



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0103892
(43) 공개일자 2018년09월19일

(51) 국제특허분류(Int. Cl.)
H04W 12/04 (2009.01) H04L 29/06 (2006.01)
H04L 29/08 (2006.01) H04W 12/06 (2009.01)
H04W 4/70 (2018.01) H04W 4/80 (2018.01)
(52) CPC특허분류
H04W 12/04 (2013.01)
H04L 63/0876 (2013.01)
(21) 출원번호 10-2018-7019934
(22) 출원일자(국제) 2016년11월22일
심사청구일자 없음
(85) 번역문제출일자 2018년07월12일
(86) 국제출원번호 PCT/US2016/063349
(87) 국제공개번호 WO 2017/127156
국제공개일자 2017년07월27일
(30) 우선권주장
15/000,105 2016년01월19일 미국(US)

(71) 출원인
켈컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
번즈 그레고리
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
카바스 크리스토퍼
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
특허법인코리아나

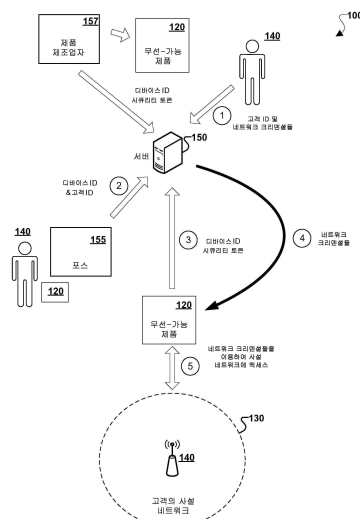
전체 청구항 수 : 총 25 항

(54) 발명의 명칭 네트워크에서 무선-가능 제품들을 온보딩하기 위한 방법 및 시스템

(57) 요약

다양한 실시형태들은 무선 네트워크들에 무선-가능 제품들을 접속하기 위한 시스템들 및 방법들을 제공한다. 고객 네트워크 크리덴셜들은 원-타임 등록 동안에 고객 식별자 ("고객 ID") 와 함께 서버에 저장될 수도 있다. 무선-가능 제품이 구매될 때, 제품 식별자 ("제품 ID") 및 고객의 ID 는 구매한 제품을 고객에 링크하는, 2 개의 식별자들을 상관시키는, 서버로 포워딩된다. 무선-가능 제품이 파워 온될 때, 제품은 공중 네트워크 접속을 통해 서버에 액세스하고, 제품 ID 및 시큐리티 토큰을 서버로 전송한다. 서버는 제품 ID 및 시큐리티 토큰을 이용하여 제품을 인증한다. 일단 인증되면, 서버는 상관된 고객 ID 를 이용하여 고객의 사설 네트워크에 대한 네트워크 크리덴셜들을 룩업하고, 네트워크 크리덴셜들을 무선-가능 제품에 제공한다. 무선-가능 제품은 그 후 다운로드된 크리덴셜들을 이용하여 고객의 사설 네트워크에 액세스한다.

대표도 - 도1b



(52) CPC특허분류

H04L 63/102 (2013.01)

H04L 67/12 (2013.01)

H04W 12/06 (2013.01)

H04W 4/70 (2018.02)

H04W 4/80 (2018.02)

(72) 발명자

로이 마르셀로

미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775

스웬슨 케네스

미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775

말스베리 토드

미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775

마이클 매튜

미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775

명세서

청구범위

청구항 1

무선-가능 제품을 사설 통신 네트워크에 접속하는 것을 촉진하는 방법으로서,

고객의 식별자 ("고객 ID") 및 상기 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들을 서버에 저장하는 단계;

상기 서버에서, 상기 고객이 상기 무선-가능 제품을 구매하는 구매 트랜잭션을 인에이블하는 컴퓨팅 디바이스로부터 상기 무선-가능 제품과 연관된 디바이스 ID 및 상기 무선-가능 제품을 구매하는 상기 고객의 상기 고객 ID를 수신하는 단계;

상기 디바이스 ID 와의 상기 고객 ID 의 연관 (association) 을 상기 서버에 저장하는 단계;

상기 서버에서, 상기 무선-가능 제품에 의해 개시된 네트워크 접속을 통하여 상기 무선-가능 제품으로부터 상기 디바이스 ID 및 시큐리티 토큰을 수신하는 단계;

상기 서버에 의해, 수신된 상기 디바이스 ID 및 시큐리티 토큰에 기초하여 상기 무선-가능 제품을 인증하는 단계;

상기 무선-가능 제품을 인증하는 것에 응답하여, 상기 서버에 의해 상기 무선-가능 제품에, 상기 고객의 상기 사설 통신 네트워크에 액세스하기 위한 상기 네트워크 크리덴셜들을 제공하는 단계를 포함하는, 무선-가능 제품을 사설 통신 네트워크에 접속하는 것을 촉진하는 방법.

청구항 2

제 1 항에 있어서,

상기 고객 ID 및 상기 고객의 사설 통신 네트워크에 액세스하기 위한 상기 네트워크 크리덴셜들은, 고객 정보가 입력되는 고객 등록 프로세스 동안에 상기 서버에 의해 획득되는, 무선-가능 제품을 사설 통신 네트워크에 접속하는 것을 촉진하는 방법.

청구항 3

제 2 항에 있어서,

상기 고객 등록 프로세스는 고객 로열티 프로그램에 대한 사인 업 프로시저를 포함하는, 무선-가능 제품을 사설 통신 네트워크에 접속하는 것을 촉진하는 방법.

청구항 4

제 1 항에 있어서,

상기 무선-가능 제품의 제조업자로부터 상기 디바이스 ID 및 디바이스 시큐리티 키를 상기 서버에 의해 수신하는 단계; 및

상기 디바이스 ID 에 링크된 상기 서버에 의해 액세스가능한 메모리에 상기 디바이스 시큐리티 키를 저장하는 단계를 더 포함하고,

상기 서버에 의해, 수신된 상기 디바이스 ID 및 시큐리티 토큰에 기초하여 상기 무선-가능 제품을 인증하는 단계는,

수신된 상기 디바이스 ID 를 이용하여 메모리로부터의 상기 디바이스 시큐리티 키에 액세스하는 단계;

저장된 상기 디바이스 시큐리티 키를 이용하여 수신된 상기 시큐리티 토큰을 인증하는 단계; 및

수신된 상기 디바이스 ID 가 수신된 상기 시큐리티 토큰을 인증하는 디바이스 시큐리티 키에 상기 서버가 액세스하는 것을 인에이블하면 상기 무선-가능 제품을 인증하는 단계를 포함하는, 무선-가능 제품을 사설 통신 네트

워크에 접속하는 것을 촉진하는 방법.

청구항 5

제 4 항에 있어서,

상기 무선-가능 제품의 상기 제조업자로부터 수신된 상기 디바이스 시큐리티 키는 상기 서버가 시큐리티 토큰을 생성하기 위해 이용할 수 있는 정보를 포함하고; 그리고

저장된 상기 디바이스 시큐리티 키를 이용하여 수신된 상기 시큐리티 토큰을 인증하는 단계는,

상기 무선-가능 제품의 상기 제조업자로부터 수신된 상기 디바이스 시큐리티 키를 이용하여 생성된 시큐리티 토큰을 획득하는 단계; 및

상기 생성된 시큐리티 토큰과 수신된 상기 시큐리티 토큰을 비교하는 단계를 포함하는, 무선-가능 제품을 사설 통신 네트워크에 접속하는 것을 촉진하는 방법.

청구항 6

제 4 항에 있어서,

상기 무선-가능 제품의 상기 제조업자로부터 수신된 상기 디바이스 시큐리티 키는 제조업자-제공 시큐리티 토큰을 포함하고; 그리고

저장된 상기 디바이스 시큐리티 키를 이용하여 수신된 상기 시큐리티 토큰을 인증하는 단계는 상기 제조업자-제공 시큐리티 토큰과 수신된 상기 시큐리티 토큰을 비교하는 단계를 포함하는, 무선-가능 제품을 사설 통신 네트워크에 접속하는 것을 촉진하는 방법.

청구항 7

제 1 항에 있어서,

상기 무선-가능 제품에 의해 개시된 상기 네트워크 접속은 상기 고객의 사설 통신 네트워크에 대한 액세스 디바이스의 게스트 액세스 메커니즘을 통한 상기 서버에 대한 접속인, 무선-가능 제품을 사설 통신 네트워크에 접속하는 것을 촉진하는 방법.

청구항 8

제 1 항에 있어서,

상기 무선-가능 제품에 의해 개시된 상기 네트워크 접속은 공중 네트워크를 통한 접속인, 무선-가능 제품을 사설 통신 네트워크에 접속하는 것을 촉진하는 방법.

청구항 9

무선-가능 제품을 사설 통신 네트워크에 접속하는 것을 촉진하도록 구성된 서버로서,

서버 프로세서를 포함하고,

상기 서버 프로세서는,

고객의 식별자 ("고객 ID") 및 상기 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들을 저장하는 것;

상기 고객에 의한 무선-가능 제품의 구매에 수반된 컴퓨팅 디바이스로부터 고객 ID 및 상기 무선-가능 제품의 디바이스 ID 를 수신하는 것;

상기 디바이스 ID 와의 상기 고객 ID 의 연관을 저장하는 것;

상기 무선-가능 제품에 의해 확립된 네트워크 접속을 통하여 상기 무선-가능 제품으로부터 상기 디바이스 ID 및 시큐리티 토큰을 수신하는 것;

수신된 상기 디바이스 ID 및 시큐리티 토큰에 기초하여 상기 무선-가능 제품을 인증하는 것; 및

상기 무선-가능 제품을 인증하는 것에 응답하여, 상기 무선-가능 제품에, 상기 고객의 상기 사설 통신 네트워크에 액세스하기 위한 상기 네트워크 크리덴셜들을 제공하는 것을 포함하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성된, 서버.

청구항 10

제 9 항에 있어서,

상기 서버 프로세서는, 고객 정보가 입력되는 고객 등록 프로세스 동안에 상기 고객 ID 및 상기 고객의 사설 통신 네트워크에 액세스하기 위한 상기 네트워크 크리덴셜들을 획득하기 위한 프로세서-실행가능 명령들로 구성되는, 서버.

청구항 11

제 10 항에 있어서,

상기 고객 등록 프로세스는 고객 로열티 프로그램에 대한 사인 업 프로시저를 포함하는, 서버.

청구항 12

제 9 항에 있어서,

상기 서버 프로세서는,

상기 무선-가능 제품의 제조업자로부터 상기 디바이스 ID 및 디바이스 시큐리티 키를 수신하는 것; 및

상기 디바이스 ID 에 링크된 상기 서버에 의해 액세스가능한 메모리에 상기 디바이스 시큐리티 키를 저장하는 것을 더 포함하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되고,

상기 서버 프로세서는, 수신된 상기 디바이스 ID 및 시큐리티 토큰에 기초하여 상기 무선-가능 제품을 인증하는 것이,

수신된 상기 디바이스 ID 를 이용하여 메모리로부터의 상기 디바이스 시큐리티 키에 액세스하는 것;

저장된 상기 디바이스 시큐리티 키를 이용하여 수신된 상기 시큐리티 토큰을 인증하는 것; 및

수신된 상기 디바이스 ID 가 수신된 상기 시큐리티 토큰을 인증하는 디바이스 시큐리티 키에 상기 서버가 액세스하는 것을 인에이블하면 상기 무선-가능 제품을 인증하는 것을 포함하도록 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는, 서버.

청구항 13

제 12 항에 있어서,

상기 서버 프로세서는,

상기 무선-가능 제품의 상기 제조업자로부터 수신된 상기 디바이스 시큐리티 키가 상기 서버가 시큐리티 토큰을 생성하기 위해 이용할 수 있는 정보를 포함하도록 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되고; 그리고

저장된 상기 디바이스 시큐리티 키를 이용하여 수신된 상기 시큐리티 토큰을 인증하는 것은,

상기 무선-가능 제품의 상기 제조업자로부터 수신된 상기 디바이스 시큐리티 키를 이용하여 생성된 시큐리티 토큰을 획득하는 것; 및

상기 생성된 시큐리티 토큰과 수신된 상기 시큐리티 토큰을 비교하는 것을 포함하는, 서버.

청구항 14

제 12 항에 있어서,

상기 서버 프로세서는,

상기 무선-가능 제품의 상기 제조업자로부터 수신된 상기 디바이스 시큐리티 키가 제조업자-제공 시큐리티 토큰

을 포함하도록 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되고; 그리고

저장된 상기 디바이스 시큐리티 키를 이용하여 수신된 상기 시큐리티 토큰을 인증하는 것은 상기 제조업자-제공 시큐리티 토큰과 수신된 상기 시큐리티 토큰을 비교하는 것을 포함하는, 서버.

청구항 15

무선-가능 제품으로서,

무선 트랜시버;

메모리; 및

상기 무선 트랜시버 및 상기 메모리에 커플링된 프로세서를 포함하고,

상기 프로세서는,

공중 액세스 네트워크를 통해 서버에 대한 접속을 확립하는 것;

상기 메모리에 저장된 디바이스 식별자 및 시큐리티 토큰을 확립된 상기 접속을 통하여 상기 서버에 송신하는 것; 및

상기 서버로부터, 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들을 수신하는 것;

상기 서버에 대한 확립된 상기 접속을 접속해제하는 것; 및

상기 사설 통신 네트워크에 액세스하기 위해 상기 서버에 의해 제공된 상기 네트워크 크리덴셜들을 이용하여 상기 사설 통신 네트워크에 대한 액세스 디바이스의 범위에 들어갈 때 상기 사설 통신 네트워크와 접속을 확립하는 것을 포함하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성된, 무선-가능 제품.

