(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06F 15/00 (2006.01)
G06F 17/00 (2006.01)

(11) 공개번호 10-2006-0034244
(43) 공개일자 2006년04월21일

(21) 출원번호 10-2005-7025065
(22) 출원일자 2005년12월27일
번역문 제출일자 2005년12월27일
(86) 국제출원번호 PCT/JP2004/009608
국제출원일자 2004년06월30일
(87) 국제공개번호 WO 2005/002133
국제공개일자 2005년01월06일

(30) 우선권주장 JP-P-2003-00188139 2003년06월30일 일본(JP)
JP-P-2004-00179562 2004년06월17일 일본(JP)

(71) 출원인 소니 가부시끼 가이샤
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고

(72) 발명자 카츠베 토모히로
일본 도쿄도 시나가와쿠 기타시나가와 6-7-35 소니 가부시끼가이샤 내
다테 히데키
일본 도쿄도 시나가와쿠 기타시나가와 6-7-35 소니 가부시끼가이샤 내
사토 아츠시
일본 도쿄도 시나가와쿠 기타시나가와 4-7-35 소니 글로벌 솔류션가부시끼 가이샤 내
스기타 유우
일본 도쿄도 시나가와쿠 기타시나가와 4-7-35 소니 글로벌 솔류션가부시끼 가이샤 내
미우라 타카유키
일본 도쿄도 시나가와쿠 기타시나가와 6-7-35 소니 가부시끼가이샤 내
오노 츠요시
일본 도쿄도 시나가와쿠 기타시나가와 6-7-35 소니 가부시끼가이샤 내
미야타 코우지
일본 도쿄도 시나가와쿠 기타시나가와 6-7-35 소니 가부시끼가이샤 내

(74) 대리인 최달용

심사청구 : 없음

(54) 기기 인증 정보 조립 시스템

요약

CE 기기 내에 기기 인증 정보를 안전하게 조립할 수 있는 단말 기기이다. 관리 서버(7)는. 기기 인증 정보를 암호화하여 공장(5)에 송신한다. 접속 수단(10)은 공장의 작업자에 의해 CE 기기(9)의 커넥터에 접속되고, 관리 서버(7)로부터 송신되어 온 기기 인증 정보를 암호화된 채로 CE 기기(9)에 입력한다. CE 기기(9)의 내부에는 암호화된 기기 인증 정보를 복호화하

여 격납하기 위한 기록 모듈이 내장되어 있다. 접속 수단(10)으로부터 입력된 기기 인증 정보는. 기록 모듈에 의해 복호화되고, CE 기기(9) 내부의 기억 장치에 기억된다. 기기 인증 정보는 암호화된 채로 CE 기기(9)에 입력되기 때문에 안전하게 기기 인증 정보를 조립할 수 있다.

대표도

도 1

색인어

기기 인증 정보 조립 시스템

명세서

기술분야

본 발명은, 단말 기기 등에 관한 것이며, 특히, 기기 인증 정보를 암호화하여 기기에 기록하고, 이것을 기기 내에서 복호화함에 의해 기기 인증 정보를 안전하게 기기 내에 기록하는 것에 관한 것이다.

배경기술

근래, CE(CE : Consumer Electronics) 기기의 보급이 확산되고 있다. CE 기기란, 예를 들면, 비디오 덱, 스테레오, 텔레비전 등의 시청각 기기나, 취사기, 냉장고 등의 가전 제품이나, 그 밖의 전자 기기에 컴퓨터를 내장시키고, 네트워크를 통하여 서비스를 이용할 수 있는 것이다.

서버가 제공하는 서비스에는, CE 기기의 기기 인증을 필요로 하는 것이 있다. 그 때문에, CE 기기에는 기기 인증을 행하기 위한 기기 인증 정보가 미리 제조 공장에서 조립된다.

도 18은, 종래의 기기 인증 정보의 조립 방법을 설명하기 위한 도면이다. CE 기기에 조립되는 기기 인증 정보는 관리 센터(103)의 관리 서버(107)에서 관리되고 있다.

관리 서버(107)는 기기 인증 정보를 CE 기기의 제조 공장인 공장(105)에 송신한다.

기기 인증 정보는, 기밀성을 필요로 하는 비밀 정보이기 때문에, 외부에 누출되지 않도록 암호화되어 송신된다.

공장(105)에서는 접속 수단(110)을 CE 기기(109)의 커넥터에 접속하여, 관리 서버(107)로부터 송신되어 온 기기 인증 정보를 CE 기기(109)에 입력한다.

접속 수단(110)에는 암호화된 기기 인증 정보를 복호화하는 기능이 내장되어 있고, 관리 서버(107)로부터 송신되어 온 기기 인증 정보는 접속 수단(110)에서 복호화된다.

기기 인증 정보는, 복호화된 상태에서 접속 수단(110)이나 CE 기기(109)에 입력되고, CE 기기(109)의 기억 장치에 기억된다.

이와 같은, CE 기기에 기기 인증 정보를 조립하는 발명으로서는, 다음의 전자 기기 제조 시스템 및 전자 기기 제조 방법이 있다(특개2001-134654호 공보).

본 발명은, CE 기기에 첨부한 바코드 라벨 실에 기록되어 있는 제품 시리얼 번호로부터, 데이터베이스에 등록되어 있는 기기 인증 정보를 판독하여 기기에 조립하는 것이다.

그런데, 종래의 방법에서는 접속 수단(110)에서 기기 인증 정보를 복호화하여 버리기 때문에, 접속 수단(110)으로부터 기기 인증 정보가 누출되어 버릴 가능성이 있다.

특히 근래에는, 비용이 낮은 해외의 사업자에게 생산을 위탁하는 경우 등도 많고, 공장(105)에 보낸 기기 인증 정보가 외부에 누출되는 일 없이 확실하게 CE 기기(109)에 조립할 수 있는 구조가 필요하게 되어 있다.

그래서, 본 발명의 제 1의 목적은, 기기 내에 기기 인증 정보를 안전하게 조립할 수 있는 단말 기기 등을 제공하는 것이다.

또한, 본 발명의 제 2의 목적은, 기기 내에 기기 인증 정보가 적절하게 조립된 것을 기기 인증 정보의 비밀 상태를 유지한 상태에서 확인한 것이다.

발명의 상세한 설명

본 발명은, 상기 목적을 달성하기 위해, 제공 서버와 단말 기기로 이루어지고, 기기 인증 서버에서 기기 인증할 때의 기기 인증 정보를 단말 기기에 조립하는 기기 인증 정보 조립 시스템으로서, 상기 제공 서버는 기기 인증 정보를 생성하는 기초가 되는 원 정보를 상기 단말 기기에 제공함과 함께, 상기 기기 인증 정보, 또는 상기 원 정보를, 상기 단말 기기의 기기 인증을 행하는 기기 인증 서버에 제공하고, 상기 단말 기기는 상기 제공된 원 정보를 이용하여, 기기 인증 정보를 송신하기 위해 필요한 정보를 기억하고, 기기 인증시에 상기 기억한 정보를 이용하여 상기 원 정보로부터 생성한 기기 인증 정보를, 상기 기기 인증 서버에 송신하는 것을 특징으로 하는 기기 인증 정보 조립 시스템을 제공한다(제 1의 구성).

제 1의 구성에 있어서, 상기 제공 서버는, 상기 원 정보로부터 생성된 기기 인증 정보를 소정의 일방향성 함수로 변환한 변환치를 상기 단말 기기에 제공하고, 상기 단말 기기는, 상기 제공된 원 정보로부터 생성한 기기 인증 정보를 상기 일방향성 함수로 변환하여 변환치를 생성하고, 상기 생성한 변환치와, 상기 제공 서버로부터 제공된 변환치의 동일성을 판단하도록 구성할 수 있다(제 2의 구성).

또한, 제 1의 구성에 있어서, 상기 단말 기기는, 상기 제공된 원 정보로부터 생성한 기기 인증 정보를 소정의 일방향성 함수로 변환하여 변환치를 상기 제공 서버에 제공하고, 상기 제공 서버는, 상기 원 정보로부터 생성되는 기기 인증 정보를 상기 일방향성 함수로 변환한 변환치와, 상기 단말 기기로부터 제공된 변환치의 동일성을 판단하도록 구성할 수도 있다(제 3의 구성).

또한, 본 발명은, 상기 목적을 달성하기 위해, 제공 서버로부터 제공되는, 기기 인증 정보를 생성하는 기초가 되는 원 정보를 취득하는 원 정보 취득 수단과, 상기 취득한 원 정보로부터 기기 인증 정보를 생성하는 생성 수단과, 기기 인증시에, 상기 생성한 기기 인증 정보를 기기 인증 서버에 송신하는 기기 인증 정보 송신 수단을 구비하는 것을 특징으로 하는 단말 기기를 제공한다(제 4의 구성).

또한, 제 4의 구성에 있어서, 상기 원 정보는, 상기 기기 인증 정보를 암호화한 암호화 기기 인증 정보이고, 상기 생성 수단은, 상기 암호화 기기 인증 정보를 복호화함에 의해, 상기 기기 인증 정보를 생성하도록 구성할 수도 있다(제 5의 구성).

또한, 제 4의 구성에 있어서, 상기 생성 수단에서 생성한 기기 인증 정보를 암호화하여 기억하는 기억 수단을 구비하고, 상기 기기 인증 정보 송신 수단은, 상기 기억 수단에 기억된 기기 인증 정보를 복호화하여 송신하도록 구성할 수도 있다(제 6의 구성).

또한, 제 6의 구성에 있어서, 상기 기억 수단에 기억하는 기기 인증 정보의 암호화, 및 복호화에 사용하는 암호 키를, 상기 암호 키의 사용시에 상기 단말 기기에 고유한 정보를 이용하여 생성하는 키 생성 수단을 구비하도록 구성할 수도 있다(제 7의 구성).

또한, 제 7의 구성에 있어서, 상기 생성한 암호 키를, 상기 암호 키의 사용 후의 소정 기간 내에 소거하는 키 소거 수단을 구비하도록 구성할 수도 있다(제 8의 구성).

또한, 제 4의 구성에 있어서, 상기 제공 서버로부터 상기 기기 인증 정보를 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 수단과, 상기 생성한 기기 인증 정보를, 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 수단과, 상기 취득한 변환치와, 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 수단을 구비하도록 구성할 수도 있다(제 9의 구성).

또한, 제 9의 구성에 있어서, 상기 생성한 기기 인증 정보를 다른 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 수단과, 상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 수단을 구비하도록 구성할 수도 있다(제 10의 구성).

또한, 제 4의 구성에 있어서, 상기 생성한 기기 인증 정보를 소정의 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 수단과, 상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 수단을 구비하도록 구성할 수도 있다(제 11의 구성).

또한, 제 4의 구성에 있어서, 상기 취득한 원 정보를 기억하는 기억 수단을 구비하고, 상기 기기 인증 정보 송신 수단은, 상기 기억한 원 정보로부터 기기 인증 정보를 생성하여 상기 기기 인증 서버에 송신하도록 구성할 수도 있다(제 12의 구성).

또한, 본 발명은, 상기 목적을 달성하기 위해, 원 정보 취득 수단과, 생성 수단과, 기기 인증 정보 송신 수단을 구비한 컴퓨터로 구성된 단말 기기에 있어서, 제공 서버로부터 제공되는, 기기 인증 정보를 생성하는 기초가 되는 원 정보를 상기 원 정보 취득 수단에서 취득하는 원 정보 취득 스텝과, 상기 취득한 원 정보로부터 기기 인증 정보를, 상기 생성 수단에서 생성하는 생성 스텝과, 기기 인증시에, 상기 생성한 기기 인증 정보를, 상기 기기 인증 정보 송신 수단에서 기기 인증 서버에 송신하는 기기 인증 정보 송신 스텝으로 구성된 것을 특징으로 하는 기기 인증 정보 처리 방법을 제공한다(제 13의 구성).

또한, 제 13의 구성에 있어서, 상기 원 정보는, 상기 기기 인증 정보를 암호화한 암호화 기기 인증 정보이고, 상기 생성 스텝에서는, 상기 암호화 기기 인증 정보를 복호화함에 의해, 상기 기기 인증 정보를 생성하도록 구성할 수도 있다(제 14의 구성).

또한, 제 13의 구성에 있어서, 상기 컴퓨터는 기억 수단을 구비하고, 상기 생성 수단에서 생성한 기기 인증 정보를 암호화하여 상기 기억 수단에서 기억하는 기억 스텝을 구비하고, 상기 기기 인증 정보 송신 스텝에서는, 상기 기억 수단에 기억된 기기 인증 정보를 복호화하여 송신하도록 구성할 수도 있다(제 15의 구성).

또한, 제 15의 구성에 있어서, 상기 컴퓨터는 키 생성 수단을 구비하고, 상기 기억 수단에 기억하는 기기 인증 정보의 암호화, 및 복호화에 사용하는 암호 키를, 상기 키 생성 수단에서 상기 암호 키의 사용시에 상기 단말 기기에 고유한 정보를 이용하여 생성하는 키 생성 스텝을 구비하도록 구성할 수도 있다(제 16의 구성).

또한, 제 16의 구성에 있어서, 상기 컴퓨터는 키 소거 수단을 구비하고, 상기 생성한 암호 키를, 상기 암호 키의 사용 후의 소정 기간 내에 상기 키 소거 수단에서 소거하는 키 소거 스텝을 구비하도록 구성할 수도 있다(제 17의 구성).

