(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년05월19일
(11) 등록번호 10-2534072
(24) 등록일자 2023년05월15일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 11/14* (2006.01)
G06F 21/60 (2013.01)
(52) CPC특허분류
G06F 21/6209 (2013.01)
G06F 11/1458 (2013.01)
(21) 출원번호 10-2019-7023133
(22) 출원일자(국제) 2018년01월09일
심사청구일자 2021년01월08일
(85) 번역문제출일자 2019년08월06일
(65) 공개번호 10-2019-0104579
(43) 공개일자 2019년09월10일
(86) 국제출원번호 PCT/EP2018/050474
(87) 국제공개번호 WO 2018/127606
국제공개일자 2018년07월12일
(30) 우선권주장
17305020.4 2017년01월09일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
JP2008504592 A*
JP2010539856 A*
JP2014525709 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인터디지털 매디슨 페턴트 홀딩스 에스에이에스
프랑스 75017 빠리 뤼 뒤 꼴로넬 몰 3
(72) 발명자
마르텐스, 데이비드
벨기에 2650 에데겜 프린스 보우데위진란 테크니컬러 딜리버리 테크놀로지스 벨지엄 내
하르두앙, 올리비에
벨기에 1970 웨젬비크 오퀨 스콘 루크트란 23
(74) 대리인
양영준, 이민호, 백만기

전체 청구항 수 : 총 12 항 심사관 : 구대성

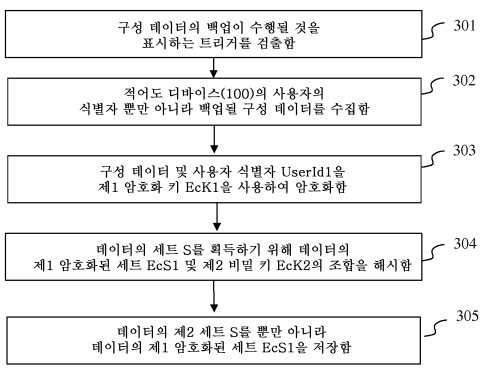
(54) 발명의 명칭 **보안 백업 및 복원을 수행하기 위한 방법들 및 장치**

(57) 요 약

디폴트로 리셋될 때 디바이스 상에서 또는 디바이스가 도난되거나 파괴될 때 다른 디바이스 상에서 상기 구성 데이터를 복원하는 것을 가능하게 하는, 그러한 구성 데이터를 저장하기 위한 백업 절차들이 제공된다. 이러한 구성 데이터는 민감한 데이터이기 때문에, 백업 및 복원 프로세스 전반에 걸쳐 이들의 신뢰도 및 이들의 무결성을

(뒷면에 계속)

대 표 도 - 도3



보호하는 것이 중요하다. 현재 솔루션들은, 백업된 구성 데이터가 오직 디바이스에만 공지된 크리덴셜들을 사용하여 암호화되기 때문에 동일한 디바이스 상에서의 보안 백업 및 복원 프로세스를 가능하게 한다. 이러한 단점들을 극복하기 위해, 동일한 디바이스에 대해 또는 별개의 디바이스에 대해 백업 데이터의 복원을 가능하게 하는 보안 백업 프로세스를 수행하기 위한 솔루션이 제안된다. 이는 디바이스들의 풀에 공통인 암호화 키들을 사용함으로써 가능하게 된다. 그러한 공통 암호화 키들은 디바이스들의 제조 동안 제공된다.

(52) CPC특허분류
G06F 21/602 (2013.01)

명 세 서

청구범위

청구항 1

제2 디바이스로 백업 데이터를 복원하기 위해 제1 디바이스에 저장된 데이터의 백업을 수행하기 위한 방법으로서,

상기 방법은 상기 제1 디바이스에 의해 구현되고, 상기 제1 디바이스는 상기 제1 디바이스와 상기 제2 디바이스를 포함하는 디바이스의 세트에 공통인 제1 미리 프로비저닝된(pre-provisioned) 키와 제2 미리 프로비저닝된 키를 포함하고,

상기 방법은,

상기 제1 미리 프로비저닝된 키를 사용하여, 상기 데이터 및 제1 디바이스의 사용자의 적어도 하나의 식별자를 암호화함으로써 데이터의 제1 세트를 획득하는 단계;

상기 데이터의 제1 세트와 제2 미리 프로비저닝된 키의 조합을 해시(hash)함으로써 데이터의 제2 세트를 획득하는 단계; 및

상기 데이터의 제1 세트와 상기 데이터의 제2 세트를 저장함으로써 상기 제1 디바이스로부터 상기 데이터를 백업하는 단계

를 포함하는, 방법.

청구항 2

제1항에 있어서,

상기 제1 미리 프로비저닝된 키는 대칭적 암호화 키인, 방법.

청구항 3

제1항에 있어서,

상기 제2 미리 프로비저닝된 키는 공통 비밀 키인, 방법.

청구항 4

제1항에 있어서,

상기 백업은 정기적 시간 간격들로 수행되는, 방법.

청구항 5

제1항에 있어서,

상기 백업은 상기 제1 디바이스의 사용자 인터페이스 상에서 검출된 액션에 의해 트리거링되는, 방법.