청구항 16

제 15 항에 있어서,

상기 공중 액세스 네트워크를 통해 서버에 대한 접속을 확립하는 것은 상기 사설 통신 네트워크에 대한 상기 액세스 디바이스의 게스트 액세스 메커니즘을 통하여 상기 서버에 대한 상기 접속을 확립하는 것을 포함하는, 무선-가능 제품.

청구항 17

사설 통신 네트워크들에 대한 무선-가능 제품들의 접속들을 촉진하기 위한 시스템으로서,

공중 네트워크를 통해 액세스가능하도록 구성된 서버;

무선-가능 제품;

고객의 사설 통신 네트워크를 제공하는 액세스 디바이스; 및

상기 공중 네트워크에 커플링되고 상기 무선-가능 제품의 상기 고객에 의한 구매 트랜잭션을 지원하도록 구성된 컴퓨팅 디바이스를 포함하고,

상기 서버는 상기 고객의 식별자 ("고객 ID") 및 상기 고객의 상기 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들을 저장하는 것을 포함하는 동작들을 수행하도록 구성되고,

상기 컴퓨팅 디바이스는,

상기 무선-가능 제품과 연관된 디바이스 ID 및 상기 무선-가능 제품을 구매하는 상기 고객의 상기 고객 ID 를 획득하는 것; 및

상기 고객 ID 및 상기 디바이스 ID 를 상기 서버에 제공하는 것을 포함하는 동작들을 수행하도록 구성되고;

상기 서버는 상기 고객 ID 와 상기 디바이스 ID 의 연관을 저장하는 것을 더 포함하는 동작들을 수행하도록 구성되고,

상기 무선-가능 제품은,

상기 서버에 대한 접속을 확립하는 것; 및

상기 디바이스 ID 및 시큐리티 토큰을 확립된 상기 접속을 통하여 상기 서버에 송신하는 것을 포함하는 동작들을 수행하도록 구성되고;

상기 서버는,

상기 디바이스 ID 및 시큐리티 토큰에 기초하여 상기 무선-가능 제품을 인증하는 것; 및

상기 무선-가능 제품을 인증하는 것에 응답하여, 확립된 상기 접속을 통해 상기 무선-가능 제품에, 상기 고객의 상기 사설 통신 네트워크에 액세스하기 위한 상기 네트워크 크리덴셜들을 제공하는 것을 더 포함하는 동작들을 수행하도록 구성되고, 그리고

상기 무선-가능 제품은,

상기 서버에 대한 확립된 상기 접속을 접속해제하는 것; 및

상기 서버에 의해 제공된 상기 고객의 사설 통신 네트워크에 액세스하기 위한 상기 네트워크 크리덴셜들을 이용하여 상기 사설 통신 네트워크에 대한 상기 액세스 디바이스의 범위에 들어갈 때 상기 사설 통신 네트워크와 접속을 확립하는 것을 더 포함하는 동작들을 수행하도록 구성되는, 시스템.

청구항 18

제 17 항에 있어서,

상기 서버는, 고객 정보가 입력되는 고객 등록 프로세스 동안에 상기 고객 ID 및 상기 고객의 사설 통신 네트워크에 액세스하기 위한 상기 네트워크 크리덴셜들을 획득하기 위한 프로세서-실행가능 명령들로 구성되는, 시스템.

청구항 19

제 18 항에 있어서,

상기 고객 등록 프로세스는 고객 로열티 프로그램에 대한 사인 업 프로시저를 포함하는, 시스템.

청구항 20

제 18 항에 있어서,

상기 서버는,

상기 무선-가능 제품의 제조업자로부터 상기 디바이스 ID 및 디바이스 시큐리티 키를 수신하는 것; 및

상기 디바이스 ID 에 링크된 상기 서버에 의해 액세스가능한 메모리에 상기 디바이스 시큐리티 키를 저장하는 것을 더 포함하는 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되고,

상기 서버는, 수신된 상기 디바이스 ID 및 시큐리티 토큰에 기초하여 상기 무선-가능 제품을 인증하는 것이,

수신된 상기 디바이스 ID 를 이용하여 메모리로부터의 상기 디바이스 시큐리티 키에 액세스하는 것;

저장된 상기 디바이스 시큐리티 키를 이용하여 수신된 상기 시큐리티 토큰을 인증하는 것;

수신된 상기 디바이스 ID 가 수신된 상기 시큐리티 토큰을 인증하는 디바이스 시큐리티 키에 상기 서버가 액세스하는 것을 인에이블하면 상기 무선-가능 제품을 인증하는 것을 포함하도록 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되는, 시스템.

청구항 21

제 20 항에 있어서,

상기 서버는,

상기 무선-가능 제품의 상기 제조업자로부터 수신된 상기 디바이스 시큐리티 키가 상기 서버가 시큐리티 토큰을 생성하기 위해 이용할 수 있는 정보를 포함하도록 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되

고; 그리고

저장된 상기 디바이스 시큐리티 키를 이용하여 수신된 상기 시큐리티 토큰을 인증하는 것은,

상기 무선-가능 제품의 상기 제조업자로부터 수신된 상기 디바이스 시큐리티 키를 이용하여 생성된 시큐리티 토큰을 획득하는 것; 및

상기 생성된 시큐리티 토큰과 수신된 상기 시큐리티 토큰을 비교하는 것을 포함하는, 시스템.

청구항 22

제 20 항에 있어서,

상기 서버는,

상기 무선-가능 제품의 상기 제조업자로부터 수신된 상기 디바이스 시큐리티 키가 제조업자-제공 시큐리티 토큰을 포함하도록 동작들을 수행하기 위한 프로세서-실행가능 명령들로 구성되고; 그리고

저장된 상기 디바이스 시큐리티 키를 이용하여 수신된 상기 시큐리티 토큰을 인증하는 것은 상기 제조업자-제공 시큐리티 토큰과 수신된 상기 시큐리티 토큰을 비교하는 것을 포함하는, 시스템.

청구항 23

제 19 항에 있어서,

상기 컴퓨팅 디바이스는, 상기 고객 ID 를 획득하는 것이 소매업자와 연관된 고객 로열티 데이터베이스로부터 상기 고객 ID 를 획득하는 것을 포함하도록 동작들을 수행하도록 구성되는, 시스템.

청구항 24

제 17 항에 있어서,

상기 무선-가능 제품은, 상기 서버에 대한 접속을 확립하는 것이 상기 고객의 사설 통신 네트워크에 대한 액세스 디바이스의 게스트 액세스 메커니즘을 통하여 상기 서버에 대한 상기 접속을 확립하는 것을 포함하도록 동작들을 수행하도록 구성되는, 시스템.

청구항 25

제 17 항에 있어서,

상기 무선-가능 제품은, 상기 서버에 대한 접속을 확립하는 것이 공중 네트워크를 통하여 상기 서버에 대한 상기 접속을 확립하는 것을 포함하도록 동작들을 수행하도록 구성되는, 시스템.

발명의 설명

기술 분야

배경 기술

[0001] 일반적인 고객 어플라이언스 (customer appliance) 들 및 전기 디바이스들은 스마트폰들에 의해 제어되는 스마트 홈들 및 조명 시스템을 제공하기 위해 무선 네트워크들에 접속하는 능력이 있다. 일반적인 전기 컴포넌트들 및 어플라이언스들을 네트워킹하는 것은 때때로 "사물 인터넷 (Internet of Things)" (IoT) 또는 "만물 인터넷 (Internet of Everything)" (IoE) 으로 지칭된다.

[0002] 보통의 어플라이언스들에 무선 접속성을 포함시키는 것 및 무선 네트워크들에 이러한 스마트 어플라이언스들을 통합시키는 것은 고객들에게 편의성 및 새로운 서비스들을 제공할 것이지만, 이러한 기술들의 광범위한 전개는 고객들에게 이러한 디바이스들을 구현 및 이용하는 방법을 배울 것을 요구할 것이다. 고객들이 네트워킹된 디바이스들을 구현하는 것에 저항할 수도 있는 하나의 이유는 고객의 사설 네트워크에 스마트 어플라이언스를 설치하는 인지된 어려움이다. 사설 무선 네트워크와 통신하기 위해 스마트 어플라이언스를 구성하는 프로세스는, 보안 통신 링크가 그 어플라이언스와 네트워크 간에 확립될 수 있도록 크리덴셜 (credential) 들을 교환

하는 것을 수반한다. 이 프로세스는 때때로 "온보딩 (onboarding)" 으로 지칭된다.

[0003]

고객들은 컴퓨터 또는 스마트 폰을 사설 무선 네트워크 (예를 들어, WiFi 네트워크) 에 접속하는 것에 점점 더 익숙해지지만, 디스플레이 및 사용자 인터페이스 (예를 들어, 키보드) 가 없는 어플라이언스들의 경우 온보딩 프로세스가 더 어려워진다. 디스플레이 및 편리한 사용자 인터페이스 없는 디바이스들은 때때로 "헤드리스 디바이스들 (headless devices)" 로 지칭된다. 헤드리스 디바이스들은 통상적으로 온보딩 프로세스를 완료하기 위해 다른 컴퓨팅 디바이스의 이용을 요구하여, 고객들에게, 다른 디바이스를 획득하거나 또는 그들이 이용하는 방법을 배워야 하는 온보드 애플리케이션으로 그들의 스마트폰 또는 다른 디바이스를 구성할 것을 요구한다. 따라서, 헤드리스 디바이스의 온보딩은 기술로 인해 불편한 고객들이 겁을 먹게 하거나 또는 불만스러워 하게 할 수 있다. 따라서, 사물 인터넷 디바이스들의 광범위한 전개를 인에이블하기 위해서는, 단순하고 편리한 설치 프로시저들이 바람직하다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0004]

다양한 실시형태들은 사설 통신 네트워크에 대한 무선-가능 제품 (wireless-enabled product) 의 접속을 촉진하기 위해 구성된 방법들, 디바이스들 및 시스템을 포함한다. 다양한 실시형태들은 구매 트랜잭션 (purchase transaction) 이전에 고객의 식별자 ("고객 ID") 및 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들을 서버에 저장하는 것을 포함할 수도 있다. 고객이 무선-가능 제품을 구매하는 구매 트랜잭션을 인에이블하는 동안에, 구매 트랜잭션을 인에이블하는 컴퓨팅 디바이스는 고객의 ID 및 무선-가능 제품과 연관된 디바이스 ID 를 획득하고, 고객 ID 및 디바이스 ID 를 서버에 제공할 수도 있다. 이 정보를 수신 시에, 서버는 서버에 의해 고객 ID 와 디바이스 ID 의 연관 (association) 을 저장할 수도 있다. 구매 트랜잭션 후 또는 동안의 언젠가 무선-가능 제품은 이를 태면 공중 네트워크를 통해, 서버에 대한 접속을 확립하고 메모리에 저장되는 디바이스 ID 및 시큐리티 토큰을 확립된 접속을 통하여 서버에 송신할 수도 있다. 이 정보를 수신 시에, 서버는 디바이스 ID 및 시큐리티 토큰에 기초하여 무선-가능 제품을 인증하고 무선-가능 제품을 인증하는 것에 응답하여 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들을 무선-가능 제품에 제공할 수도 있다. 무선-가능 제품은 그 후 서버에 대한 확립된 접속으로부터 접속해제하고, 사설 통신 네트워크에 대한 액세스 디바이스의 범위에 들어갈 때, 서버에 의해 제공된 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들을 이용하여 사설 통신 네트워크와 접속을 확립할 수도 있다.

[0005]

일부 실시형태들에서, 고객 ID 및 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들은 고객 정보가 입력되는 고객 등록 프로세스 동안에 서버에 의해 획득될 수도 있다. 일부 실시형태들에서, 고객 등록 프로세스는 고객 로열티 프로그램 (customer royalty program) 에 대한 사인 업 프로시저일 수도 있다. 일부 실시형태들에서, 구매 트랜잭션을 인에이블하는 컴퓨팅 디바이스는 소매업자와 연관된 고객 로열티 데이터베이스로부터 고객 ID 를 획득할 수도 있다.

[0006]

일부 실시형태들에서, 무선-가능 제품은 고객의 사설 통신 네트워크에 대한 액세스 디바이스의 게스트 액세스 메커니즘을 통하여 서버에 대한 접속을 확립할 수도 있다. 일부 실시형태들에서, 무선-가능 제품은 공중 네트워크를 통하여 서버에 대한 접속을 확립할 수도 있다.

[0007]

일부 실시형태들은 사설 통신 네트워크에 대한 무선-가능 제품의 접속을 촉진하기 위해 서버에서 구현되는 방법들을 포함할 수도 있다. 이러한 실시형태들에서, 서버는 고객의 식별자 ("고객 ID") 및 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들을 저장할 수도 있다. 서버는 무선-가능 제품과 연관된 디바이스 ID 및 무선-가능 제품을 구매하는 고객의 고객 ID 를 고객이 무선-가능 제품을 구매하는 구매 트랜잭션을 인에이블하는 컴퓨팅 디바이스로부터 수신할 수도 있다. 서버는 디바이스 ID 와의 고객 ID 의 연관을 저장할 수도 있다. 추후에, 서버는 디바이스 ID 및 시큐리티 토큰을 무선-가능 제품에 의해 개시된 네트워크 접속을 통하여 무선-가능 제품으로부터 수신할 수도 있다. 네트워크 접속은 고객의 사설 통신 네트워크에 대한 액세스 디바이스의 게스트 액세스 메커니즘을 통한 것이거나 또는 공중 네트워크를 통한 접속일 수도 있다. 서버는 수신된 디바이스 ID 및 시큐리티 토큰에 기초하여 무선-가능 제품을 인증하고, 무선-가능 제품을 인증하는 것에 응답하여 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들을 무선-가능

제품에 제공할 수도 있다. 일부 실시형태들에서, 고객 ID 및 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들은 고객 정보가 입력되는 고객 등록 프로세스 동안에, 이를 테면 고객 로열티 프로그램에 대한 사인 업 프로시저 동안에 서버에 의해 획득될 수도 있다.

