M2M 애플리케이션이라고 하면, e-Health, City Automation, Connected Consumer, Automotive 등의 서비스 로직을 구현한 소프트웨어라고 볼 수 있으며, 이러한 다양한 M2M 애플리케이션들을 구현하기 위해, 공통적으로 필요한 기능들을 oneM2M 서비스 프레임워크는 포함하고 있다. 따라서, oneM2M 서비스 프레임워크를 이용하면, 다양한 M2M 애플리케이션들 마다 필요한 각각의 프레임워크를 구성할 필요 없이, 이들 M2M 애플리케이션들을 쉽게 구현할 수 있다. 이는 현재 Smart Building, Smart Grid, e-Health, Transportation, Security 등 여러 M2M 버티컬(Vertical)들로 분열되어 있는 M2M 시장을 공통 oneM2M 서비스 프레임워크를 중심으로 통합할 수 있으며, 이는 M2M 시장을 크게 촉진할 것으로 기대된다.

[53] 도 1은 M2M 통신 시스템에서의 기능 구조를 도시한다. 각 엔티티를 설명하도록 한다.

[54] 애플리케이션 엔티티 (AE, 101): 애플리케이션 엔티티는 단대단 M2M 솔루션을 위한 애플리케이션 로직을 제공한다. AE의 예로는 화물 추적, 원격 혈당 모니터링, 원격 전력 측정 및 제어 애플리케이션이 있다. (Application Entity provides Application logic for the end-to-end M2M solutions. Examples of the

Application Entities can be fleet tracking application, remote blood sugar monitoring application, or remote power metering and controlling application.) 보다 쉬운 이해를 위해, AE는 M2M 애플리케이션으로 지칭될 수 있다.

[55] 공통 서비스 엔티티 (CSE, 102): CSE는 M2M 환경에 공통적인 oneM2M에서 정의된 서비스 기능들로 이루어져 있다. 이러한 서비스 기능들은 레퍼런스 포인트 Mca, Mcc를 통해 노출되어 등록된(연결된) AE와 타 CSE에 의해 사용될 수 있다. 레퍼런스 포인트 Mcn는 언더라잉 네트워크의 서비스를 접근하는데 사용된다. (A Common Services Entity comprises the set of "service functions" that are common to the M2M environments and specified by oneM2M. Such service functions are exposed to other entities through Reference Points Mca and Mcc. Reference point Mcn is used for accessing Underlying Network Service Entities.)

[56] CSE에서 제공하는 서비스 기능들의 예로는 데이터 관리, 디바이스 관리, M2M 구독(subscription) 관리, 위치 서비스 등이 있다. 이러한 기능들은 논리적으로 CSF(Common Services Functions)로 나뉘어 질 수 있다. CSE안의 몇몇 CSF는 필수적으로 존재하여야 하고, 몇몇은 선택적으로 존재 가능하다. 또한 CSF안의 몇몇 기능은 필수적으로 존재하여야 하고, 몇몇 기능은 선택적으로 존재 가능하다. (예, "디바이스 관리" CSF안에, 애플리케이션 소프트웨어 설치, 펌웨어 업데이트, 로깅, 모니터링 중 몇몇은 필수 기능이며, 몇몇은 선택 기능이다.)

[57] 언더라잉 네트워크 서비스 엔티티 (NSE, 103): NSE는 CSE에 서비스를 제공하는데, 이러한 서비스의 예로는 디바이스 관리, 위치 서비스, 디바이스 트리거링 등이 있다. NSE는 특정 기술로 한정하지 않으며, 네트워크가 기본적으로 제공해주는 트랜스포트(transport)의 경우 NSE의 서비스로 생각하지 않는다.(An Underlying Network Services Entity provides services to the CSEs. Examples of such services include device management, location services and device triggering. No particular organization of the NSEs is assumed. Note: Underlying Networks provide data transport services between entities in the oneM2M system. Such data transport services are not included in the NSE.)

[58] 아울러, 도 1에 도시된 각 레퍼런스 포인트에 대해 설명하도록 한다.

[59] <u>Mca 레퍼런스 포인트</u>

[60] Mca 레퍼런스 포인트는 AE와 CSE간의 레퍼런스 포인트이다. Mca 레퍼런스 포인트는 AE가 CSE가 제공하는 서비스를 사용할 수 있도록, AE가 CSE와 통신할 수 있도록 한다. (This is the reference point between an Application Entity and a CSE. The Mca reference point shall allow an Application Entity to use the services provided by the CSE, and for the CSE to communicate with the Application Entity.)

[61] Mca 레퍼런스 포인트를 통해 제공되는 서비스들은 CSE에서 제공하는 기능들에 의존한다. AE와 CSE는 같은 물리적 장치에 있을 수도 있으며, 다른 물리적 장치에 있을 수도 있다. (The services offered via the Mca reference point are

thus dependent on the functionality supported by the CSE. The Application Entity and the CSE it invokes may or may not be co-located within the same physical entity.)

[62] Mcc 레퍼런스 포인트

[63] Mcc 레퍼런스 포인트는 두 CSE간의 레퍼런스 포인트이다. Mcc 레퍼런스 포인트는 CSE가 다른 CSE의 필요한 기능의 서비스를 사용할 수 있도록 한다. Mcc 레퍼런스 포인트를 통해 제공되는 서비스들은 CSE에서 제공하는 기능들에 의존한다. (This is the reference point between two CSEs. The Mcc reference point shall allow a CSE to use the services of another CSE in order to fulfill needed functionality. Accordingly, the Mcc reference point between two CSEs shall be supported over different M2M physical entities. The services offered via the Mcc reference point are dependent on the functionality supported by the CSEs)

[64] Mcn 레퍼런스 포인트

[65] Mcn 레퍼런스 포인트는 CSE와 NSE간의 레퍼런스 포인트이다. Mcn 레퍼런스 포인트는 CSE가 NSE가 제공하는 서비스들을 사용할 수 있도록 한다. (This is the reference point between a CSE and the Underlying Network Services Entity. The Mcn reference point shall allow a CSE to use the services (other than transport and connectivity services) provided by the Underlying Network Services Entity in order to fulfill the needed functionality.) NSE가 제공하는 서비스는 전송(transport)과 접속(connectivity) 서비스 같은 단순한 서비스 이외의 것을 뜻하며, 디바이스 트리거링(device triggering), 스몰 데이터 전송(small data transmission), 위치 결정(positioning)과 같은 서비스가 그 예이다.

[66] Mcc' 레퍼런스 포인트

[67] Mcc' 레퍼런스 포인트는 서로 다른 M2M 서비스 제공자에게 속하는 CSE 간의 통신을 위해 사용된다. Mcc' 레퍼런스 포인트는 Mcc 레퍼런스 포인트와 CSE를 서로 연결한다는 점에서 비슷할 수 있으나, 기존 Mcc 레퍼런스 포인트가 단일 M2M 서비스 제공자 내의 통신으로 국한되어 있었다면 Mcc' 레퍼런스 포인트는 서로 다른 M2M 서비스 제공자로 Mcc를 확장한다는 개념으로 볼 수 있다.

[68] 도 2는 M2M 기능 구조에 기반하여 M2M 통신 시스템이 지원하는 구성을 도시한다. M2M 통신 시스템은 도시된 구성에 국한되지 않고 더 다양한 구성을 지원할 수 있다. 상기 도시된 구성을 이해하는데 중요한 노드(Node)라는 개념에 대해 먼저 설명하도록 한다.

[69] 애플리케이션 전용 노드(Application Dedicated Node; ADN): CSE가 존재하지 않고, 적어도 하나의 AE를 갖는 노드 (An Application Dedicated Node is a Node that contains at least one Application Entity and does not contain a Common Services Entity). Mca 레퍼런스 포인트를 통해 하나의 미들 노드 또는 하나의 인프라스트럭쳐 노드와 연결될 수 있다. ADN은 M2M 디바이스에 존재할 수 있다.

[70] 애플리케이션 서비스 노드(Application Service Node; ASN): 하나의 CSE가

존재해야 하고, 적어도 하나의 AE를 갖는 노드(An Application Service Node is a Node that contains one Common Services Entity and contains at least one Application Entity). Mcc 레퍼런스 포인트를 통해 하나의 미들 노드 또는 하나의 인프라스트럭쳐 노드에 연결될 수 있다. ASN은 M2M 디바이스에 존재할 수 있다.

[71] 미들 노드(Middle Node; MN): 하나의 CSE가 존재해야 하고, AE를 가질 수도 있는 노드(A Middle Node is a Node that contains one Common Services Entity and may contain Application Entities). Mcc 레퍼런스 포인트를 통해서 아래 다른 카테고리에 속하는 두 노드와 연결되어야 함 (A Middle Node communicates over a Mcc references point with at least two other Nodes among either (not exclusively)):

[72] - 하나 이상의 애플리케이션 서비스 노드(ASN)들;

[73] - 하나 이상의 미들 노드(MN)들;

[74] - 하나 인프라스트럭쳐 노드(IN).

[75] 또한, MN은 ADN과 Mca 레퍼런스 포인트를 통해 연결될 수 있다. MN은 M2M 게이트웨이에 존재할 수 있다.

[76] 인프라스트럭쳐 노드(Infrastructure Node; IN): 하나의 CSE가 존재해야 하고, AE를 가질 수도 있는 노드 (An Infrastructure Node is a Node that contains one Common Services Entity and may contain Application Entities). IN은 M2M 서버에 존재할 수 있다.

[77] 인프라스트럭쳐 노드는 MN 또는 ASN과 Mcc 레퍼런스 포인트를 통해 다음 노드들과 통신할 수 있다. (An Infrastructure Node communicates over a Y reference point with either:

[78] - 하나 이상의 미들 노드(들);

[79] - 및/또는 하나 이상의 애플리케이션 서비스 노드(들)

[80] 인프라스트럭쳐 노드는 ADN과 Mca 레퍼런스 포인트를 통해 통신할 수 있다. (An Infrastructure Node may communicate with one or more Application Dedicated Nodes over one or more respective Mca reference points.)

[81] 도 3은 M2M 통신 시스템에서 제공되는 공통 서비스 기능을 도시한다.

[82] M2M 통신 시스템이 제공하는 M2M 서비스 기능(즉, 공통 서비스 기능)으로는 도 3에 도시된 것처럼 'communication Management and Delivery Handling', 'Data Management and Repository', 'Device Management', 'Discovery', 'Group Management', 'Addressing and Identification', 'Location', 'Network Service Exposure, Service Execution and Triggering', 'Registration', 'Security', 'Service Charging and Accounting', 'Session Management', 'Subscription and Notification'이 있다.

[83] 아래는 각 기능의 간략한 소개이다.

[84] Communication Management and Delivery Handling (CMDH): 타 CSE들, AE들, NSE들과의 통신을 제공하고 어떻게 메시지를 전달할 지의 역할을 수행한다.

[85] Data Management and Repository (DMR): M2M 애플리케이션이 데이터를 교환,

공유할 수 있도록 하는 역할을 수행한다.

[86] Device Management (DMG): M2M 디바이스/게이트웨이를 관리하기 위한 역할을 수행한다. 세부 기능을 살펴보면, 애플리케이션 설치 및 세팅, 설정값 설정, 펌웨어(Firmware) 업데이트, 로깅(Logging), 모니터링(Monitoring), 진단(Diagnostics), 토폴로지(Topology) 관리 등이 있다.

[87] Discovery (DIS): 조건에 기반한 리소스 및 정보를 찾을 수 있도록 하는 역할을 수행한다.

[88] Group Management (GMG): 리소스, M2M 디바이스, 또는 게이트웨이를 묶어 그룹을 생성할 수 있는데, 그룹과 관련된 요청을 처리하는 역할을 수행한다.

[89] Addressing and Identification (AID): 물리 또는 논리 리소스를 식별 및 어드레싱(addressing)하는 역할을 수행한다.

[90] Location (LOC): M2M 애플리케이션들이 M2M 디바이스 또는 게이트웨이의 위치 정보를 획득하도록 하는 역할을 수행한다.

[91] Network Service Exposure, Service Execution and Triggering (NSE): 언더라잉 네트워크의 통신을 가능하게 하고, 언더라잉 네트워크가 제공하는 기능을 사용할 수 있도록 한다.

[92] Registration (REG): M2M 애플리케이션 또는 다른 CSE가 특정 CSE에 등록을 처리하는 역할을 수행한다. 등록은 특정 CSE의 M2M 서비스 기능을 사용하기 위해 수행된다.

[93] Security (SEC): 보안 키와 같은 민감한 데이터 핸들링, 보안 관계(Association) 설립, 인증(Authentication), 인가(Authorization), 식별(Identity) 보호 등의 역할을 수행한다.

[94] Service Charging and Accounting (SCA): CSE에 요금 부가 기능을 제공하는 역할을 수행한다.

[95] Session Management (SM): 단대단(end-to-end) 통신을 위한 M2M 세션을 관리하는 역할을 수행한다.

[96] Subscription and Notification (SUB): 특정 리소스에 대한 변경을 구독(Subscription)하면 해당 리소스가 변경되면 이를 알리는 역할을 수행한다.

[97] 이러한 M2M 공통 서비스 기능은 CSE를 통해 제공되며, AE(혹은, M2M 애플리케이션들)이 Mca 레퍼런스 포인트를 통해, 또는 타 CSE가 Mcc 레퍼런스 포인트를 통해 해당 공통 서비스 기능들을 이용할 수 있다. 또 이러한 M2M 공통 서비스 기능은 언더라잉 네트워크(Underlying Network)(또는 언더라잉 네트워크 엔티티(Underlying Network Service Entity; NSE), 예: 3GPP, 3GPP2, WiFi, Bluetooth)와 연동하여 동작할 수 있다.

[98] 모든 디바이스/게이트웨이/인프라스트럭처가 상위 기능을 다 가지는 것은 아니다. 해당 기능들 중 필수 기능들과 선택 기능들 몇몇을 가질 수 있다.

[99] M2M 통신 시스템에서 리소스는 M2M 통신 시스템에서 정보를 구성 및 표현하기 위한 것으로 URI로 식별될 수 있는 모든 것을 의미한다. 상기 리소스는

일반적인 리소스, 가상 리소스 및 어나운스된 리소스(announced resource)로 분류할 수 있다. 각 리소스에 대한 정의는 다음과 같다.

[100] 가상 리소스: 가상 리소스는 특정 프로세싱을 트리거하거나 그리고/또는 결과를 리트리브(retrieve)하는데 사용되나, CSE에 영구적으로 존재하지 않는다.

[101] 어나운스된 리소스: 어나운스된 리소스는 어나운스된(또는 통지된) 원본 리소스에 연결된 원격 CSE에 있는 리소스이다. 어나운스된 리소스는 원본 리소스의 특징 중 일부를 유지한다. 리소스 어나운스먼트는 리소스 탐색 또는 발견(discovery)를 원활하게 한다. 원격 CSE에 있는 어나운스된 리소스는 상기 원격 CSE에서 원본 리소스의 자식으로서 존재하지 않거나 원본 리소스의 어나운스된 자식이 아닌 자식 리소스들을 생성하기 위해 사용된다.

[102] 일반 리소스: "가상" 또는 "어나운스된" 중 하나로 명시되지 않으면, 해당 리소스는 일반 리소스이다.

[103] 도 4는 M2M 애플리케이션 서비스 노드와 M2M 인프라스트럭쳐 노드에 존재하는 리소스 구조를 도시한다.

[104] M2M 통신 시스템은 다양한 리소스(또는 자원)를 정의하는데, 이 리소스를 조작해서, 애플리케이션을 등록하고, 센서 값을 읽어 오는 등의 M2M 서비스를 수행할 수 있다. 상기 리소스는 하나의 트리 구조로 구성이 되며, CSE과 논리적으로 연결 또는 CSE에 저장되어 M2M 디바이스, M2M 게이트웨이, 네트워크 도메인 등에 저장될 수 있다. 이러한 측면에서, CSE는 리소스를 관리하는 엔티티로 지칭될 수 있다. 상기 리소스는 <cseBase>를 트리 루트로 가지며, 대표적인 리소스는 아래와 같다.

[105] <cseBase> 리소스: 트리로 구성된 M2M 리소스의 루트 리소스이며, 다른 모든 리소스를 포함한다.

[106] <remoteCSE> 리소스: <cseBase> 하위에 존재하는 리소스로써 해당 CSE에 등록(연결)된 타 CSE의 정보가 포함된다.

[107] <AE> 리소스: <cseBase> 나 <remoteCSE> 리소스 하위에 존재하는 리소스로써, <cseBase> 의 하위에 존재할 경우 해당 CSE에 등록(연결)된 애플리케이션들의 정보가 저장되며, <remoteCSE> 하위에 존재할 경우 타 CSE(CSE 이름을 가진)에 등록된 애플리케이션들의 정보가 저장된다.

[108] <accessControlPolicy> 리소스: 특정 리소스에 대한 접근 권한과 관련된 정보를 저장하는 리소스이다. 본 리소스에 포함된 접근 권한 정보를 이용하여, 인증(authorization)이 이루어지게 된다.

[109] <container> 리소스: CSE별, 또는 AE마다 데이터를 저장하는 리소스이다.

[110] <group> 리소스: 여러 리소스를 하나로 묶어 함께 처리할 수 있도록 하는 기능을 제공하는 리소스이다.

[111] <subscription> 리소스: 리소스의 값 등의 상태가 변경되는 것을 통지(notification)을 통해 알려주는 기능을 수행하는 리소스이다.

[112] 도 5는 M2M 애플리케이션 서비스 노드(예컨대, M2M 디바이스)와 M2M

인프라스트럭쳐 노드에 존재하는 리소스 구조를 도시한다.

[113] 예를 들어, M2M 인프라스트럭쳐 노드에 등록된 AE(application2)가 M2M 디바이스의 센서 값을 읽어오는 방법에 대해 설명한다. 상기 센서는 보통 물리적인 장치를 가리키며, M2M 디바이스 상에 존재하는 AE(application1)은 이 센서에서 값을 읽어 자신이 등록한 CSE(CSE1)에 container 리소스 형태로 읽은 값을 저장한다. 해당 M2M 디바이스 상에 존재하는 AE는 이를 위해 M2M 디바이스에 존재하는 CSE에 먼저 등록되어야 하며, 등록이 완료되면, 도 5에서와 같이 cseBaseCSE1/application1 리소스의 형태로 등록된 M2M 애플리케이션 관련 정보가 저장된다.

