(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년10월25일
(11) 등록번호 10-2458922
(24) 등록일자 2022년10월20일

(51) 국제특허분류(Int. Cl.)
G06F 21/44 (2013.01) *G06F 21/45* (2013.01)
G06F 3/12 (2017.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
G06F 21/445 (2013.01)
G06F 21/45 (2013.01)
(21) 출원번호 10-2016-0005975
(22) 출원일자 2016년01월18일
심사청구일자 2020년12월14일
(65) 공개번호 10-2017-0086301
(43) 공개일자 2017년07월26일
(56) 선행기술조사문헌
US20060140647 A1*
US20110170146 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
신종훈
경기도 수원시 장안구 정자천로188번길 64, 342동 1306호 (정자동, 두견마을 현대벽산아파트)
(74) 대리인
리앤목특허법인

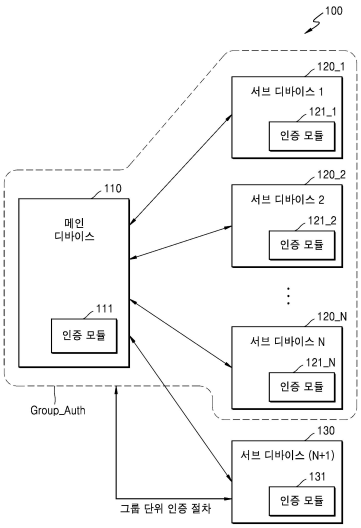
전체 청구항 수 : 총 9 항 심사관 : 문남두

(54) 발명의 명칭 **그룹 단위의 인증을 수행하는 디바이스 시스템 및 그 동작방법**

(57) 요 약

그룹 단위의 인증을 수행하는 디바이스 시스템 및 그 동작방법이 개시된다. 본 발명의 기술적 사상에 따른 다수의 디바이스들을 포함하는 디바이스 시스템의 동작방법은, 새로이 연결되는 제1 디바이스에 대해 제1 인증 절차를 수행하는 단계와, 상기 다수의 디바이스들 중에서 선택된 적어도 두 개의 디바이스들을 포함하는 인증 그룹을 이용하여 상기 제1 디바이스에 대해 그룹 단위의 제2 인증 절차를 수행하는 단계 및 상기 제1 및 제2 인증 절차가 성공함에 따라, 상기 제1 디바이스의 연결을 승인하는 단계를 구비하는 것을 특징으로 한다.

대 표 도 - 도1



(52) CPC특허분류
G06F 3/12 (2018.05)
H04L 9/3271 (2013.01)

명 세 서

청구범위

청구항 1

다수의 디바이스들을 포함하는 디바이스 시스템의 동작방법에 있어서,

새로이 연결되는 제1 디바이스에 대해 제1 인증 절차를 수행하는 단계;

상기 다수의 디바이스들 중에서 선택된 적어도 두 개의 디바이스들을 포함하는 인증 그룹을 이용하여 상기 제1 디바이스에 대해 그룹 단위의 제2 인증 절차를 수행하는 단계; 및

상기 제1 및 제2 인증 절차가 성공함에 따라, 상기 제1 디바이스의 연결을 승인하는 단계를 구비하고,

상기 디바이스 시스템은 프린터 시스템이고,

상기 다수의 디바이스들은 프린터 및 하나 이상의 카트리지들을 포함하며,

상기 인증 그룹은, 상기 하나 이상의 카트리지들 중 적어도 일부와 상기 프린터를 포함하고,

상기 제2 인증 절차는, 상기 인증 그룹에 포함되는 디바이스들로부터의 정보를 조합함에 의해 생성된 고유 정보를 기초로 수행되는 것을 특징으로 하는 디바이스 시스템의 동작방법.

청구항 2

제1항에 있어서,

상기 제1 디바이스는 상기 프린터에 새로이 연결되는 제1 카트리지인 것을 특징으로 하는 디바이스 시스템의 동작방법.

청구항 3

제2항에 있어서,

상기 제1 인증 절차는, 상기 프린터와 상기 제1 카트리지 사이의 1 대 1 챌린지-응답 기반의 인증 절차인 것을 특징으로 하는 디바이스 시스템의 동작방법.

청구항 4

삭제

청구항 5

제2항에 있어서,

상기 하나 이상의 카트리지들은 다수 개의 카트리지들을 포함하며,

상기 인증 그룹은, 상기 다수 개의 카트리지들을 포함하는 것을 특징으로 하는 디바이스 시스템의 동작방법.

청구항 6

제1항에 있어서,

상기 다수의 디바이스들로부터 N 개의 인증 그룹들이 설정되고(단, N은 2 이상의 정수),

상기 제2 인증 절차를 수행하는 단계는, 상기 N 개의 인증 그룹들 각각과 상기 제1 디바이스 사이에서의 인증 절차를 수행하는 것을 특징으로 하는 디바이스 시스템의 동작방법.

청구항 7

제1항에 있어서, 상기 제2 인증 절차를 수행하는 단계는,

상기 인증 그룹에 포함되는 디바이스들 중에서 선택된 인증 엔티티와 상기 제1 디바이스 사이에서의 인증 절차를 수행하는 것을 특징으로 하는 디바이스 시스템의 동작방법.

청구항 8

제1항에 있어서,

상기 인증 그룹에 포함되는 디바이스들의 개수에 따라 조합 가능한 인증 그룹의 개수는 M 가지에 해당하고(단, M은 2 이상의 정수),

상기 제2 인증 절차를 수행하는 단계는, 상기 M 가지의 조합들 중 두 가지 이상의 조합에 따른 인증 그룹들 각각과 상기 제1 디바이스 사이에서의 인증 절차를 수행하는 것을 특징으로 하는 디바이스 시스템의 동작방법.

청구항 9

디바이스의 동작방법에 있어서,

메인 디바이스와의 연결을 감지함에 따라, 상기 메인 디바이스에 대한 인증 절차를 요청하는 단계;

상기 메인 디바이스에 기존에 연결된 하나 이상의 서브 디바이스들을 포함하는 인증 그룹과의 인증 절차 요청을 수신하는 단계; 및

상기 인증 절차 요청의 수신에 응답하여, 상기 인증 그룹과의 인증 절차를 수행하는 단계를 구비하고,

상기 메인 디바이스는 프린터이고,

상기 서브 디바이스들은 하나 이상의 카트리지들을 포함하며,

상기 인증 그룹은, 상기 하나 이상의 카트리지들 중 적어도 일부와 상기 프린터를 포함하고,

상기 인증 그룹과의 인증 절차는, 상기 인증 그룹에 포함되는 상기 프린터 및 상기 카트리지들 중 적어도 일부의 정보를 조합함에 의해 생성된 고유 정보를 기초로 수행되는 것을 특징으로 하는 디바이스의 동작방법.

청구항 10

제9항에 있어서,

상기 메인 디바이스에 대한 인증 절차의 요청에 따라, 상기 메인 디바이스와 1 대 1 챌린지-응답 기반의 인증 절차를 수행하는 단계를 더 구비하는 것을 특징으로 하는 디바이스의 동작방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 기술적 사상은 인증 모듈을 포함하는 디바이스에 관한 것으로서, 상세하게는 그룹 단위의 인증을 수행하는 디바이스 시스템 및 그 동작방법에 관한 것이다.

배 경 기 술

[0002] 물리적 또는 전기적으로 연결되는 디바이스들에 대한 보안을 강화하기 위한 방법으로서 디바이스들 사이의 인증 절차가 수행될 수 있다. 일 예로서, 화상 형성 장치로서 널리 이용되고 있는 프린터 시스템에서, 프린터 본체와 카트리지 사이에서 인증 절차가 수행됨에 따라 카트리지의 정품 여부가 확인될 수 있다. 프린터 본체에 새로운 카트리지의 연결이 감지되면, 프린터 본체에 구비되는 인증 모듈과 새로이 연결되는 카트리지에 구비되는 인증 모듈 사이에서 1 대 1 인증 절차가 수행되고, 인증 절차가 성공되면 카트리지가 프린터 시스템에서 유효하게 이용될 수 있다.

[0003] 그러나, 프린터 본체에 구비되는 인증 모듈이 해킹 등의 이유에 기인하여 보안 기능이 정상적으로 동작하지 않는 경우에는, 불법 카트리지가 무분별하게 이용될 수 있으므로, 프린터 본체 생산 업체에 막대한 피해가 발생될 뿐 아니라, 불법 카트리지가 이용됨에 따라 프린터 본체가 고장나는 등의 문제가 발생될 수 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 기술적 사상이 해결하려는 과제는, 새로이 연결되는 디바이스에 대한 보안을 강화함으로써, 불법 디바이스의 불법적인 연결을 방지할 수 있는 디바이스 시스템의 동작방법을 제공하는 데 있다.

과제의 해결 수단

[0005] 본 발명의 기술적 사상에 따른 다수의 디바이스들을 포함하는 디바이스 시스템의 동작방법은, 새로이 연결되는 제1 디바이스에 대해 제1 인증 절차를 수행하는 단계와, 상기 다수의 디바이스들 중에서 선택된 적어도 두 개의 디바이스들을 포함하는 인증 그룹을 이용하여 상기 제1 디바이스에 대해 그룹 단위의 제2 인증 절차를 수행하는 단계 및 상기 제1 및 제2 인증 절차가 성공함에 따라, 상기 제1 디바이스의 연결을 승인하는 단계를 구비하는 것을 특징으로 한다.

[0006] 일 실시예에 따라, 상기 디바이스 시스템은 프린터 시스템이고, 상기 다수의 디바이스들은 프린터 및 하나 이상의 카트리지들을 포함하며, 상기 제1 디바이스는 상기 프린터에 새로이 연결되는 제1 카트리지인 것을 특징으로 한다.

[0007] 또한, 일 실시예에 따라, 상기 제1 인증 절차는 상기 프린터와 상기 제1 카트리지 사이의 1 대 1 챌린지-응답 기반의 인증 절차인 것을 특징으로 한다.

[0008] 또한, 일 실시예에 따라, 상기 인증 그룹은 상기 하나 이상의 카트리지들 중 적어도 일부와 상기 프린터를 포함하는 것을 특징으로 한다.

[0009] 또한, 일 실시예에 따라, 상기 다수의 디바이스들은 프린터 및 다수 개의 카트리지들을 포함하며, 상기 인증 그룹은 상기 다수 개의 카트리지들을 포함하는 것을 특징으로 한다.

[0010] 한편, 본 발명의 기술적 사상에 따른 디바이스의 동작방법은, 메인 디바이스와의 연결을 감지함에 따라, 상기 메인 디바이스에 대한 인증 절차를 요청하는 단계와, 상기 메인 디바이스에 기존에 연결된 하나 이상의 서브 디바이스들을 포함하는 인증 그룹과의 인증 절차 요청을 수신하는 단계 및 상기 인증 절차 요청의 수신에 응답하여, 상기 인증 그룹과의 인증 절차를 수행하는 단계를 구비하는 것을 특징으로 한다.

[0011] 일 실시예에 따라, 상기 디바이스의 동작방법은, 상기 메인 디바이스에 대한 인증 절차의 요청에 따라 상기 메인 디바이스와 1 대 1 챌린지-응답 기반의 인증 절차를 수행하는 단계를 더 구비하는 것을 특징으로 한다.

발명의 효과

[0012] 본 발명의 기술적 사상의 그룹 단위의 인증을 수행하는 디바이스 시스템 및 그 동작방법에 따르면, 프린터 본체 등의 메인 디바이스의 보안 기능이 정상적으로 동작하지 않더라도, 불법 카트리지 등의 서브 디바이스가 메인 디바이스에 의해 정상적으로 승인되는 것을 방지할 수 있는 효과가 있다.

[0013] 또한, 본 발명의 기술적 사상의 그룹 단위의 인증을 수행하는 디바이스 시스템 및 그 동작방법에 따르면, 추가의 보안 수단이 필요 없이 기존에 구비되는 디바이스들 만을 이용하여 불법 카트리지 등에 대한 보안을 강화할 수 있으므로, 보안에 소요되는 비용 증가를 최소화할 수 있는 효과가 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 실시 예에 따른 디바이스를 포함하는 디바이스 시스템을 나타내는 블록도이다.

도 2는 본 발명의 실시예에 따른 디바이스 시스템이 화상 형성 시스템에 적용되는 예를 나타내는 블록도이다.

도 3은 도 2의 화상 형성 시스템에서 시스템 온 칩과 CRUM들 사이의 연결 관계를 나타내는 블록도이다.

도 4는 본 발명의 일 실시예에 따른 화상 형성 시스템의 동작방법을 나타내는 플로우차트이다.

도 5는 본 발명의 변형 가능한 실시예에 따른 화상 형성 시스템의 동작방법을 나타내는 플로우차트이다.

도 6은 인증 그룹에 대응하는 인증 엔티티에 의해 인증 절차가 수행되는 예를 나타내는 블록도이다.

도 7a,b 내지 도 10a,b,c는 다양한 방식에 따라 인증 그룹을 설정하는 예 및 이에 기반하여 그룹 인증 절차를 수행하는 예를 나타내는 블록도이다.

도 11은 다수 개의 인증 그룹들을 포함하는 화상 형성 시스템의 동작방법을 나타내는 플로우차트이다.

도 12a,b는 본 발명의 변형 가능한 실시예에 따라 인증 그룹을 설정하는 예를 나타내는 블록도이다.

도 13은 본 발명의 실시예에 따른 디바이스를 포함하는 사물 인터넷 시스템을 나타내는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 이하, 첨부한 도면을 참조하여 본 발명의 실시예에 대해 상세히 설명한다. 본 발명의 실시예는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위하여 제공되는 것이다. 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용한다. 첨부된 도면에 있어서, 구조물들의 치수는 본 발명의 명확성을 기하기 위하여 실제보다 확대하거나 축소하여 도시한 것이다.

[0016] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서 상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0017] 또한, 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로 사용될 수 있다. 예를 들어, 본 발명의 권리 범위로부터 벗어나지 않으면서, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.

[0018] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 갖는다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0019] 도 1은 본 발명의 실시 예에 따른 디바이스를 포함하는 디바이스 시스템을 나타내는 블록도이다.

[0020] 도 1을 참조하면, 디바이스 시스템(100)은 다수 개의 디바이스들을 포함할 수 있으며, 예컨대 디바이스 시스템(100)은 메인 디바이스(110)와 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N)을 포함할 수 있다. 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N) 각각은 상기 메인 디바이스(110)에 장착되어 물리적으로 연결되거나, 또는 유선 또는 무선 등의 통신망을 통해 상기 메인 디바이스(110)에 연결될 수 있다. 또한, 메인 디바이스(110)와 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N)은 인증 절차를 통하여 정품으로서 정상적으로 인증된 것으로 가정된다.