[0008] 일부 실시형태들에서, 서버는 무선-가능 제품의 제조업자로부터 디바이스 ID 및 디바이스 시큐리티 키를 수신하고, 디바이스 시큐리티 키를 디바이스 ID 에 링크된 서버에 의해 액세스가능한 메모리에 저장할 수도 있다. 이러한 실시형태들에서, 서버는, 수신된 디바이스 ID 를 이용하여 메모리로부터의 디바이스 시큐리티 키에 액세스하는 것, 저장된 디바이스 시큐리티 키를 이용하여 수신된 시큐리티 토큰을 인증하는 것, 및 수신된 디바이스 ID 가 수신된 시큐리티 토큰을 인증하는 디바이스 시큐리티 키에 서버가 액세스하는 것을 인에이블하면 무선-가능 제품을 인증하는 것에 의해, 수신된 디바이스 ID 및 시큐리티 토큰에 기초하여 무선-가능 제품을 인증할 수도 있다. 일부 실시형태들에서, 무선-가능 제품의 제조업자로부터 수신된 디바이스 시큐리티 키는 서버가 시큐리티 토큰을 생성하기 위해 이용할 수 있는 정보일 수도 있고, 저장된 디바이스 시큐리티 키를 이용하여 수신된 시큐리티 토큰을 인증하는 것은, 무선-가능 제품의 제조업자로부터 수신된 디바이스 시큐리티 키를 이용하여 생성된 시큐리티 토큰을 획득하는 것, 및 생성된 시큐리티 토큰과 수신된 시큐리티 토큰을 비교하는 것을 포함할 수도 있다. 일부 실시형태들에서, 무선-가능 제품의 제조업자로부터 수신된 디바이스 시큐리티 키는 제조자-제공 시큐리티 토큰일 수도 있고, 저장된 디바이스 시큐리티 키를 이용하여 수신된 시큐리티 토큰을 인증하는 것은 제조업자-제공 시큐리티 토큰과 수신된 시큐리티 토큰을 비교하는 것을 포함할 수도 있다.

[0009] 일부 실시형태들은 상기 설명된 방법들의 여러 동작들을 수행하도록 구성된 서버를 포함한다. 일부 실시형태들은 상기 설명된 방법들의 무선-가능 디바이스 동작들을 수행하도록 구성된 무선-가능 디바이스를 포함한다. 일부 실시형태들은 서버, 무선-가능 디바이스, 고객의 사설 통신 네트워크를 지원하는 액세스 디바이스, 및 시스템 컴포넌트들의 각각이 상기 설명된 방법들의 개별의 동작들을 수행하도록 구성되는 구매 트랜잭션을 지원하도록 인에이블되도록 구성된 컴퓨팅 디바이스로 이루어진 시스템을 포함한다.

도면의 간단한 설명

[0010] 본 명세서에 통합되고 본 명세서의 일부를 구성하는 첨부 도면들은, 예시적인 실시형태들을 예시하고, 상기 주어진 일반적인 설명 및 이하에 주어진 상세한 설명과 함께, 본 발명의 피처들을 설명하도록 기능한다.

도 1a 는 다양한 실시형태들을 구현하기 위한 예의 컴포넌트들 및 통신 경로들을 예시하는 통신 네트워크 다이어그램이다.

도 1b 는 다양한 실시형태들을 구현하기 위한 다양한 디바이스들 간의 상이한 통신 경로들을 예시하는 통신 네트워크 다이어그램이다.

도 2 는 다양한 실시형태들에의 이용에 적합한 일 예의 무선-가능 제품 또는 어플라이언스의 컴포넌트들을 예시하는 블록 다이어그램이다.

도 3a 는 다양한 실시형태들에 따른 디바이스 ID 를 무선-가능 제품에 매정하는 것과 연관된 메시지 플로우들을 예시하는 메시지 플로우 다이어그램이다.

도 3b 는 다양한 실시형태들에 따른 고객 정보의 등록과 연관된 메시지 플로우들을 예시하는 메시지 플로우 다이어그램이다.

도 3c 는 다양한 실시형태들에 따른 트랜잭션 동안에 획득된 고객 ID 및 디바이스 ID 를 제공하는 것과 연관된 메시지 플로우들을 예시하는 메시지 플로우 다이어그램이다.

도 3d 는 다양한 실시형태들에 따른 무선-가능 제품을 인증하는 것 및 무선-가능 제품에 의해 사설 네트워크에 액세스하기 위한 정보를 획득하는 것과 연관된 메시지 플로우들을 예시하는 메시지 플로우 다이어그램이다.

도 3e 는 다양한 실시형태들에 따른 사설 네트워크에 액세스하기 위한 정보를 이용하여 무선-가능 제품에 의해 사설 네트워크에 액세스하는 것과 연관된 메시지 플로우들을 예시하는 메시지 플로우 다이어그램이다.

도 4 는 다양한 실시형태들에 따른 무선-가능 제품에 대해 사설 통신 네트워크에 대한 액세스를 제공하는 시스템에 대한 일 실시형태 방법을 예시하는 프로세스 플로우 다이어그램이다.

도 5 는 다양한 실시형태들에 따른 무선-가능 제품에 의해 사설 네트워크에 액세스하기 위한 일 실시형태 방법을 예시하는 프로세스 플로우 다이어그램이다.

도 6 은 다양한 실시형태들에 따른 무선-가능 제품을 구매하기 위한 트랜잭션 동안에 포스 (point-of-sale) 디바이스에서 구현될 수도 있는 방법을 예시하는 프로세스 플로우 다이어그램이다.

도 7 은 다양한 실시형태들에 따른 서버에서 구현되는 무선-가능 제품의 자동 온보딩을 지원하기 위한 방법을 예시하는 프로세스 플로우 다이어그램이다.

도 8 은 다양한 실시형태들에 따른 이용에 적합한 일 예의 서버를 예시하는 컴포넌트 다이어그램이다.

발명을 실시하기 위한 구체적인 내용

- [0011] 다양한 실시형태들이 첨부 도면들을 참조하여 상세히 설명될 것이다. 가능하면 언제나, 동일하거나 또는 유사한 부분들을 지칭하기 위해 동일한 참조 번호들이 도면들 전반에 걸쳐 사용될 것이다. 특정한 예들 및 구현들에 대해 이루어진 참조들은 예시적인 목적들을 위한 것이며 본 발명 또는 청구항들의 범위를 제한하도록 의도되지 않는다.
- [0012] 다양한 실시형태들은 무선-가능 제품들 및 어플라이언스들의 온보딩을 촉진하기 위한 시스템들 및 방법들을 제공하여, 이러한 스마트 디바이스들이 고객에 의한 디바이스의 구매 후에 고객의 무선 네트워크에 접속하도록 그것들 자체를 본질적으로 구성하는 것을 인에이블한다. 다양한 실시형태들은 헤드리스 디바이스들을 고객 네트워크 크리덴셜들에 상관시키는 것, 및 고객의 네트워크 크리덴셜들을 다운로드하기 전에 헤드리스 디바이스를 인증하는 것을 인에이블하는 서버에 유지된 데이터베이스들을 레버리징한다. 고객들은 고객 식별자 ("고객 ID") 및 고객의 무선 네트워크에 액세스하기 위한 크리덴셜들을 제공하는 서버에 한번 등록할 수도 있다. 고객이 무선-가능 제품 또는 어플라이언스를 구매할 때, 그 제품의 식별자 ("제품 ID") 및 고객의 ID 가 서버로 포워딩된다. 서버는 이 정보를 이용하여 적합한 데이터베이스에서 제품 ID 를 고객 ID 에 상관시킨다. 추후에, 무선-가능 제품 또는 어플라이언스가 오픈 인터넷 접속을 통해 서버에 액세스할 때, 그 제품 또는 어플라이언스는 그 제품 ID 및 고유 토큰을 서버로 전송한다. 서버는 제품 ID 를 이용하여 제품에 대한 대응하는 토큰 또는 인증 크리덴셜을 록업하고, 수신된 토큰에 기초하여 제품을 인증한다. 일단 인증되면, 서버는 상관된 고객 ID 를 이용하여 고객의 사설 네트워크에 대한 네트워크 크리덴셜들을 록업하고, 그 크리덴셜들을 무선-가능 제품 또는 어플라이언스로 다운로드한다. 무선-가능 제품 또는 어플라이언스는 그 후 다운로드된 크리덴셜들을 이용하여 고객의 사설 네트워크에 액세스한다.
- [0013] 단어 "예시적인" 은 본 명세서에서 "일 예, 인스턴스, 또는 예시로서 기능하는 것" 을 의미하는데 사용된다. 본 명세서에서 "예시적인" 으로서 설명된 임의의 구현이 반드시 다른 구현들에 비해 유리하거나 또는 선호되는 것으로 해석될 필요는 없다.
- [0014] 용어 "컴퓨팅 디바이스" 는 본 명세서에서 사물 인터넷 (IoT) 디바이스들, 스마트 홈 디바이스들, 스마트 어플라이언스들, 스마트 유틸리티 미터들 (가스, 전기 등), 스마트 파킹 미터들, 셀룰러 전화기들, 스마트 폰들, 개인 또는 모바일 멀티-미디어 플레이어들, PDA (personal data assistant) 들, 랩톱 컴퓨터들, 데스크톱 컴퓨터들, 태블릿 컴퓨터들, 스마트 복들, 팜-톱 컴퓨터들, 무선 전자 메일 수신기들, 멀티미디어 인터넷 가능 셀룰러 전화기들, 텔레비전들, 스마트 TV들, 스마트 TV 셋-톱 버디 박스들, 통합된 스마트 TV들, 스트리밍 미디어 플레이어들, 스마트 케이블 박스들, 셋-톱 박스들, 디지털 비디오 레코더들 (DVR), 디지털 미디어 플레이어들, 및 프로그래밍가능 프로세서를 포함하는 유사한 개인 전자 디바이스들, 특히 SoC 를 포함하는 것들 중 임의의 하나 또는 전부를 지칭하는데 사용된다.
- [0015] 무선-가능 제품들을 의도된 네트워크에 용이하게 접속할 수 없음은 고객을 위한 열악한 OOB (out-of-box experience) 또는 리턴된 제품들을 야기한다. 매장에서는 또는 온라인/배달로든, 통상의 소매 구매 프레임워크를 고려해 볼 때, 제조업자들 및 소매업자들은, 일단 디바이스가 구매되고, 집으로 가져가거나 또는 배달되고, 개봉되면, 고객의 네트워크에 Wi-Fi 디바이스들을 온보딩하는 것에 중점을 둔 신뢰성 및/또는 복잡성 이슈들로 고심한다. 소매업자 및 제조업자는, 적어도 초기에, 고객과의 관계 및 상호작용의 레벨에 있어서 제한되기 때문에, 고객의 초기 제품 경험이 일관되게 좋은 것을 보장할 필요가 있을 수도 있는 종류의 기술 지원을 제공하기가 어렵다.
- [0016] 직접 구매 시에 또는 무선-가능 제품 또는 어플라이언스의 선적물 (shipment) 의 수령 시에, 일단 박스가 개봉되고 활성화가 시도되면 고객이 그 제품을 적절히 활성화 및 설치할 수 있음을 보장할 방법이 없다. 게다가, 디바이스 활성화는 처음에 정확히 행해진다면 종종 가장 성공적이고 가장 적게 불만스럽다. 고객이 집에서 인터넷에 액세스하였다 하더라도, 디바이스의 초기 활성화는 다루기 힘들 수 있고 그것이 성공적일 것이고 디바이스가 작동할 것이라는 보장 없이, 활성화를 완료하기 위해 여러 인가 및 온-오프 사이클들을 요구할

수도 있다. 이것은 고객 불만 및 전반적인 열악한 고객 경험을 야기할 수 있다.