또한, 제 13의 구성에 있어서, 상기 컴퓨터는 변환치 취득 수단과, 변환치 산출 수단과, 판단 수단을 구비하고, 상기 제공 서버로부터 상기 기기 인증 정보를 소정의 일방향성 함수로 변환한 변환치를 상기 변환치 취득 수단에서 취득하는 변환치 취득 스텝과, 상기 변환치 산출 수단에서 상기 생성한 기기 인증 정보를, 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 스텝과, 상기 판단 수단에서, 상기 취득한 변환치와, 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 스텝을 구비하도록 구성할 수도 있다(제 18의 구성).

또한, 제 18의 구성에 있어서, 상기 컴퓨터는 변환치 산출 수단과, 변환치 제공 수단을 구비하고, 상기 변환치 산출 수단에서, 상기 생성한 기기 인증 정보를 다른 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 스텝과, 상기 변환치 산출 수단에서, 상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 스텝을 구비하도록 구성할 수 있다(제 19의 구성).

제 13의 구성에 있어서, 상기 컴퓨터는 변환치 산출 수단과, 변환치 제공 수단을 구비하고, 상기 변환치 산출 수단에서, 상기 생성한 기기 인증 정보를 소정의 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 스텝과, 상기 변환치 제공 수단에서, 상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 스텝을 구비하도록 구성할 수 있다(제 20의 구성).

또한, 제 13의 구성에 있어서, 상기 컴퓨터는, 상기 취득한 원 정보를 기억하는 기억 수단을 구비하고, 상기 기기 인증 정보 송신 스텝에서는, 상기 기억한 원 정보로부터 기기 인증 정보를 생성하여 상기 기기 인증 서버에 송신하도록 구성할 수 있다(제 21의 구성).

또한, 본 발명은, 상기 목적을 달성하기 위해, 제공 서버로부터 제공되는, 기기 인증 정보를 생성하는 기초가 되는 원 정보를 취득하는 원 정보 취득 기능과, 상기 취득한 원 정보로부터 기기 인증 정보를 생성하는 생성 기능과, 기기 인증시에, 상기 생성한 기기 인증 정보를 기기 인증 서버에 송신하는 기기 인증 정보 송신 기능을 컴퓨터에서 실현하는 기기 인증 정보 처리 프로그램을 제공한다(제 22의 구성).

제 22의 구성에 있어서, 상기 원 정보는, 상기 기기 인증 정보를 암호화한 암호화 기기 인증 정보이고, 상기 생성 기능은, 상기 암호화 기기 인증 정보를 복호화함에 의해, 상기 기기 인증 정보를 생성하도록 구성할 수 있다(제 23의 구성).

제 22의 구성에 있어서, 상기 생성 기능에서 생성한 기기 인증 정보를 암호화하여 기억하는 기억 기능을 실현하고, 상기 기기 인증 정보 송신 기능은, 상기 기억 기능에 기억된 기기 인증 정보를 복호화하여 송신하도록 구성할 수 있다(제 24의 구성).

제 24의 구성에 있어서, 상기 기억 기능에 기억하는 기기 인증 정보의 암호화, 및 복호화에 사용하는 암호 키를, 상기 암호 키의 사용시에 상기 단말 기기에 고유한 정보를 이용하여 생성하는 키 생성 기능을 컴퓨터에서 실현하도록 구성할 수도 있다(제 25의 구성).

또한, 제 25의 구성에 있어서, 상기 생성한 암호 키를, 상기 암호 키의 사용 후의 소정 기간 내에 소거하는 키 소거 기능을 컴퓨터에서 실현하도록 구성할 수도 있다(제 26의 구성).

제 22의 구성에 있어서, 상기 제공 서버로부터 상기 기기 인증 정보를 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 기능과, 상기 생성한 기기 인증 정보를, 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 기능과, 상기 취득한 변환치와, 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 기능을 컴퓨터에서 실현하도록 구성할 수 있다(제 27의 구성).

제 27의 구성에 있어서, 상기 생성한 기기 인증 정보를 다른 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 기능과, 상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 기능을 컴퓨터에서 실현하도록 구성할 수 있다(제 28의 구성).

제 22의 구성에 있어서, 상기 생성한 기기 인증 정보를 소정의 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 기능과, 상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 기능을 컴퓨터에서 실현하도록 구성할 수 있다(제 29의 구성).

제 22의 구성에 있어서, 상기 취득한 원 정보를 기억하는 기억 기능을 컴퓨터에서 실현하고, 상기 기기 인증 정보 송신 기능은, 상기 기억한 원 정보로부터 기기 인증 정보를 생성하여 상기 기기 인증 서버에 송신하도록 구성할 수 있다(제 30의 구성).

또한, 본 발명은, 상기 목적을 달성하기 위해, 제공 서버로부터 제공되는, 기기 인증 정보를 생성하는 기초가 되는 원 정보를 취득하는 원 정보 취득 기능과, 상기 취득한 원 정보로부터 기기 인증 정보를 생성하는 생성 기능과, 기기 인증시에, 상기 생성한 기기 인증 정보를 기기 인증 서버에 송신하는 기기 인증 정보 송신 기능을 컴퓨터에서 실현하는 기기 인증 정보 처리 프로그램을 기억한 컴퓨터가 판독 가능한 기억 매체를 제공한다(제 31의 구성).

또한, 본 발명은, 상기 목적을 달성하기 위해, 단말 기기에 기기 인증 정보를 생성하는 기초가 되는 원 정보를 제공하는 원 정보 제공 수단과, 상기 기기 인증 정보, 또는 상기 원 정보를, 상기 단말 기기의 기기 인증을 행하는 기기 인증 서버에 제공하는 기기 인증 정보 제공 수단과, 상기 단말 기기로부터, 상기 원 정보로부터 생성된 기기 인증 정보의, 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 수단과, 상기 기기 인증 정보를 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 수단과, 상기 취득한 변환치와 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 수단을 구비한 것을 특징으로 하는 제공 서버를 제공한다(제 32의 구성).

제 32의 구성에 있어서, 상기 판단 수단에서 출력된 판단 결과를, 상기 원 정보의 조립 주체에 송신하는 판단 결과 송신 수단을 구비하도록 구성할 수 있다(제 33의 구성).

또한, 본 발명은, 상기 목적을 달성하기 위해, 원 정보 제공 수단과, 기기 인증 정보 제공 수단과, 변환치 취득 수단과, 변환치 산출 수단과, 판단 수단을 구비한 컴퓨터에 있어서, 단말 기기에 기기 인증 정보를 생성하는 기초가 되는 원 정보를, 상

기 원 정보 제공 수단에서 제공하는 원 정보 제공 스텝과, 상기 기기 인증 정보, 또는 상기 원 정보를, 상기 기기 인증 정보 제공 수단에서 상기 단말 기기의 기기 인증을 행하는 기기 인증 서버에 제공하는 기기 인증 정보 제공 스텝과, 상기 변환치 취득 수단에서, 상기 단말 기기로부터, 상기 원 정보로부터 생성된 기기 인증 정보의, 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 스텝과, 상기 변환치 산출 수단에서, 상기 기기 인증 정보를 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 스텝과, 상기 판단 수단에서, 상기 취득한 변환치와 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 스텝으로 구성된 것을 특징으로 하는 기기 인증 정보 제공 방법을 제공한다(제 34의 구성).

제 34의 구성에 있어서, 상기 컴퓨터는, 판단 결과 송신 수단을 구비하고, 상기 판단 수단에서 출력된 판단 결과를, 상기 판단 결과 송신 수단에서 상기 원 정보의 조립 주체에 송신하는 판단 결과 송신 스텝을 구비하도록 구성할 수 있다(제 35의 구성).

또한, 본 발명은, 상기 목적을 달성하기 위해, 단말 기기에 기기 인증 정보를 생성하는 기초가 되는 원 정보를 제공하는 원 정보 제공 기능과, 상기 기기 인증 정보, 또는 상기 원 정보를, 상기 단말 기기의 기기 인증을 행하는 기기 인증 서버에 제공하는 기기 인증 정보 제공 기능과, 상기 단말 기기로부터, 상기 원 정보로부터 생성된 기기 인증 정보의, 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 기능과, 상기 기기 인증 정보를 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 기능과, 상기 취득한 변환치와 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 기능을 컴퓨터에서 실현하는 기기 인증 정보 제공 프로그램을 제공한다(제 36의 구성).

제 36의 구성에 있어서, 상기 판단 기능에서 출력된 판단 결과를, 상기 원 정보의 조립 주체에 송신하는 판단 결과 송신 기능을 컴퓨터에서 실현하도록 구성할 수 있다(제 37의 구성).

또한, 본 발명은, 상기 목적을 달성하기 위해, 단말 기기에 기기 인증 정보를 생성하는 기초가 되는 원 정보를 제공하는 원 정보 제공 기능과, 상기 기기 인증 정보, 또는 상기 원 정보를, 상기 단말 기기의 기기 인증을 행하는 기기 인증 서버에 제공하는 기기 인증 정보 제공 기능과, 상기 단말 기기로부터,

상기 원 정보로부터 생성된 기기 인증 정보의, 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 기능과, 상기 기기 인증 정보를 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 기능과, 상기 취득한 변환치와 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 기능을 컴퓨터에서 실현하는 기기 인증 정보 제공 프로그램을 기억한 컴퓨터가 판독 가능한 기억 매체를 제공한다(제 38의 구성).

본 발명에 의하면, 기기 내에 기기 인증 정보를 안전하게 조립할 수 있다. 또한, 기기 내에 기기 인증 정보가 적절하게 조립된 것을 기기 인증 정보의 비밀 상태를 유지한 채로 확인할 수 있다.

도면의 간단한 설명

도 1은 제 1의 실시의 형태의 개요를 설명하기 위한 도면.

도 2는 제 1의 실시의 형태의 제조 인증 시스템의 구성의 한 예를 도시한 도면.

도 3은 제 1의 실시의 형태의 기기 인증부의 구성의 한 예를 도시한 도면.

도 4는 제 1의 실시의 형태에서, 기기 인증 정보를 조립하는 준비 단계에서의 작업 순서를 설명하기 위한 플로우 차트.

도 5는 제 1의 실시의 형태에서, CE 기기에 기기 인증 정보를 조립하는 순서를 설명하기 위한 플로우 차트.

도 6은 제 1의 실시의 형태에서, CE 기기에 기기 인증 정보가 적절하게 조립된 것을 확인하는 순서를 설명하기 위한 플로우 차트.

도 7은 제 1의 실시의 형태에서, 기기 인증 서버가 CE 기기를 기기 인증하는 순서를 설명하기 위한 플로우 차트.

도 8은 제 1의 실시의 형태의 기기 인증 서버 등에 기억되어 있는 각 테이블을 설명하기 위한 도면.

도 9는 제 1의 실시의 형태의 CE 기기의 하드웨어적인 구성의 한 예를 도시한 도면.

도 10은 제 2의 실시의 형태의 개요를 설명하기 위한 도면.

도 11은 제 2의 실시의 형태에서, CE 기기에 기기 인증 정보를 조립하는 순서를 설명하기 위한 플로우 차트.

도 12는 제 2의 실시의 형태에서, CE 기기에 기기 인증 정보가 적절하게 조립된 것을 확인하는 순서를 설명하기 위한 플로우 차트.

도 13은 제 2의 실시의 형태에서, 기기 인증 서버가 CE 기기를 기기 인증하는 순서를 설명하기 위한 플로우 차트.

도 14는 제 2의 실시의 형태의 기기 인증 서버 등에 기억되어 있는 각 테이블을 설명하기 위한 도면.

도 15는 제 3의 실시의 형태에서, 키 정보가 포함되어 있는 어플리케이션을 갱신하는 순서를 설명하기 위한 플로우 차트.

도 16은 제 4의 실시의 형태의 기기 인증부의 구성의 한 예를 도시한 도면.

도 17은 제 4의 실시의 형태에서, CE 기기에 기기 인증 정보가 적절하게 조립된 것을 확인하는 순서를 설명하기 위한 플로우 차트.

도 18은 종래의 인증 정보의 조립 방법을 설명하기 위한 도면.

실시예

이하, 본 발명의 알맞은 실시의 형태에 관해, 도면을 참조하여 상세히 설명한다.

[제 1의 실시의 형태의 개요]

도 1은, 제 1의 실시의 형태의 개요를 설명하기 위한 도면이다.

기기 인증 정보를 관리하는 관리 서버(7)는, 관리 센터(3)에 설치되어 있고, 기기 인증 정보를 암호화하여 공장(5)에 송신한다.

접속 수단(10)은, 공장의 작업자에 의해 CE 기기(9)의 커넥터에 접속되고, 관리 서버(7)로부터 송신되어 온 기기 인증 정보를 암호화된 채의 상태로 CE 기기(9)에 입력한다.

CE 기기(9)의 내부에는, 암호화된 기기 인증 정보를 복호화하여 격납하기 위한 기록 모듈이 내장되어 있다.

접속 수단(10)으로부터 입력된 기기 인증 정보는, 기록 모듈에 의해 복호화되고, CE 기기(9) 내부의 기억 장치에 기억된다.