[0021] 일 예로서, 메인 디바이스(110)가 프린터 본체 등의 화상 형성 장치에 해당하는 경우에는, 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N) 각각은 카트리지 등의 프린터 본체에 결합 가능한 디바이스일 수 있다. 이외에도, 도 1에 도시된 각각의 디바이스는 인증 절차를 수행할 수 있는 다양한 종류의 전자 장치일 수 있으며, 예컨대 각각의 디바이스는 이동 단말기(mobile device), 스마트 폰(smart phone), PDA(personal digital assistant), PC(personal computer), 태블릿(tablet) PC, 노트북, 넷-북(net-book), 가전 장치 등 다양한 전자 장치가 적용될 수 있다.

[0022] 도 1에서는 프린터 본체가 메인 디바이스(110)에 해당하고, 카트리지가 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N) 각각에 해당하는 것으로 도시되었으나, 본 발명의 실시예에 따르면 각각의 디바이스는 다양한 용어로 정의되어도 무방하다. 예컨대, 메인 디바이스(110)는 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N) 각각에 대해 호스트 및 슬레이브 기능을 함께 수행할 수 있으며, 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N) 각각 또한 메인 디바이스(110)에 대하여 호스트 및 슬레이브 기능을 함께 수행할 수 있다. 즉, 프린터 본체와 카트리지에 대해 메인 및 서브 디바이스로 지칭될 필요 없이 서로 대등한 디바이스로 지칭되어도 무방하다.

[0023] 메인 디바이스(110)와 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N) 각각은 서로 소정의 인증 절차를 통해 상

대 디바이스의 정품 여부를 인증할 수 있다. 예컨대, 메인 디바이스(110)와 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N) 각각은, 1 대 1 챌린지-응답(Challenge-Response) 기반의 인증 절차를 수행할 수 있다. 인증 절차에 이용되는 알고리즘의 일 예로서, AES(Advanced Encryption Standard), DES(Data Encryption Standard) 등의 대칭키 알고리즘에 기반하여 인증 절차가 수행되거나, RSA(Rivest Shamir Adleman), ECC(Elliptic Curve Cryptography) 등의 비대칭키 알고리즘에 기반하여 인증 절차가 수행될 수 있다.

[0024] 한편, 상기와 같은 인증 절차를 위하여, 메인 디바이스(110)는 인증 모듈(111)을 포함할 수 있으며, 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N) 또한 인증 모듈(121_1 ~ 121_N)을 포함할 수 있다. 상기 인증 모듈들(111, 121_1 ~ 121_N) 각각에는 인증 절차에 이용되는 파라미터 등의 각종 정보가 설치되거나, 또는 상기 각종 파라미터 등을 생성하기 위한 정보 생성 모듈(미도시)이 구비될 수 있다. 메인 디바이스(110)와 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N)은 상기 인증 모듈들(111, 121_1 ~ 121_N)을 통해 일 방향 인증 프로토콜이나 상호 인증 프로토콜을 이용하여 인증 절차를 수행할 수 있다.

[0025] 한편, 새로운 디바이스(예컨대, 제N+1 서브 디바이스(130))가 디바이스 시스템(100)에 새로이 연결될 수 있으며, 일 예로서 제N+1 서브 디바이스(130)가 메인 디바이스(110)에 새로이 연결될 수 있다. 본 발명의 일 실시예에 따라, 새로운 디바이스의 연결이 감지되면, 새로이 연결되는 디바이스에 대해 그룹 단위의 인증 절차(또는, 1 대 그룹 인증 절차)가 수행될 수 있다.

[0026] 일 동작 예로서, 메인 디바이스(110)와 제N+1 서브 디바이스(130) 사이에서 상호 인증 절차가 수행될 수 있으며, 이에 따라 메인 디바이스(110)는 제N+1 서브 디바이스(130)로 인증 절차를 요청할 수 있으며, 또한 제N+1 서브 디바이스(130)는 메인 디바이스(110)로 인증 절차를 요청할 수 있다. 이로써, 메인 디바이스(110)와 제N+1 서브 디바이스(130) 사이에서 1 대 1 챌린지-응답 기반의 인증 절차가 먼저 수행될 수 있다. 상기 메인 디바이스(110)와 제N+1 서브 디바이스(130) 사이의 인증 절차가 실패하는 경우, 제N+1 서브 디바이스(130)는 디바이스 시스템(100)에의 연결이 허용되지 않는다.

[0027] 상기 인증 절차가 성공하면, 본 발명의 일 실시예에 따라 제N+1 서브 디바이스(130)에 대한 그룹 단위의 인증 절차가 수행될 수 있다. 예컨대, 디바이스 시스템(100)에 기존에 연결된 디바이스들 중 두 개 이상의 디바이스들이 하나의 인증 그룹(Group_Auth)으로 설정되고, 상기 인증 그룹(Group_Auth)과의 그룹 단위의 인증 절차 요청이 제N+1 서브 디바이스(130)로 제공될 수 있다. 이로써, 상기 인증 그룹(Group_Auth)과 제N+1 서브 디바이스(130) 사이에서 인증 절차가 수행될 수 있다.

[0028] 일 실시예에 따라, 그룹 단위의 인증 절차는, 인증 그룹(Group_Auth)에 포함되는 디바이스들 각각과 제N+1 서브 디바이스(130) 사이에서의 상호 인증 절차에 의해 수행될 수 있다. 예컨대, 제N+1 서브 디바이스(130)는 인증 그룹(Group_Auth)에 포함되는 각각의 디바이스와 1 대 1 챌린지-응답 기반의 인증 절차를 수행할 수 있다.

[0029] 또는, 그룹 단위의 인증 절차를 수행하기 위하여, 상기 인증 그룹(Group_Auth)에 포함되는 디바이스들 사이에서 그룹 연산이 수행되고, 상기 그룹 연산 과정에서 생성되는 정보를 이용하여 제N+1 서브 디바이스(130)에 대한 그룹 단위의 인증 절차가 수행될 수 있다. 일 예로서, 상기 그룹 단위의 인증 절차는 다양한 알고리즘에 따라 수행될 수 있으며, 예컨대 ECC(Elliptic Curve Cryptography) 페어링(pairing) 방식 등의 알고리즘에 따라 상기 인증 그룹(Group_Auth)과 제N+1 서브 디바이스(130) 사이에서 인증 절차가 수행될 수 있다.

[0030] 일 실시예로서, 인증 그룹(Group_Auth)에 포함되는 디바이스들 중 어느 하나의 디바이스가 인증 엔티티(entity)로 선택되고, 제N+1 서브 디바이스(130)와 인증 엔티티(entity) 사이에서 챌린지-응답 기반의 인증 절차가 수행될 수 있다. 전술한 ECC 페어링 알고리즘을 예로 들면, 인증 절차를 위한 알고리즘 과정에서, 인증 그룹(Group_Auth)에 대응하는 고유 정보(예컨대, ID 정보)나 공개키(Public Key) 생성에 관련된 고유 정보(예컨대, 파라미터 값) 등이 생성될 수 있다. 일 실시예에 따라, 그룹 단위의 인증 절차에서, 인증 그룹(Group_Auth)에 포함되는 디바이스들로부터의 정보를 조합함에 의해 상기 인증 그룹(Group_Auth)에 대응하는 고유 정보가 생성되고, 상기 고유 정보에 기반하여 제N+1 서브 디바이스(130)와의 인증 절차가 수행될 수 있다.

[0031] 상기와 같은 그룹 단위의 인증 절차가 성공되면, 메인 디바이스(110)와 제N+1 서브 디바이스(130) 사이의 정상적인 연결이 허용된다. 예컨대, 메인 디바이스(110)와 제N+1 서브 디바이스(130) 사이의 세션(session)이 설정되고, 전술한 메인 디바이스(110)와의 인증 절차나 그룹 단위의 인증 절차에서 생성된 암호화 키를 이용하여 통신이 수행될 수 있다.

[0032] 상기와 같은 그룹 단위의 인증 절차에 따라, 메인 디바이스(110)가 해킹되어 그 내부의 중요 정보가 노출되었더라도, 보안이 유지되고 있는 하나 이상의 다른 디바이스를 포함하는 인증 그룹(Group_Auth)을 기반으로 하여 제

N+1 서브 디바이스(130)에 대한 인증이 수행될 수 있다. 이에 따라, 메인 디바이스(110)가 해킹 등의 원인으로 인해 보안 기능이 정상적으로 동작하지 않더라도, 메인 디바이스(110)에 의해 불법 디바이스가 잘못 승인 처리되는 문제가 개선될 수 있다.

[0033] 한편, 도 1에 도시된 실시예에서, 디바이스 시스템(100)에 기존에 연결된 제1 내지 제N 서브 디바이스들(120_1 ~ 120_N) 또한 전술한 그룹 단위의 승인 절차를 통해 승인이 완료된 디바이스일 수 있다. 예컨대, 제N 서브 디바이스(120_N)가 새로이 메인 디바이스(110)에 연결되는 경우, 기존의 서브 디바이스들(예컨대, 제1 내지 제(N-1) 서브 디바이스들(120_1 ~ 120_(N-1))을 포함하는 인증 그룹(Group_Auth)이 설정되고, 제N 서브 디바이스(120_N)에 대해 전술한 실시예에 따른 그룹 단위의 인증 절차가 수행될 수 있다.

[0034] 또한, 도 1에 도시된 실시예에서는 기존에 디바이스 시스템(100)에 연결된 디바이스들 전체가 하나의 인증 그룹(Group_Auth)으로 설정되는 예가 도시되었으나, 본 발명의 실시예들은 이에 국한될 필요가 없다. 일 예로서, 기존에 디바이스 시스템(100)에 연결된 디바이스들 중 특정한 일부의 디바이스들이 인증 그룹(Group_Auth)으로 설정되거나, 또는 기존에 디바이스 시스템(100)에 연결된 디바이스들 중 임의의 디바이스들이 인증 그룹(Group_Auth)으로 설정될 수 있다. 또는, 기존에 디바이스 시스템(100)에 연결된 디바이스들은 적어도 두 개의 인증 그룹(Group_Auth)들로 설정될 수 있으며, 인증 그룹(Group_Auth)들 각각이 새로이 연결되는 제N+1 서브 디바이스(130)에 대해 그룹 단위의 인증 절차를 수행할 수도 있다.

[0035] 전술한 실시예에 따르면, 메인 디바이스(110)의 보안 기능이 정상적으로 동작하지 않음에 따라 무분별하게 불법 디바이스들에 대해 인증이 성공하는 문제가 방지될 수 있다. 또한, 불법 디바이스에 대한 인증을 방지하기 위한 다른 수단이 추가로 구비될 필요 없이, 디바이스 시스템(100)에 기존에 연결된 디바이스들만을 이용하여 불법 디바이스의 인증이 방지될 수 있으므로, 보안 시스템에 구현되는 비용 증가를 최소화할 수 있다.

[0036] 도 2는 본 발명의 실시예에 따른 디바이스 시스템이 화상 형성 시스템에 적용되는 예를 나타내는 블록도이다.

[0037] 도 2를 참조하면, 화상 형성 시스템(200)은 화상 형성 장치로서 프린터 본체(210)를 포함할 수 있으며, 또한 프린터 본체(210)에 연결 가능한 디바이스로서 다수 개의 카트리지들(220_1 ~ 220_5)을 포함할 수 있다. 이하의 설명에서, 프린터 본체(210)는 프린터로 지칭될 것이다.

[0038] 일 예로서, 프린터(210)는 카트리지들을 통해 다양한 색상의 화상을 형성할 수 있으며, 예컨대 색상 종류에 따라 카트리지들(220_1 ~ 220_5)은 블랙 카트리지 및 R,G,B 카트리지들을 포함할 수 있다. 또한, 카트리지들(220_1 ~ 220_5)은 그 구조에 따라 다양한 종류의 카트리지들을 포함할 수 있으며, 예컨대 드럼과 토너가 일체형으로 형성되는 드럼 카트리지를 포함할 수 있다. 이하의 설명에서는, 제1 내지 제5 카트리지들(220_1 ~ 220_5)이 화상 형성 시스템(200)에 포함되는 것으로 가정되나, 다른 개수의 카트리지들이 화상 형성 시스템(200)에 포함되어도 무방하다. 또한, 화상 형성 시스템(200)에 기존에 연결된 제2 내지 제5 카트리지들(220_2 ~ 220_5) 중 적어도 일부는 본 발명의 실시예에 따른 인증 절차(예컨대, 그룹 단위의 인증 절차)를 통해 정품으로 인증된 카트리지에 해당할 수 있다. 이하에서는, 제1 카트리지(220_1)가 화상 형성 시스템(200)에 새로이 연결되는 경우가 가정된다.

[0039] 프린터(210)와 카트리지들(220_1 ~ 220_5) 각각은 인증 동작을 수행하기 위한 인증 모듈을 포함할 수 있다. 예컨대, 프린터(210)는 그 내부에 인증 모듈을 포함하는 반도체 칩으로서 시스템 온 칩(System on Chip, 211)을 포함할 수 있다.

[0040] 한편, 카트리지들(220_1 ~ 220_5) 각각은 보안 집적 회로(Security IC)를 포함하는 CRUM을 포함할 수 있다. 상기 CRUM은 Customer Replaceable Unit Monitor 또는 Customer Replaceable Unit Memory 로 정의될 수 있다. CRUM에 적용되는 보안 IC는 높은 수준의 보안성을 요구하며, 이에 따라 카트리지에 적용되는 보안 IC에 대한 해킹이 어렵도록 함으로써 불법 카트리지가 이용되는 것이 방지되도록 한다.

[0041] 보안 IC는 인증 절차와 관련된 중요 정보를 안전하게 저장하며, 일 실시예에 따라 보안 IC의 제조 공정 과정에서, Hardware Security Module(HSM)을 통하여 인증 절차에 이용되는 고유 정보가 인스톨될 수 있다. 일 실시예에 따라, 그룹 단위의 인증 절차에 이용되는 고유 정보가 보안 IC에 인스톨될 수 있다. 또한, 보안 IC는 사이드 채널 공격(Side Channel Attack)을 방어하기 위한 하드웨어적 수단을 포함할 수 있다.

[0042] 반면에, 프린터(210)는 그 제조 단가를 낮추기 위하여 상대적으로 낮은 보안성을 갖는 수단을 통해 인증 절차를 수행하도록 인증 모듈이 구현될 수 있다. 일 예로서, 프린터(210)는 전술한 보안 IC에서 지원하는 높은 수준의 보안성을 제공하지 않으며, 이에 따라 프린터(210)의 시스템 온 칩(211)에 대한 해킹을 통해 인증 동작에 이용되는 각종 정보들이 외부로 노출될 수 있다. 프린터(210)가 해킹되면, 이후 불법 카트리지가 프린터(210)에 연

결될 때, 불법 카트리지에 대한 인증 절차가 성공한 것으로 잘못 판단될 수 있다.

[0043] 화상 형성 시스템(200)에 기존에 연결된 디바이스들 중 적어도 일부가 하나의 인증 그룹(Group_Auth)으로 설정될 수 있으며, 일 예로서 프린터(210)와 제2 내지 제5 카트리지들(220_2 ~ 220_5)이 하나의 인증 그룹(Group_Auth)으로 설정될 수 있다. 제1 카트리지(220_1)가 화상 형성 시스템(200)에 새로이 연결됨이 감지되면, 인증 그룹(Group_Auth)과 제1 카트리지(220_1) 사이에서 인증 절차가 수행될 수 있다.

