(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0028367
(43) 공개일자 2025년02월28일

(51) 국제특허분류(Int. Cl.)
G06F 21/64 (2013.01) *A24F 40/50* (2020.01)
G06F 21/44 (2013.01) *G06F 21/60* (2013.01)
H04L 9/06 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
G06F 21/64 (2013.01)
A24F 40/50 (2022.01)
(21) 출원번호 10-2025-7001592
(22) 출원일자(국제) 2023년05월22일
심사청구일자 없음
(85) 번역문제출일자 2025년01월16일
(86) 국제출원번호 PCT/EP2023/063563
(87) 국제공개번호 WO 2023/247120
국제공개일자 2023년12월28일
(30) 우선권주장
22181048.4 2022년06월24일
유럽특허청(EPO)(EP)

(71) 출원인
필립모리스 프로덕츠 에스.에이.
스위스, 씨에이취-2000, 네우차텔, 쿠아이 얀레나우드 3
(72) 발명자
파린, 로빈
스위스, 2000 뇌샤텔, 께 장르노 3
맥라우클런, 앤드류 제임스
스위스, 2000 뇌샤텔, 께 장르노 3
(74) 대리인
강철중

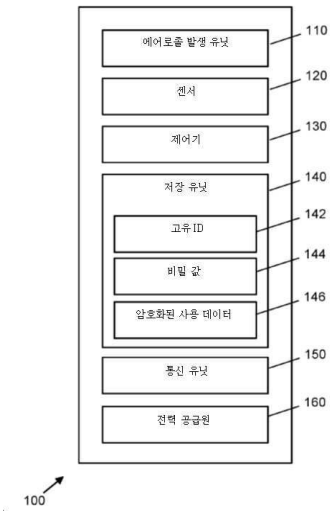
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **암호화된 데이터 관리를 갖는 에어로졸 발생 장치**

(57) 요 약

에어로졸 발생 장치로서, 비밀 값 및 고유 식별 값을 저장한 저장 유닛; 통신 유닛; 및 상기 에어로졸 발생 장치의 사용을 나타내는 사용 데이터를 생성하고, 적어도 저장된 비밀 값, 선택적으로, 고유 식별 값으로부터 암호화 키를 유도하고, 생성된 사용 데이터를 유도된 암호화 키로 암호화하고, 암호화된 사용 데이터를 저장 유닛에 저장하고, 및 암호화된 사용 데이터 및 고유 식별 값을 통신 유닛을 통해 외부 장치로 송신하도록 구성된 제어기를 포함하는, 에어로졸 발생 장치.

대 표 도 - 도1



(52) CPC특허분류
G06F 21/44 (2013.01)
G06F 21/602 (2013.01)
H04L 9/06 (2013.01)
H04L 9/3242 (2013.01)

명 세 서

청구범위

청구항 1

에어로졸 발생 장치로서,

비밀 값 및 고유 식별 값을 저장한 저장 유닛;

통신 유닛; 및

제어기를 포함하되, 상기 제어기는,

상기 에어로졸 발생 장치의 사용을 나타내는 사용 데이터를 생성하고,

적어도 저장된 비밀 값 및, 선택적으로, 고유 식별 값으로부터 암호화 키를 유도하고,

생성된 사용 데이터를 유도된 암호화 키로 암호화하고,

암호화된 사용 데이터를 저장 유닛에 저장하고,

상기 암호화된 사용 데이터 및 상기 고유 식별 값을 통신 유닛을 통해 외부 장치로 송신하도록 구성된 제어기를 포함하는, 에어로졸 발생 장치.

청구항 2

제1항에 있어서, 상기 제어기는 적어도 비밀 값 및 선택적으로 고유 식별 값으로부터 인증 키를 유도하고, 저장된 사용 데이터를 유도된 인증 키로 인증하도록 추가로 구성되는, 에어로졸 발생 장치.

청구항 3

제1항 또는 제2항에 있어서, 상기 제어기는 생성된 사용 데이터를 암호화하기 위해 대칭 키 알고리즘을 사용하도록 구성되는, 에어로졸 발생 장치.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 제어기는 상기 비밀 값 및/또는 상기 고유 식별 값으로부터 초기화 벡터를 유도하고, 상기 암호화 키 및 상기 초기화 벡터를 사용하여 카운터 모드에서 블록 암호를 적용함으로써 상기 생성된 사용 데이터를 암호화하도록 추가로 구성되는, 에어로졸 발생 장치.

청구항 5

제1항 내지 제4항 중 어느 한 항에 있어서, 상기 제어기는 상기 생성된 사용 데이터에 대한 메시지 인증 코드, MAC를 연산함으로써 상기 생성된 사용 데이터를 인증하도록 추가로 구성되는, 에어로졸 발생 장치.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서, 상기 제어기는 상기 암호화된 사용 데이터에 대한 MAC를 연산함으로써 암호화된 사용 데이터를 인증하도록 추가로 구성되는, 에어로졸 발생 장치.

청구항 7

제5항 또는 제6항에 있어서, 상기 제어기는, 해시 함수의 출력을 미리 정의된 바이트 수로 잘라내어, 생성된 사용 데이터에 대한 MAC 및/또는 암호화된 사용 데이터에 대한 MAC를 연산하도록 추가로 구성되는, 에어로졸 발생 장치.

청구항 8

제5항 내지 제7항 중 어느 한 항에 있어서, 상기 제어기는 상기 생성된 사용 데이터에 대한 MAC 및/또는 상기 암호화된 사용 데이터에 대한 MAC를 상기 저장 유닛 내의 암호화된 사용 데이터와 함께 저장하도록 추가로 구성

되는, 에어로졸 발생 장치.

청구항 9

제1항 내지 제8항 중 어느 한 항에 있어서, 상기 제어기는, 상기 비밀 값 및/또는 상기 고유 식별 값으로부터, 상기 생성된 사용 데이터를 암호화하기 위한 암호화 키, 카운터 모드에서 블록 암호로 상기 생성된 사용 데이터를 암호화하기 위한 초기화 벡터, 및 상기 사용 데이터를 인증하기 위한 인증 키 중 적어도 하나를 유도하기 위해, 해시 기반 키 유도 함수인 HKDF를 사용하도록 추가로 구성되는, 에어로졸 발생 장치.

청구항 10

제9항에 있어서, 생성된 사용 데이터로부터 연산된 메시지 인증 코드 MAC의 적어도 일부는 초기화 벡터를 유도하기 위한 솔트로서 사용되는, 에어로졸 발생 장치.

청구항 11

에어로졸 발생 시스템으로서,

제1항 내지 제10항 중 어느 한 항에 따른 에어로졸 발생 장치;

상기 에어로졸 발생 장치의 비밀 값과 연관된 복수의 에어로졸 발생 장치 각각의 고유 식별 값을 저장하도록 구성된 데이터베이스; 및

상기 에어로졸 발생 장치로부터, 암호화된 사용 데이터 및 상기 에어로졸 발생 장치의 고유 식별 값을 수신하고,

상기 고유 식별 값을 사용하여 상기 데이터베이스로부터 상기 고유 식별 값과 연관된 상기 비밀 값을 검색하고,

검색된 비밀 값을 사용하여 암호화된 사용 데이터를 복호화하도록 구성되는,

서버를 포함하는, 에어로졸 발생 시스템.

청구항 12

에어로졸 발생 장치를 작동시키기 위한 방법으로서, 상기 방법은,

비밀 값 및 고유 식별 값을 상기 에어로졸 발생 장치의 저장 유닛에 저장하는 단계;

상기 에어로졸 발생 장치의 사용을 나타내는 사용 데이터를 생성하는 단계;

적어도 상기 저장된 비밀 값 및 선택적으로 상기 고유 식별 값으로부터 암호화 키를 유도하는 단계;

상기 생성된 사용 데이터를 상기 유도된 암호화 키로 암호화하는 단계;

상기 암호화된 사용 데이터를 상기 저장 유닛에 저장하는 단계; 및

상기 암호화된 사용 데이터 및 상기 고유 식별 값을 통신 유닛을 통해 외부 장치로 송신하는 단계를 포함하는, 방법.

청구항 13

에어로졸 발생 장치로부터 호스트로 사용 데이터를 송신하는 방법으로서, 상기 에어로졸 발생 장치는 비밀 값 및 고유 식별 값을 저장하고, 상기 방법은,

호스트에서 에어로졸 발생 장치로부터 고유 식별 값을 수신하는 단계;

각각의 고유 식별 값과 연관된 복수의 에어로졸 발생 장치 각각의 비밀 값이 저장된 데이터베이스로부터 에어로졸 발생 장치의 비밀 값을 검색하는 단계;

호스트에서, 적어도 검색된 비밀 값 및 선택적으로 수신된 고유 식별 값으로부터 암호화 키를 유도하는 단계;

호스트에서 에어로졸 발생 장치로부터 암호화된 사용 데이터를 수신하는 단계; 및

수신된 암호화된 사용 데이터를 암호화 키로 복호화하는 단계를 포함하는, 방법.

청구항 14

제13항에 있어서,

상기 호스트에서, 적어도 검색된 비밀 값 및 선택적으로 고유 식별 값으로부터 인증 키를 유도하는 단계;

상기 호스트에서 에어로졸 발생 장치로부터 암호화된 사용 데이터와 함께 제1 메시지 인증 코드 MAC를 수신하는 단계;

복호화된 사용 데이터 및 유도된 인증 키로부터 제2 MAC를 연산하는 단계; 및

제1 MAC와 제2 MAC를 비교하는 단계를 추가로 포함하는, 방법.

청구항 15

제14항에 있어서,

초기화 벡터를 유도하는 단계를 추가로 포함하고;

상기 수신된 암호화된 사용 데이터는, 상기 암호화 키 및 상기 초기화 벡터를 사용하여 카운터 모드에서 블록 암호를 적용함으로써 복호화되는, 방법.

발명의 설명

기 술 분 야

[0001] 본 개시는 에어로졸 발생 장치, 특히 사용 데이터를 생성, 저장 및 송신하는 에어로졸 발생 장치, 뿐만 아니라 에어로졸 발생 장치 및 서버를 포함하는 시스템, 에어로졸 발생 장치를 작동시키기 위한 방법, 에어로졸 발생 장치로부터 서버로 데이터를 송신하기 위한 방법, 및 에어로졸 발생 장치를 제조하기 위한 방법에 관한 것이다.

배 경 기 술

[0002] 액체 또는 고체 전구체 물질을 가열함으로써 흡입 가능한 에어로졸을 발생시키는 전자 궐련 또는 위험 감소 장치와 같은, 에어로졸 발생 장치는 작동 중에 사용 데이터를 생성하고 저장한다. 사용 데이터는 장치의 기능적 작동 및 상태 및 장치의 소비자 사용 둘 모두에 관한 것일 수 있다. 실시예는 에어로졸 발생, 온도, 배터리 수준, 이벤트 및 오류를 포함한다. 이 데이터 중 일부는 제조업자 서버에 통신될 수 있다.

[0003] 이렇게 생성된 사용 데이터의 보호가 바람직한 몇 가지 이유가 있다. 우선, 데이터 보호 규정은 고객의 개인 정보를 보호하기 위한 조치를 규정할 수 있다. 또한, 기능 정보의 기밀성을 보장하면, 제조업자가 장치 기능 또는 성능에 대한 통찰력을 경쟁업자에게 제공하는 것을 보호한다. 이는 또한, 고객의 경험을 저하시키는 악의적이거나 품질이 불량한 제3자 서비스에 제조업자 생태계를 개방하는 것을 피할 수 있게 한다. 또한, 제조업자 서버에서 수집된 데이터의 무결성 및 진위성을 보장하면 이들 서버가 악의적으로 또는 실수로 업로드된 거짓 또는 손상된 정보로 오염되는 것을 보호한다.

[0004] 따라서, 에어로졸 발생 장치에 저장된 데이터를 보호하고 장치 내부 및 외부 송신 시 데이터 기록의 기밀성을 보장할 필요가 있다. 또한, 에어로졸 발생 장치로부터 데이터를 수집하는 서버가 거짓 또는 손상된 정보로 오염되는 것을 보호할 필요가 있다.

[0005] 데이터 암호화, 복호화 및 인증을 위한 암호화 알고리즘이 당 업계에 많이 알려져 있다. 이들 알고리즘 중 다수는 연산적으로 복잡하거나, 임베디드 시스템에서 구현하기에 적합하지 않거나, 안전하지 않다.

발명의 내용

[0006] 본 발명의 목적은 복잡성 및 제조 비용의 과도한 증가 없이 그리고 유용성에 대한 임의의 제한 없이 사용 데이터를 보호할 수 있는 에어로졸 발생 장치뿐만 아니라 상응하는 방법 및 시스템을 제공하는 것이다.

[0007] 이는 독립 청구항의 특징부에 의해 달성된다. 바람직한 구현예는 종속 청구항의 주제이다.

[0008] 본 발명의 특정 접근법은 각각의 에어로졸 발생 장치에 장치 내에 저장되는 고유 식별자 및 비밀 값을 제공하는 것이다. 적어도 비밀 값은 사용 데이터를 암호화하기 위한 암호화 키를 유도하기 위해 장치에 의해 사용된다. 암호화된 사용 데이터 및 고유 식별자는 제조업자 서버에 송신될 수 있다. 제조업자 서버는 고유 식별자와 관련

하여 비밀 값을 저장하는 데이터베이스에 액세스할 수 있다. 따라서, 제조업자 서버는 데이터베이스로부터 비밀 값을 검색하고, 장치로부터 송신된 암호화된 사용 데이터를 해독하기 위한 암호화 키를 유도할 수 있다.

[0009] 본 발명의 제1 측면에 따르면, 비밀 값 및 고유 식별 값을 저장한 저장 유닛을 포함하는 에어로졸 발생 장치가 제공된다. 에어로졸 발생 장치는 또한 통신 유닛 및 제어기를 더 포함한다. 제어기는 에어로졸 발생 장치의 사용을 나타내는 사용 데이터를 생성하고, 적어도 저장된 비밀 값 및 선택적으로 고유 식별 값으로부터 암호화 키를 유도하고, 생성된 사용 데이터를 유도된 암호화 키로 암호화하고, 암호화된 사용 데이터를 저장 유닛에 저장하고, 암호화된 사용 데이터 및 고유 식별 값을 통신 유닛을 통해 외부 장치에 송신 하도록 구성된다.

[0010] 본 발명의 제2 측면에 따르면, 에어로졸 발생 장치를 작동시키기 위한 방법이 제공된다. 상기 방법은 에어로졸 발생 장치의 저장 유닛에 비밀 값 및 고유 식별 값을 저장하는 단계, 에어로졸 발생 장치의 사용을 나타내는 사용 데이터를 생성하는 단계, 적어도 저장된 비밀 값 및 선택적으로 고유 식별 값으로부터 암호화 키를 유도하는 단계, 생성된 사용 데이터를 유도된 암호화 키로 암호화하는 단계, 암호화된 사용 데이터를 저장 유닛에 저장하는 단계, 및 암호화된 사용 데이터 및 고유 식별 값을 통신 유닛을 통해 외부 장치로 송신하는 단계를 포함한다.

[0011] 에어로졸 발생 장치에 저장된 비밀 값으로부터 암호화 키를 유도함으로써, 에어로졸 발생 장치와 제조업자 서버와 같은 외부 장치 사이의 키 교환을 위한 복잡한 프로토콜이 구현될 필요가 없다. 에어로졸 발생 장치 내에 고유 식별 값을 저장하고 암호화된 사용 데이터와 함께 외부 장치에 송신하면, 상이한 에어로졸 발생 장치가 사용 데이터를 암호화하기 위해 상이한 암호화 키를 사용하는 경우에도 외부 장치가 적절한 암호화 키를 유도할 수 있게 한다. 상이한 에어로졸 발생 장치에 대해 상이한 암호화 키를 사용하면, 다른 에어로졸 발생 장치가 파손되거나 그 비밀 값이 유출되는 경우에도 에어로졸 발생 장치의 암호화된 사용 데이터가 안전하게 유지되는 것을 보장한다.

[0012] 용어 "유도"는 "B"(예: 비밀 값)로부터 "A"(예: 암호화 키)를 획득하거나 결정하는 것을 지칭하기 위해 본원에서 사용된다. 일 실시예에서, "A"는 "B"로부터 직접 유도되며, 예를 들어, "A"가 "B", 또는 "B"의 적어도 일부와 같은 경우이다. 다른 예에서, 예를 들어 "B" 상에서 연산을 수행하여 "A"를 획득함으로써 "A"는 "B"로부터 간접적으로 유도된다.