청구항 6

제1 디바이스로부터 제2 디바이스로 백업 데이터를 복원하기 위한 방법으로서,

상기 방법은 상기 제2 디바이스에 의해 구현되고, 상기 제2 디바이스는 상기 제1 디바이스와 제2 디바이스를 포함하는 디바이스의 세트에 공통인 제1 미리 프로비저닝된 키와 제2 미리 프로비저닝된 키를 포함하고,

상기 방법은,

상기 백업 데이터로부터 암호화된 데이터의 제1 세트 및 데이터의 제2 세트를 검색하는 단계;

상기 제2 디바이스에서, 검색한 암호화된 데이터의 제1 세트와 상기 제2 미리 프로비저닝된 키의 조합을 해시함

으로써 데이터의 제3 세트를 획득하는 단계; 및

획득한 데이터의 제3 세트가 검색한 데이터의 제2 세트와 동일하다는 조건 하에서, 상기 제1 미리 프로비저닝된 키를 사용하여 상기 검색한 데이터의 제2 세트를 암호해독함으로써 암호해독된 데이터의 제2 세트를 획득하고, 상기 암호해독된 데이터의 제2 세트로부터 복원 데이터 및 상기 제1 디바이스의 사용자의 적어도 하나의 식별자를 검색하고, 검색한 상기 제1 디바이스의 사용자의 적어도 하나의 식별자가 상기 제2 디바이스에 제공된 제2 사용자 식별자와 동일하다는 조건 하에서, 상기 복원 데이터를 상기 제2 디바이스에 복원하는 단계

를 포함하는, 방법.

청구항 7

제1항 내지 제5항 중 어느 한 항에 따른 방법을 실행하도록 구성되는 프로세서를 포함하는 제1 장치.

청구항 8

제6항에 따른 방법을 실행하도록 구성되는 프로세서를 포함하는 제2 장치.

청구항 9

기록 매체에 저장된 컴퓨터 프로그램으로서,

상기 프로그램이 프로세서에 의해 실행될 때 제1항 내지 제5항 중 어느 한 항에 따른 방법의 구현을 위한 프로그램 코드 명령어들을 포함하는 것을 특징으로 하는, 기록 매체에 저장된 컴퓨터 프로그램.

청구항 10

프로세서 판독가능 매체로서,

프로세서로 하여금 제1항 내지 제5항 중 어느 한 항에 따른 방법을 수행하게 하기 위한 명령어들을 저장한, 프로세서 판독가능 매체.

청구항 11

기록 매체에 저장된 컴퓨터 프로그램으로서,

상기 프로그램이 프로세서에 의해 실행될 때 제6항에 따른 방법의 구현을 위한 프로그램 코드 명령어들을 포함하는 것을 특징으로 하는, 기록 매체에 저장된 컴퓨터 프로그램.

청구항 12

프로세서 판독가능 매체로서,

프로세서로 하여금 제6항에 따른 방법을 수행하게 하기 위한 명령어들을 저장한, 프로세서 판독가능 매체.

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 구성 데이터를 복원하기 위한 솔루션들에 관한 것이다. 더 상세하게는, 본 발명은 구성 데이터의 보안 백업 및 상기 백업 데이터의 용이한 복원을 수행하기 위한 방법들에 관한 것이다.

배 경 기 술

[0002] 기존의 통신 디바이스들, 예를 들어, 주거지 게이트웨이들, 액세스 포인트들, 중계기들, 모바일 폰들, 컴퓨터들 등은 이들의 사용자들이 원하는 대로 거동하기 위해 상이한 세팅들에 따라 구성된다.

[0003] 디폴트로 리셋될 때 디바이스 상에서 또는 디바이스가 도난되거나 파괴될 때 다른 디바이스 상에서 상기 구성 데이터를 복원하는 것을 가능하게 하는, 그러한 구성 데이터를 저장하기 위한 백업 절차들이 제공된다.

[0004] 이러한 구성 데이터는 민감한 데이터이기 때문에, 백업 및 복원 프로세스 전반에 걸쳐 이들의 신뢰도 및 이들의 무결성을 보호하는 것이 중요하다.

[0005] 현재 솔루션들은, 백업된 구성 데이터가 오직 디바이스에만 공지된 크리덴셜들을 사용하여 암호화되기 때문에 동일한 디바이스 상에서의 보안 백업 및 복원 프로세스를 가능하게 한다.

[0006] 따라서, 구성 데이터가 다른 디바이스 상에서 복원되려는 경우, 구성 데이터는 평문(plaintext)으로 저장되는데, 즉, 이들은 암호화되지 않아서 상기 다른 디바이스 상에서의 복원을 허용한다. 이러한 보안의 결핍은 기존의 백업 및 복원 솔루션들의 주요 단점이다.

[0007] 본 발명은 상기 내용을 고려하여 고안되었다.

발명의 내용

[0008] 본 발명의 제1 양태에 따르면, 제1 디바이스의 구성 데이터의 보안 백업을 수행하기 위한 컴퓨터에 의해 구현된 방법이 제공되며, 상기 방법은,

[0009] 상기 제1 디바이스의 판독 전용 메모리에 저장된 제1 미리 프로비저닝된(pre-provisioned) 암호화 키를 사용하여, 상기 구성 데이터 및 상기 제1 디바이스의 사용자의 적어도 하나의 식별자를 암호화하는 단계,

[0010] 암호화된 구성 데이터 및 상기 제1 디바이스의 사용자의 적어도 하나의 식별자와, 상기 제1 디바이스의 상기 판독 전용 메모리에 저장된 제2 미리 프로비저닝된 비밀 키의 조합을 해시(hash)함으로써 획득된 데이터의 세트를 암호화하는 단계,

[0011] 암호화된 구성 데이터 및 상기 제1 디바이스의 사용자의 적어도 하나의 식별자 및 암호화된 데이터의 세트를 저장하는 단계를 포함한다.

[0012] 이러한 솔루션은 동일한 디바이스 상에서 또는 별개의 디바이스 상에서 백업 데이터의 복원을 가능하게 하는 보안 백업 프로세스를 제공한다. 이는 디바이스들, 예를 들어, 동일한 제품 모델의 디바이스들 또는 동일한 회사에 의해 제조된 다른 제품 모델의 디바이스들의 풀(pool)에 공통이고 상기 디바이스의 메모리에 미리 로딩된(pre-loaded) 암호화 키들을 사용함으로써 가능하게 된다.

[0013] 그러한 공통 암호화 키들은, 예를 들어, 디바이스들의 제조 동안 제공되고 디바이스들의 메모리의 섹션에 저장된다.

[0014] 본 발명의 실시예에서, 제1 미리 프로비저닝된 암호화 키는 대칭적 암호화 키이다.