[0044] 일 실시예에 따라, 프린터(210)와 제1 카트리지(220_1) 사이에서 1 대 1 챌린지-응답 방식 등의 인증 절차가 먼저 수행될 수 있다. 또는, 변형 가능한 실시예로서, 프린터(210)와 제1 카트리지(220_1) 사이의 인증 절차는 생략되고, 전술한 인증 그룹(Group_Auth)과 제1 카트리지(220_1) 사이에서 인증 절차가 수행될 수도 있다.

[0045] 프린터(210)와 제1 카트리지(220_1) 사이의 인증 절차에서, 프린터(210)의 시스템 온 칩(211)과 제1 카트리지(220_1)의 CRUM(221_1)에 구비되는 보안 IC는 각각 인증 절차를 수행하고, 프린터(210)는 제1 카트리지(220_1)를 정상 디바이스로서 인증함과 함께, 제1 카트리지(220_1)는 프린터(210)를 정상 디바이스로서 인증할 수 있다. 프린터(210)와 제1 카트리지(220_1) 사이에서 상호 인증 절차가 성공되면, 제1 카트리지(220_1)에 대해 그룹 단위의 인증 절차가 수행될 수 있다.

[0046] 그룹 단위의 인증 절차에 있어서, 제1 카트리지(220_1)는 인증 그룹(Group_Auth)에 포함되는 디바이스들 각각에 대해 인증 절차를 수행하는 방식에 따라 그룹 단위의 인증 절차가 수행될 수 있다.

[0047] 또는, 인증 그룹(Group_Auth)에 포함되는 디바이스들 중 어느 하나가 인증 엔티티(entity)로 선택되고, 제1 카트리지(220_1)와 인증 엔티티(entity) 사이에서 인증 절차가 수행될 수 있다. 상기 인증 엔티티(entity)는 인증 그룹(Group_Auth)에 포함된 적어도 두 개의 디바이스들의 정보의 조합에 기반하여 인증 그룹(Group_Auth)에 대응하는 고유 정보를 생성하고, 상기 생성된 고유 정보에 기반하여 제1 카트리지(220_1)와 인증 절차를 수행할 수 있다. 일 예로서, 상기 인증 엔티티(entity)와 제1 카트리지(220_1) 사이에서 챌린지-응답(예컨대, 1 대 그룹 챌린지-응답) 기반의 인증 절차가 수행될 수 있다.

[0048] 전술한 예에 따라, 제1 카트리지(220_1)와 프린터(210)와의 1 대 1 챌린지-응답 기반의 인증 절차가 성공되고, 또한 제1 카트리지(220_1)와 인증 그룹(Group_Auth) 사이의 1 대 그룹 챌린지-응답 기반의 인증 절차가 성공되면, 제1 카트리지(220_1)가 프린터(210)에 정상적으로 연결되어 동작할 수 있다. 반면에, 어느 하나의 인증 절차가 실패하면 상기 제1 카트리지(220_1)는 불법 카트리지로 판단되어 프린터(210)에 정상적으로 연결되지 않는다.

[0049] 도 3은 도 2의 화상 형성 시스템(200)에서 시스템 온 칩(211)과 CRUM들 사이의 연결 관계를 나타내는 블록도이다.

[0050] 도 2 및 도 3을 참조하면, 제1 카트리지(220_1)가 화상 형성 시스템(200)에 새로이 연결되는 경우, 제1 카트리지(220_1)의 CRUM(CRUM 1)은 하나 이상의 배선을 통해 프린터(210)의 시스템 온 칩(211)에 연결된다. 또한, CRUM(CRUM 1)은 상기 배선을 통해 화상 형성 시스템(200)에 구비되는 기존에 연결된 카트리지들의 CRUM들과 전기적으로 연결될 수 있다. 예컨대, 제1 카트리지(220_1)의 CRUM(CRUM 1)은 제2 내지 제5 카트리지들(220_2 ~ 220_5)의 CRUM들(CRUM 2 ~ CRUM 5)과 전기적으로 연결될 수 있다.

[0051] 상기와 같은 연결 관계에 따라, 화상 형성 시스템(200)에서 다수의 디바이스들이 하나의 인증 그룹(Group_Auth)으로 설정되고, 인증 그룹(Group_Auth) 내의 어느 하나의 디바이스가 인증 엔티티(entity)로 선택되어 새로이 연결되는 제1 카트리지(220_1)와의 사이에서 인증 절차가 수행될 수 있다.

[0052] 도 4는 본 발명의 일 실시예에 따른 화상 형성 시스템의 동작방법을 나타내는 플로우차트이다.

[0053] 도 4를 참조하면, 새로운 카트리지가 화상 형성 시스템(또는, 프린터)에 연결됨에 따라, 새로운 카트리지의 연결이 감지된다(S11). 카트리지의 새 연결이 감지되면 프린터와 새로운 카트리지 사이의 1 대 1 인증 절차가 수행될 수 있으며, 예컨대 프린터와 새로운 카트리지 사이에서 1 대 1 챌린지-응답 기반의 제1 인증 절차가 수행될 수 있다(S12).

[0054] 상기 제1 인증 절차에 따라 인증이 성공하였는지 여부가 판단되고(S13), 판단 결과 인증이 실패된 것으로 판단되면 새로운 카트리지의 정상적인 연결이 차단된다(S14). 반면에, 인증이 성공한 경우에는, 화상 형성 시스템에서 기존에 연결된 두 개 이상의 디바이스들이 하나의 인증 그룹으로 설정된다(S15).

[0055] 상기 설정된 인증 그룹과 새로운 카트리지 사이에서 그룹 단위의 인증 절차가 수행될 수 있으며, 예컨대 1 대

그룹(Group) 챌린지-응답 기반의 인증 절차가 수행될 수 있다(S16). 일 실시예에 따라, 새로운 카트리지와 인증 그룹에 포함되는 각각의 디바이스 사이에서 챌린지-응답 기반의 인증 절차가 수행될 수 있다. 또는, 인증 그룹에 대해 인증 엔티티(entity)가 선택되고, 상기 선택된 인증 엔티티(entity)는 인증 그룹에 대응하는 고유 정보를 이용하여 새로운 카트리지 사이와 인증 절차를 수행할 수 있다.

[0056] 상기와 같은 그룹 단위의 제2 인증 절차가 성공하였는지 여부가 판단되고(S17), 인증이 실패된 것으로 판단되면 새로운 카트리지의 정상적인 연결이 차단된다(S14). 반면에, 인증 절차가 성공한 경우에는, 상기 새로운 카트리지에 대한 인증 절차가 최종 성공한 것으로 판단되고, 이에 따라 새로운 카트리지의 프린터에 대해 정상적으로 연결을 승인한다(S18).

[0057] 도 5는 본 발명의 변형 가능한 실시예에 따른 화상 형성 시스템의 동작방법을 나타내는 플로우차트이다. 도 5에서는 새로운 카트리지와 프린터와의 1 대 1 챌린지-응답 인증 절차 없이 그룹 단위의 인증만으로서 새로운 카트리지에 대한 인증 절차가 수행되는 예가 도시된다.

[0058] 도 5를 참조하면, 새로운 카트리지가 화상 형성 시스템(또는, 프린터)에 연결됨에 따라, 새로운 카트리지의 연결이 감지된다(S21). 상기 새로운 카트리지의 연결이 감지되면, 화상 형성 시스템에서 기존에 연결된 두 개 이상의 디바이스들에 대해 하나 이상의 인증 그룹들을 설정하는 동작이 수행된다(S22). 예컨대, 새로운 카트리지와의 그룹 단위의 인증 절차가 수행될 두 개 이상의 인증 그룹들이 설정될 수 있다. 일 예로서, 화상 형성 시스템에서 기존에 연결된 디바이스들 중 일부는 제1 인증 그룹으로 설정되고, 다른 일부의 디바이스들은 제2 인증 그룹으로 설정될 수 있다. 본 발명의 실시예들은 이외에도 다양하게 변형이 가능하며, 예컨대, 3 개 이상의 인증 그룹들이 설정되어도 무방하다.

[0059] 상기 설정된 하나 이상의 인증 그룹들 각각에 대해 새로운 카트리지와의 사이에서 그룹 단위의 인증 절차가 수행된다(S23). 그룹 단위의 인증 절차가 다수 회 수행되는 경우, 그룹 단위의 인증 절차가 모두 성공하였는지가 판단되고(S24), 적어도 하나의 인증 절차가 실패된 것으로 판단되면 새로운 카트리지의 정상적인 연결이 차단된다(S26). 반면에, 그룹 단위의 인증 절차가 모두 성공한 경우에는, 상기 새로운 카트리지에 대한 인증 절차가 최종 성공한 것으로 판단되고, 이에 따라 새로운 카트리지의 프린터에 대해 정상적으로 연결을 승인한다(S25).

[0060] 도 6은 인증 그룹에 대응하는 인증 엔티티(entity)에 의해 인증 절차가 수행되는 예를 나타내는 블록도이다.

[0061] 도 6을 참조하면, 하나 이상의 디바이스를 포함하는 인증 그룹(Group_Auth)이 설정될 수 있으며, 일 예로서 인증 그룹(Group_Auth)은 프린터와 제1 및 제2 카트리지들을 포함할 수 있다. 인증 그룹(Group_Auth)에 대응하여 인증 엔티티(entity)가 선택되고, 인증 그룹(Group_Auth) 내의 그룹 연산에 기반하여, 그룹 단위의 인증 절차에 이용되는 정보(예컨대, 조합 ID 정보나 조합 파라미터 정보)가 생성될 수 있다.

[0062] 프린터 및 카트리지의 제조 과정에서, 상기와 같은 그룹 기반의 인증 절차에 이용되는 고유 정보가 인스톨될 수 있다. 예컨대, 새로운 카트리지는 그 내부의 보안 IC에 저장된 고유 정보 및 인증 그룹(Group_Auth)으로부터의 조합 정보를 이용한 연산을 통해 인증 그룹(Group_Auth)에 대한 인증을 수행할 수 있다. 또한, 새로운 카트리지로부터의 고유 정보가 인증 그룹(Group_Auth)으로 제공되고, 인증 그룹(Group_Auth)은 새로운 카트리지로부터의 고유 정보와 내부에서 생성된 조합 정보를 이용한 연산을 통해 새로운 카트리지에 대한 인증을 수행할 수 있다.

[0063] 도 7a,b 내지 도 10a,b,c는 다양한 방식에 따라 인증 그룹을 설정하는 예 및 이에 기반하여 그룹 인증 절차를 수행하는 예를 나타내는 블록도이다. 또한, 도 7a,b 내지 도 10a,b,c에서는 디바이스 시스템으로서 프린터 및 다수의 카트리지들을 포함하는 화상 형성 시스템이 도시된다.

[0064] 도 7a를 참조하면, 화상 형성 시스템(300A)은 화상 형성 장치로서 프린터(310A)를 포함할 수 있으며, 또한 프린터(310A)에 연결 가능한 장치로서 제1 내지 제N 카트리지들(320A_1 ~ 320A_N)을 포함할 수 있다. 이후, 추가의 카트리지로서 제(N+1) 카트리지(330A)가 프린터(310A)에 더 연결될 수 있다.

[0065] 도 7a의 실시예에서는, 화상 형성 시스템(300A)에서 기존에 연결된 모든 디바이스들로서 프린터(310A)와 제1 내지 제N 카트리지들(320A_1 ~ 320A_N)이 하나의 인증 그룹(Group_Auth)으로 설정되는 예가 도시된다. 일 실시예에 따라, 새로이 연결되는 제(N+1) 카트리지(330A)와 프린터(310A) 사이에서 1 대 1 챌린지-응답 기반의 제1 인증 절차가 먼저 수행되고, 제1 인증 절차가 성공하면 인증 그룹(Group_Auth)과 제(N+1) 카트리지(330A) 사이에서의 그룹 단위의 제2 인증 절차가 수행될 수 있다. 일 실시예에 따라, 인증 그룹(Group_Auth)에 포함되는 각각의 디바이스와 제(N+1) 카트리지(330A) 사이에서 인증 절차가 수행되거나, 또는 인증 그룹(Group_Auth)에 대응하는 인증 엔티티(entity)와 제(N+1) 카트리지(330A)와의 사이에서 인증 절차가 수행될 수 있다. 제2 인증 절차

가 성공되면, 제(N+1) 카트리지(330A)에 대한 정상적인 연결이 허용될 수 있다.

[0066] 한편, 도 7b를 참조하면, 화상 형성 시스템(300B)은 화상 형성 장치로서 프린터(310B)와 이에 연결 가능한 장치로서 제1 내지 제N 카트리지들(320B_1 ~ 320B_N)을 포함할 수 있다. 이후, 추가의 카트리지로서 제(N+1) 카트리지(330B)가 프린터(310B)에 더 연결될 수 있다.

[0067] 도 7b의 실시예에서는, 화상 형성 시스템(300B)에서 프린터 본체를 제외한 나머지 디바이스들이 하나의 인증 그룹(Group_Auth)으로 설정되는 예가 도시된다. 예컨대, 새로이 연결되는 제(N+1) 카트리지(330B)와 프린터(310B) 사이에서 1 대 1 챌린지-응답 기반의 제1 인증 절차가 수행되고, 이후 제(N+1) 카트리지(330B)와 인증 그룹(Group_Auth) 사이에서 그룹 단위의 제2 인증 절차가 수행될 수 있다. 인증 그룹(Group_Auth)을 설정하는 일 예로서, 프린터(310B)를 포함함이 없이 인증 그룹(Group_Auth)이 설정될 수 있으며, 예컨대 제1 내지 제N 카트리지들(320B_1 ~ 320B_N)이 하나의 인증 그룹(Group_Auth)으로 될 수 있다. 일 실시예에 따라, 상기 인증 그룹(Group_Auth)에 대응하는 인증 엔티티(entity)와 제(N+1) 카트리지(330B) 사이에서 1 대 그룹 챌린지-응답 기반의 인증 절차가 수행될 수 있다.

[0068] 한편, 도 8a은 화상 형성 시스템에 포함되는 디바이스들 중 일부의 디바이스들만이 인증 그룹(Group_Auth)으로 설정되는 예가 도시된다.

[0069] 도 8a를 참조하면, 화상 형성 시스템(400A)은 화상 형성 장치로서 프린터(410A)를 포함할 수 있으며, 또한 제1 내지 제N 카트리지들(420A_1 ~ 420A_N)은 프린터(410A)에 정상적으로 연결된 상태를 갖는다. 이후, 추가의 카트리지로서 제(N+1) 카트리지(430A)가 프린터(410A)에 더 연결될 수 있다.