[0013] 바람직하게는, 제어기 및/또는 방법은 적어도 비밀 값 및 선택적으로 고유 식별 값으로부터 인증 키를 유도하고, 저장된 사용 데이터를 유도된 인증 키로 인증하도록 추가로 구성된다.

[0014] 사용 데이터에 (암호화) 인증 코드를 제공하면 사용 데이터의 인증 및 의도적이거나 우발적인 수정의 검출을 가능하게 한다. 에어로졸 발생 장치에 저장된 비밀 값으로부터 인증 키를 유도함으로써, 각각의 에어로졸 발생 장치에 전용 인증 키를 제공하기 위한 추가 프로토콜은 필요하지 않다.

[0015] 바람직하게는, 고유 식별 값은 제품 식별자, 플랫폼 식별자, 고유 장치 식별자 및 제조 현장 식별자 중 적어도 하나를 포함한다.

[0016] 고유 식별 값으로서, 일련 번호와 같은 고유 장치 식별자 대신에 또는 이와 조합하여 제품 관련 정보를 제공하면 외부 장치가 통신하는 에어로졸 발생 장치의 종류를 쉽게 이해할 수 있게 한다.

[0017] 바람직하게는, 비밀 값은 에어로졸 발생 장치의 제조 단계 동안 생성된 난수 값이다.

[0018] 난수를 비밀 값으로 사용하면, 에어로졸 발생 장치의 비밀 값이 다른 에어로졸 발생 장치의 (유출된) 비밀 값으로부터 유도될 수 없고, 이에 따라 가능한 암호화 공격에 대해 시스템을 추가로 강화시킬 수 있다는 이점을 갖는다. 에어로졸 발생 장치의 제조 단계 동안 비밀 값을 생성하면 이러한 민감한 정보를 보호하기 위해 적절한 주의가 취해질 수 있게 한다.

[0019] 바람직하게는, 에어로졸 발생 장치는 에어로졸 발생 장치의 작동 상태를 검출하기 위한 센서를 더 포함한다. 따라서, 제어기 및/또는 방법은 검출된 작동 상태에 기초하여 사용 데이터를 생성하도록 구성될 수 있다. 다양한 유형의 센서, 특히, 에어로졸 발생 장치와의 사용자 상호 작용을 검출하도록 구성된 센서, 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프를 검출하도록 구성된 센서, 에어로졸 발생 장치의 에어로졸 발생 유닛에 관한 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하도록 구성된 센서, 에어로졸 발생 장치의 전력 공급부에 관한 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하기 위한 센서, 에어로졸 발생 장치에 연결된 충전 장치에 관한 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하기 위한 센서, 및/또는 에어로졸 발생 유닛에 의해 사용되는 소모성 재료의 유형 또는 양을 검출하기 위한 센서가 사용될 수 있다.

[0020] 따라서, 상이한 유형의 센서는 사용자 및/또는 제조업자와 관련될 수 있는 상이한 종류의 사용 정보가 검출될 수 있게 한다. 예를 들어, 사용 데이터는 다음 중 적어도 하나의 표시를 포함할 수 있다:

[0021] 시작 시간, 지속 시간, 종료 시간, 또는 사용자 상호 작용의 유형,

[0022] 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프 또는 퍼프 횟수의 시작 시간, 지속 시간, 또는 종료 시간,

[0023] 에어로졸 발생 장치를 충전 장치에 연결함으로써 사용자에 의해 수행되는 충전 동작의 시작 시간, 지속 시간, 또는 종료 시간, 또는 충전 동작 수,

[0024] 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프의 시작 시, 퍼프 도중, 또는 퍼프의 종료 시 에어로졸 발생 장치의 에어로졸 발생 유닛과 관련된 전압, 전류, 저항, 전하, 에너지 또는 온도,

[0025] 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프의 시작 시, 퍼프 동안, 또는 퍼프의 종료 시 에어로졸 발생 장치의 전력 공급부와 관련된 전압, 전류, 저항, 전하, 에너지 또는 온도,

[0026] 충전 동작의 시작 시, 충전 동작 동안, 또는 충전 동작의 종료 시 에어로졸 발생 장치의 전력 공급부에 관한 전압, 전류, 저항, 충전, 에너지 또는 온도,

[0027] 에어로졸 발생 유닛에 의해 사용되는 소모성 재료의 유형 또는 양.

[0028] 바람직하게는, 제어기 및/또는 방법은 암호화된 사용 데이터를 데이터 레코드의 페이로드 섹션에 저장하도록 구성된다. 각각의 데이터 레코드는 헤더, 페이로드 섹션, 및 인증 섹션을 포함할 수 있다. 또한, 각각의 헤더는 데이터 레코드의 형식을 나타내는 제1 데이터 필드 및 데이터 레코드의 길이를 나타내는 제2 데이터 필드를 포함할 수 있다.

[0029] 사용 데이터를 저장 및/또는 송신하기 위한 미리 정의된 데이터 형식을 사용하면 에어로졸 발생 장치와 외부 장치 간의 소프트웨어 인터페이스를 정의할 수 있으므로, 에어로졸 발생 장치 측과 외부 장치 측의 소프트웨어가 서로 독립적으로 개발되고 유지될 수 있다. 또한, 상이한 유형의 에어로졸 발생 장치는 동일한 데이터 형식을 사용할 수 있으므로, 상이한 장치의 상호 운용성을 개선할 수 있다.

[0030] 바람직하게는, 각각의 데이터 레코드는 또한 레코드 인덱스와 연관될 수 있다. 따라서, 레코드 인덱스는 에어로졸 발생 장치 내에 저장된 복수의 상이한 데이터 레코드를 관리하는 데 사용될 수 있다. 레코드 인덱스는 또한 에어로졸 발생 장치로부터 외부 장치로 송신된 각각의 데이터 기록에 대한 고유 식별자(Record Unique Identity, RUID)로서(의 일부로서) 사용될 수 있다.

[0031] 바람직하게는, 각각의 헤더는 레코드 인덱스가 롤오버된 횟수를 나타내는 제3 데이터 필드를 더 포함한다. 이러한 방식으로, 레코드 인덱스가 데이터 레코드를 관리하기 위해 에어로졸 발생 장치에 의해 내부적으로만 사용되는 경우 및 이전 데이터 레코드 중 일부가 더 최근의 데이터 레코드에 의해 이미 덮어쓰여진 경우에도, 각각의 데이터 레코드는 고유하게 식별된다.

[0032] 바람직하게는, 제어기 및/또는 방법은 생성된 사용 데이터를 암호화하기 위한 대칭 키 알고리즘을 사용하도록 적응된다. 바람직하게는, AES가 대칭 키 알고리즘으로서 사용된다.

[0033] 대칭 키 알고리즘은 키 생성/분배 및 암호화/복호화 모두에서 비대칭 키 기반 알고리즘보다 훨씬 덜 복잡하다. 종래의 대칭 키 알고리즘 중에서, AES는 임베디드 시스템에서 구현하기에 특히 적합한 잘 확립된 알고리즘이다.

[0034] 바람직하게는, 제어기 및/또는 방법은 비밀 값 및/또는 고유 식별 값으로부터 초기화 벡터를 유도하고, 암호화 키 및 초기화 벡터를 사용하여 카운터 모드에서 블록 암호를 적용함으로써 생성된 사용 데이터를 암호화하도록 적응된다.

[0035] 카운터 모드에서 블록 암호를 적용하면 블록 암호를 가변 길이 데이터 블록에 적용하기 위한 보안 방법이며, 암호화 및 복호화 측면 모두에서 낮은 복잡성 구현을 허용한다. 카운터 모드를 위한 초기화 벡터를 비밀 값 및/또는 고유 식별 값으로부터 유도함으로써, 추가 정보를 저장 및/또는 송신할 필요가 없다.

[0036] 바람직하게는, 제어기 및/또는 방법은 비밀 값 및/또는 고유 식별 값으로부터 초기화 벡터를 유도하기 위해 해시 기반 키 유도 함수인 HKDF를 사용하도록 적응된다. 구체적으로, 제어기 및/또는 방법은 바람직하게는, 미리 정의된 값, 생성된 사용 데이터를 포함하는 데이터 레코드와 연관된 레코드 인덱스의 값, 데이터 레코드의 유형, 및 생성된 사용 데이터에 대해 연산된 메시지 인증 코드인, MAC의 적어도 일부 중 적어도 하나를 포함하는 솔트를 사용해 비밀 값 및/또는 고유 식별 값으로부터 초기화 벡터를 유도하도록 구성될 수 있다.

[0037] HKDF는 제한된 길이의 입력 키 재료로부터 임의의 길이를 갖는 키 자료를 유도하기 위한 안전한 수단을 제공한다. 미리 정의된 값을 포함하는 솔트를 사용함으로써, 특히 생성된 사용 데이터를 포함하는 데이터 레코드와 연관된 레코드 인덱스의 값, 데이터 레코드의 유형, 및 생성된 사용 데이터에 대해 연산된 메시지 인증 코드 MAC의 적어도 일부 중 적어도 하나를 포함하는 솔트를 사용함으로써 보안이 추가로 개선된다. 이 방식으로, 상이한 초기화 벡터가 상이한 데이터 레코드에 사용됨으로써, 동일한 키로 암호화되는 암호문의 양을 극적으로 감소시킴으로써 암호화 분석에 대해 시스템을 더욱 강화시킨다. 초기화 벡터가 페이로드의 특성으로부터 유도되거나 구성되도록 보장하면, 반복된 레코드 인덱스 또는 고유 레코드 식별자(RUID)를 강제하는 데 성공할 수 있는 공격의 경우에 반복된 초기화 벡터를 생성하는 것을 방지할 수 있다.

[0038] 바람직하게는, 제어기 및/또는 방법은 생성된 사용 데이터에 대한 메시지 인증 코드 MAC를 연산함으로써 생성된 사용 데이터를 인증하도록 적응된다. 구체적으로, 제어기 및/또는 방법은 생성된 사용 데이터로부터 및 제1 인증 키로부터 생성된 사용 데이터에 대한 MAC를 연산하도록 구성될 수 있다.

[0039] 생성된 사용 데이터, 즉 일반 텍스트의 사용 데이터에 대한 MAC를 연산하면 MAC가 키 유도 함수에 대한 추가 입력으로서 사용될 수 있게 하여, 상이한 키 및/또는 초기화 벡터가 사용 데이터의 상이한 항목에 사용되는 것을 보장한다.

[0040] 바람직하게는, 제어기 및/또는 방법은 암호화된 사용 데이터에 대한 MAC를 연산함으로써 암호화된 사용 데이터를 인증하도록 적응된다. 구체적으로, 제어기 및/또는 방법은 암호화된 사용 데이터로부터 및 제2 인증 키로부터 암호화된 사용 데이터에 대한 MAC를 연산하도록 구성될 수 있다. 제어기 및/또는 방법은 또한 암호화된 사용 데이터로부터, 생성된 사용 데이터를 위한 MAC로부터, 및 제2 인증 키로부터 암호화된 사용 데이터에 대한 MAC를 연산하도록 구성될 수 있다.

[0041] 일반 텍스트 사용 데이터에 대한 MAC 대신에 또는 이에 추가하여, 암호화된 사용 데이터에 대한 MAC를 연산하면 암호화 분석에 대해 시스템을 추가로 강화하는데, 이는 변조된 데이터 레코드가 복호화 전에 이미 검출될 수 있기 때문이다. 이 방식으로, 조작된 암호 텍스트에 기초한 암호화 공격이 저지될 수 있다. 암호화된 사용 데이터 및 제2 인증 키뿐만 아니라 생성된 사용 데이터를 위한 MAC로부터 암호화된 사용 데이터에 대한 MAC를 연산하면, 생성된 사용 데이터에 대한 MAC가 인증될 수 있게 함으로써 스푸핑 공격에 대한 보안을 더욱 개선한다.

[0042] 바람직하게는, 제어기 및/또는 방법은 비밀 값 및/또는 고유 식별 값으로부터 제1 인증 키 및/또는 제2 인증 키를 유도하도록 적응된다.

[0043] 에어로졸 발생 장치에 저장된 비밀 값으로부터 인증 키를 유도함으로써, 각각의 에어로졸 발생 장치에 전용 인증 키를 제공하기 위한 추가 프로토콜은 필요하지 않다.

[0044] 바람직하게는, 제어기 및/또는 방법은 생성된 사용 데이터에 대한 MAC 및/또는 암호화된 사용 데이터에 대한 MAC를 연산하기 위한 해시 함수를 사용하도록 적응된다. 또한, 제어기 및/또는 방법은 해시 함수의 출력을 미리 정의된 수의 바이트로 잘라내어 생성된 사용 데이터에 대한 MAC 및/또는 암호화된 사용 데이터에 대한 MAC를 연산하도록 추가로 구성될 수 있다. 또한, 제어기 및/또는 방법은, 생성된 사용 데이터에 대한 MAC 및/또는 암호화된 사용 데이터에 대한 MAC를 저장 유닛 내의 암호화된 사용 데이터와 함께 저장하도록 추가로 구성될 수 있다.

[0045] 생성된 사용 데이터에 대한 MAC 및/또는 암호화된 사용 데이터에 대한 MAC로서 해시 함수의 출력으로부터 잘라낸 제한된 수의 바이트, 특히 2바이트, 3바이트 또는 4바이트를 사용하면 MAC를 저장하는 데 필요한 추가 저장 용량의 양과 사용 데이터를 변조 방지하기 위해 달성될 수 있는 보안 수준 사이에서 최적의 절충안을 제공한다.

[0046] 바람직하게는, 제어기 및/또는 방법은, 비밀 값 및/또는 고유 식별 값으로부터, 생성된 사용 데이터를 암호화하기 위한 암호화 키, 카운터 모드에서 블록 암호로 생성된 사용 데이터를 암호화하기 위한 초기화 벡터, 및 사용 데이터를 인증하기 위한 인증 키 중 적어도 하나를 유도하기 위한 해시 기반 키 유도 함수인, HKDF를 사용하도록 적응된다. 구체적으로, 비밀 값 및/또는 고유 식별 값의 적어도 일부는 키 유도 함수를 위한 입력 키 자료로서 사용될 수 있다.

[0047] 해시 기반 키 유도 함수는 제한된 양의 입력 키 자료로부터 암호화 보안 키를 유도하기 위한 특히 효율적인 수단이다. 비밀 값 및/또는 고유 식별 값의 적어도 일부를 암호화 키, 초기화 벡터 또는 인증 키를 유도하기 위한 프로세스에 포함시키면 각각의 에어로졸 발생 장치가 사용자 데이터를 암호화 및/또는 인증하기 위해 상이한 키

를 사용하는 것을 보장한다. 따라서, 복수의 에어로졸 발생 장치를 포함하는 시스템의 전체 보안은 동일한 키로 인코딩 및/또는 인증되는 암호문의 양을 감소시킴으로써 상당히 개선된다.

[0048] 바람직하게는, 솔트는 비밀 값 및/또는 고유 식별 값의 적어도 일부와 함께 키 유도 함수를 위한 입력 키 자료로서 사용된다. 또한, 고정된 솔트는 암호화 키 및/또는 인증 키를 유도하는 데 사용될 수 있다.

[0049] 솔트, 즉 해시 함수에 대한 추가 입력으로서 사용되는 랜덤 데이터를 사용하면, 특히 사전 계산된 해시 체인을 기반으로 하는 공격으로부터 시스템을 강화함으로써, 암호화 보안을 더욱 개선한다.

[0050] 바람직하게는, 비밀 값의 비트 표현의 미리 정의된 서브세트가, 고유 식별 값 및 솔트와 함께, 키 유도 함수를 위한 입력 키 자료로서 사용될 수 있다. 또한, 암호화 키 및/또는 인증 키를 유도하기 위한 입력 키 자료로서 사용된 비밀 값의 비트 표현의 미리 정의된 서브세트는 바람직하게는 초기화 벡터를 유도하기 위한 입력 키 자료로서 사용된 비밀 값의 비트 표현의 미리 정의된 서브세트와 상이하다.

[0051] 비밀 값의 비트 표현의 상이한 서브세트로부터 암호화 키 및 인증 키를 유도하면 암호화 분석에 대해 시스템을 더욱 강화시킬 수 있다.

[0052] 바람직하게는, 생성된 사용 데이터로부터 연산된 메시지 인증 코드 MAC의 적어도 일부는 초기화 벡터를 유도하기 위한 솔트로서 사용된다.

[0053] 이 방식으로, 상이한 사용 데이터 아이템에 대한 초기화 벡터를 유도하기 위해 상이한 솔트가 사용되며, 따라서 이들 사용 데이터 아이템을 암호화하기 위한 상이한 키를 효과적으로 생성한다.