[0015] 본 발명의 실시예에서, 제2 미리 프로비저닝된 암호화 키는 공통 비밀 키이다.

[0016] 본 발명의 실시예에서, 보안 백업은 정기적 시간 간격들로 수행된다.

[0017] 이러한 실시예는 디바이스의 사용자로부터의 액션을 요구하지 않는다. 이는, 구성 데이터의 감도에 따라 유용한 것으로 입증될 수 있는 정기적 백업을 갖는 것을 가능하게 한다.

[0018] 본 발명의 실시예에서, 보안 백업은 제1 디바이스의 사용자 인터페이스 상에서 검출된 액션에 의해 트리거링된다.

[0019] 디바이스의 사용자는 자신의 필요에 따라 구성 데이터의 백업을 트리거링할 수 있다.

[0020] 본 발명의 다른 목적은 제1 디바이스 상에서 구성 데이터를 복원하기 위한 컴퓨터에 의해 구현된 방법에 관한 것이고, 상기 방법은,

[0021] 상기 제1 디바이스의 판독 전용 메모리에 저장된 제1 미리 프로비저닝된 비밀 키를 사용하여 복원될 구성 데이터와 관련된 데이터의 제2 세트의 무결성을 확인하는 단계,

[0022] 데이터의 제2 세트의 무결성이 확인될 때, 상기 제1 디바이스의 상기 판독 전용 메모리에 저장된 제2 미리 프로비저닝된 암호해독 키를 사용하여 구성 데이터를 포함하는 데이터의 제2 세트를 암호해독하는 단계,

[0023] 암호해독된 데이터의 제2 세트에 포함된 상기 제1 디바이스의 사용자의 적어도 하나의 식별자가 제1 디바이스에 제공된 상기 제1 디바이스의 상기 사용자의 적어도 하나의 식별자에 매칭할 때, 구성 데이터를 복원하는 단계를 포함한다.

[0024] 이러한 솔루션은 제1 디바이스 상에 보안 백업된 데이터를 제2 디바이스 상에서 복원하는 것을 가능하게 한다. 이는 디바이스들, 예를 들어, 동일한 제품 모델의 디바이스들 또는 동일한 회사에 의해 제조된 다른 제품 모델의 디바이스들의 풀에 공통인 미리 프로비저닝된 암호해독 키들을 사용함으로써 가능하게 된다.

[0025] 그러한 공통 미리 프로비저닝된 암호해독 키들은, 예를 들어, 디바이스들의 제조 동안 제공되고 디바이스들의 메모리의 섹션에 저장된다. 따라서 이러한 암호해독 키들은, 백업 프로세스 동안 자신들의 구성 데이터를 암호화하기 위해 동일한 디바이스들에 의해 사용된 암호화 키들로 암호화된 데이터를 암호해독하기 위해 사용될 수 있다.

[0026] 이러한 솔루션에서, 복원될 데이터의 무결성이 확인되지 않으면 복원된 프로세스가 중단되기 때문에, 백업된 데이터의 무결성은 보장된다.

[0027] 또한, 전체 프로세스의 보안을 증가시키기 위해, 최종 확인이 수행된 경우에만 데이터가 디바이스 상에서 복원된다. 이러한 최종 확인은, 백업이 수행된 디바이스의 사용자가, 데이터가 복원될 디바이스의 동일한 사용자임을 검증하는 것으로 이루어진다. 이러한 확인은, 상이한 디바이스들이 동일한 암호화 및 암호해독 키들을 사용하기 때문에 중요하다.

[0028] 본 발명의 실시예에서, 데이터의 제2 세트의 무결성을 확인하는 것은,

[0029] 암호화된 데이터의 제2 세트와 제1 미리 프로비저닝된 비밀 키의 조합을 해시함으로써 데이터의 제3 세트를 생성하는 것,

[0030] 상기 데이터의 제1 세트를 상기 데이터의 제3 세트와 비교하는 것을 포함하고,

[0031] 데이터의 제1 세트의 무결성은 상기 데이터의 제1 세트가 상기 데이터의 제3 세트와 동일할 때 확인된다.

[0032] 본 발명의 다른 목적은 구성 데이터의 보안 백업을 수행할 수 있는 장치이고, 상기 장치는,

[0033] 상기 제1 디바이스의 제조 동안 상기 제1 디바이스의 판독 전용 메모리에 저장된 상기 구성 데이터 및 상기 제1 디바이스의 사용자의 적어도 하나의 식별자를 암호화하고,

[0034] 암호화된 구성 데이터 및 상기 제1 미리 프로비저닝된 디바이스의 사용자의 적어도 하나의 식별자와, 상기 제1 디바이스의 상기 판독 전용 메모리에 저장된 제2 미리 프로비저닝된 비밀 키의 조합을 해시(hash)함으로써 획득된 데이터의 세트를 암호화하고,

[0035] 암호화된 구성 데이터 및 상기 제1 디바이스의 사용자의 적어도 하나의 식별자 및 암호화된 데이터의 세트를 저장하도록 구성된 프로세서를 포함한다.

[0036] 본 발명의 다른 목적은 제1 디바이스 상에서 구성 데이터를 복원할 수 있는 장치이고, 장치는,

[0037] 상기 제1 디바이스의 판독 전용 메모리에 저장된 제1 미리 프로비저닝된 비밀 키를 사용하여 복원될 구성 데이터와 관련된 데이터의 제2 세트의 무결성을 확인하고,

[0038] 데이터의 제2 세트의 무결성이 확인될 때, 상기 제1 디바이스의 상기 판독 전용 메모리에 저장된 제2 미리 프로비저닝된 암호해독 키를 사용하여 구성 데이터를 포함하는 그 데이터의 제2 세트를 암호해독하고,

[0039] 암호해독된 데이터의 제2 세트에 포함된 상기 제1 디바이스의 사용자의 적어도 하나의 식별자가 제1 디바이스에 제공된 상기 제1 디바이스의 상기 사용자의 적어도 하나의 식별자에 매칭할 때, 구성 데이터를 복원하도록 구성된 프로세서를 포함한다.