[114] cseBaseCSE1/application1 리소스 하위의 container 리소스에 센서 값이 M2M 디바이스상에 존재하는 AE에 의해 저장되면, 인프라스트럭쳐 노드에 등록된 AE가 해당 값에 접근이 가능할 수 있다. 접근이 가능하게 하기 위해서는 상기 인프라스트럭쳐 노드에 등록된 AE도 역시 상기 인프라스트럭쳐 노드의 CSE(CSE2)에 등록이 되어있어야 하며, 이는 application1가 CSE1에 등록하는 방법과 같이 cseBaseCSE2/application2 리소스에 application2에 대한 정보를 저장함으로써 이루어진다. 또, application1는 application2와 직접 통신하는 것이 아니라 중간의 CSE1과 CSE2을 통해 통신하게 되는데, 이를 위해 먼저 CSE1는 CSE2에 등록되어 있어야 한다. CSE1이 CSE2에 등록되게 되면, cseBaseCSE2 리소스 하위에 CSE1 관련 정보(예컨대, Link)가 <remoteCSE> 리소스 형태로 저장된다. 즉, <remoteCSE>는 등록된 CSE에 대한 CSE 타입, 접근 주소(IP 주소 등), CSE ID, reachability 정보 등을 제공해 준다.

[115] 한편, 리소스 탐색(resource discovery)이란 원격의 CSE에 있는 리소소를 탐색하는 과정을 말한다. 리소스 탐색은 리트리브(RETRIEVE) 요청을 통해 이루어 지며 리소스 탐색을 위해 리트리브 요청은 아래의 내용을 포함한다.

[116] <startURI>: URI을 지시하며, 이 URI는 리소스 탐색을 행할 리소스의 범위를 제한하는데 사용될 수 있다. 만약 <startURI>가 리소스의 루트인 <cseBase>를 가리킨다면, 본 리트리브 요청을 받은 수신자의 전 리소스를 대상으로 리소스 탐색을 수행하게 된다. 수신자는 <startURI>가 지칭하는 리소스와 그 하위 리소스를 대상으로만 리소스 탐색을 수행하게 된다.

[117] filterCriteria: 이 정보에는 탐색할 리소스와 관련된 정보가 기술된다. 수신자는 <startURI>가 정의한 리소스 탐색 범위 안의 리소스 중에서 filterCriteria를 만족시키는 리소스만을 검색하여 본 요청의 요청자에게 전송하게 된다.

[118] 도 4 또는 도5에 도시된 것처럼 M2M 시스템에서는 리소스가 트리 구조로서 표현될 수 있으며, 루트 리소스의 타입은 <CSEBase>로 표현된다. 따라서, <CSEBase> 리소스 타입은 공통 서비스 엔티티(CSE)가 있는 경우에는 반드시 존재해야 한다.

[119] 도 6은 Mca 및 Mcc 레퍼런스 포인트들 상의 일반적인 통신 플로우를 도시한다. M2M 시스템의 동작은 데이터 교환을 기반으로 수행된다. 예를 들어, 제1장치가

제2장치의 특정 동작을 멈추기 위한 명령을 전송 또는 수행하기 위해서 상기 제1장치는 해당 명령을 데이터 형태로 상기 제2장치에 전달해야한다. M2M시스템에서는 어플리케이션(또는 CSE)와 CSE간의 연결에서 요청 및 응답 메시지들로 데이터를 교환할 수 있다.

[120] 요청(Request) 메시지에는 다음과 같은 정보가 포함된다.

[121] ·Operation: 실행될 동작의 형태 (Create/Retrieve/Update/Delete/Notify 중 택일)

[122] ·To: 요청을 수신할 엔티티의 ID(즉, 수신자의 ID)

[123] ·From: 요청을 생성한 발신자의 ID

[124] ·Request Identifier: 요청 메시지의 ID(요청 메시지를 구분하기 위해 사용되는 ID)

[125] ·Content: 전달되는 리소스의 내용

[126] 응답(Response) 메시지에는 다음과 같은 정보가 포함된다. 우선 해당 요청 메시지가 성공적으로 처리된 경우에는, 상기 응답 메시지는

[127] ·To: 요청을 생성한 발신자의 ID

[128] ·From: 요청을 수신한 수신자의 ID

[129] ·Request Identifier: 요청 메시지의 ID(요청 메시지를 구분하기 위해 사용되는 ID)

[130] ·Result content: 요청의 처리 결과 (예를 들어, Okay, Okay and Done, Okay and in progress)

[131] ·Content: 전달되는 리소스의 내용 (결과값(rs)만 전달될 수 있음)

[132] 를 포함하고, 요청 메시지의 처리가 실패한 경우 상기 응답 메시지는

[133] ·To: 요청을 생성한 발신자의 ID

[134] ·From: 요청을 수신한 수신자의 ID

[135] ·Request Identifier: 요청 메시지의 ID(요청 메시지를 구분하기 위해 사용되는 ID)

[136] ·rs: 요청의 처리 결과 (예를 들어, Not Okay)

[137] 를 포함할 수 있다.

[138] 한편, 다음의 표와 같은 다양한 리소스 타입이 존재한다.

[139] 표 1

[표1]

Resource Type	**Short Description**	**Child Resource Types**	**Parent Resource Types**
AE	AE에 관한 정보를 저장한다. 등록자 CSE와 AE의 성공적인 등록의 결과로서 생성된다)Stores information about the AE. It is created as a result of successful registration of an AE with the registrar CSE).	*subscription, container, group, accessControlPolicy, mgmtObj, commCapabilities, pollingChannel*	*remoteCSE, CSEBase*
cmdhNwAccessRule	네트워크의 사용을 위한 규칙을 정의한다(Defines a rule for the usage of underlying networks).	*schedule*subscription	*cmdhNetworkAccessRules*
CSEBase	해당 CSE 상에 존재하는 모든 리소스들을 위한 구조적인 뿌리(root)이다. 해당 CSE 자체에 관한 정보를 저장해야 한다(The structural root for all the resources that are residing on a CSE. It shall store information about the CSE itself).	*remoteCSE, node, application, container, group, accessControlPolicy, subscription, mgmtObj, mgmtCmd, locationPolicy, statsConfig*	*None*
group	그룹으로 처리될 필요가 있는 동일한 타입의 리소스에 관한 정보를 저장한다. 그룹 리소스에	*fanOutPoint*subscription	*Application, remoteCSE, CSEBase*

	대한 동작은 해당 그룹에 속한 모든 멤버들을 위한 벌크 모드로 수행되어야 한다(Stores information about resources of the same type that need to be addressed as a Group. Operations addressed to a Group resource shall be executed in a bulk mode for all members belonging to the Group).		
locationPolicy	지리적 위치를 획득하고 관리하기 위한 정보를 포함한다. 오직 컨테이너로부터 지칭되며 해당 컨테이너의 contentInstances가 위치 정보를 제공한다(Includes information to obtain and manage geographical location. It is only referred from container, the *contentInstances* of the container provides location information).	*subscription*	*CSEBase*
remoteCSE	CSEBase 리소스에 의해 식별되는 등록자 CSE와 등록 절차를 한 원격 CSE를 나타낸다(Represents a remote CSE for which there has been a registration procedure with the registrar CSE identified by the CSEBase resource).	*application, container, group, accessControlPolicy, subscription, mgmtObj, pollingChannel, node*	*CSEBase*
subscription	리소스와 관련된 구독 정보를 나타낸다. 이러한 리소스는 subscribe-to 리소스를 위한 자식 리소스이다(Subscription resource represents the subscription information related to a resource.	*schedule*	*accessControlPolicy, application, cmdhBuffer, cmdhDefaults, cmdhEcDefParamValues, cmdhDefEcValue,*

	Such a resource shall be a child resource for the subscribe-to resource).		*cmdhLimits, cmdhNetworkAccessRules, cmdhNwAccessRule, cmdhPolicy, container, CSEBase, delivery, eventConfig, execInstance, group, contentInstance, locationPolicy, mgmtCmd, mgmtObj, m2mServiceSubscription, node, nodeInfo, parameters, remoteCSE, request, schedule, statsCollect, statsConfig*
container	엔티티들 사이에서 데이터 인스턴스들을 공유함. AE들 또는 CSE들 사이에서 "데이터"를 교환하기 위한 데이터를 버퍼링에 책임이 있는 중재자로서 사용됨(Shares data instances among entities. Used as a mediator that takes care of buffering the data to exchange "data" between AEs and/or CSEs).	*container, contentInstance, subscription*	*application, container, remoteCSE, CSEBase*
contentInstance	상기 container 리소스에 존재하는 데이터 인스턴스들을 나타낸다(Represents a data instance in the container resource).	*subscription*	*container*

[140] 각 리소스 타입은 해당 리소스 타입의 부모 리소스 타입(Parent Resource Type) 아래 위치할 수 있으며, 자식 리소스 타입(Child Resource Type)을 가질 수도 있다. 또한 각각의 리소스 타입은 속성(Attribute)들을 가지며, 속성에 실제 값들이 저장된다.

[141] 다음으로 아래 표 2은 <container> 리소스 타입의 속성(Attribute)들을 정의한

것이다. 실제 값들이 저장되는 속성은 Multiplicity를 통하여 반드시 설정('1')되거나, 선택적으로 설정('0..1')될 수 있다. 또한 해당 속성들은 생성시 특성에 따라 RO(Read Only), RW(Read and Write), WO(Write Only)와 같이 설정된다. 한편, 표 1에 나타낸 것처럼, <container> 리소스는 자식 리소스로서 <container>, <contentInstance> 및 <subscription>를 가질 수 있다.

[142] 표 2

[표2]

Attributes of <*container*>	**Multiplicity**	**RW/RO/ WO**	**Description**
resourceType	1	RO	리소스 타입. 이는 한번 쓰여지며(특정 시간 이후 변경될 수 없음)리소스들의 타입을 식별한다. 각각의 리소스는 리소스 타입 속성을 갖는다(Resource Type. This Write Once (at creation time then cannot be changed) resourceType attribute identifies the type of resources. Each resource shall have a *resourceType* attribute.)
resourceID	1	RO	이 속성은 '비-계층적 URI 방법' 또는 'ID 기반 방법' 경우를 위해 사용되는 리소스를 위한 식별자이다. 이 속성은 호스팅 CSE가 리소스 생성 절차를 수락하는 경우에 상기 호스팅 CSE에 의해 제공된다. 상기 호스팅 CSE는 고유한 리소스 ID를 할당한다(This attribute is an identifier for resource that is used for 'non-hierarchical URI method'or 'IDs based method' cases. This attribute shall be provided by the Hosting CSE when it accepts a resource creation procedure. The Hosting CSE shall assign a *resourceID* which is unique in the CSE).
parentID	1	RO	시스템은 생성(CREATE) 요청에서 주어진 파라미터들에 따라 이 속성에 값을 할당한다. 이 자식 리소스의 부모의 식별자에 의해 부모-자식 관계가

			성립된다. 이러한 식별자는 비-계층적 URI 표현 방법을 사용한다. 예를 들어, 리소스 ".../example.com/oneM2M/myCSE "하위에 생성된 식별자 "mytAE1"를 갖는 AE 리소스의 부모ID의 값은 ".../parentID"를 포함한다(The system shall assign the value to this attribute according to the parameters given in the CREATE Request.It establishes the parent-child relationship by identification of the parent of this child resource. Such identifier shall use the non-hierarchical URI representation. For example, an AE resource with the identifier "myAE1" which has been created under the resource ".../example.com/oneM2M/myCSE ", the value of the *parentID* attribute will contain ".../parent*ID* ".)
expirationTime	1	RW	호스팅 CSE에 의해 리소스가 지워질 시간/날짜. 이 속성은 발신자(originator)에 의해 제공될 수 있고, 이러한 경우에 리소스의 수명(lifetime)에 대한 호스트 CSE에 대한 힌트(hint)로 여겨진다. 상기 호스팅 CSE는 그러나 실제 만료 시간에 대해 결정할 수 있다. 만약 상기 호스팅 CSE가 만료 시간 속성 값을 변경하고자 결정하면, 이는 상기 발신자에게 알려진다. 상기 리소스의 수명은 갱신(UPDATE) 동작에서 이 속성에 대한 새 값을

			제공함으로써 연장될 수 있다. 또는 상기 속성 값을 삭제함으로써, 예컨대 상기 호스팅 CSE가 새 값을 결정할 수 있는 전체 갱신을 하는 경우에 상기 속성을 제공하지 않음으로써, 상기 리소스의 수명은 연장될 수 있다. 이 속성은 필수 속성이다. 만약 상기 발신자가 생성(CREATE) 동작에서 값을 제공하지 않으면, 시스템이 로컬 정책 및/또는 M2M 서비스 구독 협의에 따라 적절한 값을 할당한다(Time/date after which the resource will be deleted by the hosting CSE. This attribute can be provided by the Originator, and in such a case it will be regarded as a hint to the hosting CSE on the lifetime of the resource. The hosting CSE can however decide on the real expirationTime. If the hosting CSE decides to change the *expirationTime* attribute value, this is communicated back to the Originator.The lifetime of the resource can be extended by providing a new value for this attribute in an UPDATE operation. Or by deleting the attribute value, e.g. by not providing the attribute when doing a full UPDATE, in which case the hosting CSE can decide on a new value.This attribute shall be mandatory. If the Originator does not provide a value in the CREATE operation the

			system shall assign an appropriate value depending on its local policies and/or M2M service subscription agreements).
accessControlPolicyIDs	0..1 (L)	RW	이 속성은 <accessControlPolicy> 리소스의 식별자(로컬 리소스가 존재하는지 여부에 따라 ID 또는 URI임)의 리스트를 포함한다. 참조된 <accessControlPolicy> 리소스에서 정의된 권한들은 누가 특정 목적(예컨대, 검색(Retrieve), 갱신, 삭제(Delete) 등)을 위해 이 속성을 포함하는 리소스에 접근하도록 허용되는지를 결정한다(The attribute contains a list of identifiers (either an ID or a URI depending if it is a local resource or not) of an <accessControlPolicy> resource. The privileges defined in the <accessControlPolicy> resource that are referenced determine who is allowed to access the resource containing this attribute for a specific purpose (e.g. Retrieve, Update, Delete, etc.)).
labels	0..1	WR	리소스들을 발견하기 위한 키(key)들로서 사용되는 토큰들. 이 속성은 선택 속성이며 만약 존재하지 않으면 상기 리소스가 상기 발견의 키 파라미터로서 이 속성을 사용하는 발견 절차를 통해 발견될 수 없음을 의미한다(Tokens used as keys for discovering resources.This attribute is optional and if not present it

			means that the resource cannot be found by means of discovery procedure which uses *labels* as key parameter of the discovery).
creationTime	1	RO	상기 리소스의 생성 시간/날짜.이 속성은 모든 리소스들에 대해 필수 속성이며 상기 값은 리소스가 국부적으로 생성되는 경우에 시스템에 의해 할당된다. 이러한 속성은 변경될 수 없다(Time/date of creation of the resource.This attribute is mandatory for all resources and the value is assigned by the system at the time when the resource is locally created. Such an attribute cannot be changed.)
creator	0..1	RO	상기 <container> 리소스를 생성한 AE-ID 또는 CSE-ID(The AE-ID or CSE-ID of the entity which created the resource).
lastModifiedTime	1	RO	상기 리소스의 마지막으로 변경된 시간/날짜.이 속성은 필수 속성이며 해당 값은 타깃 리소스가 갱신 동작을 통해 변경될 때마다 시스템에 의해 자동으로 할당된다(Last modification time/date of the resource.This attribute shall be mandatory and its value is assigned automatically by the system each time that the addressed target resource is modified by means of the UPDATE operation.)
stateTag	1	RO	리소스에 대한 변경의 회수를 새는 카운터(counter). 리소스가 생성되면, 이 카운터는 0으로

			설정되고, 매 리소스의 변경시에 따라 증가됨. 새로운 인스턴스가 부모 리소스에 추가되면, 상기 부모 리소스의 stateTag 속성이 먼저 증가되고 이 stateTag 속성에 복사되어야 한다 (An incremental counter of modification on the resource. When a resource is created, this counter is set to 0, and it will be incremented on every modification of the resource. The *stateTag* attribute of the parent resource should be incremented first and copied into this *stateTag* attribute when a new instance is added to the parent resource).
announceTo	0..1	RW	이 속성은 생성 또는 갱신 요청이 생성/갱신된 리소스가 어나운스될 URI들/CSE-ID들의 리스트를 포함하는 경우에 상기 생성 또는 갱신 요청에 포함될 수 있다. 이 속성은 원 리소스가 성공적으로 다른 CSE들에게 어나운스되면 상기 원 리소스에 대해서만 존재한다. 이 속성은 성공적으로 어나운스된 리소스들로의 URI들의 리스트를 유지한다. 이 속성에 대한 갱신들은 새로운 리소스 어나운스 또는 어나운스 해제를 트리거할 것이다(This attribute may be included in a CREATE or UPDATE Request in which case it contains a list of URIs/CSE-IDs which the resource being created/updated shall be announced

			to.This attribute shall only be present on the original resource if it has been successfully announced to other CSEs. This attribute maintains the list of URIs to the successfully announced resources. Updates on this attribute will trigger new resource announcement or de-announcement).
announcedAttribute	0..1	RW	이 속성은 몇몇 선택적 어나운스(OA)된 타입 속성들이 다른 CSE들로 어나운스된 경우 원 리소스에 대해서만 존재한다. 이 속성은 원 리소스에서 어나운스된 선택적 속성들(OA 타입 속성들)의 리스트를 유지한다. 이 속성에 대한 갱신은 만약 새로운 속성이 추가되는 경우 새로운 속성 어나운스 또는 존재하는 속성이 제거되는 경우 어나운스 해제를 트리거할 것이다(This attributes shall only be present on the original resource if some Optional Announced **(OA)** type attributes have been announced to other CSEs. This attribute maintains the list of the announced Optional Attributes (**OA** type attributes) in the original resource. Updates to this attribute will trigger new attribute announcement if a new attribute is added or de-announcement if the existing attribute is removed.)
maxNrOfInstances	0..1	RW	<contentInstance> 자식 리소스들의 최대 인스턴스의 수(Maximum number of instances

			of <contentInstance> child resources).
maxByteSize	0..1	RW	<container> 리소스에 있는 모든 인스턴스들을 위한 상기 <container> 리소스를 위해 할당된 최대 바이트 수(Maximum number of bytes that are allocated for a <container> resource for all instances in the <container> resource).
maxInstanceAge	0..1	RW	<container> 내의 <containerInstance> 리소스들의 인스턴스의 최대 나이(age). 해당 값은 초로 표현됨(Maximum age of the instances of <contentInstance> resources within the <container>. The value is expressed in seconds).
currentNrOfInstances	1	RO	<container> 리소스에 현재 있는 인스턴스의 수. maxNrOfInstances에 의해 제한됨(Current number of instances in a <container> resource. It is limited by the maxNrOfInstances).
currentByteSize	1	RO	<container> 리소스에 저장된 데이터의 바이트로 표현되는 현재 크기. maxNrOfBytes에 의해 제한됨(Current size in bytes of data stored in a <container> resource. It is limited by the maxNrOfBytes).
latest	0..1	RO	존재하는 경우, 최근 <contentInstance> 리소스에 대한 참조(Reference to latest <contentInstance> resource, when

			present).
locationID	0..1	RW	어떻게 위치 정보가 획득되고 관리되는지를 정의하는 속성들/정책들이 있는 리소스의 URI. 이 속성은 <container> 리소스가 위치 정보를 포함하기 위해 사용되는 경우에만 정의됨(URI of the resource where the attributes/policies that define how location information are obtained and managed. This attribute is defined only when the <container> resource is used for containing location information).
ontologyRef	0..1	RW	상기 AE에 의해 관리되고 이해되는 정보를 나타내기 위해 사용되는 온톨로지(ontology)의 URI(A URI of the ontology used to represent the information that is managed and understood by the AE).여기서, 온톨로지는 다루고자하는 도메인에서 사용되는 용어들을 정의하고 그들 사이의 관계를 정의하는 명세를 지칭한다.