[0070] 새로이 연결되는 제(N+1) 카트리지(430A)와 프린터(410A) 사이에서 1 대 1 챌린지-응답 기반의 제1 인증 절차가 수행될 수 있으며, 또한 일부의 디바이스들을 포함하는 인증 그룹(Group_Auth)과 새로이 연결되는 제(N+1) 카트리지(430A) 사이에서 그룹 단위의 제2 인증 절차가 수행될 수 있다. 인증 그룹(Group_Auth)의 일 예로서, 프린터(410A)와 제1 및 제2 카트리지들(420A_1, 420A_2)이 하나의 인증 그룹(Group_Auth)으로 설정될 수 있다. 그러나, 이는 일 실시예에 불과한 것으로서, 화상 형성 시스템(400A) 내에서 하나의 인증 그룹(Group_Auth)은 다양하게 설정될 수 있으며, 예컨대 특정한 디바이스들이 인증 그룹(Group_Auth)으로 설정되거나, 다양한 개수의 디바이스들이 임의적으로 하나의 인증 그룹(Group_Auth)으로 설정되어도 무방하다.

[0071] 한편, 도 8b를 참조하면, 화상 형성 시스템(400B)에서 그룹 단위의 인증 동작을 수행할 인증 그룹(Group_Auth)은 다양한 방식에 따라 설정될 수 있으며, 예컨대 인증 그룹(Group_Auth)은 프린터(410B) 없이 카트리지만으로 구성될 수도 있다.

[0072] 예컨대, 새로운 카트리지로서 제(N+1) 카트리지(430B)가 프린터(410B)에 연결됨에 따라, 기존에 연결된 제1 내지 제N 카트리지들(420B_1 ~ 420B_N) 중 일부가 인증 그룹(Group_Auth)으로 설정될 수 있다. 예컨대, 제1 및 제2 카트리지들(420B_1, 420B_2)이 인증 그룹(Group_Auth)으로 설정됨에 따라, 제 인증 그룹(Group_Auth)에 대응하는 인증 엔티티(entity)와 제(N+1) 카트리지(430B) 사이에서 그룹 단위의 인증 절차가 수행될 수 있다. 또한, 전술한 실시예에 따라, 제(N+1) 카트리지(430B)와 프린터(410B) 사이의 1 대 1 챌린지-응답 기반의 인증 절차와, 인증 그룹(Group_Auth) 내에서의 그룹 연산이 더 수행되어도 무방하다.

[0073] 한편, 도 9는 설정 가능한 인증 그룹(Group_Auth)의 종류를 나타내는 블록도이다.

[0074] 도 9를 참조하면, 화상 형성 시스템(500)은 기존에 연결되는 프린터와 다수 개의 카트리지들을 포함할 수 있다. 예컨대, 화상 형성 시스템(500)은 프린터(510)와 제1 내지 제N 카트리지들(520_1 ~ 520_N)을 포함할 수 있다. 또한, 제(N+1) 카트리지(530)가 새로이 연결됨에 따라, 상기 제(N+1) 카트리지(530)와 인증 그룹(Group_Auth) 사이에서 그룹 단위의 인증 절차가 수행될 수 있다. 또한, 일 예로서, 도 9에서는 인증 그룹(Group_Auth)을 설정함에 있어서, 프린터(510)가 기본적으로 인증 그룹(Group_Auth)에 포함되는 예가 도시된다. 프린터(510)는 인증 절차를 수행하는 시스템 온 칩을 포함할 수 있으며, 또한 제1 내지 제(N+1) 카트리지들(520_1 ~ 520_N, 530) 각각은 인증 절차를 수행하는 보안 IC를 포함할 수 있다.

[0075] 전술한 실시예에서와 같이, 화상 형성 시스템(500)에 있어서 인증 그룹(Group_Auth)은 다양한 개수의 디바이스들이 임의적으로 선택됨에 따라 설정될 수 있다. 예컨대, 기존에 N 개의 카트리지들이 화상 형성 시스템(500)에 포함되는 경우, 최소 하나의 카트리지에서 최대 N 개의 카트리지들이 인증 그룹(Group_Auth)에 포함될 수 있다. N 개의 카트리지들이 기존에 포함되는 것으로 가정할 때, 조합 가능한 인증 그룹(Group_Auth)의 개수는 (N-1)!에 해당하는 값을 가질 수 있다.

[0076] 본 발명의 일 실시예에 따라, 상기 조합 가능한 (N-1)! 개의 인증 그룹(Group_Auth)들 중에서 선택된 하나 이상의 인증 그룹(Group_Auth)을 이용하여 그룹 단위의 인증 절차가 수행될 수 있다. 즉, 하나의 디바이스에 대해 복수 회의 그룹 단위의 인증 절차가 수행되는 경우, 상기와 같은 조합 가능한 인증 그룹(Group_Auth)들 중 적어도 두 개의 인증 그룹(Group_Auth)을 이용하여 그룹 단위의 인증 절차가 수행될 수 있다.

[0077] 예컨대, 제1 조합에 따라 프린터(510)와 제1 카트리지(520_1)가 인증 그룹(Group_Auth)으로 설정되고, 제(N+1) 카트리지(530)와 제1 조합에 따른 인증 그룹(Group_Auth) 사이에서 인증 절차(예컨대, 챌린지-응답 기반의 인증 절차)가 수행될 수 있다. 이후, 제2 조합에 따라 프린터(510)와 일부의 카트리지가 인증 그룹(Group_Auth)으로 설정되고, 제(N+1) 카트리지(530)와 제2 조합에 따른 인증 그룹(Group_Auth) 사이에서 인증 절차가 수행될 수 있다.

[0078] 한편, 도 10a,b,c는 화상 형성 시스템에서 다수 개의 인증 그룹들(Group_Auth)이 설정되는 예를 나타낸다.

[0079] 도 10a를 참조하면, 화상 형성 시스템(600A)은 화상 형성 장치로서 프린터(610A)를 포함할 수 있으며, 또한 프린터(610A)에 연결 가능한 장치로서 제1 내지 제N 카트리지들(620A_1 ~ 620A_N)을 포함할 수 있다. 이후, 추가의 카트리지로서 제(N+1) 카트리지(630A)가 프린터(610A)에 더 연결되는 예가 도시된다.

[0080] 일 예로서, 화상 형성 시스템(600A)에 기존에 연결된 디바이스들에 대해, 프린터(610A) 및 일부의 카트리지들(예컨대, 제1 및 제2 카트리지들(620A_1, 620A_2))이 제1 인증 그룹(Group_Auth1)으로 설정되고, 나머지 카트리지들(예컨대, 제3 내지 제N 카트리지들(620A_3 ~ 620A_N))이 제2 인증 그룹(Group_Auth2)으로 설정될 수 있다. 상기와 같이 인증 그룹들(Group_Auth)이 설정됨에 따라, 제(N+1) 카트리지(630A)가 새로이 연결되면, 제(N+1) 카트리지(630A)와 제1 인증 그룹(Group_Auth1) 사이에서 그룹 단위의 챌린지-응답 기반의 인증 절차가 수행됨과 함께, 제(N+1) 카트리지(630A)와 제2 인증 그룹(Group_Auth2) 사이에서 그룹 단위의 챌린지-응답 기반의 인증 절차가 수행될 수 있다.

[0081] 한편, 도 10b는 화상 형성 시스템(600B)에 기존에 연결된 디바이스들 중 일부의 디바이스들만이 인증 그룹으로 설정되고, 또한 화상 형성 시스템(600B)에 두 개 이상의 인증 그룹들(Group_Auth)이 설정되는 예를 나타낸다.

[0082] 도 10b를 참조하면, 화상 형성 시스템(600B)에 기존에 연결된 디바이스들 중 일부의 디바이스들이 두 개의 인증 그룹들(Group_Auth)로 설정될 수 있으며, 예컨대 프린터(610B) 및 일부의 카트리지들(예컨대, 제1 및 제2 카트리지들(620B_1, 620B_2))이 제1 인증 그룹(Group_Auth1)으로 설정되고, 나머지 카트리지들 중 일부(예컨대, 제(A+1) 내지 제N 카트리지들(620B_(A+1), 620B_N))이 제2 인증 그룹(Group_Auth2)으로 설정될 수 있다. 전술한 바와 유사하게, 제(N+1) 카트리지(630B)가 새로이 연결되면, 제(N+1) 카트리지(630B)와 제1 인증 그룹(Group_Auth1) 사이에서 그룹 단위의 챌린지-응답 기반의 인증 절차가 수행됨과 함께, 제(N+1) 카트리지(630B)와 제2 인증 그룹(Group_Auth2) 사이에서 그룹 단위의 챌린지-응답 기반의 인증 절차가 수행될 수 있다.

[0083] 한편, 도 10c에서는 화상 형성 시스템(600C)에 다수 개의 인증 그룹들(Group_Auth)이 설정되는 예가 도시된다.

[0084] 도 10c를 참조하면, 화상 형성 시스템(600C)에 기존에 연결된 디바이스들이 M 개의 인증 그룹들(Group_Auth1 ~ Group_AuthM)로 설정될 수 있다. 또는, 화상 형성 시스템(600C)에 기존에 연결된 디바이스들 중 일부의 디바이스들이 M 개의 인증 그룹들(Group_Auth1 ~ Group_AuthM)로 설정될 수 있다. 전술한 바와 유사하게, 제(N+1) 카트리지(630C)가 새로이 연결되면, M 개의 인증 그룹들(Group_Auth1 ~ Group_AuthM) 각각과 새로이 연결된 제(N+1) 카트리지(630B) 사이에서 그룹 단위의 챌린지-응답 기반의 인증 절차가 수행될 수 있다.

[0085] 도 11은 다수 개의 인증 그룹들을 포함하는 화상 형성 시스템의 동작방법을 나타내는 플로우차트이다.

[0086] 전술한 실시예에서와 같이, 화상 형성 시스템에서 다수 개의 인증 그룹들이 설정될 수 있으며, 일 예로서 일부의 디바이스들이 어느 하나의 인증 그룹으로 설정되고, 다른 일부의 디바이스들이 다른 인증 그룹으로 설정될 수 있다. 또는, 전술한 실시예에서와 같이 디바이스들의 개수에 따라 인증 그룹들의 다양한 조합들이 발생될 수 있으며, 이들 조합들 중 두 개 이상의 조합의 인증 그룹에 따라 그룹 단위의 인증 절차가 수행될 수 있다.

[0087] 도 11을 참조하면, 새로운 카트리지가 화상 형성 시스템(또는, 프린터)에 연결됨에 따라 새로운 카트리지에 대해 그룹 단위의 인증 절차가 수행된다. 예컨대, 화상 형성 시스템에 기존에 연결된 디바이스들에 따라 다수 개의 인증 그룹들이 설정될 수 있으며, 새로운 카트리지와 제1 인증 그룹 사이에서 인증 절차가 수행될 수 있다(S31).

[0088] 그룹 단위의 인증이 성공하였는지가 판단되고(S32), 인증이 실패된 것으로 판단되면 새로운 카트리지의 정상적인 연결이 차단된다(S33). 반면에, 인증이 성공한 것으로 판단되면, 새로운 카트리지와 다른 인증 그룹 사이에

서 그룹 단위의 상호 인증 절차를 수행하는 단계와, 이에 대해 인증이 성공하였는지 여부를 판단하는 단계가 반복하게 수행된다. 마지막 인증 그룹으로서, 제M 인증 그룹과 새로운 카트리지 사이에서 그룹 단위의 상호 인증 절차가 수행되고(S34), 제M 인증 그룹에 의한 인증이 성공하였는지가 판단된다(S35). 제M 인증 그룹에 의한 인증이 성공하는 경우, 상기 새로운 카트리지에 대한 인증 절차가 최종 성공한 것으로 판단되고, 이에 따라 새로운 카트리지에 대해 정상적으로 연결을 승인한다(S36).

[0089] 도 12a,b는 본 발명의 변형 가능한 실시예에 따라 인증 그룹을 설정하는 예를 나타내는 블록도이다. 도 12a,b에서는 새로이 연결되는 디바이스가 인증 그룹에 포함되는 예가 설명된다.

[0090] 도 12a를 참조하면, 화상 형성 시스템(700A)에서 프린터(710A)와 제1 내지 제N 카트리지들(720A_1 ~ 720A_N)은 기존에 연결된 상태를 가지고, 추가의 카트리지로서 제(N+1) 카트리지(730A)가 프린터(710A)에 더 연결될 수 있다. 일 실시예에 따라, 프린터(710A)와 제(N+1) 카트리지(730A) 사이에서 1 대 1 챌린지-응답 기반의 인증 절차가 먼저 수행될 수 있다.

[0091] 또한, 본 발명의 실시예에 따라, 새로 연결되는 제(N+1) 카트리지(730A)가 인증 그룹(Group_Auth)에 포함될 수 있으며, 화상 형성 시스템(700A)에서 어느 하나의 카트리지와 상기 인증 그룹(Group_Auth) 사이에서 그룹 단위의 인증 절차가 수행될 수 있다. 도 12a에서는 제1 카트리지(720A_1)를 제외한 나머지 모든 카트리지들(720A_2 ~ 720A_N, 730)이 하나의 인증 그룹(Group_Auth)으로 설정되는 예가 도시되었으나, 본 발명의 실시예는 이에 국한될 필요가 없다. 변형 가능한 실시예로서, 상기 인증 그룹(Group_Auth)은 제(N+1) 카트리지(730A)와 함께, 일부의 다른 카트리지만을 포함하여도 무방하다.

[0092] 제1 카트리지(720A_1)와 인증 그룹(Group_Auth) 사이에서 그룹 기반의 인증 절차가 수행될 수 있다. 전술한 실시예들에 따라 다양한 방식으로서 그룹 기반의 인증 절차가 수행될 수 있으며, 이 때 제(N+1) 카트리지(730A)가 불법 카트리지에 해당하더라도, 정상적으로 보안 기능을 수행하는 다른 정품 카트리지에 의해 그룹 기반의 인증 절차가 실패한 것으로 판단될 수 있다.

[0093] 한편, 도 12b는 새로 연결되는 제(N+1) 카트리지(730A)가 인증 그룹(Group_Auth)에 포함되고, 프린터(710B)와 인증 그룹(Group_Auth) 사이에서 그룹 단위의 인증 절차가 수행되는 예를 나타낸다. 일 실시예에 따라, 프린터(710B)와 제(N+1) 카트리지(730B) 사이에서 1 대 1 챌린지-응답 기반의 인증 절차가 먼저 수행될 수 있다.

[0094] 상기 인증 그룹(Group_Auth)은 기존의 카트리지들(720B_1 ~ 720B_N) 및 새로운 제(N+1) 카트리지(730A)를 포함하도록 설정될 수 있다. 이 때, 프린터(710B)가 정상적으로 보안 기능을 수행하지 않고, 제(N+1) 카트리지(730B)가 불법 카트리지에 해당하더라도, 정상적으로 보안 기능을 수행하는 다른 정품 카트리지에 의해 그룹 기반의 인증 절차가 실패한 것으로 판단될 수 있다.

[0095] 도 13은 본 발명의 실시예에 따른 디바이스를 포함하는 사물 인터넷 시스템을 나타내는 블록도이다. 도 13의 실시예에서는, 사물 인터넷 시스템으로서 스마트 홈 시스템이 예시되고, 본 발명의 실시예들에 따른 디바이스는 스마트 홈 시스템의 디바이스에 해당하는 예가 도시된다.