[0040] 본 발명의 요소들에 의해 구현되는 일부 프로세스들은 컴퓨터로 구현될 수 있다. 따라서, 이러한 요소들은 완전한 하드웨어 실시예, 완전한 소프트웨어 실시예(펌웨어, 상주 소프트웨어, 마이크로-코드 등을 포함함), 또는 모두가 일반적으로 본원에서 "회로", "모듈" 또는 "시스템"으로 지칭될 수 있는 소프트웨어 및 하드웨어 양태들을 결합한 실시예의 형태를 취할 수 있다. 또한, 이러한 요소들은 매체에 구현되는 컴퓨터 사용가능 프로그램

코드를 갖는 표현의 임의의 유형의 매체로 구현되는 컴퓨터 프로그램 제품의 형태를 취할 수 있다.

[0041] 본 발명의 요소들은 소프트웨어로 구현될 수 있기 때문에, 본 발명은 임의의 적절한 캐리어 매체 상에서 프로그래밍가능 장치로의 제공을 위한 컴퓨터 판독가능 코드로서 구현될 수 있다. 유형의 캐리어 매체는 플로피 디스크, CD-ROM, 하드 디스크 드라이브, 자기 테이프 디바이스 또는 솔리드 스테이트 메모리 디바이스 등과 같은 저장 매체를 포함할 수 있다. 일시적인 캐리어 매체는 전기 신호, 전자 신호, 광학 신호, 음향 신호, 자기 신호 또는 전자기 신호, 예를 들어, 마이크로파 또는 RF 신호와 같은 신호를 포함할 수 있다.

도면의 간단한 설명

[0042] 이제, 본 발명의 실시예들이 단지 예시의 방식으로, 하기 도면들을 참조하여 설명될 것이다.

도 1은 본 발명의 실시예에 따른 백업 및 복원 방법들을 구현하는 통신 디바이스를 표현한다.

도 2는 본 발명의 실시예에 따른 통신 디바이스의 예를 예시하는 개략적 블록도이다.

도 3은 본 발명의 실시예에 따라 구성 데이터의 보안 백업을 수행하기 위한 프로세스를 설명하기 위한 흐름도를 표현한다.

도 4는 본 발명의 실시예에 따라 보안 백업된 구성 데이터를 복원하기 위한 프로세스를 설명하기 위한 흐름도를 표현한다.

발명을 실시하기 위한 구체적인 내용

[0043] 본 기술분야의 통상의 기술자에 의해 인식될 바와 같이, 본 원리들의 양태들은 시스템, 방법 또는 컴퓨터 판독가능 매체로서 구현될 수 있다. 따라서, 본 원리들의 양태들은 완전한 하드웨어 실시예, 완전한 소프트웨어 실시예(펌웨어, 상주 소프트웨어, 마이크로-코드 등을 포함함), 또는 모두가 일반적으로 본원에서 "회로", "모듈" 또는 "시스템"으로 지칭될 수 있는 소프트웨어 및 하드웨어 양태들을 결합한 실시예의 형태를 취할 수 있다. 또한, 본 원리들의 양태들은 컴퓨터 판독가능 저장 매체의 형태를 취할 수 있다. 하나 이상의 컴퓨터 판독가능 저장 매체(들)의 임의의 조합이 활용될 수 있다.

[0044] 도 1에 표현된 바와 같이, 제1 통신 디바이스(100)는 홈 게이트웨이이다. 제1 통신 디바이스(100)는 예를 들어, 광대역 네트워크와 통신하기 위한 적어도 하나의 네트워크 인터페이스(110)를 포함한다. 이러한 네트워크 인터페이스(110)는 예를 들어, xDSL(x Digital Subscriber Line)을 사용하여 DSLAM(Digital Subscriber Line Access Multiplexer)으로부터 및 DSLAM으로 또는 광섬유를 통해 OLT(Optical Line Termination)로부터 또는 OLT로 데이터를 수신 및 송신하도록 구성된다.

[0045] 본 발명의 실시예에서, 제1 통신 디바이스(100)는 무선 및 유선 송신 인터페이스들 둘 모두를 임베딩할 수 있다.

[0046] 도 2는 본 발명의 실시예에 따른 제1 통신 디바이스(100)의 예를 예시하는 개략적 블록도이다.

[0047] 제1 통신 디바이스(100)는 버스(206)에 의해 접속되는 프로세서(201), 저장 유닛(202), 입력 디바이스(203), 디스플레이 디바이스(204) 및 인터페이스 유닛(205)을 포함한다. 물론, 제1 통신 디바이스(100)의 구성 요소들은 버스 접속 이외의 접속에 의해 접속될 수 있다.

[0048] 프로세서(201)는 제1 통신 디바이스(100)의 동작들을 제어한다. 저장 유닛(202)은 프로세서(201)에 의해 실행될 제1 통신 디바이스(100)의 구성 데이터, 및 다양한 데이터, 프로세서(201)에 의해 수행되는 계산들에 의해 사용되는 파라미터들, 프로세서(201)에 의해 수행되는 계산들의 중간 데이터 등의 보안 백업 및 복원을 수행할 수 있는 적어도 하나의 프로그램을 저장한다. 프로세서(201)는 임의의 공지되고 적합한 하드웨어, 또는 소프트웨어, 또는 하드웨어와 소프트웨어의 조합으로 형성될 수 있다. 예를 들어, 프로세서(201)는 프로세싱 회로와 같은 전용 하드웨어에 의해 또는 메모리에 저장된 프로그램을 실행하는 CPU(Central Processing Unit)와 같은 프로그래밍가능 프로세싱 유닛에 의해 형성될 수 있다.