[0054] 바람직하게는, 키 유도 함수에 의해 생성된 출력 키 자료의 제1 부분은 암호화 키로서 사용되고, 제1 부분과 상이한 출력 키 자료의 제2 부분은 인증 키로서 사용된다.

[0055] 이 방식으로, 키 유도 함수에 대한 단일 호출로 암호화 키 및 인증 키 둘 다를 생성하기에 충분하다.

[0056] 바람직하게는, 제어기 및/또는 방법은 통신 유닛을 통해 암호화된 사용 데이터의 인증 코드와 함께 암호화된 사용 데이터를 외부 장치로 송신하도록 적응된다.

[0057] 이 방식으로, 외부 장치는, 송신된 사용 데이터를 인증하기 위해 암호화된 데이터에 대한 인증 코드를 검증할 수 있다.

[0058] 본 개시의 맥락에서, 외부 장치는 충전 스테이션, 도킹 스테이션, 모바일 단말기, 개인용 컴퓨터, 호스트 컴퓨터, 및 서버와 같은 에어로졸 발생 장치에 통신 가능하게 결합될 수 있는 임의의 장치일 수 있다. 또한, 에어로졸 발생 장치와 외부 장치 사이의 데이터 통신은 데이터 케이블, 근거리 통신, 블루투스, BLE, 및 WiFi 등을 포함하지만 이에 한정되지 않는 임의의 적합한 통신 프로토콜 및/또는 매체에 기초할 수 있다.

[0059] 본 발명의 제3 측면에 따르면, 본 발명의 제1 측면에 따른 에어로졸 발생 장치, 에어로졸 발생 장치의 비밀 값과 관련하여 복수의 에어로졸 발생 장치 각각의 고유 식별 값을 저장하도록 구성된 데이터베이스, 및 서버를 포함하는 에어로졸 발생 시스템이 제공된다. 서버는, 에어로졸 발생 장치로부터, 암호화된 사용 데이터 및 에어로졸 발생 장치의 고유 식별 값을 수신하고, 고유 식별 값을 사용하여 데이터베이스로부터 고유 식별 값과 연관된 비밀 값을 검색하고, 검색된 비밀 값을 사용하여 암호화된 사용 데이터를 복호화하도록 구성된다.

[0060] 각각의 비밀 값과 관련하여 복수의 에어로졸 발생 장치 각각의 고유 식별 값을 저장하는 데이터베이스를 제공하면, 서버가 에어로졸 발생 장치로부터 수신된 고유 식별 값을 사용하여 대응하는 비밀 값을 검색할 수 있게 한다. 일단 서버가 비밀 값을 소유하게 되면, 에어로졸 발생 장치로부터 수신된 암호화된 데이터가 복호화될 수 있다. 이 방식으로, 암호화된 보안 채널을 설정하지 않고, 서버와 에어로졸 발생 장치 간에 교환되는 메시지 중 어느 하나에 비밀 값을 포함하지 않고, 보안 키 교환을 위한 복잡한 알고리즘을 구현하지 않고, 에어로졸 발생 장치와 서버 사이에 보안 교환이 설정될 수 있다.

[0061] 본 발명의 제4 측면에 따르면, 본 발명의 제1 측면에 따른 에어로졸 발생 장치를 제조하는 방법이 제공된다. 상기 방법은 비밀 값 및 고유 식별 값을 생성하는 단계, 비밀 값 및 고유 식별 값을 에어로졸 발생 장치의 저장 유닛에 기록하는 단계, 및 복수의 에어로졸 발생 장치 각각에 대해, 고유 식별 값과 연관된 비밀 값을 데이터베이스에 저장하는 단계를 포함한다.

[0062] 각각의 에어로졸 발생 장치에 비밀 값 및 고유 식별 값을 제공함으로써, 에어로졸 발생 장치는 장치 특정 키로 사용 데이터를 암호화할 수 있다. 동시에, 에어로졸 발생 장치는 고유 식별 값에 의해 서버와의 통신 세션에서

자신을 식별할 수 있다. 복수의 에어로졸 발생 장치 각각의 고유 식별 값을 각각의 비밀 값과 연관하여 데이터베이스에 저장하면, 서버가 에어로졸 발생 장치로부터 수신된 고유 식별 값을 사용하여 대응하는 비밀 값을 검색하고, 검색된 비밀 값을 사용 데이터를 복호화하기 위해 사용할 수 있게 한다. 이 방식으로, 암호화된 보안 채널을 설정하지 않고, 서버와 에어로졸 발생 장치 사이에서 교환된 메시지 중 어느 하나에 비밀 값을 포함하지 않고, 보안 키 교환을 위한 복잡한 알고리즘을 구현하지 않고 에어로졸 발생 장치와 서버 사이에서 보안 교환이 수행될 수 있다.

[0063] 바람직하게는, 고유 식별 값은 제품 식별자, 플랫폼 식별자, 고유 장치 식별자 및 제조 현장 식별자 중 적어도 하나를 포함한다.

[0064] 고유 식별 값으로서, 일련 번호와 같은 고유 장치 식별자 대신에 또는 이와 조합하여 제품 관련 정보를 제공하면 서버가 통신하는 에어로졸 발생 장치의 종류를 쉽게 이해할 수 있게 한다.

[0065] 바람직하게는, 비밀 값은 제조 단계 동안 에어로졸 발생 장치에 의해 발생된 난수다.

[0066] 난수를 비밀 값으로서 사용하면, 에어로졸 발생 장치의 비밀 값이 다른 에어로졸 발생 장치의 (유출된) 비밀 값으로부터 유도될 수 없고, 이에 따라 가능한 암호화 공격에 대해 시스템을 추가로 강화시킬 수 있다는 이점을 갖는다. 에어로졸 발생 장치의 제조 단계 동안 비밀 값을 생성하면 이러한 민감한 정보를 보호하기 위해 적절한 주의가 취해질 수 있게 한다.

[0067] 상기 방법은 또한 생성된 난수를 에어로졸 발생 장치로부터 호스트 컴퓨터로, 바람직하게는 암호화된 형태로 송신하는 단계를 포함할 수 있다. 그런 다음, 호스트 컴퓨터는 데이터베이스 내의 고유 식별 값과 연관하여 비밀 값을 저장하는 것을 처리할 수 있다.

[0068] 본 발명의 제5 측면에 따르면, 에어로졸 발생 장치로부터 호스트로 사용 데이터를 송신하는 방법이 제공된다. 에어로졸 발생 장치는 그 안에 비밀 값 및 고유 식별 값을 저장한다. 상기 방법은 호스트에서 에어로졸 발생 장치로부터 고유 식별 값을 수신하는 단계, 각각의 고유 식별 값과 관련하여 복수의 에어로졸 발생 장치 각각의 비밀 값이 저장된 데이터베이스로부터 에어로졸 발생 장치의 비밀 값을 검색하는 단계를 포함한다. 상기 방법은 또한, 호스트에서, 적어도 검색된 비밀 값 및 선택적으로 수신된 고유 식별 값으로부터 암호화 키를 유도하는 단계를 포함한다. 상기 방법은 호스트에서 에어로졸 발생 장치로부터 암호화된 사용 데이터를 수신하는 단계, 및 수신된 암호화된 사용 데이터를 암호화 키로 복호화하는 단계를 추가로 포함한다.

[0069] 에어로졸 발생 장치로부터 호스트로 고유 식별 값만을 송신하고 데이터베이스로부터 에어로졸 발생 장치의 비밀 값을 검색함으로써, 암호화된 보안 채널을 설정하지 않고, 호스트와 에어로졸 발생 장치 간에 교환된 메시지 중 어느 하나에 비밀 값을 포함하지 않고, 안전한 키 교환을 위해 복잡한 알고리즘을 구현하지 않고, 에어로졸 발생 장치와 호스트 간에 데이터의 보안 교환이 수행될 수 있다.

[0070] 바람직하게는, 상기 방법은, 호스트에서, 적어도 검색된 비밀 값, 선택적으로, 고유 식별 값으로부터 인증 키를 유도하는 단계, 호스트에서 에어로졸 발생 장치로부터 암호화된 사용 데이터와 함께 제1 메시지 인증 코드, MAC를 수신하는 단계, 복호화된 사용 데이터 및 유도된 인증 키로부터 제2 MAC를 연산하는 단계, 및 제1 MAC와 제2 MAC를 비교하는 단계를 추가로 포함한다.

[0071] 복호화된 사용 데이터로부터 호스트에서 제2 MAC를 연산하고, 이 MAC를 암호화된 사용 데이터와 함께 수신된 제1 MAC와 비교하면, 호스트가 수신된 사용 데이터를 인증하고, 수신된 사용 데이터에 대한 의도하지 않은 수정을 검출하고, 악성 장치에 의한 스푸핑 공격을 차단할 수 있게 한다.

[0072] 바람직하게는, 상기 방법은 초기화 벡터를 유도하는 단계를 추가로 포함하되, 수신된 암호화된 사용 데이터는 암호화 키 및 초기화 벡터를 사용하여 카운터 모드에서 블록 암호를 적용함으로써 복호화된다. 또한, 초기화 벡터는 바람직하게는 고유 식별 값, 비밀 값, 및 제1 MAC로부터 유도될 수 있다.

[0073] 이 방식으로, 에어로졸 발생 장치가 카운터 모드에서 블록 암호화를 적용하더라도 암호화된 사용 데이터는 복호화될 수 있으며, 이는 가변 길이 데이터 블록에 블록 암호를 적용하기 위한 보안 방법이며 인코더 및 디코더 측 모두에서 낮은 복잡성 구현을 허용한다.

[0074] 바람직하게는, 암호화된 사용 데이터는 고유 레코드 식별자를 갖는 데이터 레코드의 페이로드 섹션에 포함된다. 이 경우, 초기화 벡터는 바람직하게는 고유 식별 값, 비밀 값, 제1 MAC, 및 고유 레코드 식별자로부터 유도될 수 있다.

[0075] 이 방식으로, 고유 기록 식별자는 에어로졸 발생 장치로부터 특정 사용 정보 조각을 요청하고/하거나 상이한 데이터 기록에 대해 상이한 키를 효과적으로 사용함으로써 데이터 보안을 추가로 개선하는 데 사용될 수 있다.

[0076] 본 발명의 제6 측면에 따르면, 처리 유닛에 의해 실행될 때, 본 발명의 제5 측면에 따른 방법의 모든 단계를 수행하도록 적응되는 컴퓨터 판독 가능 명령어가 저장된 메모리 및 처리 유닛을 갖는 호스트 컴퓨터가 제공된다.

[0077] 본 발명은 청구범위에 정의된다. 그러나, 아래에 비제한적인 예의 비포괄적인 목록이 제공된다. 이들 실시예의 특징 중 임의의 하나 이상은 본원에서 설명된 또 다른 실시예, 구현예, 또는 측면의 임의의 하나 이상의 특징과 조합될 수 있다.

[0078] 실시예 Ex1: 에어로졸 발생 장치로서, 비밀 값 및 고유 식별 값을 저장한 저장 유닛; 통신 유닛; 및 상기 에어로졸 발생 장치의 사용을 나타내는 사용 데이터를 생성하고, 적어도 저장된 비밀 값, 선택적으로, 고유 식별 값으로부터 암호화 키를 유도하고, 생성된 사용 데이터를 유도된 암호화 키로 암호화하고, 암호화된 사용 데이터를 저장 유닛에 저장하고, 및 암호화된 사용 데이터, 선택적으로, 고유 식별 값을 통신 유닛을 통해 외부 장치로 송신하도록 구성된 제어기를 포함하는, 에어로졸 발생 장치.

[0079] 실시예 Ex2: Ex1에 있어서, 제어기는 적어도 비밀 값 및 선택적으로 고유 식별 값으로부터 인증 키를 유도하고, 저장된 사용 데이터를 유도된 인증 키로 인증하도록 추가로 구성되는, 에어로졸 발생 장치.

[0080] 실시예 Ex3: 이전 실시예 중 어느 하나에 있어서, 상기 고유 식별 값은 제품 식별자, 플랫폼 식별자, 고유 장치 식별자 및 제조 사이트 식별자 중 적어도 하나를 포함하는, 에어로졸 발생 장치.

[0081] 실시예 Ex4: 이전 실시예 중 어느 하나에 있어서, 상기 비밀 값은 상기 에어로졸 발생 장치의 제조 단계 동안 발생된 난수 값인, 에어로졸 발생 장치.

[0082] 실시예 Ex5: 이전 실시예 중 어느 하나에 있어서, 상기 에어로졸 발생 장치의 작동 상태를 검출하기 위한 센서를 포함하는, 에어로졸 발생 장치.

[0083] 실시예 Ex6: 이전 실시예에 있어서, 상기 제어기는 상기 검출된 작동 상태에 기초하여 상기 사용 데이터를 생성하도록 구성되는, 에어로졸 발생 장치.

[0084] 실시예 Ex7: 이전 실시예에 따른 에어로졸 발생 장치로서, 상기 센서는 에어로졸 발생 장치와의 사용자 상호 작용을 검출하도록 구성된 센서, 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프를 검출하도록 구성된 센서, 에어로졸 발생 장치의 에어로졸 발생 유닛에 관한 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하도록 구성된 센서, 에어로졸 발생 장치의 전력 공급부에 관한 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하기 위한 센서, 에어로졸 발생 장치에 연결된 충전 장치에 관한 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하기 위한 센서, 및/또는 에어로졸 발생 유닛에 의해 사용되는 소모성 재료의 유형 또는 양을 검출하기 위한 센서를 포함하는, 에어로졸 발생 장치.

[0085] 실시예 Ex8: 이전 실시예 중 어느 하나에 있어서, 상기 사용 데이터는 시작 시간, 지속 시간, 종료 시간, 또는 사용자 상호 작용의 유형; 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프 또는 퍼프 횟수의 시작 시간, 지속 시간, 또는 종료 시간; 에어로졸 발생 장치를 충전 장치에 연결함으로써 사용자에 의해 수행되는 충전 동작의 시작 시간, 지속 시간, 또는 종료 시간, 또는 충전 동작 수; 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프의 시작 시, 퍼프 도중, 또는 퍼프의 종료 시 에어로졸 발생 장치의 에어로졸 발생 유닛과 관련된 전압, 전류, 저항, 전하, 에너지 또는 온도; 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프의 시작 시, 퍼프 동안, 또는 퍼프의 종료 시 에어로졸 발생 장치의 전력 공급부와 관련된 전압, 전류, 저항, 전하, 에너지 또는 온도; 충전 동작의 시작 시, 충전 동작 동안, 또는 충전 동작의 종료 시 에어로졸 발생 장치의 전력 공급부에 관한 전압, 전류, 저항, 충전, 에너지 또는 온도; 에어로졸 발생 유닛에 의해 사용되는 소모성 재료의 유형 또는 양 중 적어도 하나의 표시를 포함하는, 에어로졸 발생 장치.

[0086] 실시예 Ex9: 이전 실시예 중 어느 하나에 있어서, 상기 제어기는 상기 암호화된 사용 데이터를 데이터 레코드의 페이로드 섹션에 저장하도록 구성되는, 에어로졸 발생 장치.

[0087] 실시예 Ex10: 이전 실시예에 있어서, 각각의 데이터 레코드는 헤더, 페이로드 섹션, 및 인증 섹션을 포함하는, 에어로졸 발생 장치.

[0088] 실시예 Ex11: 이전 실시예에 있어서, 각각의 헤더는 상기 데이터 레코드의 형식을 나타내는 제1 데이터 필드 및 상기 데이터 레코드의 길이를 나타내는 제2 데이터 필드를 포함하는, 에어로졸 발생 장치.

[0089] 실시예 Ex12: 이전 실시예에 있어서, 각각의 데이터 레코드는 레코드 인덱스와 연관되는, 에어로졸 발생 장치.

[0090] 실시예 Ex13: 이전 실시예에 있어서, 각각의 헤더는 레코드 인덱스가 롤오버된 횟수를 나타내는 제3 데이터 필드를 추가로 포함하는, 에어로졸 발생 장치.

[0091] 실시예 Ex14: 이전 실시예 중 어느 하나에 있어서, 상기 제어기는 생성된 사용 데이터를 암호화하기 위해 대칭 키 알고리즘을 사용하도록 구성되는, 에어로졸 발생 장치.

[0092] 실시예 Ex15: 이전 실시예에 있어서, AES가 대칭 키 알고리즘으로서 사용되는, 에어로졸 발생 장치.

[0093] 실시예 Ex16: 이전 실시예 중 어느 하나에 있어서, 상기 제어기는 상기 비밀 값 및/또는 상기 고유 식별 값으로부터 초기화 벡터를 유도하고, 상기 암호화 키 및 상기 초기화 벡터를 사용하여 카운터 모드에서 블록 암호를 적용함으로써 상기 생성된 사용 데이터를 암호화하도록 추가로 구성되는, 에어로졸 발생 장치.