- [0017] 다양한 실시형태들은 사설 무선 네트워크 (예를 들어, 홈 또는 커머셜 WiFi 네트워크) 에 접속하도록 구매된 디바이스들을 구성하기 위한 자동화된 프로세스를 제공하는 것에 의해 현재의 온보딩 메커니즘들의 결점들을 다루고 극복한다. 다양한 실시형태들에서, 무선-가능 제품은 구매 또는 선적 시에 고객과 연관될 수 있고, 따라서 고객은 디바이스가 고객의 사설 네트워크로 온보딩되게 (즉, 그 고객의 사설 네트워크에 접속되고 그와 통합되게) 하기 위하여 그 디바이스와 추가로 상호작용할 필요가 없다.
- [0018] 도 1a 는 다양한 실시형태들을 구현하기 위한 시스템 (100) 으로서 기능할 수도 있는 다양한 컴퓨팅 디바이스들 및 네트워크들을 예시한다. 다양한 실시형태들은 사설 무선 네트워크 (130) 로의 무선-가능 제품들 (120a 내지 120d) 의 온보딩을 촉진한다. 사설 무선 네트워크 (130) 는 다수의 무선-가능 제품들 (120b 내지 120d) 과 무선 접속들 (121) 을 확립하는 액세스 포인트 (140) 주변에 구축되거나 또는 그에 의해 촉진될 수도 있다. 무선-가능 제품들 (120b 내지 120d) 은 IoT 디바이스들, 이를 태면 스마트 백열 전구들, 네트워크-가능 어플라이언스들, 및 네트워킹된 홈 또는 오피스 시스템들일 수도 있다. 액세스 포인트 (140) 는 유선 또는 무선 접속일 수도 있는 접속 (141) 을 통하여 인터넷과 같은 공중 네트워크 (151) 에 대한 접속을 제공할 수도 있다.
- [0019] 다양한 실시형태들에서, 제품 제조업자들 (157), 서버 (150), 및 소매업자 포스 (point-of-sale) 디바이스 (155) 는 무선-가능 제품들 (120a 내지 120d) 의 자동 온보딩을 인에이블하기 위해 네트워크 (151) 를 통해 함께 작동할 수도 있다. 무선-가능 제품 (120a) 의 제조업자 (157) 는 제품 제조 동안에, 이를 태면 최종 테스트 및 구성 동안에 또는 선적을 위해 제품을 준비하면서 메모리에 저장되는 제품 ID 및 시큐리티 토큰으로 제품을 구성할 수도 있다. 제품 ID 는 유사한 제품들의 팝플레이션 내에 고유할 수도 있거나 또는 제품 시리얼 넘버, MAC ID, 또는 다른 고유 식별자와 같이, 글로벌로 고유할 수도 있다. 비휘발성 메모리에 제품 ID 를 저장하는 것에 더하여, 제품 ID 는 제품 라벨 상에 및/또는 패키징 상에 인쇄될 수도 있거나, 바 코드로 인코딩될 수도 있거나, RFID 태그에 저장될 수도 있거나, 또는 다르게는 포스에서 판독될 수 있는 방식으로 패키징된 제품 상에 제공될 수도 있다. 메모리에 저장되는 시큐리티 토큰은 추측 또는 타협될 가능성을 감소시키기 위해 충분한 디지트 (digit) 들의 고유 값일 수도 있다. 무선-가능 제품 (120a) 을 구성하는 것에 더하여, 제조업자 (157) 는 이를 태면, 인터넷 (151) 을 통해, 서버 (150) 에 디바이스 ID 및 시큐리티 토큰 (메시지 (158)) 을 통신할 수도 있다.
- [0020] 서버 (150) 는 무선-가능 제품에 네트워크 크리덴셜들을 자동으로 제공하는 서비스를 제공하고, 따라서 이러한 기능들을 수행하기에 충분한 데이터베이스들 및 네트워크 능력들로 구성될 수도 있다. 서버 (150) 는 제조업자 (157) 와 연관될 수도 있거나, 소매업자에 의해 제공될 수도 있거나, 또는 제 3 자에 의해 독립적인 서비스로서 제공될 수도 있다. 서버 (150) 는 각각의 무선-가능 제품에 대해 제조업자 (157) 에 의해 제공된 디바이스 ID 및 시큐리티 토큰을 수신한다. 이 정보는, 디바이스 ID 를 제공할 때 대응하는 시큐리티 토큰을 서버가 발견하는 것을 인에이블하는 임의의 타입의 것일 수도 있는 데이터베이스에 저장될 수도 있다.
- [0021] 소매업자 포스 (POS) 디바이스 (155) 는 무선-가능 제품들에 대한 구매 트랜잭션들을 지원하는데 이용될 수도 있는 다양한 포스 컴퓨팅 시스템들 중 임의의 것일 수도 있다. 예를 들어, 소매업자 포스 디바이스 (155) 는 온라인 소매업자 (online retailer) 에서의 서버, 또는 오프라인 거래의 소매업자의 계산대에 있는 컴퓨터, 개인이 휴대하는 휴대용 트랜잭션 단말기 등일 수도 있다. 소매업자 POS 디바이스 (155) 는 구매 트랜잭션 동안에 정보가 서버 (150) 에 전달될 수 있는 네트워크 (151) (예를 들어, 인터넷) 에 대한 접속 (156) 을 포함한다. 아래에 더 상세히 설명되는 바와 같이, 트랜잭션 동안에 획득되고 서버 (150) 에 전달될 수도 있는 정보는 통상적으로 구매되는 무선-가능 제품의 디바이스 ID 뿐만 아니라 고객 ID 를 포함할 것이다.
- [0022] 다양한 실시형태들에 따른 무선-가능 제품 (120a 내지 120d) 을 온보딩하는 프로세스는 그것이 사설 네트워크 (130) 에 접속할 수 있기 전에 네트워크 크리덴셜들을 수신하기 위하여 공중 네트워크 (예를 들어, 인터넷 (151)) 를 통해 서버 (150) 에 액세스하는 무선-가능 제품들 (120a 내지 120d) 을 포함한다. 인터넷 (151) 에 액세스하는 것은 인터넷 (151) 에의 액세스를 제공하는 공중 네트워크 액세스 포인트 (160) 에 대한 무선 접속 (162) 을 통해 달성될 수도 있다. 서버 (150) 에의 액세스는 또한, 고객의 소유 네트워크 (130) 내의 액세스 포인트 (140) 에 의해 제공된 게스트 네트워크를 통해 달성될 수도 있다.
- [0023] 추가적으로, 고객들은 그들 자신을 서버 (150) 에 등록하기 위해 다양한 컴퓨터들 (165) 중 임의의 것을 이용할 수도 있다. 아래에 설명한 바와 같이, 이 등록은 고객의 사설 네트워크 (130) 에 접속하기 위하여 고객 ID 를 제공 또는 수신하는 것 및 무선 가능 제품들이 요구하는 네트워크 크리덴셜들 및 다른 정보를 제공하는 것을

수반할 수도 있다. 고객 등록은 사설 네트워크를 처음 셋업하기 전에 액세스 포인트 디바이스의 구매 동안 또는 고객 로열티 프로그램에 대해 사인 업하면서와 같이 소매업자 컴퓨터 (예를 들어, POS 디바이스) 를 이용하여, 고객의 소유 컴퓨터 (165) 를 이용한 웹사이트 등록을 통해 달성될 수도 있다. 일부 실시형태들에서, 동일한 제조업자로부터의 액세스 포인트 및 무선-가능 제품은 소매업자에 함께 구매될 수도 있다. 이러한 일 예에서, 액세스 포인트의 네트워크 크리덴셜들은 무선-가능 제품으로 사전-프로그래밍될 수도 있거나, 또는 네트워크 액세스 정보를 고객이 제공할 필요성 없이 서버 (150) 에 사전에 저장될 수도 있다.

[0024] 도 1b 는 다양한 실시형태들에 따른 온보딩 프로세스를 완료하는 다양한 동작들 동안의 시스템 (100) 엘리먼트들의 상호작용들을 예시한다.

[0025] 제조 동안에, 제품 제조업자 (157) 는 시큐리티 토큰 및 디바이스 ID 를 무선-가능 제품 또는 어플라이언스 (120) 의 비휘발성 메모리로 저장할 수도 있다. 추가적으로, 제품 제조업자 (157) 는 무선-가능 제품 또는 어플라이언스의 추후 인증을 인에이블하기 위해 서버에 유지되거나 또는 그 서버에 액세스가능한 데이터베이스에 레코딩하기 위해 시큐리티 토큰 및 디바이스 ID 를 서버 (150) 에 제공할 수도 있다.

[0026] 구매 이전 또는 구매 동안의 엔진가, 고객 (140) 은 자동 온보딩을 위해 서버 (150) 에 등록한다 (통신 1). 이 원-타임 (one-time) 등록 동안에, 고객은 다양한 무선-가능 제품들 또는 어플라이언스들이 온보딩될 고객의 사설 무선 네트워크에 액세스하기 위한 크리덴셜들 및 구성 정보 (일반적으로 본 명세서에서 "네트워크 크리덴셜들" 로 지칭됨) 를 서버에 제공한다. 등록 프로세스의 일부로서, 고객 (140) 은 고객 ID 를 입력하거나 또는 그 고객 ID 를 제공받을 수도 있고, 서버는 고객 ID 를 링크한 데이터베이스에 네트워크 크리덴셜들을 저장할 수도 있다. 등록 프로세스는 소매업자, 제조업자, 또는 다른 엔티티에 대한 로열티 프로그램 사인 업 프로시저의 일부로서, 또는 다른 등록 프랙티스들에 의해, 포스에서, 웹사이트 등록을 통해 달성될 수도 있다. 일부 경우들에서, 등록은 고객의 사설 무선 네트워크의 근거를 제공할 무선 액세스 포인트의 구매 동안에 달성될 수도 있다. 따라서, 고객 (140) 은 고객의 사설 네트워크에 통합되도록 무선-가능 제품들 또는 어플라이언스들에 필요한 정보를 서버에 제공한다.

[0027] 구매 시에, 소매업자는, 이를 테면 바코드를 스캔하는 것, 라벨에 인쇄된 것을 포스 컴퓨터로 타이핑하는 것, 또는 NFC (near field communication) 또는 RFID (radiofrequency identifier) 로부터 디바이스 ID 를 무선으로 수신하는 것에 의해, 어플라이언스, 디바이스 또는 다른 무선-가능 제품 (120) 에 대한 디바이스 ID 를 획득할 수도 있다. 또한, 구매 시에, 소매업자는 고객 (140) 의 고객 ID 를 획득할 수도 있다. 고객 ID 는 소매업자의 로열티 카드 (또는 다른 식별 메커니즘) 를 스캔하는 것, 고객이 식별자를 키패드로 타이핑하는 것을 인에이블하는 것에 의해, 또는 고객의 스마트폰과의 NFC 통신을 통해 무선으로 획득될 수도 있다. 온-라인 구매들 동안, 고객은 트랜잭션을 완료하는 것의 일부로서 그/그녀의 고객 ID 를 입력하도록 요구될 수도 있다. 구매 트랜잭션을 완료하는 것의 일부로서, 소매업자는 획득된 디바이스 ID 및 고객 ID 를 서버로 전송한다 (통신 2). 서버는 그 후 디바이스 ID 를 데이터베이스에서 고객 ID 과 상관시킨다 (예를 들어, 2 개의 식별자들을 링크하거나, 새로운 데이터베이스를 생성하거나, 또는 식별자들 중 하나를 다른 식별자에 키잉된 데이터베이스 추가함).

[0028] 고객 (140) 이 구매한 무선-가능 제품 또는 어플라이언스를 받으면, 고객은 무선-가능 제품을 파워 온하고 무선-가능 제품이 오픈 네트워크 (예를 들어, 게스트 네트워크 또는 공중 WiFi 액세스 포인트) 를 통해 인터넷에 접속하는 것을 인에이블한다. 인터넷에 접속 시, 무선-가능 제품은 서버에 액세스 및 등록하여 (통신 3), 제조 시에 메모리에 로드된 디바이스 ID 및 시큐리티 토큰을 제공한다. 서버는 데이터베이스에 대응하는 레코드를 로케이트하기 위해 디바이스 ID 를 이용하고 수신된 시큐리티 토큰과 데이터베이스에 저장된 시큐리티 토큰을 비교하는 것과 같이, 다양한 인증 메커니즘들 중 임의의 것을 이용하여 디바이스 ID 및 시큐리티 토큰에 기초하여 무선-가능 제품을 인증한다. 일부 실시형태들에서, 시큐리티 토큰은 무선-가능 제품 및 서버가 암호화된 통신 프로토콜을 통해 통신하는 것을 인에이블하는 공유 키를 포함할 수도 있다. 적절한 키 없이는, 무선-가능 제품은 서버와 통신할 수 없다.

[0029] 일단 무선-가능 제품이 서버에 의해 인증되면, 서버는 디바이스 ID 에 상관된 고객 ID 를 이용하여 고객 등록 프로세스 동안에 저장된 고객의 네트워크 크리덴셜들에 액세스할 수도 있다. 서버는 확립된 인터넷 접속을 이용하여 고객의 네트워크 크리덴셜들 및 다른 정보 (액세스 포인트 SSID 등) 를 무선-가능 제품에 다운로드 또는 다르게는 제공할 수도 있다 (통신 4). 무선-가능 제품은 그 정보를 메모리 (예를 들어, 비휘발성 메모리) 에 저장할 수도 있다. 다운로드 프로세스 동안에, 서버는 또한, 크리덴셜들이 정확히 다운로드 및 레코딩되었음을 확인하는 것, 다양한 통신 파라미터들을 구성하도록 제품을 다이렉팅하는 것, 및 다르게는 제품

이 고객의 사설 네트워크에 접속하는 것을 인에이블하는 것과 같이, 온보딩 프로세스를 촉진하기 위한 커맨드들을 무선-가능 제품으로 전송할 수도 있다.

[0030] 일단 네트워크 크리덴셜들이 다운로드되었고 무선-가능 제품이 고객의 사설 네트워크를 위해 구성되면, 무선-가능 제품은 공중 네트워크로부터 접속해제하고 수신된 네트워크 크리덴셜들을 이용하여 고객의 사설 네트워크 (130) 에 접속하려고 시도할 수도 있다 (통신 5). 사실 네트워크 (130) 의 액세스 포인트 (140) 및 무선-가능 제품 (120) 은 서버로부터 수신된 네트워크 크리덴셜들을 이용하여 자동으로 온보딩 프로세스를 완료할 수도 있다. 따라서, 다양한 실시형태들은 서버에의 사전의 원-타임 등록을 제외한 고객 (140) 측의 어떤 노력 없이도 무선-가능 제품이 고객의 사설 무선 네트워크 (130) 에 온보딩되는 것을 인에이블한다 (통신 1).