[0096] 도 13을 참조하면, 스마트 홈 시스템(800)에 구비되는 다수의 디바이스들(821 ~ 824)은 게이트 웨이(825) 및 외부 통신망을 통하여 외부 단말기(811)나 외부 서버(812)에 접속할 수 있다. 다수의 디바이스들(821 ~ 824)은 스마트 홈에 이용되는 냉장고, 에어컨, 세탁기 및 청소기 등 가전 제품일 수 있으며, 디바이스들(821 ~ 824)의 상태나 고장 진단 등의 정보가 외부 서버(812)로 제공될 수 있다. 외부 서버(812)는 디바이스들(821 ~ 824)의 정보를 수신하고 이들에 대한 스마트한 관리 서비스를 제공한다.

[0097] 또한, 이동 단말기(811)를 이용하는 이용자는 외부 통신망 및 게이트 웨이(825)를 통해 디바이스들(821 ~ 824)에 접속할 수 있다. 또한, 이동 단말기(811)를 이용하는 이용자는 외부 통신망을 통해 외부 서버(812)에 접속하여 디바이스들(821 ~ 824)의 상태를 판단할 수 있다.

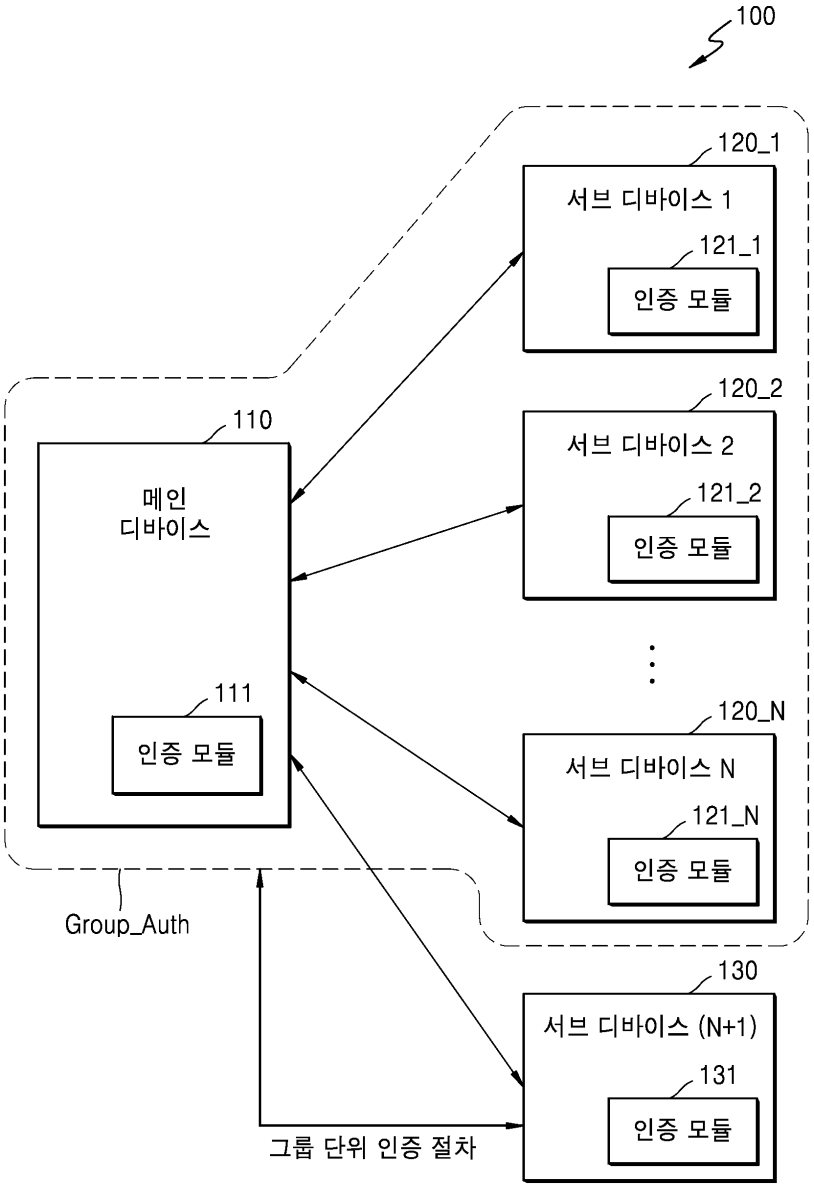
[0098] 상기와 같이 구성될 수 있는 스마트 홈 시스템(800)에 새로운 디바이스(예컨대, 제5 디바이스(830))가 새로이 연결될 수 있으며, 이 경우 전술한 실시예들에 따른 그룹 단위의 인증 절차가 새로이 연결되는 제5 디바이스(830)에 대해 수행될 수 있다. 일 예로서, 게이트 웨이(825)에 구비되는 인증 모듈과 제5 디바이스(830) 사이에서 1 대 1 챌린지-응답 기반의 인증 절차가 수행되고, 또한 스마트 홈 시스템(800)에 기존에 연결된 디바이스들을 포함하는 인증 그룹(Group_Auth)이 설정됨에 따라, 상기 인증 그룹(Group_Auth)과 제5 디바이스(830) 사이에서 그룹 단위의 인증 절차가 수행될 수 있다. 도 13에 도시된 실시예에서는 제1 내지 제4 디바이스들(821 ~ 824)이 하나의 인증 그룹(Group_Auth)으로 설정되는 예가 도시된다.

[0099] 상기와 같은 인증 절차에 따라, 스마트 홈 시스템(800)에 구비되는 기존의 디바이스들에 대한 보안이 강화될 수 있으며, 또한 정품에 해당하지 않는 디바이스들이 스마트 홈 시스템(800)의 구성으로서 동작하는 것이 방지될 수 있다.

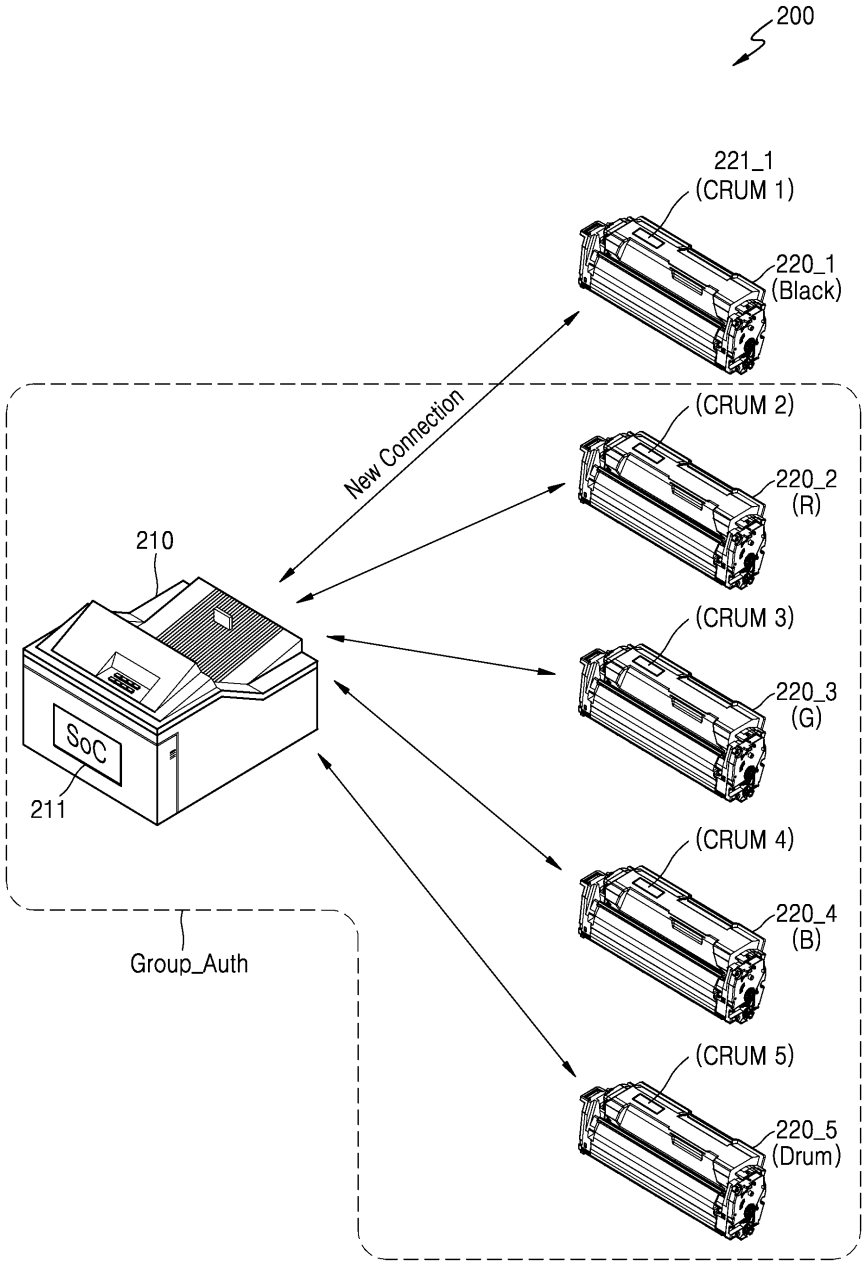
[0100] 상기한 실시예의 설명은 본 발명의 더욱 철저한 이해를 위하여 도면을 참조로 예를 든 것에 불과하므로, 본 발명을 한정하는 의미로 해석되어서는 안될 것이다. 또한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기본적 원리를 벗어나지 않는 범위 내에서 다양한 변화와 변경이 가능함은 명백하다 할 것이다.

도면

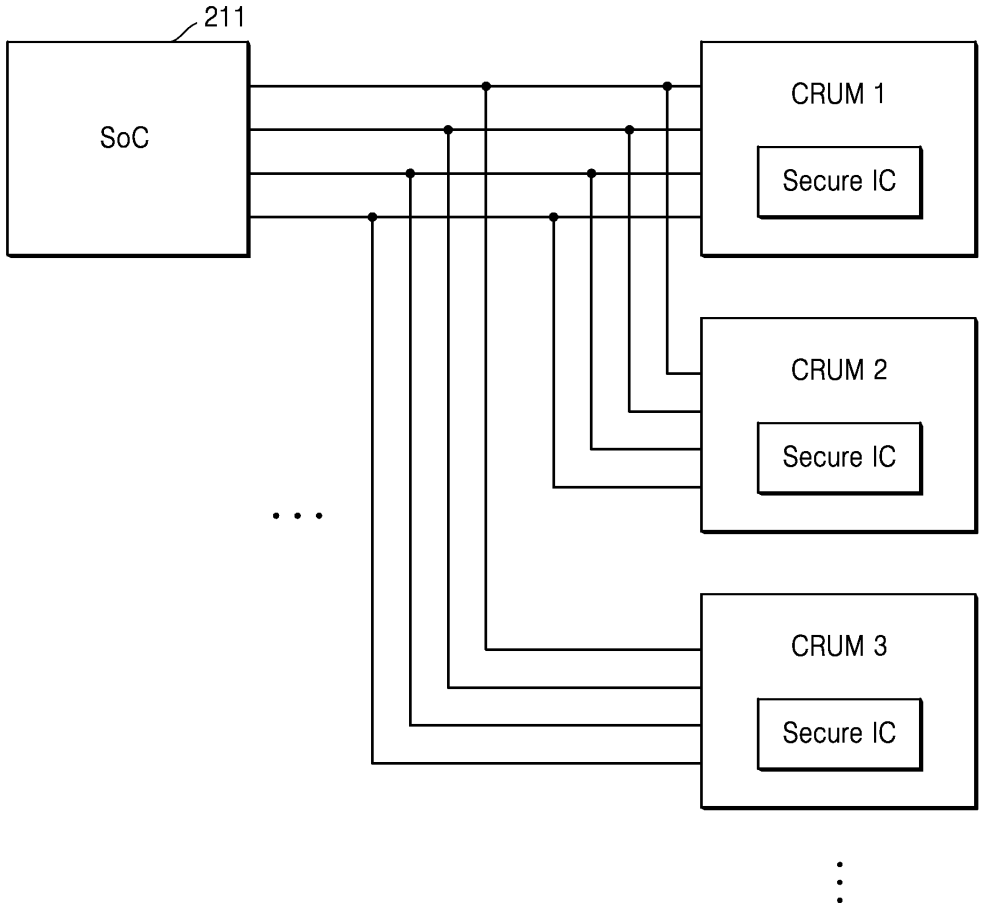
도면1



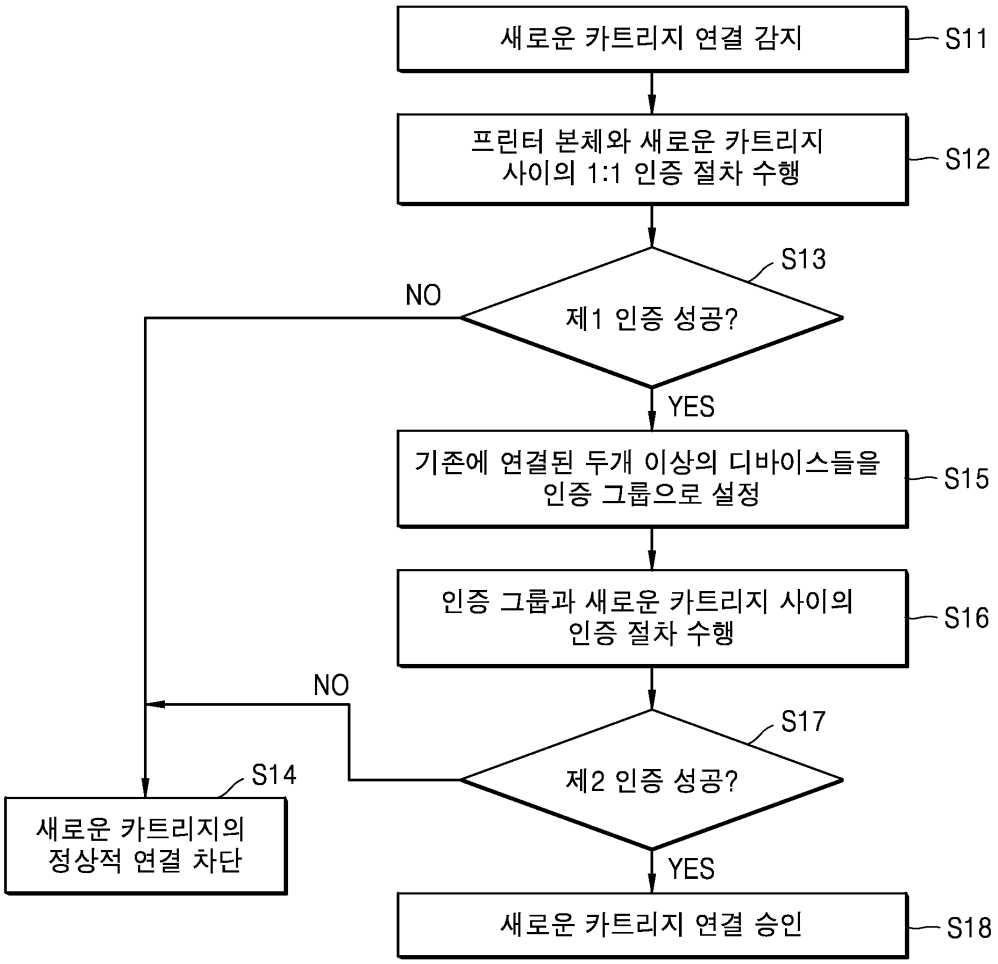
도면2


200
221_1
(CRUM 1)
220_1
(Black)
New Connection
(CRUM 2)
220_2
(R)
210
(CRUM 3)
220_3
(G)
SoC
211
(CRUM 4)
220_4
(B)
Group_Auth
(CRUM 5)
220_5
(Drum)