[0094] 실시예 Ex17: 이전 실시예에 있어서, 상기 제어기는, 상기 비밀 값 및/또는 상기 고유 식별 값으로부터 초기화 벡터를 유도하기 위해, 해시 기반 키 유도 함수인 HKDF를 사용하도록 구성되는, 에어로졸 발생 장치.

[0095] 실시예 Ex18: 이전 실시예에 있어서, 상기 제어기는, 상기 비밀 값 및/또는 상기 고유 식별 값으로부터 상기 초기화 벡터를 미리 정의된 값, 상기 생성된 사용 데이터를 포함하는 데이터 레코드와 연관된 레코드 인덱스의 값, 상기 데이터 레코드의 유형, 및 상기 생성된 사용 데이터로부터 연산된 메시지 인증 코드의 적어도 일부인 MAC 중 적어도 하나를 포함하는 솔트로 유도하도록 구성되는, 에어로졸 발생 장치.

[0096] 실시예 Ex19: 이전 실시예 중 어느 하나에 있어서, 상기 제어기는 상기 생성된 사용 데이터에 대한 메시지 인증 코드, MAC를 연산함으로써 상기 생성된 사용 데이터를 인증하도록 추가로 구성되는, 에어로졸 발생 장치.

[0097] 실시예 Ex20: 이전 실시예에 있어서, 상기 제어기는 상기 생성된 사용 데이터로부터 및 제1 인증 키로부터 상기 생성된 사용 데이터에 대한 MAC를 연산하도록 추가로 구성되는, 에어로졸 발생 장치.

[0098] 실시예 Ex21: 이전 실시예 중 어느 하나에 있어서, 상기 제어기는 상기 암호화된 사용 데이터에 대한 MAC를 연산함으로써 암호화된 사용 데이터를 인증하도록 추가로 구성되는, 에어로졸 발생 장치.

[0099] 실시예 Ex22: 이전 실시예에 있어서, 상기 제어기는 상기 암호화된 사용 데이터 및 제2 인증 키로부터 상기 암호화된 사용 데이터에 대한 MAC를 연산하도록 추가로 구성되는, 에어로졸 발생 장치.

[0100] 실시예 Ex23: 이전 실시예에 있어서, 상기 제어기는 상기 암호화된 사용 데이터로부터, 상기 생성된 사용 데이터를 위한 MAC로부터, 및 상기 제2 인증 키로부터 상기 암호화된 사용 데이터에 대한 MAC를 연산하도록 추가로 구성되는, 에어로졸 발생 장치.

[0101] 실시예 Ex24: 실시예 Ex20-Ex23 중 어느 하나에 있어서, 상기 제어기는 상기 비밀 값 및/또는 상기 고유 식별 값으로부터 상기 제1 인증 키 및/또는 상기 제2 인증 키를 유도하도록 추가로 구성되는, 에어로졸 발생 장치.

[0102] 실시예 Ex25: 실시예 Ex19-Ex24 중 어느 하나에 있어서, 상기 제어기는 상기 생성된 사용 데이터에 대한 MAC 및/또는 상기 암호화된 사용 데이터에 대한 MAC를 연산하기 위한 해시 함수를 사용하도록 추가로 구성되는, 에어로졸 발생 장치.

[0103] 실시예 Ex26: 이전 실시예에 있어서, 상기 제어기는, 해시 함수의 출력을 미리 정의된 바이트 수로 잘라내어, 생성된 사용 데이터에 대한 MAC 및/또는 암호화된 사용 데이터에 대한 MAC를 연산하도록 추가로 구성되는, 에어로졸 발생 장치.

[0104] 실시예 Ex27: 실시예 E19-Ex26 중 어느 하나에 있어서, 상기 제어기는 상기 생성된 사용 데이터에 대한 MAC 및/또는 상기 암호화된 사용 데이터에 대한 MAC를 상기 저장 유닛 내의 암호화된 사용 데이터와 함께 저장하도록 추가로 구성되는, 에어로졸 발생 장치.

[0105] 실시예 Ex28: 이전 실시예 중 어느 하나에 있어서, 상기 제어기는, 상기 비밀 값 및/또는 상기 고유 식별 값으로부터, 상기 생성된 사용 데이터를 암호화하기 위한 암호화 키, 카운터 모드에서 블록 암호로 상기 생성된 사용 데이터를 암호화하기 위한 초기화 벡터, 및 상기 사용 데이터를 인증하기 위한 인증 키 중 적어도 하나를 유도하기 위해, 해시 기반 키 유도 함수인 HKDF를 사용하도록 추가로 구성되는, 에어로졸 발생 장치.

[0106] 실시예 Ex29: 이전 실시예에 있어서, 상기 비밀 값 및/또는 상기 고유 식별 값의 적어도 일부는 상기 키 유도 함수를 위한 입력 키 자료로서 사용되는, 에어로졸 발생 장치.

[0107] 실시예 Ex30: 이전 실시예에 있어서, 솔트는 비밀 값 및/또는 고유 식별 값의 적어도 일부와 함께 키 유도 함수를 위한 입력 키 자료로서 사용되는, 에어로졸 발생 장치.

[0108] 실시예 Ex31: 실시예 Ex28-Ex30에 있어서, 상기 비밀 값의 비트 표현의 미리 정의된 서브세트는, 상기 고유 식별 값 및 솔트와 함께, 상기 키 유도 함수를 위한 입력 키 자료로서 사용되는, 에어로졸 발생 장치.

[0109] 실시예 Ex32: 이전 실시예에 있어서, 상기 암호화 키 및/또는 상기 인증 키를 유도하기 위한 입력 키 자료로서 사용된 비밀 값의 비트 표현의 미리 정의된 서브세트는, 상기 초기화 벡터를 유도하기 위한 입력 키 자료로서 사용된 비밀 값의 비트 표현의 미리 정의된 서브세트와 상이한, 에어로졸 발생 장치.

[0110] 실시예 Ex33: 실시예 Ex28-Ex32 중 어느 하나에 있어서, 고정된 솔트는 암호화 키 및/또는 인증 키를 유도하기 위해 사용되는, 에어로졸 발생 장치.

[0111] 실시예 Ex34: 실시예 Ex28-Ex33 중 어느 하나에 있어서, 생성된 사용 데이터로부터 연산된 메시지 인증 코드 MAC의 적어도 일부는 초기화 벡터를 유도하기 위한 솔트로서 사용되는, 에어로졸 발생 장치.

[0112] 실시예 Ex35: 실시예 Ex28-Ex34 중 어느 하나에 있어서, 상기 키 유도 함수에 의해 생성된 출력 키 자료의 제1 부분은 암호화 키로서 사용되고, 상기 제1 부분과 상이한 출력 키 자료의 제2 부분은 인증 키로서 사용되는, 에어로졸 발생 장치.

[0113] 실시예 Ex36: 이전 실시예 중 어느 하나에 있어서, 상기 제어기는 상기 통신 유닛을 통해 상기 암호화된 사용 데이터의 인증 코드와 함께 상기 암호화된 사용 데이터를 송신하도록 추가로 구성되는, 에어로졸 발생 장치.

[0114] 실시예 Ex37: 이전 실시예 중 어느 하나에 있어서, 상기 외부 장치는 충전 스테이션, 도킹 스테이션, 모바일 단말기, 개인용 컴퓨터, 호스트 컴퓨터, 및 서버 중 하나인, 에어로졸 발생 장치.

[0115] 실시예 Ex38: 이전 실시예 중 어느 하나에 있어서, 상기 암호화된 사용 데이터는 데이터 케이블, 근거리 통신, 블루투스, BLE, 및 WiFi 중 어느 하나를 통해 송신되는, 에어로졸 발생 장치.

[0116] 실시예 Ex39: 에어로졸 발생 시스템으로서, 실시예 Ex1 내지 Ex38 중 어느 하나에 따른 에어로졸 발생 장치; 상기 에어로졸 발생 장치의 비밀 값과 관련하여 복수의 에어로졸 발생 장치 각각의 고유 식별 값을 저장하도록 구성된 데이터베이스; 및 상기 에어로졸 발생 장치로부터, 암호화된 사용 데이터 및 상기 에어로졸 발생 장치의 고유 식별 값을 수신하고, 상기 고유 식별 값을 사용하여 상기 데이터베이스로부터 상기 고유 식별 값과 연관된 상기 비밀 값을 검색하고, 및 검색된 비밀 값을 사용하여 암호화된 사용 데이터를 복호화하도록 구성된 서버를 포함하는, 에어로졸 발생 시스템.

[0117] 실시예 Ex40: 에어로졸 발생 장치를 작동시키기 위한 방법으로서, 상기 방법은, 비밀 값 및 고유 식별 값을 상기 에어로졸 발생 장치의 저장 유닛에 저장하는 단계; 상기 에어로졸 발생 장치의 사용을 나타내는 사용 데이터를 생성하는 단계; 적어도 저장된 비밀 값으로부터 암호화 키를 유도하는 단계; 상기 생성된 사용 데이터를 상기 유도된 암호화 키로 암호화하는 단계; 상기 암호화된 사용 데이터를 상기 저장 유닛에 저장하는 단계; 및 상기 암호화된 사용 데이터 및 선택적으로, 고유 식별 값을 통신 유닛을 통해 외부 장치로 송신하는 단계를 포함하는, 방법.

[0118] 실시예 Ex41: Ex40에 있어서, 적어도 상기 비밀 값 및 선택적으로 상기 고유 식별 값으로부터 인증 키를 유도하는 단계; 및 상기 유도된 인증 키로 상기 저장된 사용 데이터를 인증하는 단계를 추가로 포함하는, 방법.

[0119] 실시예 Ex42: 이전 실시예 중 어느 하나에 있어서, 상기 고유 식별 값은 제품 식별자, 플랫폼 식별자, 고유 장치 식별자 및 제조 현장 식별자 중 적어도 하나를 포함하는, 방법.

[0120] 실시예 Ex43: 이전 실시예 중 어느 하나에 있어서, 상기 에어로졸 발생 장치의 제조 단계 동안 상기 비밀 값으로서 난수 값을 생성하는 단계를 더 포함하는, 방법.

[0121] 실시예 Ex44: 이전 실시예 중 어느 하나에 있어서, 상기 에어로졸 발생 장치의 작동 상태를 검출하는 단계를 포함하는, 방법.

[0122] 실시예 Ex45: 이전 실시예에 있어서, 상기 사용 데이터는 상기 검출된 작동 상태에 기초하여 생성되는, 에어로졸 발생 장치.

[0123] 실시예 Ex46: 이전 실시예에 따른 방법으로서, 상기 작동 상태를 검출하는 단계는 상기 에어로졸 발생 장치와의 사용자 상호 작용을 검출하는 단계; 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프를 검출하는 단계; 에어

로졸 발생 장치의 에어로졸 발생 유닛에 관한 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하는 단계; 에어로졸 발생 장치의 전력 공급부에 관한 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하는 단계; 에어로졸 발생 장치에 연결된 충전 장치에 관한 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하는 단계; 및/또는 에어로졸 발생 유닛에 의해 사용되는 소모성 재료의 유형 또는 양을 검출하는 단계를 포함하는, 방법.

[0124] 실시예 Ex47: 이전 실시예 중 어느 하나에 있어서, 상기 사용 데이터는 시작 시간, 지속 시간, 종료 시간, 또는 사용자 상호 작용의 유형; 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프 또는 퍼프 횟수의 시작 시간, 지속 시간, 또는 종료 시간; 에어로졸 발생 장치를 충전 장치에 연결함으로써 사용자에 의해 수행되는 충전 동작의 시작 시간, 지속 시간, 또는 종료 시간, 또는 충전 동작 수; 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프의 시작 시, 퍼프 도중, 또는 퍼프의 종료 시 에어로졸 발생 장치의 에어로졸 발생 유닛과 관련된 전압, 전류, 저항, 전하, 에너지 또는 온도; 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프의 시작 시, 퍼프 동안, 또는 퍼프의 종료 시 에어로졸 발생 장치의 전력 공급부와 관련된 전압, 전류, 저항, 전하, 에너지 또는 온도; 충전 동작의 시작 시, 충전 동작 동안, 또는 충전 동작의 종료 시 에어로졸 발생 장치의 전력 공급부에 관한 전압, 전류, 저항, 충전, 에너지 또는 온도; 에어로졸 발생 유닛에 의해 사용되는 소모성 재료의 유형 또는 양 중 적어도 하나의 표시를 포함하는, 방법.

[0125] 실시예 Ex48: 이전 실시예 중 어느 하나에 있어서, 상기 암호화된 사용 데이터는 데이터 레코드의 페이로드 섹션에 저장되는, 방법.

[0126] 실시예 Ex49: 이전 실시예에 있어서, 각각의 데이터 레코드는 헤더, 페이로드 섹션, 및 인증 섹션을 포함하는, 방법.

[0127] 실시예 Ex50: 이전 실시예에 있어서, 각각의 헤더는 상기 데이터 레코드의 형식을 나타내는 제1 데이터 필드 및 상기 데이터 레코드의 길이를 나타내는 제2 데이터 필드를 포함하는, 방법.

[0128] 실시예 Ex51: 이전 실시예에 있어서, 각각의 데이터 레코드는 레코드 인덱스와 연관되는, 방법.

[0129] 실시예 Ex52: 이전 실시예에 있어서, 각각의 헤더는 레코드 인덱스가 롤오버된 횟수를 나타내는 제3 데이터 필드를 추가로 포함하는, 방법.

[0130] 실시예 Ex53: 이전 실시예 중 어느 하나에 있어서, 생성된 사용 데이터를 암호화하기 위해 대칭 키 알고리즘이 사용되는, 방법.

[0131] 실시예 Ex54: 이전 실시예에 있어서, AES가 대칭 키 알고리즘으로서 사용되는, 방법.

[0132] 실시예 Ex55: 이전 실시예 중 어느 하나에 있어서, 상기 비밀 값 및/또는 상기 고유 식별 값으로부터 초기화 벡터를 유도하는 단계; 및 상기 암호화 키 및 상기 초기화 벡터를 사용하여 카운터 모드에서 블록 암호를 적용함으로써 상기 생성된 사용 데이터를 암호화하는 단계를 추가로 포함하는, 방법.

[0133] 실시예 Ex56: 이전 실시예에 있어서, 해시 기반 키 유도 함수인 HKDF는 상기 비밀 값 및/또는 상기 고유 식별 값으로부터 상기 초기화 벡터를 유도하기 위해 사용되는, 방법.

[0134] 실시예 Ex57: 이전 실시예에 있어서, 상기 초기화 벡터는, 미리 정의된 값, 상기 생성된 사용 데이터를 포함하는 데이터 레코드와 연관된 레코드 인덱스의 값, 상기 데이터 레코드의 유형, 및 상기 생성된 사용 데이터로부터 연산된 메시지 인증 코드의 적어도 일부인 MAC 중 적어도 하나를 포함하는 솔트를 갖는 비밀 값 및/또는 고유 식별 값으로부터 유도되는, 방법.

[0135] 실시예 Ex58: 이전 실시예 중 어느 하나에 있어서, 생성된 사용 데이터에 대한 메시지 인증 코드 MAC를 연산함으로써 생성된 사용 데이터를 인증하는 단계를 추가로 포함하는, 방법.

[0136] 실시예 Ex59: 이전 실시예에 있어서, 상기 생성된 사용 데이터에 대한 MAC는 상기 생성된 사용 데이터 및 제1 인증 키로부터 연산되는, 방법.

[0137] 실시예 Ex60: 이전 실시예 중 어느 하나에 있어서, 상기 암호화된 사용 데이터에 대한 MAC를 연산함으로써 상기 암호화된 사용 데이터를 인증하는 단계를 추가로 포함하는, 방법.

[0138] 실시예 Ex61: 이전 실시예에 있어서, 상기 암호화된 사용 데이터를 위한 MAC는 상기 암호화된 사용 데이터 및 제2 인증 키로부터 연산되는, 방법.

[0139] 실시예 Ex62: 이전 실시예에 있어서, 암호화된 사용 데이터로부터, 생성된 사용 데이터를 위해 MAC로부터, 및

제2 인증 키로부터 암호화된 사용 데이터를 위해 MAC를 연산하는 단계를 추가로 포함하는, 방법.

[0140] 실시예 Ex63: 실시예 Ex59-Ex62 중 어느 하나에 있어서, 상기 비밀 값 및/또는 상기 고유 식별 값으로부터 상기 제1 인증 키 및/또는 상기 제2 인증 키를 유도하는 단계를 추가로 포함하는, 방법.