[143] 리소스 접근 제어 정책

[144] 접근 제어 정책은 "화이트 리스트(white list)"또는 권한(privileges)으로 정의되며, 각각의 권한은 특정 접근 모드들에 대한 "허용된" 엔티티들을 정의한다. 권한들의 집합들은 권한 그룹을 위한 권한들이 개별 권한들의 총합(sum)이 되도록 다루어지며, 즉, 상기 집합 내 몇몇/임의의 권한들에 의해 허용되면 그 동작(action)이 허용된다. selfPrivilege 속성은 리소스 <accessControlPolicy> 그 자체를 위한 읽기/갱신/삭제(Read/Update/Delete)에 대한 권리를 갖는 엔티티들을 열거한다.

[145] 또한, 접근 제어 정책에서 정의된 모든 권한들은 위치, 타임 윈도우 및 IP 어드레스와 또한 관련된다.

[146] 리소스 상의 accessControlPolicyID 속성을 설정함으로써, 해당 리소스에 접근하기 위한 권한들이 <accessControlPolicy> 리소스에서 정의되는 권한들에

의해 정의된다.

[147] 도 7은 <accessControlPolicy> 리소스의 구조를 도시한다. 다음의 표는 <accessControlPolicy> 리소스의 속성을 나타낸다.

[148] 표 3

[표3]

Attribute Name of <accessControlPolicy>	**Multiplicity**	**RW/RO/WO**	**Description**
resourceType (rT)	1	RO	표 2 참조
parentID (pID)	1	RO	표 2 참조
expirationTime (eT)	1	RW	표 2 참조
labels (lBs)	0..1	RW	표 2 참조
creationTime (cT)	1	RO	표 2 참조
lastModifiedTime (lMT)	1	RO	표 2 참조
link	1	WO	This attribute shall be present only on the announced resource. This attribute shall provide the link (URI) to the original resource. This is only for <accessControlPolicyAnnc>.
announceTo	1	RW	표 2 참조
announcedAttribute	1	RW	This attributes shall only be present on the original resource if some Optional Announced **(OA)** type attributes have been announced to other CSEs. This attribute maintains the list of the announced Optional Attributes (**OA** type attributes) in the original resource. Updates to this attribute will trigger new attribute announcement if a new attribute is added or de-announcement if the existing attribute is removed.
privileges (ps)	1	RW	The list of privileges defined by this <accessControlPolicy> resource. These privileges are applied to resources referencing this <accessControlPolicy> resource using the *accessControlPolicyID* attribute.
selfPrivileges (sP)	1	RW	Defines the list of privileges for the <accessControlPolicy> resource itself.

[149] 권한들은 동작들(접근을 승인하는 것일 수 있으나, 좀더 상세하게는 서브셋에 대한 접근을 승인, 즉 데이터의 부분을 필터링하는 것과 같은 것일 수 있음)에 일반화(generalize)될 수 있다. 권한들은 요청자(발신자, requestor)의 식별자, 특정된 식별자를 제외한 모두와 같은 것을 포함할 수 있는, 조건들로 일반화될 수 있으나, 시간 기반 조건들을 또한 포함할 수 있을 것이다.

[150] 접근 제어 정책에 기반한 접근 승인 메커니즘은 <accessControlPolicy> 리소스에 저장된 발신자와 발신자의 권한을 매칭함으로써 동작한다. 긍정적인 매치가 발견되면 요청된 동작(예컨대, RETRIEVE)이 매칭 권한 소유자와 연관된 허용된 동작들의 집합을 이용하여 체크되며; 만약 이 체크가 실패하면 상기 요청은 거절된다. 이러한 집합이 권한 플래그로 지칭된다.

[151] 셀프 권한들 및 권한들은 <accessControlPolicy> 리소스 그 자체 그리고 <accessControlPolicy> 리소스 및 accessControlPolicyID 공통 속성을 어드레싱(address)하는 모든 다른 리소스 타입들에 각각 적용되는 권한 플래그들과 연관되는 발신자 권한의 리스트들이다.

[152] 접근 제어 정책에서 정의된 모든 권한들은 또한 접근 승인 전에 위치, 시간 윈도우 및 IP 어드레스와 관련된다.

[153] 셀프 권한들 및 권한들 내 각각의 권한은 또한 하나의 역할로 구성될 수 있다. 이러한 역할은 역할 이름 및 그 역할이 정의된 M2M 서비스 구독 리소스를 어드레싱하는 URL에 의해 식별된다. 발신자가 특정 역할로 그 자신을 나타내는 경우, 접근 제어 정책은 M2M 서비스 구독 리소스에서 명시된 특정 역할에 속하는 리스트들과 요청 발신자를 매칭함으로써 동작한다.

[154] 권한들 및 셀프 권한들 리스트에서 각각의 권한은 다음의 엘리먼트들로 구성된다.

[155] 표 4

[표4]

Name	**Description**
originatorPrivileges	표 5 참조
contexts	표 6 참조
operationFlags	표 7 참조

[156] 상기 originatorPrivileges는 아래의 표와 같은 정보를 포함한다.

[157] 표 5

[표5]

Name	Description
Domain	FQDN domain
originator identifier	CSE ID or AE ID which represent a originator identity
Token	Access token usually provided as query parameter
All	All originators
Role	A role name associated with the URL the a Service Subscription resource where such role is defined

[158] 표 4의 contexts는다음의 표와 같은 정보를 포함한다.

[159] 표 6

[표6]

Name	Description
Context	Defines the context in which every privileges of the present access control policy resource applies, e.g. time windows, location, IP address.

[160] 표 4의 operationFlags는 다음의 표와 같은 정보를 포함한다.

[161] 표 7

[표7]

Name	Description
RETRIEVE	Privilege to retrieve the content of an addressed resource
CREATE	Privilege to create a child resource
UPDATE	Privilege to update the content of an addressed resource
DELETE	Privilege to delete an addressed resource
DISCOVER	Privilege to discover the resource
NOTIFY	Privilege to receive a notification

[162] M2M 통신 시스템에서는 접근 제어 정책 리소스를 접근 제어 정책이 적용된 리소스와 분리하여 저장하도록 한다. 접근 제어 정책이 적용된 리소스는 접근 제어 정책 리소스의 AccessRightID(접근 제어 정책 리소스의 URI)만을 가지고 있다. 그러므로, M2M 엔티티가 특정 리소스의 접근 제어 정책을 확인하려면 AccessRightID를 참조해야한다.

[163] **엔티티 등록(Entity Registration)**

[164] M2M 엔티티는 필드 도메인에 있든 인프라스트럭쳐 도메인에 있든 자기 주변의 엔티티와 등록(Registration) 과정을 수행하여 시스템/서비스를 이용할

준비를 마친다. 이러한 등록은 등록대상자(Registree)의 요청에 의해 동작이 수행되며 결과로써 일반적으로 등록대상자의 정보를 등록담당자(Registrar)에 저장한다.

[165] 이러한 등록 과정이 끝난 후 비로서 oneM2M 엔티티는 도 3과 같이 CSE가 제공하는 공통 기능들을 이용해서 M2M 서비스를 이용할 수 있다.

[166] oneM2M 엔티티에는 AE와 CSE가 있고, 이에 따라 상기 등록 과정은 AE 등록과 CSE 등록으로 나눌 수 있으며, 이 때 AE와 CSE는 모두 등록대상자를 의미하고 등록담당자는 CSE이다. CSE 등록의 경우 추가적으로 등록담당자 CSE의 정보를 등록대상자 CSE에도 저장한다.

[167] 도 8은 AE 등록 과정과 CSE 등록 과정을 도시한다. 도 8의 (a)은 AE 등록 과정을 도시하며, 등록하고자 하는 AE1은 등록담당자인 CSE1에게 <AE> 생성 요청을 하며(S81-1), 이에 CSE1은 상기 AE1의 정보를 이용하여 <AE> 자원을 생성할 수 있다(S82-2). 그리고나서, CSE1은 상기 등록 과정에 대한 결과를 포함한 응답을 AE1에게 전송할 수 있다(S83-2).

[168] 도 8의 (b)는 CSE 등록 과정을 도시한다. 도 8의 (b)는 등록하고자 하는 주체가 CSE1이고 등록담당자가 CSE2인 것과 CSE2가 CSE1의 등록 요청에 대한 결과를 전송(S83-2)하면, CSE1은 CSE2의 정보를 이용하여 <remoteCSE> 자원을 생성(S84-2)하는 것만 제외하고는 도 8의 (a)와 동일하다.

[169] **보안 연계 수립 프레임워크(Security association establishment framework)**

[170] 보안 연계 수립 프레임워크의 목적은 두 엔티티(이후 엔티티(entity) A, 엔티티 B라 지칭, 여기서 엔티티 A, B는 AE 또는 CSE일 수 있음, MAF(M2M Authentication Function) 기반 보안 연계 수립의 경우에는 엔티티 A와 MAF간 보안 연계 수립을 수행하고 MAF가 엔티티 B에게 엔티티 A와 엔티티 B 간의 보안 연계 수립에서 사용하는 크리덴셜 정보를 제공하여 두 엔티티 간의 보안 연계 수립을 돕는 역할을 수행) 간의 인증 및 보안 연계 수립 이후의 메시지 암호화/복호화 및 메시지 무결성 보증(메시지 무결성 보증을 통한 메시지를 전송한 엔티티 인증 가능)을 위함에 있다. 보안 연계 수립을 수행하기 위해서는 두 엔티티에 크리덴셜(Credential) 정보가 미리 설정되어 있어야 한다.

[171] 크리덴셜 정보가 미리 설정되는 방법은 제조 단계에서부터 설정되어 있을 수도 있으며, 또는 이후 원격으로 설정될 수도 있다. 여기서, 크리덴셜이라 함은 보안 연계 수립을 포함한 보안 절차를 수행하기 위한 보안 키 정보들로서, 예컨대 대칭키 기반의 보안 절차의 경우 두 엔티티간 공유된 대칭키(=비밀키, symmetric key), 대칭키의 식별자(Identifier) 등이 되며, 공개키 기반의 보안 절차의 경우 공개키(=public key) 또는 공개키를 포함한 인증서(Certificate), 공개키와 쌍(pair)을 이루는 비밀키(=private key), 인증서를 검증하는데 사용하는 인증서 체인(Certificate Chain), 공개키 ID 또는 인증서 ID 등이 그 예이다.

[172] oneM2M에서 정의한 보안 연계 수립 프레임워크들은 제공된 대칭키 보안 연계 수립 프레임워크(Provisioned Symmetric Key Security Association Establishment

Framework), 인증서-기반 보안 연계 수립 프레임워크(Certificate-based Security Association Establishment Framework), MAF-기반 대칭키 보안 연계 수립 프레임워크(MAF-based Symmetric Key Security Association Establishment Framework)가 있으며, 여기서 제공된 대칭키 보안 연계 수립 프레임워크와 MAF-기반 대칭키 보안 연계 수립 프레임워크는 대칭키 기반의 보안 절차를 사용하며, 인증서-기반 보안 연계 수립 프레임워크는 공개키 기반의 보안 절차를 사용한다. 제공된 대칭키 보안 연계 수립 프레임워크와 인증서-기반 보안 연계 수립 프레임워크는 두 엔티티 간의 통신을 통해 수행되며, MAF-기반 대칭키 보안 연계 수립 프레임워크는 MAF(M2M Authentication Function) 서버가 존재하여 엔티티 A와 엔티티 B가 보안 연계가 가능하도록 엔티티 A와 엔티티 B에 대칭키를 설정해준다.

[173] 보안 연계 수립 프레임워크는 크리덴셜 설정, 연계 설정, 연계 보안 핸드쉐이크(handshake)로 구성되는 총 3단계로 이루어져 있다.

[174] 크리덴셜 설정에서는 엔티티 각각에 엔티티의 크리덴셜을 설정하는 단계이고, 연계 설정에서는 설정된 크리덴셜과 보안 연계를 맺을 엔티티의 정보가 연계된다. 엔티티에는 보안 연계를 맺을 엔티티의 정보가 포함되어 있지 않고 엔티티가 등록담당자와의 등록이 이루어지고 난 이후 보안 연계를 맺을 엔티티의 정보를 획득할 수 있다. 이 경우 연계 보안 핸드쉐이크 시 연계 구성 단계에서 연계된 엔티티가 인증되지 않고, 등록 이후 보안 연계 수립이 되어 연계된 엔티티가 인증될 수 있다. 연계 보안 핸드쉐이크에서는 설정된 크리덴셜을 통해서 엔티티 A와 엔티티 B가 상호 인증하고 보안 콘텍스트(Security Context)를 맺는다. 이 때 크리덴셜이 검증(인증)되면 연계 구성 단계에서 연계된 엔티티가 인증된다.

[175] 상기 연계 설정을 통해 보안 연계 수립 프레임워크에서 키 ID 또는 인증서 이름을 인증함으로써 oneM2M 엔티티간의 인증(즉, 상대방 식별자 검증)이 가능하다.

[176] 그러나, 문제는 보안 연계 절차 이후 발생하는 메시지에 대한 인증에 있다. 즉, 악의적인 AE의 경우 보안 연계에서 사용한 oneM2M ID(AE-ID 또는 CSE-ID)를 사용하지 않고 다른 식별자를 사용할 수 있다. 예컨대 AE-ID(0x1234)를 상기 보안 연계에서 사용하였는데, 해당 AE가 oneM2M 메시지를 보낼 시 0x5678을 AE-ID(oneM2M 메시지의 fr 파라미터에 해당 ID 삽입)로 사용하는 것이다. 이 경우 두 엔티티간의 이미 인증이 완료되어 있는 상태이기 때문에 상기 메시지의 수신자는 인증이 완료되었다고 판단한다.

[177] 가장 간단한 솔루션은 상기 메시지 안의 fr 파라미터에 포함된 AE-ID와 해당 메시지를 보낼 때의 보안 세션을 수립하기 위한 보안 연계에서 수행한 연계 설정에서 사용한 oneM2M 엔티티 ID가 동일한지 검증하는 것이다. 도 9를 참조하여 이를 설명하도록 한다.

[178] 발신자(originator, 910)와 호스팅 CSE(920)는 사전에 보안 연계 수립이

완료(S910) 되었다고 가정한다. 그리고나서, 상기 발신자는 발신자의 ID를 포함한 메시지를 상기 호스팅 CSE로 전송할 수 있다(S920). 이에, 상기 호스팅 CSE는 상기 연계 설정에서 연계된 ID와 상기 메시지 내 발신자 ID를 비교할 수 있다(S930). 이때, 만약 상기 메시지에 포함된 발신자 ID가 상기 연계 설정에서 연계된 ID와 달랐다면, 상기 호스팅 CSE는 인증이 실패했다고 판단할 것이다.

[179] 하지만, 상기 발신자와 상기 호스팅 CSE 간의 멀티 홉(multi-hop) 환경에서는 상기와 같은 솔루션이 적용되지 않는다. 예컨대, 상기 발신자와 상기 호스팅 CSE 사이에 하나의 중간(transit) CSE(즉, 상기 발신자에 의해 전송된 메시지를 상기 호스팅 CSE로 전달하는 역할을 하는 CSE)가 존재할 경우, 각 홉마다 연계 설정 및 보안 연계가 이루어지기 때문에 상기 호스팅 CSE는 상기 중간 CSE와의 보안 연계만을 맺을 뿐, 상기 발신자와는 보안 연계가 존재하지 않는다.

[180] 이러한 현상은 oneM2M의 특성에 기인한다. 즉, 발신자가 전송하는 메시지는 홉 바이 홉(hop by hop)으로 전송되며, 각 홉 또는 몇몇 홉에서 상기 메시지에 대한 조작이 수행될 수 있다.

