(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년05월29일
(11) 등록번호 10-2116399
(24) 등록일자 2020년05월22일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04W 12/06* (2009.01)
H04W 12/08 (2009.01) *H04W 4/70* (2018.01)
(52) CPC특허분류
H04L 63/0823 (2013.01)
H04L 63/0435 (2013.01)
(21) 출원번호 10-2018-7003104
(22) 출원일자(국제) 2016년06월30일
심사청구일자 2018년01월31일
(85) 번역문제출일자 2018년01월31일
(65) 공개번호 10-2018-0025923
(43) 공개일자 2018년03월09일
(86) 국제출원번호 PCT/US2016/040438
(87) 국제공개번호 WO 2017/004391
국제공개일자 2017년01월05일
(30) 우선권주장
62/188,141 2015년07월02일 미국(US)
62/248,808 2015년10월30일 미국(US)
(56) 선행기술조사문헌
EP02890073 A1*
US20150033312 A1*
WO2015080515 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
콘비다 와이어리스, 엘엘씨
미국 19809-3727 델라웨어주 윌밍턴 스위트 300 벨레뷰 파크웨이 200
(72) 발명자
초이, 비노드, 쿠마
미국 19403 펜실베이니아주 노리스타운 미닛멘 레인 1201
시아, 요젠드라, 씨.
미국 19341 펜실베이니아주 엑스톤 레전시 코트 10
(뒷면에 계속)
(74) 대리인
양영준, 김연송, 백만기

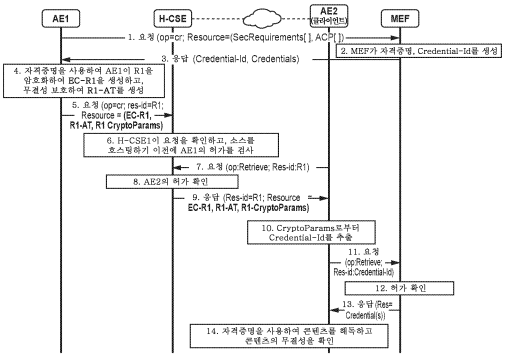
전체 청구항 수 : 총 17 항 심사관 : 오수정

(54) 발명의 명칭 **서비스 레이어에서의 콘텐츠 보안**

(57) 요 약

예로서 oneM2M 네트워크와 같은 네트워크 내의 보안에 대한 기존 접근법은 제한적이다. 예로서, 콘텐츠가 서로 신뢰하는 엔티티간에 전송되는 동안에만 콘텐츠가 보호될 수 있다. 여기에서 M2M 네트워크의 콘텐츠 무결성과 기밀성이 보호된다. 이러한 콘텐츠는 호스팅 노드에 콘텐츠가 저장되는 "휴지 상태"일 수 있다. 허가된 엔티티만이 호스팅 노드에 저장된 데이터를 저장 및 검색할 수 있으며 데이터는 기밀성 관점 및 무결성 관점에서 보호될 수 있다.

대 표 도 - 도24



(52) CPC특허분류
H04L 63/061 (2013.01)
H04L 63/101 (2013.01)
H04W 12/06 (2019.01)
H04W 12/08 (2019.01)
H04W 4/70 (2018.02)
(72) 발명자
시드, 데일, 엔.
미국 18104 펜실베이니아주 앨런타운 노스 36번 스트리트 229
스타시닉, 마이클, 에프.
미국 18940 펜실베이니아주 뉴타운 앤드류 드라이브 190
라만, 샤밈, 아크바
캐나다 큐씨 에이치4브이 1비8 코테 세인트-룩 콘클린 로드 6704
리, 취앙
미국 19454 펜실베이니아주 노스 웨일즈 스털링 드라이브 115
천, 쥐
미국 19703 델라웨어주 클레이몬트 파리쉬 애비뉴 1397
플린, 윌리엄, 로버트, 4세
미국 19473 펜실베이니아주 슈웬크스빌 메이베리 로드 451

명 세 서

청구범위

청구항 1

프로세서, 메모리 및 통신 회로를 포함하는 장치로서,

상기 장치는 그 통신 회로를 통해 네트워크에 접속되고, 상기 장치는 상기 장치의 메모리에 저장된 컴퓨터 실행 가능 명령어들을 추가로 포함하며, 상기 컴퓨터 실행 가능 명령어들은 상기 장치의 상기 프로세서에 의해 실행될 때, 상기 장치로 하여금

제1 애플리케이션으로부터, 콘텐츠를 호스팅하기 위한 리소스를 생성하기 위한 제1 요청을 수신하는 동작 - 상기 콘텐츠는 상기 제1 애플리케이션과 연관되고 상기 콘텐츠와 연관된 보안 요구 사항들에 기초하여 보안됨 -;

상기 제1 애플리케이션이 상기 장치에서 상기 리소스를 생성하도록 허가되는지 여부를 결정하는 동작; 및

상기 제1 애플리케이션이 허가되는 경우, 상기 보안된 콘텐츠를 호스팅하는 동작을 포함하는 동작들을 수행하게 하는 장치.

청구항 2

제1항에 있어서, 상기 제1 애플리케이션은 상기 장치와는 별개의 공통 서비스 엔티티에 의해 상기 리소스를 생성하도록 허가되는 장치.

청구항 3

제2항에 있어서, 상기 요청은 상기 공통 서비스 엔티티에 의해 생성된 자격증명 아이덴티티를 포함하는 장치.

청구항 4

제1항에 있어서, 상기 장치로 하여금,

제2 애플리케이션으로부터 상기 보안된 콘텐츠에 액세스하기 위한 제2 요청을 수신하는 동작;

상기 제2 애플리케이션이 상기 보안된 콘텐츠에 액세스하도록 허가되는지 여부를 결정하는 동작; 및

상기 제2 애플리케이션이 상기 보안된 콘텐츠에 액세스하도록 허가된 경우, 상기 보안된 콘텐츠를 상기 제2 애플리케이션에 송신하는 동작을 포함하는 추가 동작들을 수행하게 하는 컴퓨터 실행 가능 명령어들을 추가로 포함하는 장치.

청구항 5

제4항에 있어서, 상기 보안된 콘텐츠는 공통 서비스 엔티티가 상기 보안된 콘텐츠와 연관된 하나 이상의 자격증명을 상기 제2 애플리케이션에 송신할 때 해독될 수 있는 장치.

청구항 6

제4항에 있어서, 상기 제2 애플리케이션은 상기 제1 애플리케이션의 액세스 제어 정책에 의해 상기 보안된 콘텐츠에 액세스하도록 허가되는 장치.

청구항 7

프로세서, 메모리 및 통신 회로를 포함하는 장치로서,

상기 장치는 그 통신 회로를 통해 네트워크에 접속되고, 상기 장치는 상기 장치의 메모리에 저장된 컴퓨터 실행 가능 명령어들을 추가로 포함하며, 상기 컴퓨터 실행 가능 명령어들은 상기 장치의 상기 프로세서에 의해 실행될 때, 상기 장치로 하여금

호스팅 공통 서비스 엔티티 상에 휴지 상태에서(at rest) 저장될 때 애플리케이션 콘텐츠를 암호화 또는 무결성

보호하는 하나 이상의 자격증명에 대한 요청을 공통 서비스 엔티티로 송신하는 동작 - 상기 요청은 상기 애플리케이션 콘텐츠와 연관된 하나 이상의 보안 파라미터들에 기초함 -;

상기 요청에 응답하여, 상기 공통 서비스 엔티티로부터, 상기 하나 이상의 자격증명을 획득하는 동작;

상기 하나 이상의 자격증명을 사용하여 상기 애플리케이션 콘텐츠를 암호화 또는 무결성 보호하는 동작; 및

상기 암호화된 또는 무결성 보호된 컨텐츠를 저장하는 리소스를 생성하기 위한 요청을 상기 호스팅 공통 서비스 엔티티로 전송하는 동작을 포함하는 동작들을 수행하게 하는 장치.

청구항 8

제7항에 있어서, 상기 하나 이상의 자격증명은 대칭 키 기밀성 보호를 위한 마스터 키를 포함하는 장치.

청구항 9

삭제

청구항 10

삭제

청구항 11

제7항에 있어서, 상기 애플리케이션 콘텐츠를 암호화 또는 무결성 보호하는 동작은 상기 애플리케이션 콘텐츠를 암호화하여 암호화된 콘텐츠를 생성하는 동작을 포함하고,

상기 장치는, 상기 장치로 하여금

상기 콘텐츠와 관련된 인증 태그를 생성하는 동작- 상기 인증 태그는 호스팅 공통 서비스 엔티티에서의 호스팅을 위한 상기 콘텐츠의 무결성 및 신뢰성을 나타냄 -을 포함하는 추가 동작들을 수행하게 하는 컴퓨터 실행 가능 명령어들을 추가로 포함하는 장치.

청구항 12

삭제

청구항 13

제7항에 있어서, 상기 장치는 애플리케이션 엔티티이며, 상기 자격증명은 신뢰 인에이블먼트(trust enablement) 기능으로부터 획득되는 장치.

청구항 14

제13항에 있어서, 상기 콘텐츠를 획득하도록 허가된 제2 애플리케이션 엔티티는 상기 신뢰 인에이블먼트 기능으로부터 상기 하나 이상의 자격증명을 획득할 수 있는 장치.

청구항 15

프로세서, 메모리 및 통신 회로를 포함하는 장치로서,

상기 장치는 그 통신 회로를 통해 네트워크에 접속되고, 상기 장치는 상기 장치의 메모리에 저장된 컴퓨터 실행 가능 명령어들을 추가로 포함하며, 상기 컴퓨터 실행 가능 명령어들은 상기 장치의 상기 프로세서에 의해 실행될 때, 상기 장치로 하여금

콘텐츠와 연관된 보안 요구 사항들에 기초하여, 호스팅 노드 상에 휴지 상태에서 저장될 때 애플리케이션 콘텐츠를 암호화 또는 무결성 보호하는 하나 이상의 자격증명을 생성하는 동작;

상기 하나 이상의 자격증명을 사용하여 상기 애플리케이션 콘텐츠를 암호화 또는 무결성 보호하는 동작; 및

허가된 클라이언트 만이 상기 호스팅 노드로부터 상기 콘텐츠를 검색할 수 있도록, 상기 호스팅 노드가 상기 암호화 또는 무결성 보호된 콘텐츠를 저장하게 하는 요청을 상기 호스팅 노드로 송신하는 동작을 포함하는 동작들을 수행하게 하는 장치.

청구항 16

제15항에 있어서, 상기 장치로 하여금

상기 하나 이상의 자격증명을 신뢰 인에이블먼트 기능에 등록하는 동작을 포함하는 추가 동작들을 수행하게 하는 컴퓨터 실행 가능 명령어들을 추가로 포함하는 장치.

청구항 17

제16항에 있어서, 상기 하나 이상의 자격증명은 상기 장치와 신뢰 인에이블먼트 기능 사이의 연계를 부트스트래핑함으로써 생성되는 장치.

청구항 18

제16항에 있어서, 상기 장치로 하여금

상기 요청에 응답하여, 상기 신뢰 인에이블먼트 기능으로부터 자격증명 아이덴티티를 수신하는 동작- 상기 요청은 상기 자격증명 아이덴티티와 연관된 자격증명을 포함하고, 상기 요청은 상기 자격증명의 등록을 추구함 -을 포함하는 추가 동작들을 수행하게 하는 컴퓨터 실행 가능 명령어들을 추가로 포함하는 장치.

청구항 19

제18항에 있어서, 상기 자격증명 아이덴티티는 공통 서비스 엔티티에 고유한 장치.

청구항 20

제15항에 있어서, 상기 장치로 하여금

상기 호스팅 노드가 상기 장치가 상기 호스팅 노드에서 리소스를 생성하도록 허가되어 있다고 결정하면 성공 메시지를 수신하는 동작을 포함하는 추가 동작들을 수행하게 하는 컴퓨터 실행 가능 명령어들을 추가로 포함하는 장치.

발명의 설명

기 술 분 야

[0001] 관련 출원들에 대한 상호 참조

[0002] 본 출원은 2015년 7월 2일자로 출원된 미국 가특허 출원 제62/188,141호 및 2015년 10월 30일자로 출원된 미국 가특허 출원 제62/248,808호에 대한 우선권을 주장하며, 이들 출원은 모두는 그 전체가 참조로 포함된다.

배 경 기 술

[0003] 전형적인 통신 세션은 일반적으로 노드들이라고도 지칭될 수 있는 2개 이상의 통신 엔티티들(예로서, 디바이스들, 애플리케이션들 등) 사이의 정보의 지속적인 상호작용적 교환을 수반한다. 현재의 RESTful 접근 방식에서는 실제 지속적인 연결이 없다. 대신 주문형 요청 및 응답 메시지들을 통해 통신이 수행된다. 통신 세션이 특정 시점에서 수립되고, 이후의 시점에서 다양한 상황들에 기초하여(예를 들어, 세션 타임들의 종료 후에 또는 엔티티들 중 하나가 세션을 종료하기로 결정할 때) 해제(torn down)된다. 통신 세션은 종종 엔티티들간의 다수의 메시지들의 교환을 수반하고 통상적으로 상태 저장이 가능할 수 있으며(stateful), 이는 통신 세션을 유지할 수 있도록 통신하는 엔티티들 중 적어도 하나가 세션 히스토리에 관한 정보를 저장할 필요가 있음을 의미한다. 저장될 수 있는 예시적 정보는 자격증명, 식별자 등과 같은 보안 컨텍스트를 포함한다. 통신 세션들은 네트워크 프로토콜 스택의 다양한 레이어들에서 프로토콜들 및 서비스들의 일부로서 구현될 수 있다. 예로서, 도 1은 전송 프로토콜 레이어, 애플리케이션 프로토콜 레이어, 애플리케이션 서비스 레이어, 및 애플리케이션들 사이에서의 네트워크 노드들 사이에 확립된 통신 세션들을 도시한다.

[0004] M2M(machine-to-machine) 서비스 레이어는 M2M 유형 디바이스들 및 애플리케이션들에 대한 부가 가치 서비스들을 제공하는 것을 구체적으로 목표로 하는 일 타입의 애플리케이션 서비스 레이어의 예이다. 예를 들어, M2M 서비스 레이어는 애플리케이션들 및 디바이스들에게 서비스 레이어에 의해 지원되는 M2M 중심 능력들의 집합체(collection)에 대한 액세스를 제공하는 API들(Application Programming Interfaces)을 지원할 수 있다. 예시

적 능력들은 제한적이지는 않지만 보안, 과금, 데이터 관리, 디바이스 관리, 발견, 프로비저닝, 및 접속성 관리를 포함한다. 도 2는 oneM2M 사양들에 지정된 공통 서비스 기능(CSF; common services function)을 보여준다.

[0005] 도 2를 참조하면 예시된 기능(능력들)은 M2M 서비스 레이어에 의해 정의되는 메시지 포맷들, 리소스 구조들, 및 리소스 표현들을 사용하는 API들을 통해 애플리케이션들에 이용가능하게 된다. M2M 네트워크 기술들의 표준화의 추세는 M2M 서비스 레이어의 표준화이다. M2M 서비스 레이어의 표준화의 예들에는 다양한 oneM2M 사양들이 포함된다.

[0006] M2M 서비스 레이어 세션은 M2M 서비스 레이어 인스턴스와 M2M 애플리케이션 또는 다른 M2M 서비스 레이어 인스턴스간에 확립된 통신 세션을 나타낸다. M2M 서비스 레이어 세션은 연결, 보안, 스케줄링, 데이터, 컨텍스트 등과 관련된 M2M 서비스 레이어 상태로 구성될 수 있다. 이 상태는 M2M 서비스 레이어, M2M 애플리케이션 또는 그 조합에 의해 유지될 수 있다. M2M 서비스 레이어 세션은 하나 이상의 기본 하위 레이어 통신 세션들 위에 계층화될 수 있다. 그렇게 함에 있어서, 세션 상태(예로서, 보안 자격증명, 혼잡 정보 등)는 상이한 세션들 사이에서 공유되고 이용될 수 있다. 또한, 하위 레이어 세션들이 설정되고 해제되는 것과 무관하게 M2M 서비스 레이어 세션이 지속되고 유지될 수 있도록 M2M 서비스 레이어 세션은 하위 레이어 세션들과 관련하여 지속성을 지원할 수 있다. M2M 서비스 레이어 세션이 그 상단에 계층화될 수 있는 하위 레이어 세션들의 예들은 애플리케이션 프로토콜 레이어 세션들(예를 들어, HTTP 또는 CoAP) 및 전송 프로토콜 레이어 세션들(예를 들어 TCP 및/또는 UDP)을 포함하지만 이에 한정되지 않으며, 이들은 예로서 TLS(Transport Layer Security)(TCP용 TLS) 또는 DTLS(Datagram Transport Layer Security)(UDP용 DTLS)와 같은 프로토콜을 사용하여 보안될 수 있다.

[0007] oneM2M 서비스 레이어 보안에 대한 현재 접근법과 관련하여, oneM2M 엔드포인트들이 안전한 방식으로 서로 통신할 때, 노드들과 중간 노드들은 서로 홉-바이-홉(hop-by-hop) 방식으로 서로 보안 연계를 확립한다. 각 홉에는 다른 홉과 독립적인 별도의 보안 연계가 있을 수 있다. 홉-바이-홉 보안 연계는 대칭 키들을 사용하거나, 인증서/원시 공개 키들을 사용하거나, 디바이스 제조업체나 서비스 공급자의 서비스들을 사용하여 직접 프로세스 또는 원격으로 수행할 수 있는 부트스트래핑 프로세스에 의해 확립될 수 있다. 또한 oneM2M 보안 솔루션의 최신 버전인 oneM2M-TS-0003 보안 솔루션에 따르면 "서비스 레이어 레벨에서 보안 연계 확립은 TLS 또는 DTLS 세션을 초래하며, 이는 인접한 AE/CSE 사이에서, 즉 홉-바이-홉(hop-by-hop)으로 교환되는 메시지를 보호한다."

[0008] 도 3은 관련된 두 통신 엔티티들에 대해 고유하고 기밀인 자격증명을 사용하는 (D)TLS 보안 연계에 의한 엔티티들 사이의 HbH(Hop-by-Hop) 보안 연계들의 예를 도시한다. 도시된 바와 같이, 제1 애플리케이션 엔티티(AE1) 및 제1 호스팅 공통 서비스 엔티티(HCSE1)는 두 엔티티들(AE1, HCSE1)에 의해 공유되는 HbH 자격증명(H1)에 기초하여 보안 (D)TLS 연결을 생성한다. 마찬가지로 HCSE1과 중간 노드(IN-CSE1)는 H2 자격증명을 사용하여 보안 (D)TLS 연결을 설정한다. 도시된 바와 같이, 자격증명 H3은 IN-CSE와 제2 HCSE(HCSE2) 사이에 (D)TLS 연결을 생성하기 위해 사용되며 자격증명 H4는 제2 AE(AE2)와 HCSE2 사이의 보안 연결을 생성하는 데 사용된다.

[0009] 여전히 도 3을 참조하면, HCSE1이 AE2에 정보를 통신하기를 원한다면, 정보는 먼저 HCSE1과 IN-CSE 사이의 (D)TLS 연결을 통해 송신된다. 그런 다음 정보는 (D)TLS 애플리케이션에 의해 해독된 후 추출된 다음 서비스 레이어에서 처리되고 IN-CSE와 HCSE2 사이의 별도 (D)TLS 터널을 통해 재패키징 송신된다. HCSE2는 메시지를 처리한 다음 HCSE2와 AE2 사이의 다른 보안 터널을 통해 메시지를 다시 터널링한다. 도시된 예에 도시된 바와 같이, 임의의 두 개의 HbH 엔티티들 사이의 통신은 (D)TLS로 보호되므로 엔티티들간에 전송되는 메시지의 기밀성 또는 무결성 파괴(breach)는 이들이 (D)TLS 연결에 의해 보호되기 때문에 어려워질 수 있지만, 메시지가 다음 홉으로 전달되기 전에 서비스 레이어(SL)에서 메시지가 처리되게 되는 엔티티에서는 보호되지 않을 수 있다.

[0010] 이제 객체 보안 이니셔티브로 돌아가면, 객체 보안 이니셔티브가 IETF에서 연구되고 표준화되었으며, 다양한 단일 사인-온(single sign-on) 솔루션들(예로서, OpenID)을 위해 구현되어 있다. IETF RFC 7165, Use Cases and Requirements for JSON Object Signing and Encryption에 기재된 바에 따르면, "많은 인터넷 애플리케이션에는 네트워크 레이어이나 전송 레이어의 보안 메커니즘 외에도 객체 기반 보안 메커니즘이 필요하다. 다년간 CMS(Cryptographic Message Syntax)는 ASN.1을 기반으로 하는 이진 보안 객체 포맷을 제공한다. 시간이 지남에 따라 ASN.1과 같은 이진 오브젝트 인코딩들은 JavaScript Object Notation(JSON)과 같은 텍스트 기반 인코딩들보다 덜 일반적인 상태가 되었다." JSON을 기반으로하는 다양한 보안 양태는 1) 무결성/신뢰성에 대해 JSON 웹 서명, IETF-RFC(7515); 2) 기밀성에 대해 JSON 웹 암호화, IETF-RFC(7516); 3) 자격증명 표현에 대해 JSON 웹 키, IETF-RFC(7516); 4) 알고리즘에 대해 JSON 웹 알고리즘, IETF-RFC(7518)에 명시되어 있다.

[0011] 전술한 바와 같이, 예로서 oneM2M 네트워크 내의 기존 보안 접근법은 제한적이다. 예로서, 서로 신뢰하는 엔티티들간에 콘텐츠가 전송되는 동안(비휴지 상태)에만 콘텐츠가 보호될 수 있다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0012] 이 발명의 내용은 이하에서 발명을 실시하기 위한 구체적인 내용에 추가로 기술되는 일련의 개념들을 간략화된 형태의 선택을 소개하기 위해 제공되어 있다. 이 발명의 내용은 청구된 발명 요지의 핵심적인 특징들 또는 필수적인 특징들을 확인해주는 것을 의도하지도 않고, 청구된 발명 요지의 범위를 제한하는 데 사용되는 것을 의도하지도 않는다. 게다가, 청구된 발명 요지는 본 개시내용의 임의의 부분에서 언급된 임의의 또는 모든 단점들을 해결하는 제한들로 제한되지 않는다.

[0013] 위에 설명된 문제와 같은 다양한 단점들이 여기서 다루어진다. 일 실시예에서, M2M 네트워크에서 콘텐츠의 무결성 및 기밀성이 보호된다. 그러한 콘텐츠는 콘텐츠가 노드 또는 장치에 저장되도록 "휴지상태(at rest)"일 수 있다.

[0014] 일 실시예에서, 장치, 예로서 애플리케이션 엔티티는 콘텐츠 보호를 제공하는 하나 이상의 자격증명에 대한 요청을 송신한다. 요청은 콘텐츠와 관련된 하나 이상의 보안 파라미터를 기반으로할 수 있다. 장치는 하나 이상의 자격증명을 획득하고, 하나 이상의 자격증명을 사용하여 콘텐츠를 보안할 수 있다. 자격증명은 대칭 키 기밀성 보호를 위한 마스터 키를 포함할 수 있다. 자격증명은 무결성 보호 및 기밀성 보호를 위한 자격증명을 포함할 수 있다. 장치는 암호화된 콘텐츠를 생성하기 위해 콘텐츠를 암호화할 수 있다. 장치는 콘텐츠와 관련된 인증 태그를 생성할 수 있다. 또한, 장치는 보안 콘텐츠 및 보안 파라미터를 포함하는 리소스를 생성하기 위해 호스팅 공통 서비스 엔티티에 요청을 송신할 수 있다. 자격증명은 하나의 예에 따라, 신뢰 인에이블먼트 기능, 예로서 M2M 인롤먼트 기능으로부터 획득될 수 있다. 호스팅 공통 서비스 엔티티는 인증된 애플리케이션들이 리소스를 생성하는 것만을 허용할 수 있으며, 호스팅 공통 서비스 엔티티는 인증된 애플리케이션들이 암호화된 콘텐츠를 검색하는 것만을 허용할 수 있다.

[0015] 다른 실시예에서, 하나 이상의 보안 요구 사항에 기초하여, 장치는 하나 이상의 암호 파라미터를 결정한다. 장치는 보안 호스팅 요청 메시지를 콘텐츠 호스팅 기능에 추가로 송신할 수 있으며, 보안 호스팅 요청 메시지는 하나 이상의 암호 파라미터 및 이와 관련된 콘텐츠를 포함할 수 있으므로 콘텐츠 호스팅 기능이 하나 이상의 암호 파라미터를 사용하여 콘텐츠를 안전하게 저장할 수 있다. 하나 이상의 암호 파라미터에 기초하여, 장치는 콘텐츠가 기밀화되도록 콘텐츠를 암호화할 수 있다. 일 예에서, 콘텐츠는 하위 컴포넌트들로 구성될 수 있고, 노드는 하나 이상의 암호 파라미터에 기초하여 각각의 하위 컴포넌트가 기밀화되도록 각각의 하위 컴포넌트를 암호화한다. 다른 예에서, 콘텐츠는 속성들 및 값들의 쌍들로 구성될 수 있고, 노드는 하나 이상의 암호 파라미터들에 기초하여 각각의 값이 기밀화되도록 각각의 값들을 암호화할 수 있다. 노드는 또한 콘텐츠가 무결성 보호되도록 콘텐츠와 연관된 인증 태그를 계산할 수 있다.

도면의 간단한 설명

[0016] 본 출원의 보다 견고한 이해를 용이하게 하기 위해서, 동일한 엘리먼트들은 동일한 번호들로 참조되는 첨부 도면들에 대한 참조가 이제 이루어진다. 이러한 도면들은 본 출원을 제한하는 것으로 해석되어서는 안 되며, 단지 예시적인 것으로 의도된다.

도 1은 네트워크 노드들 사이에 확립되는 다양한 통신 세션들의 예를 도시하는 도면이다.

도 2는 oneM2M에 의해 특정된 공통 서비스 기능들을 나타내는 도면이다.

도 3은 홉-바이-홉 방식으로 서로 보안 연계들을 확립하는 oneM2M 노드들의 예를 도시하는 호 흐름이다.

도 4는 애플리케이션 엔티티(AE), 호스팅 공통 서비스 엔티티(HCSE) 및 중간 노드 공통 서비스 엔티티(IN-CSE)를 포함하는 네트워크에서의 취약성을 악용하는 악성 엔티티의 예를 도시하는 예시적 사용 사례를 예시하는 호 흐름이다.

도 5는 공격자가 IN-CSE 또는 HCSE에서 취약성을 악용할 수 있는 다른 예시적 사용 사례를 도시하는 호 흐름이다.

도 6은 예시적인 실시예에 따른 예시적인 기능들 및 그 사이의 상호 작용들을 도시한 호 흐름이다.

도 7은 컴포넌트들 및 하위 컴포넌트들로 구성된 콘텐츠를 포함하는 예시적인 콘텐츠를 도시한다.

도 8은 예시적인 콘텐츠와 관련된 예시적인 암호 파라미터들을 도시한다.

도 9는 예시적인 콘텐츠와 관련된 예시적인 클라이언트-특정 암호 파라미터들을 도시한다.

도 10은 예시적인 실시예에 따른, 콘텐츠 생성 및 보안 결정 기능(CCSDF; Content Creation and Security Determination Function)과 신뢰도가 낮은 콘텐츠 호스팅 기능(CHF; Content Hosting Function) 사이의 예시적인 메시징을 나타내는 호 흐름이다.

도 11은 예시적인 실시예에 따른, CCSDF와 보안 콘텐츠 호스팅 기능(SCHF; Secure Content Hosting Function) 사이의 예시적인 메시징을 나타내는 호 흐름이다.

도 12는 임의의 예시적인 실시예에 따라 콘텐츠를 호스팅하기 위한 위치를 결정하기 위한 예시적인 흐름도이다.

도 13은 예시적인 실시예에 따라 보호된 콘텐츠 저장소(PCS; Protected Content Store) 내에 저장된 예시적인 보호된 콘텐츠 구조를 도시한다.

도 14는 콘텐츠와 관련된 예시적인 암호 파라미터들을 나타낸다.

도 15는 예시적인 실시예에 따른 콘텐츠 특정 자격증명 요청을 나타내는 호 흐름이다.

도 16은 예시적인 실시예에 따른 클라이언트 특정 자격증명 요청을 나타내는 호 흐름이다.

도 17은 예시적인 실시예에 따른 콘텐츠 특정 자격증명 등록을 나타내는 호 흐름이다.

도 18은 다른 예시적인 실시예에 따른 클라이언트 자격증명 등록을 도시하는 호 흐름이다.

도 19는 예시적인 실시예에 따른 제3 기관 자격증명 요청을 나타내는 호 흐름이다.

도 20은 예시적인 실시예에 따른 콘텐츠 검색을 위한 호 흐름이다.

도 21은 예시적인 실시예에 따라 클라이언트에 의해 수행될 수 있는 예시적인 보안 검사를 도시하는 흐름도이다.

도 22는 여기에 기술된 예시적인 보안 기능과 함께 도시된 도 2로부터의 도면이다.

도 23은 도시된 예시적인 보안 기능들을 갖는 공통 서비스 기능(CSF; Common Service Functions)의 도면이다.

도 24는 콘텐츠가 oneM2M 리소스로 표현되는 예시적인 실시예를 도시하는 호 흐름이다.

도 25는 예시적인 실시예에 따라 CSE에서 생성된 Credential-Id 리소스의 예시적인 구조를 도시한다.

도 26은 서비스 인에이블링 기능(SEF; Service Enabling Function)이 CSE에 존재하는 다른 예시적인 실시예를 도시하는 호 흐름이다.

도 27은 예시적인 실시예에 따른 신뢰 인에이블먼트 기능, 특히 머신-투-머신(M2M) 인롤먼트 기능(MEF; Enrollment Function)에서 생성된 Credential-Id 리소스의 예시적인 구조를 도시한다.

도 28은 예시적인 실시예에 따른 예시적인 액세스 제어 정책의 예시적인 구조를 도시한다.

도 29는 예시적인 실시예에 따른 보호 콘텐츠에 대한 예시적인 리소스 구조를 도시한다.

도 30은 예시적인 실시예에 따른 예시적인 암호 파라미터 리소스를 도시한다.

도 31은 무결성 보호된 관리 객체의 예를 도시한다.

도 32는 예시적인 보안 정책 리소스를 도시한다.

도 33은 예시적인 실시예에 따라 CCSDF에서 제공될 수 있는 예시적인 그래픽 사용자 인터페이스(GUI)를 도시한다.

도 34는 예시적인 실시예에 따라 SCHF에서 제공될 수 있는 예시적인 GUI를 도시한다.

도 35는 예시적인 실시예에 따라 SEF에 제공될 수 있는 예시적인 GUI를 도시한다.

도 36a는 하나 이상의 개시된 실시예들이 구현될 수 있는 예시적 M2M 또는 IoT(Internet of Things) 통신 시스템의 시스템 도면이다.

도 36b는 도 36a에 도시된 M2M/IoT 통신 시스템 내에서 사용될 수 있는 예시적인 아키텍처의 시스템 도면이다.

도 36c는 도 36a에 도시되는 통신 시스템 내에서 사용될 수 있는 예시적인 M2M/IoT 단말 또는 게이트웨이 디바이스의 시스템 도면이다.

도 36d는 도 36a의 통신 시스템의 양태들이 구현될 수 있는 예시적인 컴퓨팅 시스템의 블록도이다.

도 37은 리소스-특정 콘텐츠 보호를 위한 예시적인 실시예를 도시하는 호 흐름이다.

도 38은 클라이언트-특정 콘텐츠 보호를 위한 예시적인 실시예를 도시하는 호 흐름이다.

발명을 실시하기 위한 구체적인 내용

[0017] 전술한 바와 같이, 예로서 M2M 네트워크 내의 기존 보안 접근법은 제한적이다. 예로서 oneM2M에서 콘텐츠는 전송 레이어 프로토콜들(예로서, TLS/DTLS)을 통해 두 개의 '신뢰되는' 엔티티간에 '전송 중'인 동안에만 보호될 수 있다. 따라서 콘텐츠가 엔티티(휴지상태)에서 호스팅되는 동안 콘텐츠가 보호되지 않는다. 이는 콘텐츠(객체) 보호는 조금이라도 수행되는 경우 애플리케이션 레이어에서 수행되어야 한다는 것을 의미한다. 본 명세서에서 애플리케이션 콘텐츠 보호 접근법과 관련된 문제가 있음이 인식된다. 예로서, 애플리케이션은 애플리케이션 콘텐츠 보호를 위한 균일한 메커니즘을 제공하지 않는다. 또한 서비스 레이어 리소스는 자체적으로 보호되지 않는다. 또한 애플리케이션 레이어 보호들이 존재하는 경우 이들은 실제 애플리케이션 데이터 보호만 제공하고 SL(service layer)과 관련된 리소스들은 그렇지 않을 수 있다. 본 명세서에서, 콘텐츠를 보호하기 위한 별도의 애플리케이션 레이어 프로토콜들이 애플리케이션 콘텐츠 보호 접근법에 대해 수행되어야 한다는 것이 또한 인식되며, 이는 성가시다. 특정 시나리오에서 서비스 레이어가 부가 가치 서비스들을 제공할 수 있으려면 콘텐츠가 그 암호화되지 않은 형식으로 존재하여야 할 수 있다. 또한 oneM2M 리소스들과 관련된 보안 자격증명 및 보안 보호들의 라이프 사이클 관리가 현재 수행되지 않는다는 점도 인식된다. 폐기된 엔티티들에서 호스트되는 데이터의 보안을 처리하는 메커니즘은 현재 다루어지지 않는다.

[0018] 본 명세서에서 사용될 때, "서비스 레이어"라는 용어는 네트워크 서비스 아키텍처 내의 기능 레이어(functional layer)를 지칭한다. 서비스 레이어들은 전형적으로 HTTP, CoAP 또는 MQTT와 같은 애플리케이션 프로토콜 레이어 위쪽에 위치되고 클라이언트 애플리케이션들에게 부가 가치 서비스들을 제공한다. 서비스 레이어는 또한, 예로서, 제어 레이어 및 전송/액세스 레이어와 같은, 하위 리소스 레이어에서 코어 네트워크들에 대한 인터페이스를 제공한다. 서비스 레이어는 서비스 정의, 서비스 런타임 인에이블먼트(service runtime enablement), 정책 관리, 액세스 제어, 및 서비스 클러스터링을 포함하는 다수의 카테고리들의 (서비스) 능력들 또는 기능들을 지원한다. 최근에, 몇 개의 산업 표준 단체들, 예컨대, oneM2M이 M2M 유형의 디바이스들 및 애플리케이션들을 인터넷/웹, 셀룰러, 엔터프라이즈, 및 홈 네트워크들과 같은 배치들에 통합시키는 것과 연관된 과제들을 해결하기 위해 M2M 서비스 레이어들을 개발해오고 있다. M2M 서비스 레이어는 애플리케이션들 및/또는 다양한 디바이스들에게, CSE 또는 SCL이라고 지칭될 수 있는, 서비스 레이어에 의해 지원되는, 앞서 언급된 능력들 또는 기능들의 집합체 또는 세트에 대한 액세스를 제공할 수 있다. 몇 가지 예들은, 다양한 애플리케이션들에 의해 흔히 사용될 수 있는, 보안, 과금, 데이터 관리, 디바이스 관리, 발견, 프로비저닝, 및 접속성 관리를 포함하지만, 이들로 제한되지 않는다. 이 능력들 또는 기능들은 M2M 서비스 레이어에 의해 정의되는 메시지 포맷들, 리소스 구조들, 및 리소스 표현들을 사용하는 API들을 통해 이러한 다양한 애플리케이션들에게 이용가능하게 된다. CSE 또는 SCL은 하드웨어 및/또는 소프트웨어로 구현될 수 있는 그리고 다양한 애플리케이션들 및/또는 디바이스들에 노출된 (서비스) 능력들 또는 기능들(예를 들어, 이러한 기능 엔티티들 사이의 기능 인터페이스들)을, 그들이 이러한 능력들 또는 기능들을 사용하도록, 제공하는 기능 엔티티이다.

[0019] 예로서, 현재의 oneM2M 솔루션들에 대한 문제를 추가로 설명하기 위해, 도 4 및 도 5는 각각의 사용 사례들을 도시한다. 도 4에서, 데이터/콘텐츠 프라이버시에 대한 영향들이 도시되어 있고, 도 5는 데이터/콘텐츠의 무결성 보호 및 인증의 부족과 관련된 문제점들을 예시한다.

[0020] 도 4를 특히 참조하면, 네트워크(400)는 4개의 예시적인 엔티티들을 포함한다: 제1 애플리케이션 엔티티(AE1), 호스팅 공통 서비스 엔티티(HCES1), 중간 노드 CSE(IN-CSE) 및 악성 엔티티- 해커 애플리케이션 또는 비-악성 기능일 수 있음 -. 402에서, AE1은 속성들 및 콘텐츠/콘텐츠 인스턴스들을 저장하는 서비스 레이어에서 HCSE1 내의 리소스를 생성한다. 이 사용 사례에서는 예들로서 두 가지 속성이 제공된다: 속성 1 및 속성 2. 이 예에

따르면, AE1 및 HCSE1은 서로간에 상호 인증되고, 402에서 "리소스 생성" 동작을 수행하기 전에 보안 통신 채널을 사용한다. 소정 시점에서, 404에서, 악성 엔티티(예로서, 해킹 애플리케이션)는 IN-CSE를 통해 HCSE1 내의 취약성을 악용한다. 일부 경우에, 해킹 애플리케이션이 IN-CSE를 거치지 않고도 HCSE1에 도달할 수 있다. 다른 경우에, IN-CSE에서 프로토콜 지원의 다양성(예를 들어, 열린 포트들 및 실행되는 서비스들)으로 인해 가능하게는 IN-CSE의 취약성을 마찬가지로 악용하는 것에 의해 해킹 애플리케이션에 대한 좋은 진입점이 될 수 있다. 해커가 HCSE1에 액세스할 수 있으면 해커는 406에서 AE1 리소스 내에 저장된 콘텐츠를 도용한다. 이것은 정교함을 그다지 필요로하지 않는 고전적인 공격일 수 있다. 이러한 공격을 완화하는 한 가지 방법은 전체 디스크를 암호화하거나 파일 단위로 암호화를 사용하는 것이다. 그러나 콘텐츠는 SL에서 처리되어야하고 통신 경로상의 통과 노드에서 해독되어야 하므로 콘텐츠가 공격에 취약해질 수 있다. 또 다른 완화 기법은 JSON 기반 객체 서명 및 암호화 메커니즘을 사용하여 콘텐츠를 보호하는 것이다. 그러나 현재 SL 리소스를 보호하기 위해 이러한 메커니즘을 사용할 수 있는 프레임워크가 없다. 추가적인 문제는 HCSE1의 플랫폼이 신뢰할 수 없으므로 보안 프로세스들이 수행되지 않을 수 있다는 것이다. 또한 루트 키(root key)가 손상된 경우, 이는 HCSE1에 저장된 모든 AE의 데이터를 노출시킨다. 요약하면, 애플리케이션 데이터 또는 사용자의 기밀 데이터의 보안이 사용자나 애플리케이션에 많은 제어권이 없는 엔티티에 오프로드되며 플랫폼의 신뢰도는 사용자가 SP에 대해 갖는 신뢰를 기반으로 한다. 또한 HCSE1이 폐기될 때 데이터가 HCSE1 내에 남아있을 수 있으며 파일 기반 암호화에 의해서만 보호되고, 이러한 파일 기반 암호화는 리소스들을 보호하는 구식 운영 체제에서 쉽게 손상될 수 있다.