[0049] 저장 유닛(202)은 프로그램, 데이터 등을 컴퓨터 판독가능 방식으로 저장할 수 있는 임의의 적절한 스토리지 또는 수단에 의해 형성될 수 있다. 저장 유닛(202)의 예는 반도체 메모리 디바이스와 같은 비일시적 컴퓨터 판독가능 저장 매체, 및 판독 및 기록 유닛에 로딩된 자기, 광학 또는 광-자기 기록 매체를 포함한다. 프로그램은 프로세서(201)로 하여금 도 3 및 도 4를 참조하여 이하 설명된 바와 같이 본 개시내용의 실시예에 따른 보안 백

업 및 복원의 프로세스를 수행하게 한다.

[0050] 입력 디바이스(203)는 사용될 송신 인터페이스를 선택하기 위해 사용되는 파라미터들의 사용자 선택들을 수행하기 위해, 입력 커맨드들에 대해 사용자에 의해 사용하기 위한 키보드, 마우스와 같은 포인팅 디바이스 등에 의해 형성될 수 있다. 출력 디바이스(204)는, 디스플레이하기 위한 디스플레이 디바이스, 예를 들어, 그래픽 사용자 인터페이스(GUI)에 의해 형성될 수 있다. 입력 디바이스(203) 및 출력 디바이스(204)는 예를 들어 터치스크린 패널에 의해 일체형으로 형성될 수 있다.

[0051] 인터페이스 유닛(205)은 제1 통신 디바이스(100)와 외부 장치 사이의 인터페이스를 제공한다. 인터페이스 유닛(205)은 케이블 또는 무선 통신을 통해 외부 장치와 통신가능할 수 있다. 실시예에서, 외부 장치는 실제 카메라와 같은 광학 포착 시스템일 수 있다.

[0052] 본 발명은 모바일 폰들, 컴퓨터들, 캡터(captor)들 등과 같은, 게이트웨이들 이외의 디바이스들에서 실행될 수 있다.

[0053] 도 3은 구성 데이터의 보안 백업을 수행하기 위한 프로세스를 설명하기 위한 흐름도이다. 본 발명은, 데이터가 백업될 디바이스와 상기 백업 데이터가 복원될 디바이스 사이에서 암호화 및 비밀 키들과 같은 공유된 비밀의 사용에 의존한다. 그러한 2개의 디바이스들은 하나일 수 있고 동일하거나 별개의 디바이스들일 수 있다. 디바이스들의 사용자는 공유된 비밀로 디바이스들을 구성할 필요가 없다.

[0054] 단계(301)에서, 프로세서(201)는 디바이스(100)의 구성 데이터의 백업이 수행될 것을 표시하는 트리거를 검출한다.

[0055] 본 발명의 제1 실시예에서, 트리거는 타이머의 만료이다. 예를 들어, 디바이스(100)의 구성 데이터의 백업은 구성 데이터의 감도에 따라 매일 또는 매 시간 또는 매 X분 등마다 스케줄링된다.

[0056] 본 발명의 다른 실시예에서, 트리거는 입력 디바이스(203) 상의 액션의 검출이다. 이러한 경우 이러한 액션의 검출은 백업 프로세스를 트리거링한다.

[0057] 단계(302)에서, 프로세서(201)는 고객 식별자, 폰 번호 등과 같은 적어도 디바이스(100)의 사용자의 식별자 UserId1 뿐만 아니라 백업될 구성 데이터를 수집한다.

[0058] 단계(303)에서, 구성 데이터 및 사용자 식별자 UserId1은 제1 미리 프로비저닝된 암호화 키 EcK1을 사용하여 암호화된다. 그러한 암호화된 데이터는 데이터의 제1 암호화된 세트 EcS1로 이루어진다.

[0059] 이러한 제1 암호화 키 EcK1은 예를 들어 디바이스(100)의 제조 동안 및 더 일반적으로는 디바이스(100)와 동일한 제품 모델의 모든 디바이스들 또는 동일한 제조자의 다른 제품 모델들의 디바이스들에 프로비저닝된다. 제1 미리 프로비저닝된 암호화 키 EcK1은 하드웨어 보안 모듈(HSM)에 의해 생성된 진정으로 무작위의 데이터로 이루어진다. 제1 미리 프로비저닝된 암호화 키 EcK1은 저장 유닛(202)의 파티션에 저장된다.

[0060] 제1 미리 프로비저닝된 암호화 키는 예를 들어, AES-256 프로토콜(진보된 암호화 표준)에 따른 대칭적 키이다.

[0061] 제1 미리 프로비저닝된 암호화 키 EcK1은 또한 디바이스(100)와 동일한 제품 모델의 모든 디바이스들 또는 동일한 제조자의 다른 제품 모델들의 디바이스들에 공통인 암호화 뿐만 아니라 제품 모델의 식별자 및 일련 번호와 같은 디바이스(100)의 식별자를 사용하여 프로세서(201)에 의해 생성될 수 있다.

[0062] 단계(304)에서, 예를 들어, HMAC 방식(keyed-Hash Message Authentication Code)을 사용하여 데이터의 제1 미리 프로비저닝된 암호화된 세트 EcS1 및 제2 미리 프로비저닝된 비밀 키 EcK2의 조합을 해시함으로써 데이터의 제2 세트 S가 획득된다.

[0063] 이러한 제2 미리 프로비저닝된 비밀 키 EcK2는 예를 들어 디바이스(100)의 제조 동안 및 더 일반적으로는 디바이스(100)와 동일한 제품 모델의 모든 디바이스들 또는 동일한 제조자의 다른 제품 모델들의 디바이스들에 프로비저닝된다. 제2 미리 프로비저닝된 비밀 키 EcK2는 하드웨어 보안 모듈(HSM)에 의해 생성된 진정으로 무작위의 데이터로 이루어진다. 제2 미리 프로비저닝된 비밀 키 EcK2는 저장 유닛(202)의 파티션에 저장된다.