[0141] 실시예 Ex64: 실시예 Ex58-Ex63 중 어느 하나에 있어서, 생성된 사용 데이터에 대한 MAC 및/또는 암호화된 사용 데이터에 대한 MAC를 연산하기 위해 해시 함수가 사용되는, 방법.

[0142] 실시예 Ex65: 이전 실시예에 있어서, 상기 생성된 사용 데이터를 위한 MAC 및/또는 상기 암호화된 사용 데이터를 위한 MAC는 해시 함수의 출력을 미리 정의된 수의 바이트로 잘라내어 연산되는, 방법.

[0143] 실시예 Ex66: 실시예 Ex58-Ex65 중 어느 하나에 있어서, 상기 생성된 사용 데이터에 대한 MAC 및/또는 상기 암호화된 사용 데이터에 대한 MAC를 상기 암호화된 사용 데이터와 함께 저장하는 단계를 추가로 포함하는, 방법.

[0144] 실시예 Ex67: 이전 실시예 중 어느 하나에 있어서, 상기 비밀 값 및/또는 상기 고유 식별 값으로부터, 상기 생성된 사용 데이터를 암호화하기 위한 암호화 키, 카운터 모드에서 블록 암호로 상기 생성된 사용 데이터를 암호화하기 위한 초기화 벡터, 및 상기 사용 데이터를 인증하기 위한 인증 키 중 적어도 하나를 유도하기 위한 해시 기반 키 유도 함수인 HKDF를 사용하는 단계를 추가로 포함하는, 방법.

[0145] 실시예 Ex68: 이전 실시예에 있어서, 상기 비밀 값 및/또는 상기 고유 식별 값의 적어도 일부는 상기 키 유도 함수를 위한 입력 키 자료로서 사용되는, 방법.

[0146] 실시예 Ex69: 이전 실시예에 있어서, 솔트는 비밀 값의 적어도 일부 및/또는 고유 식별 값과 함께 키 유도 함수를 위한 입력 키 자료로서 사용되는, 방법.

[0147] 실시예 Ex70: 실시예 Ex67에 있어서, 상기 비밀 값의 비트 표현의 미리 정의된 서브세트는, 상기 고유 식별 값 및 솔트와 함께, 상기 키 유도 함수를 위한 입력 키 자료로서 사용되는, 방법.

[0148] 실시예 Ex71: 이전 실시예에 있어서, 상기 암호화 키 및/또는 상기 인증 키를 유도하기 위한 입력 키 자료로서 사용된 비밀 값의 비트 표현의 미리 정의된 서브세트는, 상기 초기화 벡터를 유도하기 위한 입력 키 자료로서 사용된 비밀 값의 비트 표현의 미리 정의된 서브세트와 상이한, 방법.

[0149] 실시예 Ex72: 실시예 Ex67-Ex71 중 어느 하나에 있어서, 고정된 솔트는 상기 암호화 키 및/또는 상기 인증 키를 유도하기 위해 사용되는, 방법.

[0150] 실시예 Ex73: 실시예 Ex67-Ex72 중 어느 하나에 있어서, 생성된 사용 데이터로부터 연산된 메시지 인증 코드 MAC의 적어도 일부는 초기화 벡터를 유도하기 위한 솔트로서 사용되는, 방법.

[0151] 실시예 Ex74: 실시예 Ex67-Ex73 중 어느 하나에 있어서, 상기 키 유도 함수에 의해 생성된 출력 키 자료의 제1 부분은 암호화 키로서 사용되고, 상기 제1 부분과 상이한 출력 키 자료의 제2 부분은 인증 키로서 사용되는, 방법.

[0152] 실시예 Ex75: 이전 실시예 중 어느 하나에 있어서, 상기 암호화된 사용 데이터는 상기 암호화된 사용 데이터의 인증 코드와 함께 송신되는, 방법.

[0153] 실시예 Ex76: 이전 실시예 중 어느 하나에 있어서, 상기 외부 장치는 충전 스테이션, 도킹 스테이션, 모바일 단말기, 개인용 컴퓨터, 호스트 컴퓨터, 및 서버 중 하나인, 방법.

[0154] 실시예 Ex77: 이전 실시예 중 어느 하나에 있어서, 상기 암호화된 사용 데이터는 데이터 케이블, 근거리 통신, 블루투스, BLE, 및 WiFi 중 어느 하나를 통해 송신되는, 방법.

[0155] 실시예 Ex78: 이전 실시예 중 어느 하나에 따른 에어로졸 발생 장치를 제조하기 위한 방법으로서, 상기 방법은 비밀 값 및 고유 식별 값을 생성하는 단계; 상기 비밀 값 및 고유 식별 값을 상기 에어로졸 발생 장치의 저장 유닛에 기록하는 단계; 및 복수의 에어로졸 발생 장치 각각에 대해, 상기 비밀 값을 상기 고유 식별 값과 연관하여 데이터베이스에 저장하는 단계를 포함하는, 방법.

[0156] 실시예 Ex79: 이전 실시예에 있어서, 상기 고유 식별 값은 제품 식별자, 플랫폼 식별자, 고유 장치 식별자 및 제조 현장 식별자 중 적어도 하나를 포함하는, 방법.

[0157] 실시예 Ex80: 실시예 Ex78 또는 Ex79에 있어서, 상기 비밀 값은 제조 단계 동안 상기 에어로졸 발생 장치에 의해 생성된 난수인, 방법.

[0158] 실시예 Ex81: 이전 실시예에 있어서, 상기 발생된 난수를 상기 에어로졸 발생 장치로부터 호스트 컴퓨터로 송신하는 단계를 더 포함하는, 방법.

[0159] 실시예 Ex82: 이전 실시예에 있어서, 상기 생성된 난수는 암호화된 형태로 상기 에어로졸 발생 장치로부터 상기 호스트 컴퓨터로 송신되는, 방법.

[0160] 실시예 Ex83: 에어로졸 발생 장치로부터 호스트로 사용 데이터를 송신하는 방법으로서, 상기 에어로졸 발생 장치는 비밀 값 및 고유 식별 값을 저장하고, 상기 방법은, 호스트에서 에어로졸 발생 장치로부터 고유 식별 값을 수신하는 단계; 각각의 고유 식별 값과 관련하여 복수의 에어로졸 발생 장치 각각의 비밀 값이 저장된 데이터베이스로부터 에어로졸 발생 장치의 비밀 값을 검색하는 단계; 호스트에서, 적어도 검색된 비밀 값 및 선택적으로 수신된 고유 식별 값으로부터 암호화 키를 유도하는 단계; 호스트에서 에어로졸 발생 장치로부터 암호화된 사용 데이터를 수신하는 단계; 및 수신된 암호화된 사용 데이터를 암호화 키로 복호화하는 단계를 포함하는, 방법.

[0161] 실시예 Ex84: 이전 실시예에 있어서, 호스트에서, 적어도 검색된 비밀 값 및 선택적으로 고유 식별 값으로부터 인증 키를 유도하는 단계; 호스트에서 에어로졸 발생 장치로부터 암호화된 사용 데이터와 함께 제1 메시지 인증 코드 MAC를 수신하는 단계; 복호화된 사용 데이터 및 유도된 인증 키로부터 제2 MAC를 연산하는 단계; 및 제1 MAC와 제2 MAC를 비교하는 단계를 추가로 포함하는, 방법.

[0162] 실시예 Ex85: 이전 실시예에 있어서, 초기화 벡터를 유도하는 단계를 추가로 포함하고, 상기 수신된 암호화된 사용 데이터는, 상기 암호화 키 및 상기 초기화 벡터를 사용하여 카운터 모드에서 블록 암호를 적용함으로써 복호화되는, 방법.

[0163] 실시예 Ex86: 이전 실시예에 있어서, 상기 초기화 벡터는 상기 고유 식별 값, 상기 비밀 값, 및 상기 제1 MAC로부터 유도되는, 방법.

[0164] 실시예 Ex87: 이전 실시예에 있어서, 상기 암호화된 사용 데이터는 고유 레코드 식별자를 갖는 데이터 레코드의 페이로드 섹션에 포함되는, 방법.

[0165] 실시예 Ex88: 이전 실시예에 있어서, 상기 초기화 벡터는 상기 고유 식별 값, 상기 비밀 값, 상기 제1 MAC, 및 상기 고유 레코드 식별자로부터 유도되는, 방법.

[0166] 실시예 Ex89: 처리 유닛 및 그 위에 저장된 컴퓨터 판독 가능 명령어를 갖는 메모리를 갖는 호스트 컴퓨터로서, 상기 명령어는, 상기 처리 유닛에 의해 실행될 때, 실시예 Ex83-Ex88 중 어느 하나에 따른 방법의 모든 단계를 수행하도록 구성되는, 호스트 컴퓨터.

도면의 간단한 설명

[0167] 이제, 실시예가 도면을 참조하여 추가로 설명될 것이다:

도 1은 일 구현예에 따른 에어로졸 발생 장치의 블록도를 도시하고;

도 2는 일 구현예에 따른 에어로졸 발생 장치 및 서버를 포함하는 시스템의 블록도를 도시하고;

도 3은 일 구현예에 따른 데이터 구조의 개략도를 도시하고;

도 4는 일 구현예에 따라 사용 데이터를 암호화하기 위한 방법에서 데이터 흐름을 도시하는 다이어그램을 도시하고;

도 5는 일 구현예에 따라 MAC를 계산하기 위한 방법에서 데이터 흐름을 도시하는 다이어그램을 도시하고;

도 6은 일 구현예에 따라 암호화 및 인증 키를 유도하기 위한 방법에서 데이터 흐름을 도시하는 다이어그램을 도시하고;

도 7은 일 실시예에 따른 초기 벡터를 유도하기 위한 방법에서의 데이터 흐름을 도시하는 도면을 도시하고;

도 8은 일 구현예에 따라 사용 데이터를 암호화하기 위한 방법의 흐름도를 도시하고;

도 9는 일 구현예에 따라 사용 데이터를 송신하고 복호화하기 위한 방법의 흐름도를 도시하고;

도 10은 일 구현예에 따른 제조 방법의 흐름도를 도시하고;

도 11은 추가 구현예에 따른 제조 방법의 흐름도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0168] 도 1은 본 발명의 일 구현예에 따른 에어로졸 발생 장치(100)의 블록도를 도시한다. 에어로졸 발생 장치(100)는 에어로졸 발생 유닛(110), 센서(120), 통신 유닛 센서(130), 저장 유닛(140), 통신 유닛(150), 및 전력 공급원(160)을 포함할 수 있다.

[0169] 에어로졸 발생 유닛(110)은 전구체 물질(소모성 재료)로부터 에어로졸 발생 장치의 사용자에 의한 흡입을 위한 에어로졸을 발생시키기 위한 유닛이다. 예로서, 에어로졸 발생 유닛(110)은 기화기 또는 가열 요소를 포함할 수 있다. 전구체 물질은 액체 또는 고체 형태로 제공될 수 있다. 에어로졸 발생 유닛(110)은 전력 공급원(160)에 의해 제공되는 전기 에너지에 의해 전력이 공급되고 제어기(130)에 의해 제어된다.

[0170] 센서(120)는 에어로졸 발생 장치의 작동을 제어하는 데 사용될 수 있는 데이터를 전달한다. 예를 들어, 센서는 버튼 누르기, 전구체 물질 용기 열기 또는 닫기, 특정 방식으로 장치를 움직여 제스처를 수행하기 등과 같이, 에어로졸 발생 장치와 사용자 상호작용을 감지하도록 구성될 수 있다. 센서는 또한 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프를 검출하도록 구성될 수 있다. 다른 실시예에서, 센서는 에어로졸 발생 유닛(110)의 작동과 관련된 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하도록 구성될 수 있다. 센서는 또한 에어로졸 발생 장치 및/또는 에어로졸 발생 장치에 연결된 충전 장치의 전력 공급원(160)과 관련된 전압, 전류, 저항, 전하, 에너지 또는 온도를 검출하도록 구성될 수 있다. 추가 예에서, 센서는 에어로졸 발생 유닛(110)에 의해 사용되는 소모성 재료의 유형 또는 양을 검출하도록 구성될 수 있다.

[0171] 제어기(130)는 에어로졸 발생 장치의 전체 작동을 제어하는 것, 특히 가능하게는 센서(120)에 의해 전달된 데이터에 기초하여 에어로졸 발생 유닛(110)을 작동시키는 것, 저장 유닛(140)에서 사용 데이터를 생성, 암호화 및 저장하는 것, 통신 유닛(150)을 통해 데이터를 수신 및 송신하는 것, 전력 공급원(160)의 충전을 모니터링 및/또는 제어하는 것 등을 담당한다. 제어기(130)는 마이크로프로세서, 마이크로컨트롤러, 또는 하나 초과의 마이크로프로세서 및/또는 마이크로컨트롤러의 조합일 수 있다. 제어기(130)는 또한 컴퓨터 프로그램 명령어를 저장하기 위한 저장 장치 및/또는 컴퓨터 프로그램의 실행과 관련된 데이터를 저장하기 위한 메모리를 구비할 수 있다.

[0172] 저장 유닛(140)은 제어기(130)에 연결되고, 사용 데이터를 암호화하기 위해 제어기에 의해 사용될 수 있는 고유 식별자(142) 및 비밀 값(144)을 그 안에 저장하고 있다. 저장 유닛(140)은 제어기(130)에 의해 생성된 암호화된 사용 데이터를 저장하도록 추가로 구성된다. 저장 유닛은 휘발성 또는 비휘발성일 수 있다. 예로서, 플래시 메모리가 저장 유닛으로서 제공된다. 저장 유닛은 마이크로컨트롤러 또는 제어기 외부의 구성요소의 일체형 부분일 수 있다. 저장 유닛은 상이한 데이터 아이템을 저장하기 위한 하나 초과의 물리적 또는 논리적으로 분리된 저장 섹션 또는 구성요소를 포함할 수 있다. 고유 식별자(142), 비밀 값(144), 및 암호화된 사용 데이터(144)는, 예를 들어, 저장 유닛(140)의 상이한 섹션 또는 구성 요소에 저장될 수 있다. 비밀 값은 무단 액세스에 대해 구체적으로 보안되는 섹션 또는 구성 요소에 저장될 수 있다.

[0173] 고유 식별자(142)는 각각의 에어로졸 발생 장치에 대해 고유한 데이터 조각, 예를 들어 고유 장치 ID이다. 예를 들어, 각각의 에어로졸 발생 장치는 저장 유닛(140)에 고유 식별자로서 저장된 고유 일련 번호를 구비할 수 있다. 고유 식별자는 또한, 일련 번호에 더하여 또는 그 대신에, 제품 식별자, 플랫폼 식별자, 및 제조 사이트 중 적어도 하나를 나타내는 정보를 포함할 수 있다. 고유 식별자는 또한 고유 제조 정보 블록(또는 제조 시설 ID), MIB로서, 즉 제품 ID, 플랫폼 ID, 고유 ID(또는 직렬화된 장치 유닛 ID) 및 제조 현장과 같은 제조 공정에 관한 정보를 포함하는 데이터 블록으로서 제공될 수 있다.

[0174] 비밀 값(144)은 사용 데이터를 암호화하기 위한 암호화 키를 유도하기 위해 제어기에 의해 사용되는 값이다. 비밀 값은 일반적으로 사용자 또는 임의의 다른 미인가자에게 알려지지 않고 에어로졸 발생 장치 또는 송신 데이터로부터 (쉽게) 유도될 수 없다는 의미에서 비밀이다. 비밀 값은 또한 정상 작동 동안 임의의 데이터 송신에 포함되지 않는다. 비밀 값은 임의의 외부 장치에 대해 접근 가능하지 않은 저장 유닛(140)의 특히 고정된 부분에 저장될 수 있다.

[0175] 비밀 값은 또한, 각각의 고유 식별자와 연관하여, 제조업자 서버에 대해 액세스 가능한 데이터베이스에 저장된다. 이 방식으로, 서버는 장치의 사용 데이터를 암호화하는 데 사용된 암호화 키를 유도하기 위해 특정 에어로졸 발생 장치의 비밀 값을 획득하기 위해 조회 작동에서 고유 식별자를 사용할 수 있다. 이렇게 유도된 암호화 키를 사용하여, 서버는 이 특정 장치로부터 송신된 암호화된 사용 데이터를 복호화할 수 있다.

[0176] 비밀 값은 암호화된 데이터에 대한 무차별-힘 공격을 방지하기 위해 충분히 클 수 있다. 예를 들어, 비밀 값은

8, 16, 32, 64, 128 또는 256 바이트의 데이터를 포함할 수 있다. 2의 거듭제곱 크기나 2의 거듭제곱과 다른 크기를 포함하여, 비밀 값에 대한 다른 크기가 또한 사용될 수 있다.