[0021] 따라서, 요약하면, 도 4의 사용 사례는 콘텐츠가 휴지 상태에 있을 때 호스팅 엔티티(예로서, HCSE)에서 기밀성 보호 메커니즘의 부재, 콘텐츠를 클라이언트로 송신할 때 데이터가 TLS/DTLS 터널을 통해 들어오고 나서 각 홉(예로서, 통과 CSE)이 콘텐츠에 대한 암호화되지 않은 액세스를 갖는 HCSE(예로서, 신뢰할 수 없는 HCSE)로부터도 콘텐츠를 은닉하기 위한 메커니즘의 부재, 및 콘텐츠의 라이프 사이클에 대해 정기적으로 콘텐츠의 보안성을 다시 순환시킬 수 있는 능력의 부재를 예로서 도시하지만, 이들에만 한정되는 것은 아니다.

[0022] 이제, 도 5에 도시된 사용 사례를 참조하면, 네트워크(500)는 콘텐츠를 생성하는 제1 애플리케이션 엔티티(AE1) 및 AE1에 의해 생성된 콘텐츠를 소비하는 클라이언트 애플리케이션들인 제2 AE(AE2) 및 제3 AE(AE3)를 포함한다. 네트워크는 호스팅 CSE(HCSE1) 및 중간 노드-CSE(IN-CSE)를 더 포함한다. 이 예에서 콘텐츠는 어떠한 무결성 보호도 없이 HCSE1에서 호스팅된다. 도 4에 도시된 예시적인 사용 사례와 유사하게, 공격자는 IN-CSE 또는 HCSE1의 취약성들을 악용할 수 있다. 1에서, AE1은 HCSE1에서 리소스를 생성한다. 예로서, 공격자는 리소스 및/또는 리소스 구조(예컨대, 속성들 및/또는 콘텐츠)를 2 및 3에서 수정할 수 있다. 도시된 바와 같이, 도 5는 공격자가 AE1의 속성(속성 1이라 칭함)의 비허가된 수정을 수행할 수 있는 시나리오를 도시한다. AE1의 리소스에 가입한 AE2는 4 및 5에서 수정된 리소스 사본을 획득한다. 일부 경우에, 예로서 AE1에서 얻은 리소스를 사용하여 AE2의 중요한 결정들 또는 동작들을 수행하는 경우 수정사항이 중요한 영향들을 가질 수 있다. 6 및 7에서, 예시된 예에 따라, 공격자는 속성 2를 삭제하고 새로운 속성들(속성 3 및 속성 4)을 추가한다. 따라서 이 예에서 공격자는 리소스를 변경하는 것뿐만 아니라 리소스의 구조도 변경한다. 이때, 리소스에 가입한 AE3은 AE1이 생성한 것과는 완전히 다른 리소스 트리를 가진다. 따라서, 도 5의 예시적인 사용 사례에 의해 도시된 바와 같이, 현재의 보안 접근법들은 리소스에 무결성 보호를 제공하지 못할 수 있고, 리소스 구조에 무결성 보호를 제공하지 못할 수 있고, 및/또는 시스템 중요 리소스들에 무결성 보호를 제공하지 못할 수 있다.

[0023] 위에 설명된 문제와 같은 다양한 단점들이 여기서 다루어진다. 일 실시예에서, 콘텐츠의 무결성 및 기밀성이 보호된다. 본 명세서에서 사용될 때, 달리 명시되지 않은 한, 용어 콘텐츠는 기계 제어 또는 사람이 제어하는 클라이언트 애플리케이션들 또는 서비스 기능들(예를 들어, 펌웨어, 구성 파라미터들, 정책들, 컨텍스트, 문서들 등)에 의해 생성되거나 소비되는 모든 데이터를 지칭한다. 따라서, 콘텐츠 및 데이터라는 용어는 제한없이 본 명세서에서 상호 교환적으로 사용될 수 있다. 콘텐츠는 가장 원시적 형태(예를 들어, 온도 판독치, 기타 센서 판독치들 등)일 수 있다. 일부 경우에, 콘텐츠는 그와 연계된 추가 메타데이터를 갖는 원시 데이터이거나 원시 데이터와 메타데이터를 갖는 원시 데이터의 조합일 수 있다. 콘텐츠는 또한 예로서 머신 실행 가능 콘텐츠(예로서, 컴퓨터 프로그램, 바이너리 코드, 컴파일 또는 번역될 수 있는 실행 가능 머신 코드, 컴퓨터 프로그램 스크립트들 등), 컴퓨터 관련 구성 파라미터들, 운영 정책들(예를 들어, 보안 또는 서비스 정책들), 멀티미디어 콘텐츠(예를 들어, 비디오, 오디오 등), 문서들 또는 특정 금전적, 전략적 또는 지적 가치를 갖는 모든 것 같은 다양한 정보를 지칭할 수 있다. 콘텐츠는 객체라고도 지칭될 수 있다.

[0024] 본 명세서에서 사용될 때, 달리 명시되지 않는 한, 인증은 엔티티와 관련된 아이덴티티(identity)에 대한 신뢰

를 확립하는 프로세스를 말한다. 기밀성이란 일반적으로 허가된 엔티티만 데이터를 볼 수 있도록 하는 프로세스를 말한다. 본 명세서에 사용될 때, 달리 명시되지 않는 한, 엔티티 또는 노드는 애플리케이션, 애플리케이션 서브세트, 서비스 인에이블링 기능, 또는 디바이스(예로서, 센서 디바이스)를 지칭할 수 있다. 본원에 기술되는 다양한 기술들은 하드웨어, 펌웨어, 소프트웨어, 또는 적절한 경우, 이들의 조합들과 관련하여 구현될 수 있다. 이러한 하드웨어, 펌웨어, 및 소프트웨어는 통신 네트워크의 다양한 노드들에 위치된 장치들에 존재할 수 있다. 장치들은 본원에 기술되는 방법들을 수행하기 위해 단독으로 또는 서로 조합하여 동작할 수 있다. 본 명세서에서 사용될 때, "장치", "네트워크 장치", "노드", "디바이스", "엔티티" 및 "네트워크 노드"라는 용어들은 서로 바꾸어 사용될 수 있다. "무결성"이란 용어는 메시지나 시스템이 비허가 엔티티에 의해 변경되지 않는다는 신뢰를 확립하는 프로세스를 지칭할 수 있다. 사물 인터넷(IoT)은 일반적으로 인터넷에 연결될 수 있는 고유하게 식별 가능한 객체들 및 그 가상 표현들을 지칭한다. 본 명세서에서 사용될 때, 라이프 사이클 관리라는 용어는 그와 연계된 데이터 및 자격증명을 프로비저닝, 유지 보수 및 폐기 페이즈들을 통해 관리하는 메커니즘을 의미한다.

[0025] 다양한 M2M 용어들이 본 명세서에 사용된다. M2M 서비스 레이어는 일반적으로 한 세트의 API들(Application Programming Interfaces) 및 기본 네트워킹 인터페이스들을 통해 M2M 애플리케이션들 및 디바이스들에 대한 부가 가치 서비스들을 지원하는 소프트웨어 미들웨어 레이어를 지칭한다. M2M 서비스 레이어 홉은 두 개의 M2M 서비스 레이어간 또는 M2M 서비스 레이어와 M2M 애플리케이션 사이의 M2M 서비스 레이어 통신 세션을 지칭한다. M2M 서비스 레이어 세션은 일반적으로 본질적으로 상태 저장이 가능한(stateful) 2개 이상의 통신 엔티티들간에 확립된 메시지 교환을 지칭한다. 본 명세서에 사용될 때, 달리 명시되지 않는 한, M2M 서비스 레이어 세션 엔드포인트는 M2M 서비스 레이어 세션 통신의 소스 또는 목적지일 수 있는 논리적 엔티티를 지칭한다. 또한, 본 명세서에 사용될 때, 달리 명시되지 않는 한, M2M 서비스 레이어 세션 관리자는 M2M 서비스 레이어 세션 관리를 위한 서비스들을 제공하는 논리적 엔티티를 지칭한다. 난스(nonce)는 세션과 연관될 수 있고 그 유효성이 세션/시간 컴포넌트와 연관될 수 있는 무작위 값을 나타낸다.

[0026] 서론으로, 콘텐츠의 보안 보호를 가능하게 하기 위해 다양한 기능 및 프로세스 메커니즘이 본 명세서에서 정의된다. 다양한 기능들은 예로서 명명된 것이며, 기능들은 대안적으로 필요에 따라 명명될 수 있음을 이해할 것이다. 콘텐츠 생성 및 보안 결정 기능(CCSDF; Content Creation and Security Determination Function)이 아래에 설명되어 있다. CCSDF는 다수의 기능들로 구성될 수 있으며 동일한 엔티티(노드)에서 호스팅되거나 다른 관리 도메인들에 존재할 수도 있는 다수 엔티티(노드)들에 분산되어 있을 수 있다. 콘텐츠 생성 기능(CCF; Content Creation Function)은 수집된 데이터를 기반으로 콘텐츠를 생성할 수 있다. 일부 경우에, 콘텐츠는 원시 데이터 또는 정보일 수 있고, 콘텐츠는 센서 데이터 또는 원시 데이터로부터 생성된 정보를 포함할 수 있다. CCF는 콘텐츠의 서브-컴포넌트들을 기반으로 콘텐츠에 대한 구조 및 콘텐츠에 대한 구조의 일부 형태를 만들 수 있다. 보안 결정 기능(SDF; Security Determination Function)은 콘텐츠와 관련된 보안 요구 사항들을 결정하는 것을 담당할 수 있다. SDF는 콘텐츠를 보호하기 위해 필요한 보안 수준을 결정할 수 있다. 예로서, SDF는 확립된 정책에 기초하여 콘텐츠 보호를 위한 일반 보안 요구 사항을 결정할 수 있다.

[0027] 보안 콘텐츠 호스팅 기능(SCHF; Secure Content Hosting Function)이 본 명세서에서 설명된다. 예시적인 실시예에서, SCHF는 콘텐츠를 안전하게 호스트하는 기능이다. 또한 SCHF는 보안 정책 시행 엔티티로 기능하고 액세스 제어 검사들을 수행할 수 있다. SCHF는 콘텐츠를 보안하기 위해 필요한 암호화 절차들을 처리, 식별 및 수행할 수 있다. SCHF는 적절한 자격증명을 요청하고 등록하기 위해 SEF(Security Enabling Function)와 상호작용할 수 있다. 일 실시예에서, SEF는 콘텐츠를 보호 및/또는 액세스하기 위한 자격증명을 제공하는 인에이블링 기능이다. SEF는 예로서 클라이언트에게 콘텐츠에 대한 액세스를 제공하기 위해 신뢰할 수 있는 제3 기관(TTP)과 같은 신뢰할 수 있는 중개자로 작용할 수 있다. SEF는 적절한 콘텐츠 특정 자격증명을 프로비저닝하고 등록할 수 있다. SEF는 적절한 클라이언트 특정 자격증명을 프로비저닝하고 등록할 수 있다.

[0028] 보안 파라미터 결정 프로세스(SPDP; Security Parameters Determination Process)가 예시적인 실시예에 따라 아래에서 설명된다. 예시적인 SPDP의 일부로서, 올바른 보안 파라미터들의 세트가 "휴지 상태"의 특정 콘텐츠에 대해 결정된다. 또한 콘텐츠의 라이프 사이클 관리가 결정될 수도 있다. 예로서, 휴지 상태에서의 콘텐츠 보안과 관련된 보안 정책들이 쿼리될 수 있다. 적절한 보안 파라미터가 유도되도록 정책들이 처리될 수 있다. 라이프 사이클 관리 파라미터들이 결정 및 유도될 수도 있다.

[0029] 예시적인 실시예에서, 보안 호스팅 요청 프로세스(SHRP; Secure Hosting Requisition Process)는 CCSDF에 의해 개시될 수 있다. 일부 경우들에서, SHRP는 SCHF에 의해 개시될 수도 있다. 요청의 일부로서, CCSDF는 SCHF로 콘텐츠의 보안 호스팅을 요청할 수 있다. SCHF는 제로 홉(동일한 플랫폼에서 호스팅됨), CCSDF로부터 한 홉(일

반적으로 선호되는 접근법), CCSDF로부터 다수 홉(2개 이상의 홉들만큼 떨어짐) 떨어져 있을 수 있다. SHRP는 SCHF가 특정 수준의 신뢰성을 기반으로 발견되도록 한다. 예시적인 실시예에서, 콘텐츠의 호스팅은 보안 요구 사항들에 기초하여 요청될 수 있다. SCHF는 일 실시예에 따라 보안 콘텐츠를 호스팅할 수 있다.

[0030] 아래에 CRRP(Credential Requisition & Registration Process)가 설명되어 있으며, 이는 CQP(Credential Requisition Process) 및 CGP(Credential Registration Process)를 포함할 수 있다. CQP 동안 SCHF는 콘텐츠의 보안 저장을 위한 적절한 자격증명의 프로비저닝을 요청할 수 있다. 예로서 일부 경우에는 SCHF가 콘텐츠에 대한 적절한 자격증명을 생성하기에 충분할 수 있기 때문에 이 프로세스는 선택적일 수 있다. 클라이언트 특정 콘텐츠가 보호되어야 하는 예에서, 이때, SDP는 클라이언트의 자격증명을 요청할 수 있다. 예로서, 특정 콘텐츠와 연관된 자격증명이 요청될 수 있다. 다른 예로서, 알고리즘 및 자격증명 유형에 기초하여 자격증명이 요청될 수 있다. 또한 클라이언트에 특정한 자격증명이 요청될 수도 있다. 예시적 CGP의 일부로서 콘텐츠 보호에 사용되는 자격증명의 세트가 SEF와 함께 공개될 수 있다. 예로서 확장성을 이유로 자격증명이 여러 SEF들에서 공개될 수 있다. CGP는 콘텐츠와 관련된 생성된 자격증명의 등록을 요청할 수 있는 능력; 사용할 알고리즘, 자격증명 유형, 자격증명 사용 방법에 대한 메커니즘 및 자격증명과 관련된 액세스 제어 정책(ACP)을 지정하는 능력; 및 클라이언트가 사용할 자격증명을 등록할 수 있는 능력을 제공할 수 있다.

[0031] 보안 호스팅 프로세스(SHP; Secure Hosting Process)의 예가 여기에 설명되어 있다. 이 프로세스의 일부로서, SCHF는 CCSDF로부터의 SHRP 메시지에 기초하여 콘텐츠를 호스팅할 수 있다. 콘텐츠는 콘텐츠를 보유하기 위한 올바른 컨테이너들/속성들의 세트를 포함시킴으로써 CCSDF가 요청한 적절한 포맷으로 호스팅될 수 있다. 대안적으로, 또는 추가적으로, SCHF는 콘텐츠를 보안 호스팅하기 위해 적절한 암호화 동작을 수행해야 할 수도 있다. 수행되는 암호화 동작의 유형은 콘텐츠와 관련된 보안 파라미터들에 기초할 수 있다. SCHP는 콘텐츠를 보호하기 위해 적절한 암호 프로세스들을 획득하고 수행할 수 있다. 또한, SHRP 메시지에 기초하여, SCHF는 콘텐츠와 관련된 보안 특성들을 업데이트하기 위해 트리거되는 적절한 라이프 사이클 관리 프로세스들을 생성할 수 있다. 예로서, 콘텐츠가 삭제되거나 액세스할 수 없게 될 수 있다.

[0032] 예로서 TPCRP(Third-Party Credential Requisition Process)가 여기에 설명되어 있다. 경우에 따라 SEF는 클라이언트(제3 기관)가 리소스에 액세스하고 그 신뢰성을 확인할 수 있도록 클라이언트에게 허가하고 필요한 자격증명을 제공해야 할 수 있다. TPCRP는 임의의 엔티티(예로서, 클라이언트)가 콘텐츠와 연관된 아이덴티티(content-Id)에 기초하여 SEF 또는 SCHF에 자격증명을 요청할 수 있게 한다. 예시적인 콘텐츠 검색 프로세스(CRP; Content Retrieval Process) 동안, 클라이언트는 콘텐츠에 대한 액세스를 요청하는 메커니즘을 개시한다. 클라이언트는 사전 구성된 정보로부터 SCHF에 관한 정보를 얻을 수 있거나 정보가 DNS-SD 또는 RD를 사용하여 동적으로 발견될 수 있다. 필요한 암호화 파라미터들을 포함하여 보안 콘텐츠(암호화 및/또는 무결성 보호)가 검색될 수 있다. 콘텐츠 처리(CP)도 여기에 설명되어 있다. CP 동안, 콘텐츠에 액세스하기를 원하는 클라이언트는 콘텐츠의 신뢰성 및/또는 무결성을 확인하고자 할 수 있다. 또한 클라이언트는 콘텐츠와 관련된 콘텐츠 구조 및 속성들을 확인하고자 할 수 있다. 일 예에서, 클라이언트는 콘텐츠의 신뢰성/무결성, 콘텐츠의 하위 컴포넌트들 및 콘텐츠의 구조를 확인할 수 있다. 콘텐츠는 프로비저닝된 암호화 파라미터를 기반으로 해독될 수 있다.

[0033] 예로서, CLMP(Content Life-cycle Management Process)에서 CCSDF는 선택적으로 명시적인 CLMP 메시지를 송신하여 특정 콘텐츠의 라이프 사이클 관리를 업데이트할 수 있다. CCSDF가 명시적 라이프 사이클 관리 요구 사항들을 SHRP의 일부로 통신한 경우 이 프로세스/메시징을 생략할 수 있다. 자격증명은 리프레시되고 암호화 동작들은 주기적으로 수행될 수 있다. 폐기 기간에 기초하여 콘텐츠가 소거될 수 있다. 임시 또는 영구적으로 자격증명을 재프로비저닝, 재보호 또는 제거할 수 있도록 콘텐츠와 관련된 자격증명을 관리할 수 있다.

[0034] 일반적으로 도 6을 참조하면, 전술한 다양한 단점에 대응하기 위해, 본 명세서에 기술된 바와 같이 콘텐츠/데이터의 보호가 이행된다. 본 명세서에 기술된 바와 같이, 데이터의 보호는 데이터에 대한 액세스를 요청하는 엔티티가 데이터에 액세스하도록 허가되었는지를 보증하는 것을 포함할 수 있다(인증을 포함할 수도 있음). 데이터의 보호는 데이터가 비허가 엔티티들로부터 은닉(예로서, 암호화)되고 비허가 엔티티들에 불투명하게 나타나는 것을 포함할 수 있다. 데이터 보호는 데이터의 비허가 수정을 검출하는 것을 포함할 수 있다. 콘텐츠 보호에는 정기적 또는 영구적으로 콘텐츠의 라이프 사이클을 관리하는 것이 포함될 수 있다.

[0035] 일 실시예에서, 콘텐츠는 하위 컴포넌트들로부터 생성되고(필요한 경우), 콘텐츠에 대한 구조는 하위 컴포넌트들에 기초하여 생성될 수 있다. 이는 CCP가 수행할 수 있다. SDF는 하위 컴포넌트들의 보안 요구 사항들을 평가하여 콘텐츠 보호에 대한 보안 요구 사항들의 위험 기반 평가를 수행할 수 있다. 일 실시예에서, 휴지 상태

에서 콘텐츠를 보호하는데 필요한 적절한 보안 파라미터들이 식별된다. 이것은 SPDP를 사용하여 달성할 수 있다. CRRP는 자격증명을 얻거나 생성하고 콘텐츠 보호를 위한 자격증명을 등록할 수 있다. 예시적인 실시예에서, 콘텐츠는 SHP를 사용하여 보안 방식으로 호스팅된다. 여기에 설명된 TPCRP는 콘텐츠에 액세스하기 위해 허가된 제3 기관들에게 자격증명을 프로비저닝하기 위한 능력을 제공할 수 있다.

[0036] 이하의 설명은 주로 콘텐츠의 보호에 초점을 두지만 여기에 설명된 자격증명은 다양한 서비스 인에이블링 기능들에 의해 생성, 업데이트, 삭제 및 검색되는 시스템 리소스들을 보호하기 위해 적절히 조정될 수 있음을 이해할 수 있을 것이다.

[0037] 도 6 내지 도 35, 도 37 및 도 38은 콘텐츠를 보호하기 위한 방법 및 장치의 다양한 실시예들을 도시한다. 이들 도면에서, 다양한 단계 또는 동작이 하나 이상의 노드 또는 장치에 의해 수행되는 것으로 도시된다. 이들 도면에 도시된 노드들 및 장치들은 통신 네트워크에서 논리적 엔티티들을 나타낼 수 있고, 이런 네트워크의 노드 또는 장치의 메모리에 저장되고 프로세서 상에서 실행되는 소프트웨어(예로서, 컴퓨터 실행 가능 명령어들)의 형태로 구현될 수 있으며, 그러한 네트워크의 노드 또는 장치는 후술된 도 36a 또는 도 36b에 도시된 일반적인 아키텍처들 중 하나를 포함할 수 있다. 즉, 도 6 내지 도 35, 37 및 38에 도시된 방법은 네트워크 노드 또는 장치, 예로서 도 36c 또는 도 36d에 도시된 노드 또는 컴퓨터 시스템의 메모리에 저장된 소프트웨어(예로서, 컴퓨터 실행 가능 명령어들)의 형태로 구현될 수 있으며, 컴퓨터 실행 가능 명령어들은 노드 또는 장치의 프로세서에 의해 실행될 때 도면들에 도시된 단계들을 수행한다. 또한, 이들 도면들에 도시되는 임의의 송신 및 수신 단계들은 노드 또는 장치의 프로세서 및 그것이 실행하는 컴퓨터-실행가능 명령어들(예로서, 소프트웨어)의 제어 하에 노드 또는 장치의 통신 회로(예로서, 도 36c 및 도 36d의 회로(34 또는 97)에 의해 수행될 수 있다는 것이 이해된다.

[0038] 예로서 사용자 장비(UE; User Equipment) 또는 서버 상에 호스팅된 다른 애플리케이션들과 함께 소프트웨어로 구현될 수 있고 엔티티 상에 존재할 수 있는 예시적인 기능들이 아래에서 설명된다. 이러한 기능들은 전용 하드웨어 엔티티들에 존재할 수 있으므로 이 문서 전체에서 용어, 기능, 엔티티, 장치 및 노드는 제한없이 상호 교환하여 사용할 수 있다. 예로서, 클라이언트는 사용자 디바이스에 존재하는 애플리케이션 또는 서비스일 수 있다. 클라이언트는 머신 상의 애플리케이션 또는 서비스, 전용 하드웨어 또는 클라우드 기반 애플리케이션 또는 서비스를 지칭할 수도 있다. 클라이언트는 플랫폼 내에서 또는 다른 플랫폼들에서 분산 방식으로 함께 작동하는 애플리케이션들 또는 서비스들의 그룹의 일부일 수도 있다. 클라이언트는 일반적으로 콘텐츠에 액세스하기 위해 요청을 개시한다. 클라이언트가 콘텐츠에 액세스하기 위해 요청을 송신하는 트리거는 사용자, 머신, 애플리케이션 또는 서비스에 의해 개시될 수 있다.

[0039] 도 6을 참조하면, CCSDF(Content Creation and Security Determination Function)는 다수의 기능들로 구성될 수 있고, 동일한 엔티티(노드) 상에 호스팅되거나 상이한 관리 도메인들 상에 존재할 수도 있는 엔티티들(다수의 노드들)에 걸쳐 분산될 수 있다. 기능들이 다른 관리 도메인들 내에 존재하면, 트랜잭션들을 수행하기 위해 기능들이 있는 다양한 엔티티들간에 신뢰 관계가 있을 수 있다. CCSDF는 콘텐츠를 생성하거나 데이터 소스들(예로서, 센서들)를 사용하여 콘텐츠를 생성하는 엔티티일 수 있다. 일부 경우에, CCSDF와 SCHF는 동일한 물리적 엔티티(예를 들어, 서버, 게이트웨이)에서 공동 호스팅될 수 있다. 일 실시예에서, 콘텐츠 생성 기능(CCF; Content Creation Function)은 다양한 소스들(예로서, 센서들, 애플리케이션들, 데이터 베이스들 등)로부터 데이터를 수집하고 콘텐츠를 생성하는 것에 연루된다. 데이터는 센서(들) 및 애플리케이션들에 의해 사전 수집되거나 공개될 수 있다. CCF는 콘텐츠 생성에 연루된 프로세스들을 관리한다. 보안 결정 기능(SDF; Security Determination Function)은 콘텐츠와 관련된 보안 요구 사항들을 결정하는 것을 담당할 수 있다. SDF는 콘텐츠를 보호하기 위해 필요한 보안 수준을 결정할 수 있다. 본 개시내용에서, 콘텐츠가 "휴지 상태"일 때 콘텐츠와 관련된 보안 요구 사항들이 결정된다. 즉, 저장에 관한 보안 요구 사항들 및 콘텐츠 보안 관리가 여기에 설명되어 있다. 전술한 바와 같이, CCF 및 SDF는 동일한 노드/엔티티에서 수행될 수 있거나, 기능들은 상이한 노드들/엔티티들 상에 존재할 수 있다.

[0040] 보안 콘텐츠 호스팅 기능(SCHF; Secure Content Hosting Function)이 콘텐츠를 호스팅할 수 있다. 또한 SCHF는 보안 정책 시행 엔티티로 기능하고 액세스 제어 검사들을 수행할 수 있다. 일부 경우에, SCHF는 콘텐츠와 관련된 보안 동작들(예를 들어, 보안 정책 시행)을 수행하는 데 필요한 능력들(예를 들어, 기능성, 컴퓨팅 리소스들)을 가져야 하며, 또한, 보안 방식으로 콘텐츠를 호스팅하는 리소스들을 가져야한다. 보안 인에이블링 기능(SEF; Security Enabling Function)은 콘텐츠 보호 및/또는 액세스를 위한 자격증명을 제공할 수 있다. SEF는 클라이언트(들)에게 콘텐츠에 대한 액세스를 제공하기 위해 신뢰할 수 있는 제3 기관(TTP)과 같은 신뢰할 수 있는 중개자로 작용할 수 있다. SEF는 대칭 자격증명과 공개 키 자격증명을 프로비저닝할 수 있다. 또한 이는

외부 인증 기관(CA; Certificate Authority)과 기능 또는 인터페이스할 수 있다.

[0041] 도 6에 도시된 바와 같이, 콘텐츠 보안 제공에 연루된 프로세스는 이하에서 식별되는 다양한 프로세스로 분류될 수 있다. 예로서, CCP(Content Creation Process)의 일부로 콘텐츠의 하위 컴포넌트들은 특정 관계와 구조가 있는 조합된 콘텐츠를 만드는 데 사용된다. 예시적인 콘텐츠는 하나 이상의 속성/값 쌍들로 구성될 수 있으며, 각 속성/값 쌍은 하위 컴포넌트이다. 보안 파라미터 결정 프로세스(SPDP; Security Parameters Determination Process)의 일부로 "휴지 상태"의 특정 콘텐츠에 대해 올바른 보안 파라미터 세트가 결정된다. 또한 콘텐츠의 라이프 사이클 관리도 결정된다. 보안 호스팅 요청 프로세스(SHRP; Secure Hosting Requisition Process)는 CCSDF 또는 SCHF에 의해 개시될 수 있다. 일 예에서, 요청의 일부로 CCSDF는 SCHF에서 콘텐츠의 보안 호스팅을 요청한다. SCHF는 제로 홉(동일한 플랫폼에서 호스팅됨), CCSDF로부터 한 홉(일반적으로 선호되는 접근법) 또는 다수 홉(2개 이상의 홉들만큼 떨어짐) 떨어져 있을 수 있다. CCF, SDF 및 SCHF가 동일한 노드/엔티티에서 구현되는 예에서, 단계 0, 1 및 2는 노드/엔티티 내에서 내부적으로 수행될 수 있고, 따라서 기능들 사이의 통신이 인트라-프로세스 통신을 사용하여 수행될 수 있다.

[0042] 예시적인 실시예에서, CRRP(Credential Requisition & Registration Process)는 CRP(Credential Requisition Process) 및 CGP(Credential Registration Process)를 포함할 수 있다. CRP 동안 SCHF는 콘텐츠의 보안 저장을 위한 적절한 자격증명의 프로비저닝을 요청할 수 있다. 다수의 경우에서 SCHF가 해당 콘텐츠에 대한 적절한 자격증명을 생성하기에 충분할 수 있기 때문에 이 프로세스는 선택적일 수 있다. 클라이언트 특정 콘텐츠가 보호되어야 하는 경우, 이때, CCSDF/SDP는 클라이언트의 자격증명을 요청할 수 있다. CGP의 일부로서 콘텐츠 보호에 사용되는 자격증명의 세트가 SEF와 함께 공개될 수 있다. 확장성을 이유로 자격증명이 여러 SEF들에서 공개될 수 있다. 일부 경우에 CCSDF가 자체적으로 자격증명을 생성할 수 있으면, 이때, CCSDF는 CGP만 수행할 수 있다. 그러나 다른 경우 CCSDF가 적절한 자격증명을 생성할 수 없는 경우, 이때, 이는 완전한 CRRP 프로세스들을 수행해야 한다. 예시적 SHP(Secure Hosting Process)의 일부로서, SCHF는 CCSDF로부터의 SHRP 메시지를 기반으로 콘텐츠 호스팅을 수행할 수 있다. 여기서 가정은 CCSDF가 필요한 암호화 동작들을 수행하여 콘텐츠가 보호되고 CCSDF의 명령어들에 기초하여, SCHF가 콘텐츠를 적절하게 호스팅한다는 것이다. 대안적으로, SCHF는 콘텐츠를 보안 호스팅하기 위해 적절한 암호화 동작들을 수행해야 할 수도 있다. 수행되는 암호화 동작의 유형은 콘텐츠와 관련된 보안 파라미터들에 기초할 수 있다. SHRP 메시지를 기반으로 SCHF는 콘텐츠와 관련된 보안 특성들을 업데이트하고 선택적으로 콘텐츠를 삭제하거나 액세스할 수 없게 하기 위해 트리거되어야 하는 적절한 라이프 사이클 관리 프로세스들을 생성할 수 있다.

[0043] 이제, 제3 기관(예로서, 클라이언트)이 리소스에 액세스할 수 있도록 하기 위한 제3 기관 자격증명 요청 프로세스(TPCRP; Third-Party Credential Requisition Process)로 돌아가서 SEF는 클라이언트를 인증하고 필요한 자격증명을 제공해야만 클라이언트가 콘텐츠를 해독 및/또는 콘텐츠의 무결성/신뢰성을 확인할 수 있을 수 있다. TPCRP는 인증 및 허가뿐만 아니라 제3 기관(예를 들어, 클라이언트)에 대한 자격증명 배포를 수반할 수 있다. 예시적인 콘텐츠 검색 프로세스(CRP; Content Retrieval Process) 동안, 클라이언트는 콘텐츠에 대한 액세스 요청을 개시한다. 클라이언트는 사전 구성된 정보로부터 SCHF에 관한 정보를 얻을 수 있거나 정보가 DNS-SD 또는 RD를 사용하여 동적으로 발견될 수 있다. 일 예의 CP(Content Processing) 동안, 콘텐츠에 액세스하기를 원하는 클라이언트는 콘텐츠의 신뢰성 및/또는 무결성을 확인하고자 할 수 있다. 또한 클라이언트는 콘텐츠와 관련된 콘텐츠 구조 및 속성들을 확인하고자 할 수 있다. 콘텐츠가 기밀성을 위해 보호되는 경우 콘텐츠는 암호화된 콘텐츠로서 송신될 수 있으며 콘텐츠는 SCHF에 의해 클라이언트에게 콘텐츠를 송신하기 전에 해독될 수 있다. 콘텐츠가 SCHF에 의해 해독되어야 하는지 여부의 결정은 콘텐츠와 관련된 정책 및 보안 요구 사항들에 기반할 수 있다.

[0044] 예시적 CLMP(Content Life-cycle Management Process)의 일부로서, CCSDF는 선택적으로 명시적인 CLMP 메시지를 송신하여 특정 콘텐츠의 라이프 사이클 관리를 업데이트할 수 있다. CCSDF가 명시적 라이프 사이클 관리 요구 사항들을 SHRP의 일부로 통신한 경우 이 프로세스/메시징을 생략할 수 있다. 또한 SCHF의 로컬 정책들이 콘텐츠의 라이프 사이클 관리를 다루도록 미리 구성되어 있는 경우 이는 생략될 수도 있다. SCHF의 정책들은 콘텐츠와 관련된 보안 특성들을 업데이트, 예컨대, 콘텐츠를 삭제하거나 콘텐츠를 임의의 엔티티가 사용할 수 없게 하기 위해 수행해야 하는 필요한 동작들을 결정할 수 있다.

[0045] 이제 CCP(Content Creation Process)에 대해 상세히 설명한다. 이 프로세스의 일부로서, 데이터 수집기에 의해 수집된 원시 데이터(예로서, 센서 데이터)가 특정 구조에 저장될 콘텐츠를 생성하기 위해 CCF에 의해 사용될 수 있다. CCP의 일부로서, 예시적인 실시예에 따라, 콘텐츠의 하위 컴포넌트들은 특정 관계 및 구조를 갖는 조합된 콘텐츠를 생성하는데 사용된다. 예시적인 콘텐츠는 하나 이상의 속성/값 쌍들로 구성될 수 있으며, 각 속성

/값 쌍은 하위 컴포넌트이다. 전술한 바와 같이, 편의상, 데이터 또는 정보 또는 콘텐츠는 일반적으로 제한없이 콘텐츠로서 언급될 수 있다. 콘텐츠는 전역적 URI(globally Unique Resource Identifier)에 의해 식별될 수 있거나 로컬적으로 식별가능할 수 있다. 콘텐츠는 하위 컴포넌트 사이에 특정 관계 구조(예를 들어, 계층적 또는 평면적 웹)가 있는 하나 이상의 하위 콘텐츠(들)(컴포넌트들)로 구성될 수 있다. 하위 컴포넌트 또는 속성들을 갖는 콘텐츠의 일 예가 도 7에 도시되어 있다. 도 7은 콘텐츠 식별자 "ABC"를 가지며, 3개의 컴포넌트, 즉 컴포넌트-A, 컴포넌트-B 및 컴포넌트-C로 이루어진 콘텐츠를 도시한다. 컴포넌트-C는 다시 두 개의 하위 컴포넌트로 구성된다; 하위 컴포넌트-X, 하위 컴포넌트-Y.

[0046] 이제 보안 파라미터 결정 프로세스(SPDP; Security Parameters Determination Process)로 돌아가면, 예시적인 실시예에 따라, SDPD 동안, CSSDF의 일부일 수 있는 SDF는 "휴지 상태"에서 콘텐츠를 보호하기 위해 필요한 적절한 보안 요구 사항들 및 파라미터들을 결정한다. 전술한 바와 같이, CCSDF가 자체적으로 자격증명을 생성할 수 있는 일부 경우에, 이때, CCSDF는 CGP만 수행할 수 있다. 대안적으로, CCSDF가 적절한 자격증명을 생성할 수 없는 경우, 이때 이는 완전한 CRRP 프로세스들 모두를 수행해야 할 수 있다. 결정 프로세스의 일부로서, 제한적이지 않은 예로서, CCSDF는 다음을 결정할 수 있다:

[0047] * 콘텐츠를 도청자들로부터 보호해야 하는지 여부(기밀성/개인 정보 보호)

[0048] o 보호 수준: 알고리즘 강도, 자격증명 유형/크기

[0049] * 콘텐츠의 비허가 수정으로부터 보호-무결성 보호

[0050] o 보호 수준: 알고리즘 강도, 다이제스트/서명 길이

[0051] * 보호 메커니즘을 업데이트할 수 있는 능력

[0052] * 자격증명의 보안 저장/보안 운영 환경의 요구 사항들

[0053] * 콘텐츠와 관련된 라이프타임 보안 관리

표 1

표 1: 높은 수준의 보안 요구 사항들 및 콘텐츠와 관련된 파라미터들의 예

[0054]

Content Id/서브	기밀성 보호		무결성 보호		보안 환경	라이프 사이클/보안 보호 업데이트
	알고리즘 강도	자격증명 강도	알고리즘 강도	인증 코드/서명 길이		
XYZ / 아니오	높음	> 200 비트	중간	MAC >= 256	아니오	10 년/3 년
ABC/예	높음	> 200 비트	높음	DS >= 4096	예	5 년/1 년
MNO / 아니오	낮음	> 120 비트	중간	MAC >= 256	아니오	15 년/아니오

[0055] 위의 표 1에는 콘텐츠 XYZ(XYZ-Id로 식별됨), ABC 및 MNO와 관련된 높은 수준의 보안 파라미터들의 예가 예시되어 있다. 각 콘텐츠는 그 대응하는 보안 파라미터들과 연관된다. 일 예로서, 도시된 바와 같이, 콘텐츠 XYZ는 기밀성 요구 사항 "높음"을 가지며, 사용된 키 크기가 적어도 200 비트가 되도록 요구한다. 자격증명 강도는 암호화의 유형(예로서, 대칭 키)에 기초할 수 있고, 따라서 다른 암호화 유형들(예컨대, 공개 키)에 대한 등가의 키 크기가 적절하게 사용될 수 있다. 일부 경우에 제한된 엔티티들에서 콘텐츠를 호스팅할 수 있다는 점을 감안하여 자격증명 강도에 대한 최대 크기 한계가 존재할 수 있다. 도시된 바와 같이, 예시적인 무결성 보호 알고리즘은 "중간"이고 256 비트 이상의 MAC 길이를 갖는다. 콘텐츠는 보안 환경을 사용할 필요가 없다. 라이프 사이클 관리와 관련하여, 예시된 예에 따르면, 콘텐츠는 10 년 기간 후에 소거되거나 액세스가 불가능해질 수 있으며 보안 보호는 매 3 년마다 업데이트될 수 있다. 이 표는 단지 콘텐츠 보호를 위한 가능한 높은 수준의 보안 요구 사항들의 예를 보여준다. 특정 구현에 적합하도록 추가적인 요구 사항들이 추가되거나 제거될 수 있음을 이해할 것이다. 예로서 라이프 사이클 관리와 관련된 요구 사항들은 특정 유형의 콘텐츠에는 없을 수 있다.

[0056] SPDP는 예로서 CCF의 로컬 정책들 또는 콘텐츠 소유자/서비스 제공자가 프로비저닝한 정책들을 기반으로 하는

SDF의 프로세스에 의해 트리거될 수 있다. SPDP를 트리거하는 데 사용되는 메커니즘은 특정 콘텐츠에 대한 요청에 따라 사전 대응적이거나 반응적일 수 있다. SPDP는 국이 보안 의미 또는 상업적 가치가 있는 중요한 데이터/콘텐츠를 보호하기 위한 최상의 관례들에 기초하여 프로비저닝 또는 구현된 보안 특정 정책들을 사용하여 수행될 수 있다. SPDP에서 사용되는 정책들의 단순화된 예가 아래 표 2에 나와 있지만 정책은 필요에 따라 달라질 수 있다.

표 2

표 2: SPDP를 위한 예시적 정책들

[0057]

보안 값	기밀성	무결성	보안 환경	라이프 사이클 관리
낮음	낮음	중간	아니오	아니오
중간	중간	높음	아니오	예
높음	높음	높음	예	예

[0058] 일부 경우에 콘텐츠가 하위 컴포넌트들로 구성될 수 있으며 각 하위 컴포넌트는 고유한 아이덴티티를 갖거나 콘텐츠와 관련된 속성들/값들이 있을 수 있다. 각 하위 컴포넌트 또는 속성/값은 대응하는 그 자체의 보안 요구사항을 가질 수 있다. 모든 하위 컴포넌트(예를 들어, 속성들/값들)가 개별적으로 보호되기 때문에 이때 전체 콘텐츠가 보호될 수 있다(예를 들어, 무결성 보호).