[0064] 제2 미리 프로비저닝된 비밀 키 EcK2는 또한 디바이스(100)와 동일한 제품 모델의 모든 디바이스들 또는 동일한 제조자의 다른 제품 모델들의 디바이스들에 공통인 암호화 뿐만 아니라 제품 모델의 식별자 및 일련 번호와 같은 디바이스(100)의 식별자를 사용하여 프로세서(201)에 의해 생성될 수 있다.

[0065] 본 발명의 실시예에서, 제1 미리 프로비저닝된 암호화 키 EcK1 및 제2 미리 프로비저닝된 비밀 키 EcK2는 디바

이스(100)의 제조자 또는 디바이스(100)를 관리하는 제공자와 같은 제3자에 의해 디바이스(100)에 송신된다. 제1 미리 프로비저닝된 암호화 키 EcK1 및 제2 미리 프로비저닝된 비밀 키 EcK2는 디바이스(100)와 동일한 제품 모델의 모든 디바이스들 또는 동일한 제조자의 다른 제품 모델들의 디바이스들에 공통이어서, 비밀이 상이한 디바이스들 사이에 공유될 수 있게 한다.

[0066] 단계(304) 동안 획득된 데이터의 제2 세트 S는 복원 프로세스 동안 백업된 구성 데이터의 무결성을 확인하기 위해 사용된다.

[0067] 단계(305)에서, 프로세서(201)는 암호화된 구성 데이터 및 디바이스(a100)의 사용자의 적어도 하나의 식별자 뿐만 아니라 데이터의 제2 세트 S를 포함하는 데이터의 제1 암호화된 세트 EcS1을 저장한다.

[0068] 그러한 데이터는 디바이스(100)의 저장 유닛(202) 또는 원격 서버에 저장된다. 이러한 나중의 실시예는 디바이스 상에서 구성을 복원하는데 필요한 데이터를 원격으로 검색할 수 있게 한다.

[0069] 도 4는 보안 백업된 구성 데이터를 복원하기 위한 프로세스를 설명하기 위한 흐름도이다. 본 발명은, 데이터가 백업된 디바이스와 상기 백업 데이터가 복원될 디바이스 사이에서 암호해독 및 비밀 키들과 같은 공유된 비밀의 사용에 의존한다. 그러한 2개의 디바이스들은 하나일 수 있고 동일하거나 별개의 디바이스들일 수 있다. 디바이스들의 사용자는 공유된 비밀로 디바이스들을 구성할 필요가 없다.

[0070] 단계(401)에서, 프로세서(201)는 디바이스(100)의 구성 데이터의 복원이 수행될 것을 표시하는 트리거를 검출한다.

[0071] 본 발명의 실시예에서, 트리거는 리셋 커맨드 또는 부트 커맨드와 같은 입력 디바이스(203) 상의 액션의 검출이다. 다른 실시예에서, 트리거는 입력 디바이스(203) 상의 액션의 검출이다. 이러한 경우 이러한 액션의 검출은 복원 프로세스를 트리거링한다.

[0072] 단계(402)에서, 프로세서(201)는 데이터의 제1 세트 S 및 데이터의 제2 암호화된 세트 EcS1을 검색한다. 데이터의 제1 세트 S는 데이터의 제2 암호화된 세트 EcS1의 무결성을 확인하기 위해 사용되는 한편, 데이터의 제2 암호화된 세트 EcS1은 복원 프로세스를 완료하는데 필요한 구성 데이터를 포함한다.

[0073] 실시예에서, 구성의 복원은 동일한 디바이스(100) 상에서 발생한다. 이러한 경우, 프로세서(201)는 저장 유닛(202)에서 데이터의 제1 세트 S 및 데이터의 제2 암호화된 세트 EcS1을 검색할 수 있다.

[0074] 다른 실시예에서, 구성의 복원은 디바이스(100)와 동일한 제품 모델의 디바이스 또는 동일한 제조자의 다른 제품 모델의 디바이스와 같은 다른 디바이스 상에서 발생한다. 이러한 경우, 프로세서(201)는 원격 서버로부터 데이터의 제1 세트 S 및 데이터의 제2 암호화된 세트 EcS1을 검색할 수 있다.

[0075] 단계(403)에서, 프로세서(201)는 데이터의 제2 암호화된 세트 EcS1의 무결성을 확인한다. 프로세서(201)는, 도 3을 참조하여 설명된 백업 프로세스 동안 사용된 제2 미리 프로비저닝된 비밀 키 EcK2에 대응하는 제1 미리 프로비저닝된 비밀 키 DcK2를 사용하여 데이터의 상기 제2 암호화된 세트 EcS1의 무결성을 확인한다.

[0076] 제1 미리 프로비저닝된 비밀 키 DcK2는 예를 들어 디바이스(100)의 제조 동안 및 더 일반적으로는 디바이스(100)와 동일한 제품 모델의 모든 디바이스들 또는 동일한 제조자의 다른 제품 모델들의 디바이스들에 프로비저닝된다. 제1 미리 프로비저닝된 비밀 키 DcK2는 하드웨어 보안 모듈(HSM)에 의해 생성된 진정으로 무작위의 데이터로 이루어진다. 제1 미리 프로비저닝된 비밀 키 DcK2는 저장 유닛(202)의 파티션에 저장된다.

[0077] 제1 미리 프로비저닝된 비밀 키 DcK2는 또한 디바이스(100)와 동일한 제품 모델의 모든 디바이스들 또는 동일한 제조자의 다른 제품 모델들의 디바이스들에 공통인 암호화 뿐만 아니라 제품 모델의 식별자 및 일련 번호와 같은 디바이스(100)의 식별자를 사용하여 프로세서(201)에 의해 생성될 수 있다.

[0078] 프로세서(201)는, 예를 들어, HMAC 방식을 사용하여 암호화된 데이터의 제2 세트 EcS1 및 제2 미리 프로비저닝된 비밀 키 EcK2의 조합을 해시함으로써 데이터의 제3 세트 S'을 생성하고 데이터의 제1 세트 S를 데이터의 제3 세트 S'와 비교한다.