[181] 예를 들어, 상기 발신자가 전송하는 이벤트 카테고리(event category)가 상기 발신자가 허용하는 이벤트 카테고리의 범위를 벗어나는 경우, 중간 CSE는 상기 이벤트 카테고리를 변경하여 전달할 수 있다. 또는, 발신자가 AE일 경우, AE가 CSE-상대적-AE-ID를 사용(fr 파라미터에 사용)하여 등록담당자 CSE(상기 AE가 등록된 CSE를 의미)이외의 타 엔티티에게 메시지를 전송하는 경우(즉, to 파라미터가 등록담당자 CSE가 아닌 경우), 상기 등록담당자 CSE는 자신의 CSE-ID를 통해 SP-상대적-AE-ID를 생성하고, 이를 상기 메시지에 설정(fr 파라미터에 설정)하여 메시지를 전송할 수 있다.

[182] 이렇듯, CSE는 단순한 메시지 전달 이외의 메시지에 대한 조작 가능하고, 이는 중간 CSE와 같은 중간 엔티티가 신뢰(trusted) 관계에 없을 시 또는 공격자로부터 공격을 받았을 시 상당 수의 데이터가 공격자로 노출이 되는 문제점이 발생한다. 공격자가 또 할 수 있는 공격은 위장 공격(impersonation)으로써, 자신이 마치 중간 CSE인 것처럼 보이게 메시지의 출처를 조작함에 있다. 특정 자원 A에 대해 권한이 있는 엔티티로 메시지 출처를 조작하게 되면 공격자는 자원 A에 대한 권한을 획득할 수 있다.

[183] 이하에서, 본 발명의 실시예들을 설명하도록 한다. 후술될 실시예들에서 엔티티는 AE 또는 CSE일 수 있다.

[184] 도 10은 본 발명의 일 실시예에 따른 방법을 도시한다.

[185] 보안 연계 수립 완료(S1010) 이후 제1엔티티(1010)는 제2엔티티(1020)로 발신자 ID를 포함한 메시지를 전송할 수 있다(S1020). 제2엔티티는 상기 메시지를 전송한 제1엔티티와 직접(direct) 연결 관계(즉, 제1엔티티 및 제2엔티티 사이에 중간 엔티티(CSE)가 없음)가 있는지 확인한다.

[186] 여기서, 직접 연결 관계를 간주하는 방법은 아래와 같다.

[187] - 메시지를 전송한 엔티티(이하, 전송 엔티티)와 메시지를 수신한 엔티티(이하,

수신 엔티티)가 등록 관계에 있을 경우 직접 연결 관계로 판단할 수 있다.

[188] 상세하게는, 상기 보안 연계 과정에서 사용한 크리덴셜과 연계된 oneM2M 엔티티 ID가 상기 수신 엔티티에 전송 엔티티의 등록 정보가 저장되어 있는 자원 타입(예컨대, <AE>, <remoteCSE> 자원 타입)의 자원들 중 엔티티 ID를 저장하는 속성의 값에 상기 크리덴셜과 연계된 ID와 상관관계가 있는 자원이 있을 경우 등록 관계에 있다고 판단한다.

[189] - 수신 엔티티에 직접 연결 관계에 있는 엔티티 리스트가 저장되어 있고 상기 보안 연계 과정에서 사용한 크리덴셜과 연계된 oneM2M 엔티티 ID가 상기 엔티티 리스트에 포함되어 있는 경우 직접 연결 관계로 판단한다.

[190] 한편, 메시지를 수신하였을 시 상기 보안 연계 과정에서 사용한 크리덴셜과 연계된 oneM2M 엔티티 ID가 존재하지 않을 수 있다. 이 경우 본 실시예는 수행되지 않고 이후의 절차가 수행된다.

[191] 그리고나서, 수신 엔티티, 즉 제2엔티티가 제1엔티티와 직접 연결 관계에 있다고 판단한 경우, 상기 제2엔티티는 상기 메시지의 발신자 정보(예컨대, 상기 메시지의 from 파라미터 값)와 상기 oneM2M 엔티티 ID가 상관관계에 있는지 판단할 수 있다.

[192] 상관관계가 있다고 판단되는 경우, 제2엔티티는 발신자 정보에 대한 위장 공격(impersonation)이 없다고 판단하고, 상기 수신된 메시지를 처리할 수 있다.

[193] 상관 관계가 없다고 판단되는 경우, 제2엔티티는 발신자 정보에 대한 위장 공격이 있다고 판단하고, 상기 수신된 메시지에 대한 적절한 상태 코드(status code)(예컨대, 위장 공격 또는 ID 불일치)와 함께 응답 메시지를 전송할 수 있다.

[194] 한편, 여기서 상기 발신자 정보의 상기 oneM2M 엔티티 ID가 동일한지 여부를 판단하지 않고 상관관계에 있는지를 판단하는 이유는 상기 발신자 정보의 포맷이 다를 수 있음에 기인한다.

[195] 발신자 정보는 아래와 같은 옵션이 존재한다. 즉, 동일한 엔티티임에도 수신 엔티티에 의존적으로 아래와 같은 옵션이 존재한다.

[196] (a) 서비스 제공자ID(예컨대, //m2m.lguplus.com, //m2m.skt.com, m2m.kt.com) + 서비스 제공자 상대적인 엔티티 ID(예컨대, /CSE1/CAE1, /SsmartMeterAE1, /CSE1), 여기서 +는 문자열 조합(concatenation)

[197] (b) Service Provider Relative Entity ID (예컨대, /CSE1/CAE1, 서비스 제공자 상대적인 엔티티 ID(예컨대, /CSE1/CAE1, /SsmartMeterAE1, /CSE1)

[198] 도 11은 본 발명의 다른 일 실시예에 따른 방법을 도시한다.

[199] 보안 연계 수립 완료(S1110) 이후 AE(1110)는 등록담당자 CSE(1120)로 발신자 ID를 포함한 메시지를 전송할 수 있다(S1120). 상기 등록담당자 CSE는 상기 메시지를 전송한 상기 AE와 직접 연결 관계(즉, 상기 AE 및 상기 등록담당자 CSE 사이에 중간 엔티티(CSE)가 없음)가 있는지 확인한다.

[200] 여기서, 직접 연결 관계를 간주하는 방법은 아래와 같다.

[201] - 메시지를 전송한 엔티티(이하, 전송 엔티티)와 상기 메시지를 수신한

엔티티(이하, 수신 엔티티)가 등록관계에 있을 경우 직접 연결 관계가 있는 것으로 판단할 수 있다.

[202] 상세하게는, 상기 보안 연계 과정에서 사용한 크리덴셜과 연계된 oneM2M 엔티티 ID가 상기 수신 엔티티에 전송 엔티티의 등록 정보가 저장되어 있는 자원 타입(예컨대, <AE> 자원 타입)의 자원들 중 엔티티 ID를 저장하는 속성의 값에 상기 크리덴셜과 연계된 ID와 상관관계가 있는 자원이 있을 경우 등록 관계에 있다고 판단한다. 여기서, <AE> 자원 타입만을 확인하는 것은 AE만을 확인하기 위함이다.

[203] - 수신 엔티티에 직접 연결 관계에 있는 엔티티 리스트가 저장되어 있고 상기 보안 연계 과정에서 사용한 크리덴셜과 연계된 oneM2M 엔티티 ID가 상기 엔티티 리스트에 포함되어 있는 경우 직접 연결 관계로 판단한다.

[204] 한편, 메시지를 수신하였을 시 상기 보안 연계 과정에서 사용한 크리덴셜과 연계된 oneM2M 엔티티 ID가 존재하지 않을 수 있다. 이 경우 본 실시예는 수행되지 않고 이후의 절차가 수행된다.

[205] 그리고나서, 수신 엔티티, 즉 제2엔티티가 제1엔티티와 직접 연결 관계에 있다고 판단한 경우, 상기 제2엔티티는 상기 메시지의 발신자 정보(예컨대, 상기 메시지의 from 파라미터 값)와 상기 oneM2M 엔티티 ID가 상관관계에 있는지 판단할 수 있다.

[206] 상관관계가 있다고 판단되는 경우, 제2엔티티는 발신자 정보에 대한 위장 공격(impersonation)이 없다고 판단하고, 상기 수신된 메시지를 처리할 수 있다.

[207] 상관 관계가 없다고 판단되는 경우, 제2엔티티는 발신자 정보에 대한 위장 공격이 있다고 판단하고, 상기 수신된 메시지에 대한 적절한 상태 코드(status code)(예컨대, 위장 공격 또는 ID 불일치)와 함께 응답 메시지를 전송할 수 있다.

[208] 한편, 여기서 상기 발신자 정보의 상기 oneM2M 엔티티 ID가 동일한지 여부를 판단하지 않고 상관관계에 있는지를 판단하는 이유는 상기 발신자 정보의 포맷이 다를 수 있음에 기인한다.

[209] 발신자 정보는 아래와 같은 옵션이 존재한다. 즉, 동일한 엔티티임에도 수신 엔티티에 의존적으로 아래와 같은 옵션이 존재한다.

[210] (a) 서비스 제공자ID(예컨대, //m2m.lguplus.com, //m2m.skt.com, m2m.kt.com) + 서비스 제공자 상대적인 엔티티 ID(예컨대, /CSE1/CAE1, /SsmartMeterAE1, /CSE1), 여기서 +는 문자열 조합(concatenation)

[211] (b) Service Provider Relative Entity ID (예컨대, /CSE1/CAE1, 서비스 제공자 상대적인 엔티티 ID(예컨대, /CSE1/CAE1, /SsmartMeterAE1, /CSE1)

[212] 본 발명의 또다른 일 실시예에 따른 방법을 설명하도록 한다.

[213] 본 방법은 호스팅 CSE에서의 위장 공격(Impersonation)을 방지하는 기법이다. 본 방법은 발신자가 호스팅 CSE에 전송할 메시지에 대해 상기 메시지에 대한 메시지 무결성 코드(Integrity Code)를 생성할 수 있고, 상기 호스팅 CSE는 수신한 메시지에 대해 상기 메시지 무결성 코드를 검증할 수 있는 상황에서 가능하다.

따라서, 상기 발신자와 상기 호스팅 CSE간 무결성 코드를 생성할 때 사용되는 비밀 정보(예컨대, 키 정보)가 공유되어야 한다.

[214] 본 방법에서는 상기 발신자와 상기 호스팅 CSE의 중간 통신 경로 상에 있는 엔티티(즉, 중간(Transit) CSE)가 메시지의 특정 부분을 변경을 할 수 있는 환경을 고려하고 있다. 이러한 메시지의 변경을 통해서 메시지 처리에 대한 QoS(Quality of Service)를 유연하게 대처 가능하고, 상기 발신자의 편의를 위해 중간 엔티티가 상기 발신자를 대신하여 수행해야 하는 처리들도 수행할 수 있다. 예컨대, 상기 중간 엔티티가 메시지 ID의 포맷을 변경할 수 있을 것이다.

[215] 다만, 중간 엔티티가 공격자인 경우, 변경이 허용되지 않는 메시지 의 특정 부분도 변경하여 메시지를 전송할 수 있다.

[216] 위장 공격(Impersonation)을 방지하는 가장 큰 목적은 정확한 접근 제어에 있다. 즉, 발신자를 제대로 식별함으로써 발신자의 권한을 명확히 할 수 있다.

[217] 종래에는 메시지 전체에 대해서 발신자가 전송하는 메시지에 대해 메시지 무결성 코드를 생성하고, 호스팅 CSE는 수신한 메시지에 대한 해당 무결성 코드를 검증하였으나, 본 방법에서는 메시지의 특정 부분들에 대한 재조합 값에 대해 무결성 코드를 생성하고, 이를 호스팅 CSE에서 무결성 코드를 검증하여 위장 공격을 방지하고자 한다.

[218] 무결성 코드를 통해 보호되어야 할 메시지의 부분은 아래 두 가지 중의 하나이다.

[219] - 메시지를 전송한 출처(즉 발신자 정보, 해당 메시지 내 From 파라미터), Role(접근 제어에 쓰이는 역할 값) 등 접근 제어에서 사용되는 파라미터로써 변경을 통해 접근 유무가 변경될 수 있는 인자들이다.

[220] - 중간 CSE에서 변경될 수 있는 메시지 파라미터들 이외의 메시지 파라미터들

[221] 이렇게 하기 위해서는 무결성 코드를 생성하는데 사용되는 메시지 파라미터들에 대한 값 및 파라미터들의 시퀀스, 포맷이 발신자와 호스팅 CSE에게 공유되어 있거나, 상기 메시지에 이러한 정보를 나타낼 수 있는 지시자가 포함될 수 있다. 이 때, 상기 지시자도 무결성 코드를 생성할 시 상기 메시지에 포함되어 보호될 수 있다.

[222] 이렇게 무결성 코드를 생성하는데 사용되는 메시지를 재조합하는 것은 전송하는 메시지의 포맷과는 무관하여 메시지 포맷이 중간에 바뀌는 경우에도 유용하다. 예컨대 발신자와 중간 CSE간에는 메시지가 XML(eXtensible Markup Language), 중간 CSE와 호스팅 CSE간에는 메시지가 JSON (JavaScript Object Notation) 포맷으로 전송될 경우에도 본 발명에서는 포맷과 무관하게 무결성 코드를 생성 및 검증이 가능하다.

[223] 아래는 발신자가 전송할려는 메시지 예이다.

[224] <?xml version="1.0" encoding="UTF-8"?>

[225] <m2m:reqestPrimitive xmlns:m2m="http://www.onem2m.org/xml/protocols" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.onem2m.org/xml/protocols
CDT-requestPrimitive-v1_0_0.xsd">

[226] <operation>3</operation>

[227] <to>/CSE1Base/AE1</to>

[228] <from>/AE1</from>

[229] <role>Administrator</role>

[230] <requestIdentifier>AE1/1234</requestIdentifier>

[231] <primitiveContent>

[232] <m2m:ae xmlns:m2m="http://www.onem2m.org/xml/protocols"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.onem2m.org/xml/protocols CDT-ae-v1_0_0.xsd">

[233] <label>Seoul Seocho Bangbae-dong</label>

[234] <expirationTime>20141003T111111</expirationTime>

[235] <applicationName></applicationName>

[236] <pointOfAccess>192.168.0.6/AE6</pointOfAccess>

[237] </m2m:ae>

[238] </primitiveContent>

[239] </m2m:reqestPrimitive>

[240] 이러한 메시지를 전송하고자 할 때, 발신자는 무결성 코드로 보호되어야 할 부분에 대해서 무결성 코드를 생성한다. 위 의 예에서 메시지를 전송한 출처와 Role을 보호해야할 경우, 아래의 문자열에 대해서 무결성 코드를 생성한다. 아래 문자열을 만드는 방법은 상기 발신자와 상기 호스팅 CSE간 공유되어 있다.

[241] /AE1||Administrator

[242] 이렇게 생성된 무결성 코드가 "d41d8cd98f00b204e9800998ecf8427e"이라면 발신자는 해당 무결성 코드를 아래와 같이 메시지에 포함시켜 전송할 수 있다.

[243] <?xml version="1.0" encoding="UTF-8"?>

[244] <m2m:reqestPrimitive xmlns:m2m="http://www.onem2m.org/xml/protocols"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.onem2m.org/xml/protocols
CDT-requestPrimitive-v1_0_0.xsd">

[245] <operation>3</operation>

[246] <to>/CSE1Base/AE1</to>

[247] <from>/AE1</from>

[248] <role>Administrator</role>

[249] <requestIdentifier>AE1/1234</requestIdentifier>

[250] <primitiveContent>

[251] <m2m:ae xmlns:m2m="http://www.onem2m.org/xml/protocols"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.onem2m.org/xml/protocols CDT-ae-v1_0_0.xsd">

[252] <label>Seoul Seocho Bangbae-dong</label>

[253] <expirationTime>20141003T111111</expirationTime>

[254] <applicationName></applicationName>

[255] <pointOfAccess>192.168.0.6/AE6</pointOfAccess>

[256] </m2m:ae>

[257] </primitiveContent>

[258] <integrityCode>d41d8cd98f00b204e9800998ecf8427e<integrityCode>

[259] </m2m:reqestPrimitive>

[260] 상기 메시지를 수신한 상기 호스팅 CSE는 미리 공유된 무결성 코드에 사용된 파라미터, 파라미터 시퀀스, 포맷 정보를 사용하여 무결성 코드로 보호되어야할 메시지를 도출할 수 있다.

[261] 상기 호스팅 CSE는 무결성 코드 검증을 위해 무결성 코드 생성 함수에 동일하게 공유된 키 정보, 무결성 코드로 보호되어야할 메시지를 입력하여 수신된 무결성 코드와 동일한 무결성 코드가 생성되는지를 확인할 수 있다.

[262] 도 12는 본 발명의 또다른 일 실시예에 따른 방법을 도시한다.

[263] 본 방법은 발신자와 호스팅 CSE간의 통신 경로 상의 중간 CSE의 존재 여부와는 무관하게 동작할 수 있는 방법이다. 각 홉마다 보안 연계는 완료된 상태라고 가정한다. 발신자(1210)와 수신자 CSE1(1220) 사이에는 0 또는 0 개 이상의 중간 CSE가 존재할 수 있다.

[264] 상기 발신자는 전송할 자원 접근 관련 요청 메시지(Create, Retrieve, Notify, Discovery, Delete, Notify 등)를 생성할 수 있다(S1210). 그리고나서, 상기 발신자는 전송될 메시지 중 무결성 코드로 보호되어야할 문자열을 생성할 수 있다(S1220). 어떻게 문자열을 생성하는지에 대한 정보, 예컨대 어떤 메시지 파라미터들을 상기 무결성 코드로 보호할지, 문자열 생성시의 포맷, 문자열 생성시의 파라미터들의 순서에 대한 정보는 미리 공유되어 있다고 가정한다.

[265] 상기 발신자는 위에서 생성된 문자열에 대해 호스팅 CSE와 상기 발신자간에 공유된 무결성 코드 생성을 위한 크리덴셜을 사용하여 무결성 코드를 생성할 수 있다(S1230). 그리고나서, 상기 발신자는 상기 생성된 무결성 코드가 포함된 요청 메시지를 상기 수신자 CSE1로 전송할 수 있다(S1240).