[0059] 예시적인 실시예에서, SDF는 요구 사항들에 기초하여 적절한 암호화 파라미터들(CryptoParams)을 결정한다. CSSDF가 콘텐츠를 호스팅하면 CCSDF는 콘텐츠에 대해 필요한 보안 값(들)을 도출할 수 있다. 콘텐츠 XYZ와 연관된 CryptoParams의 예가 도 8에 도시되어 있다. 도 8은 암호화/복호화 알고리즘을 기술한다: AES는 256 비트 키를 사용한다. 이 키는 키 유도 기능(KDF; Key Derivation Function)을 사용하여 생성될 수 있다. 예시적 KDF는 다음의 형태일 수 있다: 기밀성 키(CK) = KDF (KeyGenKey, "ContentId" || "RandomValue"||"ConfidentialityKeyGen").

[0060] 예로서, 키-해시-메시지-인증-코드(HMAC-SHA)와 같은 KDF가 CK를 유도하는데 사용될 수 있다. 입력 파라미터들은 본 명세서에서 KeyGenKey로 지칭될 수 있는 다른 키들을 생성하기 위해 CSSDF에 의해 사용되는 키를 수반할 수 있다. 또한, 입력 파라미터들은 CCSDF의 컨텍스트 내에서 고유한 것으로 가정할 수 있는 ContentId, SDF에서 생성한 무작위 값 및 스트링 "ConfidentialityKeyGen"을 포함할 수 있다. 전술한 바와 같이, CK의 생성은 설명의 목적으로 단지 예로서 사용되며, 입력 파라미터들은 충돌 가능성 감소를 위해 필요에 따라 변경될 수 있음을 이해할 것이다.

[0061] 여전히 도 8을 참조하면, 선택된 무결성/인증 알고리즘은 연관된 무결성 키(IK)를 갖는 HMAC-SHA-256 알고리즘이다. IK는 CK와 유사한 수단을 사용하지만 입력 파라미터의 변형들을 동반하여 도출될 수 있다. 예로서 새로운 RandomValue가 생성되고 "ConfidentialtiyKeyGen"은 "IntegrityKeyGen" 스트링으로 대체될 수 있다.

[0062] 예시적인 실시예에서, 특정 클라이언트 만이 콘텐츠에 액세스할 수 있도록 콘텐츠가 보호된다. 또한 클라이언트는 특정 SDF가 콘텐츠를 생성했음을 확인할 수 있으며 매우 높은 수준의 보증으로 임의의 다른 엔티티에 의해 수정되지 않았음을 확인할 수 있다. 예로서, 클라이언트 특정 콘텐츠 보호 메커니즘이 사용될 때 클라이언트의 공개 키를 얻기 위해 클라이언트의 디지털 인증서를 사용하고 공개 키를 사용하여 콘텐츠를 암호화하는 것이 바람직할 수 있다. 클라이언트 특정 CryptoParams의 예가 도 9에 도시되어 있다. 도시된 바와 같이, 기밀성 알고리즘은 RSA(Rivest-Shamir-Addleman) 공개 키 알고리즘으로 결정되고, 키는 클라이언트 1의 공개 키로 결정되며, 이는 클라이언트 1과 연관된 디지털 인증서로부터 획득될 수 있다. 예로서, SDF가 이미 디지털 인증서를 가지고 있지 않은 경우, 클라이언트 1의 디지털 인증서를 얻기 위해 아래에 설명된 자격증명 요청 프로세스가 수행될 수 있다. 이 예에 따르면, 무결성(디지털 서명) 알고리즘은 SHA-256 다이제스트를 사용하는 RSA로 결정되며, 사용되는 서명 키(IK)는 SDF의 디지털 인증서와 관련된 SDF의 개인 키이고, 이는 바람직하게는 보안 저장소에 저장된다. CryptoParams가 생성된 시간/날짜, ContentId 및/또는 콘텐츠와 관련된 메타데이터와 같은 난스가 난스로서 사용될 수 있다.

[0063] 예시적인 시나리오에서 클라이언트는 자격증명 세트를 공유하는 클라이언트 그룹일 수 있다. 이러한 시나리오들에서는 기밀성을 위한 공개 키잉 메커니즘을 사용하는 것은 각 엔티티가 개인 키를 공유해야 할 수 있어 보안

성을 약화시키므로 양호하게 동작하지 않을 수 있다. 대신에 대칭 키 메커니즘이 이 시나리오에서 기밀성을 위해 사용되는 것이 바람직하다. 대안적으로, 무결성/인증을 위해 공개 키잉 메커니즘이 선호되는 접근법일 수 있다. 따라서, 확장성 및 최적의 성능을 유지하기 위해, 기밀성 알고리즘은 대칭 키잉 메커니즘에 기초할 수 있고, 공개 키잉 메커니즘은 일 실시예에 따라 콘텐츠/콘텐츠 생성기의 무결성/신뢰성을 제공하는데 사용될 수 있다. 일부 경우에 콘텐츠의 기밀성은 무시될 수 있지만 콘텐츠/콘텐츠 생성기의 무결성/신뢰성은 확인된다.

[0064] 예로서, 콘텐츠가 하위 컴포넌트들로 구성되는 경우, 각각의 하위 컴포넌트는 그 자체의 보안 파라미터들 및 그와 연관된 대응하는 CryptoParams를 가질 수 있다. 예로서, 속성/값 쌍들로 구성될 수 있는 콘텐츠 및 하위 컴포넌트들은 그 자체의 고유한 CryptoParams를 가질 수 있다. 각 특정 속성/값 쌍을 보호하는 데 필요한 컴퓨팅 리소스의 양은 많은 비용이 소요될 수 있으며, 많은 경우 그 개별 컴포넌트를 개별적으로 보호하지 않고 전체로서 컴포넌트가 보호될 수 있다. 본 명세서에서 설명된 메커니즘들은 글로벌 콘텐츠 관점 또는 더 세분화된 속성/값 쌍 관점으로부터 콘텐츠의 보호를 수행하는데 사용될 수 있으며, 여기서 콘텐츠와 관련된 각각의 하위 컴포넌트들은 가변적인 보안 요구 사항들을 가질 수 있다. cryptoParams는 알고리즘들 및 키들에 대해 JWA 및 JWK를 통해 JSON 표기법을 사용하여 표현될 수 있음을 알 수 있다.

[0065] 이제, 예시적 SHRP(Secure Hosting Requisition Process)로 돌아가서 SCHF는 CCSDF와 동일한 엔티티(노드)에 위치할 수 있으며, 따라서, SHRP 메시징은 이러한 경우 내부적으로 수행될 수 있다. CCSDF와 SCHF가 서로 다른 엔티티들에 위치하는 일부 경우에, CCSDF는 하나 이상의 SCHF들로 SHRP를 개시할 수 있다. 단일 SCHF를 갖는 콘텐츠의 호스팅이 여기에 설명되어 있지만 유사한 메커니즘이 여러 SCHF들을 사용한 호스팅에 사용될 수 있다. SHRP는 다음과 같은 하위 프로세스들, 예로서, 보안 값(들) 계산, 적절한 SCHF 발견 및 메시징 프로세스로 구성될 수 있으나, 이에 한정되지는 않는다.

[0066] 컴퓨팅 보안 값들에 관하여 필요한 보안 값들은 위에서 설명한 SPDP의 일부로 결정된 SDF 및/또는 CryptoParams의 로컬 정책을 기반으로 계산할 수 있다. 특정 경우들에서, 보안 값들의 계산은 TTP(Trusted Third Party) 또는 SCHF로 오프로드될 수 있다. SDF를 호스팅하는 엔티티의 로컬 정책들은 SDF를 호스팅하는 엔티티의 서비스 공급자 정책들, 능력들(예를 들어, 제약된 디바이스, 올바른 펌웨어/소프트웨어의 가용성 등)과 콘텐츠 유형의 조합을 기반으로 할 수 있다. 여기에서 보호된 값(PV; Protected Values)이라는 용어는 계산된 보안 값들을 나타내는 데 사용된다. 계산된 PV의 예로는 암호화된 콘텐츠(EC; Encrypted Content)와 인증 태그(AT; Authentication Tag)가 있다. EC와 관련하여, 전체 콘텐츠가 암호화될 수 있거나, 하위 컴포넌트들 또는 속성/값 쌍들이 각각의 하위 컴포넌트와 연관된 CryptoParams에 기초하여 암호화될 수 있다. 일부 경우에, 속성/값 쌍들의 "값" 컴포넌트만 암호화된다. AT는 특정 내용에 대한 CryptoParams에 지정된 무결성 파라미터들을 사용하여 콘텐츠에서 계산된 무결성 값이다. 앞에서 언급한 바와 같이, 콘텐츠의 각 하위 컴포넌트에는 그 자체의 고유한 계산된 AT가 있을 수 있다.

[0067] 예시적인 실시예에서, EC 및 AT 모두는 AES-갈로아 모드(AES-GCM; AES-Galois Mode)와 같은 AEAD(Authenticated Encryption with Associated Data) 메커니즘을 사용함으로써 달성된다. AEAD의 사용은 CryptoParams 내에서 명시적으로 지정되거나 SCHF에 의해 추론될 수 있다. EC와 AT는 별도의 CK, IK를 사용하거나 무결성 및 기밀성 모두를 위해 단일 키를 구비하여 생성될 수 있다. 또한, AES-GCM의 경우, AT는 "추가 인증 데이터"일 수 있다. EC와 AT는 각각 JWE와 JWS를 통해 JSON 표기법을 사용하여 표현될 수 있다.

[0068] 예시적인 실시예에서, CCSDF는 그 콘텐츠를 호스팅하기 위한 정확한 SCHF를 결정하기 위해 발견 프로세스를 수행할 수 있다. 발견 프로세스에는 신뢰할 수 있는 엔티티 또는 사용 가능한 서비스들(예를 들어, DNS-SD, RD)의 능동적 목록화를 수행하는 다른 엔티티에 쿼리하는 것을 수반할 수 있다. 일부 경우에 CCSDF는 발견 프로세스를 로컬 호스팅 엔티티로 오프로드하여 로컬 호스팅 엔티티가 적절한 SCHF를 결정할 수 있다. 쿼리에 대한 응답으로서, CCSDF는 보안 파라미터들에 가장 적합한 특정 기준에 기초하여 주문된 SCHF의 목록 또는 SCHF에 관한 위치 정보(예로서, URI)를 제공받을 수 있다. 신뢰성이 높은 SCHF를 사용할 수 없는 경우, 이때, PV들의 계산과 연루된 암호화 동작들은 CCSDF에 의해 수행될 수 있다. 신뢰할 수 있는 SCHF가 발견되면 PV들의 계산이 SCHF로 오프로드될 수 있다.

[0069] 이제 도 10을 참조하면, 네트워크(1000)는 일례에 따라 CCSDF(1002) 및 CCSDF(1002)와 함께 보안 호스팅 요구(SHR) 메시징을 수행하는 SCHF(1004)를 포함한다. 예시적인 네트워크(1000)는 개시된 주제에 대한 설명을 용이하게 하기 위해 단순화되어 있고, 본 개시내용의 범위를 제한하고자 의도하는 것은 아님을 알 수 있을 것이다. 본 명세서에 설명된 실시예들을 구현하기 위해 네트워크(1000) 같은 네트워크에 추가로 또는 그 대신에 다른 디

바이스들, 시스템들 및 구성들이 사용될 수 있으며, 모든 이런 실시예들은 본 개시내용의 범위 내에 있는 것으로서 고려된다. CCSDF(1002)에 의해 수신된 응답의 유형에 기초하여, SCHF(1004) 상에 콘텐츠가 호스팅되기 위해 요구될 수 있는 정확한 파라미터들의 세트의 생성 및 적절한 메시지를 생성할 수 있다. SCHF가 신뢰도가 낮은 엔티티이면, 도 10에 도시된 메시지가 수행될 수 있다.

[0070] 0에서, 도시된 실시예에 따라, CCSDF(1002)는 콘텐츠의 적절한 PV들을 생성한다: EC(들) 및 연관된 AT(들). 1에서, CCSDF(1002) 및 선택된 SCHF(1004)는 서로를 상호 인증하고 보안 통신 채널을 확립할 수 있다. 2에서, CCSDF(1002)는 EC(들), 연관된 AT(들) 및 CryptoParams를 포함하는 보안 호스팅(SH) 요청 메시지를 SCHF(1004)로 송신한다. 3에서, 도시된 예에 따라, SCHF(1004)는 EC(들), AT(들), 및 CryptoParams를 호스팅하고 이들을 보호 콘텐츠 저장소(PCS; Protected Content Store) 내에 저장한다. SCHF(1004)는 ContentId와 함께 선택적으로 CryptoParams를 SEF에 포스팅할 수 있으며, 이에 대해서는 이하에서 설명한다. 4에서, EC 및 PV들이 호스팅되고 나면, AT 및 CryptoParams뿐만 아니라 EC의 위치에 대한 URI일 수 있는 선택적으로 고유한 호스트-id(H-Id)를 포함하는 성공 메시지가 CCSDF(1002)에 송신된다. EC는 하나의 물리적 엔티티에서 호스팅될 수 있으며 CryptoParams와 AT들은 상이한 신뢰할 수 있는 엔티티들에 있을 수 있다.

[0071] 이제 도 11을 참조하면, 네트워크(1100)는 신뢰할 수 있는 엔티티인 CCSDF(1102) 및 SCHF(1004)를 포함하여, CCSDF(1102)는 신뢰할 수 있는 SCHF(1104)에 의존하여 도시된 바와 같이 그 대신 암호화 동작들을 수행할 수 있다. 이 예에 따라, CCSDF(1102)는 단지 SCHF(1104)에 콘텐츠 및 연관된 CryptoParams를 제공한다. 0에서, 도시된 예에 따라, CCSDF(1102)와 SCHF(1104)는 서로를 상호 인증하고 서로 보안 통신 채널을 확립할 수 있다. 1에서, CCSDF(1102)는 연관된 CryptoParams와 함께 콘텐츠(보호되지 않음)를 포함하는 SH 요청 메시지를 송신한다. 또한 하위 컴포넌트가 개별적으로 무결성 보호되어야 함을 나타내는 Sub_I-플래그도 송신된다. SCHF(1104)가 신뢰되고 또한 메시지가 보안 통신 채널을 통해 송신되기 때문에, 콘텐츠 및 파라미터들은 '전송 중에(in transit)' 보호된다. SCHF(1104)가 CCSDF(1102)로부터 약간의 홉 거리에 위치하고, 메시징 페이로드가 신뢰되지 않은 엔티티들을 통과하는 경우, 콘텐츠 및 CryptoParams은 종단간 보안 메커니즘을 사용하여 보호되어야 한다. 2에서, SCHF(1104)는 EC(들) 및 연관된 AT(들)을 유도하기 위해 콘텐츠에 대해 CryptoParams를 사용한다. Sub_I-flag=1이므로, 각 콘텐츠의 개별 하위 컴포넌트들 또한 무결성 보호되고 적절한 AT 값들이 계산된다. SCHF(1104)는 사용되어야 하는 자격증명의 올바른 세트를 얻기 위해 SEF의 서비스들을 사용할 수 있다. 이는 보호 대상 콘텐츠가 클라이언트 특정 콘텐츠인 경우 특히 필요하다. SCHF(1104)는 EC(들) 및 AT(들)를 그에 저장할 수 있다. 예시적 보안 호스팅 프로세스의 세부 사항은 아래에 설명되어 있다. 3에서, SCHF(1104)는 "성공"을 포함하는 SH 응답을 CCSDF(1102)에 송신한다. SCHF(1104)는 마찬가지로 호스팅 식별자를 선택적으로 송신할 수 있다.

[0072] 따라서, 도 10 및 도 11을 참조하면, 노드(예로서, CCSDF)는 프로세서, 메모리 및 통신 회로를 포함할 수 있다. 노드는 그 통신 회로를 통해 네트워크에 접속될 수 있고, 노드는 노드의 프로세서에 의해 실행될 때, 노드가 하나 이상의 보안 요구 사항들에 기초하여 하나 이상의 암호 파라미터를 결정하게 하는 노드의 메모리에 저장된 컴퓨터 실행 가능 명령어들을 더 포함한다. 또한 노드는 보안 호스팅 요청 메시지를 콘텐츠 호스팅 기능(CHF)에 송신할 수 있다. 보안 호스팅 요청 메시지는 콘텐츠 호스팅 기능이 하나 이상의 암호 파라미터들을 사용하여 콘텐츠를 안전하게 저장할 수 있도록 하나 이상의 암호 파라미터들 및 그와 관련된 콘텐츠를 포함할 수 있다. 하나 이상의 암호 파라미터들에 기초하여, 노드는 콘텐츠가 기밀화되도록 콘텐츠를 암호화할 수 있다. 대안적으로, 콘텐츠는 하위 컴포넌트들로 이루어질 수 있고, 노드는 하나 이상의 암호 파라미터들에 기초하여 각 하위 컴포넌트가 기밀화되도록 하위 컴포넌트들 각각을 암호화할 수 있다. 대안적으로, 콘텐츠는 속성들과 값들의 쌍들로 구성될 수 있고, 노드는 하나 이상의 암호 파라미터들에 기초하여, 각각의 값이 기밀화되도록 값들 각각을 암호화할 수 있다. 노드는 또한 콘텐츠가 무결성 보호되도록 콘텐츠와 연관된 인증 태그(AT)를 계산할 수 있다. 대안적으로, 또는 추가적으로, 콘텐츠는 하위 컴포넌트들로 이루어질 수 있고, 노드는 하위 컴포넌트들 각각이 무결성 보호되도록 각각의 하위 컴포넌트들과 연관된 각각의 인증 태그들을 계산할 수 있다.

[0073] 콘텐츠가 로컬 또는 프록시상에서 호스팅될 수 있는지를 결정하기 위해 CCSDF에 의해 수행될 수 있는 예시적인 메커니즘이 도 12에 도시되어 있다. 도 12를 참조하면, 도시된 예에 따라, 1에서, CCSDF는 콘텐츠와 관련된 보안 요구 사항들의 평가를 수행한다. 보안 요구 사항은 콘텐츠를 생성한 엔티티 또는 도메인 외부로 콘텐츠가 반출될 수 없게 하는 것을 요구할 수 있다. 또한 콘텐츠를 호스팅할 수 있는 지리적 위치에 대한 제한(예로서, 다른 주, 주, 국가 등의 콘텐츠 저장 제한)이 있을 수 있다. 특정 보안 기능들을 수행하는 효율성 및 능력과 같은 다른 보안 평가들도 수행될 수 있다. 2에서 CCSDF는 콘텐츠가 프록시에서 호스팅될 수 있는지 평가한다. 3에서 콘텐츠가 프록시에서 호스팅될 수 있는 경우 CCSDF는 콘텐츠를 호스팅할 수 있는 잠재적인 하나 이상의

SCHF 목록을 얻을 수 있다. CCSDF는 특정 우선 순위로 순서화된 잠재적인 SCHF 목록으로 구성되었거나 TTP에서 목록을 얻을 수 있다. 일부 경우에 CCSDF는 발견 서비스 수단(예로서, DNS-SD 또는 oneM2M 발견 서비스)을 사용하여보다 동적인 방식으로 SCHF를 발견할 수 있다. 4에서, CCSDF는 SCFH(들)이 콘텐츠의 요구 사항들을 충족시키거나 초과하는지를 결정한다. 도 5에서, 도시된 예에 따라서, SCFH(들)가 콘텐츠 요구 사항들을 충족시키지 못하면 SDF는 콘텐츠가 CCSDF에서 로컬로 호스팅될 수 있는지를 결정한다. 6에서 콘텐츠를 로컬로 호스팅할 수 있으면 이는 SHP 프로세스를 트리거한다. 그렇지 않으면 CCSDF에 필요한 보안 능력들(애플리케이션, 소프트웨어, 펌웨어, 하드웨어 등)이 없는 경우 보안 호스팅 프로세스가 중단될 수 있다. 대안적으로, 새로운 발견 프로세스가 수행될 수 있거나, 보다 낮은 보안 요건을 갖는 수정된 콘텐츠가 업데이트된 발견 프로세스에 기반하여 호스팅될 수 있다.

[0074] 이제 보안 호스팅 프로세스(SHP)로 돌아가서, 예시적인 실시예에 따라, 콘텐츠는 보안 요구 사항 또는 콘텐츠와 관련된 보안 프로파일을 만족시키는 방식으로 처리된다. 보안 호스팅에는 데이터 액세스에 대한 강력한 인증 메커니즘을 제공하는 것, 강력한 허가 메커니즘을 제공하는 것, 데이터에 무결성을 제공하는 것 및/또는 데이터의 기밀성을 제공하는 것을 포함할 수 있다. 안전한 방식으로 데이터를 호스팅하는 능력은 보안 요소(SE) 또는 신뢰할 수 있는 실행 환경(TEE)의 사용을 수반할 수 있다. 일부 경우에 수반되는 오버헤드(컴퓨팅, 메모리, 배터리)가 제한된 디바이스에 대해 너무 많을 수 있다. SE 또는 TEE 내에서 암호화 자격증명(예로서, 키/인증서/아이덴티티들) 및/또는 민감한 암호화 기능들이 수행될 수 있다. 엔티티가 보안 방식으로 데이터를 호스팅할 수 없는 경우 해당 데이터를 저장하기 위해 프록시를 사용할 수 있다. RoT(Root-of-Trust)의 사용은 일반적으로 도움이되지만, 본 개시내용은 하드웨어 또는 소프트웨어 기반 RoT들의 존재에 대해 어떠한 가정도 하지 않는다.

[0075] 전술한 바와 같이, SCHF는 CCSDF로부터 1-홉 떨어져 있을 수 있거나, CCSDF로부터 다수 홉 떨어져있을 수도 있다. 홉 수는 서비스 레이어 홉들의 수를 나타낸다. CCSDF는 SCHF와 직접적인 신뢰 관계를 가질 수도 있고 가지지 않을 수도 있지만, 확립된 신뢰 계층관계를 기반으로 구축하거나 공통 신뢰 루트를 사용하여 새로운 신뢰 관계를 생성할 수 있다. 그러나 CCSDF와 SCHF 사이의 연결을 보호하기 위한 종단간(end-to-end) 접근 방법이 선호될 수 있지만 종단간 보안 메커니즘을 사용할 수 없고 홉-바이-홉 보안이 사용될 수 있다.

[0076] 예시적인 실시예에서, 엔티티는 데이터와 관련된 요구 사항들에 기초하여 엔티티가 호스팅되는 디바이스 내에 데이터를 로컬 저장하는 결정을 내릴 수 있다. 예로서, 호스트 엔티티가 보안 방식으로 데이터를 호스팅할 수 있다고 엔티티가 결정한 경우 데이터에 필요한 암호화 동작들을 수행하여 데이터가 무결성 보호 및/또는 기밀성 보호된다. 적절한 암호화 알고리즘 및 자격증명을 사용하여 데이터를 보호할 수 있다. 기밀성 보호를 위한 암호 값들의 예가 아래 표 3에 나와 있다.

표 3

표 3: 기밀성 보호를 위한 가능한 값들의 예

[0077]

보안 수준-기밀성	알고리즘	키 길이	저장 요구 사항들
낮음	3-DES	168 비트	없음
중간	AES	192 비트	FDE
높음	AES	256 비트	파일-기반
치명적	RSA	4096	TEE / SE*

[0078] PCS 내에 저장된 보호된 콘텐츠의 예가 도 13에 도시되어 있다. 도 13은 식별자를 갖는 콘텐츠를 나타낸다: 식별자 ABC는 A, B 및 C 구비하고, 컴포넌트 C는 하위 컴포넌트들(X 및 Y)로 이루어진다. CryptoParams와 보호해야 할 컴포넌트들의 표시에 따라 CCSDF는 콘텐츠와 관련된 EC 및 AT를 계산한다. 컴포넌트 A와 B는 고유할 수 있는 자격증명을 사용하여 암호화된다. 그러나 하위 컴포넌트인 X, Y는 암호화되지만 컴포넌트 C 자체는 데이터를 포함하지 않을 수 있으며 보호되지 않을 수 있다. 컴포넌트 A 및 B와 구조 및 전체 컴포넌트 C에 대한 무결성 데이터(AT)는 보호되며(컴포넌트-C-AT를 사용), 개별 하위 컴포넌트 X 및 Y가 보호된다. ABC-AT는 콘텐츠, "ABC" 및 하위 컴포넌트와 콘텐츠 내의 그 관계/구조를 무결성 보호하기 위해 계산된다.

[0079] 일부 경우에는 보호 메커니즘이 복잡하고 계산 비용이 많이 들며, 따라서 제한된 CCSDF에 적합하지 않을 수 있다. 따라서 일부 동작은 신뢰할 수 있는 SCHF로 오프로드될 수 있다. 여기에 설명된 세분화-수준에서 콘텐츠를 보호하기 위한 메커니즘은 강인한 보안 메커니즘을 제공하면서 콘텐츠 소비에 대한 많은 유연성을 제공한다.

콘텐츠의 하위 컴포넌트(예로서, 하위 컴포넌트-X)에 액세스할 수 있는 허가만을 갖는 클라이언트는 콘텐츠 그 전체에 대한 어떠한 정보도 없이 특정 하위 컴포넌트의 무결성을 확인할 수 있다(예로서, 컴포넌트-X-AT를 사용). CryptoParams의 선택 및 콘텐츠 보호의 세분성은 플랫폼에 의해 결정되는 CCSDF상의 로컬 정책들뿐만 아니라 구현되는 솔루션 유형(예로서, 서비스 제공자에 의해 결정됨)에 기초할 수 있다.

[0080] 다른 예시적인 실시예에서, CCDSF는 SCHF가 존재하는 프록시 상에 콘텐츠를 호스팅하기로 결정할 수 있다. 보안 프록시를 발견하는 데 전술한 발견 메커니즘이 사용될 수 있다. 소정 시나리오에서는 제한된 CCSDF가 CCSDF가 신뢰할 수 있는 프록시에 도달할 수 없기 때문에 완전히 신뢰할만한 프록시에 콘텐츠를 호스팅할 수 없다. 이러한 시나리오에서 CCSDF는 CryptoParams를 SCHF(프록시)에 제공하지 않을 수 있고 대신 TTP(예로서, SEF)에 저장된 CryptoParams에 대한 링크를 제공할 수 있다. 일 예에서, SEF는 적절한 허가를 가진 엔티티에만 CryptoParams를 제공한다. 그러나 프록시가 보안 SCHF인 경우 CryptoParams는 SCHF에서 보안 저장소에 위치될 수 있다. 콘텐츠를 보안 방식으로 저장하는 메커니즘은 위에서 설명한 절차들을 따를 수 있다.

[0081] CCSDF에 의해 신뢰도가 낮은 SCHF에 제공될 수 있는 예시적 CryptoParams가 도 14에 도시되어 있다. 자격증명은 제공되지 않지만 SEF에 등록된 Credential-Id가 제공될 수 있다. 엔티티는 엔티티가 허가된 후에만 SEF에서 자격증명을 얻을 수 있다. 따라서 EC를 호스팅하는 SCHF도 자격증명을 소유하지 않으므로 콘텐츠를 해독할 수 없으며 SEF와 함께 허가된 엔티티가 아닐 수도 있다.

[0082] 이제 CRRP(Credential Requisition and Registration Process)로 돌아가면 CRRP 프로세스는 SHRP와 SHP간에 인터리브될 수 있으며 CCSDF와 SEF 사이의 신뢰 관계 또는 CCSDF 또는 SCHF에서의 클라이언트 자격증명의 가용성에 기초하여 콘텐츠를 호스팅하는 데 사용되는 메커니즘에 의존할 수 있다. CRRP 프로세스는 보안 보호 프로세스를 수행하는 엔티티에 기반하여 CCSDF와 SEF 사이 또는 SCHF와 SEF 사이에서 수행될 수 있다. CRRP는 CRP(Credential Requisition Process) 및 CGP(Credential Regeneration Process)로 구성된다.

[0083] 예시적인 CRP와 관련하여, SDF가 호스팅되는 엔티티 내에서 로컬로(예컨대, 인증서, 키들) 자격증명을 생성 또는 획득할 수 없는 경우, SDF는 SEF로 CRP를 개시할 수 있다. 소정 시나리오에서 SDF는 물리적으로 그에 더 가까울 수 있는 TTP 엔티티로부터 자격증명을 얻을 수 있다. 일반적인 시나리오로서, SDF는 SEF와 신뢰 관계를 가지며, 이는 중앙 자격증명 리포지토리로도 기능할 수 있다고 가정된다. 도 15는 신뢰된 SEF를 갖는 CCSDF에 의해 개시되는 CRP를 도시하지만, 동일한 호 흐름이 또한 CHF와 SEF 사이의 CRP에 적용 가능할 수 있다.

[0084] 1에서, 도시된 예에 따라, 성공적인 인증 및 CCSDF와 SEF 사이의 보안 통신 채널의 확립(0에서) 후에, SEF는 CR(Credential Request) 메시지를 송신한다. 메시지에는 제한없이 예로서 제시된 다음 파라미터들이 포함될 수 있다.

[0085] * Content-Id[]: 콘텐츠 식별자들의 목록. 엔트리들의 수는 하나 이상일 수 있다.

[0086] * Algorithm_Strength[]: 각 콘텐츠에 대해, 대응하는 Algorithm_Strength. 이것은 선택적일 수 있으며, CCSDF는 그 자체의 강도에 기반하여 적절한 알고리즘을 선택할 수 있다.

[0087] * Credential_Type_Length_Lifetime[]: 각 콘텐츠에 대해, 대응하는 자격증명 유형, 길이 및 자격증명 유효 기간이 제공된다. 콘텐츠에 대한 Credential_Type는 "인증서"일 수 있으며 다른 콘텐츠에 대해 이는 "대칭 키"를 요청할 수 있다. "대칭 키"의 자격증명의 길이는 (예로서, 64/128/256 비트)일 수 있고, Credential_Type = "인증서"의 경우, 제공되는 자격증명의 길이는 사용된 알고리즘에 의존한다(예로서, RSA 공개 키는 2048/4096 비트일 수 있으며; ECC의 경우에는 224/256 비트일 수 있음). 라이프타임 값은 자격증명이 유효하고 유사한 CR 프로세스 또는 갱신 프로세스가 수행되어야 할 수 있는 기간이다. 자격증명의 라이프타임은 표 1에서 설명된 "보안 보호 업데이트" 값이다.

[0088] * Public_Key[]: 콘텐츠와 관련된 공개 키들의 목록이다. Credential_Type = "대칭 키"인 콘텐츠의 Public_Key 엔트리들은 비어있을 수 있다는 것에 유의해야 한다. Credential_Type가 "인증서"인 콘텐츠만이 예에 따라 대응하는 공개 키 엔트리가 존재한다.

[0089] * R-플래그: 이 플래그는 SEF에 이러한 자격증명을 등록하려고 함을 나타내기 위해 CCSDF에 의해 사용될 수 있다. 예로서, R-플래그가 1이면 CCSDF는 CRP와 CGP를 모두 수행하도록 요청한다. 플래그가 "0"으로 설정되면 자격증명 요청만 수행된다.

[0090] * 클라이언트 특정: 이 플래그는 메시지가 클라이언트 특정 자격증명 요청인 경우를 나타낸다. 여기서는 단지 콘텐츠 특정 CR임을 나타내기 위해 '0'으로 설정된다.

[0091] 여전히 도 15를 참조하면, 도시된 예에 따라, SEF는 요청에 기초하여 정확한 자격증명 세트를 생성한다. Credential_Type = "대칭 키"의 경우, KDF를 사용하여 위에서 설명한 것과 유사한 메커니즘을 사용할 수 있다. SEF는 요청된 "라이프타임" 값에 유효한 KeyGenKey를 생성하여 이를 CCSDF에 제공할 수 있다. 그런 다음 KeyGenKey가 CDB에서, SEF로 해당 특정 콘텐츠에 대해 등록된다. 대안적으로, SEF는 IK와 CK를 모두 생성하여 이를 콘텐츠에 등록하고 자격증명 데이터 베이스(CDB)에 저장한다. Credential_Type = "인증서"인 일부 경우에, SEF는 공개 키를 사용하여 SEF가 서명한 인증서를 생성하고 인증서를 Content-Id에 연계시키고 인증서의 사용을 요청의 일부로 제공된 라이프타임 값으로 제한한다. 콘텐츠에 대한 인증서도 CDB에 저장된다. 3에서 SEF는 자격증명(들) 목록을 송신한다. 대응하는 알고리즘이 선택된 경우에, 알고리즘의 목록은 등록이 성공적인지 아닌지 여부의 표시를 제공하는 플래그와 함께 제공될 수도 있다. 자격증명 목록의 일부로서 자격증명이 KeyGenKey인지의 여부 및 자격증명의 유효성을 나타내는 플래그가 제공될 수 있다. 각 자격증명과 관련된 고유 Credential-Id(들)의 목록이 또한 예에 따라 CCSDF에 제공된다. 4에서 CCSDF는 자격증명(들), Credential-Id(들) 및 CDB와 연관된 라이프타임을 저장한다. 자격증명이 KeyGenKey인 경우, CCSDF는 선택적으로 CK, IK를 생성할 수 있거나 이들의 유도를 클라이언트에게 넘길 수 있다.

[0092] 이제 도 16을 참조하면, 예시적인 클라이언트-특정 CR 프로세스가 도시된다. CCSDF는 예로서 이들 클라이언트만이 콘텐츠에 액세스할 수 있도록 요구할 경우 클라이언트 특정 자격증명을 요청할 수 있다. 0에서, CCSDF와 SEF가 서로를 상호 인증한 후에 보안 통신 채널이 CCSDF와 SEF간에 확립된다. 채널이 설정되면 1에서 CCSDF는 자격증명이 요청되는 클라이언트(들)의 목록을 포함하는 CR 메시지를 송신한다. Credential_Type는 요청중인 자격증명의 유형이다. Credential_Type는 "인증서"또는 공개 키 또는 "대칭 키"일 수 있다. "대칭 키"보다는 클라이언트와 관련된 "인증서"또는 "공개 키"를 요청하는 것이 더 바람직할 수 있다. Client-id가 여러 개의 클라이언트(들)와 연관될 수 있고 일 그룹의 클라이언트가 동일한 Client-id를 공유할 수 있다.

[0093] 2에서 SEF는 요청을 처리하고 CDB에 쿼리하여 특정 클라이언트에 대한 올바른 자격증명 세트를 획득한다. Credential_Type = "인증서"또는 "공개 키"이면, 도시된 예에 설명된 바와 같이 해당 클라이언트와 연관된 자격증명이 CDB로부터 가져와 진다. Credential_Type = "대칭 키"인 경우 SEF는 CDB로부터 CK만을 가져올 수 있다. 소정 경우에는, 대안적으로 클라이언트와 연관된 KeyGenKey를 가져올 수 있으며, 이는 그후 CK를 생성하기 위해 CCSDF에 의해 사용된다. 3에서, 도시된 예에 따라, 클라이언트(들)와 연관된 인증서 만이 송신된다. SEF는 각 클라이언트와 연계된 자격증명의 목록을 송신할 수 있다. 자격증명 각각은 특정 유형(공개 키, 인증서 또는 대칭 키)일 수 있다. 또한 한 그룹의 클라이언트들이 동일한 자격증명을 공유할 수도 있다. 4에서 송신된 자격증명이 KeyGenKey(들)인 경우 CCSDF는 이로부터 각 클라이언트(들)에 대한 CK(들)를 생성하고 로컬 CDB에 자격증명을 저장할 수 있다. 자격증명이 각 클라이언트와 관련된 "공개 키(들)"또는 "인증서(들)"일 경우, 그들은 그대로 저장될 수 있다.

[0094] 간결성을 위해, 클라이언트 자격증명 및 콘텐츠-특정 자격증명은 예에 따라 일반 CDB 내에 저장될 수 있지만, 이들은 별도의 DB에 저장될 수 있고 상이한 관리 도메인 내에서 호스팅될 수도 있음을 이해할 것이다. 콘텐츠 특정 CR 및 클라이언트 특정 CR에 사용되는 SEF는 다를 수 있으므로 CCSDF와 SEF 사이의 신뢰 관계들이 다를 수 있다.

[0095] 이제 도 17을 참조하면, CCDSF는 도 17에 도시된 바와 같이 자격증명 등록 프로세스(CGP)를 사용하여 콘텐츠와 관련된 자격증명을 SEF에 등록할 수 있다. 콘텐츠의 프록시 기반 호스팅이 사용될 때, 여기에 설명된 유사한 메커니즘이 CCDSF에 의해 자격증명(들)을 SCHF에 등록하거나 SCHF에 의해 SEF에 등록하기 위해 사용될 수 있다. 예시적인 실시예에서, CGP는 콘텐츠 특정 자격증명이 SEF에 의해 생성되지 않은 경우에만 요구된다. 자격증명이 CCSDF 또는 SCHF에 의해 생성되는 경우, 자격증명은 SEF에 등록될 수 있다.

[0096] 여전히 도 17을 참조하면, 도시된 예에 따르면, 1에서, CCDSF는 보안 통신 채널을 사용하여 SEF에 CG 요청 메시지를 송신한다. 전술한 바와 같이, CG 요청 메시지의 종점은 다른 SEF 또는 SCHF일 수 있다. 메시지의 일부로서 다음과 같은 파라미터가 포함될 수 있으며, 이들은 예로서 제시된 것이고 제한적이지 않다:

[0097] * Content-Id[]: 전역적으로 고유하거나 SEF 및 CCSDF의 도메인 내에서 고유한 것으로 가정되는 콘텐츠 식별자(들)의 목록. 콘텐츠가 등록되는 도메인 내에서 Content-Id의 고유성을 보장하기 위해 추가 메시징을 사용할 수 있다.

[0098] * Algorithm[]: 수행할 수 있는 동작의 유형뿐만 아니라 각 콘텐츠에 대해 사용되는 알고리즘 목록. 예로서, 각 콘텐츠에는 하나 이상의 관련 알고리즘(예로서, 무결성 보호: HMAC-SHA 및 기밀성 보호: AES)이 있을

수 있다.

[0099] * Credential_Type[]: 이전에 언급한 바와 같이 이는 다음과 같을 수 있다: 대칭 키, 공개 키 또는 인증서

[0100] * Usage[]: 알고리즘 및 자격증명을 사용하는 방법에 대한 일반적인 가이드라인이 될 수 있다. 대부분의 경우, 이는 베스트-프랙티스에 기반하고 정책에 따라 지정될 수 있으므로 생략될 수 있다.

[0101] * ACP[]: 자격증명 제공이 허용, 차단 또는 제한될 수 있는 엔티티들(클라이언트들)의 목록. 이 목록에는 클라이언트 클래스 또는 기반 클라이언트 도메인 정보(예로서, FQDN) 등이 포함될 수 있다.

[0102] 2에서, 도시된 예에 따라, SEF는 Content-Id(들)가 고유하고 자격증명들(예로서, 공개 키/인증서의 경우)이 정확한 Content-Id와 관련되는지를 확인한다. 올바른 개인 키(들)의 소유에 대한 사이드 채널 확인이 수행될 수 있다. 검사가 이루어지고, 성공적으로 확인되면 자격증명이 CDB에 저장된다. 3에서 SEF는 등록 성공 메시지로 응답하고, 또한, SEF에 등록된 각 자격증명과 연관된 고유 식별자인 Credential-Id(들)의 목록을 포함한다.

[0103] 클라이언트(들)는 동일한 SEF 또는 다른 SEF와 신뢰 관계를 가질 수 있다. 클라이언트 자격증명 정보와 연관된 CG 프로세스의 예시적인 예시가 도 18에 도시되어 있다. 1에서, 도시된 예에 따라, 그 자격증명을 SEF에 등록하고자 하는 클라이언트는 제한없이 예로서 제시된 다음 파라미터들을 송신할 수 있다:

[0104] * Client-Id

[0105] * Credential_Type: 이는 등록중인 자격증명 유형의 표시이다. 클라이언트에 대한 바람직한 Credential_Type는 "공개 키" 또는 그 "인증서"일 수 있다. 또한 클라이언트가 기밀성 보호를 제공하는 데에만 사용되는 "대칭 키"를 등록할 수도 있다.