[0177] 예로서, 제조 공정 동안 생성된 난수 또는 의사 난수가 비밀 값으로서 사용될 수 있다. 비밀 값은 제조 공정 동안 에어로졸 발생 장치에 의해 생성될 수 있고, 바람직하게는 암호화된 형태로, 제조업자 서버에 의해 나중에 참조하기 위해 데이터베이스에서 고유 식별자와 연관하여 비밀 값을 저장하는 것을 담당하는 호스트 컴퓨터에 송신될 수 있다. 비밀 값은 또한 호스트 컴퓨터에 의해 생성될 수 있고, 제조 공정의 단계 동안 저장 유닛(140)으로 전송되거나 저장 유닛에 직접 기록될 수 있다.

[0178] 암호화된 사용 데이터(146)는 제어기에 의해 생성되고 암호화된 형태로 저장 유닛(140)에 저장되는 사용 데이터이다. 사용 데이터는 에어로졸 발생 장치의 사용을 나타내고, 특정 이벤트에 응답하여 장치에 의해 발생된 데이터일 수 있다. 예는 장치 오류, 에어로졸 발생 또는 배터리 재충전으로 인해 생성된 데이터를 포함한다. 예를 들어, 사용 데이터는 사용자가 에어로졸 발생 장치와 수행하는 상호 작용의 시작 시간, 지속 시간, 종료 시간, 및 유형 중 적어도 하나의 표시를 포함할 수 있는데, 예컨대 버튼 누르기, 전구체 물질 용기 열기 또는 닫기, 특정 방식으로 장치를 움직여 제스처를 수행하기 등이 있다. 사용 데이터는 또한 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프의 시작 시간, 지속 시간, 및 종료 시간 또는 퍼프의 수 중 적어도 하나의 표시를 포함할 수 있다. 사용 데이터는 또한, 에어로졸 발생 장치를 충전 장치에 연결함으로써 사용자에 의해 수행되는 충전 동작의 시작 시간, 지속 시간 및 종료 시간 또는 충전 동작 수 중 적어도 하나의 표시를 포함할 수 있다.

[0179] 사용 데이터는 또한 에어로졸 발생 장치(100)의 작동 상태 또는 건강 상태에 관한 것일 수 있다. 예를 들어, 사용 데이터는 또한 에어로졸 발생 장치의 에어로졸 발생 유닛(110)에 관한 전압, 전류, 저항, 전하, 에너지 및 온도 중 적어도 하나의 표시를 포함할 수 있다. 사용 데이터는 또한 에어로졸 발생 장치의 전력 공급원(160)과 관련된 전압, 전류, 저항, 전하, 에너지 또는 온도 중 적어도 하나의 표시를 포함할 수 있다. 이들 표시 각각은 에어로졸 발생 장치의 사용자에 의해 수행되는 퍼프의 시작, 퍼프 동안, 또는 퍼프의 종료와 같은 특정 이벤트에 대해 조절될 수 있다. 적어도 일부 이들 표시는 또한 에어로졸 발생 유닛(110)에 의해 수행되는 가열 작동의 시작, 지속 시간, 또는 종료 및/또는 충전 동작의 시작, 충전 동작 동안, 또는 충전 동작의 종료로 조절될 수 있다. 사용 데이터는 또한 에어로졸 발생 유닛에 의해 사용되는 소모성 재료의 유형 또는 양을 표시할 수 있다.

[0180] 통신 유닛(150)은 외부 장치에 통신 링크를 확립하도록, 특히 암호화된 사용 데이터(146)를 제조업자 서버에 송신하도록 구성된다. 통신 링크는 직렬 통신 링크, 범용 직렬 버스(USB), 광 통신 포트, 근거리 통신(NFC), 블루투스, 블루투스 저 에너지(BLE), 무선 통신, IEEE 802.11x 표준 중 어느 하나에 따른 WiFi, 모바일 통신 등을 포함하지만 이에 한정되지 않는 임의의 유선 또는 무선 통신 기술에 기초할 수 있다. 제조업자 서버와의 통신은, 예를 들어 휴대폰, 홀더 또는 도킹 스테이션과 같은 중간 장치를 통해 직접 또는 간접적일 수 있다. 제조자 서버와의 통신은 또한, 예를 들어 에어로졸 발생 장치와 휴대폰 사이의 블루투스 연결 및 휴대폰과 인터넷 액세스 포인트 사이의 모바일 통신과 같은 하나 초과의 통신 프로토콜을 포함할 수 있다.

[0181] 전력 공급원(160)은 에어로졸 발생 장치의 모든 구성 요소에 전력을 공급한다. 전력 공급원은 리튬 이온 배터리나 리튬 폴리머 배터리와 같은 충전식 배터리일 수 있다. 다른 전력 공급원도 사용될 수 있다.

[0182] 도 2는 본 발명의 일 구현예에 따른 에어로졸 발생 장치(100) 및 서버(200)를 포함하는 시스템의 블록도를 도시한다. 에어로졸 발생 장치(100) 및 서버(200)는 암호화된 사용 데이터를 송신하기 위한 통신 링크에 의해 연결된다. 서버(200)는 각각의 고유 식별자와 관련하여 복수의 에어로졸 발생 장치 각각에 대한 비밀 값을 저장하는 데이터베이스(300)에 대한 액세스를 갖는다. 에어로졸 발생 장치는 또한 전력 공급원(160)을 충전하기 위한 충전 장치(190)로서 작동하는 홀더(190) 또는 도킹 스테이션에 연결될 수 있다. 에어로졸 발생 장치(100)와 서버(200) 사이의 통신 링크는 또한 홀더(190) 또는 중개자(미도시)로서 작동하는 휴대폰과 간접적으로 형성될 수 있다.

[0183] 도 3은 본 발명의 일 구현예에 따른 데이터 구조의 개략도를 도시한다. 사용 데이터는 데이터 레코드의 형태로 저장되고 송신될 수 있으며, 여기서 각각의 데이터 레코드는 사용자 상호 작용, 충전 동작, 온도, 배터리 수준, 오류 메시지 등과 같은 특정 이벤트에 관한 것이다. 각각의 데이터 레코드는 헤더, 페이로드 섹션, 및 인증 섹션(메시지 인증 코드, MAC)을 포함할 수 있다. 헤더는 데이터 레코드의 형식, 데이터 레코드의 길이, 및 인덱스를 지정할 수 있다. 형식은 페이로드 섹션 내의 어느 위치에 어떤 데이터가 제공되는지 나타낼 수 있다. 상이한 형식은 상이한 이벤트에 대해 미리 정의될 수 있다. 길이는 데이터 레코드의 전체 길이 또는 페이로드 섹션의 길이를 표시할 수 있다.

[0184] 인덱스, 또는 헤더의 다른 요소, 특히 길이, 데이터 유형 및 데이터 형식과 함께 인덱스는 대응하는 데이터 레코드의 고유 식별자(Record Unique Identity, RUID)를 형성할 수 있다. 레코드 인덱스는 증분 수, 또는 반복될 수 있는 작은 증분 수와 더 작은 수가 오버플로우된 횟수를 나타내는 "롤오버" 값의 조합에 기초하여 고유할 수 있다. 인덱스는 반드시 페이로드와 함께 저장 및/또는 송신되지 않으며, 특정 데이터 레코드에 대한 요청 또는 데이터 레코드의 어레이 또는 목록 내의 데이터 레코드의 위치로부터 암시적으로 공지될 수 있다. 따라서, 인덱스 값 대신에, 인덱스가 미리 정의된 최대 인덱스 값 위로 롤링된 횟수를 나타내는 롤오버 값이 저장 및/또는 송신될 수 있다.

[0185] 페이로드는 도 1과 관련하여 전술한 바와 같이, 실제 사용 데이터, 즉 각각의 이벤트에 관한 정보를 포함할 수 있다. 페이로드는 암호화될 수 있다. MAC는 인증 목적으로 사용되는 암호화 서명 또는 인증 코드일 수 있다. 데이터 암호화, 인증 및 키 유도를 위한 프로세스가 아래에 설명될 것이다.

[0186] 본 발명에 따르면, 대칭 키 알고리즘은 각 데이터 레코드의 페이로드에 저장된 사용 데이터를 암호화하기 위해 사용된다. 페이로드 길이는 달라질 수 있고 일반적으로 종래의 블록 암호화 알고리즘의 블록 크기를 초과할 것이기 때문에, 카운터 모드는 종래의 블록 암호화를 스트림 암호화로 변환하기 위해 적용된다. 카운터 모드는, 당업계에 일반적으로 공지된 바와 같이, 카운터의 연속 값을 암호화함으로써 키 스트림을 생성한다. 그런 다음, 암호텍스트는 키 스트림으로 일반텍스트를 XOR함으로써 얻어진다. 각 데이터 레코드에 대해 상이한 키 스트림이 사용되는 것을 보장하기 위해, 카운터는 데이터 레코드마다 상이한 넌스 또는 초기화 벡터와 연결된다. 그런 다음, 동일한 키 스트림으로 암호텍스트를 다시 XOR함으로써 복호화가 수행된다.

[0187] 바람직한 구현예에서, 고급 암호화 표준(AES)은 사용 데이터를 암호화하기 위한 카운터 모드(AES-CTR)에서 사용된다. 본 구현예에 따른 사용 데이터를 암호화하기 위한 데이터 흐름이 도 4에 도시되어 있다.

[0188] AES-CTR 알고리즘은 사용 데이터를 입력으로서 수신하고 암호화된 사용 데이터를 출력으로서 전달한다. 암호화 프로세스는, 암호화 키(AES 키)와 별도로, 카운터 모드에 대한 카운터 및 초기화 벡터를 추가로 요구할 수 있다.

[0189]

[0190] 본 발명의 추가 측면에 따르면, 각각의 사용 데이터 레코드의 인증은 인증 코드(디지털 서명), 또는 "다이제스트"에 의해 보장된다. 이러한 서명은 데이터 레코드의 헤더 및/또는 페이로드로부터 연산된 메시지 인증 코드(MAC)의 형태로 제공된다. 데이터 레코드에 대한 임의의 수정은 원본 데이터 레코드의 MAC와 상이한 MAC에서(압도적인 확률로) 생성되어, 변조된 데이터가 쉽게 검출될 수 있다(무결성 확인). 또한, MAC의 연산은 비밀 키(인증 키 또는 MAC 키)에 기초하므로, 공격자는 주어진 데이터 조각에 대한 "올바른" MAC를 예측할 수 없다. 이 방식으로, 시스템은 제조자 서버를 거짓 또는 손상된 정보로 오염시키려는 스푸핑 공격에 대해 강화된다(진위성 검사).

[0191] 바람직한 구현예에서, 해시 기반 MAC(HMAC), 즉 암호화 해시 알고리즘, 바람직하게는 보안 해시 알고리즘 1(SHA-1)을 인증될 데이터에 적용함으로써 연산되는 MAC가 사용된다. SHA-1에 기초하여 MAC를 연산하기 위한 알고리즘은 일반적으로 HMAC-SHA1로 지칭된다. HMAC-SHA256을 포함하는 다른 알고리즘이 또한 사용될 수 있다.

[0192] 도 5는 본 발명의 일 구현예에 따라 MAC를 계산하기 위한 방법에서 데이터 흐름을 도시하는 다이어그램을 도시한다. HMAC-SHA1 알고리즘은 입력으로서 MAC 키와 함께 데이터 레코드의 헤더 및 페이로드를 수신하고 출력으로서 MAC를 전달한다.

[0193] 일반적으로, 인증 코드 또는 "다이제스트"의 강도는 그 길이에 따라 달라진다. HMAC-SHA1 알고리즘은, 예를 들어, 160 비트(20 바이트)의 길이를 갖는 MAC를 전달한다. 그러나, 에어로졸 발생 장치에서, 레코드 당 단지 몇 바이트를 갖는 다수의 짧은 데이터 레코드가 인증될 필요가 있다. 따라서, 20 바이트 MAC를 각 레코드에 부착하면, 특히 에어로졸 발생 장치에서 이용 가능한 제한된 양의 저장 용량을 고려하여 실현 불가능하다.

[0194] 인증된 데이터 레코드의 저장 및 송신을 위한 오버헤드를 감소시키고, 에어로졸 발생 장치 내에 저장될 수 있는 데이터 레코드의 최대 수를 증가시키기 위해, HMAC 알고리즘에 의해 전달된 MAC는 몇 바이트, 예를 들어 2, 3 또는 4 바이트로 잘라낼 수 있다. 이러한 잘라낸 인증 코드의 사용은 악의적으로 생성된 암호화 레코드에 대한 충돌의 수를 증가시킨다. 그러나, 이러한 경우에, 거짓 데이터로 제조업자 서버를 오염시키려는 시도는, 거짓 인증 코드를 갖는 다수의 데이터 로그 또는 불가능한 데이터로 인해 검출될 것이다.

[0195] 암호화 키(AES 키) 및 메시지 인증 키(MAC 키) 둘 모두는 비밀 값 및 에어로졸 발생 장치에 저장된 고유 ID로부

터 유도된다. 따라서, 상이한 에어로졸 발생 장치는 데이터 레코드를 암호화하고 인증하기 위해 상이한 키를 사용한다. 따라서, 특정 장치가 손상되어 AES 및/또는 MAC 키가 알려지는 경우에도, 다른 장치는 영향을 받지 않을 것이다.

[0196] HMAC 알고리즘(HKDF)에 기초한 키 유도 함수는 AES 키 및 MAC 키 둘 다를 유도하기 위해 사용된다. 키 유도 함수(KDF)는 비밀 값으로부터 하나 이상의 비밀 키를 유도하는 암호화 알고리즘이며, 키를 더 긴 키로 늘리거나 필요한 형식의 키를 획득하는 데 사용될 수 있다. HKDF 알고리즘은 선택적인 솔트(HMAC 기능의 키로서 작용함) 및 임의의 잠재적으로 약한 입력 키 자료(IKM)(데이터로서 작용함) 상의 HMAC 해시 함수(예: HMAC-SHA256)를 사용하여 의사 랜덤 키(PRK)를 추출한다. 그런 다음, PRK-키형 해시 블록을 반복적으로 생성한 다음 이를 출력 키 자료에 첨부하여 원하는 길이로 최종 잘라냄으로써 임의의 원하는 길이의 유사하게 암호화적으로 강한 출력 키 자료(OKM)를 생성한다.

[0197] 이 프로세스를 위한 데이터 흐름이 도 6에 도시되어 있다. HKDF 알고리즘은 입력 키 자료로서 비밀 값, 컨텍스트로서 고유 식별자(UID), 및 솔트로서 일정한 값을 수신하고(비트의 서브세트), 출력 키 자료(OKM)를 전달한다. 마스크(AES 마스크)는 비밀 값으로부터 비트의 서브세트를 IKM로서 선택(복합 해제)하는 데 사용된다. 도 7과 관련하여 후술되는 바와 같이, 상이한 마스크(IV 마스크)가 초기화 벡터를 유도하기 위한 IKM으로서 비밀 값으로부터 상이한 비트 서브세트를 선택하는 데 사용된다. AES 키 및 MAC 키 둘 모두는 OKM 내의 상이한 위치(AES 오프셋, MAC 오프셋)로부터 필요한 수의 연속 비트(AES 길이, MAC 길이)를 선택함으로써 OKM으로부터 획득된다.

[0198] AES-CTR로 사용 데이터를 암호화하기 위한 초기화 벡터는 또한 AES 키 및 MAC 키를 유도하는 데 사용되는 것과 유사한 키 유도 함수에 의해 비밀 값 및 UID로부터 유도된다. 암호화 분석에 대해 이러한 방법을 더욱 강화하기 위해, 초기화 벡터는 또한 현재 데이터 레코드, 특히 데이터 레코드의 페이로드 섹션에 저장된 (암호화되지 않은) 사용 데이터의 MAC 및/또는 데이터 레코드의 고유 식별자(RUID), 예컨대 인덱스 또는 시퀀스 번호, 및/또는 암호화될 페이로드의 다른 특성에 따라 제조된다. 이 방식으로, 데이터 레코드의 크기를 더 이상 증가시키지 않고 각각의 데이터 레코드 및/또는 각각의 송신에 대해 상이한 초기화 벡터가 사용될 수 있다.

[0199] 이 프로세스를 위한 데이터 흐름이 도 7에 도시되어 있다. HKDF 알고리즘은 입력 키 자료(IKM)로서 비밀 값, 컨텍스트로서 고유 식별자(UID), 및 (잘라낸) MAC, 레코드 식별자, 및 솔트로서 상수 값을 수신하고 출력 키 자료(OKM)를 전달한다. (잘라낸) MAC, 레코드 식별자 및 상수 값의 조합은, 예를 들어 각각의 비트 문자열을 멀티플렉서(MUX)로 연결함으로써 획득될 수 있다. 마스크(IV 마스크)는 비밀 값으로부터 비트의 서브세트를 IKM로서 선택(복합 해제)하는 데 사용된다. 초기화 벡터는 OKM으로부터 요구되는 길이(IV 길이)를 갖는 특정 위치(IV 오프셋)에서 수득된다.