접속 수단(10)은, 종래예에서 사용하고 있는 접속 수단(110)과는 달리, 관리 서버(7)로부터 송신되어 온 기기 인증 정보를 복호화하지 않고 CE 기기(9)에 입력한다.

이와 같이, 본 실시의 형태에서는, 관리 서버(7)(제공 서버)로부터 송신되어 온 기기 인증 정보가 암호화된 채로 CE 기기(9)(단말 기기)에 입력되고 CE 기기(9) 내부에서 복호화되기 때문에, 기기 인증 정보 조립 작업에서의 시큐어러티를 높일 수 있다.

또한, 이상의 설명은, 본 실시의 형태의 기본적인 개념을 설명하기 위한 것이고, 각종의 변형이 가능하다.

예를 들면, 이하의 실시의 형태의 상세에서 설명하는 바와 같이, 복호화한 기기 인증 정보를 다른 암호 키로 재차 암호화하여 기억 장치에 기억함에 의해, 보다 시큐어러티를 높일 수 있다.

또한, 본 실시의 형태에서는, CE 기기(9)에 기기 인증 정보가 적절하게 조립된 것을 공장(5), 및 관리 센터(3)가 확인하는 수단도 제공한다.

[제 1의 실시의 형태의 상세]

도 2는, CE 기기의 제조 인증 시스템(1)의 구성의 한 예를 도시한 도면이다. 제조 인증 시스템(1)은, CE 기기(9)의 제조와 기기 인증을 행하는 시스템이고, CE 기기(9)에 서비스를 제공하는 서비스 서버 등은 도시하고 있지 않다.

제조 인증 시스템(1)은, 사업체(11), 관리 센터(3), 공장(5), CE 기기(9), 기기 인증 서버(8) 등으로 구성되어 있다.

사업체(11)는, CE 기기(9)의 제조 회사로서, CE 기기(9)의 기획, 개발, 판매 등, CE 기기(9)를 시장에 공급하는 사업체이다.

관리 센터(3)는 CE 기기(9)에 조립하는 기기 인증 정보의 관리를 행하는 부문이고, 기기 인증 정보의 발행이나, 기기 인증 정보에 관한 암호 정보를 관리하고 있다.

공장(5)은, 사업체(11)로부터의 의뢰에 의해 CE 기기(9)의 제조를 행하는 부문이다. 공장(5)은 사업체(11)가 갖는 경우도 있고, 또한, 사업체(11)의 위탁을 받아서 CE 기기(9)를 제조하는 제삼자가 운영하는 공장인 경우도 있다.

CE 기기(9)는, 공장(5)에서 제조된 CE 기기로서, 내부에 관리 센터(3)가 발행한 기기 인증 정보가 조립되어 있다.

기기 인증 서버(8)는, 관리 센터(3)로부터 기기 인증 정보의 제공을 받음과 함께, CE 기기(9)로부터 기기 인증 정보를 수신하여 CE 기기(9)를 기기 인증하는 서버 장치이다.

CE 기기(9)는, 기기 인증 서버(8)에서 기기 인증됨에 의해, 서비스 서버 등이 제공한 서비스를 받을 수 있다.

이하, 제조 인증 시스템(1)에서 CE 기기(9)가 제조되는 프로세스를 도면중의 번호를 참조하면서 설명한다.

(1) 우선, 사업체(11)가, CE 기기(9)의 기획 설계를 행한다. 그리고, 관리 센터(3)로부터, CE 기기(9)에 인스톨하는 펌웨어를 작성하기 위한 정보를 취득한다.

이 펌웨어는, 기기 인증 정보를 조립하기 위한 프로그램이나 CE 기기(9)를 동작시키기 위한 프로그램 등으로 이루어지고, 공장(5)에서 CE 기기(9)에 인스톨된다. 사업체(11)는, 관리 센터(3)로부터는 암호 키 등의 기기 인증 정보를 조립하기 위한 정보를 취득한다.

(2) 사업체(11)는, CE 기기(9)의 제조를 공장(5)에 의뢰함과 함께, CE 기기(9)에 인스톨하는 펌웨어를 CD-ROM (Compact Disc-Read Only Memory)에 기록하여 송부하거나, 또는, 네트워크를 통하여 송신하는 등으로 공장(5)에 건네준다.

(3) 공장(5)은, CE 기기(9)를 조립한 후, 사업체(11)로부터 취득한 펌웨어를 CE 기기(9)에 인스톨한다. 그리고, CE 기기(9)의 커넥터에 접속 수단(10)(도 1)을 접속하고, 관리 센터(3)에 대해 기기 인증 정보의 송신을 요구한다.

(4) 관리 센터(3)는, 공장(5)으로부터의 요구에 응하여 CE 기기(9)에 조립하기 위한 기기 인증 정보를 네트워크를 통하여 공장(5)에 송신한다. 이 기기 인증 정보는, 암호화되어 있다.

이 암호화된 기기 인증 정보는, 복호화하면 기기 인증 정보를 얻을 수 있기 때문에, 기기 인증 정보를 생성하기 위한 원 정보에 해당한다. 기기 인증 정보의 내용에 관해서는 후에 상세히 설명한다.

(5) 공장(5)은, 관리 센터(3)로부터 송신되어 온 기기 인증 정보를 접속 수단(10)을 통하여 CE 기기(9)에 입력한다. 기기 인증 정보는, CE 기기(9)의 펌웨어가 제공하는 암호 키에 의해 CE 기기(9) 내에서 복호화된 후, 펌웨어가 제공하는 다른 암호 키에 의해 재차 암호화되어 기억 장치에 기억된다.

(6) 그리고, 후술하는 방법에 의해 CE 기기(9)에 기기 인증 정보가 올바르게 조립되었는지의 여부를, 공장(5)과 관리 센터(3)가 확인한다. 이것을 이용하여, 공장(5)이 관리 센터(3)에 제조 실적 보고를 행할 수 있다.

(7) 공장(5)은, CE 기기(9)가 조립, 및 기기 인증 정보의 조립을 완료한 후, CE 기기(9)를 출하한다.

(8) 관리 센터(3)는, CE 기기(9)의 기기 인증 정보를 기기 인증 서버(8)에 제공한다.

(9) 기기 인증 서버(8)는, CE 기기(9)로부터 기기 인증 정보를 송신하여 받고, 이것을 관리 센터(3)로부터 제공된 기기 인증 정보와 비교함에 의해 CE 기기(9)를 기기 인증한다.

도 3은, 기기 인증부(99)의 한 예를 도시한 도면이다. 기기 인증부(99)는, 공장(5)에서 펌웨어를 인스톨함에 의해, CE 기기(9)의 내부에서 구성된 기능부이다.

기기 인증부(99)는, 인증 모듈(20), 기록 모듈(30), 인증 정보 메모리(40), 본체 식별 정보 메모리(50) 등으로 구성되어 있다.

인증 모듈(20)은, CE 기기(9)를 기기 인증 서버(8)에서 기기 인증하기 위한 기능부이다.

인증 모듈(20)은, 기기 인증 서버(8)에 인증 정보를 송신할 때에 사용하는 공개 키(21), 고유 키(23)를 생성하기 위한 고유 키 생성자(生成子)(22)를 구비하고 있다.

고유 키(23)는, 인증 정보 메모리(40)에 기억하는 기기 인증 정보를 암호화, 및 복호화하기 위한 키 정보로서, 사용시에 고유 키 생성자(22)와 MAC 어드레스(51)로부터 동적(動的)으로 생성된다.

MAC 어드레스(51)는, CE 기기(9)에 고유의 정보이다. 그리고, 고유 키(23)도 CE 기기(9)에 고유의 키 정보가 되도록 구성되어 있다.

본 실시의 형태에서는, 한 예로서 MAC 어드레스(51)를 이용하여 고유 키(23)를 생성하지만, 이 외에, i.Link(IEEE1394)의 어드레스 등, CE 기기(9)에 고유한 정보이면 좋다.

즉, CE 기기(9)에 고유한 정보를 이용하여, CE 기기(9)에 고유한 고유 키(23)가 생성되도록 되어 있다.

이와 같이, 제조되는 각 CE 기기(9)에 조립하는 고유 키 생성자(22)가 공통이라도, 생성되는 고유 키(23)는 각 CE 기기(9)에 고유인 것으로 되어, 고유 키 생성자(22)의 관리가 용이해진다.

이와 같이 구성된 인증 모듈(20)은, 기기 인증시에 인증 정보 메모리(40)로부터 기기 인증 정보를 판독하여 복호화하고, 기기 ID(41)와 함께 기기 인증 서버(8)에 송신한다.

고유 키(23)는, 사용된 후, 소정 기간 내에 신속하게 소거된다. 소정 기간은, 예를 들면, 기기 인증 정보를 복호화하고 나서 기기 인증부(99)가 기기 인증을 마칠 때까지 등, 각종의 설정이 가능하다.

또한, 본 실시의 형태에서는, 고유 키(23)는 사용 후에 소거되도록 구성하였지만, 반드시 소거할 필요는 없다.

기록 모듈(30)은, 공장(5)에서 CE 기기(9)에 기기 인증 정보를 기록하기 위한 기능부이다.

기록 모듈(30)은, 기록 전(前) 키(31), 고유 키 생성자(32), 기기측 확인 해시 함수(34), 서버측 확인 해시 함수(35) 등을 구비하고 있다.

기록 전 키(31)는, 관리 센터(3)로부터 송신되어 온 암호화된 기기 인증 정보를 복호화하기 위한 키 정보이다.

고유 키 생성자(32)는, 고유 키(33)를 생성하기 위한 기초(시드)가 되는 정보로서, 인증 모듈(20)의 고유 키 생성자(22)와 같은 것이다.

고유 키(33)는, 기록 전 키(31)에 의해 복호화된 기기 인증 정보를 암호화하기 위한 키 정보로서, 고유 키 생성자(32)와, MAC 어드레스(51)로부터 사용시에 동적으로 생성된다. 고유 키(33)는 인증 모듈(20)에서 생성된 고유 키(23)와 같은 것이다.

이와 같이 구성된 기록 모듈(30)은, 관리 센터(3)로부터 송신되어 온 기기 인증 정보를 기록 전 키(31)로 복호화하고, 고유 키(33)로 재차 암호화하여 인증 정보 메모리(40)에 기억한다.

본 실시의 형태에서는, 기기 인증 정보를 고유 키(33)로 암호화된 상태로 기억함에 의해 시큐어러티를 높이고 있다.

또한, 기록 전 키(31)로 복호화한 기기 인증 정보를 암호화하지 않고 기억 장치에 기억하도록 구성할 수도 있다. 이 경우는, 인증 모듈(20)은, 인증시에 기기 인증 정보를 복호화할 필요가 없기 때문에 고유 키(23)를 생성할 필요는 없다.

기기측 확인 해시 함수(34)는, 기기 인증 정보가 적절하게 인증 정보 메모리(40)에 기억된 것을 기록 모듈(30)이 확인하기 위한 함수이다. 후술하는 바와 같이, 기록 모듈(30)은 관리 센터(3)로부터 송신되어 온 해시 값과, 기기측 확인 해시 함수(34)에 의한 기기 인증 정보의 해시 값을 비교함에 의해 기기 인증 정보가 조립된 것을 확인한다.

서버측 확인 해시 함수(35)는, 기기 인증 정보가 적절하게 인증 정보 메모리(40)에 기억된 것을 관리 센터(3)측이 확인하기 위한 함수이다.

후술하는 바와 같이, 기록 모듈(30)은, 인증 정보 메모리(40)에 기억한 기기 인증 정보의 서버측 확인 해시 함수(35)에 의한 해시 값을 관리 센터(3)에 송신한다.

이에 대해, 관리 센터(3)는, 발행한 기기 인증 정보의 서버측 확인 해시 함수에 의한 해시 값을 생성하고, 기록 모듈(30)로부터 취득한 해시 값과 비교함에 의해, 기기 인증 정보가 CE 기기(9)에 조립된 것을 확인한다.

본 실시의 형태에서는, CE 기기(9)측에서 확인하기 위한 기기측 확인 해시 함수(34)와, 관리 서버(7)측에서 확인하기 위한 서버측 확인 해시 함수(35)의 2종류를 준비하였다.

가령, 같은 해시 함수를 이용하여 CE 기기(9)측에서의 확인과 관리 서버(7)측에서의 확인을 행한다고 하면, 관리 서버(7)가 CE 기기(9)에 송신한 해시 값을 제삼자가 그대로 관리 서버(7)에 반송한 경우, 관리 서버(7)가, 이 해시 값이 CE 기기(9)로부터 송신된 것인지, 또는 제삼자로부터 반송된 것인지 확인하는 것이 곤란하다.

그 때문에, 2종류의 해시 함수를 이용함에 의해 제삼자에 의한 모인(冒認)을 방지할 수 있다.

그런데, 해시 함수란, 전자 문서를 해시화하기 위한 함수로서, 전자 문서를 해시화함에 의해 전자 문서로부터 전자 문서에 고유한 문자열(해시 값, 또는 다이제스트 메시지라고도 불린다)을 생성할 수 있다.

같은 전자 문서로부터는 같은 해시 값을 얻을 수 있다. 전자 문서가 일부라도 변경되면, 이 문서의 해시 값은 변경 전 것과 다르다.