[0106] * 자격증명(들): 클라이언트는 여러 자격증명을 가질 수 있으며 SEF에 다양한 자격증명을 등록할 수 있다.

[0107] * 알고리즘: 자격증명의 유형에 사용되는 알고리즘.

[0108] * 사용법: 자격증명 사용 방법에 대한 정책들. 이 파라미터는 일 예에 따라 선택 사항으로 간주된다.

[0109] * ACP: 자격증명을 사용할 수 있는 사람/대상에 대한 제한 사항의 목록. 이것은 선택 사항일 수도 있다.

[0110] 2에서, 도시된 예에 따라, SEF는 CG 요청을 확인하고 자격증명을 CDB 내에 저장한다. 3에서 SEF가 자격증명을 성공적으로 등록하면 클라이언트에 "성공" 메시지를 송신한다. 또한 클라이언트에 대해 등록된 각 자격증명과 연관된 고유 Credential-Id를 보낸다.

[0111] 이제 예시적 제3 기관 자격증명 요청 프로세스(TPCRP; Third-party Credential Requisition Process)로 돌아가면, 콘텐츠 신뢰성을 확인하기를 원하는 클라이언트는 암호화된 콘텐츠를 해독할 수 있는 능력을 필요로 하는 경우 SEF로부터 자격증명을 요청할 수 있다. 대안적으로, 콘텐츠와 관련된 자격증명이 SCHF에 등록되어 있고 클라이언트가 SCHF를 발견할 수 있는 경우 클라이언트는 SCHF로 CR 요청을 발행할 수 있다. 자격증명이 외부적으로 등록되지 않고 콘텐츠 생성기(예로서, CCSDF)에 로컬로 저장되는 것도 가능하다. 이 경우 클라이언트는 CCSDF로 CR을 발행할 수 있다. SEF, SCHF 또는 CCSDF와 관련된 URI는 공통 서비스 검색/리소스 발견 메커니즘(예로서, DNS-SD, RD 메시징)을 사용하여 발견될 수 있다. 자격증명이 등록된 위치에 관계없이 엔티티들(예로서, SEF, SCHF 또는 CCSDF)는 자체적으로 인증 및 허가를 수행해야 할 수 있거나, 자격증명을 릴리즈하기 위해 엔티티들을 대신하여 수행할 수 있는 TTP 서비스를 사용할 수 있다. ACP는 CR 프로세스의 일부로 제공되었을 수 있다. 인증 및 허가 메커니즘의 강도는 요청되는 콘텐츠의 유형을 기반으로 할 수 있다. 예시적인 TPCRP는 도 19에 예시되어 있는데, 여기서 자격증명은 SEF에 등록되어 있다. 앞서 언급한 바와 같이 요청이 CCSDF 또는 SCHF를 대상으로하는 경우 유사한 메커니즘이 사용될 수 있다.

[0112] 도 19를 참조하면, 도시된 예에 따라, 1에서, 클라이언트는 TPCRP 요청을 SEF에 송신한다. 요청에는 제한 없이 예로서 제시된 다음 파라미터들이 포함될 수 있다.

[0113] * Content-Id: 클라이언트가 요청하고자하는 콘텐츠의 아이덴티티

[0114] * Credential-Id(선택 사항): 클라이언트가 콘텐츠와 관련된 특정 자격증명을 받기를 원하면 이 파라미터를 사용할 수 있다. 대부분의 경우 Credential-Id가 있으면 Content-Id를 생략할 수 있다. 그러나 Credential-Id가 여러 콘텐츠(들)를 보호하는 데 사용될 수 있는 경우 Content-Id와 Credential-Id의 조합을

사용할 수 있다.

[0115] * Credential_Type(선택 사항): 클라이언트가 Credential-Id에 액세스할 수 없는 경우 클라이언트는 특정 유형의 자격증명(예로서, 공개 키 또는 대칭 키)을 요청할 수 있다.

[0116] * 알고리즘(선택 사항): 클라이언트가 특정 암호화 알고리즘(예로서, AES) 만 수행할 수 있는 경우 예로서 클라이언트가 이를 지정할 수 있다.

[0117] 2에서 SEF는 클라이언트가 콘텐츠와 관련된 ACP(예로서, 자격증명에 액세스하는 데 필요한 인증/허가 수준)를 충족하는지 확인하고 자격증명이 CDB에 있으면 SEF는 Content-Id에 기초하여 자격증명을 검색한다. SEF가 Content-Id와 연관된 다수의 자격증명을 가지고 있고, 또한 Credential-Id가 클라이언트에 의해 제공되었다면, SEF는 그 특정 자격증명을 검색한다. Credential-Id가 없으면 SEF는 클라이언트가 그 요청 내에서 바람직한 Credential_Type를 송신했는지 검사하고, 그렇다면 Credential_Type와 일치하는 Content-Id와 연관된 자격증명을 고른다. Credential_Type가 없지만 바람직한 알고리즘이 요청된 경우 SEF는 해당 특정 알고리즘에서 사용할 수 있는 자격증명을 선택할 수 있다. 대안 실시예에서, SEF는 ACP가 그러한 트랜잭션을 허용하면, Content-Id와 관련된 모든 자격증명을 송신할 수 있다. 도시된 바와 같이, 3에서, SEF는 자격증명(들)을 포함하는 응답을 송신한다.

[0118] 도 20은 예시적인 콘텐츠 검색 프로세스(CRP)를 도시한다. 1에서, 도시된 예에 따라, 클라이언트는 CRP 요청을 개시하고 메시지의 일부로서 Content-Id를 SCHF에 제시한다. 2에서, SCHF는 클라이언트가 콘텐츠에 액세스할 허가가 있는지 결정하기 위해 허가 검사를 개시할 수 있다. 클라이언트는 SEF로부터 획득한 경우 허가 토큰을 제시할 수 있다. 그렇지 않은 경우 클라이언트와 SCHF간에 새로 허가를 수행해야 할 수 있다. 3에서, 도시된 예에 따라, 요청을 확인한 후, SCHF는 PCS로부터 EC 및 관련 AT를 검색한다. 4에서, SCHF는 EC, AT 및 CryptoParams를 포함하는 CRP 응답 메시지를 송신한다. CryptoParams는 선택적으로 SCHF에 의해 송신될 수 있다. 일부 경우에는 SCHF가 CryptoParams를 소유하지 않을 수 있다. 이 경우 클라이언트는 위에서 설명한 TPCRP를 사용하여 CryptoParams을 미리 가져올 수 있다. 콘텐츠 유형과 CryptoParams에 기초하여 일부 콘텐츠는 암호화되지 않을 수 있고, 따라서 콘텐츠는 암호화되지 않은 형식으로 송신될 수 있다. 대부분의 경우, 콘텐츠는 무결성 보호될 수 있으며 따라서 대응 AT는 SDF에 의해 유도되었을 수 있다고 가정한다.

[0119] 예시적인 실시예에서, 클라이언트가 EC 및 연관된 AT를 검색한 후에, 클라이언트는 허가되지 않은 엔티티에 의해 콘텐츠가 수정되지 않고 합법적 또는 신뢰성있는 엔티티(예로서, CCSDF 또는 높은 신뢰도를 가진 SCHF)에 의해 생성되었다는 것을 확인함으로써, 그리고, 클라이언트가 콘텐츠를 소비할 수 있게 하도록 암호화된 콘텐츠를 해독함으로써 콘텐츠를 처리한다. 도 21을 참조하면, 클라이언트에 의해 수행된 무결성/신뢰성 검사 및 해독 프로세스의 하이 레벨 도면을 도시하는 흐름도가 도시된다. 도 21의 설명은 콘텐츠가 클라이언트의 공개 키를 사용하여 암호화되고 SDP의 개인 키를 사용하여 무결성 보호되는 도 9에 도시된 클라이언트-특정 CryptoParams에 기초한다. 1에서, 도시된 예에 따라, 클라이언트는 SCHF로부터 검색된 EC를 사용하고 EC의 해시를 계산하기 위해 CryptoParams 내에서 지정된 Nonce 및 해싱 알고리즘(예로서, SHA-256)을 사용한다. 2에서, 클라이언트는 AT를 사용하고 SDF에 의해 계산된 해시를 얻기 위해 공개 키 알고리즘(예로서, RSA) 및 SDF의 공개 키를 사용하여 AT를 해독한다. 3에서, 도시된 예에 따라, 클라이언트에 의해 계산된 해시는 SDF에 의해 생성된 해독된 해시와 비교된다. 해시가 일치하지 않으면 프로세스가 중지된다. 4에서 해시가 일치하면 클라이언트는 공개 키 알고리즘(예로서, RSA)을 통해 클라이언트의 개인 키를 사용하여 EC를 해독한다. 소정 형태의 패딩이 암호화된 콘텐츠를 생성할 때 무작위성을 위해 사용된다고 가정한다. 본 명세서에 제시된 예가 RSA에 기초한 암호화이지만, 실시예가 이에 한정되는 것은 아님이 이해될 것이다. 예로서, 대칭 키 기반 암호화 알고리즘이 공개 키 기반 메커니즘이 아닌 암호화에 선호될 수 있다. 5에서 클라이언트는 콘텐츠를 소비한다.

[0120] 이제 예시적 CLMP(Content Life-cycle Management Process) 예제로 전환하여 CCSDF 및/또는 SDF는 특정 콘텐츠의 콘텐츠 라이프 사이클 관리와 연루될 수 있다. CLM 프로세스는 표 1에 제공된 보안 파라미터 내에서 제공되는 "라이프 사이클"(예로서, 년) 값에 기반하여 CCSDF에 의해 개시될 수 있다. 라이프 사이클 기간이 정책들을 기반으로 달성된 경우, 콘텐츠는 삭제되거나 사용불가하게 될 수 있다(예로서, 무작위 값을 사용하여 콘텐츠를 혼합 및 패딩하고, 일회용 키 및 강한 암호화 알고리즘을 사용하여 이를 암호화함으로써). '보안 보호 업데이트' 값(예로서, 수년)을 사용하여 콘텐츠와 관련된 보안 보호를 업데이트할 수 있다. 보안 보호를 업데이트하는 것은 선택 사항일 수 있으며 일부 경우에 콘텐츠를 보안 공격에 노출시킬 수 있으므로 신뢰할 수 있는 엔티티들(예로서, TEE가 있고 RoT를 기반으로하는 플랫폼)만이 CLM 프로세스를 수행하도록 허용될 수 있다. 자격증명을 생성하고 등록하고 콘텐츠를 보호하기 위해 새로운 CRP, CGP, 재호스팅 프로세스 및 TPCRP가 수행될 수 있

다. 요약하면 새로운 자격증명이 생성되고 등록되며 새로운 자격증명을 사용하여 콘텐츠가 보호된 다음 보호된 콘텐츠가 새롭게 생성된 자격증명과 함께, 바람직하게는 소비를 위한 별도의 채널을 사용하여, 허가된 클라이언트에게 제공된다.

[0121] 여기에 설명된 실시예는 편의상 oneM2M 아키텍처에 주로 초점을 두지만, 실시예는 oneM2M으로 제한되지 않는다는 것이 이해될 것이다. 전술한 일반적인 기능(예로서, SEF)은 도 22에 도시된 바와 같이, Mca 인터페이스를 통한 "보안"의 일부로서 oneM2M 아키텍처에 통합될 수 있다. 예로서, AE는 CCSDF를 통합할 수 있으며 CSE는 SCHF를 구현할 수 있다. SEF는 예시적인 실시예에서 M2M 인롤먼트 기능(MEF)에 통합된다. AE와 MEF 사이, 그리고 또한 CSE와 MEF 사이에 기본적인 신뢰 관계가 있다는 것을 이해할 수 있다. 앞서 기술된 기능들 및 oneM2M 엔티티들의 요약 매핑이 제한이 아닌 예로서 아래 표 4에 제공된다.

표 4

표 4: Mca 인터페이스를 통한 oneM2M 엔티티들에 대한 보안 기능들의 매핑

[0122]

oneM2M 엔티티	기능
AE	SCHF
	SDF / CCSDF
CSE	SCHF
	SEF
	SDF
	CLMP
MEF	SEF
	CLMP

[0123] 도 23은 Mcc 인터페이스에서 콘텐츠 보안을 제공하기 위한 보안 기능성을 통합하는 일례를 나타낸다. 이전에 기술된 기능들 및 oneM2M 엔티티들의 요약 매핑이 표 5에 제공되며, 이는 제한이 아닌 예로서 제시된다.

표 5

표 5: Mcc 인터페이스를 통한 oneM2M 엔티티들에 대한 보안 기능의 매핑

[0124]

oneM2M 엔티티	기능
CSE1	SCHF
	SDF
CSE2	SEF
	SCHF
	CLMP

[0125] 도시된 바와 같이, CSE1은 SDF 및 SCHF를 구현할 수 있다. SCHF 기능은 애플리케이션 콘텐츠이나 oneM2M 시스템 리소스들과 관련이 있는 oneM2M 리소스(들)를 보안 방식으로 저장하는 데 사용된다. SCHF는 데이터 관리 및 리포지토리 CSF(Data Management & Repository CSF)의 일부로서 존재하고 관리될 수 있다. SDF는 보안 CSF 내에 존재하고 관리될 수 있다. CSE2에서, 예에 따라 SEF 및 CLMP 기능은 보안 CSF의 일부로 통합될 수 있지만 보안 방식으로 자격증명(들) 리소스들을 안전하게 저장하는 것과 주로 연루된 SCHF는 데이터 관리 및 리포지토리의 일부로서 통합될 수 있다. 위에서 설명한 Credential-Id 리소스 및 cryptoParams는 SCHF가 저장하고 관리할 수 있는 적절한 리소스가 될 수 있다.

[0126] 이제 도 24를 참조하면, 예시적인 실시예가 oneM2M에 따라 도시된다. 도시된 바와 같이, 콘텐츠는 oneM2M 리소

스로 표현될 수 있는 반면, 하위 컴포넌트들은 속성들 및 콘텐츠인스턴스(들)로 표현될 수 있다. 여기서는 서비스 레이어 연결(홉)이 TLS/DTLS 기반 보안 연결을 사용하여 보호될 수 있다고 가정한다. 1에서, 도시된 예에 따라, 생성된 리소스에 대한 보호를 제공하려는 AE1은 M2M 인롤먼트 기능(MEF; Enrollment Function)에 적절한 자격증명을 요청할 수 있다. AE1과 MEF가 그들 사이의 상호 인증을 수행하고 (D)TLS를 사용하여 보안 통신 채널을 확립했다고 가정한다. 또한 MEF는 AE1이 요청을 수행할 수 있는 허가가 있음을 확인했다고 가정한다. AE1이 무결성 및 기밀성 보호를 제공하려는 경우 AE1은 이러한 자격증명을 명시적으로 요청할 수 있다. 대안적으로, AE1은 대칭 키 메커니즘을 사용하는 경우에 마스터 키(예로서, KeyGenKey) 만을 요구할 수 있다. AE1은 리소스 생성 요청을 송신하고 그 보안 요구 사항(SecRequirements)을 해당 요청과 함께 제공할 수 있다. 또한, 액세스 제어 정책(ACP; Access Control Policy) 목록이 제공될 수 있으며, 이는 허가된 엔티티들의 목록(예로서, AE2의 아이덴티티)을 포함할 수 있다. 2에서 MEF는 AE1이 MEF에서 리소스를 생성할 허가가 있는지 확인한다. AE1이 승인되면 MEF는 해당 자격증명 및 관련 Credential-Id를 생성한다. 그것은 도 25에 도시된 바와 같은 리소스 구조를 생성할 수 있다. 3에서, 도시된 예에 따라, MEF는 자격증명 및 Credential-Id를 응답으로서 AE1에 송신한다. 대안적으로, AE1은 자격증명을 얻기 위해 검색 동작을 수행할 수 있다. 자격증명은 예로서 JSON 웹 키(JWK) 포맷의 형식으로 표현되고 송신될 수 있다.

[0127] 계속해서 도 24를 참조하면, 도시된 예에 따라, 4에서, AE1에 의해 검색된 자격증명 및 CryptoParams에 기초하여, AE1은 EC-R1을 생성하기 위해 리소스를 암호화하고, 리소스의 AT(MAC 또는 디지털 서명)를 생성하며, 이는 R1-AT라 지칭된다. 난스 및 Id뿐만 아니라 알고리즘의 선택은 CryptoParams 내의 값들을 기반으로 할 수 있다. 생성된 EC-R1은 JSON 웹 암호화(JWE)를 기반으로 할 수 있으며 만들어진 R1-AT는 JSON 웹 서명을 기반으로 할 수 있다. 적절한 알고리즘은 예로서 JWA(JSON Web Algorithms) 표준에 지정된 형식으로 표현될 수 있다. 5에서 AE1은 호스팅-CSE(H-CSE)에 R1-AT 및 CryptoParams와 암호화된 콘텐츠(EC-R1)를 포함하는 리소스를 생성하라는 요청을 송신한다. 5에서의 요청은 등록 프로세스의 일부일 수 있거나 AE1은 요청을 송신하기 전에 H-CSE에 미리 등록되었을 수 있다. 일부 경우에 H-CSE가 완전히 신뢰할 수 없기 때문에 CK, IK 및 KeyGenKey가 CryptoParams의 일부로 H-CSE에 제공되거나 노출되지 않는 것을 보증하도록 주의해야 한다. 그러나 공개 키 메커니즘이 사용되는 경우 예로서 공개 키 값 또는 인증서 또는 공개 키에 대한 링크가 CryptoParams의 일부로 제공될 수 있다. 6에서, AE1이 예로서 H-CSE에서 리소스를 생성하도록 허가되면, H-CSE는 보호된 콘텐츠를 호스팅한다. 보호된 콘텐츠에 대해 생성된 예시적 리소스 구조가 도 29에 도시되어 있다. 7에서, 도시된 예에 따라, 클라이언트(AE2)는 보호된 리소스(EC-R1)를 얻기를 원하며, 따라서, R1을 검색하기 위해 요청 메시지를 H-CSE로 송신한다. 8에서 H-CSE는 EC-R1과 관련된 ACP를 사용하여 AE2의 허가를 확인한다. ACP는 AE(CCSDF)에 의해 제공되는 정책들, SP 제공 정책들 또는 H-CSE에서의 로컬 정책들을 기반으로 생성되었을 수 있다. 9에서, AE2가 허가 검사를 통과하면, H-CSE는 EC-R1, R1-AT 및 CryptoParams를 포함하는 응답을 AE2에 송신한다. 위에서 언급한 바와 같이 H-CSE는 일부 경우에 신뢰할 수 없으므로 CryptoParams에 CK, IK 또는 KeyGenKey가 포함되지 않을 수 있다. CryptoParams에는 공개 키 또는 인증서 또는 공개 키 또는 인증서에 대한 링크가 포함될 수 있다. 10에서 AE2는 CryptoParams에서 Credential-Id를 추출한다. 12에서, AE2는 MEF에 요청 메시지를 송신한다. 요청 메시지는 자격증명에 대한 검색 동작을 수행하기 위해 R1과 연결된 Credential-Id를 포함할 수 있다. 12에서, 도시된 예에 따라 MEF는 AE2가 AE1에 의해 생성된 ACP를 기반으로 자격증명을 프로비저닝받을 허가가 있다고 결정한다. 13에서 AE2가 허가된 경우 MEF는 AE2에 자격증명을 보낸다. 14에서 AE2는 자격증명을 사용하여 R1의 신뢰성/무결성을 확인하고 해독한다.

[0128] 도 24를 참조하여 상술한 실시예는 Mcc 인터페이스(예로서, 2개의 CSE들 사이: CSE1, CSE2)에 적용 가능할 수 있다는 것을 이해할 것이다. 이러한 시나리오에서, AE1은 CSE1로 대체될 수 있고, AE2는 예로서 CSE2로 대체될 수 있다.

[0129] 따라서, 도 24를 참조하면, 장치(예컨대, AE1)는 프로세서, 메모리 및 통신 회로를 포함할 수 있다. 장치는 그 통신 회로를 통해 네트워크에 접속될 수 있고, 장치는 노드의 메모리에 저장된 컴퓨터 실행 가능 명령어를 더 포함할 수 있으며, 이 명령어는 장치의 프로세서에 의해 실행될 때, 장치로 하여금 또는 콘텐츠 보호를 제공하는 하나 이상의 자격증명에 대한 요청을 송신하게 한다. 요청은 콘텐츠와 관련된 하나 이상의 보안 파라미터를 기반으로할 수 있다. 장치는 하나 이상의 자격증명을 획득하고, 하나 이상의 자격증명을 사용하여 콘텐츠를 보안할 수 있다. 자격증명은 대칭 키 기밀성 보호를 위한 마스터 키를 포함할 수 있다. 자격증명은 무결성 보호 및 기밀성 보호를 위한 자격증명을 포함할 수 있다. 장치는 암호화된 콘텐츠를 생성하기 위해 콘텐츠를 암호화할 수 있다. 장치는 콘텐츠와 관련된 인증 태그를 생성할 수 있다. 또한, 장치는 암호화된 콘텐츠 및 보안 파라미터들을 포함하는 리소스를 생성하기 위해 호스팅 공통 서비스 엔티티에 요청을 송신할 수 있다. 도시된 바

와 같이, 자격증명은 일례에 따라 M2M 인롤먼트 기능으로부터 획득될 수 있다.

[0130] SEF가 CSE에 존재하는 대안적 실시예가 도 26에 도시되어 있다. 도 26을 참조하면, 도시된 실시예에 따라, 1에서, 리소스 R1을 안전하게 호스팅하기를 원하는 AE1은 보안 요구 사항들에 기초하여 적절한 자격증명을 생성한다. 자격증명을 사용하여 AE1은 콘텐츠를 암호화하여 EC-R1을 만들고 이를 무결성 보호하여 R1-AT(사용된 자격증명의 유형에 따라 DS 또는 MAC일 수 있음)를 만들 수 있다. 예로서, 암호화된 EC-R1은 JSON 웹 암호화로 표현될 수 있다. 2에서 AE1은 자격증명 호스팅 서비스를 수행하는 CSE에서 Credential-Id 리소스를 생성하기 위해 요청을 수행한다. 이 예에서 AE와 CSE는 상호 신뢰 관계를 공유한다고 가정한다. 또한, 이 예에서 AE1과 CSE 사이의 통신은 보안 통신 채널(예를 들어, DTLS, TLS)을 통해 수행된다고 가정한다. 보안 통신 채널을 사용하여 AE1은 AE1이 생성하고 콘텐츠의 암호화 및/또는 무결성 보호에 사용하는 하나 이상의 자격증명을 CSE로 보낼 수 있다. 3에서, CSE는 AE1이 리소스를 생성할 허가가 있는지 여부를 결정할 수 있다. 예로서, CSE는 (D)TLS를 사용하는 보안 통신 채널 확립 프로세스 중에 인증 절차를 수행했을 수 있다. 대안적으로 또는 추가적으로, ACP 정책들은 서비스 제공자에 의해 CSE에 미리 프로비저닝될 수 있다. CSE는 선택적으로 AE1의 공개키를 사용하여 AT를 검증할 수 있다. CSE는 선택적으로 CSE와 관련된 고유 Credential-Id를 생성할 수 있다. 이는 선택 사항이며 AE1에 의해 제공되었을 수 있다. 일부 경우에 CSE는 도메인 내에서의 고유성 및 글로벌 도달성을 제공하기 위해 AE1 대신 Credential-Id를 생성할 수 있다. CSE에서 생성된 Credential-Id 리소스는 도 27의 예에 의해 도시된 형태일 수 있다.

[0131] 여전히 도 26을 참조하면, 도시된 실시예에 따라, CSE는 4에서 AE1에 Credential-Id를 송신한다. 5에서 AE1은 암호화된 EC-R1이며 R1-AT를 사용하여 무결성 보호되는, 보안 리소스 R1을 생성하도록 요청한다. 따라서, 도시된 예에 따르면, H-CSE는 제1 애플리케이션(AE1)으로부터 제1 요청을 수신하여 제1 애플리케이션과 연관된 보안 콘텐츠를 호스팅하기 위한 리소스를 생성한다. AE1은 필요한 CryptoParams 및 Credential-Id도 제공할 수 있다. 따라서, 요청은 H-CSE로부터 분리된 CSE에 의해 생성된 자격증명 아이덴티티를 포함할 수 있다. Credential-Id는 CryptoParams의 일부이거나 R1과 관련된 별도의 자식 리소스로서 송신될 수 있다. 이 예에서, AE1과 H-CSE는 서로를 상호 인증하고 TLS 또는 DTLS를 사용하여 보안 통신 채널을 확립한 것으로 가정한다. 또한, 예로서, 도 28에 도시된 바와 같은 연관된 액세스 제어 정책 리소스를 포함할 수도 있다. 이 ACP는 무결성 보호될 수 있으며 AE1의 개인 키를 사용하여 생성된 DS를 기반으로 AT가 생성될 수 있다. 생성된 EC-R1은 JSON 웹 암호화(JWE)를 기반으로 할 수 있으며 생성된 R1-AT는 JSON 웹 서명을 기반으로 할 수 있다. 적절한 알고리즘은 JSON 웹 알고리즘(JWA) 표준에 지정된 형식으로 표현될 수 있다. 6에서, H-CSE는 요청을 확인하고, AE1이 H-CSE에서 리소스를 생성하도록 허가되는 것을 보증(그 여부를 결정)하도록 검사한다. 7에서, 도시된 예에 따라, H-CSE는 성공으로 응답한다. 따라서, 예시적인 애플리케이션이 허가되면, H-CSE는 보안 콘텐츠를 호스팅할 수 있다. 일부 경우에 H-CSE와는 별도의 CSE에서 애플리케이션을 인증하여 리소스를 생성할 수 있다.

[0132] 8에서, 클라이언트(AE2)는 R1을 검색하기를 원하고, 따라서 제2 요청과 같은 요청을 H-CSE에 송신하여 R1을 검색한다. 따라서, H-CSE는 AE1과 연관된 보안 콘텐츠에 액세스하기 위한 제2 애플리케이션(AE2)으로부터의 제2 요청을 수신할 수 있다. R1 발견과 관련된 메커니즘은 예의 범위를 벗어나며 AE2는 R1의 보안 버전의 위치를 발견할 수 있다고 가정한다. AE2는 무결성 관점에서 덜 보증된 R1의 낮은 보안성의 버전을 발견할 수 있다. 요청은 DTLS 또는 TLS를 기반으로 상호 인증이 수행된 후 보안 채널을 통해 송신되는 것으로 가정한다. 9에서, 도시된 실시예에 따라, H-CSE는 AE1에 의해 생성된 ACP 내의 정보를 사용하여 AE2가 검색 동작을 수행할 수 있는지 여부에 대해 허가를 확인한다. 따라서, H-CSE는 AE2가 보안 콘텐츠에 액세스하는 것이 허가되는지를 결정할 수 있다. 10에서, H-CSE는 EC-R1, EC-AT 및 R1-CryptoParams를 포함하는 응답을 송신한다. 따라서, 제2 애플리케이션이 보안 콘텐츠에 액세스하도록 허가되면, H-CSE는 보안 콘텐츠를 제2 애플리케이션에 송신할 수 있다. EC-AT는 JWS를 사용하여 표현될 수 있고, R1-CryptoParams은 JWA를 사용하여 표현될 수 있는 반면, EC-R1은 예로서 JSON-기반 표기법인 JWE를 사용하여 표현될 수 있다. 11에서 Credential-Id가 CryptoParams의 일부로 포함된 경우 AE2는 Credential-Id를 추출한다. 12에서 AE2는 Credential-Id를 메시지 내의 리소스-id로 포함시켜 검색 동작을 수행하기 위해 CSE에 요청 메시지를 송신한다(예를 들어, CSE의 URI는 Credential-Id에 포함된 도메인 정보를 기반으로 결정될 수 있고 여기서 Credential-Id는 R1xyrtabsffas@CSE.com 형식으로 이루어질 수 있음). 이 예에서는 AE2와 CSE가 서로를 상호 인증하고 TLS 또는 DTLS를 사용하여 보안 통신 채널을 확립하였다고 가정한다. Credential-Id는 예로서 JWK와 같은 JSON 기반 표기법을 사용하여 송신될 수 있다. 13에서 CSE는 2에서의 자격증명 등록 프로세스 중에 AE에 의해 생성된 ACP를 기반으로 AE2의 허가를 확인한다. 14에서 AE2가 검색 허가가 있으면 CSE는 보안 채널을 통해 자격증명을 AE2로 송신한다. 15에서 자격증명을 사용하여 AE2는 R1-AT를 사용하여 무결성을 확인하고 R1을 해독한다. 따라서 보안 콘텐츠는 CSE가 보안 콘텐츠와 연계된 하나 이상의 자격증명을 제2 애플리케이션(AE2)으로 송신할 때 해독될 수 있다. 일부 경우에 위에서 설

명한대로 AE2는 AE1의 액세스 제어 정책에 따라 보안된 콘텐츠에 액세스할 수 있는 허가된다.

[0133] 도 26과 관련하여 전술한 실시예는 Mcc 인터페이스(예로서, 2개의 CSE들: CSE1, CSE2) 사이에도 적용 가능할 수 있다는 것을 이해할 것이다. 그러한 시나리오에서 엔티티 AE1은 CSE1로 대체될 수 있고 AE2는 CSE2로 대체될 수 있다.

[0134] 따라서, 도 26을 참조하면, 장치(예로서, AE1)는 프로세서, 메모리 및 통신 회로를 포함할 수 있다. 장치는 그 통신 회로를 통해 네트워크에 접속될 수 있고, 장치는 장치의 메모리에 저장된 컴퓨터 실행 가능 명령어를 더 포함할 수 있으며, 이는 장치의 프로세서에 의해 실행될 때 장치가 콘텐츠와 관련된 보안 요구 사항에 따라 하나 이상의 자격증명을 생성하게 한다. 아래에서 상세히 기술된 바와 같이(예로서, 도 37 참조), 하나 이상의 자격증명은 장치와 신뢰 인에이블먼트 기능 사이의 연관을 부트스트래핑(bootstrapping)함으로써 생성될 수 있다. 장치는 하나 이상의 자격증명을 사용하여 콘텐츠를 보안(예로서, 암호화)하고, 인증된 클라이언트 만이 호스팅 노드로부터 콘텐츠를 검색할 수 있도록 호스팅 노드가 보안 콘텐츠를 저장할 것을 요청할 수 있다. 장치는 또한 하나 이상의 자격증명을 사용하여 인증 태그를 생성할 수 있다. 인증 태그는 호스팅 공통 서비스 엔티티에서 호스팅을 위한 콘텐츠의 무결성 및 신뢰성을 나타낼 수 있다. 요청에 응답하여, 장치는 공통 서비스 엔티티로부터 자격증명 아이덴티티를 수신할 수 있다. 요청은 자격증명 아이덴티티와 관련된 자격증명을 포함할 수 있으며, 요청은 자격증명의 등록을 추구한다. 예시적인 실시예에서, 자격증명 아이덴티티는 공통 서비스 엔티티에 고유하다. 도시된 바와 같이, 호스팅 노드가 해당 노드가 호스팅 노드에서 리소스를 생성하도록 허가된 것으로 결정하면, 장치는 또한 성공 메시지를 수신할 수 있다.

[0135] 다른 실시예에 따르면, 데이터 보안 자격증명은 부트스트래핑을 사용하여 생성된다. 예로서, AE는 AE와 M2M 인롤먼트 기능(MEF), 신뢰 인에이블먼트 기능(TEF) 또는 M2M 인증 기능(MAF)과 같은 신뢰할 수 있는 제3 엔티티 사이의 기존 연계를 사용하는 부트스트래핑 프로세스를 활용하여 데이터 보안 자격증명을 생성할 수 있다. 이 문맥에서 사용되는 바와 같은 "데이터 보안"이라는 용어는 콘텐츠 보안 또는 리소스 보안을 지칭할 수 있음을 이해할 수 있다. 데이터는 또한 콘텐츠의 인스턴스를 나타낼 수도 있다. 따라서, 콘텐츠 인스턴스 보안은 본 명세서에서 일반적으로 데이터 보안이라 칭해질 수도 있다. 일부 경우에 TEF는 주로 데이터(예를 들어, 콘텐츠 또는 리소스) 특정 보안 자격증명을 원격으로 프로비저닝하는 데 주로 사용되는 MEF의 특수 구현예이다. 따라서, 달리 명시되지 않는 한, 용어 TEF 및 MEF는 제한없이 상호 교환 가능하게 사용될 수 있다.

[0136] 이제 도 37을 참조하면, 도시된 실시예에 따라, 데이터/콘텐츠 보안 자격증명은 AE와 TEF 사이의 부트스트래핑 프로세스의 결과로서 생성된다. 0에서 부트스트래핑을 사용하여 데이터 보안 자격증명을 도출함으로써 oneM2M 사양(TS-0003, 릴리스 1) 내에 현재 설명되어 있는 부트스트래핑 프로세스가 향상될 수 있다. AE와 MEF/TEF간에 공유되는 자격증명 KpmId/Kpm은 TS-0003(릴리스 1)에 설명된 대로 세션 자격증명 KeId/Ke를 생성하는 데 사용된다. 자격증명 Ke는 AE와 TEF 사이에서 데이터 보안 특정 자격증명을 생성하는 데 사용될 수 있다. 마찬가지로 AE와 CSE 사이의 부트스트래핑 프로세스는 AE와 CSE 사이의 기존 보안 연계를 활용할 수 있다. oneM2M TS-0003에 기술된 바와 같이, 보안 연계는 KpsaId/Kpsa에 의해 식별될 수 있다. 그런 다음 Kpsa가 Ke 대신 사용된다. 마찬가지로, AE와 MEF 사이의 보안 연계를 확립하는 데 사용되는 KmId/Km은 AE와 MEF 사이에 데이터 보안 자격증명을 생성하는 데 사용될 수 있다. 일부 경우에 AE 및 TEF에 대해 데이터 보안 자격증명을 생성하는 것이 더 바람직한 방법이다.

[0137] 다시 도 37을 계속 참조하면, 1에서, 도시된 예에 따라, AE(AE1)에 의해 마스터 키가 생성된다. 키 생성의 일부로 사용되는 무작위 값인 Salt는 부트스트래핑 프로세스 중에 공유되거나 부트스트래핑 중 AE와 TEF 사이의 초기 통신의 해시 값으로 계산될 수 있다. Salt는 AE1과 TEF 사이에 묶여있는 채널의 암호화 표현일 수 있다. 채널은 TLS 또는 DTLS를 사용하여 확립되는 보안 연결일 수 있다. Enrollee라고 지칭될 수 있는 AE1과 인롤먼트 타겟이라고 지칭될 수 있는 TEF는 Ke를 사용하여 데이터 보안 자격증명을 생성할 수 있다. 도시된 바와 같이, Ke_AE1-TEF는 AE1과 TEF 사이에 관련된 Ke를 나타낸다. Ke는 데이터 보안 마스터 키 K_AE1_TEF_data_sec_master을 생성하는 데 사용되는 마스터 키일 수 있다. 대안적으로, 예로서 타겟이 MEF인 경우, Km은 데이터 보안 마스터 키를 생성하기 위한 마스터 키로서 사용될 수 있다. Enrollee가 AE이고 인롤먼트 타겟이 TEF인 RFC 5809를 사용하는 데이터 보안 키 생성의 예가 다음에 제공된다:

[0138] * K_AE1_TEF_data_sec_master = HMAC-Hash (Salt, Ke_AE1_TEF)

[0139] * T(0) = 빈 스트링(길이 0)

[0140] * 일단 K_AE1_TEF_data_sec_master이 생성되면, 이는 고유한 데이터 신뢰성 및 데이터 기밀성 키를 생성

하기 위해 키 확장에 사용될 수 있다. 소정 경우에는 AEAD(예를 들어, AES-CCM 또는 AES-GCM)와 같은 알고리즘에 의해 데이터 신뢰성 및 기밀성이 제공되는 경우 단 하나의 키만 생성된다.

[0141] * K_AE1_TEF_data_auth = T (1) = HMAC-Hash (K_AE1_TEF_data_sec_master, T (0) | "데이터 신뢰성 및 무결성"| 0x01)

[0142] * K_AE1_TEF_data_auth 키는 데이터 신뢰성 및 데이터 무결성을 제공하는 데 사용되며, 따라서, 데이터 신뢰성 또는 데이터 무결성 키를 참조할 수 있다.

[0143] * K_AE1_TEF_data_conf = T(2) = HMAC-Hash(K_AE1_TEF_data_sec_master, T(1) | "데이터 기밀성 키"| 0x02)

[0144] 일부 경우에 Kpsa_AE1_CSE1(AE1과 CSE1 사이의 Kpsa)이 Ke_AE1_TEF 대신 사용될 수 있으며 위에서 설명한 프로세스를 사용하여 데이터 보안 보호(예를 들어, 데이터 인증, 무결성 및 데이터 기밀성)를 위한 고유 키를 생성할 수 있다. CSE가 AE에서 데이터 보안 자격증명 레지스트리로 사용되는 경우 Kpsa를 사용할 수 있다. 특정 경우에, Kpsa_AE1_CSE, Ke_AE_TEF 또는 Km_AE1_MAF가 K_AE1_TEF_data_sec_master 키로서 사용될 수 있고, 상술한 프로세스는 데이터 보안 보호(예로서, 데이터 인증, 무결성 및 데이터 기밀성)를 위한 고유 키를 생성하는데 사용될 수 있다. 특정 다른 경우에는 Ke_AE1_CSE1, Kpsa_AE1_TEF, Km_AE1_MAF에서 세션 키를 생성한 다음 데이터 신뢰성 및 데이터 기밀성을 위한 고유 키를 생성하는 마스터 키로서 사용한다. 특정 다른 경우에, Ke, Kpsa 또는 Kpm에서 생성된 단일 세션 키(K_AE1_TEF_data_auth_conf)만이 알고리즘의 AEAD 클래스와 함께 사용될 때 데이터 신뢰성 및 데이터 기밀성 모두를 제공하는 데 사용된다.

[0145] 2에서, 도시된 예에 따라, 키 생성의 유사한 프로세스가 TEF에 의해 수행된다. 부트스트래핑 프로세스가 AE1과 TEF 사이에서 수행될 때, 단계 0 동안 알고리즘, 키 생성 메커니즘, 키 유형 및 생성될 키의 수 등의 협상이 수행될 수 있다.

[0146] 3에서 AE1은 콘텐츠/데이터를 생성한다. 콘텐츠/데이터의 각 인스턴스는 고유한 데이터 신뢰성 및 데이터 기밀성 키로 보호될 수 있다. 다른 예에서, 콘텐츠의 인스턴스들, 예로서 콘텐츠의 모든 인스턴스들은 단일 데이터 신뢰성 키 및 단일 데이터 기밀성 키에 의해 보호될 수 있다. 여러 콘텐츠 인스턴스를 포함할 수 있는 컨테이너에 대해 단일 데이터 신뢰성 및 단일 데이터 기밀성 키만 생성되는 예시적 키 생성은 다음과 같다:

[0147] * K_AE1_Container-x_data_auth = HMAC-Hash (K_AE1_TEF_data_auth, "데이터 신뢰성 및 무결성"| "Container-x"| Nonce 또는 creationTime) 및

[0148] * K_AE1_Container-x_data_conf = HMAC-Hash (K_AE1_TEF_data_conf, "데이터 기밀성", "Container-x"| Nonce 또는 creationTime)

[0149] 대안적으로, 컨테이너 내의 콘텐츠의 각각의 인스턴스에 대해, 고유한 키 세트가 생성될 수 있다. 그러한 실시예의 예를 이하에 나타낸다:

[0150] * K_AE1_ContentInstance-x_data_auth = HMAC-Hash(K_AE1_TEF_data_auth, "데이터 신뢰성 및 무결성"| "Container-x"| Nonce 또는 creationTime) 및

[0151] * K_AE1_ContentInstance-x_data_conf = HMAC-Hash (K_AE1_TEF_data_conf, "데이터 기밀성", "ContentInstance"| Nonce 또는 creationTime)

[0152] 콘텐츠는 앞서 생성된 키를 사용하여 암호화 및/또는 무결성 보호될 수 있다. 콘텐츠를 암호화하기 위해, AE1에 의해 무작위 IV가 생성될 수 있다. 무작위 IV는 암호화된 콘텐츠(EC-R1, 암호화된 리소스)를 생성하기 위해 암호화 알고리즘 및 콘텐츠(데이터)와 함께 사용될 수 있다.