[0031] 도 2 는 다양한 실시형태들에의 이용에 적합한 통상의 무선-가능 제품 (120) 의 다양한 컴포넌트들을 예시한다. 다양한 전기 디바이스들 (예를 들어, 백열 전구들) 및 어플라이언스들 (예를 들어, 토스터들, 냉장고들 등) 중 임의의 것은 디바이스 내에 무선 인터페이스 (210) 를 포함하는 것에 의해 무선 능력을 갖추고 있을 수도 있다. 이러한 무선 인터페이스 (210) 는 디바이스의 전력 공급을 무선 인터페이스 (210) 에 적합한 형태 및 전압으로 컨버팅하도록 구성된 회로와 같은 전력 공급기 (211) 를 포함할 수도 있다. 무선 인터페이스 (210) 는 버스 (219) 를 통해 메모리 (213), 디지털 신호 프로세서 (DSP) (214), 모뎀 (215) 및 트랜시버 (216), 제어 인터페이스 (218), 다른 컴포넌트들 (미도시) 에 커플링될 수도 있는 중앙 프로세서 유닛 (CPU) (212) 을 포함할 수도 있다. CPU (212) 는 전반적인 동작들 및 통신들을 제어할 수도 있다. 모뎀 (215) 및 트랜시버 (216) 는 안테나 (217) 로부터의 무선 송신들을 통해 고객의 사설 네트워크 (130) 와 통신할 수도 있다. 제어 인터페이스 (218) 는 스마트 백열 전구에 의해 생성된 빛의 양을 제어하기 위한 가감저항기 또는 스위치와 같은, 디바이스 또는 어플라이언스 (120) 를 제어하기 위한 회로부를 포함할 수도 있다. 일부 구현들에서, 210 에서의 무선 인터페이스는 SoC (system-on-a-chip) 로서 구현될 수도 있다.

[0032] 도 3a 내지 도 3e 는 다양한 실시형태들을 구현하기 위해 시스템 (100) 과 컴포넌트들 및 컴퓨팅 디바이스들 간에 교환된 다양한 통신들을 예시한다. 도 3a 를 참조하면, 디바이스 ID 및 시큐리티 토큰은 다수의 상이한 프로세스들을 통해 무선-가능 제품 (120) 에 생성 및 업로드되거나 또는 다르게는 제공될 수도 있다. 예를 들어, 제조업자 (157) 는 통신 (311) 에서 디바이스 ID 및 시큐리티 토큰을 서버 (150) 에 제공할 수도 있고, 서버는 통신 (313) 에서 디바이스 ID 및 시큐리티 토큰을 무선-가능 제품 (120) 에 제공할 수도 있다. 다른 예로서, 제조업자 (157) 는 통신 (315) 에서 디바이스 ID 및 시큐리티 토큰을 무선-가능 제품 (120) 에 저장할 수도 있고 통신 (311) 에서 디바이스 ID 및 시큐리티 토큰을 서버 (150) 에 알릴 수도 있다. 추가의 예에서, 제조업자 (157) 는 통신 (315) 에서 디바이스 ID 및 시큐리티 토큰을 무선-가능 제품 (120) 에 저장할 수도 있고, 무선-가능 제품 (120) 은 통신 (317) 에서 디바이스 ID 및 시큐리티 토큰을 서버 (150) 에 제공할 수도 있다.

[0033] 도 3b 는 고객 (140) 을 서버 (150) 에 등록하는데 있어서 수반되는 예의 통신들을 예시한다. 일부 인스턴스들에서, 고객 (140) 은 컴퓨팅 디바이스 (예를 들어, 고객의 컴퓨터 (165)) 에 의해 액세스되는 웹사이트 (318) 를 통해 서버 (150) 에 액세스할 수도 있다. 웹사이트 (318) 와 상호작용하는 것을 통하여, 고객 (140) 은 통신 (319) 에서 서버에의 등록을 개시할 수도 있다. 이 등록 프로세스는 또한 소매업자 또는 제조업자 고객 로열티 프로그램에 등록하는 것의 일부로서 달성될 수도 있다. 서버 (150) 는 통신 (321) 에서 고객 ID 를 생성하고 그 고객 ID 를 고객 (140) 에게 제공할 수도 있다. 서버는 또한 동작 (323) 에서 고객 ID 및 데이터베이스를 저장할 수도 있다.

[0034] 등록 프로세스의 일부로서, 고객 (140) 은 통신 (325) 에서 고객의 사설 네트워크에 액세스하는데 필요한 네트워크 크리덴셜들 및 다른 정보를 제공할 수도 있다. 사실 네트워크에 액세스하기 위한 정보의 제공은 사실 네트워크의 명칭 및/또는 SSID, 및 패스워드 또는 암호화 키 (본 명세서에서 네트워크 크리덴셜들로 일괄적으로 지칭됨) 를 제공하는 것을 포함할 수도 있다. 고객 등록이 네트워크 액세스 포인트를 구매하는 것의 일부로서 달성되고 있는 인스턴스들에서, 사실 네트워크의 명칭 및 패스워드/암호화 키를 생성하는 것은 포스에서의 구매 트랜잭션의 일부로서 달성될 수도 있다. 서버는 동작 (327) 에서 사실 네트워크에 액세스하기 위한 정보를 저장할 수도 있다. 등록 프로세스가 완료되면, 서버는 등록이 성공적으로 완료되었다는 것을 확인하는 메시지 (329) 를 전송할 수도 있다. 서버 (150) 에의 등록이 고객 로열티 프로그램의 일부인 인스턴스들에서, 로열티 프로그램과 연관된 추가의 통신들이 후속될 수도 있다.

[0035] 도 3c 는 무선-가능 제품 (120) 에 대한 구매 트랜잭션 동안에 포스 컴퓨팅 디바이스, 이를 테면 소매업자 포스 디바이스 (155) 로부터 서버 (150) 로의 통신들을 예시한다. 그 트랜잭션 동안에, 소매업자는 디바이스 ID

및 고객 ID 를 획득하고, 이 정보를 통신 (333) 에서 서버 (150) 에, 이를 테면 인터넷을 통해, 제조업자와의 사설 접속, 또는 다른 접속을 통해 송신한다. 상기 언급한 바와 같이, 소매업자 포스 디바이스 (155) 는 제품 패키지 상의 바코드를 스캔하는 것, 제품 패키지 상에 인쇄된 코드를 포스 컴퓨팅 디바이스, 즉 소매 포스 디바이스 (155) 로 입력하는 것, RFID 태그를 판독하거나 또는 포스 컴퓨팅 디바이스, 즉 소매 포스 디바이스 (155) 에 포함된 RFID 또는 NFC 리더를 이용하여 제품 패키지에 임베딩된 NFC 디바이스를 스캔하는 것, 또는 다른 메커니즘에 의해 디바이스 ID 를 획득할 수도 있다. 소매업자는 고객 로열티 카드를 스캔하는 것, 고객 번호, 전화 번호 또는 다른 정보에 의해 데이터베이스에서 고객을 특업하는 것, 고객이 키패드로 ID 를 입력하게 하는 것, 또는 다른 메커니즘에 의해 고객 ID 를 획득할 수도 있다.

[0036] 도 3d 는 무선-가능 제품 (120) 을 인증하는 것 및 네트워크 액세스 정보를 제공하는 것에서 수반되는 통신들 및 프로세스들을 예시한다. 무선-가능 제품 (120) 이 고객의 사설 네트워크 액세스 포인트 (140) 의 범위 내에서 파워 온될 때, 그 제품은 오픈 네트워크 접속을 발견하려고 시도할 수도 있거나 또는 통신 (341) 에서 게스트 로그인을 요청할 수도 있다. 액세스 포인트 (140) 는 통신 (343) 에서 로그인 요청을 승인할 수도 있고, 무선-가능 제품 (120) 은 액세스 포인트 (140) 를 이용하여 서버 (150) 에 액세스하고 통신 (345) 에서 제품의 디바이스 ID 및 시큐리티 토큰을 서버 (150) 에 제공한다. 서버 (150) 는 동작 (347) 에서 디바이스 ID 및 시큐리티 토큰을 이용하여 제품이 인증되는지 여부를 결정할 수도 있다. 서버 (150) 가 무선-가능 제품 (120) 이 인증되지 않는다고 결정하면, 서버 (150) 는 액세스 거부 통신 (348) 을 무선-가능 제품 (120) 으로 전송할 수도 있다. 서버 (150) 가 무선-가능 제품 (120) 을 인증하면, 서버 (150) 는 통신 (349) 에서 고객의 사설 네트워크에 액세스하기 위한 네트워크 크리덴셜들 및 다른 정보를 무선-가능 제품으로 전송할 수도 있다.

[0037] 도 3e 는 사설 네트워크 (130) 에 액세스하는 무선-가능 제품 (120) 에서 수반되는 통신들을 예시한다. 통신 (351) 에서, 무선-가능 제품 (120) 은 서버 (150) 에 의해 제공된 네트워크에 액세스하기 위한 정보 (네트워크 크리덴셜들) 를 이용하여 로그인 요청을 사설 네트워크 액세스 포인트 (140) 로 전송할 수도 있다. 결정 블록 (352) 에서, 사설 네트워크 액세스 포인트 (140) 의 프로세서는 네트워크에 액세스하기 위한 정보가 정확한지 여부를 결정할 수도 있다. 사설 네트워크에 액세스하기 위한 정보가 정확하다고 결정하는 것 (즉, 결정 블록 (352) = "예") 에 응답하여, 사설 네트워크 액세스 포인트 (140) 의 프로세서는 통신 (353) 에서 사설 네트워크 로그인 요청을 승인하고 무선-가능 제품 (120) 과 보안 통신 링크를 확립할 수도 있다. 이 확립된 통신 링크를 이용하면, 무선-가능 제품 (120) 및 액세스 포인트 (140) 는 제어 커맨드들, 동작 스테이터스 등과 같은 통신들 (355) 을 사설 인터넷 네트워크의 일부로서 교환할 수도 있다. 사설 네트워크에 액세스하기 위한 정보가 정확하지 않다고 결정하는 것 (즉, 결정 블록 (352) = "아니오") 에 응답하여, 사설 네트워크 액세스 포인트 (140) 의 프로세서는 통신 (357) 에서 사설 네트워크에 대한 액세스를 거부할 수도 있다.

[0038] 도 4 는 다양한 실시형태들에 따른 무선-가능 제품의 온보딩을 자동화하기 위한 방법 (401) 을 예시한다. 도 1a 내지 도 4 를 참조하면, 방법 (401) 의 동작들은 상기 설명한 바와 같이 무선-가능 제품 (120), 서버 (150), 및 포스 컴퓨팅 디바이스, 즉 소매 포스 디바이스 (155) 에 의해 수행될 수도 있다.

[0039] 블록 (409) 에서, 고객은 서버에 등록하여 그 서버에 네트워크 액세스 크리덴셜들 및 관련 정보를 제공하고 고객 ID 를 수신할 수도 있다. 상기 설명한 바와 같이, 이러한 서버에의 고객의 등록은 고객 로열티 등록 프로세서의 일부로서, 네트워크 액세스 포인트의 구매의 일부로서, 고객이 웹사이트에 액세스하고 등록 폼을 작성하는 것에 의해, 또는 다른 프로세스에 의해 달성될 수도 있다. 이 등록의 일부로서, 블록 (409) 에서 네트워크 액세스 크리덴셜들 및 관련 정보를, 고객이 제공할 수도 있고 서버는 고객 ID 프로세스에 링크된 데이터베이스에 저장할 수도 있다. 고객이 무선-가능 디바이스와 함께 액세스 포인트를 구매할 때, 서버는 이미 네트워크 액세스 크리덴셜들을 저장했을 수도 있다.

[0040] 블록 (411) 에서, 소매업자 포스 디바이스는 고객이 제품을 구매하는 트랜잭션 동안에 무선-가능 제품의 디바이스 ID 를 획득할 수도 있다. 블록 (413) 에서, 소매업자 포스 디바이스는 그 트랜잭션의 일부로서 고객 ID 를 획득할 수도 있다. 블록 (415) 에서, 포스 디바이스는 고객 ID 및 디바이스 ID 를 서버에 제공할 수도 있다.

[0041] 블록 (417) 에서, 서버는, 이를 테면 고객 ID 및 디바이스 ID 를 트랜잭션 데이터베이스에 저장하는 것, 또는 상관관계를 표시하기 위해 고객의 ID들의 데이터베이스 또는 디바이스 ID들의 데이터베이스 중 어느 하나를 업데이트하는 것에 의해, 수신된 고객 ID 및 디바이스 ID 를 데이터베이스에서 연관시킬 수도 있다.

[0042] 트랜잭션이 완료된 잠시 후에, 무선-가능 제품은 파워 온되고 블록 (419) 에서 공중 네트워크를 통해 제품과 서

버 간에 접속을 확립할 수도 있다. 블록 (421) 에서, 무선-가능 제품은 제품이 제조된 때 메모리에 저장된 디바이스 ID 및 시큐리티 토큰을 제공하는 것에 의해 확립된 인터넷 접속을 통하여 서버에 등록할 수도 있다.

[0043] 블록 (423) 에서, 서버는 디바이스 ID 및 시큐리티 토큰에 기초하여 무선-가능 제품을 인증할 수도 있다. 이 인증은 2 개 이상의 고유 식별자들 및 시큐리티 정보에 기초한 임의의 형태의 인증 프로세스를 이용할 수도 있다. 예를 들어, 서버는 디바이스 ID 를 이용하여 대응하는 시큐리티 토큰이 저장되는 데이터베이스 레코드를 룩업하고, 그 후 수신된 시큐리티 토큰과 데이터베이스에 저장된 토큰을 비교하여 그들이 동일한지 여부를 결정할 수도 있다. 다른 예로서, 서버는 디바이스 ID 를 이용하여, 수신된 시큐리티 토큰과 비교되는 값을 생성하기 위해 서버가 이용할 수 있는 해시 알고리즘 또는 암호화 키가 저장되는 대응하는 레코드를 룩업할 수도 있다.