또한, 해시 값을 역변환하여 원래의 전자 문서를 얻는 것은 매우 곤란하다.

이와 같이, 해시 함수는, 순방향의 변환은 용이하지만, 변환 후의 값으로부터 원래의 값을 얻는 역변환이 곤란한 일방향성 함수라고 불리는 함수의 일종이다.

이와 같이, 비밀 정보를 확인하는 측과 확인되는 측의 쌍방에서 비밀 정보의 해시 값을 생성하고, 이것을 비교함에 의해 비밀 정보의 비밀 상태를 유지한 채로, 비밀 정보의 동일성을 확인할 수 있다.

인증 정보 메모리(40)는, 기기 인증 정보 등의 기기 인증을 행할 때에 사용하는 정보를 기억하는 기억 장치이다.

본 실시의 형태에서는, 인증 정보 메모리(40)에는 기기 ID(41), 암호화(기기 ID + 패스 프레이즈)(42)가 기억되어 있다.

기기 ID(41)는, CE 기기(9)를 식별하기 위한 ID 정보로서, 공장(5)이 기기 ID 관리기관으로부터 미리 취득하고, CE 기기(9)에 기록한 것이다.

암호화(기기 ID + 패스 프레이즈)(42)는, 기기 ID(41)의 후미에 패스 프레이즈를 배치한 것을 고유 키(23), 또는 고유 키(33)로 암호화한 것이다. 또한, 배치의 순서는 반대라도 좋다.

이후, 어떤 정보(A)의 후미에 있는 정보(B)를 배치한 정보를 (정보(A) + 정보(B)) 등으로 나타내는 것으로 하고, 또한 (정보(A) + 정보(B))를 암호화한 정보를 암호화(정보(A) + 정보(B)) 등으로 나타내는 것으로 한다.

예를 들면, 기기 ID(41)를 「123」으로 하고, 패스 프레이즈를 「abc」라고 한 경우, (기기 ID + 패스 프레이즈)는, 「123abc」로 된다. 그리고, 이것을 고유 키(23), 또는 고유 키(33)로 암호화한 것이 암호화(기기 ID + 패스 프레이즈)(42)로 된다.

패스 프레이즈는, 공장(5)이 CE 기기(9)에 기기 인증 정보를 조립할 때에 관리 서버(7)가 발행한 비밀 정보이다.

본 실시의 형태에서는, (기기 ID + 패스 프레이즈)를 기기 인증 정보로서 사용한다.

이와 같이, 패스 프레이즈에 기기 ID를 조합시킴에 의해 기기 인증 정보의 데이터량이 많아지기 때문에, 제삼자에 의한 암호화(기기 ID + 패스 프레이즈)(42)의 해독이 곤란해지고, 시큐어러티를 높일 수 있다.

또한, 복호화된 (기기 ID + 패스 프레이즈)와, 보내 오는 기기 ID를 CE 기기(9) 내에서 비교함에 의해, 기기 ID와 암호화(기기 ID + 패스 프레이즈)의 조합이 올바른 것을 검증할 수도 있다.

본체 식별 정보 메모리(50)는, CE 기기(9)의 본체를 식별하기 위한 정보가 기억되어 있다.

본체를 식별하기 위한 정보로서는, 네트워크상에서 CE 기기(9)를 식별하기 위한 CE 기기(9)에 고유한 정보인 MAC (Media Access Control) 어드레스(51)나, iLink 등으로 불리는 정보 등이 있다.

MAC 어드레스(51)는, CE 기기(9)에 유니크한 하드웨어 어드레스로서, 예를 들면 네트워크상에서 CE 기기(9)를 이동하였다고 하여도 변하지 않는다.

다음에, 이상과 같이 구성된 CE 기기(9)에 기기 인증 정보를 조립하는 순서, 조립한 기기 인증 정보를 확인하는 순서, 조립한 인증 정보를 이용하여 기기 인증을 행하는 순서에 관해 플로우 차트를 이용하여 설명한다.

도 4는, CE 기기(9)에 기기 인증 정보를 조립하는 준비 단계에서의 작업 순서를 설명하기 위한 플로우 차트이다.

우선, 사업체(11)가 CE 기기(9)를 기획한다(스텝 10). 이 작업은, 기획 담당자 등의 사람손에 의해 행하여지는 것이다.

다음에, 사업체(11)에 설치된 사업체 시스템으로부터 관리 서버(7)에 액세스하고, CE 기기(9)의 기록 모듈(30)에 조립하기 위한 기록 전 키(31)를 요구한다(스텝 12).

관리 서버(7)는, 도 8에 도시한 바와 같은 키 테이블(700)을 구비하고 있고, 키 테이블(700)로부터 기록 전 키(31)와 이 기록 전 키(31)를 다른 기록 전 키와 식별하는 키 식별자를 발행한다. 그리고 발행한 기록 전 키(31)와 키 식별자를 함께 사업체 시스템에 송신한다(스텝 20).

또한, 사업체(11)는, 제품의 기종을 특정하는 제품 코드와 후술하는 고유 키 생성자를 관리 서버에 요구하도록 구성할 수도 있다.

관리 서버(7)는, 제품 코드와 고유 키 생성자를 대응시켜 관리하고 있다.

사업체 시스템은, 관리 서버(7)로부터 기록 전 키(31)와 키 식별자를 수신하고, 기록 전 키(31)를 기록 모듈(30)에 조립하도록 구성된 펌웨어를 작성한다(스텝 14). 또한, 후술하는 고유 키 생성자도 펌웨어에 조립한다.

다음에, 사업체 시스템은, 작성한 펌웨어와 키 식별자, 및 CE 기기(9)의 기종을 특정하는 제품 코드를 공장(5)에 설치된 공장 시스템에 송신한다(스텝 16).

또한, 공장(5)에서는, 제품 코드로 특정되는 CE 기기(9)를 복수대 생산하지만, 어느 CE 기기(9)도 같은 기록 전 키(31)를 사용하는 것으로 한다. 그 때문에, 펌웨어와 키 식별자는 1조(組) 공장에 송신되고, 이 1조의 펌웨어와 키 식별자로부터 복수대의 CE 기기(9)가 생산된다.

공장 시스템은, 사업체 시스템으로부터 이들의 정보를 수신한다. 그리고 공장(5)은 수신한 제품 코드로 특정되는 CE 기기(9)의 제조를 시작한다.

이와 같이 하여 제조된 CE 기기(9)(펌웨어 조립 전)에 대해 공장 시스템은 제품 시리얼 번호를 발번(發番)한다(스텝 30).

제품 시리얼 번호는, 개개의 CE 기기(9)에 대해 고유한 번호로서, 예를 들면, 라벨 실에 숫자나 바코드 등으로서 인쇄되고, CE 기기(9)에 외부에서 참조 가능하게 부착된다.

또한, 본 실시의 형태에서는, 제품 시리얼 번호가 CE 기기(9)를 특정할 수 있는 정보인 것으로 하지만, 예를 들면, 제품 코드와 제품 시리얼 번호를 이용하여 CE 기기(9)를 특정할 수 있도록 구성할 수도 있다.

이 경우는, 기기 인증 서버(8)는, 제품 코드와 제품 시리얼 번호를 CE 기기(9)에 부착한다.

즉, CE 기기(9)를 특정할 수 있는 정보이면 좋다.

다음에, 공장 시스템은 CE 기기(9)에 펌웨어를 조립한다(스텝 32).

펌웨어의 조립은, CE 기기(9)의 커넥터로부터 펌웨어를 입력함에 의해 행하여진다.

또한, 사업체(11)가 펌웨어를 CD-ROM 등의 기억 매체에 기억시켜서 공장(5)에 송부하고, 공장(5)에서 이것을 CE 기기(9)에 판독하여 넣도록 구성할 수도 있다.

펌웨어의 조립에 의해, 기기 인증부(99)(도 3)가 CE 기기(9)의 내부에 형성된다.

또한, 공장 시스템은, 펌웨어를 조립할 때에, 미리 기기 ID 관리 기관으로부터 취득하여 둔 기기 ID(41)를 인증 정보 메모리(40)에 기억시킨다. 다만, 이 단계에서는 인증 정보 메모리(40)에는 암호화(기기 ID + 패스 프레이즈)(42)는 기억되어 있지 않다.

도 5는, CE 기기(9)에 기기 인증 정보를 조립하는(매입하는) 순서(즉, 인증 정보 메모리(40)에 암호화(기기 ID + 패스 프레이즈)(42)를 기억시키는 순서)를 설명하기 위한 플로우 차트이다.

또한, 이하의 처리는, CE 기기(9)에 접속 수단(10)이 접속된 상태에서 행한다.

공장 시스템은, 도 8에 도시한 바와 같은 키 식별자 관리 테이블(500)을 구비하고 있고, 제품(제품 코드)과 사업체 시스템으로부터 취득한 키 식별자를 대응시켜 관리하고 있다.

그리고, 공장 시스템은, 관리 서버(7)에 액세스하고, 패스 프레이즈의 발행을 요구함과 함께, 앞서 취득한 기기 ID(41)와 키 식별자 관리 테이블(500)에 기억되어 있는 CE 기기(9)의 키 식별자를 송신한다(스텝 40).

관리 서버(7)는, 패스 프레이즈의 발행 요구를 받아서 패스 프레이즈를 발행한다(스텝 50).

또한, 패스 프레이즈란, 문자나 숫자, 또는 기호 등의 문자열로 이루어지는 비밀 정보로서, 패스워드와 동종의 정보이다.

이와 같은 비밀 정보중, 문자열이 비교적 짧은 것을 패스워드라고 부르고, 비교적 긴 것을 패스 프레이즈라고 부르고 있다. 암호화한 경우에, 문자열이 길수록 제삼자에 의한 해독이 곤란해진다.

다음에, 관리 서버(7)는, 공장 시스템으로부터 수신한 키 식별자에 대응하는 기록 전 키(31)를 키 테이블(700)(도 8)로부터 취득한다.

그리고, 공장 시스템으로부터 수신한 기기 ID(41)와 스텝 50에서 발행한 패스 프레이즈로부터 (기기 ID + 패스 프레이즈)를 생성하고, 앞서 취득한 기록 전 키(31)에 이것을 암호화하여 암호화(기기 ID + 패스 프레이즈)(42)를 생성한다(스텝 52).

이 암호화(기기 ID + 패스 프레이즈)가 기기 인증 정보로서 사용된다.

관리 서버(7)는, CE 기기(9)와 마찬가지로, 기기측 확인 해시 함수(34)와, 서버측 확인 해시 함수(35)를 구비하고 있고, 기기측 확인 해시 함수(34)를 이용하여 앞서 생성한 (기기 ID + 패스 프레이즈)의 해시 값(제 1의 해시 값)을 생성한다(스텝 54}.

이 제 1의 해시 값은, 기기 인증 정보가 적절하게 조립되었는지의 여부를 CE 기기(9) 내부에서 판단할 때에 사용된다.

또한, 서버측 확인 해시 함수(35)는, 후에 CE 기기(9)에 기기 인증 정보가 적절하게 조립되었는지의 여부를 관리 서버(7)가 판단할 때에 사용된다.

관리 서버(7)는, 기기 ID(41), 생성한 암호화(기기 ID + 패스 프레이즈)(42), 및 제 1의 해시 값을 공장 시스템에 송신한다(스텝 56). 이것은, 원 정보 제공 수단에 대응한다.

또한, 관리 서버(7)는, 도 8에 도시한 발행필 기기 인증 정보 테이블(702)을 기억하고 있고, 기기 ID(41), 암호화(기기 ID + 패스 프레이즈)(42), 제 1의 해시 값을 공장 시스템에 송신함과 함께, 발행필 기기 인증 정보 테이블(702)을 갱신한다.

이로써, 발행한 패스 프레이즈와, 기기 ID(41), 키 식별자를 대응시킬 수 있다.

공장 시스템은, 이들의 정보를 관리 서버(7)로부터 수신하고, 이들의 정보를 접속 수단(10)을 통하여 CE 기기(9)에 입력한다(스텝 42).

그러면, CE 기기(9) 내부에서는, 기록 모듈(30)이 이들의 정보를 수신한다(스텝 60). 이것은, 암호화(기기 ID + 패스 프레이즈)(42)는, 원 정보에 대응하고, 그 때문에 기록 모듈(30)은 원 정보 취득 수단을 구비하고 있다.

또한, 제 1의 해시 값은 기기 인증 정보를 일방향성 함수로 변환한 변환치에 대응하고, 그 때문에, 기록 모듈(30)은 변환치 취득 수단을 구비하고 있다.

다음에, 기록 모듈(30)은 기록 전 키(31)를 이용하여 암호화(기기 ID + 패스 프레이즈)(42)를 복호화한다(스텝 62).

이 복호화에 의해, CE 기기(9)는 관리 센터(3)로부터 취득한 기기 인증 정보, 즉 (기기 ID + 패스 프레이즈)를 얻을 수 있다.

이와 같이, 기록 모듈(30)은 원 정보로부터 기기 인증 정보를 생성하는 생성 수단을 갖고 있다.

CE 기기(9)는 복호화한 (기기 ID + 패스 프레이즈)를 그대로 보존하여도 좋지만, 본 실시의 형태에서는 시큐어러티를 높이기 위해 (기기 ID + 패스 프레이즈)를 재차 암호화하여 보존하는 것으로 한다.