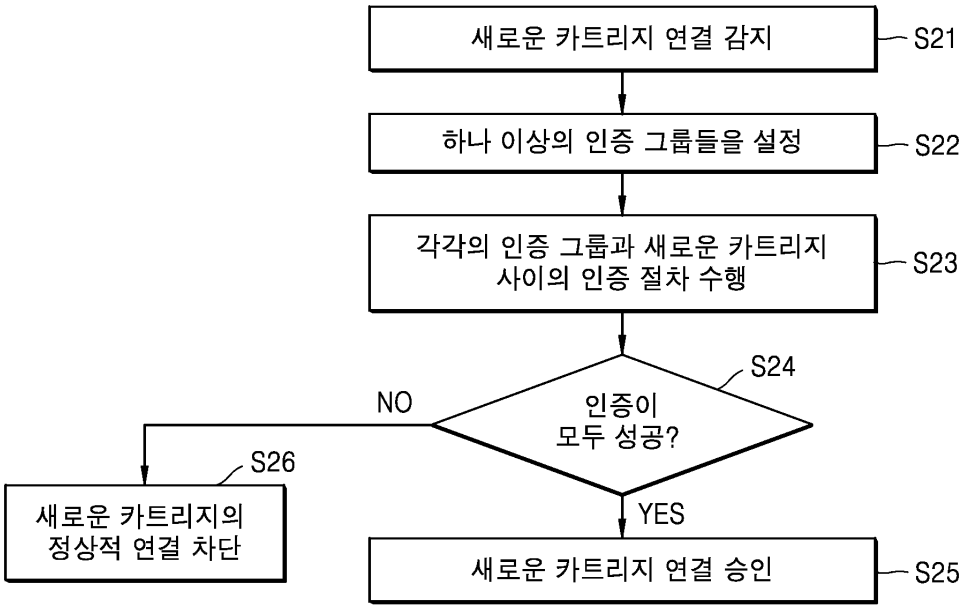
도면3



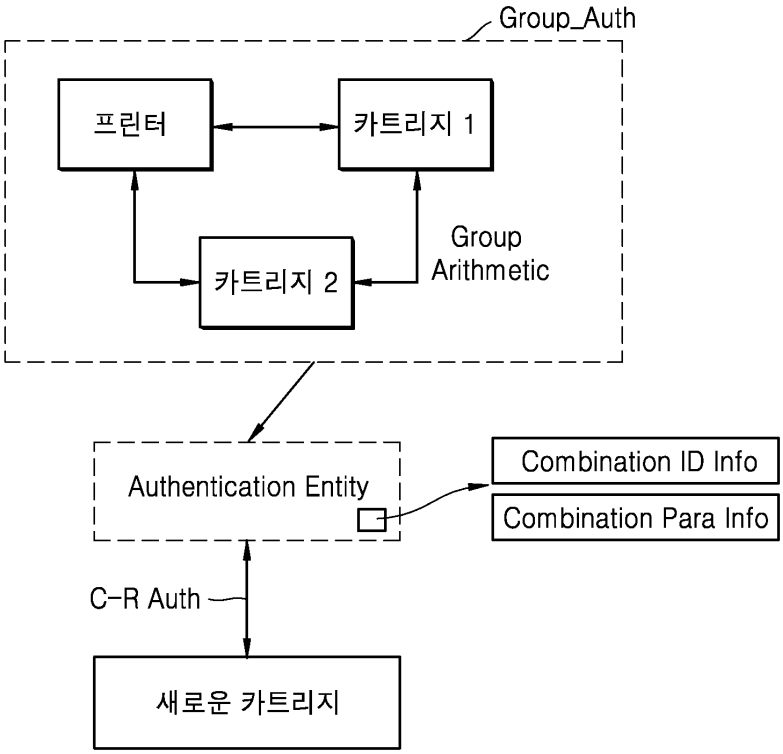
도면4


새로운 카트리지 연결 감지
S11
프린터 본체와 새로운 카트리지 사이의 1:1 인증 절차 수행
S12
S13
NO
제1 인증 성공?
YES
기존에 연결된 두개 이상의 디바이스들을 인증 그룹으로 설정
S15
인증 그룹과 새로운 카트리지 사이의 인증 절차 수행
S16
NO
S17
제2 인증 성공?
S14
새로운 카트리지의 정상적 연결 차단
YES
새로운 카트리지 연결 승인
S18

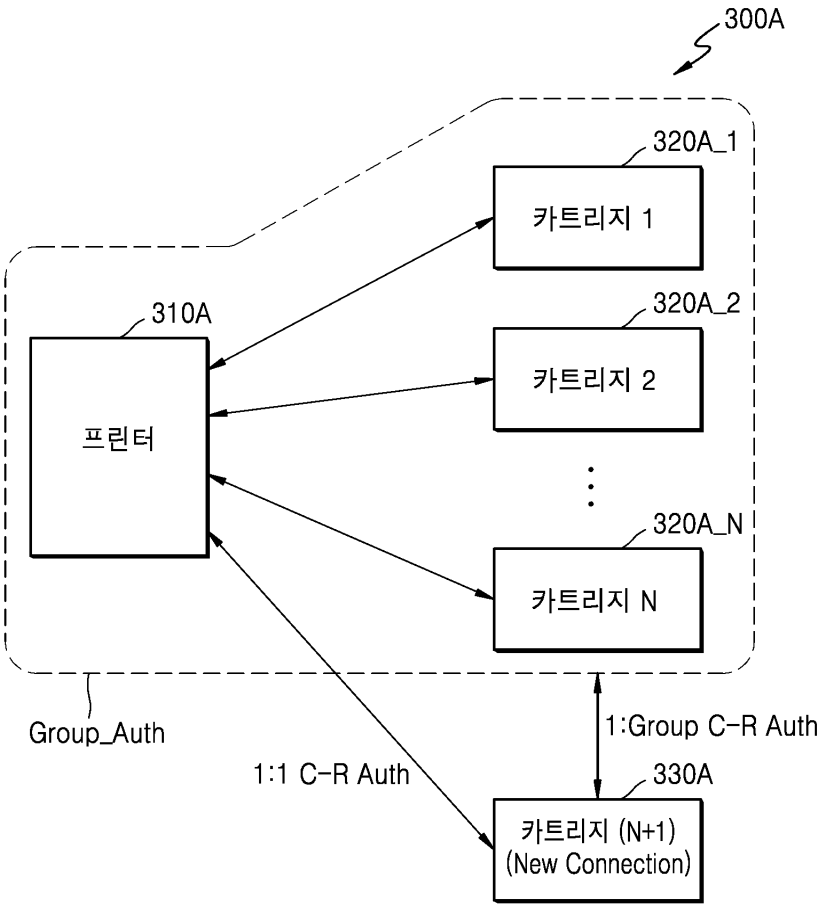
도면5


새로운 카트리지 연결 감지
S21
하나 이상의 인증 그룹들을 설정
S22
각각의 인증 그룹과 새로운 카트리지 사이의 인증 절차 수행
S23
S24
NO
인증이 모두 성공?
S26
새로운 카트리지의 정상적 연결 차단
YES
새로운 카트리지 연결 승인
S25

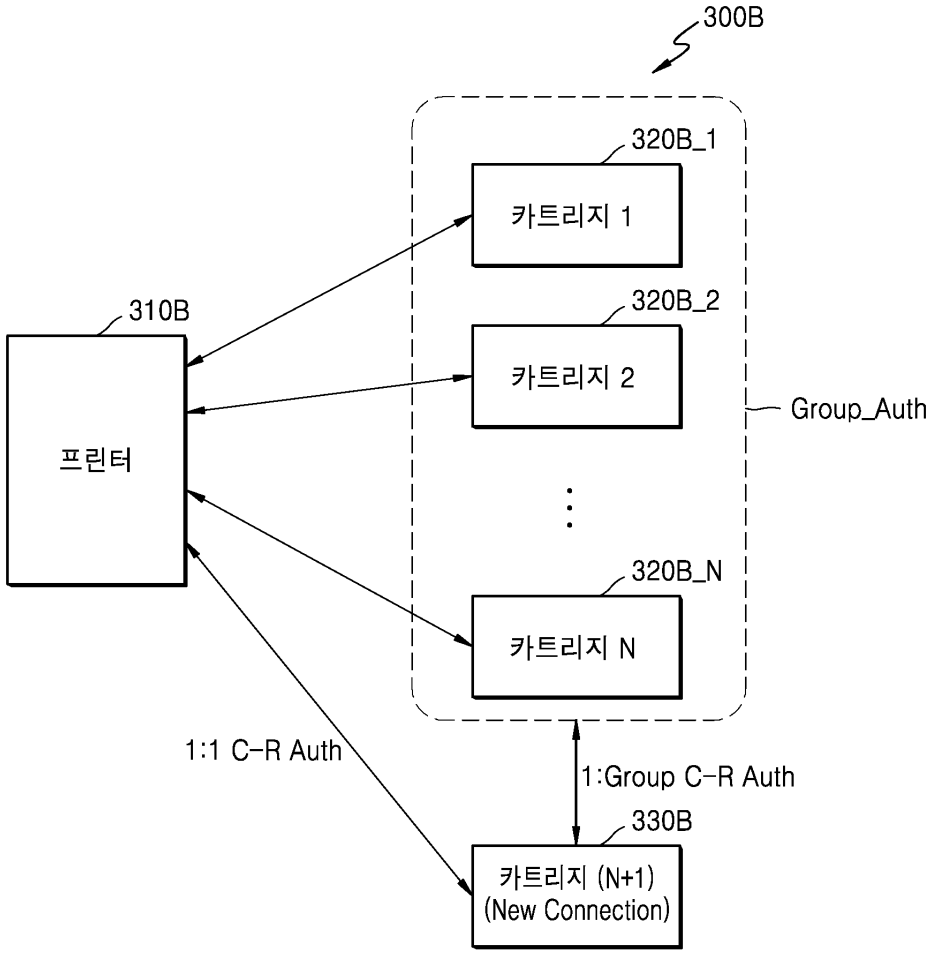
도면6


Group_Auth
프린터
카트리지 1
카트리지 2
Group
Arithmetic
Authentication Entity
Combination ID Info
Combination Para Info
C-R Auth
새로운 카트리지

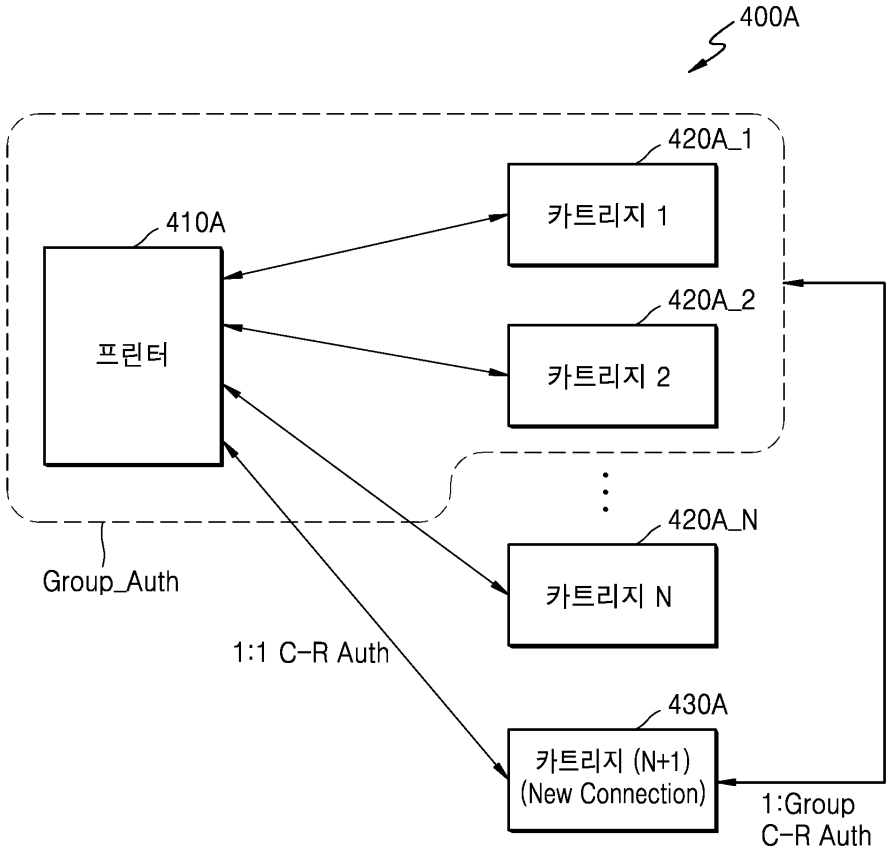
도면7a


300A
320A_1
카트리지 1
310A
320A_2
프린터
카트리지 2
320A_N
카트리지 N
Group_Auth
1:Group C-R Auth
1:1 C-R Auth
330A
카트리지 (N+1)
(New Connection)

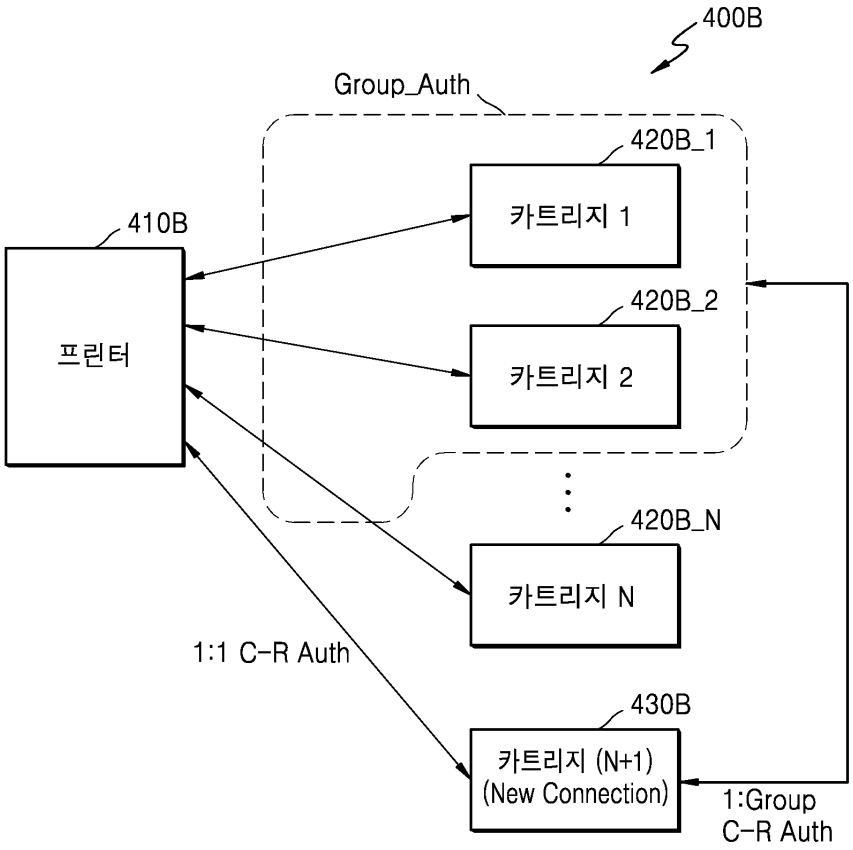
도면7b


300B
320B_1
카트리지 1
320B_2
카트리지 2
310B
프린터
Group_Auth
320B_N
카트리지 N
1:1 C-R Auth
1:Group C-R Auth
330B
카트리지 (N+1)
(New Connection)