[0200] MAC 및 고유 식별자를 포함하여, 도 7에 도시된 키 유도 함수에 대한 모든 입력 정보는 암호화된 데이터 레코드가 에어로졸 발생 장치로부터 송신되었을 때 제조자 서버에서 또한 이용 가능하다. 따라서, 서버는 동일한 초기화 벡터를 유도하고 수신된 데이터 레코드를 복호화할 수 있다.

[0201] 일반적으로, MAC는 암호화된 메시지에 대해 연산되어 복호화 시작(암호화-그 다음-MAC) 전에 진위성을 확인할 수 있도록 하는 것이 수용된다. 그러나, 본 상황에서, 초기화 벡터를 유도하기 위해 KDF에 대한 추가 입력으로서 MAC를 사용할 수 있는 이점은 잠재적으로 변조된 데이터에 복호화 알고리즘을 적용할 위험을 능가할 수 있다. 따라서, MAC는 바람직하게는 암호화되지 않은 데이터(MAC-그 다음-암호화)에 대해 연산되어 암호화 프로세스에 이용 가능하다.

[0202] 본 발명의 추가 구현예에서, 암호화되지 않은 데이터(MAC-그 다음 암호화)에 대한 MAC에 더하여 또는 그 대신에 암호화된 사용 데이터(암호화-그 다음-MAC)에 대한 MAC가 또한 연산될 수 있다. 이를 위해, 제2 인증 키는 암호화되지 않은 데이터에 대한 MAC를 연산하기 위한 (제1) 인증 키를 유도하기 위한 것과 유사한 방식으로 고유 장치 정보로부터 유도될 수 있다. 그런 다음, 제2 인증 키는 HMAC 알고리즘을 암호화된 사용 데이터에 또는 암호화된 사용 데이터에 적용함으로써 암호화된 사용 데이터에 대한 MAC 및 암호화되지 않은 데이터에 대한 MAC를 계산하는 데 사용될 수 있다. 그런 다음, 암호화된 사용 데이터에 대한 MAC가 암호화된 메시지와 함께 송신된다.

[0203] 서버 측에서, 암호화된 메시지의 무결성은 에어로졸 발생 장치에서와 동일한 방식으로 제2 인증 키를 유도하고, 암호화된 메시지로부터 서버 측 MAC를 연산하고, 서버 측 MAC를 암호화된 메시지에 부착된 MAC와 비교함으로써 확인될 수 있다. 그런 다음, 복호화 프로세스는 두 MAC가 동일한 경우에만 시작된다.

[0204] 도 8은 본 발명의 일 구현예에 따른 사용 데이터를 암호화하기 위한 방법의 흐름도를 나타낸다.

[0205] 단계 S110에서, 도 6과 관련하여 설명된 바와 같이 키 유도 프로세스로 고유 장치 정보로부터 암호화 키(K_{ENC}) 및 메시지 인증 키(K_{MAC})가 유도된다. 단계 120에서, 에어로졸 발생 장치의 작동 상태는, 예를 들어 적절한 센서에 의해 검출된다. 검출 결과에 기초하여, 사용 데이터는 단계 S130에서 생성된다. 생성된 사용 데이터의 종류에 따라, 단계 S140에서 고유 레코드 ID가 생성된다. 고유 레코드 ID는 데이터 레코드의 유형, 형식, 길이 및 인덱스를 나타내는 정보를 포함할 수 있다. 단계 S150에서, 도 5와 관련하여 설명된 바와 같은 프로세스로 메시지 인증 키(K_{MAC})를 사용하여 메시지 인증 코드인 MAC가 고유 레코드 ID 및 사용 데이터에 대해 계산된다. 단계 S160에서, 도 7과 관련하여 설명된 바와 같은 프로세스로 고유 장치 정보, 고유 레코드 ID 및 MAC로부터 고유 초기화 벡터 IV가 유도된다. 단계 S170에서, 암호화 키(K_{ENC}) 및 초기화 벡터 IV를 사용하여 도 4와 함께 설명된 바와 같은 프로세스를 사용하여 데이터 레코드가 암호화된다. 그런 다음, 단계 180에서 암호화된 데이터 레코드는 MAC와 함께 에어로졸 발생 장치에 저장된다. 그런 뒤에, 프로세스는 단계 S120로 복귀한다.

[0206] 도 9는 본 발명의 일 구현예에 따라, 에어로졸 발생 장치로부터 호스트로 사용 데이터를 송신하고 호스트에서 수신된 데이터를 복호화하기 위한 방법의 흐름도를 도시한다.

[0207] 프로세스는 에어로졸 발생 장치에 요청을 송신함으로써, 제조업자 서버일 수 있는 호스트에 의해 개시될 수 있다(S210). 에어로졸 발생 장치는 제조 정보 블록, MIB와 같은 고유 장치 ID를 송신함으로써 이 요청에 응답할 수 있다(S215). 한편, 비밀 정보는, 이러한 프로세스의 맥락에서 에어로졸 발생 장치와 호스트 사이의 이러한 송신의 일부도 아니고 임의의 다른 송신도 아니다. 고유 장치 ID를 수신하면, 호스트는 단계 S220의 데이터베이스로부터 상응하는 비밀 값(S_{DEV})를 검색한다. 비밀 값은 암호화된 형태로 데이터베이스에 저장될 수 있고, 호스트는 단계 S225에서 암호화된 비밀 값($E(S_{DEV})$)를 복호화할 수 있다. 이 시점에서, 호스트는 전체 고유 장치 정보, 즉 고유 장치 ID 및 비밀 값을 소유하며, 따라서 사용 데이터를 암호화하고 인증하기 위해 에어로졸 발생 장치에 의해 사용되는 암호화 및 메시지 인증 키를 유도하는 위치에 있다. 구체적으로, 호스트는, 단계 S230에서, 에어로졸 발생 장치에 의해 수행되고 도 6과 관련하여 설명된 것과 동일한 키 유도 프로세스로 고유 장치 정보로부터 암호화 키(K_{ENC}) 및 메시지 인증 키(K_{MAC})를 유도한다.

[0208] 단계 S235에서, 호스트는 에어로졸 발생 장치로부터 데이터를 요청할 수 있다. 요청은 에어로졸 발생 장치에 의해 송신될 하나 이상의 데이터 레코드의 표시, 예컨대 고유 레코드 ID 또는 인덱스 값의 범위 등의 적어도 일부를 포함할 수 있다. 에어로졸 발생 장치는, 요청된 데이터 레코드를 상응하는 $MAC_{데이터}$와 함께 암호화된 형태로 송신함으로써 이 요청에 응답할 수 있다(S240). 응답은 또한 송신된 각 데이터 레코드의 고유 레코드 ID를 포함할 수 있다.

[0209] 단계 S245에서, 호스트는 에어로졸 발생 장치에 의해 수행되고 도 7과 함께 설명된 것과 동일한 프로세스로 고유 장치 정보, 고유 레코드 ID 및 $MAC_{데이터}$로부터 고유 초기화 벡터 IV를 유도한다. 그런 다음, 초기화 벡터 IV는, 수신된 데이터 레코드를 복호화하고 그 안에 포함된 데이터($DATA_{호스트}$)를 복구하기 위해 암호화 키(K_{ENC})와 함께 단계 S250에서 사용된다.

[0210] 단계 S255에서, 호스트는 고유 레코드 ID 및 복구된 데이터($DATA_{호스트}$)로부터 메시지 인증 코드($MAC_{호스트}$)를 계산한다. 이렇게 계산된 메시지 인증 코드($MAC_{호스트}$)가, 단계 S260에서, 암호화된 데이터 레코드와 함께 수신된 메시지 인증 코드($MAC_{데이터}$)와 동일한 것으로 발견되는 경우, 레코드는 유효한 것으로 간주된다. 그렇지 않으면 데이터 레코드가 유효하지 않다.

[0211] 도 10은 본 발명의 일 구현예에 따른 에어로졸 발생 장치를 위한 제조 방법의 흐름도를 도시한다. 이러한 방법의 단계는 에어로졸 발생 장치의 조립 공정의 특정 단계에서 수행되거나, 예를 들어 제어기(130)의 제1 전력 공급 시 조립된 에어로졸 발생 장치의 최종 테스트에서 수행될 수 있다.

[0212] 단계 S330에서, 에어로졸 발생 장치는, 예를 들어 난수 생성기에 의해 고유한 비밀 값(S_{DEV})을 생성시킨다. 이렇게 생성된 비밀 값(S_{DEV})은 그 다음, 고유 장치 정보의 일부로서 에어로졸 발생 장치의 저장 유닛(140)에 저장되고(S340), 암호화되고(S350) 향후 참조를 위해 데이터베이스에 저장되기 위해 호스트 컴퓨터로 송신된다(S360).

[0213] 도 11은 본 발명의 추가 구현예에 따른 에어로졸 발생 장치를 위한 제조 방법의 흐름도를 도시한다. 이러한 방

법의 단계는 에어로졸 발생 장치의 조립 공정의 특정 단계에서 수행되거나, 예를 들어 제어기(130)의 제1 전력 공급 시 조립된 에어로졸 발생 장치의 최종 테스트에서 수행될 수 있다.

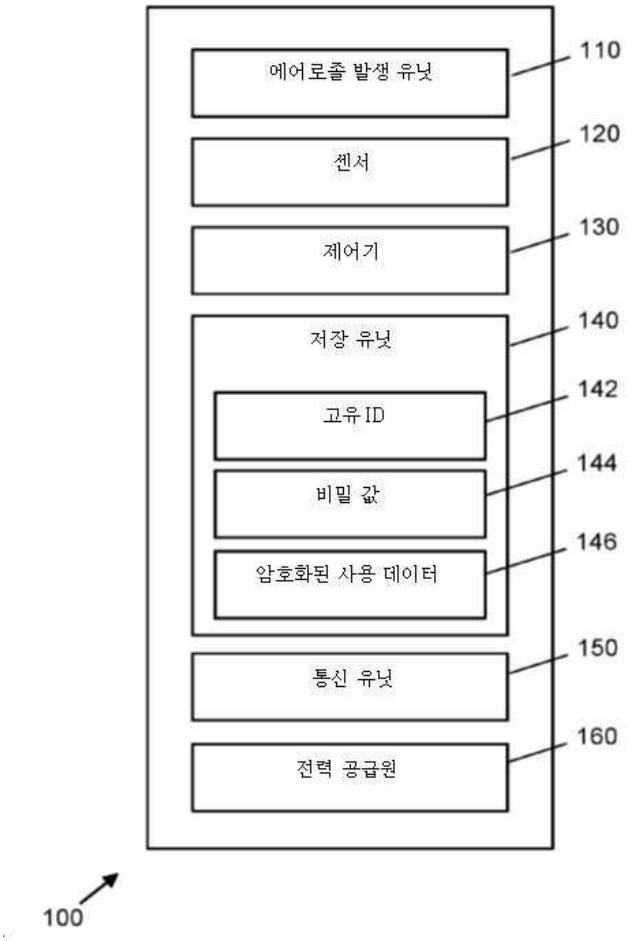
[0214] 도 11에 따른 공정은 추가 단계 S310 및 S320 만큼 도 10의 공정과 상이하다. 단계 S310에서, 호스트는 고유 장치 ID를 생성하고 에어로졸 발생 장치에 이를 송신한다. 고유 장치 ID는, 전술한 바와 같이, 고유 제조 정보 블록, MIB, 즉 제품 ID, 플랫폼 ID, 고유 ID 및 제조 현장과 같은 제조 공정에 관한 정보를 포함하는 데이터 블록을 포함할 수 있다.

[0215] 단계 S320에서, 에어로졸 발생 장치는 수용된 고유 장치 ID를 저장 유닛(140)에 저장한다. 단계 S330에서, 에어로졸 발생 장치는, 예를 들어 난수 생성기에 의해 고유한 비밀 값(S_{DEV})을 생성시킨다. 이렇게 생성된 비밀 값(S_{DEV})는 그 다음 고유 장치 ID와 함께 에어로졸 발생 장치의 저장 유닛(140)에 저장된다(S340). 단계 S530에서, 비밀 값(S_{DEV})는 암호화되어 호스트 컴퓨터에 송신되어, 나중에 검색하기 위한 고유 장치 ID와 연관하여 데이터베이스에 저장된다(S360).

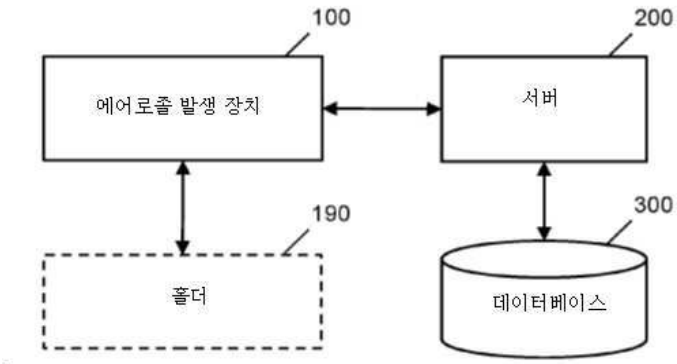
[0216] 따라서, 본 발명의 구현예는 장치 내부 및 제조업자 서버와 같은 외부 장치로의 송신 시 에어로졸 발생 장치에 저장된 사용 데이터를 보호하기 위한 기술을 제공한다. 또한, 에어로졸 발생 장치로부터 데이터를 수집하는 제조업자 서버는 거짓 또는 손상된 정보로 오염되는 것으로부터 보호된다. 본 발명의 구현예는 보안 키 교환을 위해 공개 키 인프라 또는 지나치게 복잡한 알고리즘을 필요로 하지 않고 에어로졸 발생 장치에서 사용 데이터의 저장 및 송신을 보호할 수 있다. 본 발명의 구현예는 다수의 에어로졸 발생 장치 및 다수의 개별 데이터 레코드를 갖는 시스템에서도 높은 수준의 데이터 보안을 추가로 제공한다. 본 발명의 구현예는 또한 에어로졸 발생 장치의 제한된 연산 전력 및 저장 용량에 구체적으로 적응된다.