그 때문에, 기록 모듈(30)은, 우선 MAC 어드레스(51)와 고유 키 생성자(32)로부터 고유 키(33)를 생성한다(스텝 64).

이 스텝은, CE 기기(9)에 고유의 암호화 키를 얻는 것을 목적으로서, 한 예로서 MAC 어드레스(51)를 이용하여 고유 키(33)를 생성하지만, 이것으로 한정하는 것이 아니라, CE 기기(9)에 고유의 정보라면(예를 들면, 제품 시리얼 번호) 무엇이라도 좋다.

또한, 후술하는 바와 같이, 인증 모듈(20)도 고유 키(33)와 같은 암호화 키를 생성할 수 있고, 기록 모듈(30), 인증 모듈(20)은 모두 키 생성 수단을 갖고 있다.

다음에, 기록 모듈(30)은, 생성한 고유 키(33)를 이용하여 (기기 ID + 패스 프레이즈)를 암호화하여 암호화(기기 ID + 패스 프레이즈)(42)를 생성한다(스텝 66).

또한, 암호화에 사용하는 암호 키가 다르기 때문에 암호화(기기 ID + 패스 프레이즈)(42)와, 관리 서버(7)가 송신하여 온 암호화(기기 ID + 패스 프레이즈)는 다른 것이다.

다음에, 기록 모듈(30)은, 생성한 암호화(기기 ID + 패스 프레이즈)(42)를 인증 정보 메모리(40)에 기록하고(스텝 68), 인증 정보 메모리(40)는 암호화(기기 ID + 패스 프레이즈)(42)를 기억한다(스텝 70).

또한, 고유 키(33)는 기기 인증부(99)가 고유 키(33)를 소거하도록 구성되어 있는 경우는, 사용된 후 신속하게 소거된다(키 소거 수단).

이와 같이, 암호화(기기 ID + 패스 프레이즈)(42)는, CE 기기(9)에 고유하고, 게다가 동적으로 생성되는 고유 키(33)에 의해 암호화되어 있기 때문에, 시큐어러티를 높일 수 있다.

또한, 인증 정보 메모리(40)는 기억 수단을 구성하고 있다.

이상의 순서에 의해, 관리 서버(7)가 발행한 기기 인증 정보를 CE 기기(9)에 조립할 수 있다.

또한, 기기 인증 정보는 암호화된 상태 그대로 CE 기기(9)에 입력되기 때문에, 기기 인증 정보가 공장(5)에서 누출되는 것을 미연에 방지할 수 있고, 기기 인증 정보 조립시의 시큐어러티를 높일 수 있다.

또한, 기기 인증 정보는 Cp기기(9)에 고유한 암호 키로 암호화한 상태로 CE 기기(9)에 기억되기 때문에, CE 기기(9)를 출하한 후에 CE 기기(9)로부터 기기 인증 정보가 누출되는 것을 미연에 방지할 수 있고, 출하 후의 시큐어러티도 높일 수 있다.

도 6은, CE 기기(9)에 기기 인증 정보가 적절하게 조립된 것을 관리 센터(3), 및 공장(5)이 확인하는 순서를 설명하기 위한 플로우 차트이다.

이 순서는, CE 기기(9)의 커넥터에 접속 수단(10)이 접속한 상태에서 행하여진다. 통상은, 공장 시스템이 CE 기기(9)에 기기 인증 정보를 조립한 후, 자동적으로 행하여진다.

우선, 기기 인증부(99)에서, 기록 모듈(30)이 인증 정보 메모리(40)로부터 암호화(기기 ID + 패스 프레이즈)(42)를 판독하고, 인증 정보 메모리(40)로부터 기록 모듈(30)에 암호화(기기 ID + 패스 프레이즈)(42)가 제공된다(스텝 90).

다음에, 기록 모듈(30)은, 고유 키 생성자(32)와, MAC 어드레스(51)로부터 고유 키(33)를 생성하고(스텝 100), 이것을 이용하여 암호화(기기 ID + 패스 프레이즈)(42)를 복호화한다(스텝 102).

다음에, 기록 모듈(30)은 기기측 확인 해시 함수(34)를 이용하여, 복호화한 (기기 ID + 패스 프레이즈)의 해시 값(제 1의 해시 값)을 생성한다(스텝 104).

다음에, 기록 모듈(30)은 관리 서버(7)로부터 송신되어 온 제 1의 해시 값과, 스텝 104에서 생성한 해시 값을 비교하고, 이들의 해시 값이 일치하는지의 여부의 비교 결과를 얻는다(스텝 106).

이와 같이, 기록 모듈(30)은 변환치(제 1의 해시 값) 산출 수단과, 판단 수단을 구비하고 있다.

해시 값이 일치함에 의해, 관리 서버(7)가 생성한 (기기 ID + 패스 프레이즈)가, 인증 정보 메모리(40)에 기억되어 있는 (기기 ID + 패스 프레이즈)와 동일한 것을 확인할 수 있다.

다음에, 기록 모듈(30)은, 서버측 확인 해시 함수(35)를 이용하여 (기기 ID + 패스 프레이즈)의 해시 값(제 2의 해시 값)을 생성한다(스텝 108).

그리고, 기록 모듈(30)은, 인증 정보 메모리(40)로부터 기기 ID(41)를 판독하고, 스텝 106에서의 제 1의 해시 값의 비교 결과, 기기 ID, 제 2의 해시 값을 공장 시스템에 출력한다(스텝 110). 그리고, 제 2의 해시 값은 관리 서버(7)에 송신된다.

이와 같이, 기록 모듈(30)은 변환치 산출 수단과, 변환치 제공 수단을 구비하고 있다.

공장은, CE 기기(9)로부터 출력된 비교 결과에 의해, 기기 인증 정보가 CE 기기(9)에 적절하게 조립되었는지의 여부를 알 수 있다.

해시 값이 일치하지 않은 경우는 기기 ID(41)를 폐기하고, 새로운 기기 ID를 채용하여 재차 기기 인증 정보의 조립을 시도한다.

조립에 실패한 기기 ID(41)를 재차 이용하는 것도 가능하지만, 착오 등에 의해 같은 기기 ID의 CE 기기(9)가 복수 시장에 출회되는 것을 방지하기 위해, 본 실시의 형태에서는 조립에 실패한 기기 ID(41)는 폐기하는 것으로 하였다.

또한, 종래의 제조 공정에서는, 기기 인증 정보의 기밀성을 유지하기 위해 일단 CE 기기(9)에 조립한 후는, 적절하게 기기 인증 정보가 조립되었는지의 여부를 조사하는 것은 곤란하고, 확인을 행하지 않는 경우도 있다.

그러나, 본 실시의 형태에서는, 기기 인증 정보의 해시 값을 CE 기기(9) 내부에서 비교함에 의해, 기기 인증 정보의 기밀성을 CE 기기(9) 내부에서 유지한 채로 기기 인증 정보가 조립되었는지의 여부를 조사할 수 있다.

공장 시스템은, 기기 인증 정보가 적절하게 CE 기기(9)에 조립된 것을 확인한 후, CE 기기(9)로부터 얻은 기기 ID(41)와 제 2의 해시 값에, CE 기기(9)의 제품 시리얼 번호를 부가하여 관리 서버(7)에 송신한다(스텝 120).

관리 서버(7)는, 이들의 정보를 공장 시스템으로부터 수신하고, 발행필 기기 인증 정보 테이블(702)(도 8)을 이용하여 기기 ID(41)로부터 패스 프레이즈를 검색한다(스텝 130).

이와 같이, 관리 서버(7)는 변환치(제 2의 해시 값) 취득 수단을 구비하고 있다. 다음에, 관리 서버(7)는 기기 ID(41)와 검색한 패스 프레이즈로부터 (기기 ID + 패스 프레이즈)를 생성하고, 이로부터 서버측 확인 해시 함수(35)를 이용하여 제 2의 해시 값을 생성한다(변환치 산출 수단).

그리고, 공장 시스템으로부터 수신한 제 2의 해시 값과, 앞서 생성한 제 2의 해시 값이 일치하는지의 여부를 판단한다(판단 수단)(스텝 132).

제 2의 해시 값이 일치함에 의해, 관리 서버(7)는 CE 기기(9)에 대한 기기 인증 정보의 조립이 성공한 것을 알 수 있다.

역으로 제 2의 해시 값이 일치하지 않은 경우, 기기 인증 정보의 조립이 실패한 것을 알 수 있다.

관리 서버(7)는, 도 8에 도시한 바와 같은 기기 인증 테이블(704)을 구비하고 있고, 기기 ID(41), 패스 프레이즈, 제품 시리얼 번호를 대응시켜 기억하고 있다.

제 2의 해시 값이 일치한 경우, 관리 서버(7)는 기기 ID(41)와 제품 시리얼 번호를 패스 프레이즈와 함께 묶어서 기기 인증 테이블(704)에 기억한다(스텝 134).

또한, 기기 인증 테이블(704)은 기기 인증 서버(8)에 제공되고, 기기 인증 서버(8)가 기기 인증을 행하지만 이용된다(기기 인증 정보 제공 수단).

다음에, 관리 서버(7)는, 공장 시스템으로부터 수신한 데이터(기기 ID(41), 제품 시리얼 번호, 제 2의 해시 값)에, 데이터를 수신한 날(日)의 일자 정보를 부가하여 비밀키로 서명(전자 서명)하여 공장에 송신한다(판단 결과 송신 수단)(스텝 136).

공장 시스템(원 정보 조립 주체)은, 이것을 수신하고, 기기 인증 정보가 적절하게 CE 기기(9)에 조립된 것을 확인한다(스텝 122).

이로써, 공장 시스템측에서는 관리 서버(7)에 기기 ID(41), 제품 시리얼 번호, 제 2의 해시 값(이들로서 제조 실적으로 할 수 있다)을 수취하여 받은 것을 확인할 수 있다.

그리고, 공장(5)은 제조가 완료된 CE 기기(9)를 출하한다.

도 7은, 기기 인증 서버(8)가 CE 기기(9)를 기기 인증하는 순서를 설명하기 위한 플로우 차트이다.

우선, 기기 인증부(99)(도 3)의 인증 모듈(20)이, 인증 정보 메모리(40)로부터 암호화(기기 ID + 패스 프레이즈)(42)를 판독하고, 인증 정보 메모리(40)로부터 인증 모듈(20)에 암호화(기기 ID + 패스 프레이즈)(42)가 제공된다(스텝 140).

다음에, 인증 모듈(20)은, 고유 키 생성자(22)와 MAC 어드레스(51)를 이용하여 고유 키(23)를 생성한다(스텝 150).

그리고 인증 모듈(20)은, 암호화(기기 ID + 패스 프레이즈)(42)를 고유 키(23)를 이용하여 복호화하고 (기기 ID + 패스 프레이즈)를 취득하고(스텝 152), 기기 인증 서버(8)에 송신한다(스텝 154). 이와 같이, 인증 모듈(20)은 기기 인증 정보 송신 수단을 구비하고 있다.

또한, CE 기기(9)와 기기 인증 서버(8) 사이의 통신 경로는, 예를 들면, SSL(Secure Sockets Layer) 등의 암호화 기술을 사용하여 안전한 것으로 되어 있다.

기기 인증 서버(8)는, CE 기기(9)로부터 (기기 ID + 패스 프레이즈)를 수신하고, 이것을 공개 키(21)에 대응하는 비밀키로 복호화하고, 관리 센터(3)로부터 제공된 기기 인증 테이블(704)의 패스 프레이즈와 대조하여 CE 기기(9)를 기기 인증한다(스텝 160).

또한, 기기 인증 테이블(704)을 이용하여 CE 기기(9)의 제품 시리얼 번호를 특정한다(스텝 162).

이상의 순서에 의해 기기 인증 처리는 행하여진다.

도 9는, CE 기기(9)의 하드웨어적인 구성의 한 예를 도시한 도면이다.

CPU(Central Processing Unit)(121)은, ROM(Read Only Memory)(122)에 기억되어 있는 프로그램이나, 기억부(128)로부터 RAM(Random Access Memory)(123)에 로드된 프로그램에 따라 각종의 처리를 실행하는 중앙 처리 장치이다.

ROM(122)은, CE 기기(9)를 기능시키는데 필요한 기본적인 프로그램이나 파라미터 등으로 구성되어 있다.

RAM(123)은, CPU(121)가 각종의 처리를 실행하지만 필요한 워킹 에어리어를 제공한다.

기억부(128)는, CE 기기(9)가 기능하기 위해 필요한 각 프로그램이나 데이터를 기억하고 있고, 예를 들면, 하드 디스크나 반도체 메모리 등의 기억 장치에 의해 구성되어 있다.

사업체(11)에서 작성된 펌웨어는, 공장(5)에서 기억부(128)에 기억되고, 이 펌웨어가 CPU(121)에서 실행됨에 의해, 기기 인증부(99)(도 3)의 각 구성 요소가 생성된다.

기억부(128)에 기억되어 있는 다른 프로그램으로서는, 파일의 입출력을 행하거나, CE 기기(9)의 각 부분을 제어하는 등, 기본적인 기능을 실현하기 위한 OS(Operating System) 등이 있다.

CPU(121), ROM(122), 및 RAM(123)은 버스(124)를 통하여 상호 접속되어 있다. 이 버스(124)에는 입출력 인터페이스(125)도 접속되어 있다.