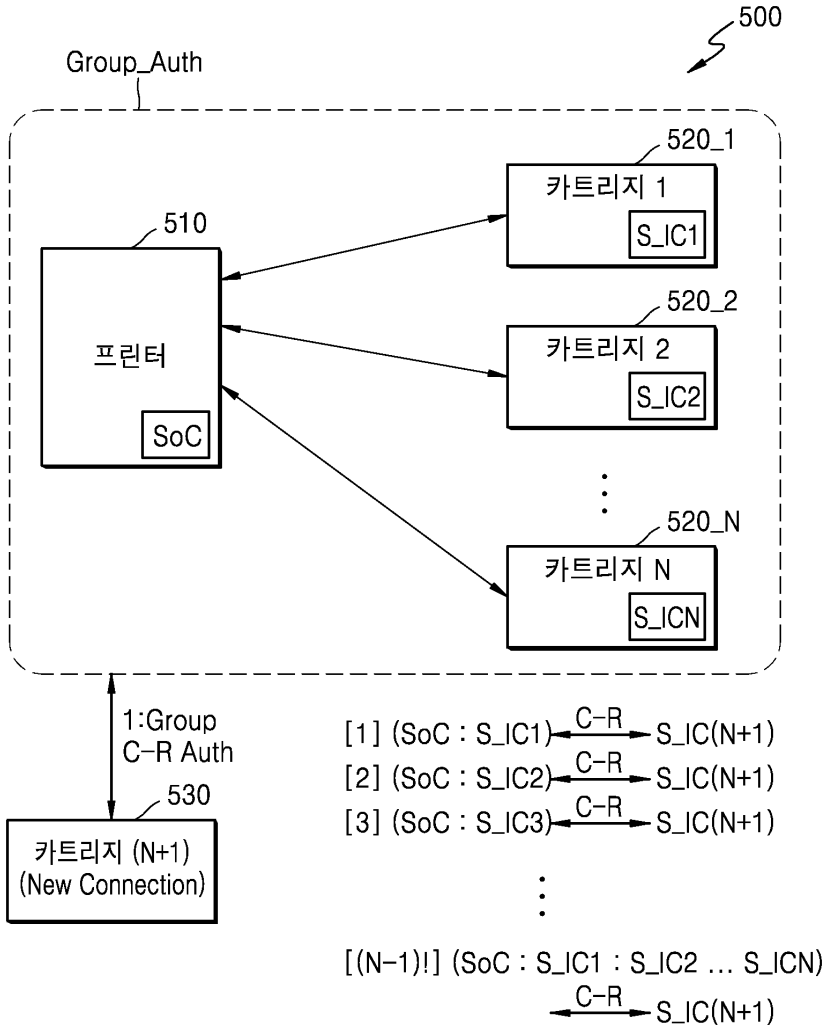
도면8a


400A
420A_1
카트리지 1
410A
프린터
420A_2
카트리지 2
420A_N
카트리지 N
Group_Auth
1:1 C-R Auth
430A
카트리지 (N+1)
(New Connection)
1:Group
C-R Auth

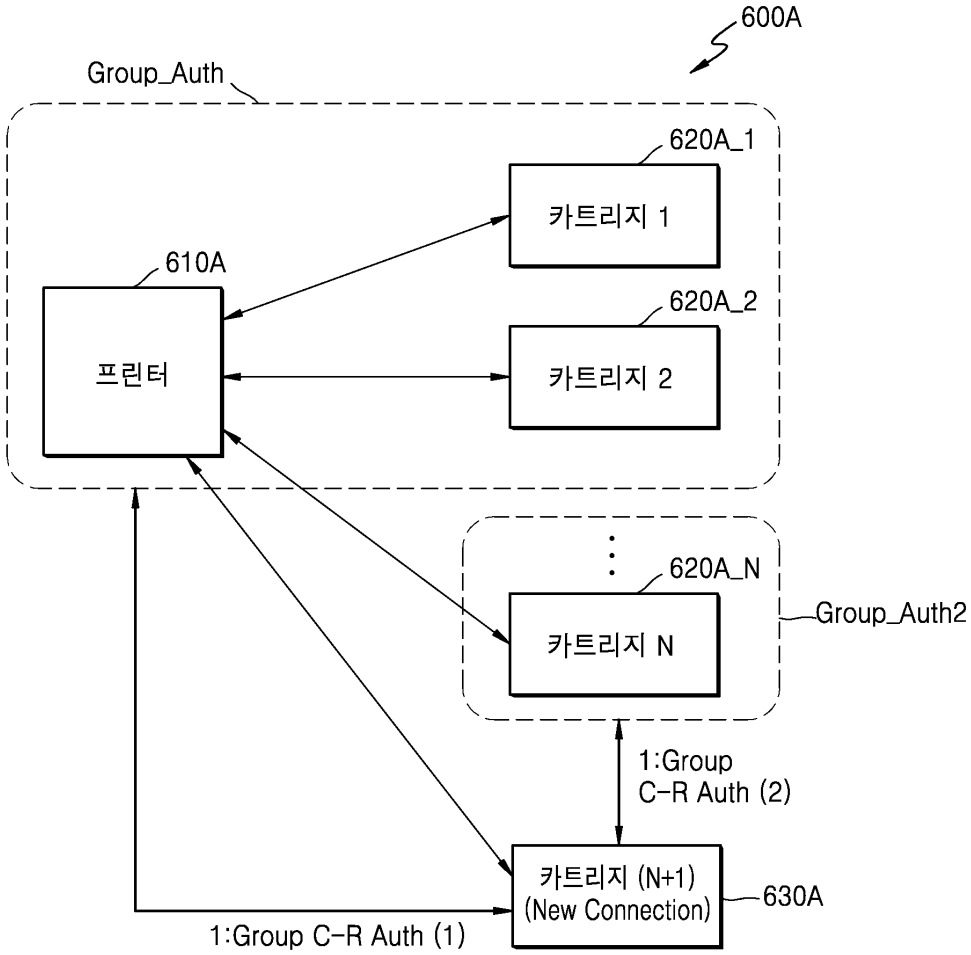
도면8b


400B
Group_Auth
420B_1
카트리지 1
410B
프린터
420B_2
카트리지 2
420B_N
카트리지 N
1:1 C-R Auth
430B
카트리지 (N+1)
(New Connection)
1:Group
C-R Auth

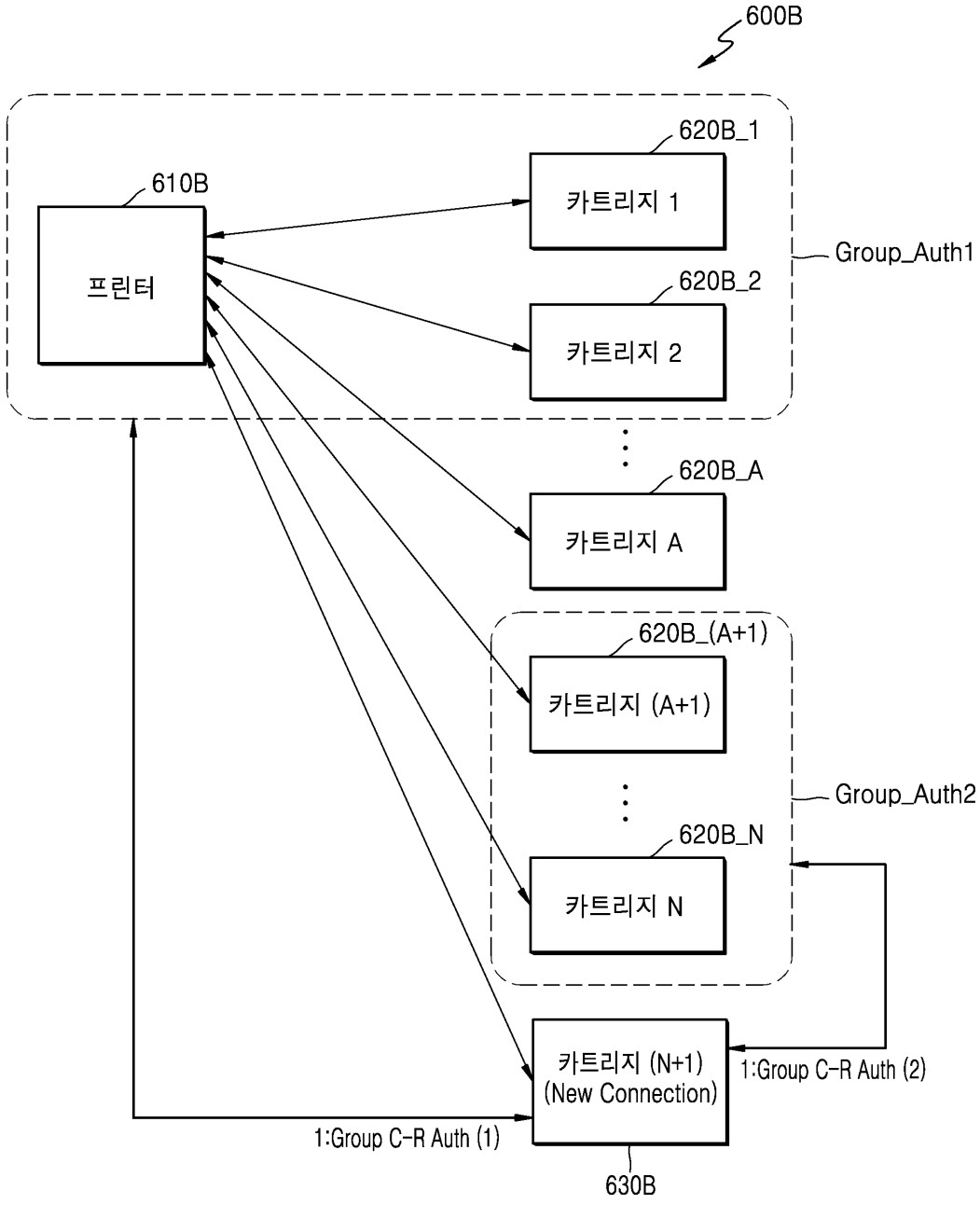
도면9


500
Group_Auth
520_1
카트리지 1
S_IC1
510
프린터
SoC
520_2
카트리지 2
S_IC2
520_N
카트리지 N
S_ICN
1:Group
C-R Auth
530
카트리지 (N+1)
(New Connection)
[1] (SoC : S_IC1) C-R S_IC(N+1)
[2] (SoC : S_IC2) C-R S_IC(N+1)
[3] (SoC : S_IC3) C-R S_IC(N+1)
[(N-1)!] (SoC : S_IC1 : S_IC2 … S_ICN)
C-R S_IC(N+1)

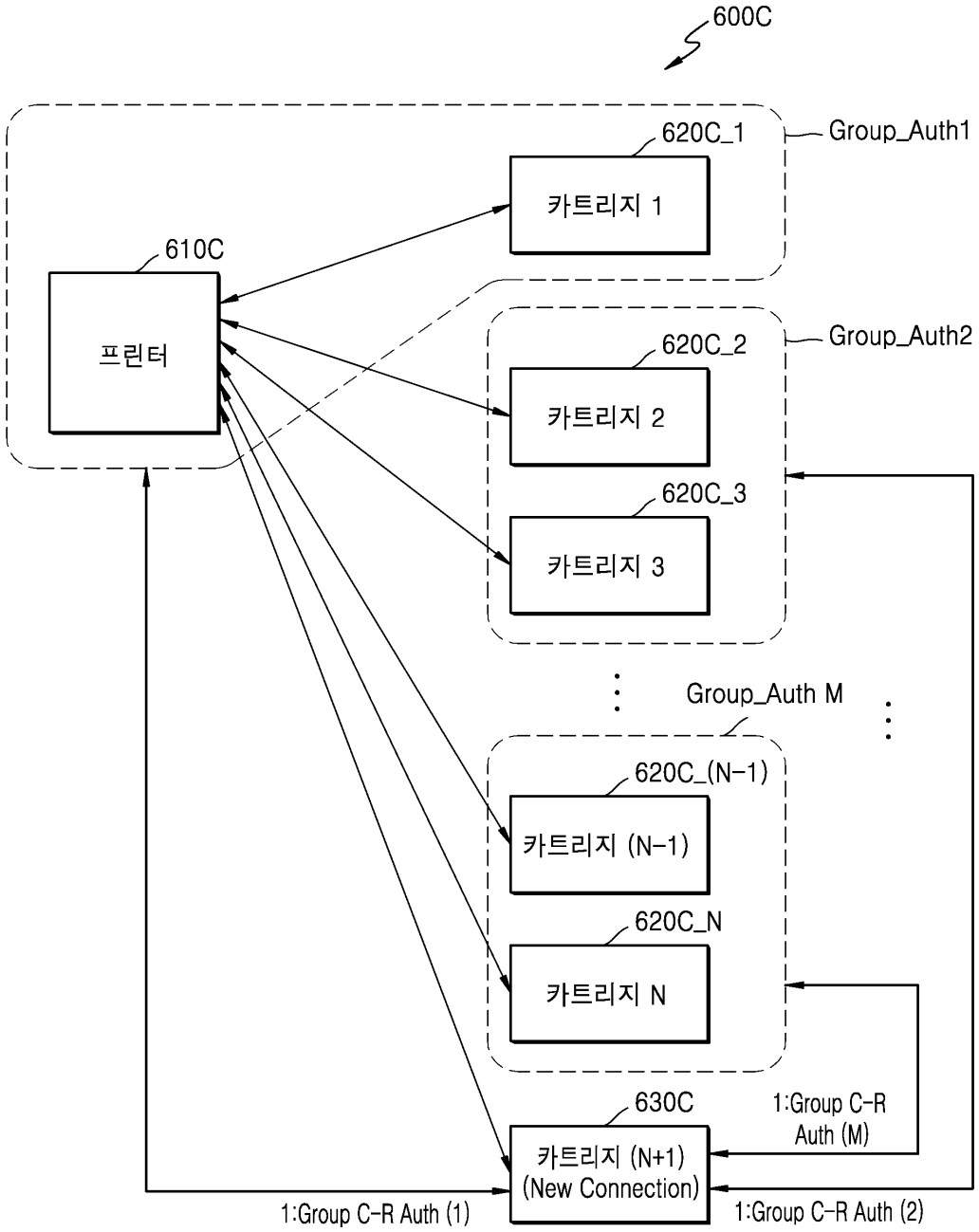
도면10a


600A
Group_Auth
620A_1
카트리지 1
610A
620A_2
프린터
카트리지 2
620A_N
Group_Auth2
카트리지 N
1:Group
C-R Auth (2)
카트리지 (N+1)
(New Connection)
630A
1:Group C-R Auth (1)