[266] 상기 수신자 CSE1은 상기 수신된 요청 메시지에 무결성 코드가 있는지를 판단할 수 있다(S1250). 상기 수신된 요청 메시지에 무결성 코드가 없으면, 상기 수신자 CSE1은 상기 발신자로 상기 요청 메시지에 무결성 코드가 포함되어 있지 않음을 알릴 수 있다(S1250-1). 즉, 상기 수신자 CSE1은 상기 발신자로 상기 요청 메시지에 대한 응답 메시지를 전송하되, 상기 응답 메시지에 상기 요청 메시지에 무결성 코드가 포함되어 있지 않음을 지시하는 지시자 또는 값이 포함될 수 있다.

[267] 상기 수신된 요청 메시지에 무결성 코드가 있으면, 상기 수신자 CSE1은 자신이

상기 수신된 요청 메시지와 관련된 호스팅 CSE인지를 판단할 수 있다(S1260). 상기 호스팅 CSE인지를 판단하는 방법은 상기 수신된 요청 메시지의 타깃 주소가 상기 수신자 CSE1의 특정 자원 또는 속성을 지시하는지 여부를 통해 이루어질 수 있다. 예컨대, 상기 수신된 요청 메시지의 타깃 주소가 상기 수신자 CSE1의 특정 자원 또는 속성을 지시하면, 상기 수신자 CSE1은 상기 수신된 요청 메시지와 관련된 호스팅 CSE이다. 그렇지 않으면, 상기 수신자 CSE1은 상기 수신된 요청 메시지와 관련된 호스팅 CSE가 아니다.

[268] 상기 수신자 CSE1이 상기 수신된 요청 메시지와 관련된 호스팅 CSE가 아닌 경우, 상기 수신자 CSE1은 상기 수신된 요청 메시지를 조작 또는 처리한 후, 수신자 CSE2(1230)로 전달할 수 있다(S1260-1).

[269] 상기 수신자 CSE1이 상기 수신된 요청 메시지와 관련된 호스팅 CSE인 경우, 상기 수신자 CSE1는 상기 수신된 요청 메시지에 대한 무결성 코드 검증을 수행할 수 있다(S1270). 즉, 상기 수신자 CSE1은 상기 수신된 요청 메시지에서 무결성 코드로 보호되어야 할 문자열을 생성하고, 생성된 문자열에 대해서 상기 발신자와 상기 수신자 CSE1(즉, 호스팅 CSE)간에 공유된 무결성 코드 생성을 위한 크리덴셜을 사용하여 무결성 코드를 생성할 수 있다. 상기 수신된 요청 메시지에 존재하는 무결성 코드와 상기 생성된 무결성 코드가 동일하면 상기 무결성 코드 검증이 완료되며, 두 무결성 코드가 다르면 검증에 실패한다.

[270] 상기 무결성 코드 검증이 실패하면, 상기 수신자 CSE1은 상기 발신자로 상기 무결성 코드 검증이 실패임을 알릴 수 있다(S1270-1). 즉, 상기 수신자 CSE1은 상기 발신자로 상기 요청 메시지에 대한 응답 메시지를 전송하되, 상기 응답 메시지에 상기 무결성 코드 검증이 실패임을 지시하는 지시자 또는 값이 포함될 수 있다.

[271] 상기 무결성 코드 검증이 성공하면, 상기 수신자 CSE1은 호스팅 CSE로서의 역할을 수행할 수 있다. 상기 호스팅 CSE로서의 역할은 접근 제어 동작을 포함할 수 있다.

[272] 한편, 상기 S1250은 상기 발신자와 상기 수신자 CSE1이 직접 연결 관계인 경우에만 수행될 수 있다.

[273] 여기서, 직접 연결 관계를 간주하는 방법은 아래와 같다.

[274] - 메시지를 전송한 엔티티(이하, 전송 엔티티)와 메시지를 수신한 엔티티(이하, 수신 엔티티)가 등록 관계에 있을 경우 직접 연결 관계로 판단할 수 있다.

[275] 상세하게는, 상기 보안 연계 과정에서 사용한 크리덴셜과 연계된 oneM2M 엔티티 ID가 상기 수신 엔티티에 전송 엔티티의 등록 정보가 저장되어 있는 자원 타입(예컨대, <AE>, <remoteCSE> 자원 타입)의 자원들 중 엔티티 ID를 저장하는 속성의 값에 상기 크리덴셜과 연계된 ID와 상관관계가 있는 자원이 있을 경우 등록 관계에 있다고 판단한다.

[276] - 수신 엔티티에 직접 연결 관계에 있는 엔티티 리스트가 저장되어 있고 상기 보안 연계 과정에서 사용한 크리덴셜과 연계된 oneM2M 엔티티 ID가 상기

엔티티 리스트에 포함되어 있는 경우 직접 연결 관계로 판단한다.

[277] 도 13은 본 발명의 또다른 일 실시예에 따른 방법을 도시한다.

[278] 아래는 직접 연결 관계가 아닌 경우에만(즉, 메시지의 발신자와 호스팅 CSE간 중간 CSE가 있을 경우) 무결성 코드를 사용하는 방법이다. 즉, 직접 연결 관계일 경우 무결성 코드와는 다른 방식으로 위장 공격(impersonation)을 방지할 수 있다.

[279] 본 방법에서는 수신된 또는 전달된 메시지를 생성한 실제 발신자와 상기 메시지를 전달한 엔티티를 구분하기 위하여, 메시지를 생성하여 최초 전송한 발신자를 메시지 발신자, 그외에 메시지를 전달한 엔티티를 메시지 전송자라고 부르며 메시지 발신자의 식별자(또는 ID) 또는 메시지 전송자의 식별자(또는 ID)는 전송 또는 전달되는 메시지에 포함될 수 있다. 즉, 중간 CSE는 메시지를 전달할 때 메시지 발신자와 관련된 정보를 조작하지 않고, 메시지 전송자와 관련된 정보에 상기 중간 CSE의 ID를 삽입할 수 있다.

[280] 메시지 발신자 또는 메시지 전송자가 같은 경우 둘 중 하나만 전송 또는 전달되는 메시지에 포함하여 전송될 수 있다. 이 때, 수신자 CSE는 해당 메시지의 발신자와 수신자가 동일하다고 판단한다.

[281] 도 13에서 각 홉 마다 보안 연계가 완료된 상태라고 가정하고, 메시지 발신자와 수신자 CSE1 사이에는 0 또는 0 개 이상의 중간 CSE가 존재할 수 있다.

[282] 직접 연결 관계에 있는 두 엔티티, 전송자(1310)와 수신자 CSE1(1320)는 보안 연계 관계를 맺고 있다.

[283] 상기 전송자는 자원 접근과 관련된 요청 메시지를 상기 수신자 CSE1에게 전송할 수 있다(S1310). 여기서, 상기 전송자는 메시지 발신자일 수도 있고 아닐 수도 있다.

[284] 상기 전송자가 상기 메시지 발신자일 경우, 상기 전송자는 상기 요청 메시지의 타깃인 호스팅 CSE와 직접 연결 관계에 있는지 판단하고, 직접 연결 관계에 있지 않다면 무결성 코드를 포함한 요청 메시지를 상기 수신자 CSE1로 전송할 수 있다. 후술되겠지만, 상기 무결성 코드는 메시지 발신자와 호스팅 CSE가 직접 연결 관계가 아닌 경우, 즉 그 둘 사이에 하나 이상의 중간 CSE가 존재하는 경우에만 전달되는 요청 메시지에 포함될 수 있다.

[285] 상기 전송자가 상기 요청 메시지에 무결성 코드를 포함해야 한다고 판단하였을 경우, 상기 전송자는 전송할 메시지 중 무결성 코드로 보호되어야 할 문자열 생성할 수 있다.

[286] 어떻게 문자열을 생성하는지에 대한 정보, 예컨대 어떤 메시지 파라미터들을 상기 무결성 코드로 보호할지, 문자열 생성시의 포맷, 문자열 생성시의 파라미터들의 순서에 대한 정보는 미리 공유되어 있다고 가정한다.

[287] 상기 전송자는 위에서 생성된 문자열에 대해 호스팅 CSE와 상기 전송자간에 공유된 무결성 코드 생성을 위한 크리덴셜을 사용하여 무결성 코드를 생성할 수 있다. 그리고나서, 상기 전송자는 상기 생성된 무결성 코드가 포함된 메시지를 상기 수신자 CSE1로 전송할 수 있다.

[288] 상기 수신자 CSE1은 상기 전송자의 ID와 상기 보안 연계와 관련된 절차에서 사용한 크리덴셜과 연계된 oneM2M 엔티티 ID가 상관관계가 있는지 여부를 확인할 수 있다(S1320). 상기 보안 연계와 관련된 절차에서 사전에 연계된 oneM2M 엔티티 ID가 없다면 S1320 단계는 생략되고 S1330으로 진행할 수 있다.

[289] 상기 전송자의 ID와 상기 크리덴셜과 연계된 oneM2M 엔티티 ID가 상관관계가 없다면, 상기 수신자 CSE1은 상기 전송자의 ID가 조작되었다고 판단하고, 상기 요청 메시지에 대한 응답 메시지를 상기 전송자로 전송할 수 있다(S1320-1). 상기 응답 메시지는 상기 상관관계가 없음을 지시하는 지시자 또는 값을 포함할 수 있다.

[290] 한편, 여기서 상기 전송자 정보의 상기 oneM2M 엔티티 ID가 동일한지 여부를 판단하지 않고 상관관계에 있는지를 판단하는 이유는 상기 전송자 정보의 포맷이 다를 수 있음에 기인한다.

[291] 전송자 정보는 아래와 같은 옵션이 존재한다. 즉, 동일한 엔티티임에도 수신 엔티티에 의존적으로 아래와 같은 옵션이 존재한다.

[292] (a) 서비스 제공자ID(예컨대, //m2m.lguplus.com, //m2m.skt.com, m2m.kt.com) + 서비스 제공자 상대적인 엔티티 ID(예컨대, /CSE1/CAE1, /SsmartMeterAE1, /CSE1), 여기서 +는 문자열 조합(concatenation)

[293] (b) Service Provider Relative Entity ID (예컨대, /CSE1/CAE1, 서비스 제공자 상대적인 엔티티 ID(예컨대, /CSE1/CAE1, /SsmartMeterAE1, /CSE1)

[294] 상기 전송자의 ID와 상기 크리덴셜과 연계된 oneM2M 엔티티 ID가 상관관계가 있다면, 상기 수신자 CSE1은 자신이 상기 요청 메시지와 관련된 호스팅 CSE인지 여부를 판단할 수 있다(S1330).

[295] 상기 호스팅 CSE인지를 판단하는 방법은 상기 수신된 요청 메시지의 타깃 주소가 상기 수신자 CSE1의 특정 자원 또는 속성을 지시하는지 여부를 통해 이루어질 수 있다. 예컨대, 상기 수신된 메시지의 타깃 주소가 상기 수신자 CSE1의 특정 자원 또는 속성을 지시하면, 상기 수신자 CSE1은 상기 수신된 요청 메시지와 관련된 호스팅 CSE이다. 그렇지 않으면, 상기 수신자 CSE1은 상기 수신된 요청 메시지와 관련된 호스팅 CSE가 아니다.

[296] 상기 수신자 CSE1가 호스팅 CSE가 아닌 것으로 판단되면, 상기 수신자 CSE1은 무결성 코드가 존재하는지 여부를 확인할 수 있다(S1340).

[297] 상기 무결성 코드가 존재하지 않으면, 상기 수신자 CSE1은 상기 요청 메시지에 대한 응답 메시지를 상기 전송자로 전송할 수 있다(S1340-1). 상기 응답 메시지는 상기 무결성 코드가 존재하지 않음을 지시하는 지시자 또는 값을 포함할 수 있다.

[298] 상기 수신자 CSE1은 무결성 코드가 존재하는지 확인하여 존재하지 않을 경우 불필요한 메시지 전달을 수행하지 않고 응답 메시지를 전송(S1340-1)하고, 상기 무결성 코드가 존재할 경우, 상기 요청 메시지를 수신자 CSE2(1330)로 전달할 수 있다(S1340-2).

[299] 상기 수신자 CSE1은 자신이 등록담당자 CSE인지 여부를 판단할 수 있다(S1350). 즉, 상기 수신자 CSE1은 자신이 상기 전송자를 등록한 CSE인지 여부를 확인할 수 있다. 상기 요청 메시지에 포함된 메시지 전송자의 식별자와 메시지 발신자의 ID가 동일한 경우에 상기 수신자 CSE1이 등록담당자 CSE에 해당하는 것으로 판단될 수 있다. 상기 수신자 CSE1이 등록담당자 CSE인 경우, 이미 S1320을 통해 위장 공격이 없음이 검증되었으므로 별도로 무결성 코드 검증이 필요없다.

[300] 상기 수신자 CSE1은 자신이 상기 전송자의 등록담당자 CSE가 아닌 것으로 판단된 경우, 무결성 코드를 검증할 수 있다(S1360).

[301] 즉, 상기 수신자 CSE1은 상기 수신된 메시지에서 무결성 코드로 보호되어야 할 문자열을 생성하고, 생성된 문자열에 대해서 상기 요청 메시지의 발신자(즉, 메시지 발신자)와 상기 수신자 CSE1간에 공유된 무결성 코드 생성을 위한 크리덴셜을 사용하여 무결성 코드를 생성할 수 있다. 상기 수신된 메시지에 존재하는 무결성 코드와 상기 생성된 무결성 코드가 동일하면 상기 무결성 코드 검증이 완료되며, 두 무결성 코드가 다르면 검증에 실패한다.

[302] 상기 무결성 코드 검증이 실패하면, 상기 수신자 CSE1은 상기 전송자로 상기 무결성 코드 검증이 실패임을 알릴 수 있다(S1360-1). 즉, 상기 수신자 CSE1은 상기 전송자로 상기 메시지에 대한 응답 메시지를 전송하되, 상기 응답 메시지에 상기 무결성 코드 검증이 실패임을 지시하는 지시자 또는 값이 포함될 수 있다.

[303] S1360에서 상기 무결성 코드 검증이 성공하거나 S1350에서 상기 수신자 CSE1이 상기 전송자의 등록담당자 CSE인 것으로 판단되면, 상기 수신자 CSE1은 호스팅 CSE로서의 역할을 수행할 수 있다(S1370).

[304] 상기 호스팅 CSE로서의 역할은 접근 제어 동작을 포함할 수 있다.

[305] 도 14는 본 발명의 또다른 일 실시예에 따른 방법을 도시한다

[306] 아래는 직접 연결 관계가 아닌 경우에만(즉, 메시지의 발신자와 호스팅 CSE간 중간 CSE가 있을 경우) 무결성 코드를 사용하는 방법이다. 즉, 직접 연결 관계일 경우 무결성 코드와는 다른 방식으로 위장 공격(impersonation)을 방지할 수 있다.

[307] 도 14에서 각 홉 마다 보안 연계가 완료된 상태라고 가정하고, 메시지 발신자와 수신자 CSE 사이에는 0 또는 0 개 이상의 중간 CSE가 존재할 수 있다.

[308] 직접 연결 관계에 있는 두 엔티티, 전송자(1410)와 수신자 CSE1(1420)는 보안 연계 관계를 맺고 있다.

[309] 상기 전송자는 자원 접근과 관련된 요청 메시지를 상기 수신자 CSE1에게 전송할 수 있다(S1410). 여기서, 상기 전송자는 상기 요청 메시지의 발신자일 수도 있고 아닐 수도 있다. 상기 전송자가 상기 요청 메시지의 발신자일 경우, 상기 전송자는 상기 요청 메시지의 타깃인 호스팅 CSE와 직접 연결 관계에 있는지 판단하고, 직접 연결 관계에 있지 않다면 무결성 코드를 포함한 요청 메시지를 상기 수신자 CSE1로 전송할 수 있다.

[310] 상기 전송자가 상기 요청 메시지에 무결성 코드를 포함해야 한다고 판단하였을

경우(즉, 상기 전송자가 상기 요청 메시지의 발신자이고 상기 요청 메시지와관련된 호스팅 CSE와는 직접 연결 관계가 아닌 경우), 상기 전송자는 전송할 메시지 중 무결성 코드로 보호되어야 할 문자열 생성할 수 있다.

[311] 어떻게 문자열을 생성하는지에 대한 정보, 예컨대 어떤 메시지 파라미터들을 상기 무결성 코드로 보호할지, 문자열 생성시의 포맷, 문자열 생성시의 파라미터들의 순서에 대한 정보는 미리 공유되어 있다고 가정한다.

[312] 상기 전송자는 위에서 생성된 문자열에 대해 호스팅 CSE와 상기 전송자간에 공유된 무결성 코드 생성을 위한 크리덴셜을 사용하여 무결성 코드를 생성할 수 있다. 그리고나서, 상기 발신자는 상기 생성된 무결성 코드가 포함된 메시지를 상기 수신자 CSE1로 전송할 수 있다.

[313] 상기 수신자 CSE1은 자신이 상기 요청 메시지에 대한 호스팅 CSE인지 여부를 판단할 수 있다(S1420). 상기 호스팅 CSE인지를 판단하는 방법은 상기 수신된 요청 메시지의 타깃 주소가 상기 수신자 CSE1의 특정 자원 또는 속성을 지시하는지 여부를 통해 이루어질 수 있다. 예컨대, 상기 수신된 메시지의 타깃 주소가 상기 수신자 CSE1의 특정 자원 또는 속성을 지시하면, 상기 수신자 CSE1은 상기 수신된 요청 메시지와 관련된 호스팅 CSE이다. 그렇지 않으면, 상기 수신자 CSE1은 상기 수신된 요청 메시지와 관련된 호스팅 CSE가 아니다.

[314] 상기 수신자 CSE1가 호스팅 CSE가 아닌 것으로 판단되면, 상기 수신자 CSE1은 무결성 코드가 존재하는지 여부를 확인할 수 있다(S1430).