입출력 인터페이스(125)에는 키보드, 마우스 등으로 이루어지는 입력부(126), CRT(Cathode-ray Tube), LCD(Liquid Crystal Disp1ay) 등으로 이루어지는 디스플레이, 및 스피커 등에 의해 이루어지는 출력부(127), 하드 디스크 등에 의해 구성되는 기억부(128), 모뎀, 터미널 어댑터 등에 의해 구성되는 통신부(129)가 접속되어 있다.

통신부(129)는, 네트워크를 통한 통신 처리를 행하는 기능부로서, 예를 들면, 접속 수단(10)과 접속하여 기기 인증 정보의 입력을 접수하거나, 또는, 기기 인증 서버(8)와 접속하여 기기 인증을 행하기 위한 통신을 행하거나 한다.

또한, 입출력 인터페이스(125)에는 필요에 따라 드라이브(130)가 접속되고, 자기 디스크(141), 광디스크(142), 광자기 디스크(143), 또는 메모리 카드(144) 등이 적절히 장착되고, 그들로부터 판독된 컴퓨터 프로그램이, 필요에 따라 기억부(128)에 인스톨된다.

또한, 관리 서버(7), 기기 인증 서버(8)의 구성은 기본적으로 CE 기기(9)와 같기 때문에 설명은 생략한다.

이상으로 설명한 제 1의 실시의 형태에 의해, 기기 인증할 때에 필요하게 되는 기기 인증 정보(기기 ID + 패스 프레이즈)를, 관리 서버(7)로부터 CE 기기(9)에 안전하게 송신할 수 있다. 또한, 기기 인증 정보가 올바르게 기록된 것을 공장(5)이나 관리 서버(7)가 확인하는 것이 가능해진다.

이상으로 설명한 제 1의 실시의 형태에 의한 효과를 종래의 문제점과 대비하면서 열거한다면 이하와 같이 된다.

(1) 종래에는, 기기 인증 정보인 (기기 ID + 패스 프레이즈)가 평문(平文)으로 CE 기기(9)에 입력되어 있기 때문에, 의도의 여하에 관계 없이 공장(5)의 작업자 등의 눈에 띄어 버릴 가능성이 있다. 이에 대해, 본 실시의 형태에서는, 이 문제를 (기기 ID + 패스 프레이즈)를 암호화한 채로 CE 기기(9)에 입력함에 의해 대응하였다.

(2) 종래에는, 예를 들면 기기 인증 정보를 암호화하여 공장(5)에 송신하였다고 하여도, 제품마다, 공장마다 기기 인증 정보의 조립 방식의 통일을 취할 수 없고, 시큐어러티 레벨의 편차가 생겨 버릴 가능성이 있다. 이에 대해, 본 실시의 형태에서는, 기기 인증 정보의 조립 방식을 공통화함에 의해, 시큐어러티 레벨의 편차를 경감할 수 있다.

(3) 종래에는, 암호화 키가 누출됨에 의해 다른 CE 기기(9)에 영향이 미치는 경우가 있다. 이에 대해, 본 실시의 형태에서는, CE 기기(9)마다 고유한 고유 키(23)를 생성함에 의해 예를 들면 고유 키(23)가 누출되었다고 하여도 다른 CE 기기(9)에 영향이 미치는 일은 없다.

또한, 기록 전 키(31)에 관해서는, 키의 단위를 제품마다 이거나 시기마다 등으로 함으로써 영향 범위를 한정할 수 있다.

(4) 종래에는, CE 기기(9) 내에 올바르게 기기 인증 정보가 기록된 것을 공장(5)이나, 기기 인증 정보의 발행원인 관리 센터(3)가 확인하는 것이 곤란하였다. 이에 대해, 본 실시의 형태에서는, 해시 값 등의 고유 정보를 사용하여 공장(5)이나 관리 센터(3)가 기기 인증 정보가 올바르게 조립된 것을 확인할 수 있다.

(5) 종래에는, 관리 센터(3)가 올바르게 실적 보고를 수취한 것을 공장(5)이 확인하는 것은 곤란하였다. 이에 대해, 본 실시의 형태에서는 관리 서버(7)가 공장 시스템으로부터 수신한 데이터에 일시 정보를 부가하여 전자 서명하고, 이것을 공장 시스템에 송신하도록 하였다.

(6) 종래에는, 기기 인증 정보로서, 전자 증명서 등의 다른 정보를 이용하는 것은 곤란하였다. 이에 대해 본 실시의 형태는 전자 증명서를 사용한 인증 방식에도 적용할 수 있다.

또한, 본 실시의 형태에서는, 한 예로서, 기기 인증 정보를 네트워크 경유로 공장(5)에 송신하여 접속 수단(10)으로부터 CE 기기(9)에 입력하였지만, 기기 인증 정보는 암호화한 채로 CE 기기(9)에 입력되기 때문에, 예를 들면, CD-ROM 등의 기억 매체에 기억하여 공장(5)에 송부하고, 공장(5)에서 기억 매체나 CE 기기(9)에 기기 인증 정보를 기록하도록 구성하여도 좋다.

또한, 본 실시의 형태에서는, 한 예로서, 관리 서버(7)로부터 송신되어 온 암호화(기기 ID + 패스 프레이즈)를 기록 전 키로 복호화한 후에 인증 정보 메모리(40)에 기억하도록 구성하였지만, 이외에, 관리 서버(7)로부터 송신되어 온 암호화(기기 ID + 패스 프레이즈)를 복호화하지 않고 인증 정보 메모리(40)에 기억하고, 기기 인증시에 기록 전 키로 복호화하도록 구성할 수도 있다.

다음에, 제 2의 실시의 형태에 관해 설명한다.

[제 2의 실시의 형태의 개요]

도 10은, 제 2의 실시의 형태의 개요를 설명하기 위한 도면이다.

본 실시의 형태에서는, 기기 인증 정보를 생성하는 기초가 되는 원 정보를 관리 서버(7)와 CE 기기(9)에서 같은 로직을 이용하여(예를 들면, 같은 암호 키를 이용하여 같은 암호 방식에 의해 암호화하여) 변환하고, 기기 인증 정보를 생성한다.

우선, 관리 서버(7)는, 원 정보를 공장(5)에 송신함과 함께, 원 정보를 변환하여 기기 인증 정보를 생성한다.

한편, 공장(5)에서는, 접속 수단(10)을 통하여 원 정보를 CE 기기(9)에 입력한다. CE 기기(9)는 입력된 원 정보를 변환하여 기기 인증 정보를 생성한다.

이상과 같이 하여, 관리 서버(7)와 CE 기기(9)는 기기 인증 정보를 공유할 수 있다.

또한, 가령 원 정보가 외부에 누출되었다고 하여도 로직을 모르면 기기 인증 정보를 알 수 없다.

이상과 같이, 기기 인증 정보는, CE 기기(9)의 내부에서 생성되기 때문에, 공장(5)에서 평문으로 출력되는 것을 방지할 수 있다.

[제 2의 실시의 형태의 상세]

제조 인증 시스템(1)의 구성(도 2), 및 기기 인증부(99)(도 3)는, 제 1의 실시의 형태와 같기 때문에 설명을 생략한다.

또한, 제 1의 실시의 형태와 같은 구성 요소에는 같은 부호를 붙여서 설명한다.

이하에, CE 기기(9)에의 기기 인증 정보가 조립, 조립의 확인, 및 기기 인증의 방법에 관해 플로우 차트를 이용하여 설명한다.

또한, CE 기기(9)에 기기 인증 정보를 조립하기 전(前) 준비는, 제 1의 실시의 형태와 같기 때문에(도 4) 설명을 생략한다.

관리 서버(7)는, 제 1의 실시의 형태와 마찬가지로, 도 14에 도시한 바와 같은 키 테이블(706)을 구비하고 있고, 키 식별자와 기록 전 키(31)를 대응시켜 관리하고 있다.

도 11은, CE 기기(9)에 기기 인증 정보를 조립하는 순서를 설명하기 위한 플로우 차트이다.

CE 기기(9)는, 이미 조립이 되어 있고, 커넥터에 접속 수단(10)이 접속된 상태로 되어 있는 것으로 한다.

우선, 공장 시스템은, 관리 서버(7)에 대해 패스 프레이즈의 발행을 요구함과 함께, 미리 기기 ID 관리 기관으로부터 취득하여 둔 기기 ID(41)를 관리 서버(7)에 송신한다(스텝 200).

또한, 이 기기 ID(41)는 인증 정보 메모리(40)에도 기억시킨다.

이에 대해, 관리 서버(7)는 패스 프레이즈를 발행한다(스텝 210).

관리 서버(7)는, 도 14에 도시한 바와 같은 발행필 기기 인증 정보 테이블(708)을 구비하고 있고, 공장 시스템으로부터 수신한 기기 ID(41)와, 이 기기 ID(41)에 대해 발행한 패스 프레이즈를 대응시켜 기억하고 있다.

그리고, 관리 서버(7)는, 패스 프레이즈를 발행한 후, 기기 ID(41)와 패스 프레이즈를 묶어서 발행필 기기 인증 정보 테이블(708)에 기억한다(스텝 212).

다음에, 관리 서버(7)는 기기 ID(41)와 패스 프레이즈로부터 (기기 ID + 패스 프레이즈)를 생성하고, 공장 시스템에 송신한다(스텝 214).

이 (기기 ID + 패스 프레이즈)가 기기 인증 정보를 생성하기 위한 원 정보가 된다.

공장 시스템은, 관리 서버(7)로부터 (기기 ID + 패스 프레이즈)를 수신하고(스텝 202), 접속 수단(10)을 통하여 CE 기기(9)에 입력한다(스텝 204).

CE 기기(9) 내부에서는, 기록 모듈(30)이 (기기 ID + 패스 프레이즈)를 수신하고(스텝 220), 기록 전 키(31)를 이용하여 이것을 암호화하여 암호화(기기 ID + 패스 프레이즈)(42)를 생성한다(스텝 222).

본 실시의 형태에서는, (기기 ID + 패스 프레이즈)를 원 정보로 하여 암호화(기기 ID + 패스 프레이즈)(42)를 생성하고, 암호화(기기 ID + 패스 프레이즈)(42)를 기기 인증 정보로서 사용한다.

즉, (기기 ID + 패스 프레이즈)를, 기록 전 키(31)를 이용한 변환식에 의해 변환하고, 변환 후의 값인 암호화(기기 ID + 패스 프레이즈)(42)를 기기 인증 정보로서 사용한다.

다음에, 기록 모듈(30)은 고유 키 생성자(32)와 MAC 어드레스(51)로부터 고유 키(33)를 생성하고(스텝 224), 생성한 고유 키(33)에 의해 암호화(기기 ID + 패스 프레이즈)(42)를 재차 암호화한다(스텝 226).

이것은, 본 실시의 형태에서는, 암호화(기기 ID + 패스 프레이즈)(42)를 기기 인증 정보로서 사용하기 때문에, 이것을 다시 암호화된 상태로 CE 기기(9)에서 보존함에 의해 시큐어러티를 높이는 것이다.

이후, 암호화(정보(A) + 정보(B))를 재차 암호화한 것을 재차 암호화(정보(A) + 정보(B)) 등이라고 기재하기로 한다.

기록 모듈(30)은, 이와 같이 하여 생성한 재차 암호화(기기 ID + 패스 프레이즈)(42)(재차 암호화(기기 ID + 패스 프레이즈)(42a)라고 한다)를 인증 정보 메모리(40)에 기록하고(스텝 228), 인증 정보 메모리(40)는 재차 암호화(기기 ID + 패스 프레이즈)(42a)를 기억한다(스텝 230).

이와 같이, 본 실시의 형태에서는, 인증 정보 메모리(40)에 기기 ID(41)와, 재차 암호화(기기 ID + 패스 프레이즈)(42a)가 기억되어 있다.

도 12는, CE 기기(9)에 기기 인증 정보가 적절하게 조립된 것을 관리 센터(3), 및 공장(5)이 확인하는 순서를 설명하기 위한 플로우 차트이다.

이 순서는, CE 기기(9)의 커넥터에 접속 수단(10)이 접속한 상태에서 행하여진다. 통상은, 공장 시스템이 CE 기기(9)에 기기 인증 정보를 조립한 후, 자동적으로 행하여진다.

우선, 기록 모듈(30)이 인증 정보 메모리(40)로부터 재차 암호화(기기 ID + 패스 프레이즈)(42a)를 판독하고, 인증 정보 메모리(40)로부터 기록 모듈(30)에 재차 암호화(기기 ID + 패스 프레이즈)(42a)가 제공된다(스텝 240).

다음에, 기록 모듈(30)은, 고유 키 생성자(32)와, MAC 어드레스(51)로부터 고유 키(33)를 생성하고(스텝 250), 이것을 이용하여 재차 암호화(기기 ID + 패스 프레이즈)(42a)를 복합화하고, 암호화(기기 ID + 패스 프레이즈)(42)를 얻는다(스텝 252).

다음에, 기록 모듈(30)은, 서버측 확인 해시 함수(35)를 이용하여 암호화(기기 ID + 패스 프레이즈)(42)로부터 제 2의 해시 값을 생성하고(스텝 254), 공장 시스템에 출력한다(스텝 256).