[0044] 서버가 블록 (423) 에서 무선-가능 제품을 인증하면, 서버는 블록 (425) 에서 공중 네트워크 위에서 오픈 통신 링크를 통해 무선-가능 제품에 고객의 사설 네트워크에 액세스하기 위한 정보를 송신 (예를 들어, 네트워크 크리덴셜들을 전송) 할 수도 있다. 블록 (425) 에서의 동작들의 일부분으로, 무선-가능 제품은 사설 네트워크에 액세스하기 위한 네트워크 크리덴셜들 및 다른 정보를 저장할 수도 있다.

[0045] 블록 (427) 에서, 무선-가능 제품은 서버에 대한 공중 접속을 종료할 수도 있고, 블록 (429) 에서, 무선-가능 제품은 서버에 의해 제공되는 네트워크 크리덴셜들 및 다른 액세스 정보를 이용하여 고객의 사설 네트워크에 접속할 수도 있다.

[0046] 블록 (409) 에서의 고객 등록 프로세스는 단지 한번만 수행되면 되지만, 방법 (401) 의 블록들 (411 내지 429) 에서의 동작들은 고객이 고객의 사설 네트워크에 대한 접속을 위한 다른 무선-가능 제품을 구매할 때마다 수행될 수도 있다.

[0047] 도 5 는 다양한 실시형태들에 따른 무선-가능 제품에서 구현될 수도 있는 방법 (501) 을 예시한다. 블록 (511) 에서, 제품은 제조업자 또는 제품 테스트/구성 동안에 시큐리티 토큰 및 고유 디바이스 ID 를 수신할 수도 있다. 블록 (513) 에서, 무선-가능 제품은 수신된 시큐리티 토큰 및 디바이스 ID 를 메모리에 저장할 수도 있다.

[0048] 블록 (517) 에서, 무선-가능 제품은 제품이 전원에 접속될 때 서버에 액세스하기 위해 공중 네트워크에 접속할 수도 있다. 따라서, 고객이 제품을 집으로 (또는 다른 로케이션으로) 가져와서 그것을 전원에 접속하면, 무선-가능 제품은 무선 네트워크를 탐색하기 시작할 수도 있다. 제품이 오픈 (즉, 공중) 네트워크를 발견할 때, 무선-가능 제품은 그 네트워크를 이용하여 서버와 통신한다. 서버에 대한 접속이 확립될 때까지, 무선-가능 제품은 이러한 통신들을 달성하기 위해 공중 네트워크를 계속 찾을 수도 있다.

[0049] 일단 서버에 대한 접속이 확립되면, 무선-가능 제품은 블록 (519) 에서 메모리에 저장된 디바이스 ID 및 시큐리티 토큰을 제공하는 것에 의해 서버에 등록할 수도 있다. 블록 (521) 에서, 이를 테면, 서버에 의한 성공적인 등록/인증에 응답하여, 무선-가능 제품은 고객의 사설 네트워크에 액세스하기 위한 네트워크 크리덴셜들 및 다른 정보를 수신할 수도 있다.

[0050] 블록 (523) 에서, 무선-가능 제품은 서버로부터 수신된 사설 네트워크에 액세스하는 것과 연관된 수신된 네트워크 크리덴셜들 및 정보를 저장할 수도 있다. 블록 (525) 에서, 무선-가능 제품은 공중 네트워크로부터 접속 해제하고, 블록 (527) 에서 수신된 네트워크 크리덴셜들 및 정보를 이용하여 사설 네트워크에 접속할 수도 있다.

[0051] 도 6 은 포스 컴퓨팅 디바이스 (예를 들어, 소매 포스 디바이스 (155)) 에서 구현될 수도 있는 방법 (601) 을 예시한다. 블록 (611) 에서, 포스 디바이스는 구매 트랜잭션과 관련하여 무선-가능 제품의 디바이스 ID 를 획득할 수도 있다. 블록 (613) 에서, 포스 디바이스는 무선-가능 제품을 구매하는 개인의 고객 ID 를 획득할 수도 있다. 블록 (615) 에서, 포스 디바이스는 획득된 디바이스 ID 및 고객 ID 를 서버에 송신할 수도 있다.

[0052] 도 7 은 다양한 실시형태들에 따른 무선-가능 제품의 자동 온보딩을 지원하기 위한 서버에서 구현될 수도 있는 방법 (701) 을 예시한다.

[0053] 블록 (711) 에서, 서버는 고객 어카운트가 고객 식별자 (예를 들어, 고객 ID) 와 관련 있는 고객에 대해 생성되는 고객 등록 프로세스를 수행할 수도 있다. 서버는 고객 대신에 고객 ID 를 생성하거나, 또는 고객으로부터 고객 ID (예를 들어, 이메일 어드레스) 를 수신할 수도 있다.

- [0054] 블록 (713) 에서, 서버는 고객 등록 프로세스의 일부로서 고객에 의해 입력될 수도 있는, 고객의 사설 네트워크에 액세스하기 위한 고객 네트워크 크리덴셜들 및 다른 정보를 고객으로부터 수신할 수도 있다. 블록 (715) 에서, 서버는 데이터베이스에 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들과 함께 고객의 식별자 (예를 들어, 고객 ID) 를 저장할 수도 있다. 일부 실시형태들에서, 네트워크 크리덴셜들은 데이터베이스에서 고객 ID 에 링크될 수도 있다.
- [0055] 블록 (717) 에서, 서버는 무선-가능 제품에 대한 디바이스 ID 및 디바이스 시큐리티 키 (예를 들어, 디바이스 시큐리티 토큰 또는 그 디바이스 시큐리티 토큰을 생성 또는 인증하는데 이용될 수 있는 정보) 를 수신할 수도 있다. 예를 들어, 일부 실시형태들에서, 서버는 블록 (717) 에서 제품 제조업자로부터 디바이스 ID 및 시큐리티 토큰을 수신하고 디바이스 시큐리티 키를 저장할 수도 있다. 다른 구현들에서, 블록 (717) 에서, 서버는 시큐리티 토큰을 생성하기 위해 서버가 이용할 수 있는 디바이스 ID 및 정보 (예를 들어, 알고리즘 또는 공유 알고리즘에 대한 시드 토큰) 를 제품 제조업자로부터 수신할 수도 있다. 추가의 구현들에서, 서버는 디바이스 ID 및 시큐리티 토큰을 생성하고 그 정보를 무선-가능 제품에의 저장을 위해 디바이스 제조업자에게 제공할 수도 있다. 블록 (719) 에서, 서버는 (예를 들어, 제품 ID 에 인덱싱된) 탐색가능한 데이터베이스에서 디바이스 ID 에 링크된 서버에 의해 액세스가능한 메모리에 무선-가능 제품에 대한 디바이스 ID 및 시큐리티 키를 저장할 수도 있다.
- [0056] 후속하여, 서버는 블록 (721) 에서 디바이스 ID 및 고객 ID 를 고객에 의해 무선-가능 제품의 구매 트랜잭션을 인에이블하는 컴퓨팅 디바이스 (예를 들어, 포스 컴퓨팅 디바이스) 로부터 수신할 수도 있다. 블록 (723) 에서, 서버는 수신된 고객 ID 와 수신된 디바이스 ID 의 연관을 데이터베이스에 저장할 수도 있다. 그 연관은 디바이스 ID 를 제공받을 때 서버가 연관된 고객 ID 를 식별하는 것을 인에이블할 수도 있다. 이 동작은 2 개의 데이터베이스들을 상관시키는 것, 이를 테면 고객 ID 를 디바이스 ID 에 링크시키는 것, 또는 새로운 데이터베이스, 이를 테면 디바이스 ID 에 인덱싱된 것과 같은, 고객 ID 및 디바이스 ID 를 포함하는 데이터베이스를 생성하는 것을 수반할 수도 있다.
- [0057] 후속하여, 서버는 블록 (731) 에서 무선-가능 제품에 의해 개시된 공중 네트워크 접속을 통해 무선-가능 제품으로부터 디바이스 ID 및 시큐리티 토큰을 수신할 수도 있다. 이것은, 무선-가능 제품이 파워 온되고 공중 네트워크에 액세스할 때 일어날 것이다.
- [0058] 블록 (733) 에서, 서버는 수신된 디바이스 ID 및 시큐리티 토큰에 기초하여 무선-가능 제품을 인증할 수도 있다. 예를 들어, 서버는 디바이스 ID 를 이용하여 디바이스 시큐리티 키 (예를 들어, 디바이스 시큐리티 토큰 또는 그 디바이스 시큐리티 토큰을 생성 또는 검증하기 위해 서버가 이용할 수 있는 정보) 또는 서버가 무선-가능 제품을 인증하기 위해 이용할 수 있는 다른 인증 정보가 저장되는 데이터베이스 레코드에 액세스할 수도 있다.
- [0059] 서버가 수신 시큐리티 토큰에 기초하여 무선-가능 제품을 인증하면, 서버는 블록 (735) 에서 고객 ID 를 이용하여 데이터베이스로부터 고객의 사설 네트워크에 액세스하기 위한 정보를 추출할 수도 있다. 정보 추출은 블록 (723) 에서 이전에 저장된 디바이스 ID 와 고객 ID 간의 연관을 이용하여 블록 (715) 에서 저장된 고객의 사설 네트워크에 액세스하기 위한 네트워크 크리덴셜들 및 정보를 포함하는 데이터베이스 레코드를 식별하는 것에 의해 달성될 수도 있다. 블록 (737) 에서, 서버는 고객의 사설 통신 네트워크에 액세스하기 위한 네트워크 크리덴셜들 및 정보를 공중 네트워크를 통한 오픈 접속을 이용하여 무선-가능 제품에 제공할 수도 있다.
- [0060] 도 5 내지 도 7 에 예시된 실시형태 방법들을 포함하는 다양한 실시형태들은 서버 및 도 8 에 예시된 서버 (800) 와 같은, 다양한 상업적으로 입수가능한 서버 디바이스들 중 임의의 것을 이용하는 포스 디바이스에서 구현될 수도 있다. 이러한 서버 (800) 는 통상적으로 휘발성 메모리 (802) 및 대용량 비휘발성 메모리, 이를 테면 디스크 드라이브 (803) 에 커플링된 프로세서 (801) 를 포함한다. 서버 (800) 는 또한, 프로세서 (801) 에 커플링된 플로피 디스크 드라이브, 콤팩트 디스크 (CD) 또는 DVD (digital versatile disc) 디스크 드라이브 (804) 를 포함할 수도 있다. 서버 (800) 는 또한 네트워크 (807), 이를 테면 다른 브로드캐스트 시스템 컴퓨터들 및 서버들에 커플링된 로컬 영역 네트워크와 네트워크 인터페이스 접속들을 확립하기 위해 프로세서 (801) 에 커플링된 네트워크 액세스 포트들 (806) 을 포함할 수도 있다.
- [0061] 프로세서 (801) 는 상기 설명된 다양한 실시형태들의 기능들을 포함하는, 다양한 기능들을 수행하기 위해 소프트웨어 명령들 (애플리케이션들) 에 의해 구성될 수 있는 임의의 프로그래밍가능 마이크로프로세서, 마이크로컴퓨터 또는 다중 프로세서 칩 또는 칩들일 수도 있다. 일부 디바이스들에서, 무선 통신 기능들에 전용된 하나의 프로세서 및 다른 애플리케이션들을 실행하는 것에 전용된 하나의 프로세서와 같이, 다중 프로세서들이 제

공될 수도 있다. 통상적으로, 소프트웨어 애플리케이션들은 그들이 액세스되어 프로세서 (801) 로 로드되기 전에 내부 메모리 (802, 또는 803) 에 저장될 수도 있다. 프로세서 (801) 는 애플리케이션 소프트웨어 명령들을 저장하는데 충분한 내부 메모리를 포함할 수도 있다. 많은 디바이스들에서, 내부 메모리는 휘발성 또는 비휘발성 메모리, 이를 테면 플래시 메모리, 또는 양자의 혼합물일 수도 있다. 이 설명의 목적들을 위해, 메모리에 대한 일반적인 언급은 내부 메모리를 포함하는 프로세서 (801) 에 의해 액세스가능한 메모리 또는 디바이스에 플로깅된 제거가능한 메모리 및 프로세서 (801) 자체 내의 메모리를 지칭한다.

[0062] 전술한 방법 설명들 및 프로세스 플로우 다이어그램들은 예시적인 예들로서 단지 제공될 뿐이며 다양한 실시형태들의 단계들이 제시된 순서로 수행되어야 하는 것을 요구하거나 또는 의미하도록 의도되지 않는다. 당업자에 의해 인식될 바와 같이, 전술한 실시형태들에서의 단계들의 순서는 임의의 순서로 수행될 수도 있다. "그 후에", "그 후", "다음에" 등과 같은 단어들은 단계들의 순서를 제한하도록 의도되지 않고; 이들 단어들은 독자를 방법들의 설명을 통하여 안내하는데 단순히 사용된다. 게다가, 예를 들어, 관사들 "a", "an" 또는 "the" 를 이용하는, 단수의 청구항 엘리먼트들에 대한 임의의 언급은 엘리먼트를 단수로 제한하는 것으로 해석되지 않아야 한다.

[0063] 본 명세서에서 개시된 실시형태들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들, 및 알고리즘 단계들은 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양자의 조합들로서 구현될 수도 있다. 하드웨어와 소프트웨어의 이 상호교환가능성을 명확히 예시하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들은 그들의 기능성의 관점에서 일반적으로 상술되었다. 이러한 기능성이 하드웨어로서 구현되는지 또는 소프트웨어로서 구현되는지 여부는 전체 시스템에 부과된 설계 제약들 및 특정한 애플리케이션에 의존한다. 당업자들은 각각의 특정한 애플리케이션에 대해 다양한 방식으로 설명된 기능성을 구현할 수도 있지만, 이러한 구현 관점들은 본 발명의 범위로부터 벗어남을 야기하는 것으로서 해석되어서는 안된다.