[315] 상기 무결성 코드가 존재하지 않으면, 상기 수신자 CSE1은 상기 요청 메시지에 대한 응답 메시지를 상기 전송자로 전송할 수 있다(S1430-1). 상기 응답 메시지는 상기 무결성 코드가 존재하지 않음을 지시하는 지시자 또는 값을 포함할 수 있다.

[316] 상기 수신자 CSE1은 무결성 코드가 존재하는지 확인하여 존재하지 않을 경우 불필요한 메시지 전달을 수행하지 않고 응답 메시지를 전송(S1430-1)하고, 상기 무결성 코드가 존재할 경우, 상기 요청 메시지를 수신자 CSE2(1330)로 전달할 수 있다(S1430-2).

[317] 상기 수신자 CSE1은 자신이 등록담당자 CSE인지 여부를 판단할 수 있다(S1440). 즉, 상기 수신자 CSE1은 자신이 상기 전송자를 등록한 CSE인지 여부를 확인할 수 있다.

[318] 여기서, 상기 등록담당자 CSE인지 여부의 판단은 상기 요청 메시지의 발신자 정보(즉, 상기 요청 메시지를 생성한 엔티티의 ID로써 from 파라미터의 값으로 설정됨)와, 등록 정보가 저장되어 있는 자원 타입(예컨대 <AE>, <remoteCSE> 자원 타입)의 자원들 중 상기 발신자 정보와 동일한 값을 저장하는 자원이 있는지를 판단한다. 상기 발신자 정보와 동일한 값을 저장하는 자원이 있을 시, 상기 수신자 CSE1은 자신을 상기 전송자의 등록담당자 CSE로 판단할 수 있다.

[319] 상기 수신자 CSE1이 상기 전송자의 등록담당자 CSE로 판단된 경우, 상기 수신자 CSE1은 상기 발신자의 ID와 상기 보안 연계와 관련된 절차에서 사용한

크리덴셜과 연계된 oneM2M 엔티티 ID가 상관관계가 있는지 여부를 확인할 수 있다(S1450).

[320] 상기 전송자의 ID와 상기 크리덴셜과 연계된 oneM2M 엔티티 ID가 상관관계가 없다면, 상기 수신자 CSE1은 상기 전송자의 ID가 조작되었다고 판단하고, 상기 요청 메시지에 대한 응답 메시지를 상기 전송자로 전송할 수 있다(S1450-1). 상기 응답 메시지는 상기 상관관계가 없음을 지시하는 지시자 또는 값을 포함할 수 있다.

[321] 한편, 여기서 상기 전송자 정보의 상기 oneM2M 엔티티 ID가 동일한지 여부를 판단하지 않고 상관관계에 있는지를 판단하는 이유는 상기 전송자 정보의 포맷이 다를 수 있음에 기인한다.

[322] 전송자 정보는 아래와 같은 옵션이 존재한다. 즉, 동일한 엔티티임에도 수신 엔티티에 의존적으로 아래와 같은 옵션이 존재한다.

[323] (a) 서비스 제공자ID(예컨대, //m2m.lguplus.com, //m2m.skt.com, m2m.kt.com) + 서비스 제공자 상대적인 엔티티 ID(예컨대, /CSE1/CAE1, /SsmartMeterAE1, /CSE1), 여기서 +는 문자열 조합(concatenation)

[324] (b) Service Provider Relative Entity ID (예컨대, /CSE1/CAE1, 서비스 제공자 상대적인 엔티티 ID(예컨대, /CSE1/CAE1, /SsmartMeterAE1, /CSE1)

[325] 한편, 상기 수신자 CSE1은 자신이 등록담당자 CSE가 아닌 것으로 판단된 경우, 무결성 코드를 검증할 수 있다(S1460).

[326] 즉, 상기 수신자 CSE1(S1420에서 상기 수신자 CSE1은 상기 요청 메시지와 관련된 호스팅 CSE로 판단되었으므로)은 상기 수신된 메시지에서 무결성 코드로 보호되어야 할 문자열을 생성하고, 생성된 문자열에 대해서 상기 요청 메시지의 발신자와 상기 수신자 CSE1간에 공유된 무결성 코드 생성을 위한 크리덴셜을 사용하여 무결성 코드를 생성할 수 있다. 상기 수신된 메시지에 존재하는 무결성 코드와 상기 생성된 무결성 코드가 동일하면 상기 무결성 코드 검증이 완료되며, 두 무결성 코드가 다르면 검증에 실패한다.

[327] 상기 무결성 코드 검증이 실패하면, 상기 수신자 CSE1은 상기 전송자로 상기 무결성 코드 검증이 실패임을 알릴 수 있다(S1460-1). 즉, 상기 수신자 CSE1은 상기 전송자로 상기 메시지에 대한 응답 메시지를 전송하되, 상기 응답 메시지에 상기 무결성 코드 검증이 실패임을 지시하는 지시자 또는 값이 포함될 수 있다.

[328] S1460에서 상기 무결성 코드 검증이 성공하거나 S1450에서 ID간의 상관관계가 있다고 판단되면, 상기 수신자 CSE1은 호스팅 CSE로서의 역할을 수행할 수 있다(S1470).

[329] 상기 호스팅 CSE로서의 역할은 접근 제어 동작을 포함할 수 있다.

[330] S1440에서 상기 수신자 CSE1이 등록담당자 CSE인 것으로 판단된 것은, 이는 상기 전송자는 상기 요청 메시지의 발신자이며 상기 수신자 CSE1은 상기 요청 메시지와 관련된 호스팅 CSE임을 의미한다. 따라서, 이미 S1450을 통해 위장 공격이 없음이 검증되므로 별도로 무결성 코드 검증이 필요없다. 즉, 직접 연결

관계에서는 직접 연결 관계가 아닌 경우와 달리 무결성 코드가 위장 공격 여부를 판단하기 위해 필요하지 않다.

[331] 도 15는 본 발명의 실시예(들)을 수행하도록 구성된 장치의 블록도를 도시한다. 전송장치(10) 및 수신장치(20)는 정보 및/또는 데이터, 신호, 메시지 등을 나르는 무선 신호를 전송 또는 수신할 수 있는 RF(Radio Frequency) 유닛(13, 23)과, 무선통신 시스템 내 통신과 관련된 각종 정보를 저장하는 메모리(12, 22), 상기 RF 유닛(13, 23) 및 메모리(12, 22)등의 구성요소와 동작적으로 연결되고, 상기 구성요소를 제어하여 해당 장치가 전술한 본 발명의 실시예들 중 적어도 하나를 수행하도록 메모리(12, 22) 및/또는 RF 유닛(13,23)을 제어하도록 구성된 프로세서(11, 21)를 각각 포함한다.

[332] 메모리(12, 22)는 프로세서(11, 21)의 처리 및 제어를 위한 프로그램을 저장할 수 있고, 입/출력되는 정보를 임시 저장할 수 있다. 메모리(12, 22)가 버퍼로서 활용될 수 있다.

[333] 프로세서(11, 21)는 통상적으로 전송장치 또는 수신장치 내 각종 모듈의 전반적인 동작을 제어한다. 특히, 프로세서(11, 21)는 본 발명을 수행하기 위한 각종 제어 기능을 수행할 수 있다. 프로세서(11, 21)는 컨트롤러(controller), 마이크로 컨트롤러(microcontroller), 마이크로 프로세서(microprocessor), 마이크로 컴퓨터(microcomputer) 등으로도 불릴 수 있다. 프로세서(11, 21)는 하드웨어(hardware) 또는 펌웨어(firmware), 소프트웨어, 또는 이들의 결합에 의해 구현될 수 있다. 하드웨어를 이용하여 본 발명을 구현하는 경우에는, 본 발명을 수행하도록 구성된 ASICs(application specific integrated circuits) 또는 DSPs(digital signal processors), DSPDs(digital signal processing devices), PLDs(programmable logic devices), FPGAs(field programmable gate arrays) 등이 프로세서(11, 21)에 구비될 수 있다. 한편, 펌웨어나 소프트웨어를 이용하여 본 발명을 구현하는 경우에는 본 발명의 기능 또는 동작들을 수행하는 모듈, 절차 또는 함수 등을 포함하도록 펌웨어나 소프트웨어가 구성될 수 있으며, 본 발명을 수행할 수 있도록 구성된 펌웨어 또는 소프트웨어는 프로세서(11, 21) 내에 구비되거나 메모리(12, 22)에 저장되어 프로세서(11, 21)에 의해 구동될 수 있다.

[334] 본 발명의 실시예들에 있어서, 애플리케이션 (엔티티) 또는 리소스 관린 엔티티 등은 각각 그들이 설치되어 있거나 탑재되어 있는 장치들, 즉 전송장치(10) 또는 수신장치(20)로 동작할 수 있다.

[335] 이와 같은, 수신장치 또는 전송장치로 애플리케이션 (엔티티) 또는 리소스 관린 엔티티 등의 구체적인 구성은, 도면과 관련하여 전술한 본 발명의 다양한 실시예에서 설명한 사항들이 독립적으로 적용되거나 또는 둘 이상의 실시예가 동시에 적용되도록 구현될 수 있다.

[336] 상술한 바와 같이 개시된 본 발명의 바람직한 실시예들에 대한 상세한 설명은 당업자가 본 발명을 구현하고 실시할 수 있도록 제공되었다. 상기에서는 본 발명의 바람직한 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된

당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다. 따라서, 본 발명은 여기에 나타난 실시형태들에 제한되려는 것이 아니라, 여기서 개시된 원리들 및 신규한 특징들과 일치하는 최광의 범위를 부여하려는 것이다.

산업상 이용가능성

[337] 본 발명은 무선 이동 통신 시스템의 단말기, 기지국, 서버 또는 기타 다른 장비에 사용될 수 있다.

청구범위

[청구항 1] 무선 통신 시스템에서 요청 메시지를 처리하기 위한 방법으로서, 상기 방법은 제1M2M 엔티티에 의해 수행되며,
제2M2M 엔티티로부터 특정 자원에 대한 동작과 관련된 요청 메시지를 수신하는 단계;
상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있는지 여부를 판단하는 단계; 및
상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있지 않으면, 상기 요청 메시지에 무결성 코드가 포함되어 있는지 여부를 판단하는 단계;
상기 요청 메시지에 상기 무결성 코드가 포함되어 있으면, 상기 요청 메시지를 제3M2M 엔티티로 전달하는 단계를 포함하고, 또는
상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있으면, 상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 있는지 여부를 판단하는 단계; 및
상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 없으면, 상기 요청 메시지에 포함된 무결성 코드에 대한 검증을 수행하는 단계를 포함하는 것을 특징으로 하는, 요청 메시지 처리 방법.

[청구항 2] 제1항에 있어서,
상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 있는지 여부를 판단하는 단계는 상기 요청 메시지에 포함된 발신자의 식별자와 제2M2M 엔티티의 식별자가 동일한지 여부를 판단하는 단계를 포함하는 것을 특징으로 하는, 요청 메시지 처리 방법.

[청구항 3] 제1항에 있어서,
상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 있는지 여부를 판단하는 단계는 상기 제1M2M 엔티티가 가지고 있는 자원의 특정 속성에 상기 제2M2M 엔티티와 상관관계가 있는 정보가 저장되어 있는지 여부를 판단하는 단계를 포함하는 것을 특징으로 하는, 요청 메시지 처리 방법.

[청구항 4] 제1항에 있어서, 상기 무결성 코드는, 상기 요청 메시지의 발신자와 상기 특정 자원을 가지고 있는 엔티티가 등록관계가 없는 경우에, 상기 발신자에 의해 상기 요청 메시지에 포함되는 것을 특징으로 하는, 요청 메시지 처리 방법.

[청구항 5] 제1항에 있어서, 상기 무결성 코드를 생성하기 위해 사용되는 정보들은 상기 요청 메시지의 발신자와 상기 특정 자원을 가지고 있는 엔티티에 의해 사전에 공유되는 것을 특징으로 하는, 요청 메시지 처리 방법.

[청구항 6] 제1항에 있어서, 상기 무결성 코드로 보호될 정보는 상기 요청 메시지의 특정 부분을 포함하는 것을 특징으로 하는, 요청 메시지 처리 방법.

[청구항 7] 제6항에 있어서,
상기 특정 부분은 상기 요청 메시지의 발신자 정보를 포함하는 것을 특징으로 하는, 요청 메시지 처리 방법.

[청구항 8] 제1항에 있어서, 상기 제2M2M 엔티티의 식별자와 보안 연계(security association)와 관련한 크리덴셜(credential)과 연계된 식별자가 상관관계가 있는지 판단하는 단계를 더 포함하는 것을 특징으로 하는, 요청 메시지 처리 방법.

[청구항 9] 제1항에 있어서, 상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있는지 여부를 판단하는 단계는 상기 제2M2M 엔티티의 식별자와 보안 연계와 관련한 크리덴셜과 연계된 식별자가 상관관계가 있다고 판단된 경우에만 수행되는 것을 특징으로 하는, 요청 메시지 처리 방법.

[청구항 10] 무선 통신 시스템에서 요청 메시지를 처리하도록 구성된 M2M 장치에 있어서,
무선 주파수(radio frequency, RF) 유닛; 및
상기 RF 유닛을 제어하도록 구성된 프로세서를 포함하되,
상기 프로세서는:
제2M2M 엔티티로부터 특정 자원에 대한 동작과 관련된 요청 메시지를 수신하고,
상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있는지 여부를 판단하고,
상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있지 않으면, 상기 요청 메시지에 무결성 코드가 포함되어 있는지 여부를 판단하고,
상기 요청 메시지에 상기 무결성 코드가 포함되어 있으면, 상기 요청 메시지를 제3M2M 엔티티로 전달하거나, 또는
상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있으면, 상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 있는지 여부를 판단하고, 그리고
상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 없으면, 상기 요청 메시지에 포함된 무결성 코드에 대한 검증을 수행하도록 구성되는 것을 특징으로 하는, M2M 장치.

[청구항 11] 제10항에 있어서, 상기 프로세서는 상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 있는지 여부를 판단하기 위해 상기 요청 메시지에 포함된 발신자의 식별자와 제2M2M 엔티티의 식별자가 동일한지 여부를 판단하도록 구성되는 것을 특징으로 하는, M2M 장치.

[청구항 12] 제10항에 있어서, 상기 프로세서는 상기 제1M2M 엔티티가 제2M2M 엔티티와 등록관계가 있는지 여부를 판단하기 위해 상기 제1M2M 엔티티가 가지고 있는 자원의 특정 속성에 상기 제2M2M 엔티티와 상관관계가 있는 정보가 저장되어 있는지 여부를 판단하도록 구성되는 것을 특징으로 하는, M2M 장치.

[청구항 13] 제10항에 있어서, 상기 무결성 코드는, 상기 요청 메시지의 발신자와 상기 특정 자원을 가지고 있는 엔티티가 등록관계가 없는 경우에, 상기 발신자에 의해 상기 요청 메시지에 포함되는 것을 특징으로 하는, M2M 장치.

[청구항 14] 제10항에 있어서, 상기 무결성 코드를 생성하기 위해 사용되는 정보들은 상기 요청 메시지의 발신자와 상기 특정 자원을 가지고 있는 엔티티에 의해 사전에 공유되는 것을 특징으로 하는, M2M 장치.

[청구항 15] 제10항에 있어서, 상기 무결성 코드로 보호될 정보는 상기 요청 메시지의 특정 부분을 포함하는 것을 특징으로 하는, M2M 장치.

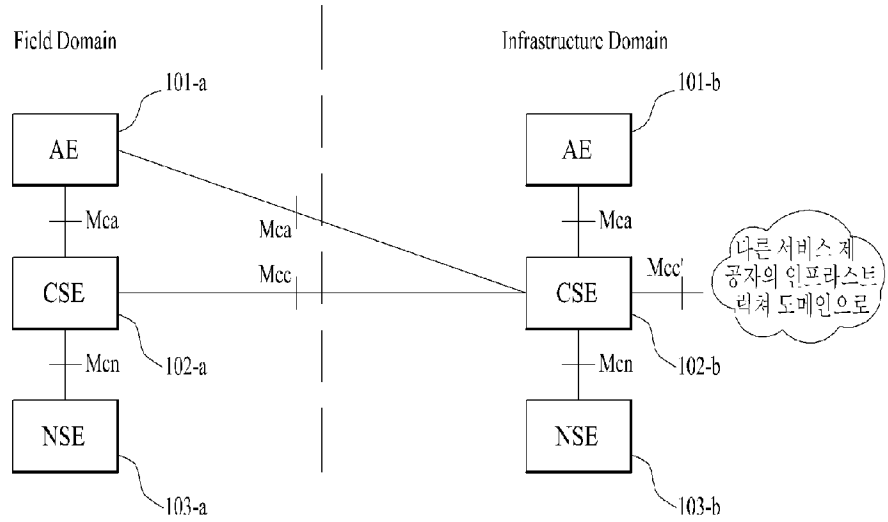
[청구항 16] 제15항에 있어서,
상기 특정 부분은 상기 요청 메시지의 발신자 정보를 포함하는 것을 특징으로 하는, M2M 장치.

[청구항 17] 제10항에 있어서, 상기 프로세서는 상기 제2M2M 엔티티의 식별자와 보안 연계(security association)와 관련한 크리덴셜(credential)과 연계된 식별자가 상관관계가 있는지 판단하도록 구성되는 것을 특징으로 하는, M2M 장치.