도면

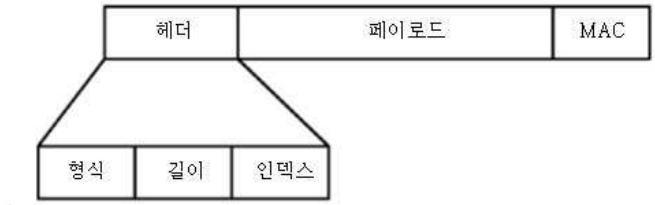
도면1



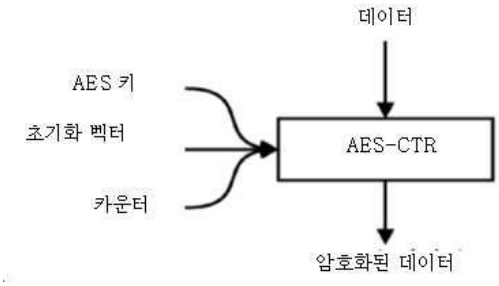
도면2



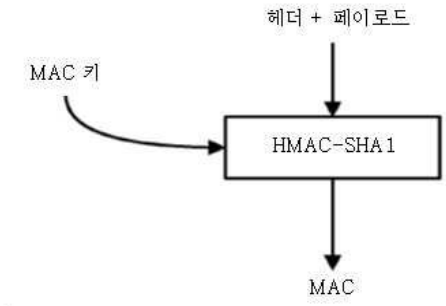
도면3



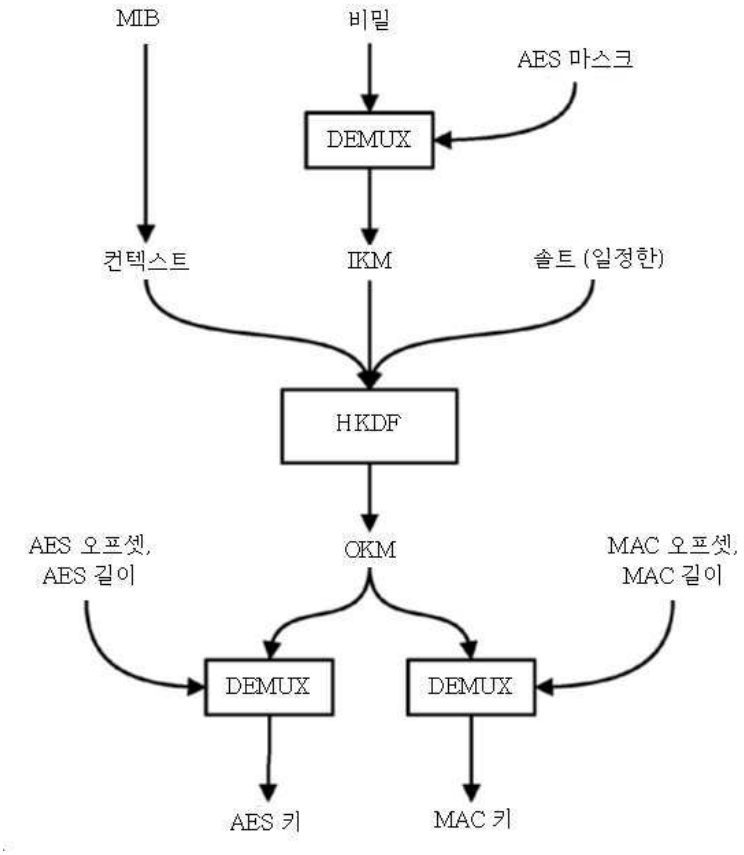
도면4



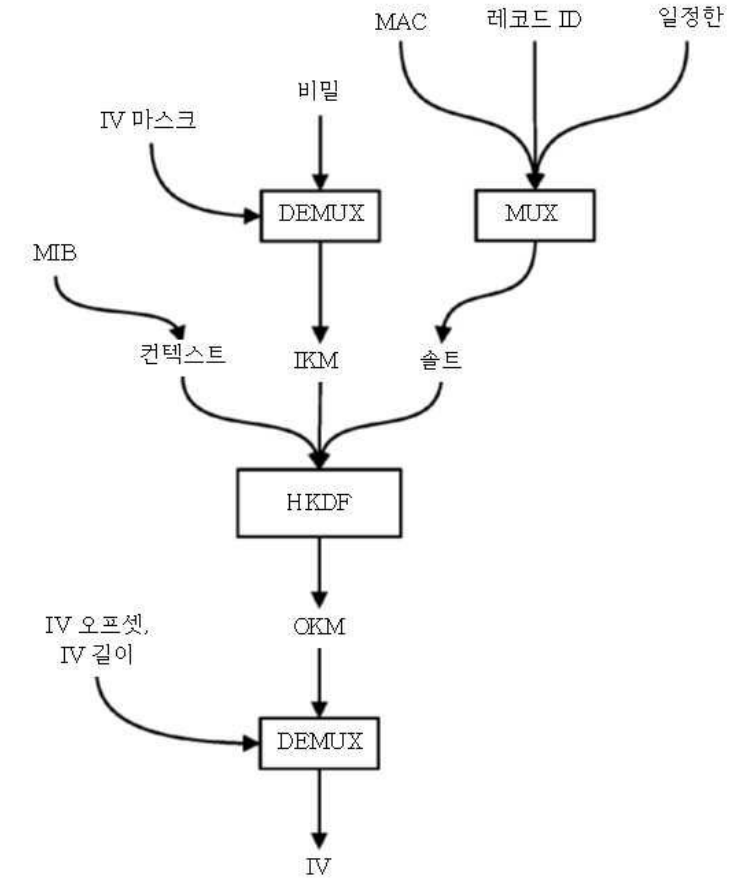
도면5



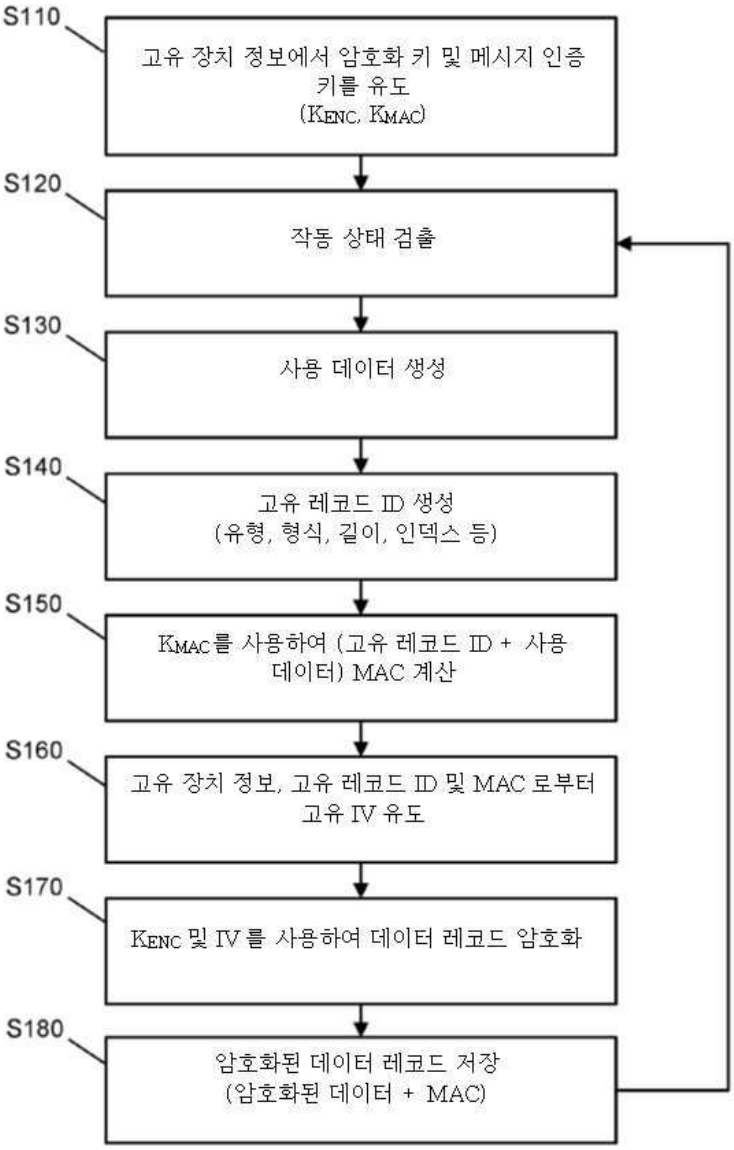
도면6


MIB
비밀
AES 마스크
DEMUX
컨텍스트
IKM
솔트 (일정한)
HKDF
AES 오프셋,
AES 길이
OKM
MAC 오프셋,
MAC 길이
DEMUX
DEMUX
AES 키
MAC 키

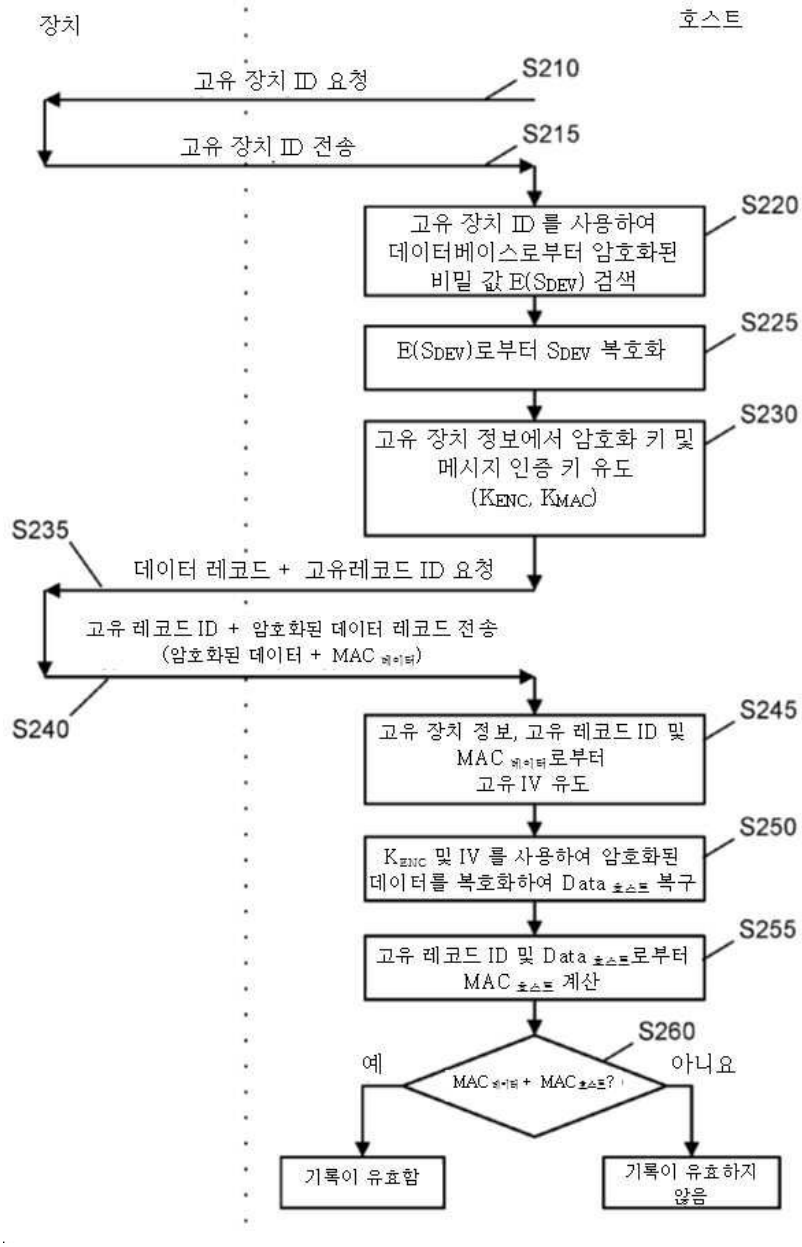
도면7


MAC
레코드 ID
일정한
비밀
IV 마스크
DEMUX
MUX
MIB
컨텍스트
IKM
솔트
HKDF
IV 오프셋,
IV 길이
OKM
DEMUX
IV

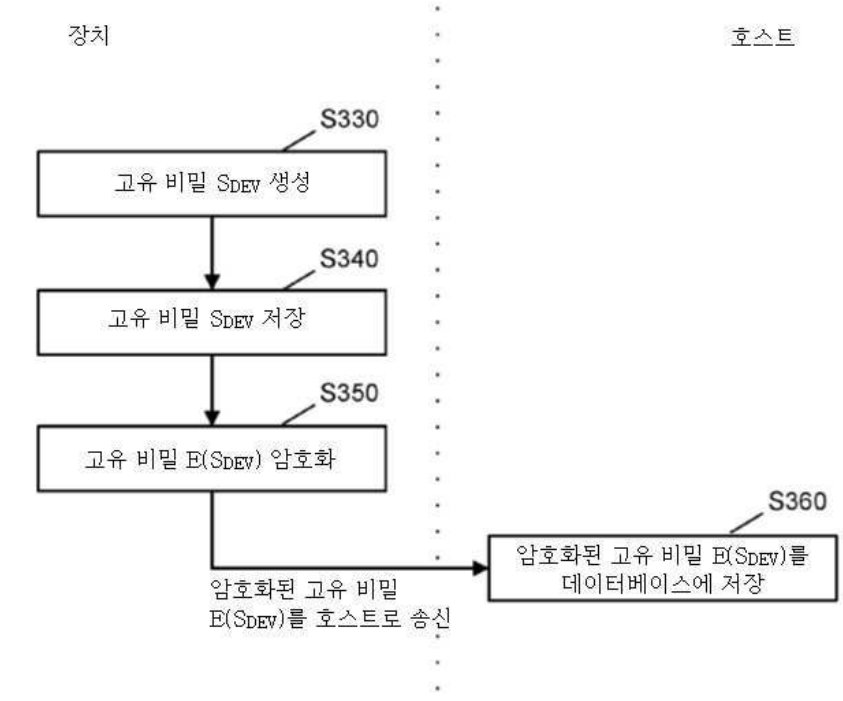
도면8


S110
고유 장치 정보에서 암호화 키 및 메시지 인증 키를 유도 (KENC, KMAC)
S120
작동 상태 검출
S130
사용 데이터 생성
S140
고유 레코드 ID 생성 (유형, 형식, 길이, 인덱스 등)
S150
KMAC를 사용하여 (고유 레코드 ID + 사용 데이터) MAC 계산
S160
고유 장치 정보, 고유 레코드 ID 및 MAC 로부터 고유 IV 유도
S170
KENC 및 IV를 사용하여 데이터 레코드 암호화
S180
암호화된 데이터 레코드 저장 (암호화된 데이터 + MAC)

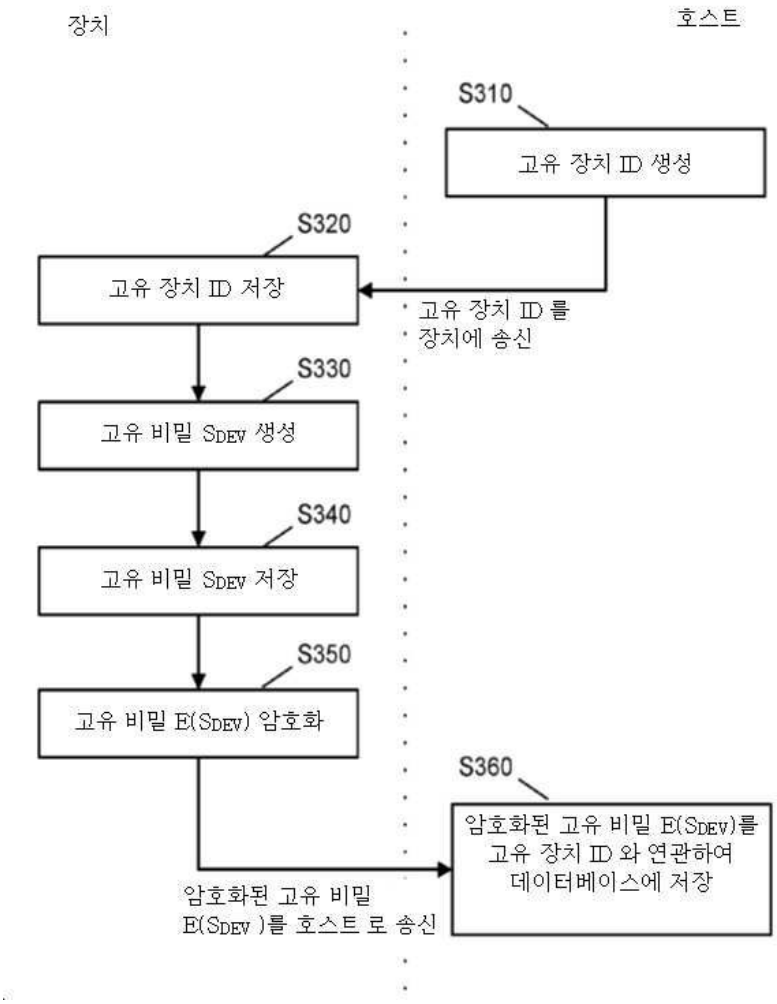
도면9


장치
호스트
고유 장치 ID 요청
S210
고유 장치 ID 전송
S215
고유 장치 ID 를 사용하여 데이터베이스로부터 암호화된 비밀 값 E(SDEV) 검색
S220
E(SDEV)로부터 SDEV 복호화
S225
고유 장치 정보에서 암호화 키 및 메시지 인증 키 유도 (KENC, KMAC)
S230
S235
데이터 레코드 + 고유레코드 ID 요청
고유 레코드 ID + 암호화된 데이터 레코드 전송 (암호화된 데이터 + MAC 데이터)
S240
고유 장치 정보, 고유 레코드 ID 및 MAC 데이터로부터 고유 IV 유도
S245
KENC 및 IV 를 사용하여 암호화된 데이터를 복호화하여 Data 호스트 복구
S250
고유 레코드 ID 및 Data 호스트로부터 MAC 호스트 계산
S255
MAC 데이터 + MAC 호스트?
S260
예
아니요
기록이 유효함
기록이 유효하지 않음

도면10


장치
호스트
S330
고유 비밀 SDEV 생성
S340
고유 비밀 SDEV 저장
S350
고유 비밀 E(SDEV) 암호화
암호화된 고유 비밀
E(SDEV)를 호스트로 송신
S360
암호화된 고유 비밀 E(SDEV)를
데이터베이스에 저장

도면11


장치
호스트
S310
고유 장치 ID 생성
S320
고유 장치 ID 저장
고유 장치 ID 를
장치에 송신
S330
고유 비밀 SDEV 생성
S340
고유 비밀 SDEV 저장
S350
고유 비밀 E(SDEV) 암호화
S360
암호화된 고유 비밀 E(SDEV)를
고유 장치 ID 와 연관하여
데이터베이스에 저장
암호화된 고유 비밀
E(SDEV)를 호스트 로 송신