[0079] 데이터의 제1 세트 S 및 데이터의 제3 세트 S'가 동일하면, 프로세서(201)는 단계(404)를 실행하고, 이들이 상이하면, 복원 프로세스가 중단된다.

[0080] 단계(404) 동안, 프로세서(201)는, 도 3을 참조하여 설명된 백업 프로세스 동안 사용된 제1 미리 프로비저닝된 암호화 키 EcK1에 대응하는 제2 미리 프로비저닝된 암호해독 키 DcK1을 사용하여 데이터의 제2 암호화된 세트

EcS1을 암호해독한다.

[0081] 제2 미리 프로비저닝된 암호해독 키 DcK1은 예를 들어 디바이스(100)의 제조 동안 및 더 일반적으로는 디바이스(100)와 동일한 제품 모델의 모든 디바이스들 또는 동일한 제조자의 다른 제품 모델들의 디바이스들에 프로비저닝된다. 제2 미리 프로비저닝된 암호해독 키 DcK1은 하드웨어 보안 모듈(HSM)에 의해 생성된 진정으로 무작위의 데이터로 이루어진다. 제2 암호해독 키 DcK1은 저장 유닛(202)의 파티션에 저장된다.

[0082] 제2 미리 프로비저닝된 암호해독 키 DcK1은 AES-256 프로토콜(진보된 암호화 표준)에 따른 대칭적 키이다.

[0083] 제2 미리 프로비저닝된 암호해독 키 DcK1은 또한 디바이스(100)와 동일한 제품 모델의 모든 디바이스들 또는 동일한 제조자의 다른 제품 모델들의 디바이스들에 공통인 암호화 뿐만 아니라 제품 모델의 식별자 및 일련 번호와 같은 디바이스(100)의 식별자를 사용하여 프로세서(201)에 의해 생성될 수 있다.

[0084] 제1 미리 프로비저닝된 비밀 키 DcK2 및 제2 미리 프로비저닝된 암호해독 DcK1은 디바이스(100)와 동일한 제품 모델의 모든 디바이스들 또는 동일한 제조자의 다른 제품 모델들의 디바이스들에 공통이어서, 비밀이 상이한 디바이스들 사이에 공유될 수 있게 한다.

[0085] 본 발명의 실시예에서, 제1 미리 프로비저닝된 비밀 키 DcK2 및 제2 미리 프로비저닝된 암호해독 키 DcK1은 디바이스(100)의 제조자 또는 디바이스(100)를 관리하는 제공자와 같은 제3자에 의해 디바이스(100)에 송신된다.

[0086] 데이터의 제2 암호화된 세트 EcS1의 암호해독이 가능하지 않으면, 복원 프로세스를 수행하는 디바이스가 인가된 디바이스가 아님을 의미하여, 복원 프로세스는 중단된다.

[0087] 데이터의 제2 암호화된 세트 EcS1의 암호해독이 성공적이면, 구성 데이터 뿐만 아니라 적어도 하나의 사용자 식별자 UserId1이 프로세서(201)에 의해 검색된다.

[0088] 단계(405)에서, 프로세서(201)는 단계(404) 동안 검색된 사용자 식별자 UserId1을, 복원 프로세스를 실행하는 디바이스에 로컬로 제공된 제2 사용자 식별자 UserId2와 비교한다. 제1 사용자 식별자 UserId1 및 제2 사용자 식별자 UserId2는 동일할 수 있는데, 예를 들어, 이들은 디바이스(100)의 사용자의 폰 번호일 수 있다.

[0089] 2개의 사용자 식별자들 UserId1 및 UserId2가 매칭하면, 프로세서(201)는 구성 데이터의 복원을 수행할 수 있고, 사용자 식별자들 UserId1 및 UserId2가 매칭하지 않으면, 복원 프로세스는 중단된다.

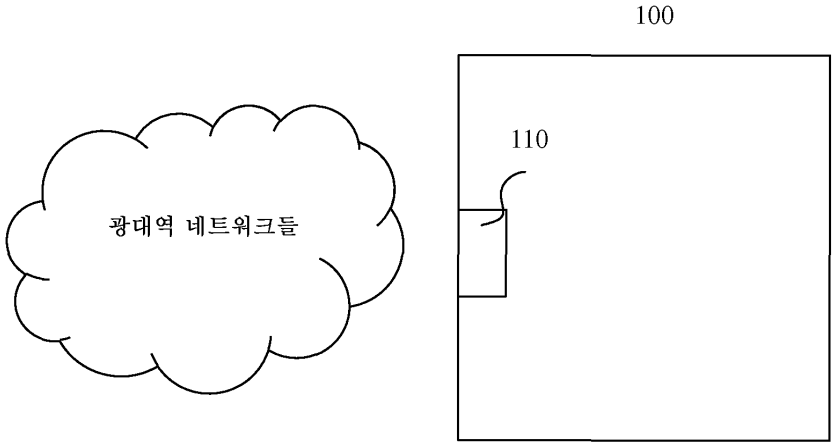
[0090] 제2 사용자 식별자 UserId2는 입력 디바이스(203)를 통해 로컬로, 또는 복원 프로세스의 시작 전에 TR-69와 같은 프로세스들을 사용하여 원격으로 제공될 수 있다.

[0091] 본 발명은 특정 실시예를 참조하여 위에서 설명되었지만, 본 발명은 특정 실시예로 제한되지 않으며, 본 발명의 범위 내에 있는 수정은 본 기술분야의 통상의 기술자에게 자명할 것이다.