[0153] 콘텐츠 인스턴스가 개별적으로 암호화되는 경우, 각 콘텐츠 인스턴스는 고유한 기밀성 키를 가질 수 있고 암호화 프로세스가 수행될 때마다 새로운 IV가 생성되어 암호화된 콘텐츠 인스턴스를 생성할 수 있다. 따라서 각 콘텐츠 인스턴스에는 연계된 별도의 암호화된 콘텐츠 인스턴스가 있을 수 있다.

[0154] 무결성 보호 또는 콘텐츠/데이터에 신뢰성을 추가하기 위해 연관된 시간 컴포넌트가 있는 무작위 Nonce가 콘텐츠와 관련된 인증 태그(AT)를 생성하는 데 사용될 수 있다. 각 콘텐츠 인스턴스가 개별적으로 보호되는 경우 각 콘텐츠 인스턴스에는 연결된 AT를 가질 수 있다. 소정 경우에 데이터 신뢰성을 제공하기 위해 각 개별 AT를 생성하는 데 단일 키를 사용하는 것이 바람직하다.

[0155] 암호화된 콘텐츠는 도 29에 도시된 바와 같이 변경된 oneM2M 컨테이너 또는 <contentInstance> 리소스로서 표현될 수 있다. 대안적으로, 생성된 EC-R1은 RFC 7516에 명시된 JSON 웹 암호화(JWE)를 기반으로 할 수 있다. 생성된 R1-AT는 RFC 7515에 명시된 JSON 웹 서명을 기반으로 할 수 있다. 적절한 알고리즘은 JSON 웹 알고리즘(JWA) 표준인 RFC 7518에 명시된 형식으로 표현될 수 있다.

[0156] 일반적으로 생성되고 사용되는 각 키는 고유한 Credential-Id와 연관될 수 있다. Credential-Id는 AE1에 의해 생성되거나 TEF에 의해 AE1에 제공될 수 있다. 일부 경우에 Credential-Id는 콘텐츠 id 또는 콘텐츠 인스턴스 id의 특성 및 자격증명 유형을 전달할 수 있다. Credential-id의 예는 키 K_AE1_Container-x_data_conf와 연관된 K_AE1_Container-x_data_conf-Id@TEF.com 형식일 수 있다.

[0157] 도 37을 계속 참조하면, 4에서, 도시된 실시예에 따라, AE1은 TEF에 Credential-Id를 등록할 수 있다. 도시된 바와 같이, AE1은 Credential-Id 및 연관된 액세스 제어 정책들에 의해 식별된 자격증명 리소스를 생성하도록 요청한다. Credential-Id는 예로서 TEF와 관련된 Credential-Id의 충돌을 피하기 위해 TEF에 의해 제공될 수 있다. AE1에 의해 생성된 id에서 해시가 수행되면 Credential-Id의 충돌을 피할 수 있다. 예시적 해시가 아래에 나와 있다:

[0158] * H1 = 해시 (K_AE1_Container-x_data_conf-Id)

[0159] * Credential-Id = H1@TEF.com

[0160] 5에서, 도시된 바와 같이 TEF는 AE1이 TEF에 자격증명을 등록할 수 있는 허가가 있다는 것을 보증하기 위해 검사한다. TEF는 또한 포함되어 있을 수 있는 Credential-Id 및 선택적 CryptoParams를 확인할 수 있다. TEF는 <Credential-Id> 리소스 유형을 생성하고 예로서 <accessControlPolicy> 값과 같은 속성으로 이를 채운다.

[0161] 6에서, 도시된 예에 따라, TEF는 AE1에 자격증명 리소스의 성공적인 생성을 나타내는 응답을 송신한다. 7에서 AE1은 암호화된 EC-R1이면서 R1-AT를 사용하여 무결성 보호되는 보안 리소스 R1을 생성할 것을 요청한다. AE1은 또한 CryptoParams 및 Credential-Id를 제공할 수 있다. Credential-Id는 CryptoParams의 일부이거나 R1과 관련된 별도의 자식 리소스로서 송신될 수 있다. 일부 경우에, AE1과 HCSE가 서로 상호 인증하고 TLS 또는 DTLS를 사용하여 보안 통신 채널을 확립한다. 요청에는 연관된 액세스 제어 정책(ACP) 리소스도 포함될 수 있다. 이 ACP는 무결성 보호될 수 있다.

[0162] 8에서, H-CSE는 요청을 검증하고 AE1이 H-CSE에서 리소스를 생성하도록 허가되는 것을 보증하기 위해 검사한다. 9에서, H-CSE는 성공 메시지로 응답한다. 10을 참조하면 소정 시점에서 클라이언트(AE2)가 R1을 검색하려고 할 수 있다. 클라이언트는 R1을 검색하라는 요청을 HCSE에 보낼 수 있다. 일부 경우에, AE2가 R1의 보안 버전 위치를 발견할 수 있을 수 있다. 일부 경우에 AE2는 무결성 관점에서 덜 보증된 R1의 낮은 보안성의 버전을 발견할 수 있다. 이 요청은 DTLS 또는 TLS를 기반으로 상호 인증이 수행된 후 보안 채널을 통해 송신될 수 있다. AE2는 리소스 R1에 대해 "검색" 동작을 수행하라는 요청을 송신할 수 있다. 11에서, 도시된 예에 따라, HCSE는 AE1에 의해 생성된 ACP 내의 정보를 사용하여 AE2가 검색 동작을 수행할 수 있는지 여부에 대해 허가를 확인한다. 12에서 HCSE는 EC-R1, EC-AT 및 R1-CryptoParams를 포함하는 응답을 송신한다. EC-R1은 예로서 JSON 기반 표기법(예를 들어, JWE)을 사용하여 표현될 수 있고 EC-AT는 JWS를 사용하여 표현될 수 있으며 R1-CryptoParams는 JWA를 사용하여 표현될 수 있다. 대안적으로, 특히 예로서, 암호화 및 무결성 보호를 위해 사용된 알고리즘이 AEAD 알고리즘(예로서, AES-GCM 또는 AES-CCM)에 기초하는 경우, EC-AT 및 EC-R1은 모두 JWE로 표현될 수 있다. 대안적으로, 암호화된 콘텐츠인 EC-R1 및 R1-AT는 적절한 CryptoParams와 함께 oneM2M 리소스로 표현될 수 있다.

[0163] 13에서, 도시된 예에 따르면, Credential-Id가 CryptoParams의 일부로서 포함되면, AE2는 Credential-Id를 그로부터 추출한다. 14에서, AE2는 예로서, Credential-Id를 메시지 내의 리소스-id로서 포함시킴으로써 검색 동작을 수행하기 위해 TEF에 요청 메시지를 송신한다. AE2와 TEF는 서로를 상호 인증할 수 있으며 TLS 또는 DTLS를 사용하여 보안 통신 채널을 확립할 수 있다. Credential-Id는 JSON 기반 표기법(예를 들어, JWK)을 사용하거나 oneM2M 리소스 구조를 사용하여 송신할 수 있다. AE2는 또한 리소스 R1(데이터)과 연관된 CryptoParams에서 Salt 또는 Nonce를 추출할 수 있다. AE2는 Credential-Id와 함께 Salt 또는 Nonce를 송신하여 리소스 특정 자격증명을 검색할 수도 있다.

[0164] 15에서 TEF는 2의 자격증명 등록 프로세스에서 AE1에 의해 생성된 ACP를 기반으로 AE2의 허가를 확인한다. 16에서 AE2가 검색할 허가가 있는 경우 TEF는 리소스 특정 자격증명을 계산하고 보안 채널을 통해 자격증명을 AE2에 송신한다. 또한 TEF는 자격증명의 사용 방법 및 사용할 수 있는 관련 알고리즘을 나타내는 사용법 정보를

송신할 수 있다. 일부 경우에, AE2가 이미 CryptoParams의 일부로 HCSE에서 얻은 사용법 정보를 소유하고 있을 수 있다. 그러나 컨테이너에 다수의 contentInstance 리소스가 포함될 수 있는 경우(그리고, 각 리소스는 자체 암호화된 contentInstance, 인증 태그, 자격증명과 연계될 수 있음), TEF는 contentInstance 무결성을 확인하고 contentInstances를 해독하는 데 자격증명이 사용되는 방식에 대한 추가 지침을 제공할 수 있다. Salt가 송신되는 예에서, TEF는 K_AE1_TEF_data_sec_master을 생성할 수 있으며, 이는 그후 AE2에 제공될 수 있다. 일 예에서, AE2는 K_AE1_TEF_data_sec_master을 사용하여 컨테이너 특정 또는 contentInstance 특정 자격증명을 생성한다. K_AE1_TEF_data_auth 및 K_AE1_TEF_data_conf(그리고 연관된 컨테이너 또는 contentInstance 특정 자격증명)를 생성하는 메커니즘은 위에서 설명한 메커니즘에 따라 구현될 수 있다. 여기서, K_AE1_TEF_data_sec_master을 프로비저닝하는 것의 이점은 AE1에 의해 새로운 콘텐츠 인스턴스가 생성되는지 여부에 관계없이 K_AE1_TEF_data_sec_master과 연관된 자격증명 라이프타임이 만료되지 않는 한 AE2가 TEF에 접촉할 필요가 없을 수 있다는 것이다. AE2는 AE2가 단계 12에서 수행한 리소스 검색 프로세스의 일부로 얻는 CryptoParams를 사용하여 K_AE1_TEF_data_sec_master에서 컨테이너 또는 contentInstance 특정 자격증명을 생성할 수 있다. 일부 경우에 K_AE1_TEF_data_sec_master을 프로비저닝하는 것은 예로서 AE1에 의해 생성된 모든 콘텐츠 및 인스턴스와 같은 콘텐츠 및 인스턴스에 대한 AE2 암호화 액세스를 제공할 수 있다. 따라서, 여기서, 이 프로비저닝은 일부 경우에는 바람직한 접근법이 아니라는 점이 인식된다.

[0165] 다른 예시적인 실시예에서, TEF는 AE2에 K_AE1_TEF_data_auth 및/또는 K_AE1_TEF_data_conf를 프로비저닝할 수 있으며, AE2는 컨테이너 특정 또는 contentInstance 특정 자격증명을 생성한다. 다른 경우 TEF는 AE2에만 컨테이너 특정 또는 contentInstance 특정 자격증명을 프로비저닝할 수 있다. 일부 경우 AE2는 키를 프로비저닝받기 때문에 어떠한 키 생성도 수행하지 않을 수 있고, 그에 의해, AE2의 특정 컨테이너 또는 contentInstance(들)에 대한 암호화 액세스를 제한한다. 일부 경우에 각 키에 대해 관련 Nonce(들), 컨테이너와 관련된 생성 시간 또는 콘텐츠 인스턴스를 TEF에 제공해야 할 수 있다. 일부 경우에 AE1이 4에서 자격증명 프로세스의 등록을 수행할 때, AE1은 Credential-Id와 연관된 CryptParams를 TEF에 포함시킬 수 있다.

[0166] 성능 및 보안 관점에서, TEF가 AE2에 K_AE1_TEF_data_auth 및/또는 K_AE1_TEF_data_conf만을 프로비저닝할 수 있는 접근법이 있을 수 있음이 여기에서 인식된다. 자격증명에는 각각 관련 라이프 타임이 있을 수 있다. 라이프타임 만료 후 새 자격증명이 생성되어야 할 수 있다.

[0167] 17에서, 도시된 예에 따라 자격증명을 사용하여 AE2는 R1-AT를 사용하여 무결성을 확인하고 프로비저닝된 또는 생성된 컨테이너 또는 contentInstance 자격증명을 사용하여 R1을 해독한다.

[0168] 대안적 실시예에서, 노드(예로서, AE1)는 특정 클라이언트(예로서, AE2)에 의한 소비에 대해 보호될 수 있는 클라이언트-특정 "보호된" 콘텐츠를 생성한다. oneM2M에서 AE는 서로 인증하기 위해 직접 통신하지 않기 때문에 CSE는 AE1을 대신하여 클라이언트 특정 보호를 수행하여 클라이언트 특정(예를 들어, AE2) 보호된 콘텐츠가 생성되어 CSE에서 호스팅된다. 대안적으로, CSE가 AE1을 대신하여 보안 기능을 수행하는 본 명세서에서 설명된 유사한 메커니즘은 CSE1에 의존할 필요없이 AE1 자체에 의해 수행될 수 있다. 클라이언트-특정 보호 콘텐츠 실시예가 도 38에 도시되어 있으며, 이를 이제 이하에서 설명할 것이다.

[0169] 전술한 바와 같이, 도 38은 클라이언트-특정 콘텐츠 보호 실시예를 도시한다. 도 38을 참조하면, 도시된 실시예에 따르면, 0에서, AE1은 (D)TLS를 사용하여 HCSE와 상호 인증된다. 유사하게 AE2는 (D)TLS를 사용하여 HCSE와 상호 인증되었다.

[0170] 1에서, 도시된 예에 따라, AE1은 콘텐츠(데이터) 및/또는 contentInstances를 생성한다. 또한 AE1은 호스팅 CSE에 의해 콘텐츠의 무결성 및/또는 기밀성에 대해 보호된다. 2에서 AE1은 고유한 클라이언트 특정 자격증명을 사용하여 콘텐츠가 각 특정 클라이언트에 대해 무결성 및/또는 기밀성에 대해 보호되도록 요청한다. 3에서, HCSE는 AE1에 의해 제공된 ACP를 처리하고, 보안 콘텐츠에 대해 CRUD 동작을 수행할 허가된 클라이언트(예컨대, AE2)를 결정한다. 또한 HCSE는 고유한 클라이언트 특정(예를 들어, AE2 특정) 자격증명을 생성해야 한다고 결정한다. 대안적으로, CSE1은 ACP를 결정할 수 있으며, 따라서 허가된 클라이언트를 결정할 수 있다. 또는 일부 경우에 AE1에서 제공하는 ACP를 서비스 공급자가 제공한 ACP와 결합하여 콘텐츠에 대해 CRUD 동작, 특히 "검색" 동작을 수행할 수 있는 허가된 클라이언트를 결정한다. 이 예에 따르면, AE2가 승인된 클라이언트이고 AE1에 의해 허가되었다고 가정하면, HCSE는 oneM2M TS-0003 사양(릴리스 1)에 따라 Kpsa_HCSE_AE2를 원격 프로비저닝 또는 부트스트래핑한 결과로서 프로비저닝되거나 생성된 사전 공유 키를 이용하여 K_HCSE_AE2_data_sec_master을 생성한다. 데이터 보안에 사용되는 마스터 키 K_HSCE_AE2_data_sec_master은 키 확장 메커니즘, 예를 들어, RFC 5869을 사용하여 생성될 수 있다:

[0171] * K_ HCSE _AE2_data_sec_master = HMAC-Hash (Salt, Kpsa_ HCSE _AE2)

[0172] * T(0) = 빈 스트링(길이 0)

[0173] 4에서 K_HCSE_AE2_data_sec_master이 생성되면 키 확장에 사용되어 고유한 데이터 신뢰성 및 데이터 기밀성 키를 생성할 수 있다. 일부 경우에 예로서 AEAD와 같은 알고리즘(예를 들어, AES-CCM 또는 AES-GCM)에 의해 데이터 신뢰성 및 기밀성이 제공되는 경우 단일 키만 생성된다. 예로서, 키는 다음과 같이 생성될 수 있다:

[0174] * K_HCSE_AE2_data_auth = T (1) = HMAC-Hash (K_HCSE_AE2_data_sec_master, T (0) | "데이터 신뢰성 및 무결성"| 0x01)

[0175] * K_HCSE_AE2_data_auth 키는 데이터 신뢰성 및 데이터 무결성을 제공하는 데 사용되며 데이터 신뢰성 또는 데이터 무결성 키라고 지칭될 수 있다.

[0176] * K_HCSE_AE2_conf = T (2) = HMAC-Hash (K_HCSE_AE2_data_sec_master, T (1) | "데이터 기밀성 키"| 0x02)

[0177] 예로서 여러 콘텐츠 인스턴스가 포함될 수 있는 컨테이너에 대해 단일 데이터 신뢰성 및 데이터 기밀성 키만을 위한 키 생성이 예시의 목적을 위해 아래에 나타나 있다:

[0178] * K_HCSE_AE2_Container-x_data_auth = HMAC-Hash (K_HCSE_AE2_data_auth, "데이터 신뢰성 및 무결성"| "Container-x"| Nonce 또는 creationTime) 및

[0179] * K_HCSE_AE2_Container-x_data_conf = HMAC-Hash (K_HCSE_AE2_data_conf, "데이터 기밀성"| "Container-x"| Nonce 또는 creationTime)

[0180] 대안적으로, 컨테이너 내의 각 콘텐츠 인스턴스에 대해, 아래에 도시된 바와 같이, 고유한 키 세트가 생성될 수 있다:

[0181] * K_HCSE_AE2_ContentInstance-x_data_auth = HMAC-Hash (K_HCSE_AE2_data_auth, "데이터 신뢰성 및 무결성"| "Container-x"| Nonce 또는 creationTime) 및

[0182] * K_HCSE_AE2_ContentInstance-x_data_conf = HMAC-Hash (K_HCSE_AE2_data_conf, "데이터 기밀성"| "ContentInstance"| Nonce 또는 creationTime)

[0183] 대안적으로 공개 키 메커니즘이 사용되는 경우 클라이언트 특정 자격증명은 아이덴티티 기반 암호화(IBE; Identity-Based Encryption) 메커니즘을 기반으로 할 수 있다.

[0184] 도 38을 참조하면, 5에서, 도시된 예에 따라, AE2는(소정 시점에서) HCSE로부터 리소스 R1(컨테이너 또는 contentInstance(들))을 "검색"하도록 요청한다. 6에서 HCSE는 AE2의 허가를 확인한다. 7에서 HCSE는 암호화된 콘텐츠 EC-R1, 인증 태그, R1-AT 및 관련 CryptoParams로 응답한다. 8에서 AE2는 CryptoParams를 사용하고 K_HCSE_AE2_data_sec_master을 생성하기 위해 UsageInfo와 "Salt"를 추출한다. 또한, AE2는 생성을 위해 요구되는 Nonces 및 다른 파라미터들을 추출한다: K_HCSE_AE2_data_conf, K_HCSE_AE2_data_auth 등. 그 다음, AE2는 컨테이너/contentInstances 내의 데이터의 신뢰성 및 무결성을 확인하기 위해 컨테이너-특정 및 contentInstance(들) 키를 생성하고, 컨테이너 내의 데이터 또는 각 containerInstances 내에 포함된 데이터를 해독한다.

[0185] 따라서, 37 및 도 38을 참조하면, 도시된 노드들은 프로세서, 메모리 및 통신 회로를 포함할 수 있다. 노드는 그 통신 회로를 통해 네트워크에 접속될 수 있고, 노드는 노드의 프로세서에 의해 실행될 때 노드가 도시되고 설명된 단계를 수행하게 하는 노드의 메모리에 저장된 컴퓨터 실행 가능 명령을 더 포함할 수 있다.

[0186] 도 27은 예시적인 Credential-Id 리소스를 도시한다. 도시된 바와 같이, 예시적인 Credential-Id 리소스는 자체적으로 자격증명-AT를 사용하여 무결성 보호되고, 이 자격증명-AT는 생성자의 자격증명(예를 들어, AE1의 개인 키) 또는 SCHF(예를 들어, H-CSE)에 의해 Credential-Id 리소스의 생성자에 의해 생성될 수 있다. 예시적인 속성들의 세부 사항이 이제 설명되고 제한이 아닌 예로서 제시된다:

[0187] * Credential-Id: 이는 도메인 내의 자격증명을 고유하게 식별한다. 이는 전역적으로 고유하거나 로컬적으로 고유할 수 있으며 일반적으로 자격증명의 범위를 기반으로 한다. 이는 무작위이지만 고유한 값을 접두사로서, 그리고, 접미사로서 FQDN을 사용(예를 들어, xyz@credentials.example.com)하는 형식일 수 있거나 URI 형식(예를 들어, //example.com/credentials/xyz)일 수 있다.

[0188] * 자격증명: 이는 자격증명에 특정한 자식 리소스 속성으로 구성된다. 속성들은 다음과 같다:

[0189] o credetialType: 자격증명의 유형, 즉 대칭 키 또는 공개 키를 설명한다. 이는 또한 공개 키의 유형(예를 들어, RSA 또는 ECC)을 지정할 수도 있다.

[0190] o 자격증명: 속성은 실제 자격증명 값(예를 들어, 대칭 키 또는 공개 키)을 저장한다. 참고: 자격증명의 크기는 자격증명 유형에 의존할 수 있다. 키가 공개 키인 경우, 다음과 연계될 수 있다:

[0191] · publicKeyParams: 파라미터는 JWK 파라미터일 수 있거나 (예를 들어, 사용된 곡선의 유형, 키 크기) 및/또는 그를 기반으로 할 수 있다. 이는 선택 사항일 수 있다.

[0192] * accessControlPolicy: oneM2M에 정의된 ACP를 기반으로 한 예시적인 ACP는 세 개의 속성들을 갖는다: accessControlOriginators, accessControlOperations 및 accesControlContexts.

[0193] * scopeUsage: 이 속성은 범위(예를 들어, 서명 또는 암호화, 키 생성 프로세스)를 정의한다. 또한 자격증명 사용법에 대한 사용법을 제공할 수도 있다. 자격증명 사용 규칙.

[0194] * 유효성: 유효성 속성은 자격증명과 관련된 라이프타임을 나타내는 데 사용될 수 있다. 자격증명은 갱신되어야 할 수 있고 정책에 기반하여 CLMP가 개시될 수 있다.

[0195] * 발급자: 자격증명을 생성하고 발급한 엔티티의 아이덴티티(예를 들어, FQDN).

[0196] * 자격증명-AT: 이 속성은 도 30에서 설명된 연관된 cryptoParams 하위 리소스를 사용하여 자격증명 리소스(자격증명-AT 속성을 제외한 모든 속성을 포함)에 대해 계산된 AT 값을 저장할 수 있다.

[0197] 무결성 보호된 일반 ACP의 예시적인 실시예가 도 28에 도시되어 있다. 도시된 ACP에는 cryptoParams가 공개 키 메커니즘을 사용하도록 지정하는 경우 AE의 개인 키를 사용하여 생성된 연관 AT가 있다. ACP를 생성하는 임의의 엔티티가 ACP를 생성 및 인증/무결성 보호할 수도 있다. 따라서 ACP가 CSE에 의해 생성된 경우, 생성된 AT는 CryptoParams가 공개 키 메커니즘을 사용해야 하는 경우 CSE의 개인 키를 기반으로 한다.

[0198] 도 29는 cryptoParams 리소스 내에 기술된 암호화 알고리즘 및 특정 자격증명(예로서, 대칭 키)을 사용하여 기밀성 보호된(EC-contentInfo) contentInstance의 예를 도시한다. 또한 이는 공개 키잉 메커니즘(예를 들어, 콘텐츠 생성기의 개인 키) 또는 마스터 키(예를 들어, KeyGenKey)에서 생성된 대칭 키를 사용하여 생성된 DS 또는 MAC(예를 들어, 콘텐츠-AT 속성에 저장됨)을 통해 무결성 보호될 수 있다.

[0199] cryptoParams 리소스와 관련된 예가 도 30에 도시되어 있다. cryptoParams 리소스와 관련된 예시적인 속성에 관한 세부 사항이 아래에 제공되며, 이는 제한이 아닌 예로서 제시되어 있다:

[0200] * cryptoParamsId: 이는 보호 대상 콘텐츠/데이터와 관련된 암호화 파라미터를 고유하게 식별하는 데 사용할 수 있는 선택적 속성이다.

[0201] * 기밀성: 암호화 프로세스와 관련된 파라미터를 설명하는 하위 리소스 유형이다. 예시적인 속성은 다음과 같다:

[0202] o 알고리즘: 사용할 암호화 알고리즘을 설명한다(예를 들어, AES-128).

[0203] o Credential-Id: 콘텐츠(예로서, 원심 분리기 온도)를 암호화하는 데 사용되는 자격증명(예로서, 키)을 검색하는 데 사용되는 Credential-Id를 설명한다.

[0204] o initializationVector: 해당 특정 알고리즘에 대한 콘텐츠 암호화/해독에 사용되어야 하는 IV를 설명한다.

[0205] o scopeUsage: 이는 콘텐츠/리소스를 암호화 또는 해독하기 위해 자격증명, IV 및 알고리즘의 사용법 및 범위를 설명할 수 있는 선택적 속성이다

[0206] * 무결성: 콘텐츠/리소스 무결성 보호와 관련된 파라미터를 설명하는 하위 리소스이다. 속성들은 다음과 같다:

[0207] o digestAlgorithm: 다이제스트(예를 들어, SHA-1)를 생성하기 위해 사용되는 알고리즘.

[0208] o signingAlgorithm: 공개 키의 경우 다이제스트에 디지털 서명을 하기 위해 사용되는 알고리즘으로 적절한 알고리즘(예를 들어, RSA)이 사용될 수 있는 반면 대칭 키의 경우 적절한 알고리즘이 사용될 수 있

다(예를 들어, HMAC-SHA-1). 대칭 키의 경우 digestAlgorithm이 Keyed-Hash-MAC 알고리즘(예를 들어, HMAC-SHA-256)으로 대체될 수 있다. 여기에 설명된 예제는 공개 키 메커니즘을 사용하지만 비슷한 메커니즘이 대칭 키에 사용될 수 있다.

[0209] o Credential-Id: 콘텐츠/리소스와 관련된 AT를 생성하기 위한 자격증명(예를 들어, 키)을 검색하는 데 사용되는 Credential-Id(예를 들어, cred2@verisign.com)를 설명한다.

[0210] o 난스: 이 값은 재생 보호에 사용되며 무작위 생성된 값 또는 콘텐츠/리소스 생성과 관련된 시간/날짜를 포함할 수 있다.

[0211] o scopeUsage: 이는 콘텐츠/리소스의 AT를 생성하기 위해 자격증명, 난스 및 알고리즘의 사용법을 기술할 수 있는 선택적 속성이다.

[0212] * crtypotoParams-AT: 이는 관련 cryptoParams 하위 리소스를 사용하여 cryptoParamsId: cp_tem_cent_30_20/10/15로 식별되는 cryptoParams 리소스와 연결된 AT이다.

[0213] 무결성 및 신뢰성에 대해 보호된 <mgmtObj> 리소스의 예가 도 31에 도시되어 있다. 예시적인 보안 정책 리소스가 도 32에 도시되어 있다.

[0214] 예시적인 실시예에 따르면, 콘텐츠 보안과 관련된 정책 및 보안 파라미터의 구성은 그래픽 사용자 인터페이스(GUI)를 사용하여 사용자에 의해 수행될 수 있다. 대안적으로, GUI 대신 또는 그에 추가로 웹 인터페이스를 사용할 수 있다. 예시적인 사용자 인터페이스(UI)가 도 33에 도시되어 있다. 예로서, 제한적이지 는 않지만, UI는 다음을 위해 사용될 수 있다:

[0215] * 콘텐츠 보안과 관련된 보안 정책들의 구성

[0216] * 사용자에게 다음과 같은 능력을 제공:

[0217] o 어떤 것이 콘텐츠를 구성하는지를 정의

[0218] o 콘텐츠의 구조 정의

[0219] * 콘텐츠/콘텐츠 유형을 기반으로 보안 요구 사항 정의

[0220] * 사용자가 관련 보안 파라미터에 보안 요구 사항을 구성/매핑할 수 있도록 사용자가 사용할 수 있는 테이블을 디스플레이

[0221] * 콘텐츠 라이프 사이클 파라미터(특히 보안 파라미터)의 구성

[0222] * 신뢰할 수 있는 SCHF를 식별하는 데 사용되는 파라미터 정의

[0223] 다양한 UI가 SCHF에서 제공될 수 있다. 도 34는 SCHF에서 제공될 수 있는 예시적인 UI를 도시한 것으로, 제한 없이 예로서 제시 다음을 포함한다:

[0224] * 콘텐츠 보안과 관련된 보안 정책 구성을 위한 UI

[0225] * 콘텐츠 라이프 사이클 파라미터(특히 보안 파라미터) 구성을 위한 UI

[0226] * 그 (SCHF) 신뢰도를 정의하는 데 사용되는 파라미터를 정의하기 위한 UI

[0227] 도 35는 SEF에서 제공될 수 있는, 제한이 아닌 예로서 제시된 예시적인 UI를 예시하며:

[0228] * 콘텐츠 보안 관련 자격증명 요청 및 등록과 관련된 보안 정책 구성을 위한 UI

[0229] * 자격증명 관련 파라미터 구성을 위한 UI

[0230] 예시적인 사용자 인터페이스는 필요에 따라 대안적 파라미터를 모니터링하고 제어하는데 사용될 수 있다는 것을 이해할 것이다. GUI가 다양한 차트 또는 대안적인 시각적 도식을 통해 사용자가 관심을 갖는 다양한 정보를 사용자에게 제공할 수 있음을 추가로 이해할 것이다.

[0231] 도 36a는 하나 이상의 개시되는 실시예들이 구현될 수 있는 예시적인 M2M(machine-to-machine), IoT(Internet of Things), 또는 WoT(Web of Things) 통신 시스템(10)의 도면이다. 일반적으로, M2M 기술들은 IoT/WoT에 대한 빌딩 블록들을 제공하고, 임의의 M2M 디바이스, M2M 게이트웨이, 또는 M2M 서비스 플랫폼은 이러한 IoT/WoT는 물론이고 IoT/WoT 서비스 레이어 등의 컴포넌트일 수 있다. 도 6 내지 도 35, 도 37 및 도 38에 도시된 임

의의 클라이언트 또는 엔티티들은 도 36a 내지 도 36d에 도시된 것 같은 통신 시스템의 노드를 포함할 수 있다.

[0232] 도 36a에 도시되는 바와 같이, M2M/IoT/WoT 통신 시스템(10)은 통신 네트워크(12)를 포함한다. 통신 네트워크(12)는 고정 네트워크(fixed network)(예컨대, 이더넷, 파이버(Fiber), ISDN, PLC 등) 또는 무선 네트워크(wireless network)(예컨대, WLAN, 셀룰러 등) 또는 이종 네트워크(heterogeneous network)들의 네트워크일 수 있다. 예를 들어, 통신 네트워크(12)는 음성, 데이터, 비디오, 메시징, 방송 등과 같은 콘텐츠를 다수의 사용자들에게 제공하는 다수의 액세스 네트워크들로 구성될 수 있다. 예를 들어, 통신 네트워크(12)는, CDMA(code division multiple access), TDMA(time division multiple access), FDMA(frequency division multiple access), OFDMA(orthogonal FDMA), SC-FDMA(single-carrier FDMA) 등과 같은, 하나 이상의 채널 액세스 방법들을 이용할 수 있다. 게다가, 통신 네트워크(12)는, 예를 들어, 코어 네트워크, 인터넷, 센서 네트워크, 산업 제어 네트워크(industrial control network), 개인 영역 네트워크(personal area network), 융합 개인 네트워크(fused personal network), 위성 네트워크, 홈 네트워크, 또는 엔터프라이즈 네트워크와 같은 다른 네트워크들을 포함할 수 있다.

[0233] 도 36a에 도시되는 바와 같이, M2M/IoT/WoT 통신 시스템(10)은 인프라스트럭처 도메인(Infrastructure Domain) 및 필드 도메인(Field Domain)을 포함할 수 있다. 인프라스트럭처 도메인은 종단간 M2M 배치(end-to-end M2M deployment)의 네트워크측을 지칭하고, 필드 도메인은, 보통 M2M 게이트웨이 후방에 있는, 영역 네트워크(area network)들을 지칭한다. 필드 도메인 및 인프라스트럭처 도메인은 양자 모두 다양하고 상이한 네트워크 노드들(예를 들어, 네트워크의 서버들, 게이트웨이들, 디바이스)를 포함할 수 있다. 예를 들어, 필드 도메인은 M2M 게이트웨이들(14) 및 단말 디바이스들(18)을 포함할 수 있다. 원하는 바에 따라, 임의의 수의 M2M 게이트웨이 디바이스들(14) 및 M2M 단말 디바이스들(18)이 M2M/IoT/WoT 통신 시스템(10)에 포함될 수 있다는 것을 잘 알 것이다. M2M 게이트웨이 디바이스들(14) 및 M2M 단말 디바이스들(18) 각각은 통신 네트워크(12) 또는 직접 무선 링크를 통해 신호들을 송신 및 수신하도록 구성된다. M2M 게이트웨이 디바이스(14)는 무선 M2M 디바이스들(예를 들어, 셀룰러 및 비-셀룰러)뿐만 아니라 고정형 네트워크 M2M 디바이스들(예를 들어, PLC)가 통신 네트워크(12) 또는 직접 무선 링크와 같은 오퍼레이터 네트워크들을 통해서 통신하게 한다. 예를 들어, M2M 단말 디바이스들(18)은 통신 네트워크(12) 또는 직접 무선 링크를 통해 데이터를 수집할 수 있고, M2M 애플리케이션(20) 또는 다른 M2M 디바이스들(18)에 데이터를 보낼 수 있다.]M2M 디바이스들(18)은 또한 M2M 애플리케이션(20) 또는 M2M 디바이스(18)로부터 데이터를 수신할 수 있다. 게다가, 이하에서 기술되는 바와 같이, 데이터 및 신호들이 M2M 서비스 레이어(22)를 통해 M2M 애플리케이션(20)에게 송신되고 그로부터 수신될 수 있다. M2M 디바이스들(18) 및 게이트웨이들(14)은, 예를 들어, 셀룰러, WLAN, WPAN(예를 들어, Zigbee, 6LoWPAN, Bluetooth), 직접 무선 링크, 및 유선을 포함하는 다양한 네트워크들을 통해 통신할 수 있다. 예시적인 M2M 디바이스들은, 이에 제한되는 것은 아니지만, 태블릿들, 스마트 폰들, 의료 기기들, 온도 및 날씨 모니터들, 접속된 차량들, 스마트 미터들, 게임 콘솔들, 개인 휴대 정보 단말기들, 건강 및 운동 모니터들, 조명들, 온도 조절기들, 가전제품들, 차고 문들 및 기타 액추에이터 기반 디바이스들, 보안 디바이스들, 및 스마트 아웃렛들을 포함한다.

[0234] 도 36b를 참조하면, 도시된 M2M 서비스 레이어(22)는 필드 도메인에서 M2M 애플리케이션(20), M2M 게이트웨이 디바이스들(14), 및 M2M 단말 디바이스들(18) 및 통신 네트워크(12)에 대한 서비스들을 제공한다. M2M 서비스 레이어(22)는 원하는 대로 임의의 수의 M2M 애플리케이션들, M2M 게이트웨이 디바이스들(14), M2M 단말 디바이스들(18), 및 통신 네트워크들(12)과 통신할 수 있다는 점이 이해될 것이다. M2M 서비스 레이어(22)는 하나 이상의 서버들, 컴퓨터들 등에 의해 구현될 수 있다. M2M 서비스 레이어(22)는 M2M 단말 디바이스들(18), M2M 게이트웨이 디바이스들(14), 및 M2M 애플리케이션들(20)에 적용되는 서비스 능력들을 제공한다. M2M 서비스 레이어(22)의 기능들은 각종의 방식들로, 예를 들어, 웹 서버로서, 셀룰러 코어 네트워크에, 클라우드에, 기타로 구현될 수 있다.

[0235] 도시되는 M2M 서비스 레이어(22)과 유사하게, 인프라스트럭처 도메인에는 M2M 서비스 레이어(22')가 있다. M2M 서비스 레이어(22')는 인프라스트럭처 도메인에서 M2M 애플리케이션(20') 및 기본 통신 네트워크(12')를 위한 서비스들을 제공한다. M2M 서비스 레이어(22')는 또한 필드 도메인에서 M2M 게이트웨이 디바이스들(14) 및 M2M 단말 디바이스들(18)에 대한 서비스들을 제공한다. M2M 서비스 레이어(22')는 임의 수의 M2M 애플리케이션들, M2M 게이트웨이 디바이스들 및 M2M 단말 디바이스들과 통신할 수 있다는 점이 이해될 것이다. M2M 서비스 레이어(22')는 상이한 서비스 제공자에 의해 서비스 레이어와 상호작용할 수 있다. M2M 서비스 레이어(22')는 하나 이상의 서버들, 컴퓨터들, 가상 머신들(예를 들어, 클라우드/계산/스토리지 팜들, 기타 등등) 또는 이와 유사한 것에 의해 구현될 수 있다.

[0236] 도 36b를 계속 참조하면, M2M 서비스 레이어(22 및 22')는 다양한 애플리케이션들 및 버티컬들이 영향력을 행사

할 수 있는 서비스 전달 능력들의 코어 세트를 제공한다. 이러한 서비스 능력들은 M2M 애플리케이션들(20, 20')이 디바이스들과 상호작용하고 또한 데이터 수집, 데이터 분석, 디바이스 관리, 보안, 과금, 서비스/디바이스 발견 등과 같은 기능들을 수행하는 것을 가능하게 한다. 본질적으로, 이 서비스 능력들은 애플리케이션들로부터 이 기능들을 구현하는 부담을 덜어주고, 따라서 애플리케이션 개발을 단순화시키며 출시까지의 비용 및 시간을 감소시킨다. 서비스 레이어(22 및 22')는 또한 M2M 애플리케이션들(20 및 20')이 서비스 레이어(22 및 22')가 제공하는 서비스들과 관련하여 다양한 네트워크들(12 및 12')을 통해 통신하는 것을 가능하게 한다.

[0237] M2M 애플리케이션들(20 및 20')은, 이에 제한되는 것은 아니지만, 운송, 건강 및 건강관리, 접속된 홈, 에너지 관리, 자산 추적, 및 보안과 감시와 같은 다양한 산업들에서의 애플리케이션들을 포함할 수 있다. 위에 언급된 바와 같이, 시스템의 디바이스들, 게이트웨이들 및 다른 서버들에 걸쳐 실행되는 M2M 서비스 레이어는, 예를 들어, 데이터 수집, 디바이스 관리, 보안, 과금, 위치 추적/지오펜싱(geofencing), 디바이스/서비스 발견, 및 레거시 시스템들 통합과 같은 기능들을 지원하고, 이러한 기능들을 서비스들로서 M2M 애플리케이션들(20, 20')에 제공한다.