제 1의 실시의 형태에서는, (기기 ID + 패스 프레이즈)로부터 제 2의 해시 값을 생성하였지만, 제 2의 실시의 형태에서는, 암호화(기기 ID + 패스 프레이즈)(42)로부터 제 2의 해시 값을 생성한다.

또한, 제 2의 실시의 형태에서는 제 1의 해시 값은 이용하지 않는다.

공장 시스템은, CE 기기(9)로부터 출력된 제 2의 해시 값에, 기기 ID(41), 제품 시리얼 번호, 키 식별자를 부가하여 관리 서버(7)에 송신한다(스텝 260).

관리 서버(7)는, 공장 시스템으로부터 수신한 기기 ID(41)를 발행필 기기 인증 정보 테이블(708)(도 14)에서 검색하고, 이 CE 기기(9)에 대해 발행한 패스 프레이즈를 취득한다(스텝 270).

다음에, 관리 서버(7)는, 공장 시스템으로부터 수신한 키 식별자를 키 테이블(706)에서 검색하고, CE 기기(9)에 기억되어 있는 것과 같은 기록 전 키(31)를 취득한다(스텝(272)).

다음에, 관리 서버(7)는, 공장 시스템으로부터 수신한 기기 ID(41)와, 스텝 270에서 검색한 패스 프레이즈를 이용하여 (기기 ID + 패스 프레이즈)를 생성하고, 이것을 스텝(272)에서 검색한 기록 전 키(31)로 암호화하여 암호화(기기 ID + 패스 프레이즈)(42)를 생성한다(스텝 274).

다음에, 관리 서버(7)는, 생성한 암호화(기기 ID + 패스 프레이즈)(42)를 서버측 확인 해시 함수(35)를 이용하여 해시화하여, 제 2의 해시 값을 생성한다(스텝 276).

다음에, 관리 서버(7)는, 스텝 276에서 생성한 제 2의 해시 값과, 공장 시스템으로부터 수신한 제 2의 해시 값의 일치를 비교함에 의해, CE 기기(9)에 기기 인증 정보가 적절하게 조립된 것을 확인한다(스텝 278).

관리 서버(7)는, 도 14에 도시한 바와 같은 기기 인증 테이블(710)을 구비하고 있고, 기기 ID(41), 암호화(기기 ID + 패스 프레이즈)(42)(즉, 기기 인증 정보), 제품 시리얼 번호, 키 식별자를 대응시켜 기억하고 있다.

관리 서버(7)는, 제 2의 해시 값의 비교에 의해, 기기 인증 정보가 CE 기기(9)에 적절하게 조립된 것을 검지하면, 이 암호화(기기 ID + 패스 프레이즈)(42)에, 기기 ID(41), 제품 시리얼 번호, 키 식별자를 묶어서 기기 인증 테이블(710)에 기억한다(스텝 280).

또한, 기기 인증 테이블(710)은 기기 인증 서버(8)에 제공되고, CE 기기(9)를 기기 인증할 때에 이용된다.

다음에, 관리 서버(7)는 공장 시스템으로부터 수신한 데이터에, 수신한 일시 정보를 부가하여 비밀로 전자 서명하고, 공장 시스템에 송신한다(스텝 282).

공장 시스템은, 전자 서명을 확인하고, 기기 인증 정보가 CE 기기(9)에 적절하게 조립된 것을 확인한다(스텝 262).

공장(5)은, 기기 인증 정보가 조립된 것을 확인한 후, CE 기기(9)를 시장에 출하한다.

도 13은, 기기 인증 서버(8)가 CE 기기(9)를 기기 인증하는 순서를 설명하기 위한 플로우 차트이다.

우선, 기기 인증부(99)(도 3)의 인증 모듈(20)이, 인증 정보 메모리(40)로부터 재차 암호화(기기 ID + 패스 프레이즈)(42a)를 판독하고, 인증 정보 메모리(40)로부터 인증 모듈(20)에 재차 암호화(기기 ID + 패스 프레이즈)(42a)가 제공된다(스텝 290).

다음에, 인증 모듈(20)은, 고유 키 생성자(22)와 MAC 어드레스(51)를 이용하여 고유 키(23)를 생성한다(스텝 300).

그리고 인증 모듈(20)은, 재차 암호화(기기 ID + 패스 프레이즈)(42a)를 고유 키(23)를 이용하여 복호화하여 암호화(기기 ID + 패스 프레이즈)(42)를 취득하고(스텝 302), 공개 키(21)로 암호화하여, 기기 ID(41)와 함께 기기 인증 서버(8)에 송신한다(스텝 304).

기기 인증 서버(8)는, CE 기기(9)로부터 암호화(기기 ID + 패스 프레이즈)(42)를 수신하고, 이것을 공개 키(21)에 대응하는 비밀키로 복호화한다. 그리고, 관리 센터(3)로부터 제공된 기기 인증 테이블(710)을 기기 ID(41)로 검색하고, CE 기기(9)의 암호화(기기 ID + 패스 프레이즈)(42)를 특정한다. 그리고 특정한 암호화(기기 ID + 패스 프레이즈)(42)와, 수신한 암호화(기기 ID + 패스 프레이즈)(42)를 대조하여 CE 기기(9)를 기기 인증한다(스텝 310).

또한, 기기 인증 테이블(710)을 이용하여 CE 기기(9)의 제품 시리얼 번호를 특정한다(스텝 312).

이상의 순서에 의해 CE 기기(9)의 기기 인증이 행하여진다.

이상으로 설명한 제 2의 실시의 형태에 의한 효과를 종래의 문제점과 대비하면서 열거한다.

(1) 종래에는, 관리 서버(7)에 기기 인증 정보를 요구하는 경우, CE 기기(9)에 매입되어 있는 기록 전 키(31)에 따른 암호화 패스 프레이즈를 요구할 필요가 있다. 그러나, 본 실시의 형태에서는, CE 기기(9)에 매입되어 있는 기록 전 키(31)를 의식하지 않고 (기기 ID + 패스 프레이즈)를 관리 서버(7)에 요구할 수 있다.

(2) 종래에는, CE 기기(9)의 제조가 정지한 경우, 취득하여 둔 (기기 ID + 패스 프레이즈)가 필요없게 되어 버린다. 그러나, 본 실시의 형태에서는, 관리 서버(7)로부터 취득한 (기기 ID + 패스 프레이즈)는 어느 CE 기기에서도 이용할 수 있기 때문에, (기기 ID + 패스 프레이즈)가 남은 경우는 다른 CE 기기에 융통할 수 있다.

(3) 종래에는, CE 기기(9)의 제조 라인을 고려에 넣는다면 자유로운 기록 전 키(31)의 단위의 설정을 할 수 없었다. 이에 대해, 본 실시의 형태에서는, 제조 라인을 걱정한 일 없이 기록 전 키(31)의 단위를 설정할 수 있다.

또한, 본 실시의 형태에서는, 관리 서버(7)에서 원 정보, (즉 (단말 ID + 패스 프레이즈))로부터 기기 인증 정보 (즉, 암호화 (단말 ID + 패스 프레이즈))를 생성하고, 기기 인증 서버(8)에 제공하였지만, 이것으로 한정되지 않고, 관리 서버(7)는 원 정보를 기기 인증 서버(8)에 제공하고, 기기 인증 서버(8)에서 원 정보로부터 기기 인증 정보를 생성하도록 구성할 수도 있다.

[제 3의 실시의 형태]

다음에, 제 3의 실시의 형태에 관해 설명한다.

이 실시의 형태는, 기기 인증 정보를 암호화·복호화하기 위한 키 정보가 포함되어 있는 어플리케이션(기기 인증 클라이언트)을 갱신하는 것이다.

기기 인증 클라이언트는, CE 기기이나 퍼스널 컴퓨터 등에 인스톨되고, 기기 인증부(99)(도 3)와 같은 모듈이 형성된다. 그리고, 모듈에 포함되는 공개 키(공개 키(21)에 대응)는, 사용 기한 등이 설정되어 있고, 신규의 것으로 갱신할 필요가 있는 경우가 있다.

종래에는, 이와 같은 경우, 기기 인증 클라이언트를 전부 새로운 것으로 교환할 필요가 있다.

본 실시의 형태에서는, 기기 인증 클라이언트에 포함되는 기기 인증부(99)에 대응하는 모듈을 새로운 것으로 교환함에 의해, 이 모듈에 포함되는 공개 키의 갱신을 행한다.

이하, CE 기기(9)의 기기 인증부(99)를 갱신하는 경우를 예로 들어, 도 15의 플로우 차트를 이용하면서 갱신의 순서를 설명한다.

또한, 갱신 서버는, 기기 인증 클라이언트를 갱신하는 서비스를 제공하는 서버 장치이고, 갱신 서버와, 기기 인증 서버는, 제품 코드(제품의 기종을 특정한 코드)와 고유 키 생성자(生成子)와의 대응 관계를 동기 시켜 보존하고 있는 것으로 한다.

또한, 대상 기기는 갱신의 대상이 되는 기기 인증 클라이언트를 구비한 단말 기기이다.

우선, 대상 기기가 갱신 서버에 액세스하고, 모듈(기기 인증 클라이언트에 조립된 기기 인증부(99))의 갱신을 요구한다(스텝 400).

이에 대해, 갱신 서버는 대상 기기의 기기 인증을 요구한다(스텝 410).

대상 기기는, 기기 인증 서버에 액세스하고, 기기 인증 서버가 기기 인증을 행한다(스텝 402, 스텝 422).

이때에, 기기 인증 서버는, 원 타임 ID를 발행하여, 대상 기기의 제품 코드와 대응시켜 기억함과 함께, 이 원 타임 ID를 대상 기기에 송신한다.

대상 기기는, 기기 인증 서버로부터 원 타임 ID를 수신하여, 이것을 갱신 서버에 송신한다(스텝 404).

갱신 서버는, 대상 기기로부터 원 타임 ID를 수신하고, 이것을 기기 인증 서버에 송신한다(스텝 412).

기기 인증 서버는, 갱신 서버로부터 원 타임 ID를 수신하고, 이것에 대응시켜 놓은 제품 코드를 갱신 서버에 송신한다(스텝 424).

갱신 서버는, 기기 인증 서버로부터 제품 코드를 수신하여, 갱신 대상으로 되어 있는 기기 인증 클라이언트를 특정한다.

그리고, 대상 기기와 통신하고, 대상 기기측의 기기 인증 클라이언트의 버전과 최신 버전의 비교 등을 행하고 다운로드하는 모듈을 확인한다(스텝 406, 스텝 414).

다음에, 갱신 서버는, 제품 코드에 대응하는 고유 키 생성자를 검색하고(스텝 416), 이 고유 키 생성자에 대응한 모듈을 생성한다(스텝 418).

이때에, 모듈에 포함되는 공개 키는 최신의 것으로 되어 있다.

그리고, 갱신 서버는 생성한 모듈을 대상 기기에 다운로드한다(스텝 420).

대상 기기는, 다운로드한 모듈을 보존한다(스텝 408).

이상과 같이, 본 실시의 형태에서는 모듈을 갱신함에 의해 모듈에 포함되는 공개 키를 갱신할 수 있다.

[제 4의 실시의 형태]

제 1의 실시의 형태에서는. CE 기기(9)는 제 2의 해시 값을 출력하여 관리 서버(7)에 송신하고, 관리 서버(7)가 이것을 확인하였지만. 본 실시의 형태에서는. CE 기기(9)는 제 1의 해시 값의 확인 결과를 관리 서버(7)에 송신한다.

도 16은. 본 실시의 형태의 기기 인증부(99a) 구성의 한 예를 도시한 도면이다. 제 1의 실시의 형태와 같은 구성 요소에는 같은 번호를 붙이고, 설명을 생략한다.

기기 인증부(99a)는. 제 1의 해시 값의 확인 결과를 관리 서버(7)에 송신하는 인증 정보 기록 확인 모듈(36)을 구비한다.

또한, 기록 모듈(30a)은. 관리 서버(7)에 제 2의 해시 값을 송신할 필요가 없기 때문에, 서버측 확인 해시 함수(35)(도 3)를 구비하고 있지 않다.

기록 모듈(30a)은. 관리 센터(3)로부터 송신되어 온 제 1의 해시 값과. 기기측 확인 해시 함수(34)에 의한 제 1의 해시 값을 비교하고, 그 비교 결과를 인증 정보 기록 확인 모듈(36)에 출력한다.

인증 정보 기록 확인 모듈(36)은. 또한 기기 ID를 취득하고, 확인 결과와 함께 접속 수단(10)을 경유하여 공장 시스템에 출력한다.

공장 시스템은. 이것에 또한 시리얼 번호를 부가하여 관리 서버(7)에 송신하고, 관리 센터(3)는. 확인 결과를 수취함에 의해 CE 기기(9)에 기기 인증 정보가 조립된 것을 확인할 수 있다.

도 17은. 본 실시의 형태에서, CE 기기에 기기 인증 정보가 적절하게 조립된 것을 확인하는 순서를 설명하기 위한 플로우 차트이다.

도 6의 플로우 차트와 같은 처리에는 같은 스텝 번호를 붙이고, 설명을 생략 또는 간략화한다.

스텝 90 내지 스텝 106까지는 제 1의 실시의 형태와 같다.