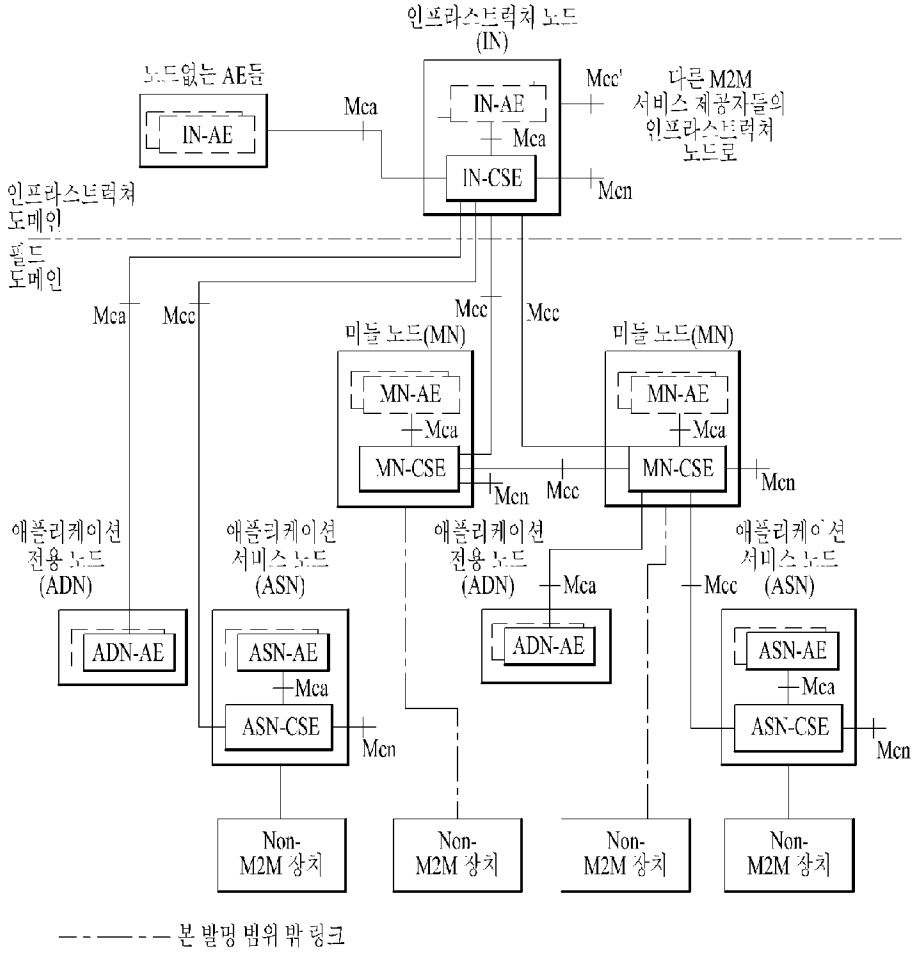
[청구항 18] 제10항에 있어서, 상기 제1M2M 엔티티가 상기 특정 자원을 가지고 있는지 여부의 판단은 상기 제2M2M 엔티티의 식별자와 보안 연계와 관련한 크리덴셜과 연계된 식별자가 상관관계가 있다고 판단된 경우에만 수행되는 것을 특징으로 하는, M2M 장치.

WO 2016/013846 PCT/KR2015/007546

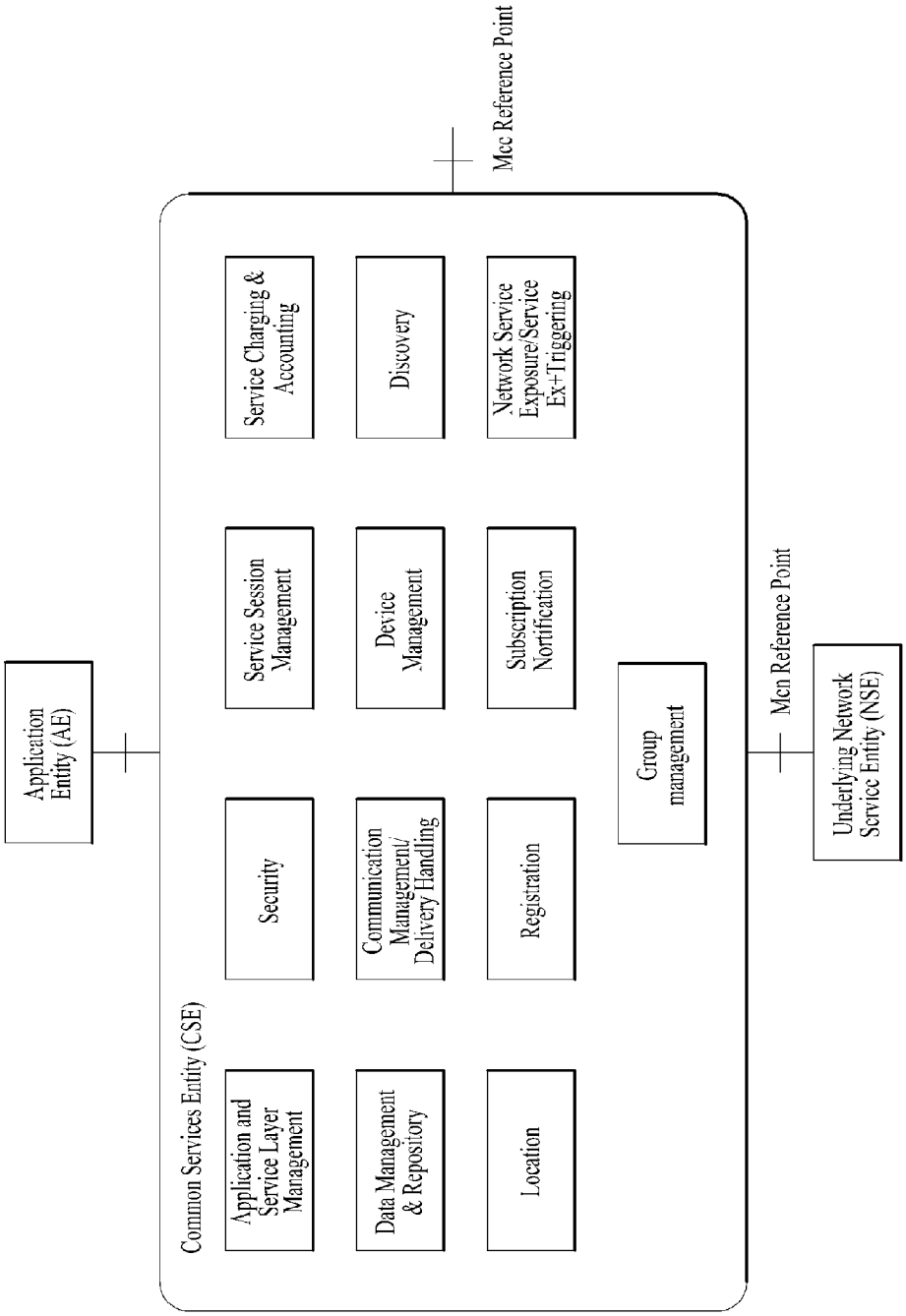
[도1]



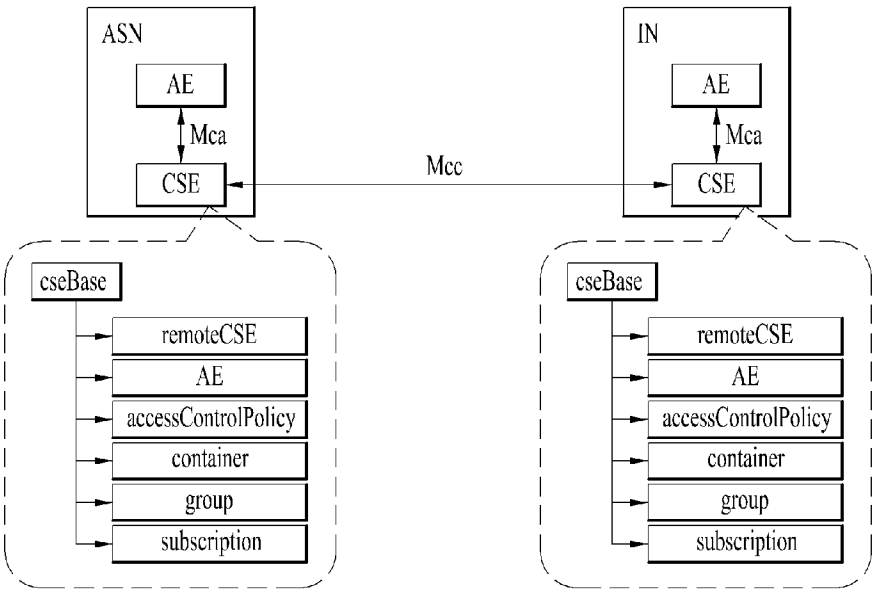
[도2]



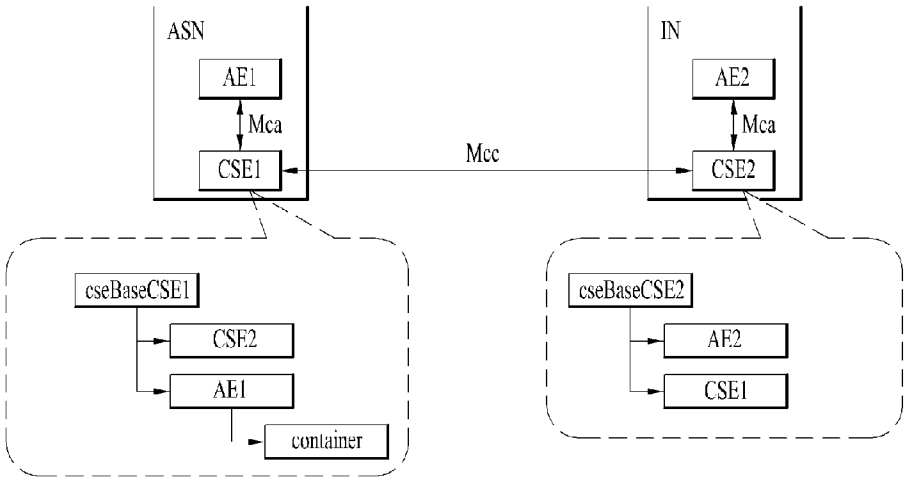
[도3]


Application Entity (AE)
Mcc Reference Point
Common Services Entity (CSE)
Application and Service Layer Management
Data Management & Repository
Location
Security
Communication Management/ Delivery Handling
Registration
Service Session Management
Device Management
Subscription Notification
Group management
Service Charging & Accounting
Discovery
Network Service Exposure/Service Ex+Triggering
Mcn Reference Point
Underlying Network Service Entity (NSE)

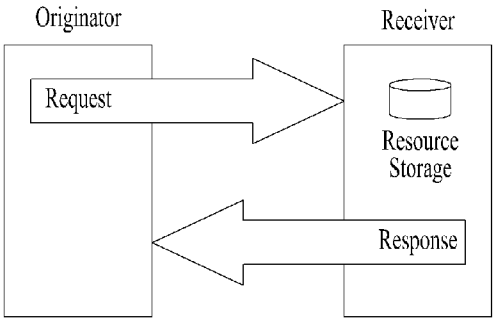
[도4]


ASN
AE
Mca
CSE
Mcc
IN
AE
Mca
CSE
cseBase
remoteCSE
AE
accessControlPolicy
container
group
subscription
cseBase
remoteCSE
AE
accessControlPolicy
container
group
subscription

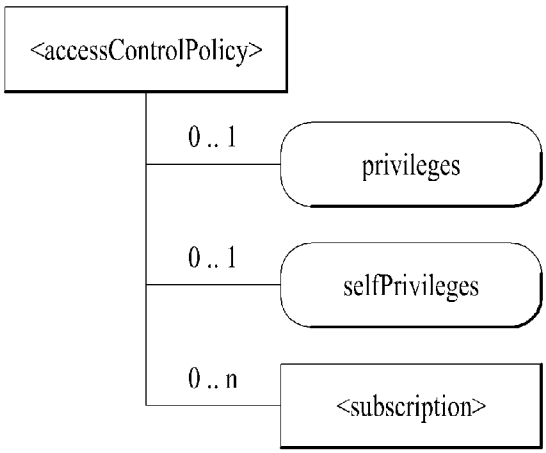
[도5]


ASN
AE1
Mca
CSE1
Mcc
IN
AE2
Mca
CSE2
cseBaseCSE1
CSE2
AE1
container
cseBaseCSE2
AE2
CSE1

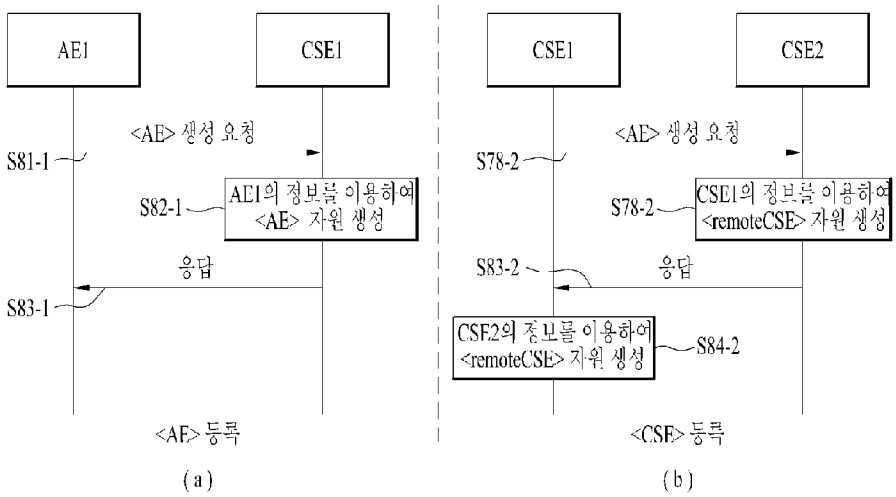
[도6]


Originator
Receiver
Request
Resource
Storage
Response

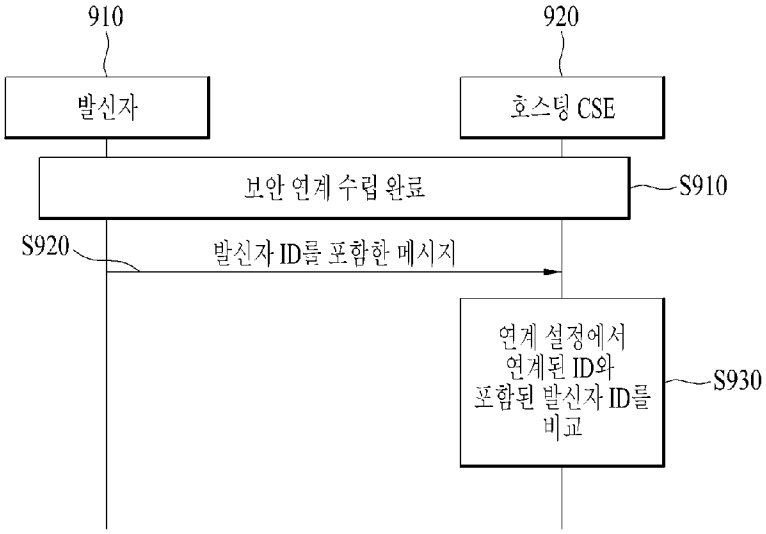
[도7]


<accessControlPolicy>
0 .. 1
privileges
0 .. 1
selfPrivileges
0 .. n
<subscription>

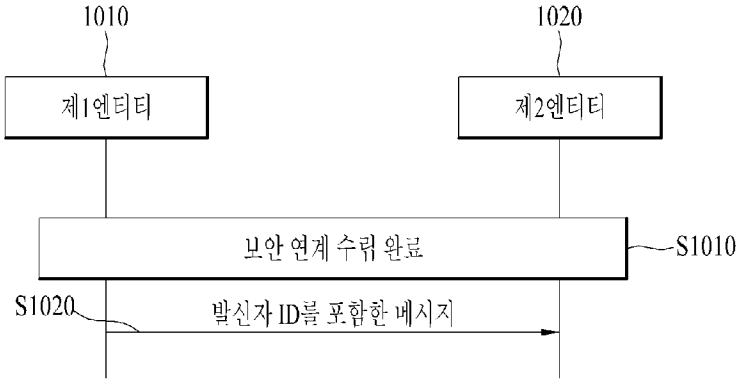
[도8]


AE1
CSE1
<AE> 생성 요청
S81-1
S82-1
AE1의 정보를 이용하여 <AE> 자원 생성
응답
S83-1
<AE> 등록
(a)
CSE1
CSE2
<AE> 생성 요청
S78-2
S78-2
CSE1의 정보를 이용하여 <remoteCSE> 자원 생성
S83-2
응답
CSE2의 정보를 이용하여 <remoteCSE> 자원 생성
S84-2
<CSE> 등록
(b)

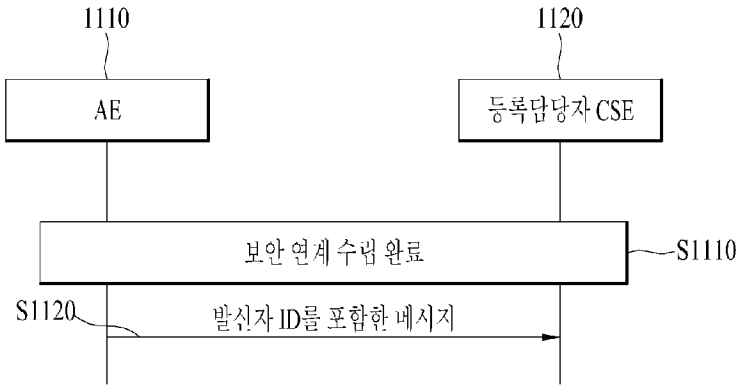
[도9]


910
920
발신자
호스팅 CSE
보안 연계 수립 완료
S910
S920
발신자 ID를 포함한 메시지
연계 설정에서 연계된 ID와 포함된 발신자 ID를 비교
S930