[0064] 본 명세서에서 개시된 실시형태들과 관련하여 설명된 다양한 예시적인 로직들, 논리 블록들, 모듈들, 및 회로들을 구현하는데 이용되는 하드웨어는 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적 회로 (ASIC), 필드 프로그래밍가능 게이트 어레이 (FPGA) 또는 다른 프로그래밍가능 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본 명세서에서 설명된 기능들을 수행하도록 설계된 그 임의의 조합으로 구현 또는 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안으로, 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수도 있다. 프로세서는 또한, 컴퓨팅 디바이스들의 조합, 예를 들어, DSP 와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 이상의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수도 있다. 대안적으로, 일부 단계들 또는 방법들은 주어진 기능에 특정한 회로부에 의해 수행될 수도 있다.

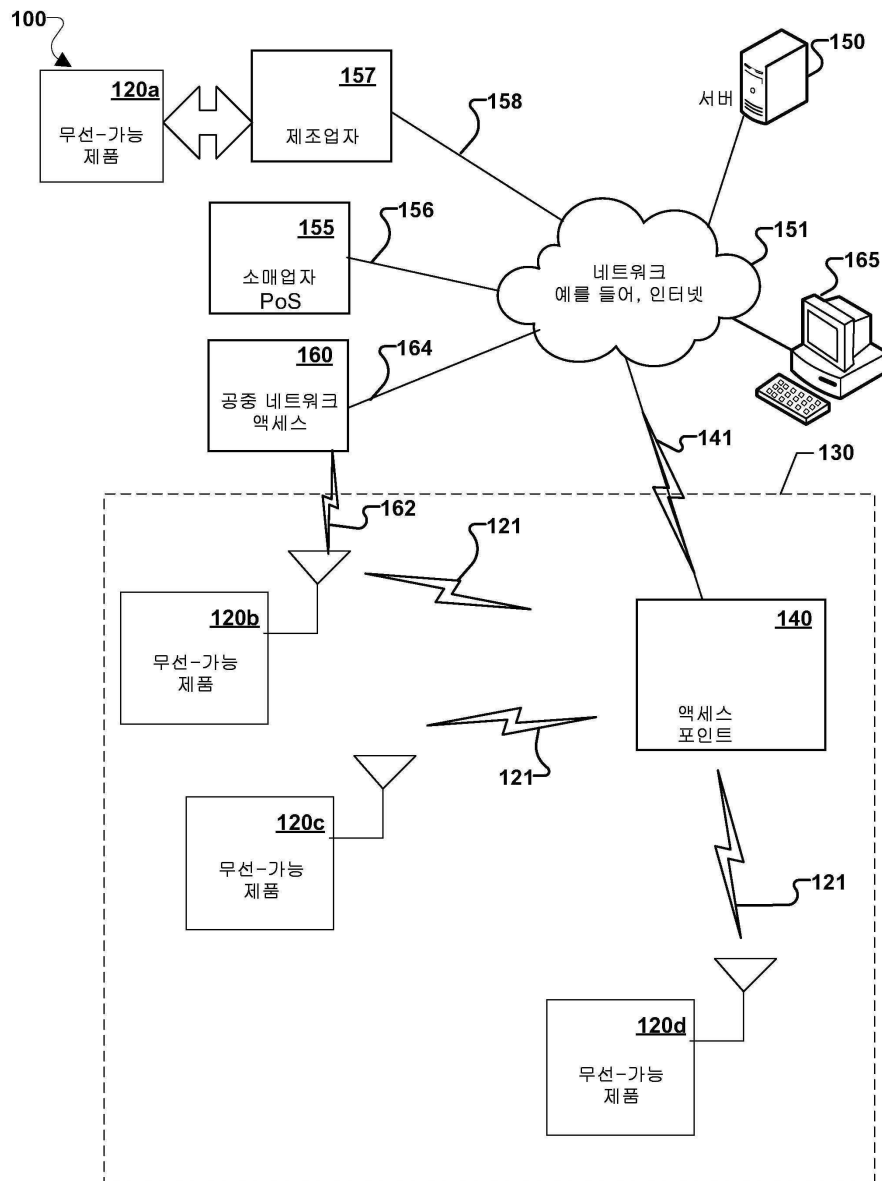
[0065] 하나 이상의 예시적인 실시형태들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 그 임의의 조합으로 구현될 수도 있다. 소프트웨어로 구현되면, 그 기능들은 컴퓨터 판독가능 매체 상에 하나 이상의 명령들 또는 코드로서 저장되거나 이를 통해 송신될 수도 있다. 본 명세서에서 개시된 방법 또는 알고리즘의 단계들은 유형의, 비일시적 컴퓨터 판독가능 저장 매체 상에 상주할 수도 있는 프로세서-실행가능 소프트웨어 모듈로 구현될 수도 있다. 유형의, 비일시적 컴퓨터 판독가능 저장 매체들은 컴퓨터에 의해 액세스될 수도 있는 임의의 이용가능한 매체들일 수도 있다. 제한 없이 일 예로, 이러한 비일시적 컴퓨터 판독가능 매체들은 RAM, ROM, EEPROM, CD-ROM 또는 다른 광 디스크 스토리지, 자기 디스크 스토리지 또는 다른 자기 저장 디바이스들, 또는 명령들 또는 데이터 구조들의 형태로 원하는 프로그램 코드를 저장하는데 이용될 수도 있고 컴퓨터에 의해 액세스될 수도 있는 임의의 다른 매체를 포함할 수도 있다. 디스크 (disk) 및 디스크 (disc) 는, 본 명세서에서 사용한 바와 같이, 콤팩트 디스크 (CD), 레이저 디스크, 광 디스크, DVD, 플로피 디스크, 및 블루-레이 디스크를 포함하고 여기서 디스크 (disk) 들은 보통 데이터를 자기적으로 재생하는 한편, 디스크 (disc) 들은 레이저들로 데이터를 광학적으로 재생한다. 상기의 조합들이 또한 비일시적 컴퓨터 판독가능 매체들의 범위 내에 포함되어야 한다. 추가적으로, 방법 또는 알고리즘의 동작들은 컴퓨터 프로그램 제품에 통합될 수도 있는, 유형의, 비일시적 머신 판독가능 매체 및/또는 컴퓨터 판독가능 매체 상에 하나 또는 임의의 조합 또는 세트의 코드들 및/또는 명령들로서 상주할 수도 있다.

[0066] 개시된 실시형태들의 전술한 설명은 당업자가 본 발명의 제조 또는 이용하는 것을 가능하게 하기 위해 제공된다. 이들 실시형태들에 대한 다양한 변형들은 당업자들에게 용이하게 명백할 것이며, 본 명세서에서 정의된 일반적인 원리들은 본 발명의 사상 또는 범위로부터 벗어남 없이 다른 실시형태들에 적용될 수도 있다. 따라서, 본 발명은 본 명세서에 도시된 실시형태들에 제한되도록 의도되지 않고 다음의 청구항들 및 본 명세

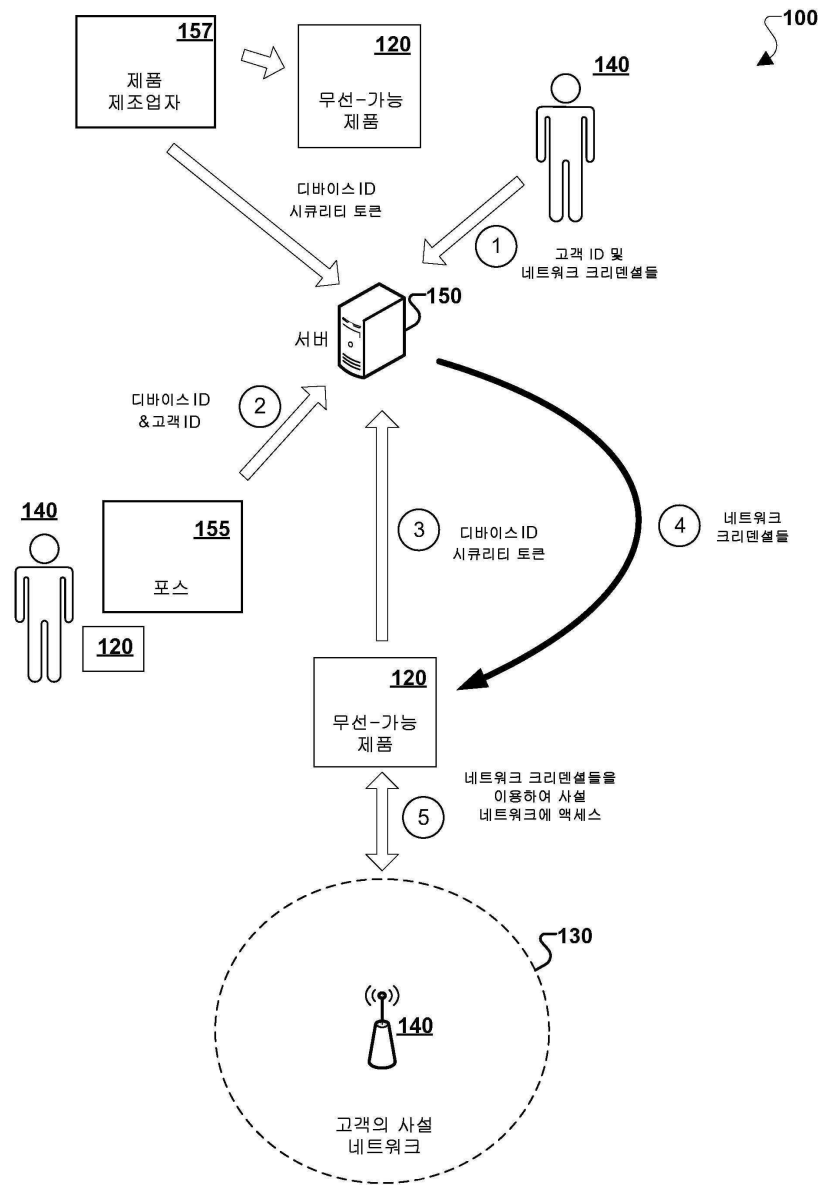
서에서 개시된 원리들 및 신규한 피쳐들에 부합하는 최광의 범위를 부여받게 하려는 것이다.