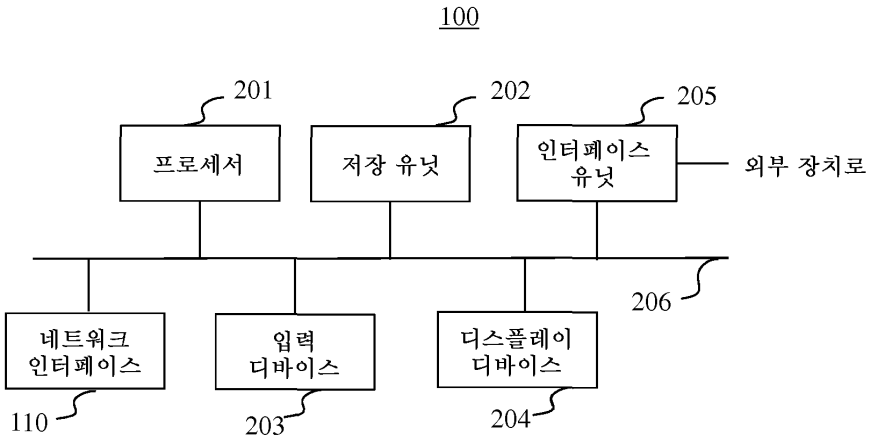
[0092] 단지 예로서 주어지며 본 발명의 범위를 제한하도록 의도되지 않고 첨부된 청구항에 의해서만 결정되는 전술된 예시적인 실시예를 참조할 때 본 기술분야의 통상의 기술자에게 많은 추가적인 수정 및 변경이 착안될 것이다. 특히, 상이한 실시예로부터의 상이한 특징부는 적절한 경우에 상호교환될 수 있다.

도면

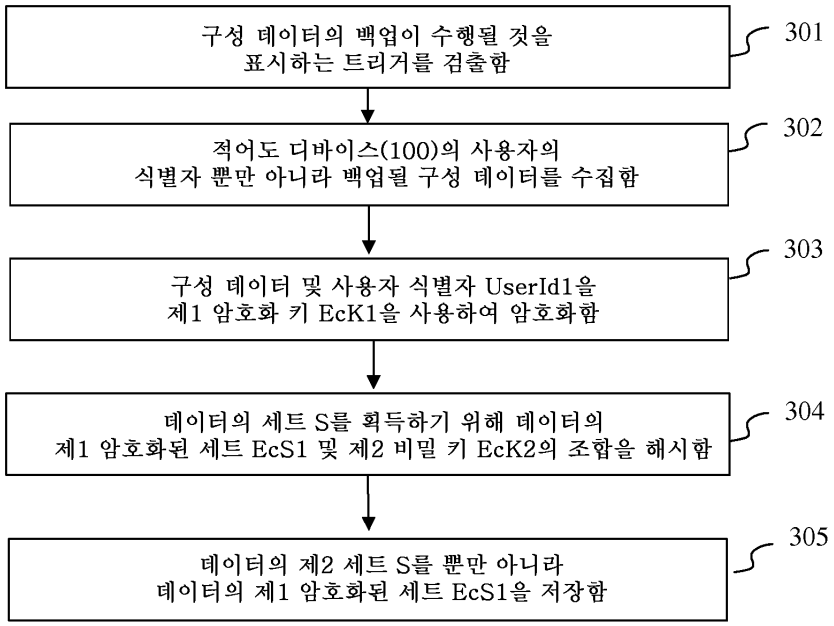
도면1


100
110
광대역 네트워크들

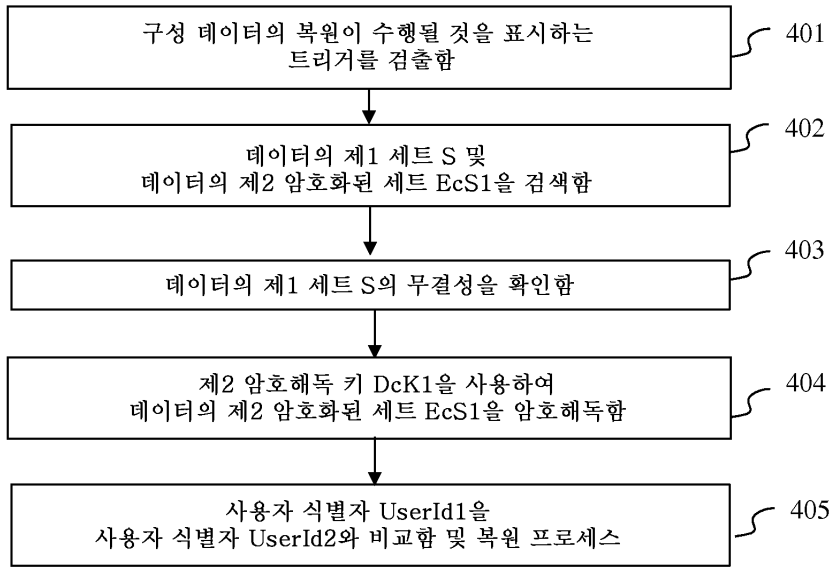
도면2


100
201
202
205
프로세서
저장 유닛
인터페이스 유닛
외부 장치로
206
네트워크 인터페이스
입력 디바이스
디스플레이 디바이스
110
203
204

도면3


구성 데이터의 백업이 수행될 것을
표시하는 트리거를 검출함
301
적어도 디바이스(100)의 사용자의
식별자 뿐만 아니라 백업될 구성 데이터를 수집함
302
구성 데이터 및 사용자 식별자 UserId1을
제1 암호화 키 EcK1을 사용하여 암호화함
303
데이터의 세트 S를 획득하기 위해 데이터의
제1 암호화된 세트 EcS1 및 제2 비밀 키 EcK2의 조합을 해시함
304
데이터의 제2 세트 S를 뿐만 아니라
데이터의 제1 암호화된 세트 EcS1을 저장함
305

도면4


구성 데이터의 복원이 수행될 것을 표시하는
트리거를 검출함
401
데이터의 제1 세트 S 및
데이터의 제2 암호화된 세트 EcS1을 검색함
402
데이터의 제1 세트 S의 무결성을 확인함
403
제2 암호해독 키 DcK1을 사용하여
데이터의 제2 암호화된 세트 EcS1을 암호해독함
404
사용자 식별자 UserId1을
사용자 식별자 UserId2와 비교함 및 복원 프로세스
405