[0238] 일반적으로, 도 36a 및 도 36b에 도시되는 서비스 레이어들(22 및 22')과 같은 서비스 레이어(SL)는 API들(Application Programming Interfaces) 및 기본 네트워킹 인터페이스들의 세트를 통해 부가 가치 서비스 능력들을 지원하는 소프트웨어 미들웨어 레이어를 정의한다. ETSI M2M 아키텍처와 oneM2M 아키텍처 둘 다는 서비스 레이어를 정의한다. ETSI M2M의 서비스 레이어는 SCL(Service Capability Layer)이라고 지칭된다. SCL은 ETSI M2M 아키텍처의 각종의 상이한 노드들에 구현될 수 있다. 예를 들어, 서비스 레이어의 인스턴스는 M2M 디바이스(여기서 이는 디바이스 SCL(DSCL)이라고 지칭됨), 게이트웨이(여기서 이는 게이트웨이 SCL(GSCL)이라고 지칭됨), 및/또는 네트워크 노드(여기서 이는 네트워크 SCL(NSCL)이라고 지칭됨) 내에 구현될 수 있다. oneM2M 서비스 레이어는 한 세트의 CSF(Common Service Function)들(즉, 서비스 능력들)을 지원한다. CSF들 중의 한 세트의 하나 이상의 특정 타입들의 인스턴스화는 상이한 타입들의 네트워크 노드들(예를 들어, 인프라스트럭처 노드, 중간 노드, 애플리케이션 특정적 노드)상에서 호스팅될 수 있는 CSE(Common Services Entity)로서 지칭된다. 3GPP(Third Generation Partnership Project)는 또한 MTC(machine-type communications)에 대한 아키텍처도 정의하였다. 그 아키텍처에서, 서비스 레이어와, 서비스 레이어가 제공하는 서비스 능력들이 서비스 능력 서버(Service Capability Server, SCS)의 일부로서 구현된다. ETSI M2M 아키텍처의 DSCL, GSCL 또는 NSCL에서, 3GPP MTC 아키텍처의 SCS(Service Capability Server)에서, 또는 oneM2M 아키텍처의 CSF 또는 CSE에서, 또는 네트워크의 일부 다른 노드에서 중 어디에서 구현되든 간에, 서비스 레이어의 인스턴스는 서버들, 컴퓨터들, 및 다른 컴퓨팅 디바이스들 또는 노드들 포함하는, 네트워크에서의 하나 이상의 독립형 노드들 상에서 또는 하나 이상의 기존 노드들의 일부 상에서 실행되는 논리적 엔티티(예를 들어, 소프트웨어, 컴퓨터 실행가능 명령어들 등)에서 구현될 수 있다. 예를 들어, 서비스 레이어 또는 그 컴포넌트의 인스턴스는 이하 설명되는 도 36c 또는 도 36d에 도시되는 일반적인 아키텍처를 갖는 네트워크 노드(예를 들어, 서버, 컴퓨터, 게이트웨이, 디바이스 등) 상에서 실행되는 소프트웨어 형태로 구현될 수 있다.

[0239] 또한, 본 명세서에 설명된 방법 및 기능은 예로서 전술한 네트워크 및 애플리케이션 관리 서비스 및 서비스와 같은 서비스들에 액세스하기 위해 서비스 지향 아키텍처(SOA) 및/또는 리소스 지향 아키텍처(ROA)를 사용하는 M2M 네트워크의 일부로서 구현될 수 있다.

[0240] 도 36c는 도 36a 및 도 36b에 도시되는 것 같은 M2M 네트워크에서 M2M 서버, 게이트웨이, 디바이스 또는 다른 노드로서 동작할 수 있는 도 6 내지 도 35, 도 37 및 도 38에 도시되는 클라이언트들 또는 엔티티들 중 하나같은 네트워크의 노드의 예시적 하드웨어/소프트웨어 아키텍처의 블록도이다. 도 36c에 도시되는 바와 같이, 노드(30)는 프로세서(32), 송수신기(34), 송신/수신 엘리먼트(36), 스피커/마이크로폰(38), 키패드(40), 디스플레이/터치 패드(42), 비-이동식 메모리(44), 이동식 메모리(46), 전원(48), GPS(global positioning system) 칩셋(50), 및 다른 주변기기들(52)을 포함할 수 있다. 노드(30)는 또한 송수신기(34) 및 전송/수신 엘리먼트(36)와 같은 통신 회로를 포함할 수 있다. 노드(30)는 실시예와 일관성을 유지하면서 전술한 엘리먼트들의 임의의 부분 조합을 포함할 수 있다는 점이 이해될 것이다. 이 노드는 여기에 설명된 보안 보호 및 방법을 구현하는 노드일 수 있다.

[0241] 프로세서(32)는 범용 프로세서, 특수 목적 프로세서, 종래의 프로세서, DSP(digital signal processor), 복수의 마이크로프로세서들, DSP 코어와 연관된 하나 이상의 마이크로프로세서들, 제어기, 마이크로컨트롤러, ASIC(Application Specific Integrated Circuit)들, FPGA(Field Programmable Gate Array) 회로들, 임의의 다른 유형의 IC(integrated circuit), 상태 머신 등일 수 있다. 프로세서(32)는 신호 코딩, 데이터 처리, 전력 제어, 입력/출력 처리, 및/또는 노드(30)가 무선 또는 유선 환경에서 동작할 수 있게 하는 임의의 다른 기능성

을 수행할 수 있다. 프로세서(32)는 송신/수신 엘리먼트(36)에 연결될 수 있는 송수신기(34)에 연결될 수 있다. 도 36c가 프로세서(32) 및 송수신기(34)를 별개의 컴포넌트들로서 묘사하지만, 프로세서(32) 및 송수신기(34)는 전자 패키지 또는 칩에 함께 통합될 수 있다는 점이 이해될 것이다. 프로세서(32)는 애플리케이션 레이어 프로그램들(예를 들어, 브라우저들) 및/또는 RAN(radio access-layer) 프로그램들 및/또는 통신 프로그램들을 수행할 수 있다. 프로세서(32)는 예를 들어, 액세스 레이어 및/또는 애플리케이션 레이어에서와 같이, 인증, 보안 키 합의, 및/또는 암호화 동작들과 같은 보안 동작들을 또한 수행할 수 있다.

[0242] 도 36c에 도시되는 바와 같이, 프로세서(32)는 그것의 통신 회로(예를 들어, 송수신기(34) 및 송신/수신 엘리먼트(36))에 연결된다. 프로세서(32)는, 컴퓨터 실행가능 명령어들의 실행을 통해, 노드(30)로 하여금 그에 접속되어 있는 네트워크를 통해 다른 노드들과 통신하게 하기 위해 통신 회로를 제어할 수 있다. 특히, 프로세서(32)는 본 명세서(예를 들어, 도 6 내지 도 35, 도 37 및 도 38에서) 및 청구범위에서 설명되는 송신 및 수신 단계들을 수행하도록 통신 회로를 제어할 수 있다. 도 36c가 프로세서(32) 및 송수신기(34)를 별개의 컴포넌트들로서 묘사하지만, 프로세서(32) 및 송수신기(34)는 전자 패키지 또는 칩에 함께 통합될 수 있다는 점이 이해될 것이다.

[0243] 송신/수신 엘리먼트(36)는 신호들을 M2M 서버들, 게이트웨이들, 디바이스 등을 포함하는 다른 노드들에 송신하거나, 또는 이들로부터 수신하도록 구성될 수 있다. 예를 들어, 일 실시예에서, 송신/수신 요소(36)는 RF 신호들을 전송 및/또는 수신하도록 구성된 안테나일 수 있다. 송신/수신 요소(36)는, WLAN, WPAN, 셀룰러 등과 같은, 다양한 네트워크들 및 무선 인터페이스(air interface)들을 지원할 수 있다. 실시예에서, 송신/수신 엘리먼트(36)는, 예를 들어 IR, UV, 또는 가시광 신호들을 송신 및/또는 수신하도록 구성되는 방출기/검출기일 수 있다. 또 다른 실시예에서, 송신/수신 요소(36)는 RF 및 광 신호들 둘 다를 전송 및 수신하도록 구성될 수 있다. 송신/수신 요소(36)가 무선 또는 유선 신호들의 임의의 조합을 전송 및/또는 수신하도록 구성될 수 있다는 것을 잘 알 것이다.

[0244] 또한, 송신/수신 엘리먼트(36)가 단일 엘리먼트로서 도 36c에 묘사되지만, 노드(30)는 임의의 수의 송신/수신 엘리먼트들(36)을 포함할 수 있다. 보다 구체적으로, 노드(30)는 MIMO 기술을 이용할 수 있다. 따라서, 실시예에서, 노드(30)는 무선 신호들을 송신 및 수신하기 위한 2개 이상의 송신/수신 엘리먼트들(36)(예를 들어, 다수의 안테나들)을 포함할 수 있다.

[0245] 송수신기(34)는 송신/수신 요소(36)에 의해 전송되어야 하는 신호들을 변조하도록 그리고 송신/수신 요소(36)에 의해 수신되는 신호들을 복조하도록 구성될 수 있다. 전술된 바와 같이, 노드(30)는 멀티-모드 능력들을 가질 수 있다. 따라서, 송수신기(34)는, 노드(30)가, 예를 들어, UTRA 및 IEEE 802.11과 같은 다수의 RAT들을 통해 통신할 수 있게 하기 위한 다수의 송수신기들을 포함할 수 있다.

[0246] 프로세서(32)는, 비-이동식 메모리(44) 및/또는 이동식 메모리(46)와 같은, 임의의 유형의 적당한 메모리로부터의 정보에 액세스하고 그에 데이터를 저장할 수 있다. 비-이동식 메모리(44)는 RAM(random-access memory), ROM(read-only memory), 하드 디스크, 또는 임의의 다른 유형의 메모리 저장 디바이스를 포함할 수 있다. 이동식 메모리(46)는 SIM(subscriber identity module) 카드, 메모리 스틱, SD(secure digital) 메모리 카드 등을 포함할 수 있다. 다른 실시예들에서, 프로세서(32)는 서버 또는 가정용 컴퓨터 상에서와 같이, 노드(30) 상에 물리적으로 위치되지 않은 메모리로부터 정보를 액세스할 수 있고, 거기에 데이터를 저장할 수 있다. 프로세서(32)는 UE(예로서, GUI(1400) 참조)의 상태, 그리고 특히 기본 네트워크들, 애플리케이션들 또는 UE와 통신하는 다른 서비스들을 반영하기 위해 디스플레이 또는 표시자(42) 상의 조명 패턴, 이미지 또는 컬러를 제어하도록 구성될 수 있다. 프로세서(32)는 전원(48)으로부터 전력을 수신할 수 있고, 노드(30)의 다른 컴포넌트들에게 전력을 분배 및/또는 제어하도록 구성될 수 있다. 전원(48)은 노드(30)에 전력을 공급하기 적합한 임의의 디바이스일 수 있다. 예를 들어, 전원(48)은 하나 이상의 건전지 배터리들(예컨대, 니켈-카드뮴(NiCd), 니켈-아연(NiZn), 니켈 금속 수소화물(NiMH), 리튬 이온(Li 이온) 등), 태양 전지들, 연료 전지들 등을 포함할 수 있다.

[0247] 프로세서(32)는 또한 GPS 칩셋(50)에 연결될 수 있으며, 이것은 노드(30)의 현재 위치에 관한 위치 정보(예를 들어, 경도 및 위도)를 제공하도록 구성된다. 노드(30)는 일 실시예에 부합하도록 유지되면서 임의의 적절한 위치-결정 방법에 의해 위치 정보를 취득할 수 있다는 점이 이해될 것이다.

[0248] 프로세서(32)는, 부가의 특징들, 기능 및/또는 유선 또는 무선 접속을 제공하는 하나 이상의 소프트웨어 및/또는 하드웨어 모듈들을 포함할 수 있는, 다른 주변기기들(52)에 추가로 결합될 수 있다. 예를 들어, 주변기기들(52)은 가속도계, e-나침반, 위성 송수신기, 센서, (사진 또는 비디오를 위한) 디지털 카메라, USB(universal serial bus) 포트 또는 다른 상호접속 인터페이스들, 진동 디바이스, 텔레비전 송수신기, 핸즈프리 헤드셋,

Bluetooth® 모듈, FM(frequency modulated) 무선 유닛, 디지털 음악 플레이어, 미디어 플레이어, 비디오 게임 플레이어 모듈, 인터넷 브라우저 등을 포함할 수 있다.

[0249] 도 36d는 도 36a 및 도 36b에 도시되는 것 같은 M2M 네트워크에서 M2M 서버, 게이트웨이, 디바이스 또는 다른 노드로서 동작할 수 있는 도 6 내지 도 35, 도 37 및 도 38에 도시되는 클라이언트들 또는 엔티티들 같은 네트워크의 하나 이상의 노드들을 구현하기 위해 또한 사용될 수 있는 예시적 컴퓨팅 시스템(90)의 블록도이다. 컴퓨팅 시스템(90)은 컴퓨터 또는 서버를 포함할 수 있고, 주로 컴퓨터 판독가능 명령어들 - 소프트웨어의 형태로 되어 있을 수 있고, 이러한 소프트웨어는 어느 곳에든 또는 어떤 수단에 의해서든 저장되거나 액세스됨 - 에 의해 제어될 수 있다. 이러한 컴퓨터 판독가능 명령어들은 컴퓨팅 시스템(90)으로 하여금 동작하게 하도록 CPU(central processing unit)(91) 내에서 실행될 수 있다. 많은 공지된 워크스테이션들, 서버들, 및 개인용 컴퓨터들에서, 중앙 처리 유닛(91)은 마이크로프로세서라고 불리는 단일 칩 CPU에 의해 구현된다. 다른 머신들에서, 중앙 처리 유닛(91)은 다수의 프로세서들을 포함할 수 있다. 코프로세서(81)는 추가적인 기능들을 수행하거나 또는 CPU(91)를 보조하는, 주 CPU(91)와는 별개인, 선택적 프로세서이다. CPU(91) 및/또는 코프로세서(81)는, 보안 보호를 위한 개시된 시스템들 및 방법들에 관련된 데이터를 수신, 생성 및 처리할 수 있다.

[0250] 동작에 있어서, CPU(91)는 명령어들을 페치, 디코드, 및 실행하고, 컴퓨터의 주 데이터 전송 경로인 시스템 버스(80)를 통해 다른 리소스들로 및 이로부터 정보를 송신한다. 이러한 시스템 버스는 컴퓨팅 시스템(90) 내의 컴포넌트들을 접속시키고, 데이터 교환을 위한 매체를 정의한다. 시스템 버스(80)는 전형적으로 데이터를 송신하기 위한 데이터 라인들, 주소들을 송신하기 위한 주소 라인들, 및 인터럽트들을 송신하고 시스템 버스를 작동시키기 위한 제어 라인들을 포함한다. 이러한 시스템 버스(80)의 일 예는 PCI(Peripheral Component Interconnect) 버스이다.

[0251] 시스템 버스(80)에 연결되는 메모리 디바이스들은 RAM(random access memory)(82) 및 ROM(read only memory)(93)을 포함한다. 이러한 메모리들은 정보가 저장 및 검색될 수 있게 하는 회로를 포함한다. ROM들(93)은 일반적으로 쉽게 수정될 수 없는 저장된 데이터를 포함한다. RAM(82)에 저장된 데이터는 CPU(91) 또는 다른 하드웨어 디바이스들에 의해 판독 또는 변경될 수 있다. RAM(82) 및/또는 ROM(93)에 대한 액세스는 메모리 제어기(92)에 의해 제어될 수 있다. 메모리 제어기(92)는, 명령어들이 실행될 때, 가상 주소들을 물리 주소들로 변환하는 주소 변환 기능(address translation function)을 제공할 수 있다. 메모리 제어기(92)는 또한 시스템 내에서 프로세스들을 격리시키고 시스템 프로세스들을 사용자 프로세스들로부터 격리시키는 메모리 보호 기능을 제공할 수 있다. 따라서, 제1 모드에서 실행하는 프로그램은 그 자신의 프로세스 가상 어드레스 공간에 의해 매핑된 메모리에만 액세스할 수 있고, 그 프로그램은 프로세스들 간에 메모리 공유가 설정되지 않았다면 다른 프로세스의 가상 어드레스 공간 내의 메모리에 액세스할 수 없다.

[0252] 그에 부가하여, 컴퓨팅 시스템(90)은 명령어들을 CPU(91)로부터, 프린터(94), 키보드(84), 마우스(95), 및 디스크 드라이브(85)와 같은, 주변기기들에게 전달하는 일을 책임지고 있는 주변기기 제어기(83)를 포함할 수 있다.

[0253] 디스플레이 제어기(96)에 의해 제어되는, 디스플레이(86)는 컴퓨팅 시스템(90)에 의해 생성된 시각적 출력을 디스플레이하는 데 사용된다. 이러한 시각적 출력은 텍스트, 그래픽, 애니메이션화된 그래픽(animated graphics), 및 비디오를 포함할 수 있다. 디스플레이(86)는 CRT 기반 비디오 디스플레이, LCD 기반 평판 디스플레이, 가스 플라즈마 기반 평판 디스플레이, 또는 터치 패널로 구현될 수 있다. 디스플레이 제어기(96)는 디스플레이(86)에게 송신되는 비디오 신호를 생성하는 데 요구된 전자 컴포넌트들을 포함한다.

[0254] 또한, 컴퓨팅 시스템(90)은 도 36a 및 도 36b의 네트워크(12)와 같은 외부 통신 네트워크에 컴퓨팅 시스템(90)을 접속하여, 컴퓨팅 시스템(90)이 네트워크의 다른 노드들과 통신할 수 있게 하는데 사용될 수 있는, 예를 들어 네트워크 어댑터(97)와 같은 통신 회로를 포함할 수 있다. 통신 회로는 단독으로 또는 CPU(91)와 조합하여 본 명세서에서(예를 들어, 도 6 내지 도 35, 도 37 및 도 38에서) 및 청구범위에서 설명된 송신 및 수신 단계들을 수행하기 위해 사용될 수 있다.

[0255] 본 명세서에 설명되는 시스템들, 방법들 및 프로세스들 중 임의의 것은 컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 실행가능 명령어들(즉, 프로그램 코드)의 형태로 구현될 수 있다는 점이 이해되며, 이 명령어들은, 컴퓨터, 서버, M2M 단말 디바이스, M2M 게이트웨이 디바이스 등 같은 머신에 의해 실행될 때, 본 명세서에 설명되는 시스템들, 방법들 및 프로세스들을 수행 및/또는 구현한다. 구체적으로, 위에 설명된 단계들, 동작들 또는 기능들 중 임의의 것이 그러한 컴퓨터 실행가능 명령어들의 형태로 구현될 수 있다. 컴퓨터 판독가능 저장 매체는 정보의 저장을 위한 방법 또는 기술로 구현되는 휘발성 및 비휘발성, 이동식 및 비-이동식 매체 모두를

포함하지만, 이러한 컴퓨터 판독가능 저장 매체는 신호들을 포함하지 않는다. 컴퓨터 판독가능 저장 매체는, 이에 제한되는 것은 아니지만, RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, CD-ROM, DVD(digital versatile disks) 또는 다른 광학 디스크 스토리지, 자기 카세트들, 자기 테이프, 자기 디스크 스토리지 또는 다른 자기 스토리지 디바이스들, 또는 원하는 정보를 저장하는데 사용될 수 있는 그리고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 물리적 매체를 포함한다.

[0256] 본 개시내용의 발명 요지의 바람직한 실시예들을 기술함에 있어서, 도면들에 예시된 바와 같이, 명확함을 위해 특정의 용어가 이용된다. 그렇지만, 청구된 발명 요지는 그렇게 선택된 특정 용어로 제한되는 것으로 의도되어 있지 않으며, 각각의 특정 요소가 유사한 목적을 달성하기 위해 유사한 방식으로 동작하는 모든 기술적 등가물들을 포함한다는 것을 잘 알 것이다.

[0257] 다음은 위의 설명에 나타날 수 있는 서비스 레벨 기술과 관련된 두문자어 목록이다. 달리 명시되지 않는 한, 본문에서 사용된 두문자어는 아래 나열된 해당 용어를 의미한다.

[0258] ACP Access Control Policy

[0259] AE Application Entity

[0260] AEAD Authenticated Encryption with Associated Data

[0261] AES Advanced Encryption Standard

[0262] AES - GCM AES - Galois Mode

[0263] Cert Digital Certificate

[0264] CCF Content Creation Function

[0265] CCP Content Creation Process

[0266] CCSDF Content Creation and Security Determination Function

[0267] CDB Credential Database

[0268] CHF Content Hosting Function

[0269] CLMP Content Life-cycle Management Process

[0270] CR Credential Registry

[0271] CGP Credential Registration Process

[0272] CQP Credential Requisition Process

[0273] CP Content Processing

[0274] CRP Content Retrieval Process

[0275] CRRP Credential Requisition and Registration Process

[0276] DES Digital Encryption Standard

[0277] DS Digital Signature

[0278] DTLS Datagram Transport Layer Security

[0279] ECC Elliptic Curve Cryptography

[0280] E2E End-to-End

[0281] IoT Internet-of-Things

[0282] IPSec Internet Protocol Security

[0283] JWA JSON Web Algorithms

[0284] JWE JSON Web Encryption

[0285] JWK JSON Web Key

[0286] JWS JSON Web Signature

[0287] JWT JSON Web Token

[0288] KDF Key Derivation Function

[0289] M2M Machine-to-Machine

[0290] MAC Message Authentication Code

[0291] MEF M2M Enrollment Function

[0292] NTP Network Time Protocol

[0293] PCS Protected Content Store

[0294] PKI Public Key Infrastructure

[0295] PSK Pre-Shared Key

[0296] RoT Root-of-Trust

[0297] RSA Rivest-Shamir-Addleman algorithm

[0298] SCHF Secure Content Hosting Function

[0299] SDF Security Determination Function

[0300] SE Secure Element

[0301] SEF Service Enabling Function

[0302] SESC Service Enabling and Security Configuration

[0303] SHRP Secure Hosting Requisition Process

[0304] SL Service Layer

[0305] SP Service Provider

[0306] SPDP Security Parameters Determination Function

[0307] TEE Trusted Execution Environment

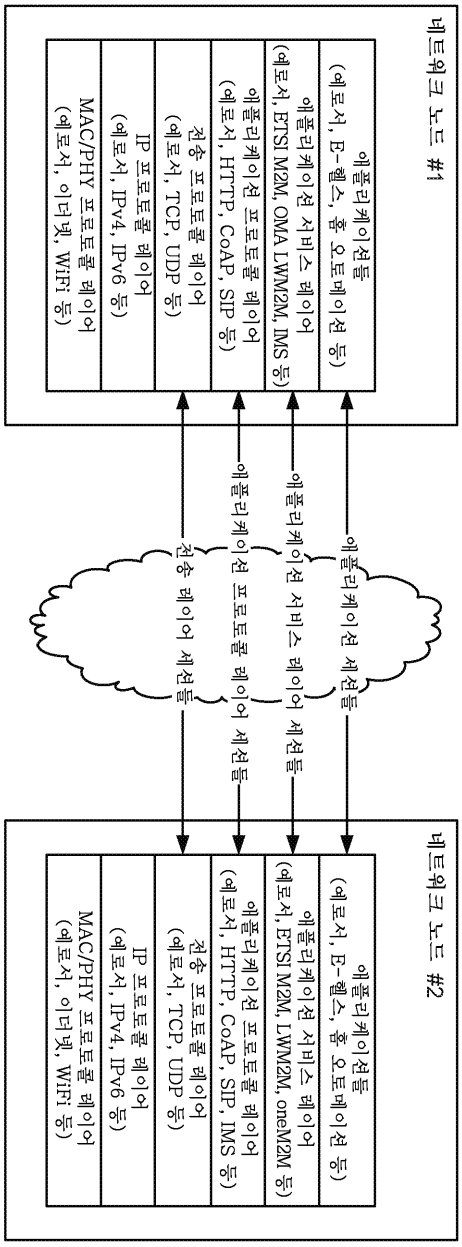
[0308] TLS Transport Layer Security

[0309] TTP Trusted Third Party

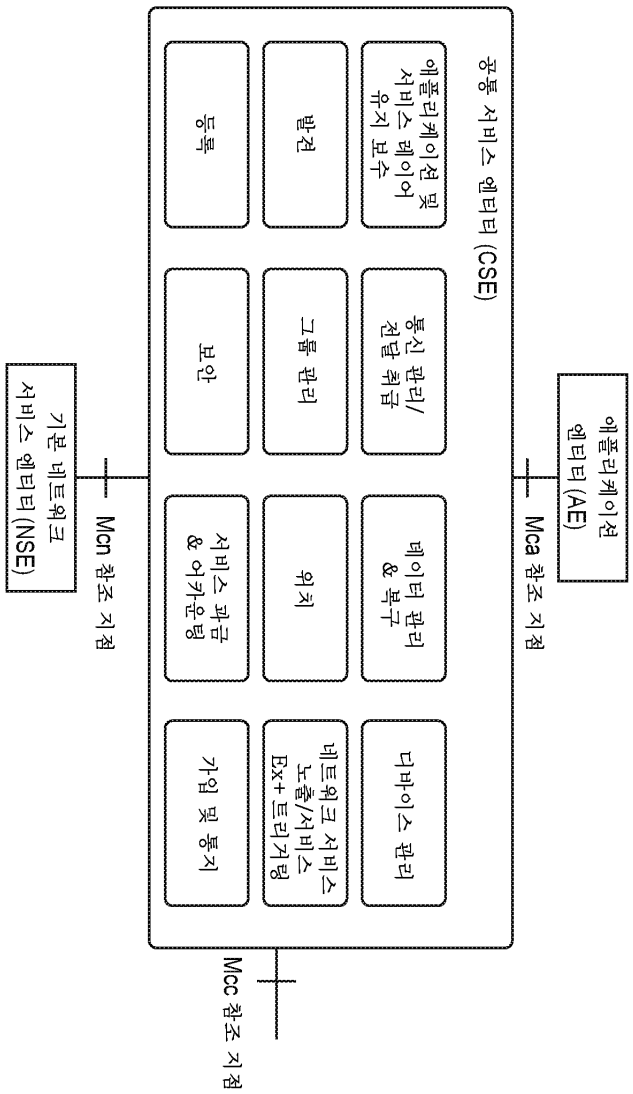
[0310] 이러한 서면 설명은 최상의 실시 형태(best mode)를 비롯한 본 발명을 개시하기 위해 그리고 또한 통상의 기술자가, 임의의 디바이스들 또는 시스템들을 제조 및 사용하는 것 그리고 임의의 포함된 방법들을 수행하는 것을 비롯하여, 본 발명을 실시할 수 있게 하기 위해 예들을 사용한다. 본 발명의 특허가능 범위는 청구항들에 의해 한정되고, 통상의 기술자에게 안출되는 다른 예들을 포함할 수 있다. 이러한 다른 예들은, 청구항들의 문자 그대로의 표현과 상이하지 않은 엘리먼트들을 가지는 경우, 또는 이들이 청구항들의 문자 그대로의 표현과 실질적인 차이가 없는 등가의 구조적 엘리먼트들을 포함하는 경우, 청구항들의 범위 내에 있는 것으로 의도된다.

도면

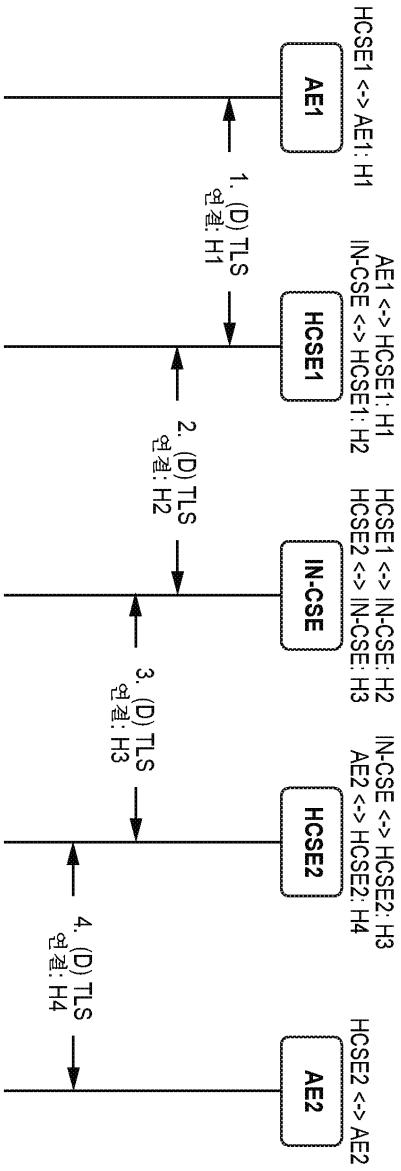
도면1


네트워크 노드 #1
애플리케이션들
(예로서, E-헬스, 홈 오토메이션 등)
애플리케이션 서비스 레이어
(예로서, ETSI M2M, OMA LWM2M, IMS 등)
애플리케이션 프로토콜 레이어
(예로서, HTTP, CoAP, SIP 등)
전송 프로토콜 레이어
(예로서, TCP, UDP 등)
IP 프로토콜 레이어
(예로서, IPv4, IPv6 등)
MAC/PHY 프로토콜 레이어
(예로서, 이더넷, WiFi 등)
애플리케이션 세션들
애플리케이션 서비스 레이어 세션들
애플리케이션 프로토콜 레이어 세션들
전송 레이어 세션들
네트워크 노드 #2
애플리케이션들
(예로서, E-헬스, 홈 오토메이션 등)
애플리케이션 서비스 레이어
(예로서, ETSI M2M, LWM2M, oneM2M 등)
애플리케이션 프로토콜 레이어
(예로서, HTTP, CoAP, SIP, IMS 등)
전송 프로토콜 레이어
(예로서, TCP, UDP 등)
IP 프로토콜 레이어
(예로서, IPv4, IPv6 등)
MAC/PHY 프로토콜 레이어
(예로서, 이더넷, WiFi 등)

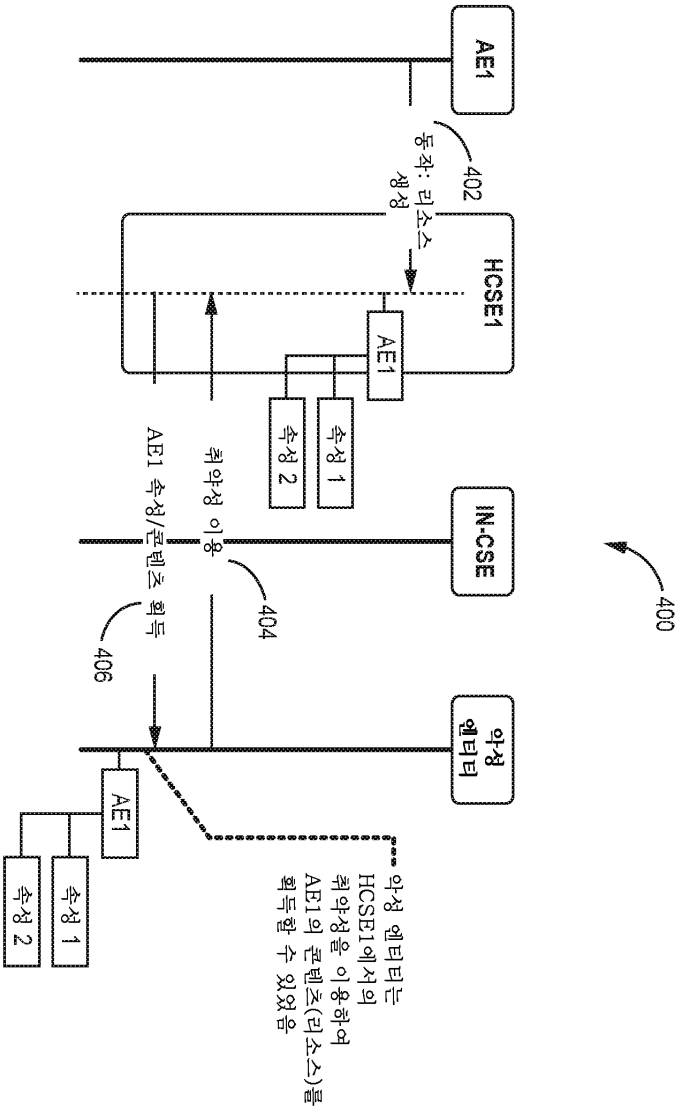
도면2


공통 서비스 엔티티 (CSE)
애플리케이션 및 서비스 레이어 유지 보수
통신 관리/ 전달 취급
데이터 관리 & 복구
디바이스 관리
발견
그룹 관리
위치
네트워크 서비스 노출/서비스 Ex+트리거링
등록
보안
서비스 과금 & 어카운팅
가입 및 통지
애플리케이션 엔티티 (AE)
Mca 참조 지점
기본 네트워크 서비스 엔티티 (NSE)
Mcn 참조 지점
Mcc 참조 지점

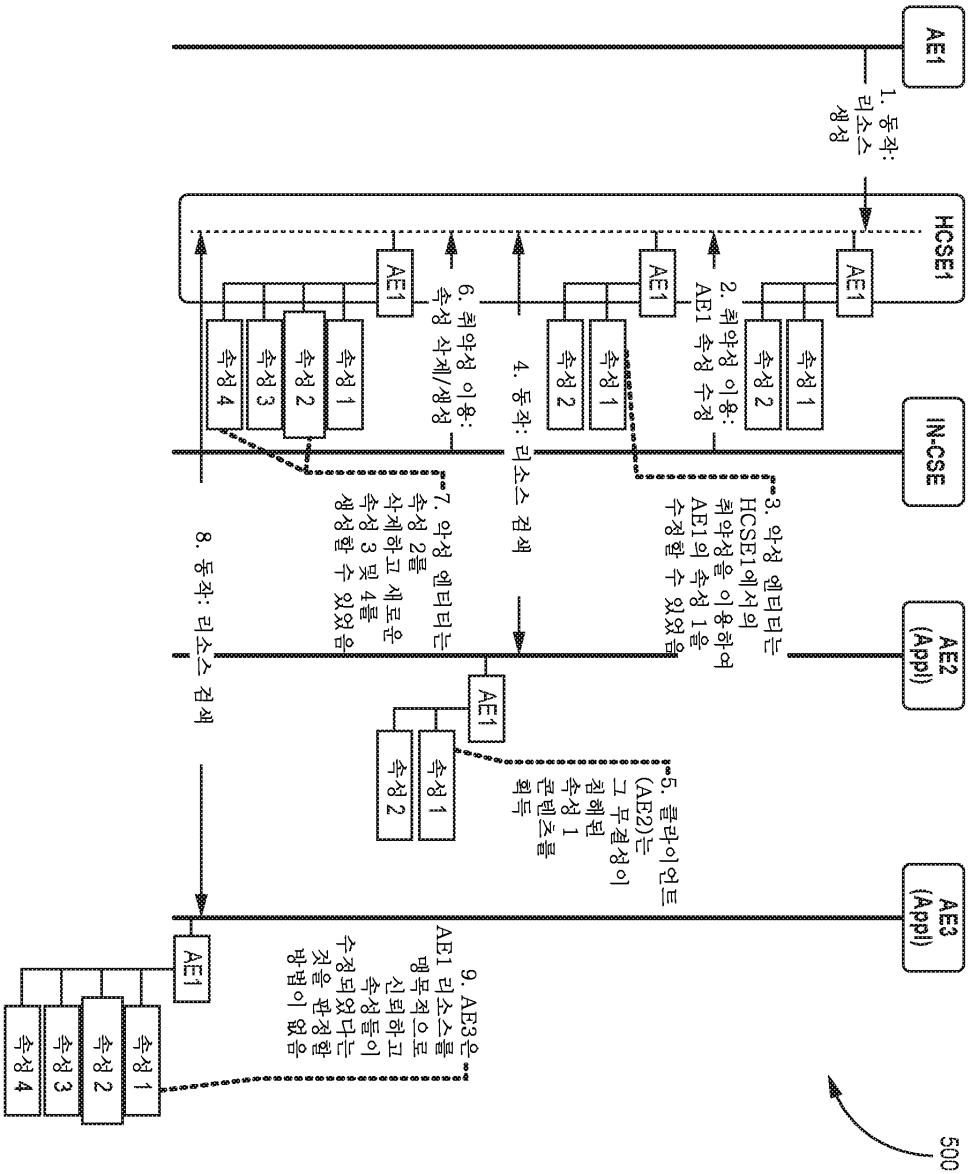
도면3


AE1
HCSE1
IN-CSE
HCSE2
AE2
HCSE1 <-> AE1: H1
AE1 <-> HCSE1: H1
IN-CSE <-> HCSE1: H2
HCSE1 <-> IN-CSE: H2
HCSE2 <-> IN-CSE: H3
IN-CSE <-> HCSE2: H3
AE2 <-> HCSE2: H4
HCSE2 <-> AE2
1. (D) TLS 연결: H1
2. (D) TLS 연결: H2
3. (D) TLS 연결: H3
4. (D) TLS 연결: H4

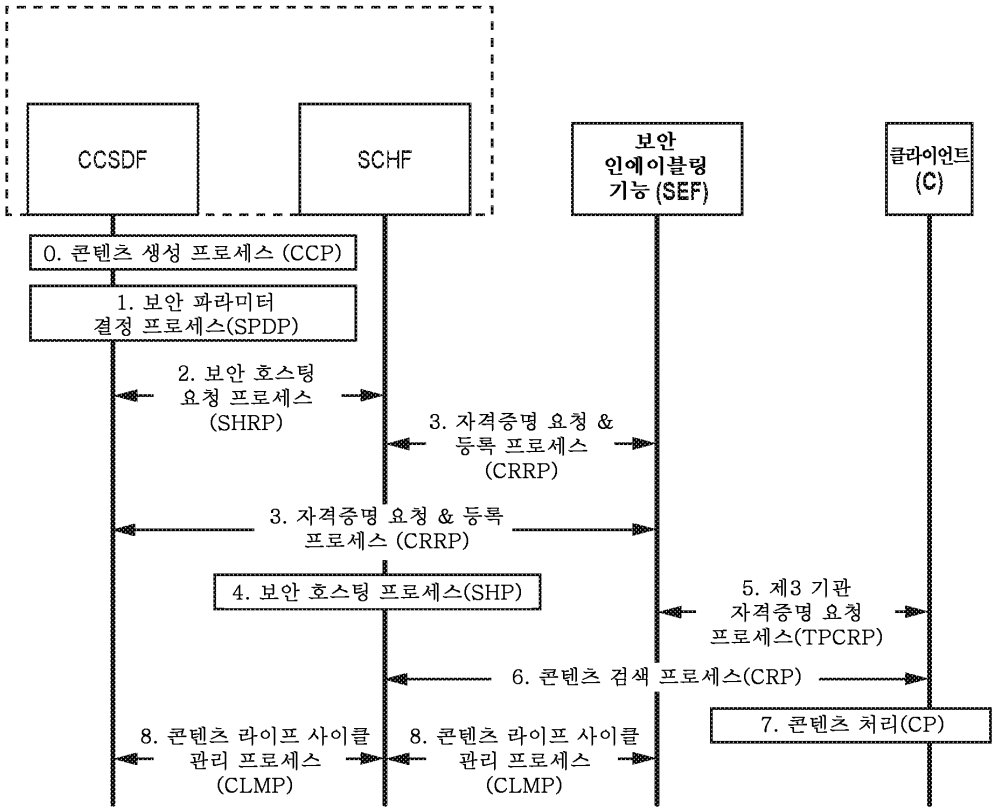
도면4


AE1
동작: 리소스 생성
402
HCSE1
AE1
속성 2
속성 1
취약성 이용
AE1 속성/콘텐츠 획득
404
406
IN-CSE
악성 엔티티
AE1
속성 2
속성 1
악성 엔티티는 HCSE1에서의 취약성을 이용하여 AE1의 콘텐츠(리소스)를 획득할 수 있었음
400

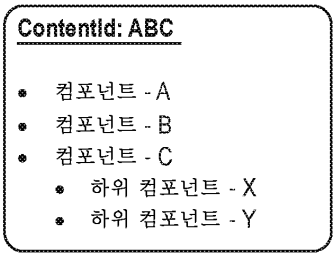
도면5


AE1
1. 동작: 리소스 생성
HCSE1
IN-CSE
AE2 (Appl)
AE3 (Appl)
AE1
속성 1
속성 2
2. 취약성 이용: AE1 속성 수정
3. 악성 엔티티는 HCSE1에서의 취약성을 이용하여 AE1의 속성 1을 수정할 수 있었음
4. 동작: 리소스 검색
5. 클라이언트 (AE2)는 그 무결성이 침해된 속성 1 콘텐츠를 획득
6. 취약성 이용: 속성 삭제/생성
7. 악성 엔티티는 속성 2를 삭제하고 새로운 속성 3 및 4를 생성할 수 있었음
8. 동작: 리소스 검색
9. AE3은 AE1 리소스를 맹목적으로 신뢰하고 속성들이 수정되었다는 것을 판정할 방법이 없음
속성 3
속성 4
500