도면

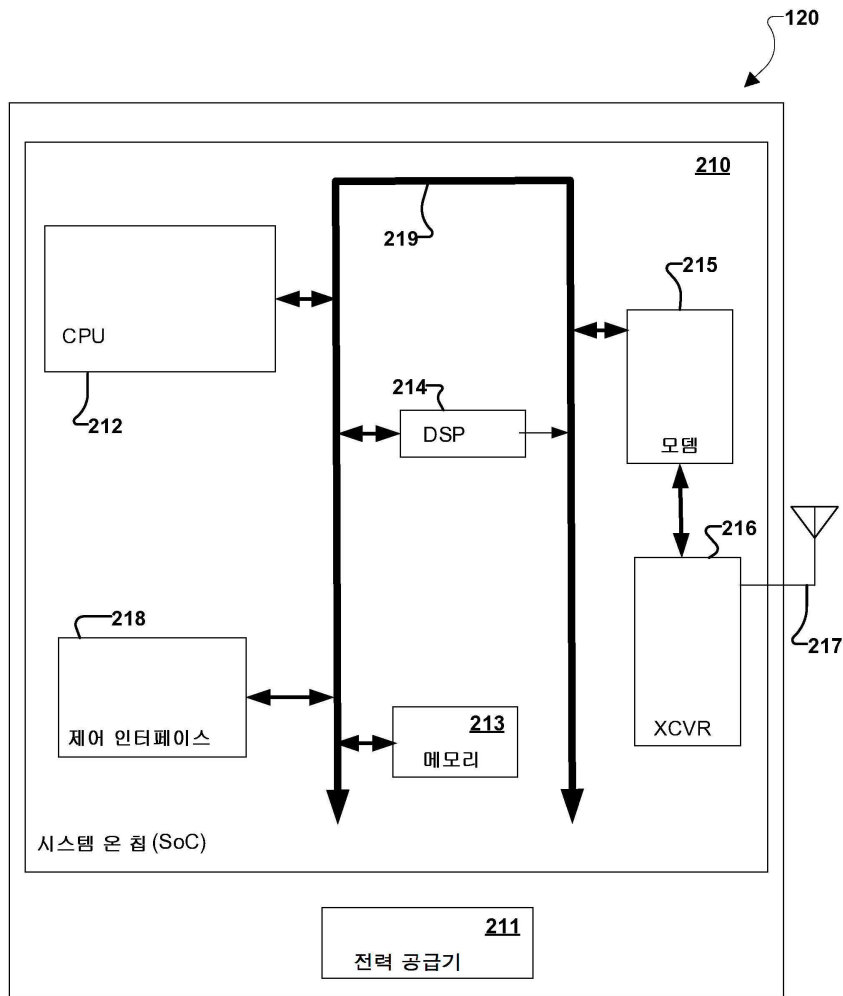
도면1a



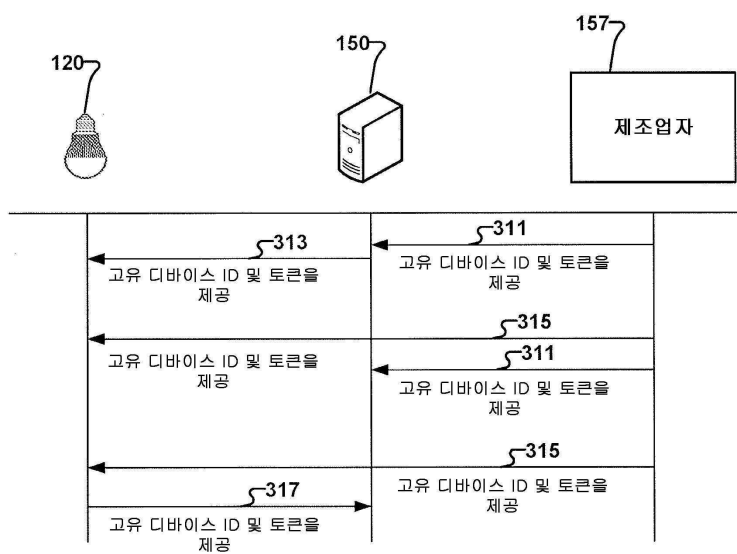
도면1b



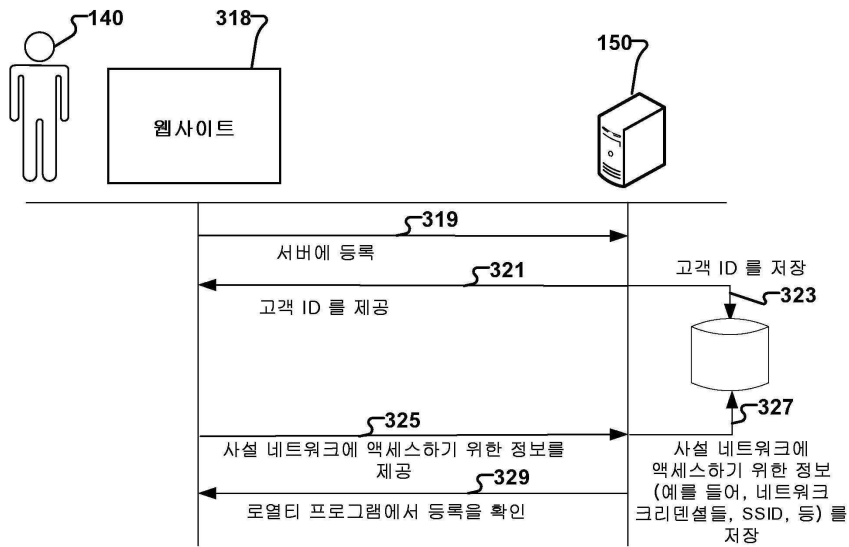
도면2



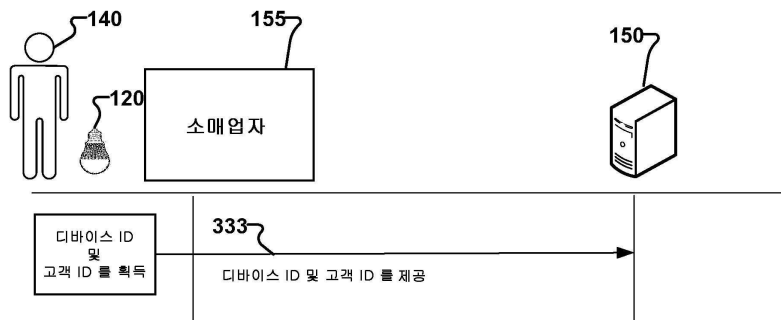
도면3a



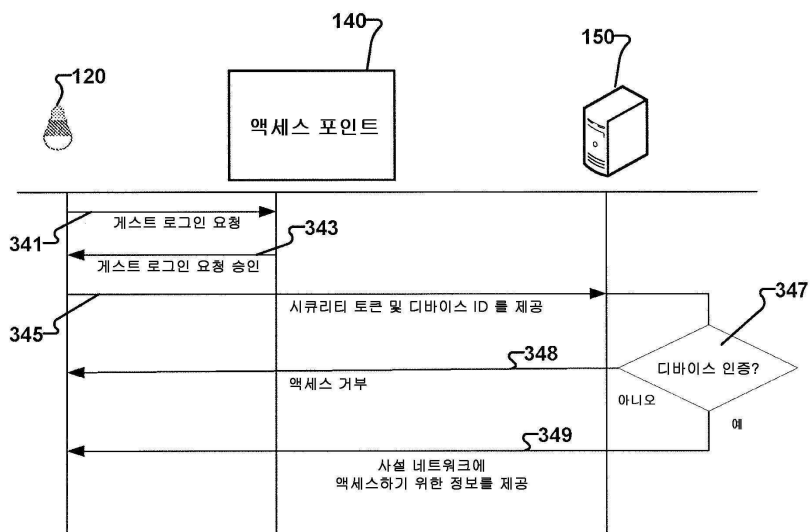
도면3b



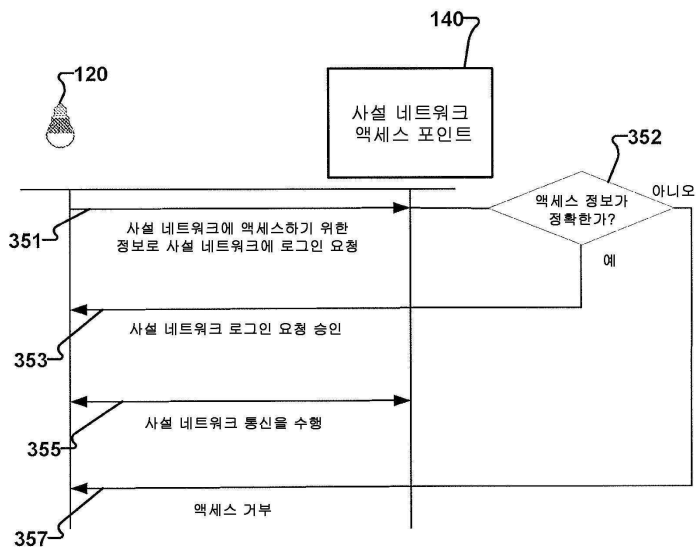
도면3c



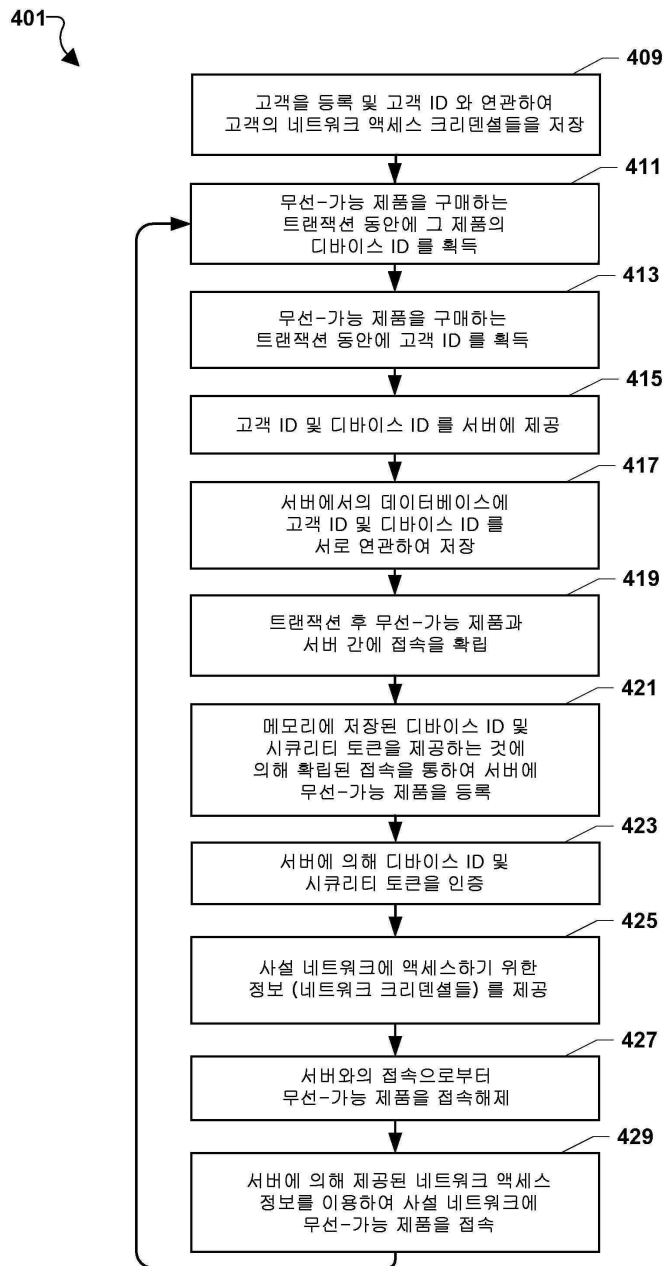
도면3d



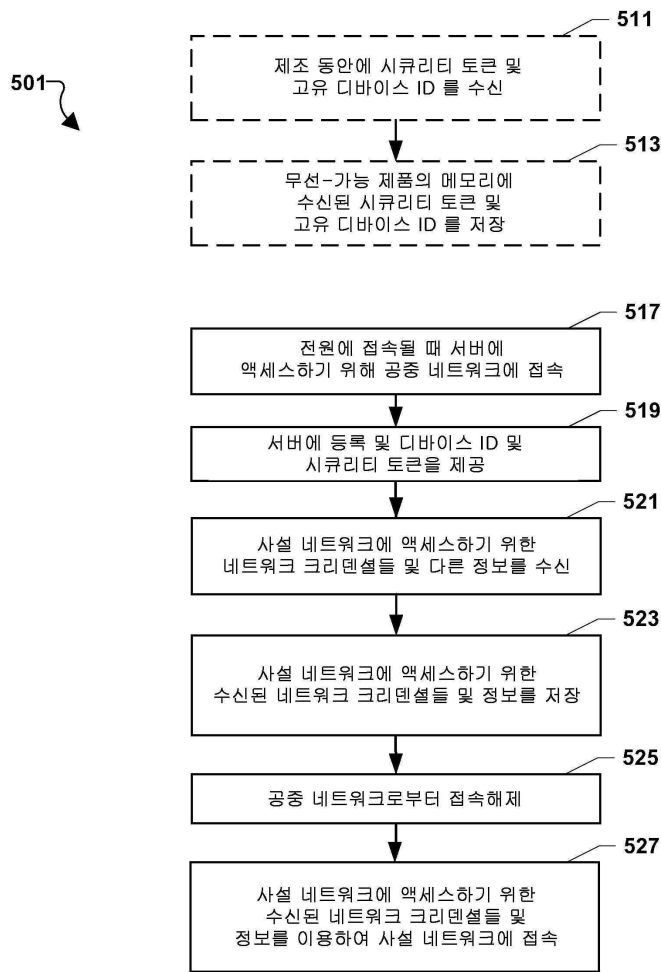
도면3e



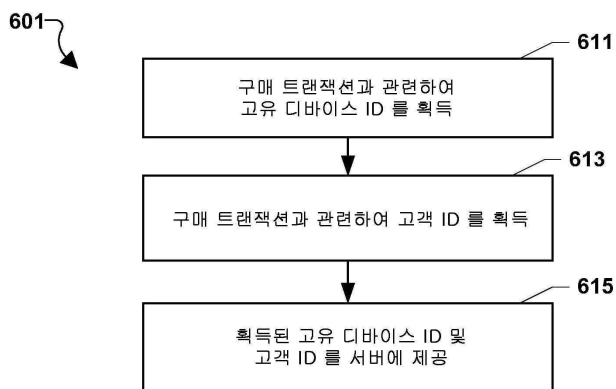
도면4



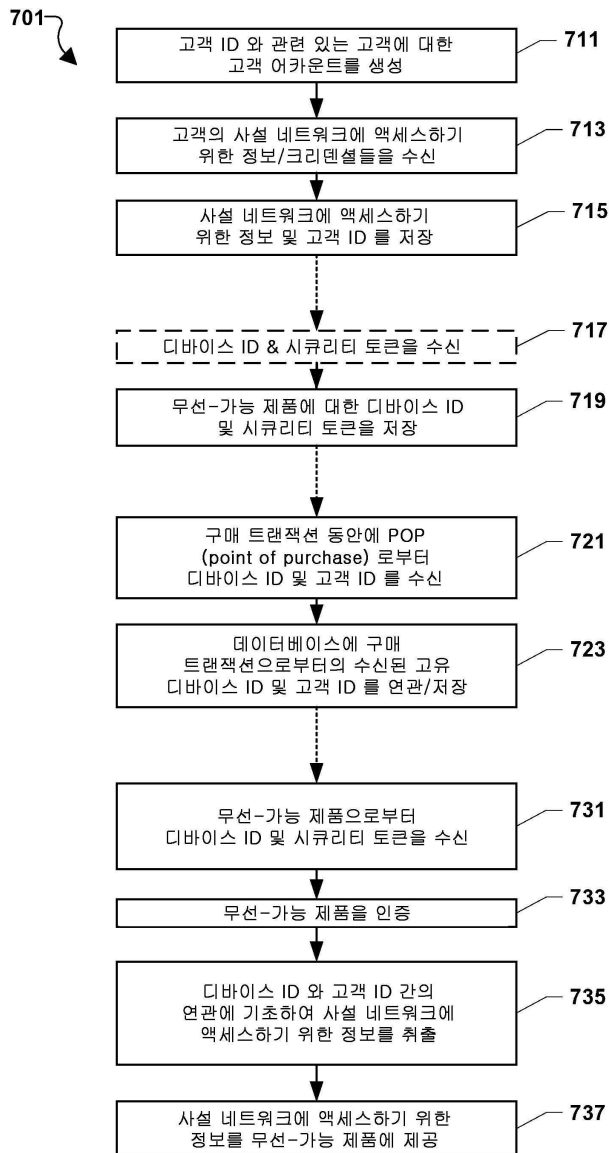
도면5



도면6



도면7



도면8