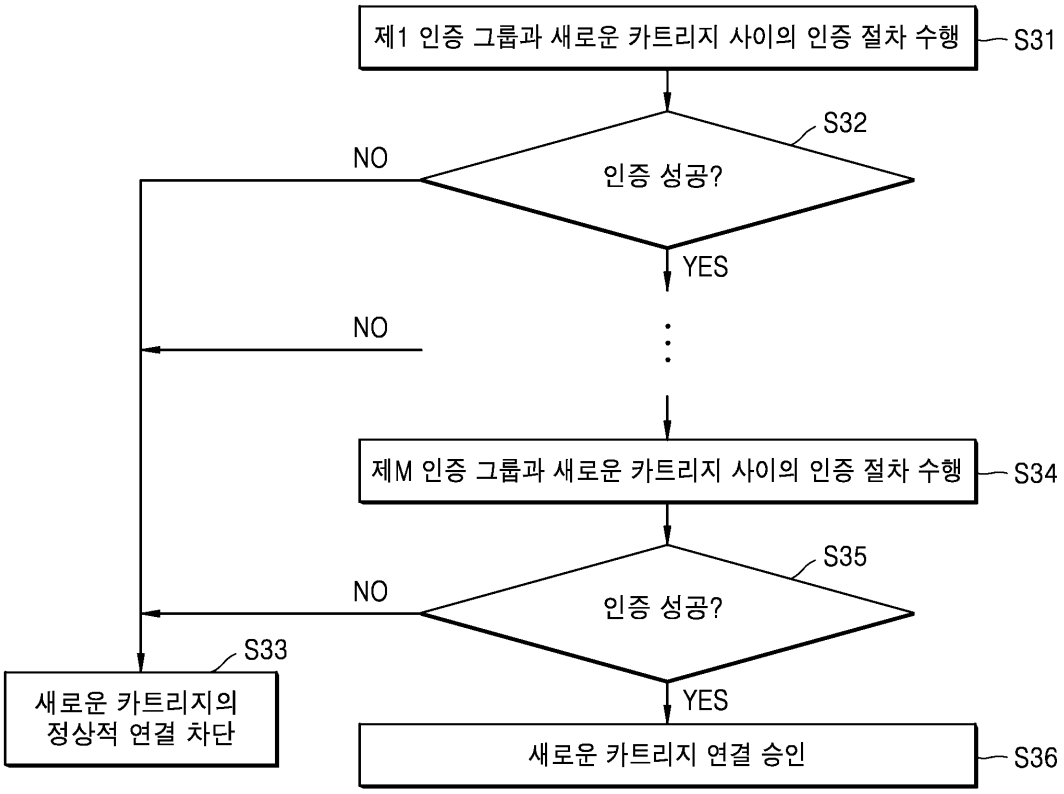
도면10b


600B
620B_1
610B
카트리지 1
프린터
Group_Auth1
620B_2
카트리지 2
620B_A
카트리지 A
620B_(A+1)
카트리지 (A+1)
Group_Auth2
620B_N
카트리지 N
카트리지 (N+1)
(New Connection)
1:Group C-R Auth (2)
1:Group C-R Auth (1)
630B

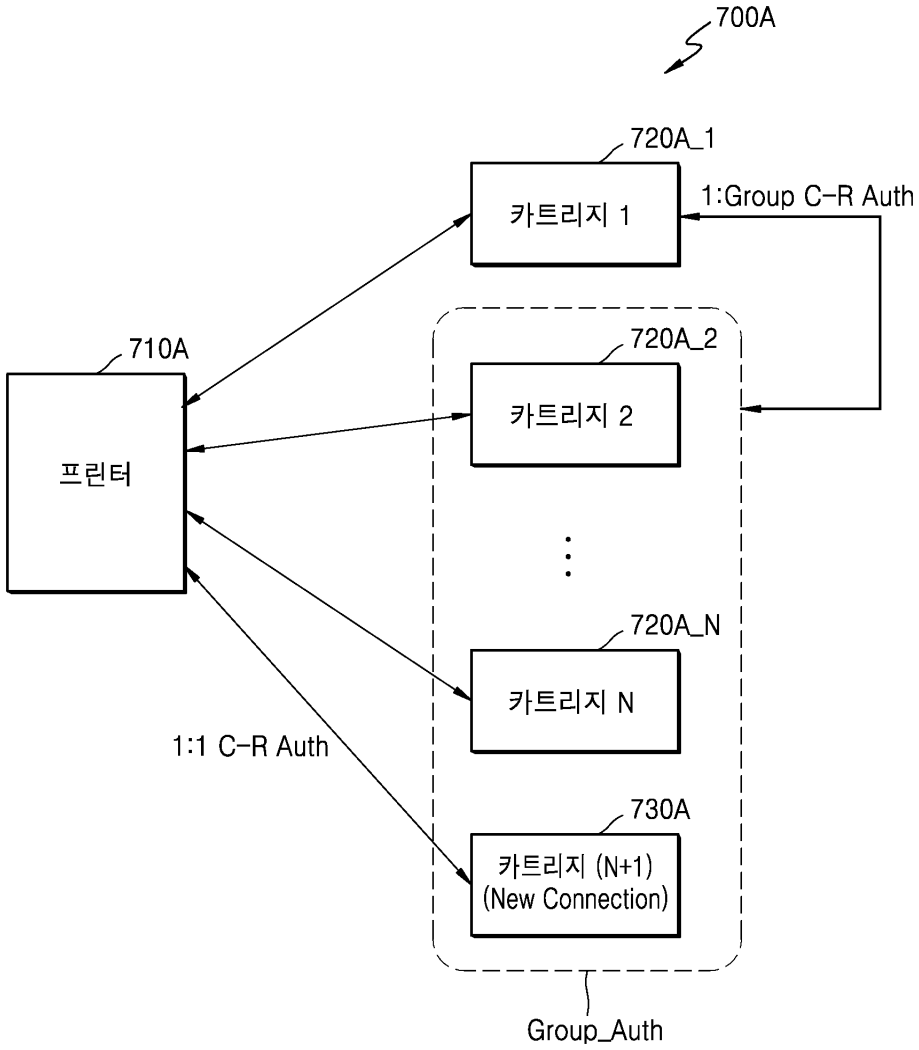
도면10c


600C
620C_1
Group_Auth1
카트리지 1
610C
프린터
620C_2
Group_Auth2
카트리지 2
620C_3
카트리지 3
Group_Auth M
620C_(N-1)
카트리지 (N-1)
620C_N
카트리지 N
630C
1:Group C-R Auth (M)
카트리지 (N+1) (New Connection)
1:Group C-R Auth (1)
1:Group C-R Auth (2)

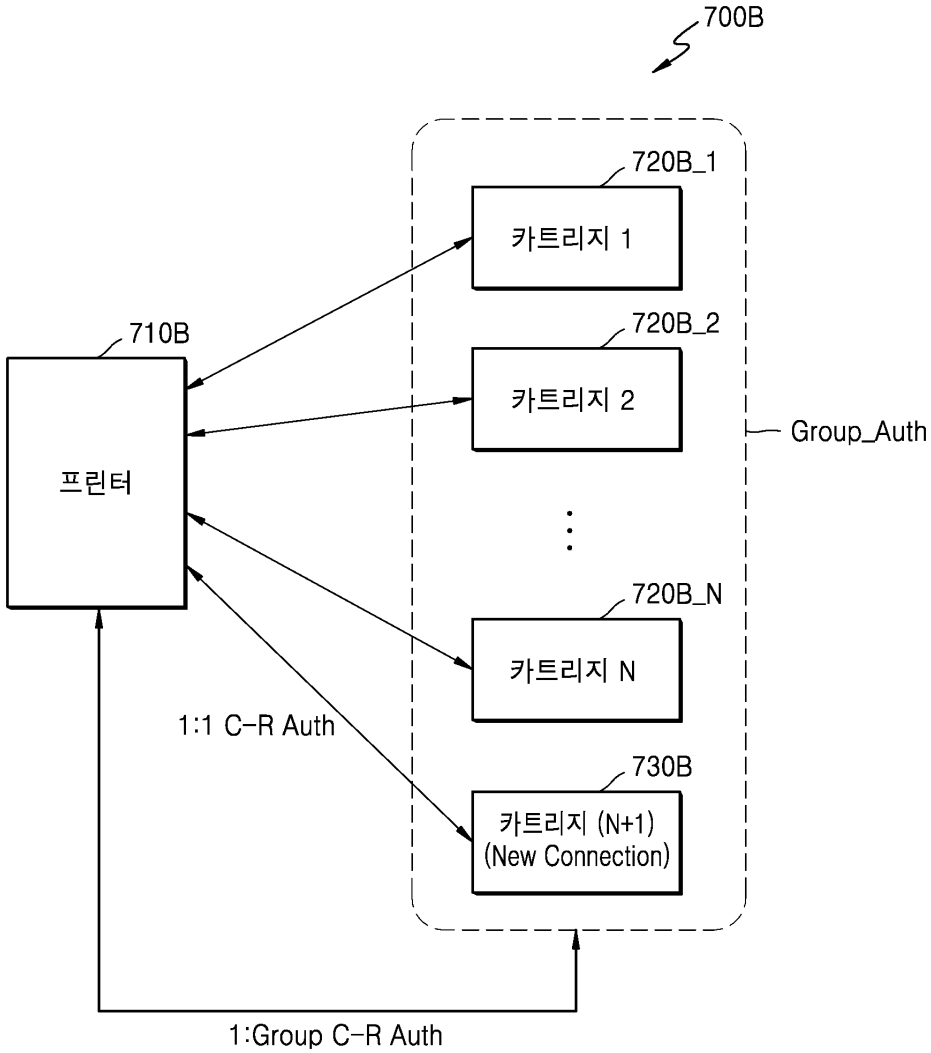
도면11


제1 인증 그룹과 새로운 카트리지 사이의 인증 절차 수행
S31
S32
인증 성공?
NO
YES
NO
제M 인증 그룹과 새로운 카트리지 사이의 인증 절차 수행
S34
S35
인증 성공?
NO
YES
S33
새로운 카트리지의
정상적 연결 차단
새로운 카트리지 연결 승인
S36

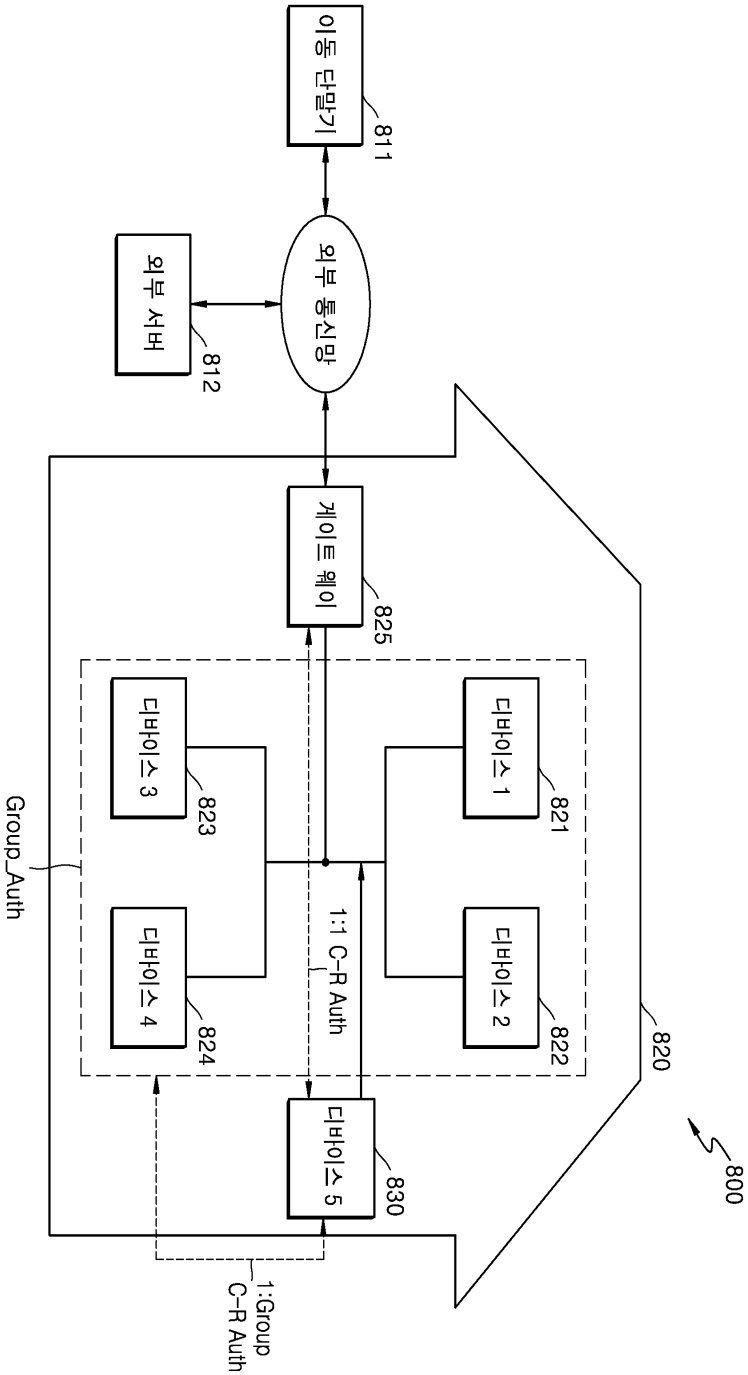
도면12a


700A
720A_1
카트리지 1
1:Group C-R Auth
710A
720A_2
카트리지 2
프린터
720A_N
카트리지 N
1:1 C-R Auth
730A
카트리지 (N+1)
(New Connection)
Group_Auth

도면12b


700B
720B_1
카트리지 1
720B_2
카트리지 2
710B
프린터
Group_Auth
720B_N
카트리지 N
1:1 C-R Auth
730B
카트리지 (N+1)
(New Connection)
1:Group C-R Auth

도면13


이동 단말기
811
외부 서버
812
외부 통신망
게이트 웨이
825
디바이스 3
823
디바이스 1
821
디바이스 4
824
디바이스 2
822
1:1 C-R Auth
디바이스 5
830
820
800
Group_Auth
1:Group
C-R Auth