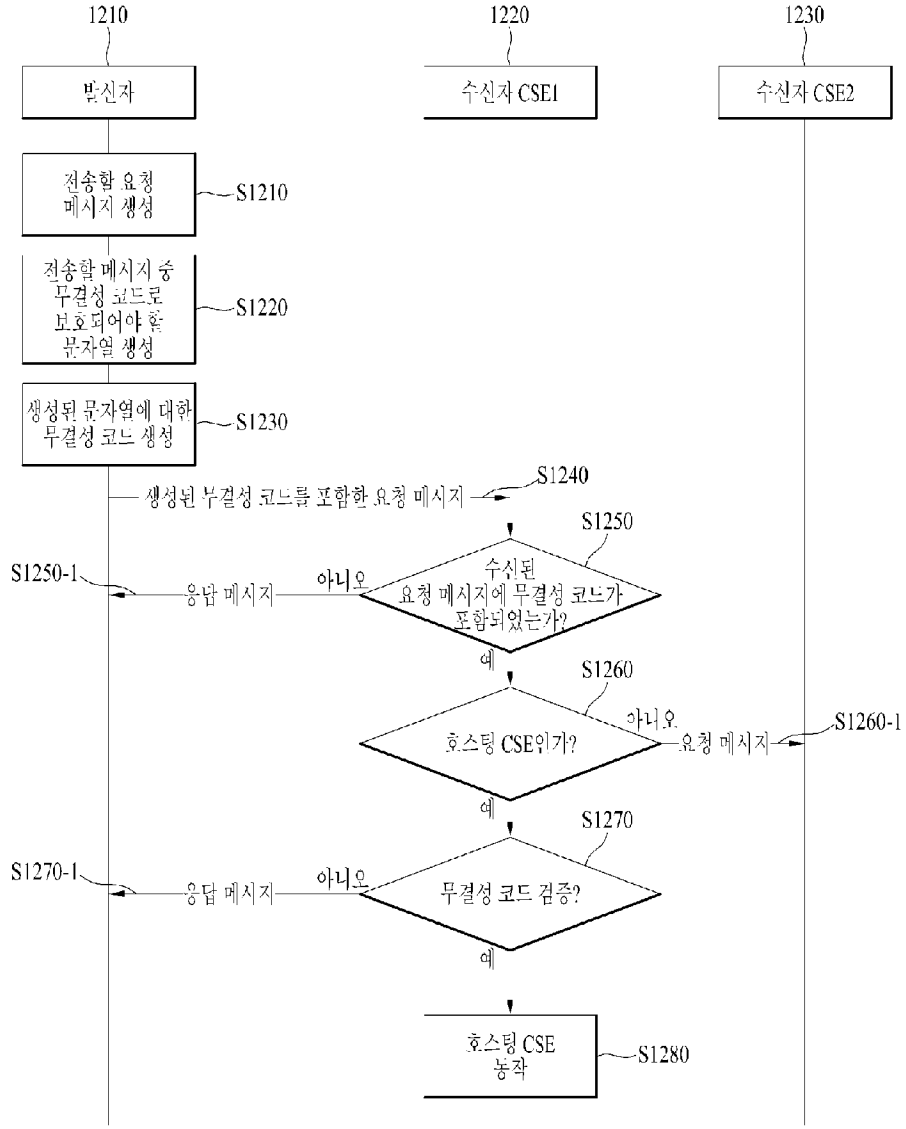
[도10]


1010
1020
제1엔티티
제2엔티티
보안 연계 수립 완료
S1010
S1020
발신자 ID를 포함한 메시지

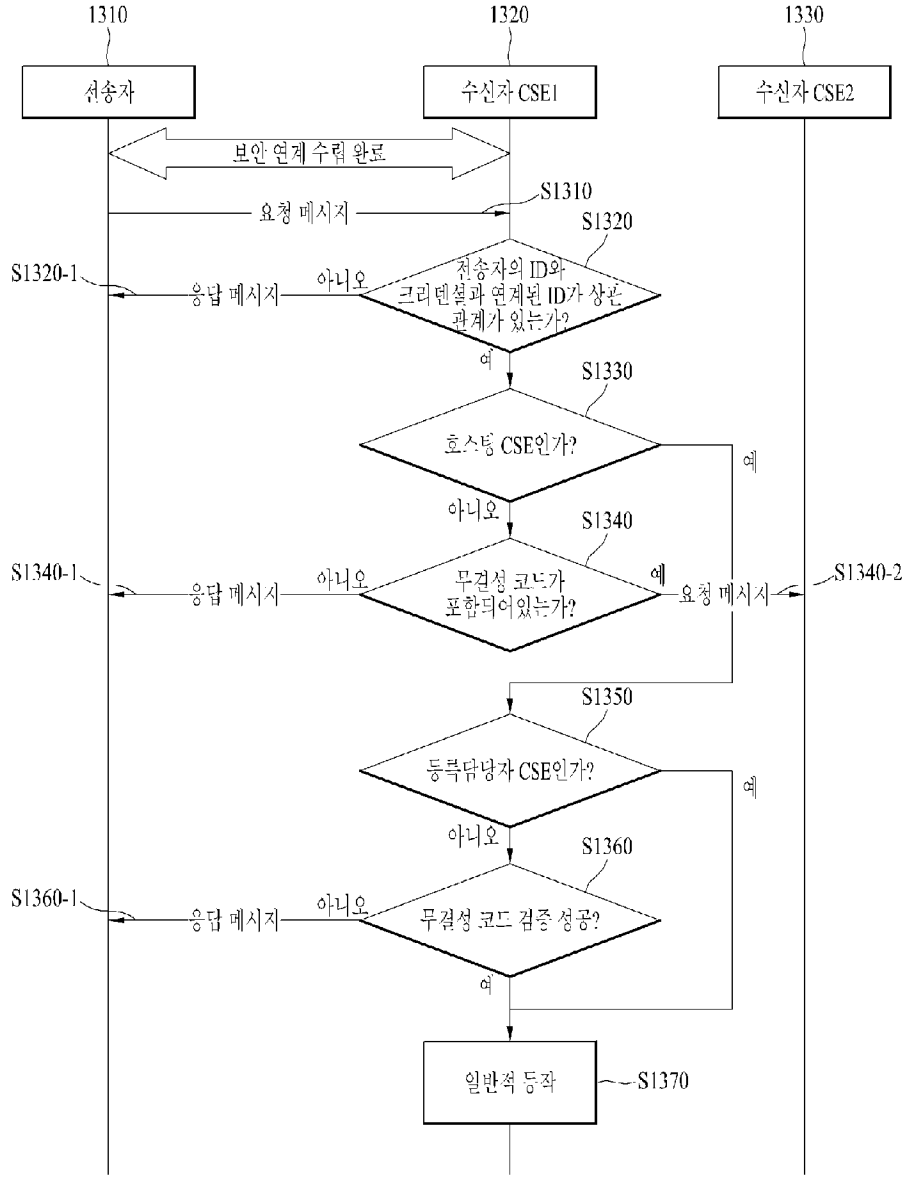
[도11]


1110
1120
AE
등록담당자 CSE
보안 연계 수립 완료
S1110
S1120
발신자 ID를 포함한 메시지

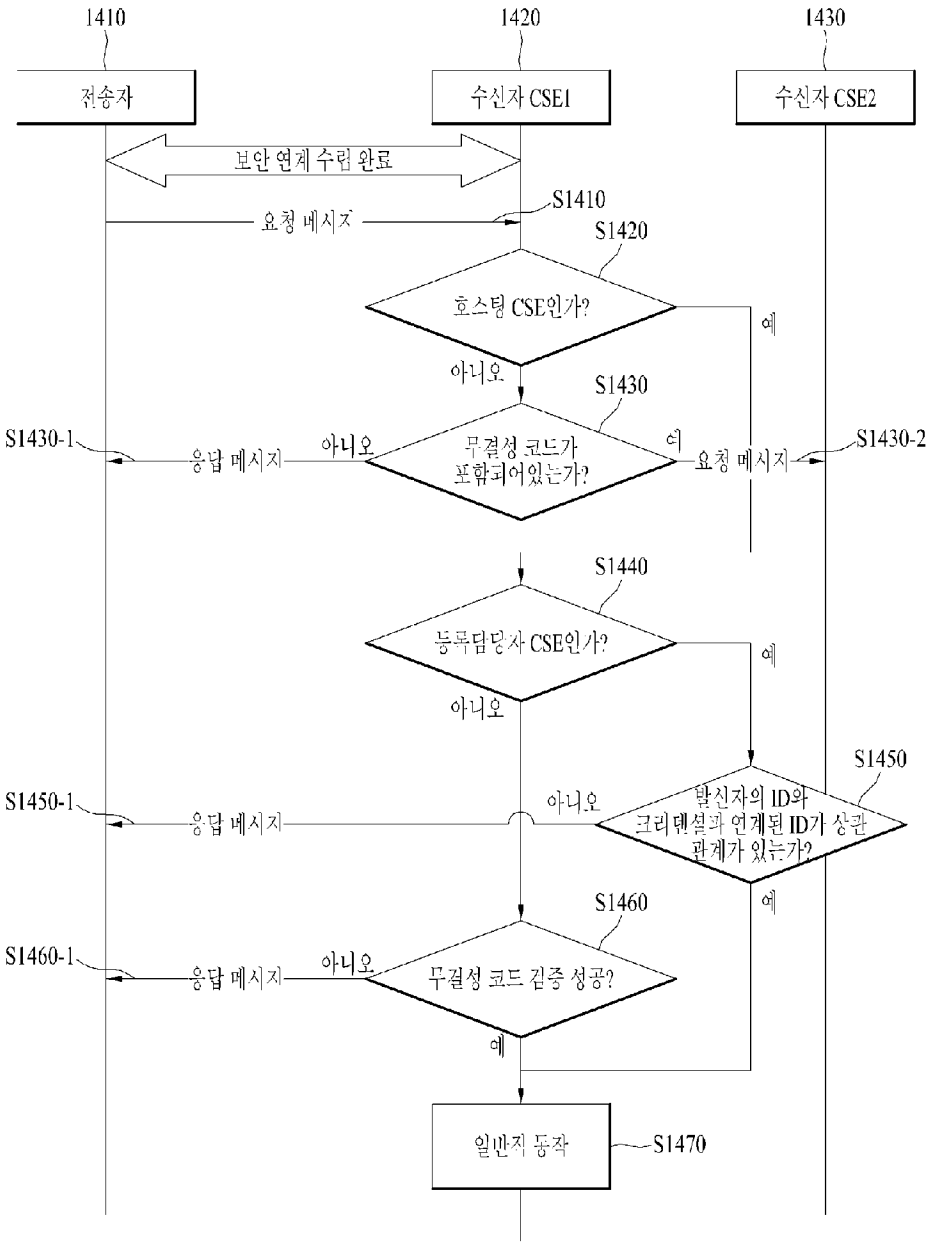
[도12]


1210
1220
1230
발신자
수신자 CSE1
수신자 CSE2
전송함 요청 메시지 생성
S1210
전송할 메시지 중 무결성 코드로 보호되어야 할 문자열 생성
S1220
생성된 문자열에 대한 무결성 코드 생성
S1230
S1240
생성된 무결성 코드를 포함한 요청 메시지
S1250
수신된 요청 메시지에 무결성 코드가 포함되었는가?
아니오
S1250-1
응답 메시지
예
S1260
호스팅 CSE인가?
아니오
S1260-1
요청 메시지
예
S1270
무결성 코드 검증?
아니오
S1270-1
응답 메시지
예
호스팅 CSE 동작
S1280

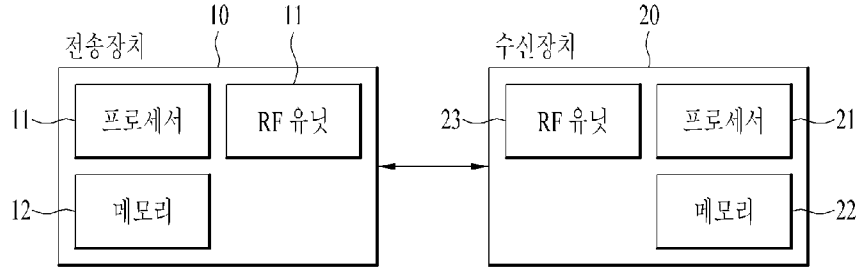
[도13]


1310
1320
1330
전송자
수신자 CSE1
수신자 CSE2
보안 연계 수립 완료
요청 메시지
S1310
S1320
S1320-1
응답 메시지
아니오
전송자의 ID와 크리덴셜과 연계된 ID가 상호 관계가 있는가?
예
S1330
호스팅 CSE인가?
예
아니오
S1340
S1340-1
응답 메시지
아니오
무결성 코드가 포함되어있는가?
예
요청 메시지
S1340-2
S1350
등록담당자 CSE인가?
예
아니오
S1360
S1360-1
응답 메시지
아니오
무결성 코드 검증 성공?
예
일반적 등작
S1370

[도14]


1410
1420
1430
전송자
수신자 CSE1
수신자 CSE2
보안 연계 수립 완료
S1410
요청 메시지
S1420
호스팅 CSE인가?
예
아니오
S1430
S1430-1
응답 메시지
아니오
무결성 코드가 포함되어있는가?
예
요청 메시지
S1430-2
S1440
등록담당자 CSE인가?
예
아니오
S1450
S1450-1
응답 메시지
아니오
발신자의 ID와 크리덴셜과 연계된 ID가 상관 관계가 있는가?
예
S1460
S1460-1
응답 메시지
아니오
무결성 코드 검증 성공?
예
일반적 동작
S1470

[도15]


10
11
전송장치
11
프로세서
RF 유닛
12
메모리
20
수신장치
23
RF 유닛
프로세서
21
메모리
22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2015/007546

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/10(2009.01)i, H04W 4/00(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W 12/10; G06F 21/30; H04W 8/20; H04W 40/24; H04W 12/06; H04W 12/08; H04W 4/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: M2M, impersonation, security, integrity, request, response

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-1274966 B1 (MODACOM CO., LTD.) 30 July 2013 See paragraphs [0010]-[0011], [0059]-[0065]; claim 1; and figures 1, 5.	1-18
A	US 2014-0056220 A1 (INTERDIGITAL PATENT HOLDINGS, INC.) 27 February 2014 See paragraphs [0023]-[0034], [0152]; and figure 1A.	1-18
A	"Machine-to-Machine communications (M2M); M2M service requirements", ETSI TS 102 689 V2.1.1, 01 July 2013 (http://www.etsi.org/deliver/etsi_ts/102600_102699/102689/02.01.01_60/ts_102689v020101p.pdf) See pages 26-27.	1-18
A	KR 10-2010-0138684 A (KT CORPORATION) 31 December 2010 See paragraphs [0051]-[0073]; and figure 3.	1-18
A	KR 10-2012-0140249 A (INTERDIGITAL PATENT HOLDINGS, INC.) 28 December 2012 See paragraphs [0425]-[0436]; and figure 9c.	1-18

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 NOVEMBER 2015 (10.11.2015)	**11 NOVEMBER 2015 (11.11.2015)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2015/007546

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-1274966 B1	30/07/2013	US 2014-0317707 A1	23/10/2014
		WO 2013-085088 A1	13/06/2013
US 2014-0056220 A1	27/02/2014	CA 2882856 A1	27/02/2014
		CN 104584670 A	29/04/2015
		EP 2888922 A2	01/07/2015
		KR 10-2015-0048180 A	06/05/2015
		TW 201424441 A	16/06/2014
		WO 2014-031829 A2	27/02/2014
		WO 2014-031829 A3	17/04/2014
KR 10-2010-0138684 A	31/12/2010	NONE	
KR 10-2012-0140249 A	28/12/2012	CN 103081432 A	01/05/2013
		EP 2543207 A1	09/01/2013
		EP 2543207 B1	06/05/2015
		JP 05457563 B2	02/04/2014
		JP 05750519 B2	22/07/2015
		JP 2013-522705 A	13/06/2013
		JP 2014-116953 A	26/06/2014
		KR 10-2014-0094008 A	29/07/2014
		US 2013-0212637 A1	15/08/2013
		US 9032473 B2	12/05/2015
		WO 2011-109518 A1	09/09/2011

국 제 조 사 보 고 서

국제출원번호
PCT/KR2015/007546

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 12/10(2009.01)i, H04W 4/00(2009.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04W 12/10; G06F 21/30; H04W 8/20; H04W 40/24; H04W 12/06; H04W 12/08; H04W 4/00

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: M2M, impersonation, security, integrity, request, response

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-1274966 B1 (모다정보통신 주식회사) 2013.07.30 단락 [0010]-[0011], [0059]-[0065]; 청구항 1; 및 도면 1, 5 참조.	1-18
A	US 2014-0056220 A1 (INTERDIGITAL PATENT HOLDINGS, INC.) 2014.02.27 단락 [0023]-[0034], [0152]; 및 도면 1A 참조.	1-18
A	`Machine-to-Machine communications (M2M); M2M service requirements`, ETSI TS 102 689 V2.1.1, 2013.07.01 (http://www.etsi.org/deliver/etsi_ts/102600_102699/102689/02.01.01_60/ts_102689v020101p.pdf) 페이지 26-27 참조.	1-18
A	KR 10-2010-0138684 A (주식회사 케이티) 2010.12.31 단락 [0051]-[0073]; 및 도면 3 참조.	1-18
A	KR 10-2012-0140249 A (인터디지탈 패튼 홀딩스, 인크) 2012.12.28 단락 [0425]-[0436]; 및 도면 9c 참조.	1-18

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2015년 11월 10일 (10.11.2015)	2015년 11월 11일 (11.11.2015)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-472-7140

심사관
양정록
전화번호 +82-42-481-5709

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2015/007546

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-1274966 B1	2013/07/30	US 2014-0317707 A1	2014/10/23
		WO 2013-085088 A1	2013/06/13
US 2014-0056220 A1	2014/02/27	CA 2882856 A1	2014/02/27
		CN 104584670 A	2015/04/29
		EP 2888922 A2	2015/07/01
		KR 10-2015-0048180 A	2015/05/06
		TW 201424441 A	2014/06/16
		WO 2014-031829 A2	2014/02/27
		WO 2014-031829 A3	2014/04/17
KR 10-2010-0138684 A	2010/12/31	없음	
KR 10-2012-0140249 A	2012/12/28	CN 103081432 A	2013/05/01
		EP 2543207 A1	2013/01/09
		EP 2543207 B1	2015/05/06
		JP 05457563 B2	2014/04/02
		JP 05750519 B2	2015/07/22
		JP 2013-522705 A	2013/06/13
		JP 2014-116953 A	2014/06/26
		KR 10-2014-0094008 A	2014/07/29
		US 2013-0212637 A1	2013/08/15
		US 9032473 B2	2015/05/12
		WO 2011-109518 A1	2011/09/09