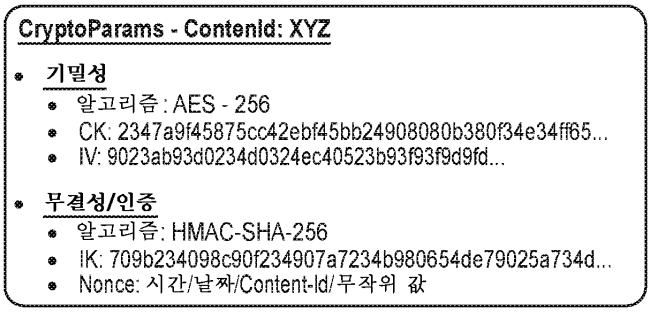
도면6


CCSDF
SCHF
보안
인에이블링
기능 (SEF)
클라이언트
(C)
0. 콘텐츠 생성 프로세스 (CCP)
1. 보안 파라미터
결정 프로세스(SPDP)
2. 보안 호스팅
요청 프로세스
(SHRP)
3. 자격증명 요청 &
등록 프로세스
(CRRP)
3. 자격증명 요청 & 등록
프로세스 (CRRP)
4. 보안 호스팅 프로세스(SHP)
5. 제3 기관
자격증명 요청
프로세스(TPCRP)
6. 콘텐츠 검색 프로세스(CRP)
7. 콘텐츠 처리(CP)
8. 콘텐츠 라이프 사이클
관리 프로세스
(CLMP)
8. 콘텐츠 라이프 사이클
관리 프로세스
(CLMP)

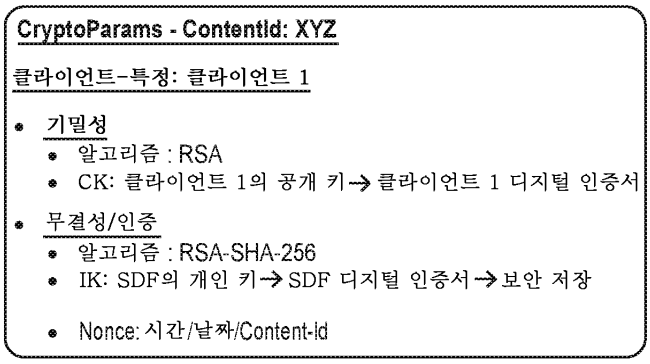
도면7


ContentId: ABC
컴포넌트 - A
컴포넌트 - B
컴포넌트 - C
하위 컴포넌트 - X
하위 컴포넌트 - Y

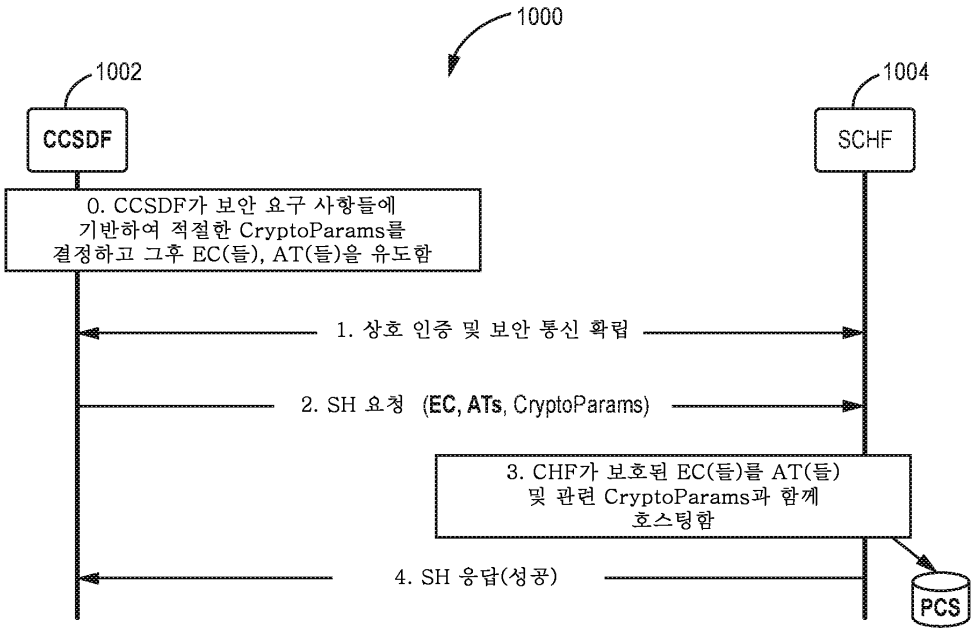
도면8


CryptoParams - ContenId: XYZ
기밀성
알고리즘 : AES - 256
CK: 2347a9f45875cc42ebf45bb24908080b380f34e34ff65...
IV: 9023ab93d0234d0324ec40523b93f93f9d9fd...
무결성/인증
알고리즘: HMAC-SHA-256
IK: 709b234098c90f234907a7234b980654de79025a734d...
Nonce: 시간/날짜/Content-Id/무작위 값

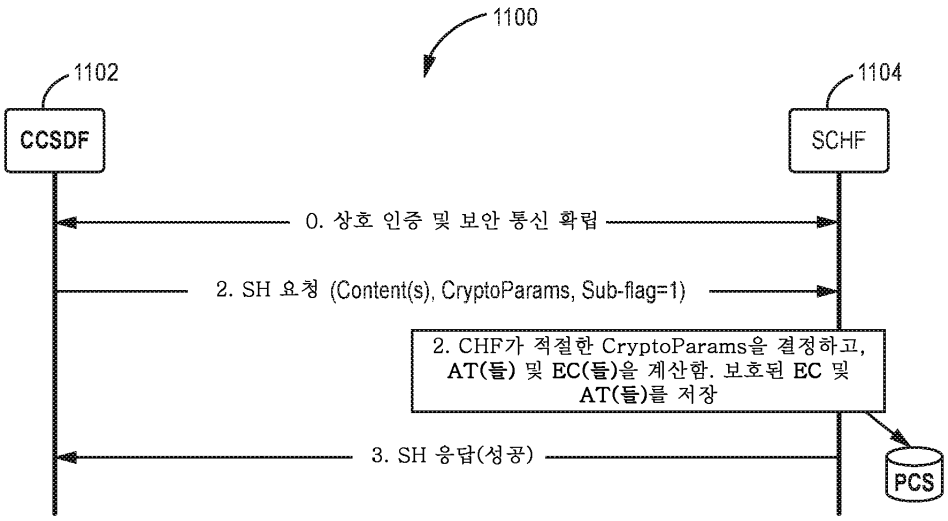
도면9



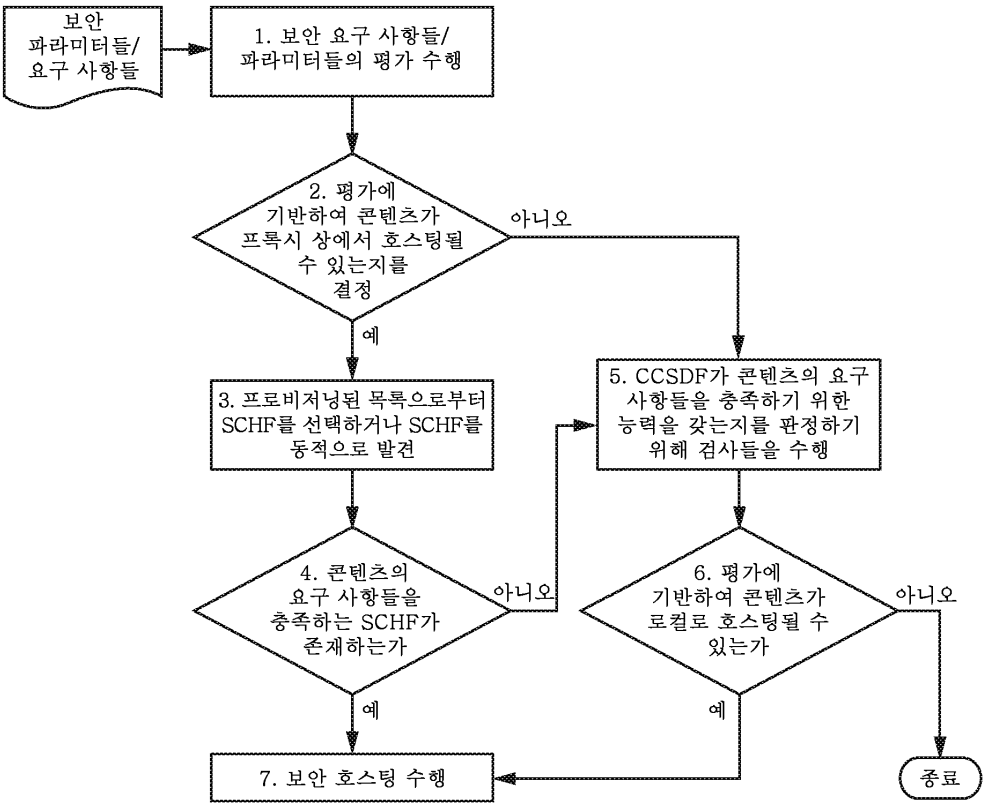
도면10



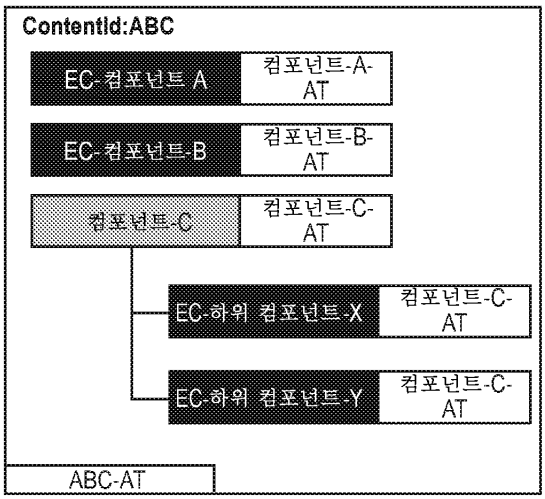
도면11



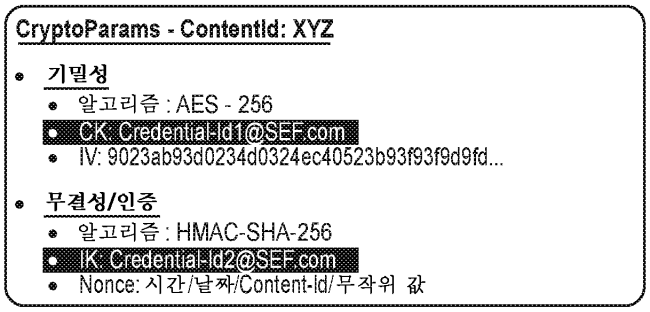
도면12


보안 파라미터들/ 요구 사항들
1. 보안 요구 사항들/ 파라미터들의 평가 수행
2. 평가에 기반하여 콘텐츠가 프록시 상에서 호스팅될 수 있는지를 결정
아니오
예
3. 프로비저닝된 목록으로부터 SCHF를 선택하거나 SCHF를 동적으로 발견
5. CCSDF가 콘텐츠의 요구 사항들을 충족하기 위한 능력을 갖는지를 판정하기 위해 검사들을 수행
4. 콘텐츠의 요구 사항들을 충족하는 SCHF가 존재하는가
아니오
6. 평가에 기반하여 콘텐츠가 로컬로 호스팅될 수 있는가
아니오
예
예
7. 보안 호스팅 수행
종료

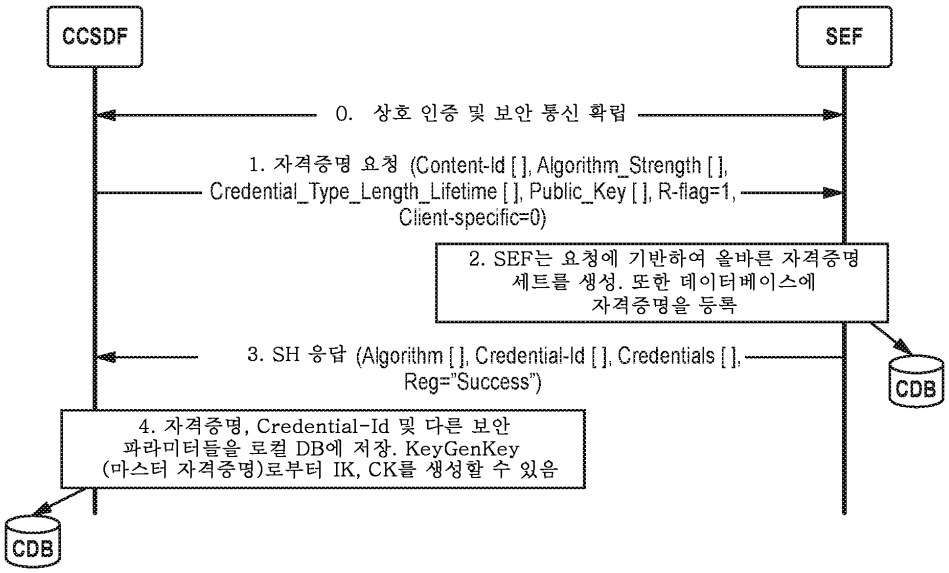
도면13


ContentId:ABC
EC-컴포넌트 A
컴포넌트-A-AT
EC-컴포넌트-B
컴포넌트-B-AT
컴포넌트-C
컴포넌트-C-AT
EC-하위 컴포넌트-X
컴포넌트-C-AT
EC-하위 컴포넌트-Y
컴포넌트-C-AT
ABC-AT

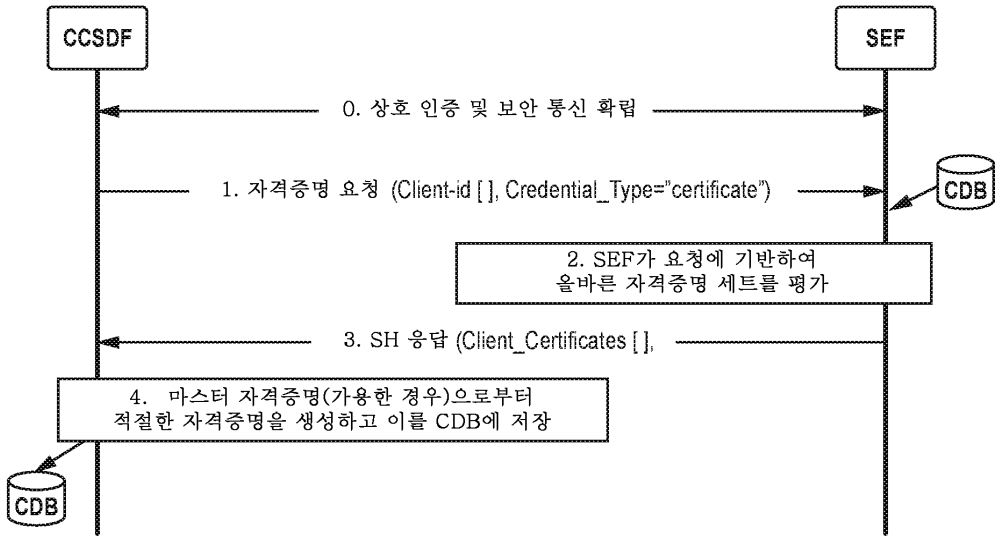
도면14



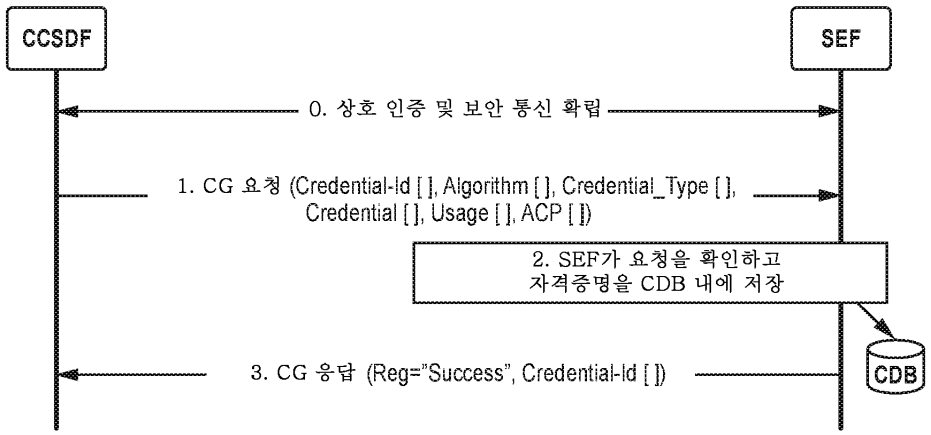
도면15



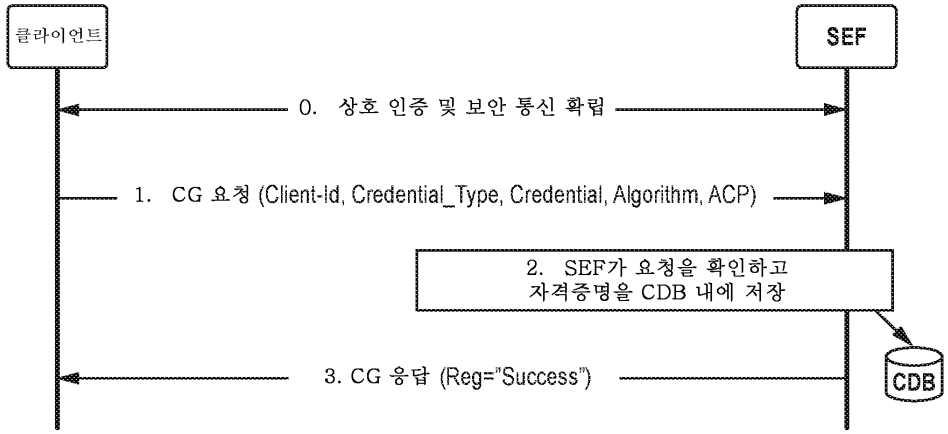
도면16



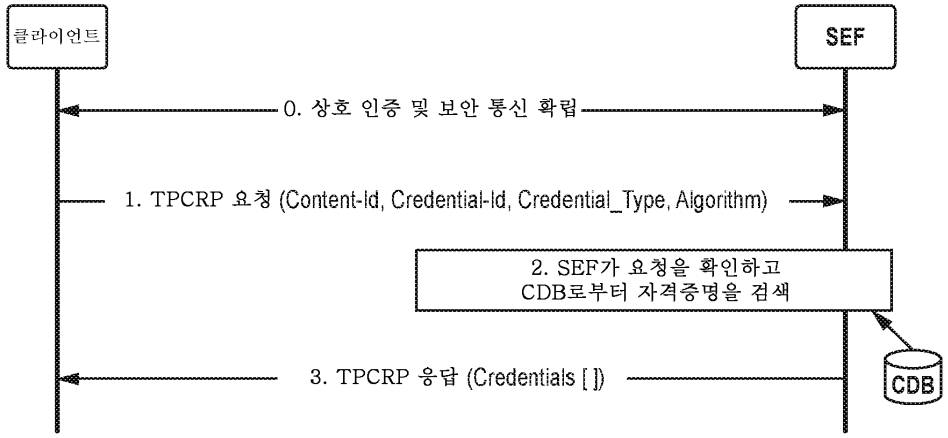
도면17



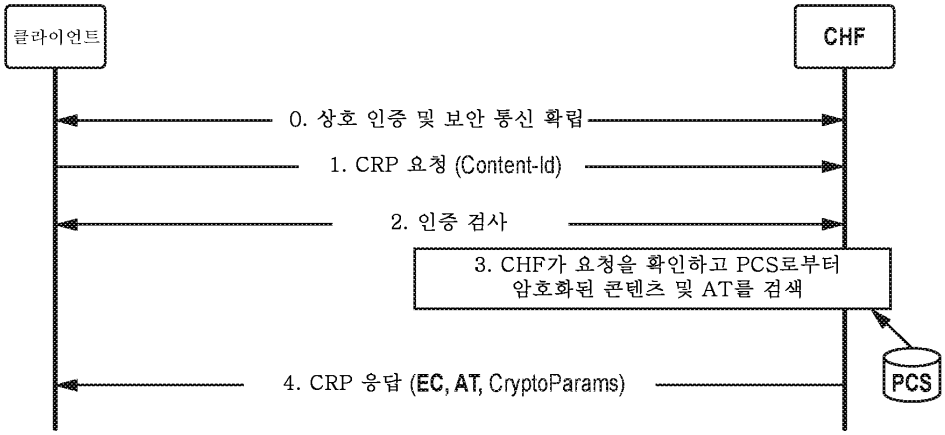
도면18



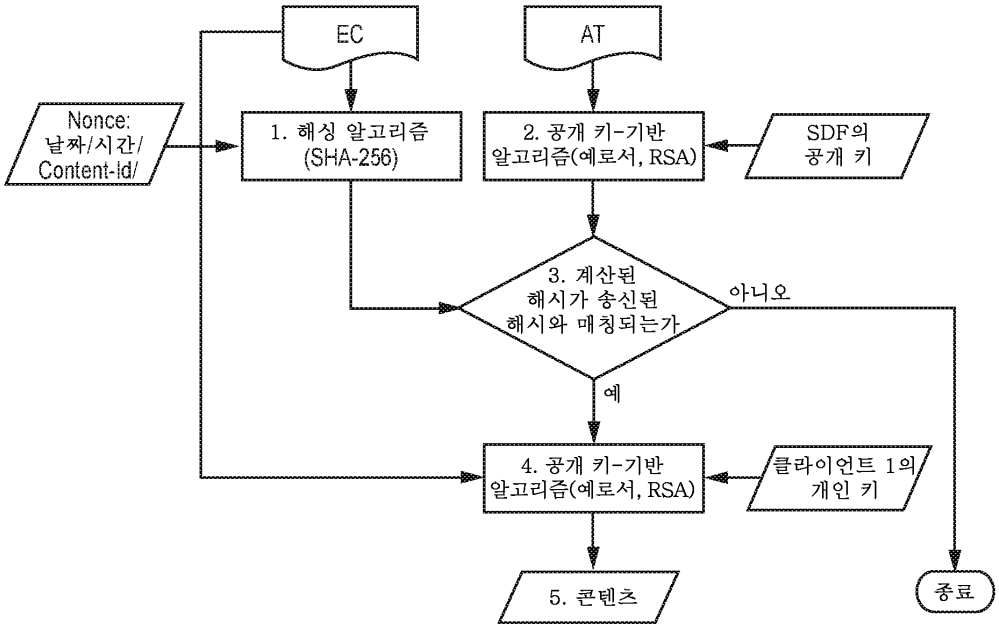
도면19



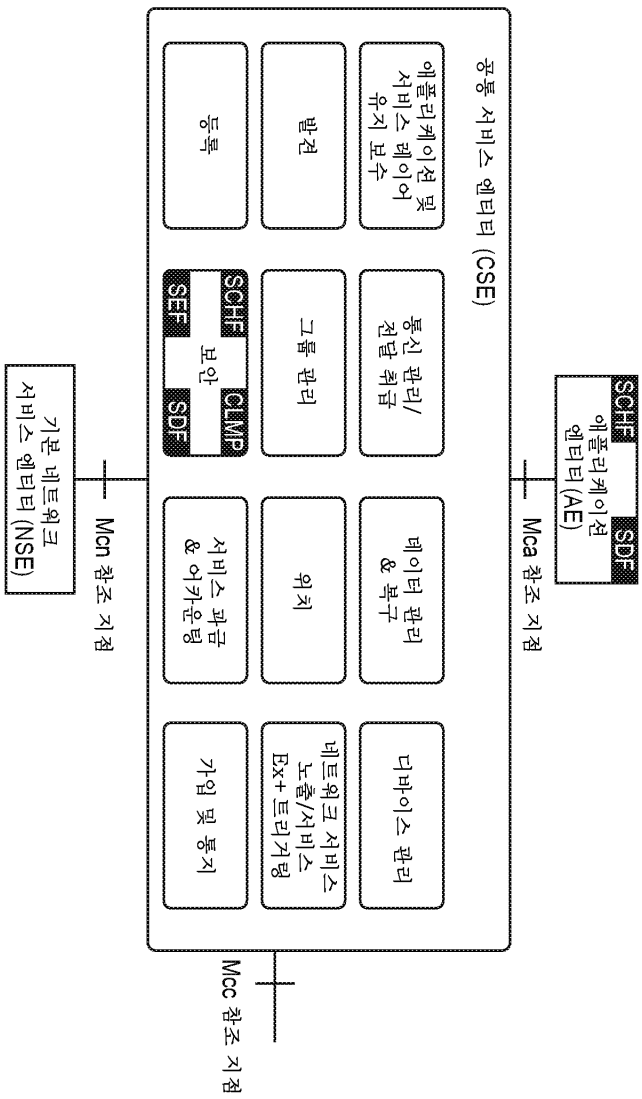
도면20


클라이언트
CHF
0. 상호 인증 및 보안 통신 확립
1. CRP 요청 (Content-Id)
2. 인증 검사
3. CHF가 요청을 확인하고 PCS로부터
암호화된 콘텐츠 및 AT를 검색
PCS
4. CRP 응답 (EC, AT, CryptoParams)

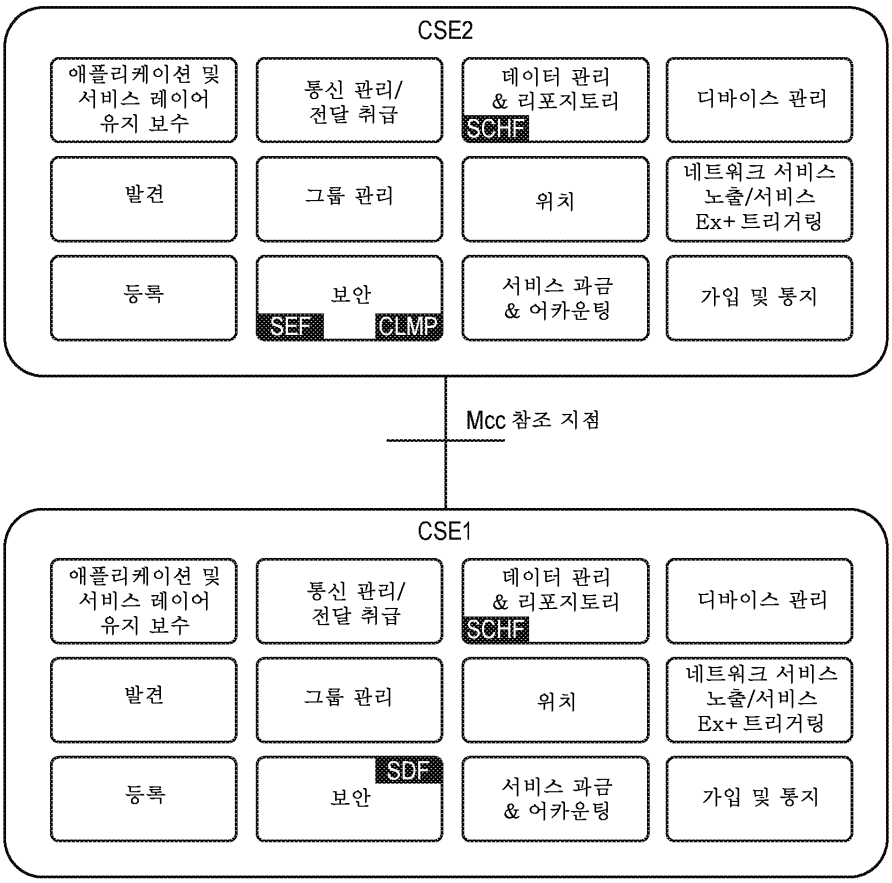
도면21


EC
AT
Nonce:
날짜/시간/
Content-Id/
1. 해싱 알고리즘
(SHA-256)
2. 공개 키-기반
알고리즘(예로서, RSA)
SDF의
공개 키
3. 계산된
해시가 송신된
해시와 매칭되는가
아니오
예
4. 공개 키-기반
알고리즘(예로서, RSA)
클라이언트 1의
개인 키
5. 콘텐츠
종료

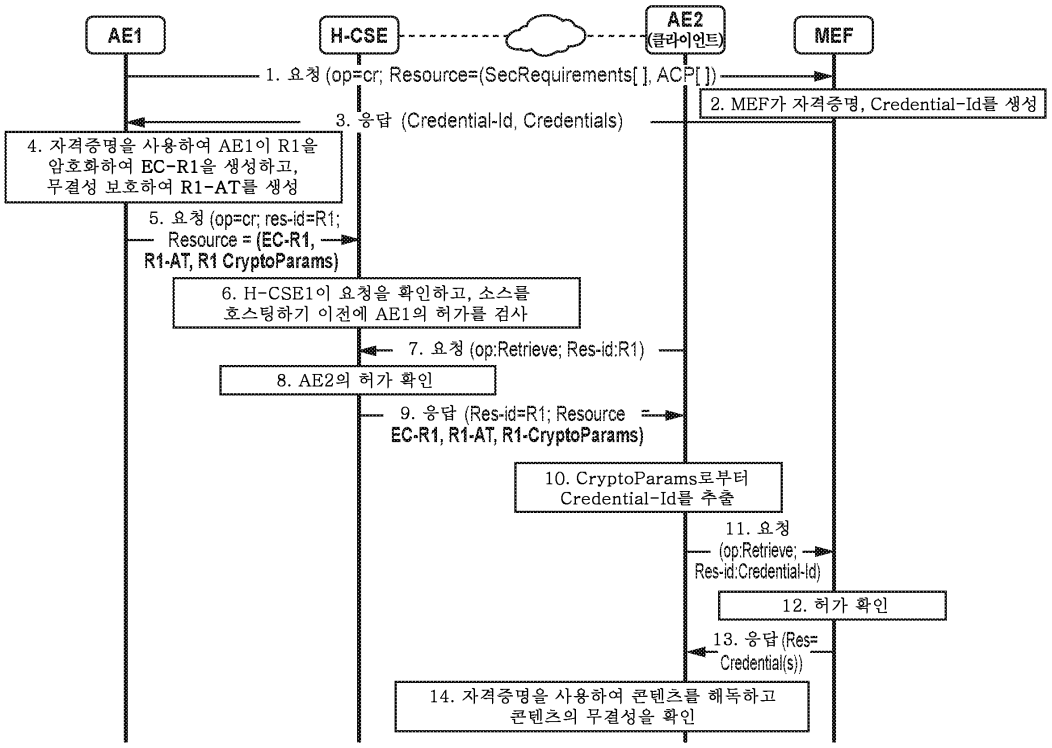
도면22


공통 서비스 엔티티 (CSE)
애플리케이션 및 서비스 레이어 유지 보수
통신 관리/ 전달 취급
데이터 관리 & 복구
디바이스 관리
발견
그룹 관리
위치
네트워크 서비스 노출/서비스 Ex+ 트리거링
등록
보안
서비스 과금 & 어카운팅
가입 및 통지
SCHF
SEF
CLMP
SDF
SCHF
에플리케이션 엔티티 (AE)
SDF
Mca 참조 지점
Mcn 참조 지점
기본 네트워크 서비스 엔티티 (NSE)
Mcc 참조 지점

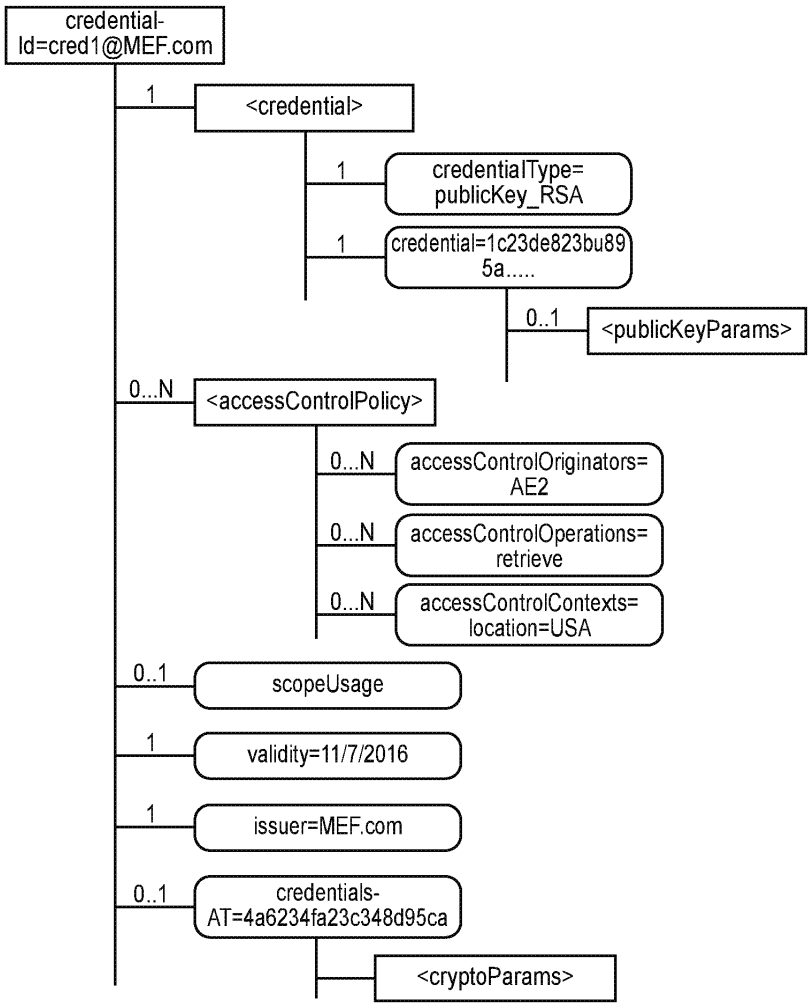
도면23


CSE2
애플리케이션 및 서비스 레이어 유지 보수
통신 관리/ 전달 취급
데이터 관리 & 리포지토리
SCHF
디바이스 관리
발견
그룹 관리
위치
네트워크 서비스 노출/서비스 Ex+ 트리거링
등록
보안
SEF
CLMP
서비스 과금 & 어카운팅
가입 및 통지
Mcc 참조 지점
CSE1
애플리케이션 및 서비스 레이어 유지 보수
통신 관리/ 전달 취급
데이터 관리 & 리포지토리
SCHF
디바이스 관리
발견
그룹 관리
위치
네트워크 서비스 노출/서비스 Ex+ 트리거링
등록
보안
SDF
서비스 과금 & 어카운팅
가입 및 통지

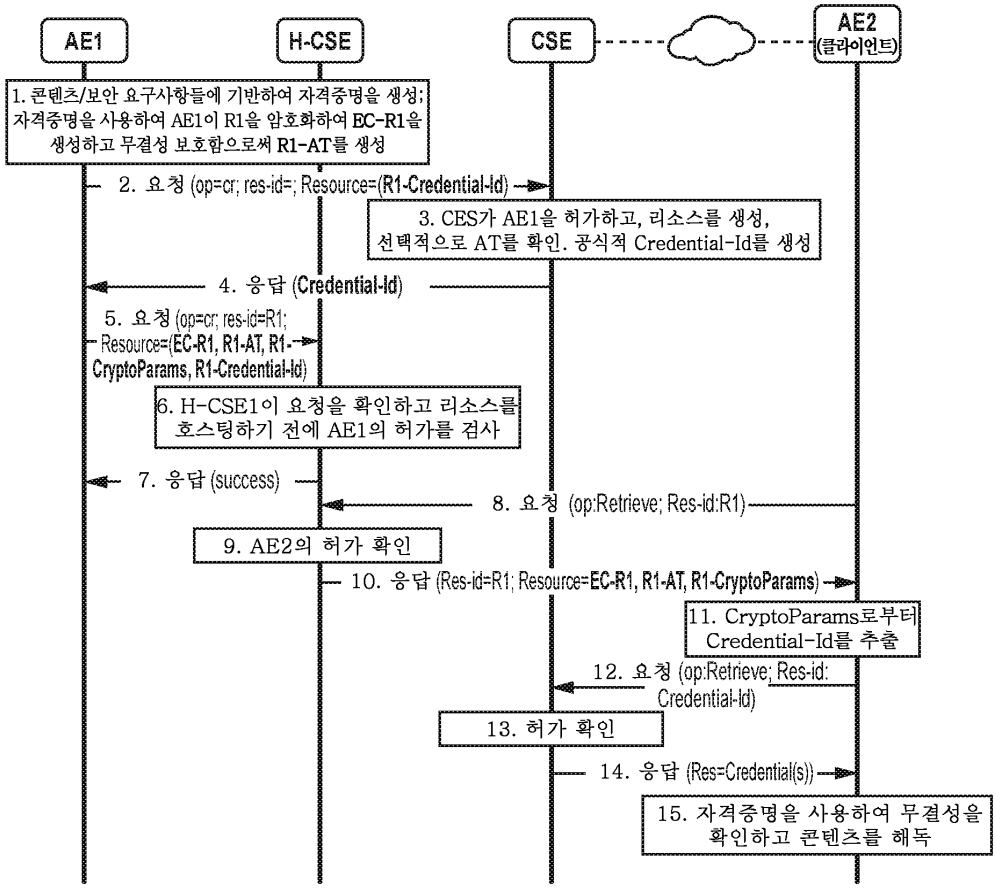
도면24


AE1
H-CSE
AE2 (클라이언트)
MEF
1. 요청 (op=cr; Resource=(SecRequirements[ ], ACP[ ])
2. MEF가 자격증명, Credential-Id를 생성
3. 응답 (Credential-Id, Credentials)
4. 자격증명을 사용하여 AE1이 R1을 암호화하여 EC-R1을 생성하고, 무결성 보호하여 R1-AT를 생성
5. 요청 (op=cr; res-id=R1; Resource = (EC-R1, R1-AT, R1 CryptoParams)
6. H-CSE1이 요청을 확인하고, 소스를 호스팅하기 이전에 AE1의 허가를 검사
7. 요청 (op:Retrieve; Res-id:R1)
8. AE2의 허가 확인
9. 응답 (Res-id=R1; Resource = EC-R1, R1-AT, R1-CryptoParams)
10. CryptoParams로부터 Credential-Id를 추출
11. 요청 (op:Retrieve; Res-id:Credential-Id)
12. 허가 확인
13. 응답 (Res= Credential(s))
14. 자격증명을 사용하여 콘텐츠를 해독하고 콘텐츠의 무결성을 확인

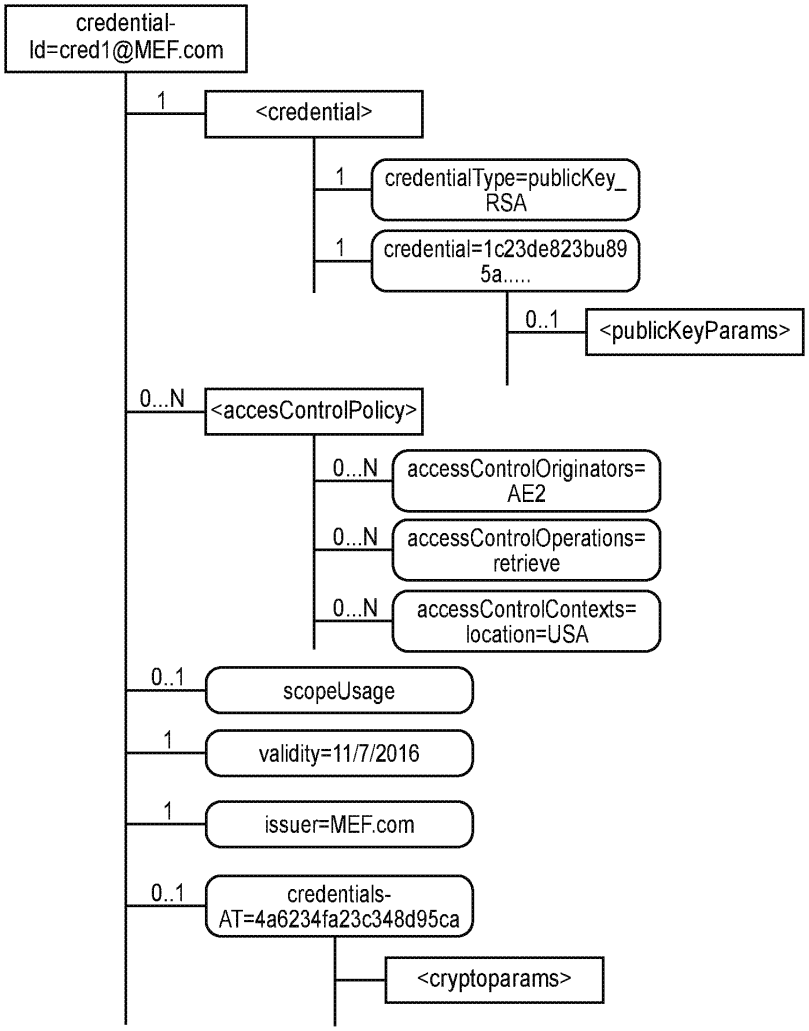
도면25


credential-Id=cred1@MEF.com
1
<credential>
1
credentialType=publicKey_RSA
1
credential=1c23de823bu895a.....
0..1
<publicKeyParams>
0...N
<accessControlPolicy>
0...N
accessControlOriginators=AE2
0...N
accessControlOperations=retrieve
0...N
accessControlContexts=location=USA
0..1
scopeUsage
1
validity=11/7/2016
1
issuer=MEF.com
0..1
credentials-AT=4a6234fa23c348d95ca
<cryptoParams>

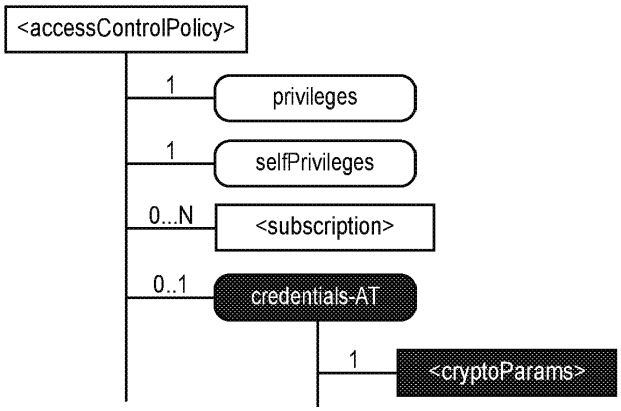
도면26


AE1
H-CSE
CSE
AE2
(클라이언트)
1. 콘텐츠/보안 요구사항들에 기반하여 자격증명을 생성; 자격증명을 사용하여 AE1이 R1을 암호화하여 EC-R1을 생성하고 무결성 보호함으로써 R1-AT를 생성
2. 요청 (op=cr; res-id=; Resource=(R1-Credential-Id)
3. CES가 AE1을 허가하고, 리소스를 생성, 선택적으로 AT를 확인. 공식적 Credential-Id를 생성
4. 응답 (Credential-Id)
5. 요청 (op=cr; res-id=R1; Resource={EC-R1, R1-AT, R1-CryptoParams, R1-Credential-Id)
6. H-CSE1이 요청을 확인하고 리소스를 호스팅하기 전에 AE1의 허가를 검사
7. 응답 (success)
8. 요청 (op:Retrieve; Res-id:R1)
9. AE2의 허가 확인
10. 응답 (Res-id=R1; Resource=EC-R1, R1-AT, R1-CryptoParams)
11. CryptoParams로부터 Credential-Id를 추출
12. 요청 (op:Retrieve; Res-id: Credential-Id)
13. 허가 확인
14. 응답 (Res=Credential(s))
15. 자격증명을 사용하여 무결성을 확인하고 콘텐츠를 해독

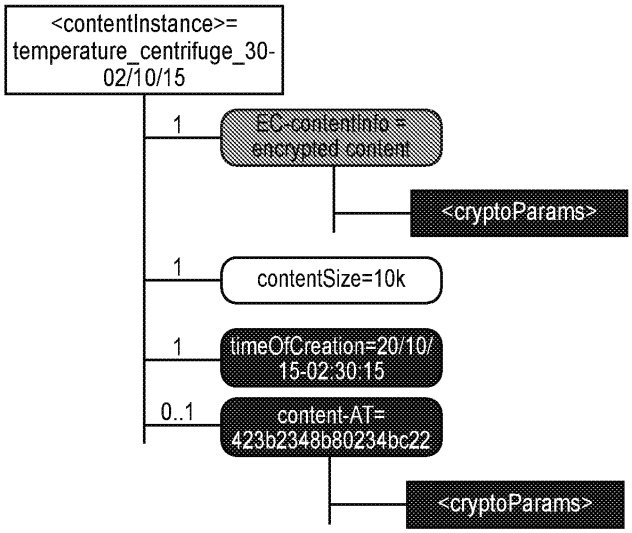
도면27


credential-Id=cred1@MEF.com
1
<credential>
1
credentialType=publicKey_RSA
1
credential=1c23de823bu895a.....
0..1
<publicKeyParams>
0...N
<accesControlPolicy>
0...N
accessControlOriginators=AE2
0...N
accessControlOperations=retrieve
0...N
accessControlContexts=location=USA
0..1
scopeUsage
1
validity=11/7/2016
1
issuer=MEF.com
0..1
credentials-AT=4a6234fa23c348d95ca
<cryptoparams>

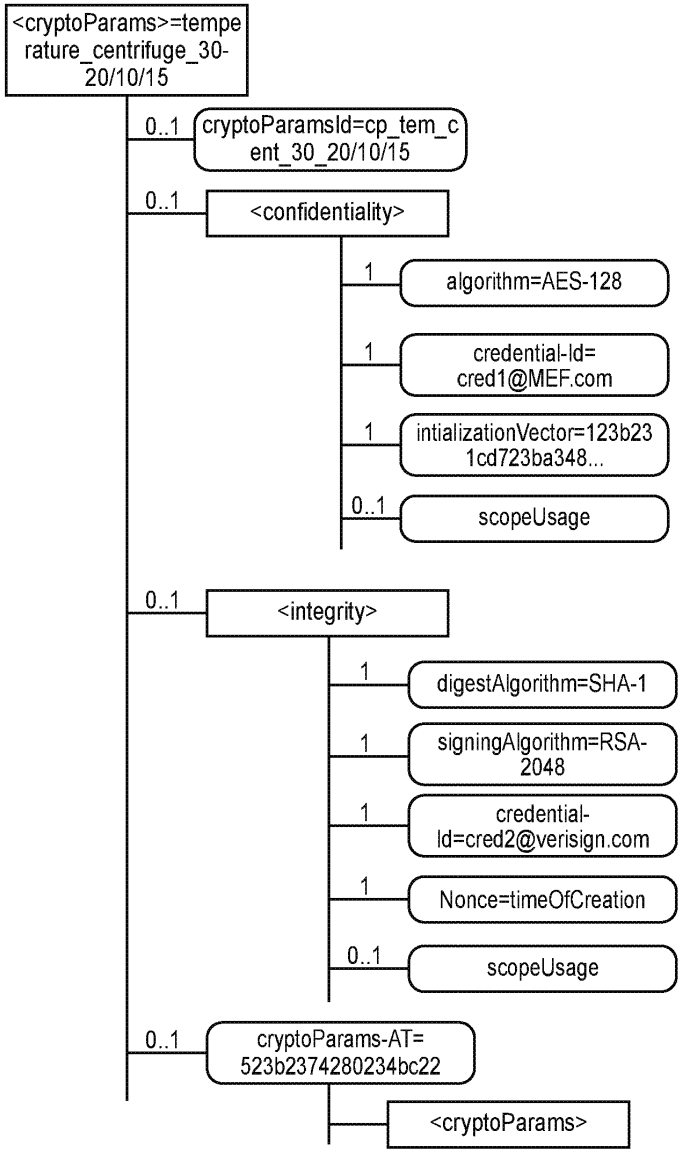
도면28


<accessControlPolicy>
1
privileges
1
selfPrivileges
0...N
<subscription>
0..1
credentials-AT
1
<cryptoParams>

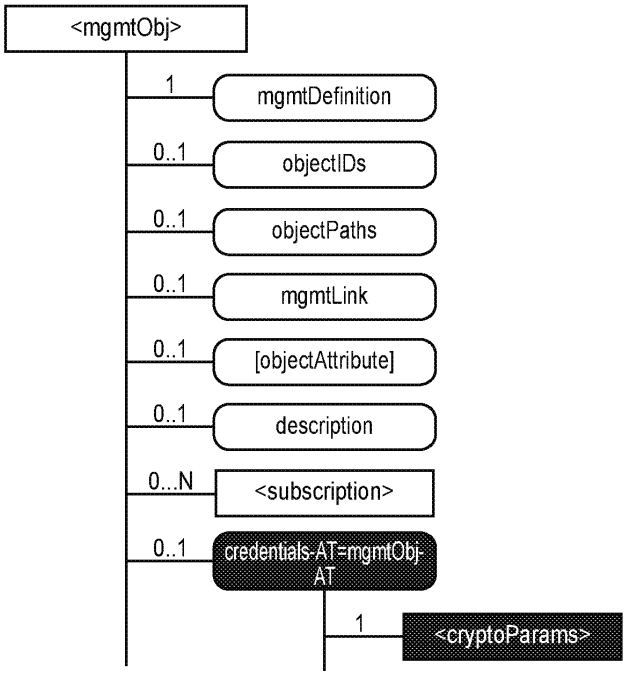
도면29


<contentInstance>=
temperature_centrifuge_30-
02/10/15
1
EC-contentInfo =
encrypted content
<cryptoParams>
1
contentSize=10k
1
timeOfCreation=20/10/
15-02:30:15
0..1
content-AT=
423b2348b80234bc22
<cryptoParams>

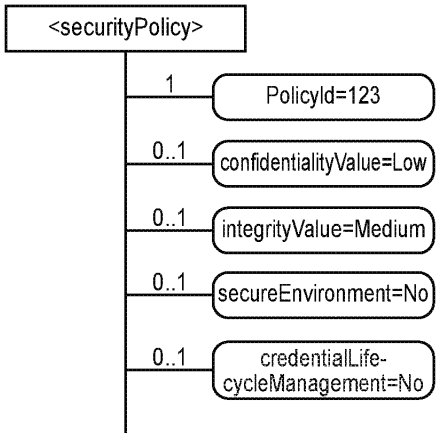
도면30


<cryptoParams>=tempe
rature_centrifuge_30-
20/10/15
0..1
cryptoParamsId=cp_tem_c
ent_30_20/10/15
0..1
<confidentiality>
1
algorithm=AES-128
1
credential-Id=
cred1@MEF.com
1
intializationVector=123b23
1cd723ba348...
0..1
scopeUsage
0..1
<integrity>
1
digestAlgorithm=SHA-1
1
signingAlgorithm=RSA-
2048
1
credential-
Id=cred2@verisign.com
1
Nonce=timeOfCreation
0..1
scopeUsage
0..1
cryptoParams-AT=
523b2374280234bc22
<cryptoParams>

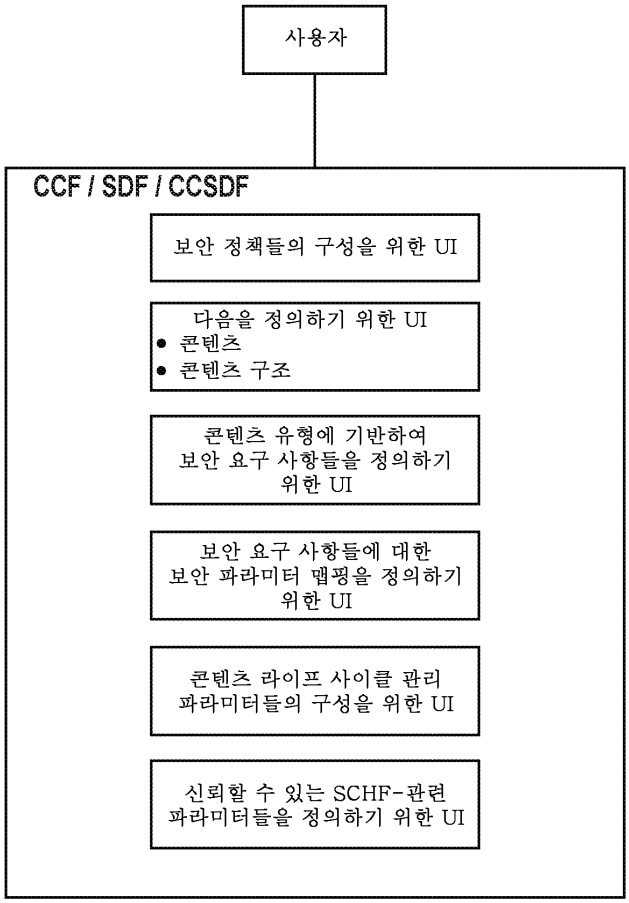
도면31


<mgmtObj>
1
mgmtDefinition
0..1
objectIDs
0..1
objectPaths
0..1
mgmtLink
0..1
[objectAttribute]
0..1
description
0...N
<subscription>
0..1
credentials-AT=mgmtObj-AT
1
<cryptoParams>

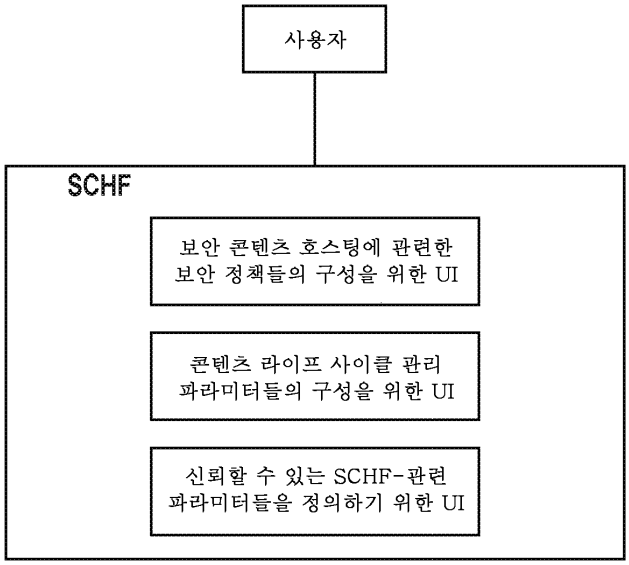
도면32


<securityPolicy>
1
PolicyId=123
0..1
confidentialityValue=Low
0..1
integrityValue=Medium
0..1
secureEnvironment=No
0..1
credentialLife-cycleManagement=No

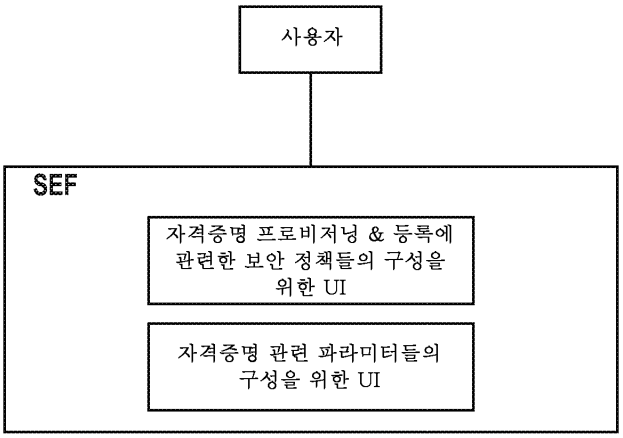
도면33


사용자
CCF / SDF / CCSDF
보안 정책들의 구성을 위한 UI
다음을 정의하기 위한 UI
• 콘텐츠
• 콘텐츠 구조
콘텐츠 유형에 기반하여
보안 요구 사항들을 정의하기
위한 UI
보안 요구 사항들에 대한
보안 파라미터 맵핑을 정의하기
위한 UI
콘텐츠 라이프 사이클 관리
파라미터들의 구성을 위한 UI
신뢰할 수 있는 SCHF-관련
파라미터들을 정의하기 위한 UI

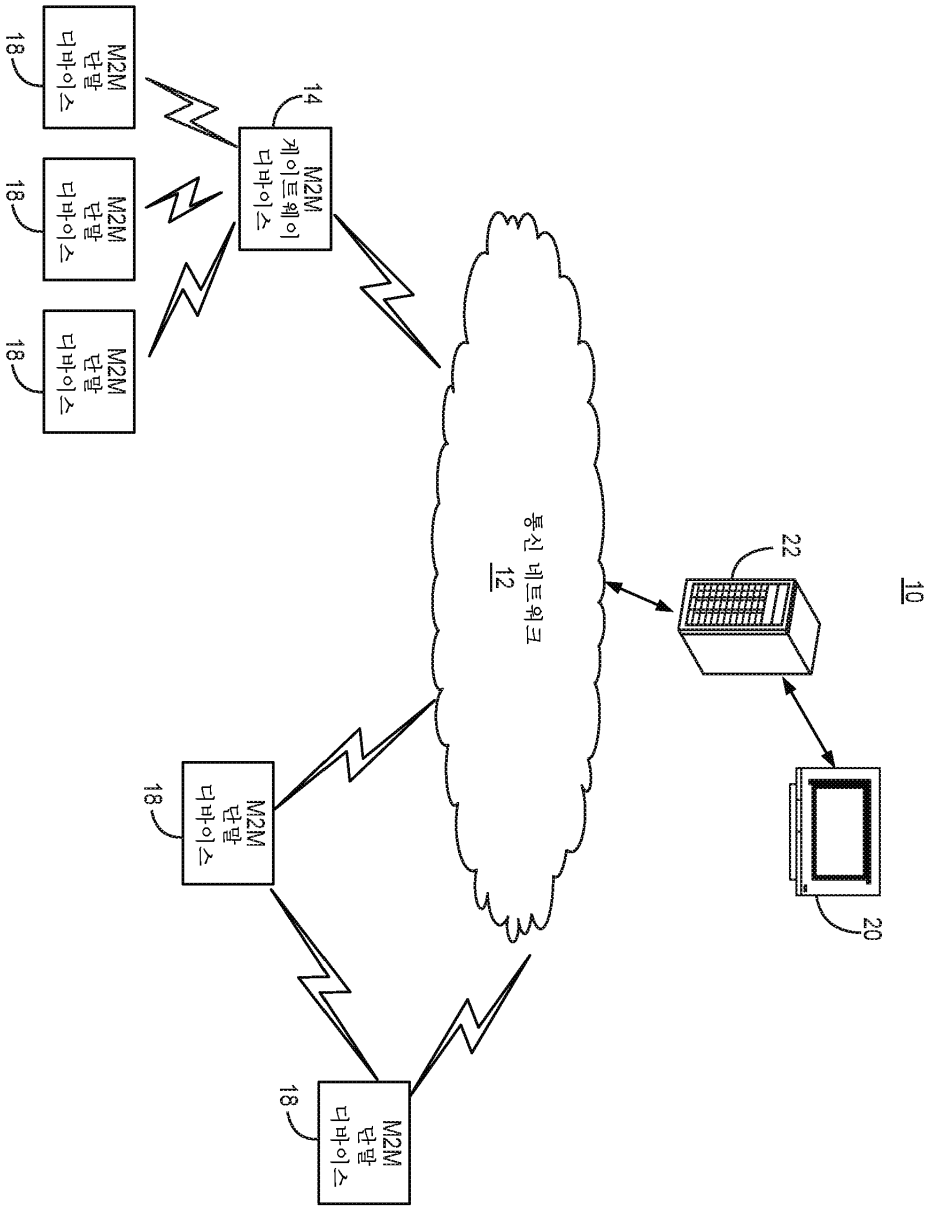
도면34


사용자
SCHF
보안 콘텐츠 호스팅에 관련한
보안 정책들의 구성을 위한 UI
콘텐츠 라이프 사이클 관리
파라미터들의 구성을 위한 UI
신뢰할 수 있는 SCHF-관련
파라미터들을 정의하기 위한 UI

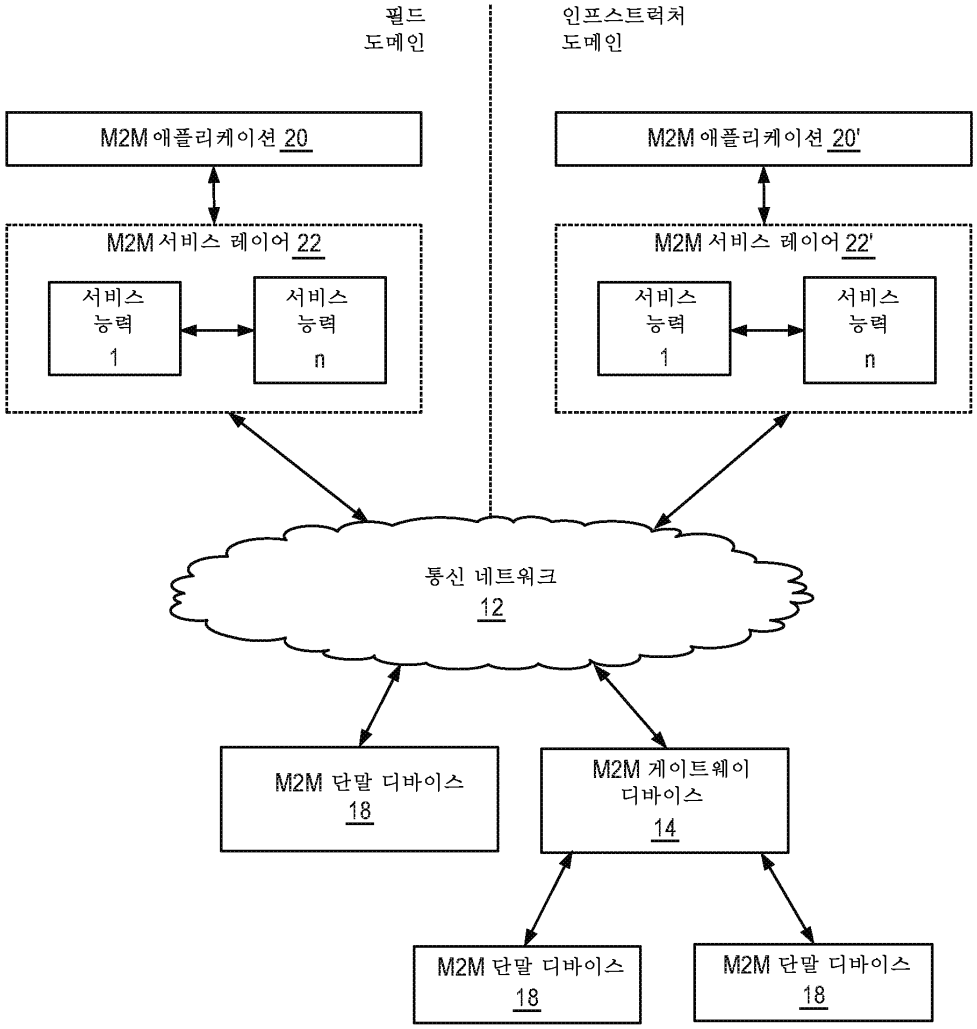
도면35


사용자
SEF
자격증명 프로비저닝 & 등록에 관련한 보안 정책들의 구성을 위한 UI
자격증명 관련 파라미터들의 구성을 위한 UI

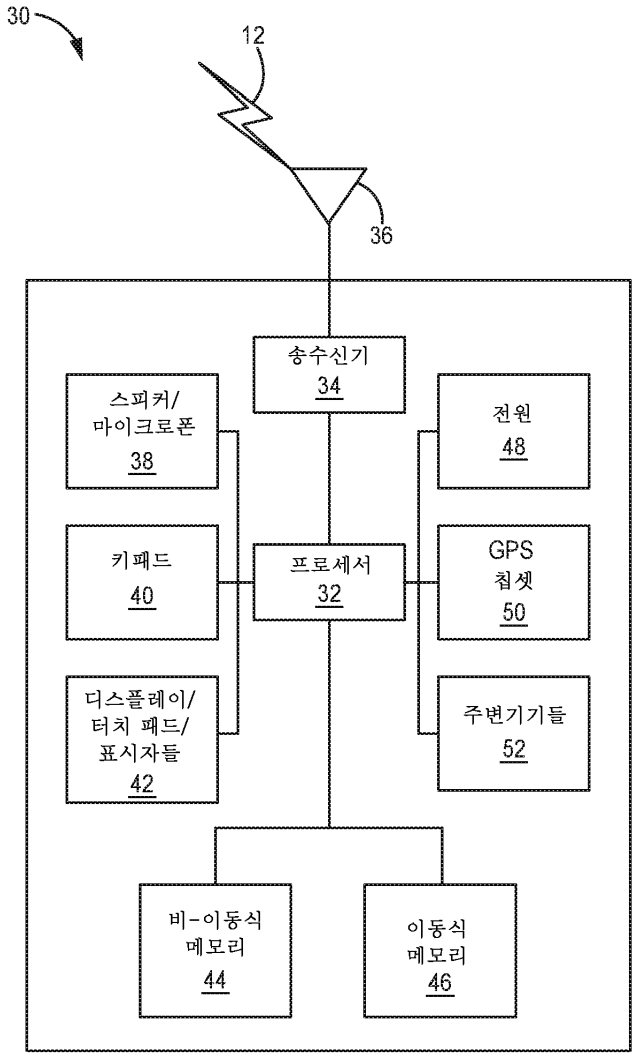
도면36a


M2M 단말 디바이스
18
M2M 게이트웨이 디바이스
14
통신 네트워크
12
22
10
20

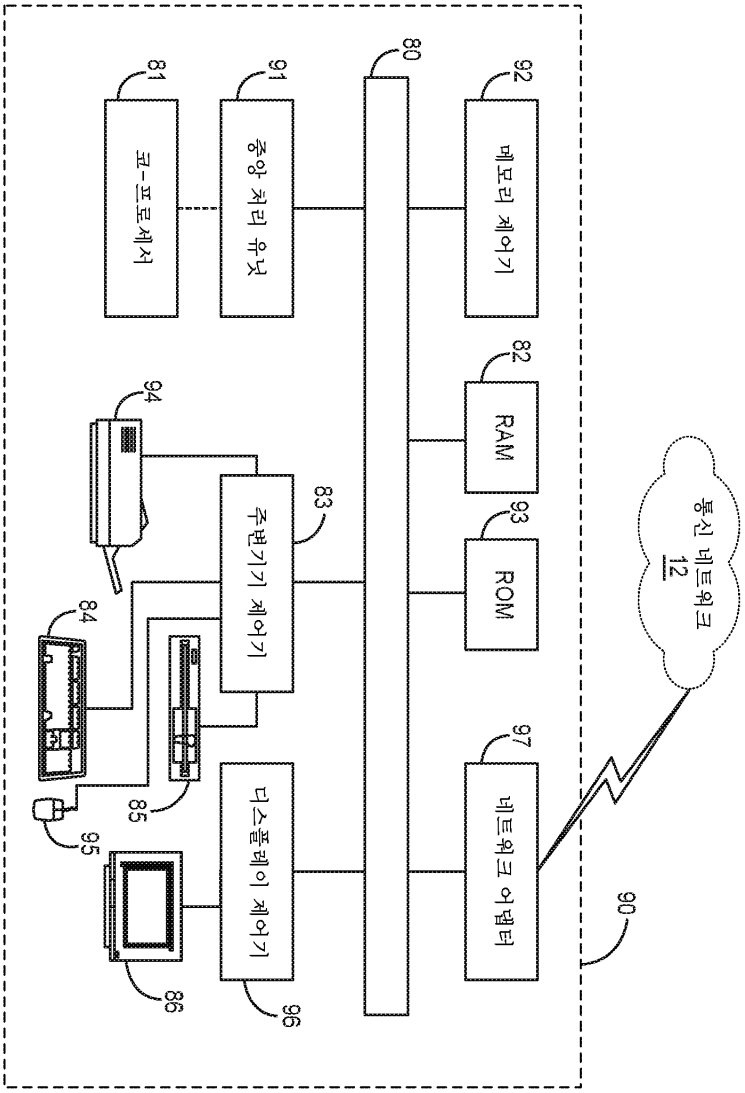
도면36b


필드
도메인
인프스트럭처
도메인
M2M 애플리케이션 20
M2M 애플리케이션 20'
M2M 서비스 레이어 22
서비스
능력
1
서비스
능력
n
M2M 서비스 레이어 22'
서비스
능력
1
서비스
능력
n
통신 네트워크
12
M2M 단말 디바이스
18
M2M 게이트웨이
디바이스
14
M2M 단말 디바이스
18
M2M 단말 디바이스
18

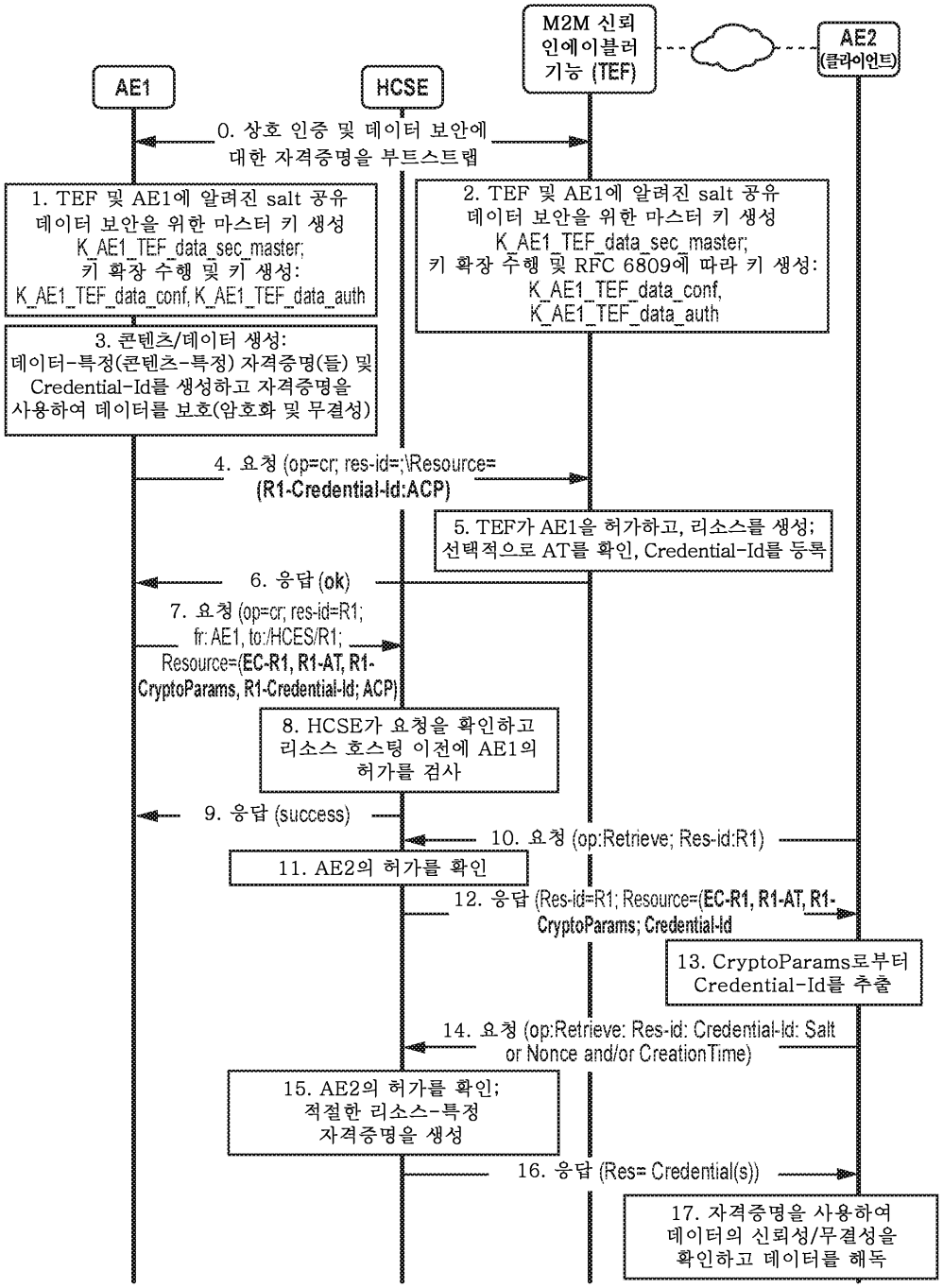
도면36c


30
12
36
송수신기
34
스피커/
마이크로폰
38
전원
48
키패드
40
프로세서
32
GPS
칩셋
50
디스플레이/
터치 패드/
표시자들
42
주변기기들
52
비-이동식
메모리
44
이동식
메모리
46

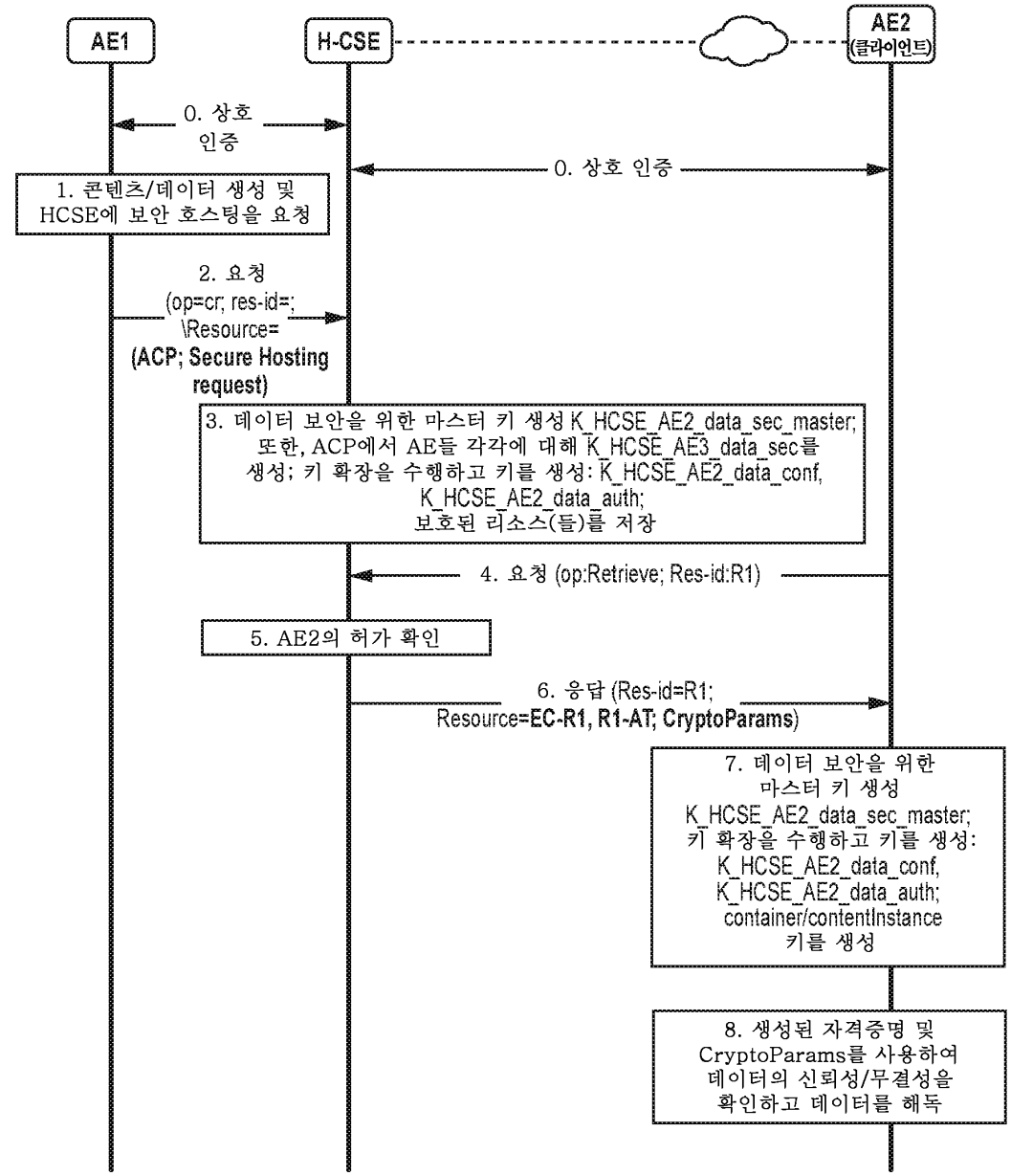
도면36d


80
81
코-프로세서
91
중앙 처리 유닛
92
메모리 제어기
82
RAM
93
ROM
97
네트워크 어댑터
90
통신 네트워크
12
83
주변기기 제어기
94
84
85
95
디스플레이 제어기
86
96

도면37


M2M 신뢰 인에이블러 기능 (TEF)
AE2 (클라이언트)
AE1
HCSE
0. 상호 인증 및 데이터 보안에 대한 자격증명을 부트스트랩
1. TEF 및 AE1에 알려진 salt 공유 데이터 보안을 위한 마스터 키 생성 K_AE1_TEF_data_sec_master; 키 확장 수행 및 키 생성: K_AE1_TEF_data_conf, K_AE1_TEF_data_auth
2. TEF 및 AE1에 알려진 salt 공유 데이터 보안을 위한 마스터 키 생성 K_AE1_TEF_data_sec_master; 키 확장 수행 및 RFC 6809에 따라 키 생성: K_AE1_TEF_data_conf, K_AE1_TEF_data_auth
3. 콘텐츠/데이터 생성: 데이터-특정(콘텐츠-특정) 자격증명(들) 및 Credential-Id를 생성하고 자격증명을 사용하여 데이터를 보호(암호화 및 무결성)
4. 요청 (op=cr; res-id=;\Resource= (R1-Credential-Id:ACP)
5. TEF가 AE1을 허가하고, 리소스를 생성; 선택적으로 AT를 확인, Credential-Id를 등록
6. 응답 (ok)
7. 요청 (op=cr; res-id=R1; fr: AE1, to:/HCES/R1; Resource={EC-R1, R1-AT, R1-CryptoParams, R1-Credential-Id; ACP}
8. HCSE가 요청을 확인하고 리소스 호스팅 이전에 AE1의 허가를 검사
9. 응답 (success)
10. 요청 (op:Retrieve; Res-id:R1)
11. AE2의 허가를 확인
12. 응답 (Res-id=R1; Resource={EC-R1, R1-AT, R1-CryptoParams; Credential-Id
13. CryptoParams로부터 Credential-Id를 추출
14. 요청 (op:Retrieve: Res-id: Credential-Id: Salt or Nonce and/or CreationTime)
15. AE2의 허가를 확인; 적절한 리소스-특정 자격증명을 생성
16. 응답 (Res= Credential(s))
17. 자격증명을 사용하여 데이터의 신뢰성/무결성을 확인하고 데이터를 해독

도면38


AE1
H-CSE
AE2
(클라이언트)
0. 상호 인증
0. 상호 인증
1. 콘텐츠/데이터 생성 및 HCSE에 보안 호스팅을 요청
2. 요청
(op=cr; res-id=;
\Resource=
(ACP; Secure Hosting request)
3. 데이터 보안을 위한 마스터 키 생성 K_HCSE_AE2_data_sec_master;
또한, ACP에서 AE들 각각에 대해 K_HCSE_AE3_data_sec를
생성; 키 확장을 수행하고 키를 생성: K_HCSE_AE2_data_conf,
K_HCSE_AE2_data_auth;
보호된 리소스(들)를 저장
4. 요청 (op:Retrieve; Res-id:R1)
5. AE2의 허가 확인
6. 응답 (Res-id=R1;
Resource=EC-R1, R1-AT; CryptoParams)
7. 데이터 보안을 위한
마스터 키 생성
K_HCSE_AE2_data_sec_master;
키 확장을 수행하고 키를 생성:
K_HCSE_AE2_data_conf,
K_HCSE_AE2_data_auth;
container/contentInstance
키를 생성
8. 생성된 자격증명 및
CryptoParams를 사용하여
데이터의 신뢰성/무결성을
확인하고 데이터를 해독