다만, 스텝 106에서는 기록 모듈(30a)은. 기기측 확인 해시 함수(34)를 이용하여 생성한 제 1의 해시 값과 관리 서버(7)로부터 수신한 제 1의 해시 값이 동일한지의 여부를 비교하고, 그 비교 결과를 인증 정보 기록 확인 모듈(36)에 출력한다(스텝 106).

인증 정보 기록 확인 모듈(36)은. 기록 모듈(30a)로부터 비교 결과를 취득하고, 또한, 인증 모듈(20)을 경유하는 등으로 기기 ID(41)를 취득하고, 이들을 접속 수단(10)을 경유하여 공장 시스템에 출력한다(스텝 502).

공장 시스템은. 인증 정보 기록 확인 모듈(36)로부터 출력된 비교 결과, 및 기기 ID에 제품 시리얼 번호를 부가하고, 관리 서버(7)에 송신한다(스텝 504).

관리 서버(7)는. 공장 시스템으로부터 이들의 정보를 수신한다. 그리고, 비교 결과에 의해 관리 서버(7)가 송신한 제 1의 해시 값과 기기측 확인 해시 함수(34)를 이용하여 생성된 제 1의 해시 값이 동일한 것을 확인하고, 이로써, 기기 인증 정보가 CE 기기(9)에 기억된 것을 인식한다(스텝 506).

후의 스텝은 제 1의 실시의 형태와 마찬가지로서, 관리 서버(7)는 기기 ID와 제품 시리얼 번호를 묶어서 기억하고(스텝 134), 또한 수신한 데이터에 일시 정보를 부가하여 비밀 키로 서명하고, 공장 시스템에 송신한다(스텝 136).

공장 시스템은. 서명을 확인하고, 기기 인증 정보가 CE 기기(9)에 적절하게 조립된 것을 확인한다.

이상과 같이, 본 실시의 형태에서는. 관리 서버(7)는 확인 결과에 의해, 기기 인증 정보가 CE 기기(9)에 조립된 것을 확인할 수 있다.

또한, 관리 서버(7)에서 제 2의 해시 값을 생성할 필요가 없기 때문에 관리 서버(7)의 부하를 저감할 수 있다.

또한, 본 실시의 형태에서는. 기록 모듈(30a)에서 제 1의 해시 값을 생성하는 것으로 하였지만. 기기측 확인 해시 함수(34)를 인증 모듈에 구비하고, 인증 모듈에서 해시 값을 생성하도록 구성하여도 좋다. 이 경우, 인증 정보 기록 확인 모듈(36)은. 인증 모듈로부터 제 1의 해시 값과 기기 ID를 수취하고, 제 1의 해시 값의 동일성을 확인하도록 구성할 수 있다.

또한, 인증 정보 기록 확인 모듈(36)의 기능을 기록 모듈(30a)에 갖게 하여, 기록 모듈(30a)이 관리 서버(7)에 확인 결과를 송신하도록 구성할 수도 있다.

산업상 이용 가능성

본 발명에 의하면, 기기 내에 기기 인증 정보를 안전하게 조립할 수 있다. 또한, 기기 내에 기기 인증 정보가 적절하게 조립된 것을 기기 인증 정보의 비밀 상태를 유지한 채로 확인할 수 있다.

(57) 청구의 범위

청구항 1.

제공 서버와 단말 기기로 이루어지고, 기기 인증 서버에서 기기 인증할 때의 기기 인증 정보를 단말 기기에 조립하는 기기 인증 정보 조립 시스템으로서,

상기 제공 서버는.

기기 인증 정보를 생성하는 기초가 되는 원 정보를 상기 단말 기기에 제공함과 함께, 상기 기기 인증 정보, 또는 상기 원 정보를. 상기 단말 기기의 기기 인증을 행하는 기기 인증 서버에 제공하고,

상기 단말 기기는.

상기 제공된 원 정보를 이용하여, 기기 인증 정보를 송신하기 위해 필요한 정보를 기억하고, 기기 인증시에. 상기 기억한 정보를 이용하여 상기 원 정보로부터 생성한 기기 인증 정보를. 상기 기기 인증 서버에 송신하는 것을 특징으로 하는 기기 인증 정보 조립 시스템.

청구항 2.

제 1항에 있어서,

상기 제공 서버는. 상기 원 정보로부터 생성되는 기기 인증 정보를 소정의 일방향성 함수로 변환한 변환치를 상기 단말 기기에 제공하고,

상기 단말 기기는. 상기 제공된 원 정보로부터 생성한 기기 인증 정보를 상기 일방향성 함수로 변환하여 변환치를 생성하고,

상기 생성한 변환치와. 상기 제공 서버로부터 제공된 변환치의 동일성을 판단하는 것을 특징으로 하는 기기 인증 정보 조립 시스템.

청구항 3.

제 1항에 있어서,

상기 단말 기기는. 상기 제공된 원 정보로부터 생성한 기기 인증 정보를 소정의 일방향성 함수로 변환하여 변환치를 상기 제공 서버에 제공하고,

상기 제공 서버는. 상기 원 정보로부터 생성되는 기기 인증 정보를 상기 일방향성 함수로 변환한 변환치와. 상기 단말 기기로부터 제공된 변환치의 동일성을 판단하는 것을 특징으로 하는 기기 인증 정보 조립 시스템.

청구항 4.

제공 서버로부터 제공되는, 기기 인증 정보를 생성하는 기초가 되는 원 정보를 취득하는 원 정보 취득 수단과.

상기 취득한 원 정보로부터 기기 인증 정보를 생성하는 생성 수단과.

기기 인증시에. 상기 생성한 기기 인증 정보를 기기 인증 서버에 송신하는 기기 인증 정보 송신 수단을 구비한 것을 특징으로 하는 단말 기기.

청구항 5.

제 4항에 있어서,

상기 원 정보는. 상기 기기 인증 정보를 암호화한 암호화 기기 인증 정보이고,

상기 생성 수단은. 상기 암호화 기기 인증 정보를 복호화함에 의해, 상기 기기 인증 정보를 생성하는 것을 특징으로 하는 단말 기기.

청구항 6.

제 4항에 있어서,

상기 생성 수단에서 생성한 기기 인증 정보를 암호화하여 기억하는 기억 수단을 구비하고,

상기 기기 인증 정보 송신 수단은. 상기 기억 수단에 기억된 기기 인증 정보를 복호화하여 송신하는 것을 특징으로 하는 단말 기기.

청구항 7.

제 6항에 있어서,

상기 기억 수단에 기억하는 기기 인증 정보의 암호화, 및 복호화에 사용하는 암호 키를. 상기 암호 키의 사용시에 상기 단말 기기에 고유한 정보를 이용하여 생성하는 키 생성 수단을 구비한 것을 특징으로 하는 단말 기기.

청구항 8.

제 7항에 있어서,

상기 생성한 암호 키를. 상기 암호 키의 사용 후의 소정 기간 내에 소거하는 키 소거 수단을 구비한 것을 특징으로 하는 단말 기기.

청구항 9.

제 4항에 있어서,

상기 제공 서버로부터 상기 기기 인증 정보를 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 수단과.

상기 생성한 기기 인증 정보를. 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 수단과.

상기 취득한 변환치와. 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 수단을 구비한 것을 특징으로 하는 단말 기기.

청구항 10.

제 9항에 있어서,

상기 생성한 기기 인증 정보를 다른 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 수단과.

상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 수단을 구비한 것을 특징으로 하는 단말 기기.

청구항 11.

제 4항에 있어서,

상기 생성한 기기 인증 정보를 소정의 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 수단과.

상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 수단을 구비한 것을 특징으로 하는 단말 기기.

청구항 12.

제 4항에 있어서,

상기 취득한 원 정보를 기억하는 기억 수단을 구비하고,

상기 기기 인증 정보 송신 수단은. 상기 기억한 원 정보로부터 기기 인증 정보를 생성하여 상기 기기 인증 서버에 송신하는 것을 특징으로 하는 단말 기기.

청구항 13.

원 정보 취득 수단과. 생성 수단과. 기기 인증 정보 송신 수단을 구비한 컴퓨터로 구성된 단말 기기에 있어서,

제공 서버로부터 제공되는, 기기 인증 정보를 생성하는 기초가 되는 원 정보를 상기 원 정보 취득 수단에서 취득하는 원 정보 취득 스텝과.

상기 취득한 원 정보로부터 기기 인증 정보를. 상기 생성 수단에서 생성하는 생성 스텝과.

기기 인증시에. 상기 생성한 기기 인증 정보를. 상기 기기 인증 정보 송신 수단에서 기기 인증 서버에 송신하는 기기 인증 정보 송신 스텝으로 구성된 것을 특징으로 하는 기기 인증 정보 처리 방법.

청구항 14.

제 13항에 있어서,

상기 원 정보는. 상기 기기 인증 정보를 암호화한 암호화 기기 인증 정보이고,

상기 생성 스텝에서는. 상기 암호화 기기 인증 정보를 복호화함에 의해, 상기 기기 인증 정보를 생성하는 것을 특징으로 하는 기기 인증 정보 처리 방법.

청구항 15.

제 13항에 있어서,

상기 컴퓨터는. 기억 수단을 구비하고,

상기 생성 수단에서 생성한 기기 인증 정보를 암호화하여 상기 기억 수단에서 기억하는 기억 스텝을 구비하고,

상기 기기 인증 정보 송신 스텝에서는. 상기 기억 수단에 기억된 기기 인증 정보를 복호화하여 송신하는 것을 특징으로 하는 기기 인증 정보 처리 방법.

청구항 16.

제 15항에 있어서,

상기 컴퓨터는. 키 생성 수단을 구비하고,

상기 기억 수단에 기억하는 기기 인증 정보의 암호화, 및 복호화에 사용하는 암호 키를. 상기 키 생성 수단에서 상기 암호 키의 사용시에 상기 단말 기기에 고유한 정보를 이용하여 생성하는 키 생성 스텝을 구비한 것을 특징으로 하는 기기 인증 정보 처리 방법.

청구항 17.

제 16항에 있어서,

상기 컴퓨터는. 키 소거 수단을 구비하고,

상기 생성한 암호 키를. 상기 암호 키의 사용 후의 소정 기간 내에 상기 키 소거 수단에서 소거하는 키 소거 스텝을 구비한 것을 특징으로 하는 기기 인증 정보 처리 방법.

청구항 18.

제 13항에 있어서,

상기 컴퓨터는. 변환치 취득 수단과. 변환치 산출 수단과. 판단 수단을 구비하고,

상기 제공 서버로부터 상기 기기 인증 정보를 소정의 일방향성 함수로 변환한 변환치를 상기 변환치 취득 수단에서 취득하는 변환치 취득 스텝과.

상기 변환치 산출 수단에서 상기 생성한 기기 인증 정보를. 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 스텝과.

상기 판단 수단에서. 상기 취득한 변환치와. 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 스텝을 구비한 것을 특징으로 하는 기기 인증 정보 처리 방법.

청구항 19.

제 18항에 있어서,

상기 컴퓨터는. 변환치 산출 수단과. 변환치 제공 수단을 구비하고,

상기 변환치 산출 수단에서. 상기 생성한 기기 인증 정보를 다른 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 스텝과.

상기 변환치 산출 수단에서. 상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 스텝을 구비한 것을 특징으로 하는 기기 인증 정보 처리 방법.

청구항 20.

제 13항에 있어서,

상기 컴퓨터는. 변환치 산출 수단과. 변환치 제공 수단을 구비하고,

상기 변환치 산출 수단에서. 상기 생성한 기기 인증 정보를 소정의 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 스텝과.

상기 변환치 제공 수단에서. 상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 스텝을 구비한 것을 특징으로 하는 기기 인증 정보 처리 방법.

청구항 21.

제 13항에 있어서,

상기 컴퓨터는. 상기 취득한 원 정보를 기억하는 기억 수단을 구비하고,

상기 기기 인증 정보 송신 스텝에서는. 상기 기억한 원 정보로부터 기기 인증 정보를 생성하여 상기 기기 인증 서버에 송신하는 것을 특징으로 하는 기기 인증 정보 처리 방법.

청구항 22.

제공 서버로부터 제공되는, 기기 인증 정보를 생성하는 기초가 되는 원 정보를 취득하는 원 정보 취득 기능과.

상기 취득한 원 정보로부터 기기 인증 정보를 생성하는 생성 기능과.

기기 인증시에. 상기 생성한 기기 인증 정보를 기기 인증 서버에 송신하는 기기 인증 정보 송신 기능을 컴퓨터에서 실현하는 것을 특징으로 하는 기기 인증 정보 처리 프로그램.

청구항 23.

제 22항에 있어서,

상기 원 정보는. 상기 기기 인증 정보를 암호화한 암호화 기기 인증 정보이고,

상기 생성 기능은. 상기 암호화 기기 인증 정보를 복호화함에 의해, 상기 기기 인증 정보를 생성하는 것을 특징으로 하는 기기 인증 정보 처리 프로그램.

청구항 24.

제 22항에 있어서,

상기 생성 기능에서 생성한 기기 인증 정보를 암호화하여 기억하는 기억 기능을 실현하고,

상기 기기 인증 정보 송신 기능은. 상기 기억 기능에 기억된 기기 인증 정보를 복호화하여 송신하는 것을 특징으로 하는 기기 인증 정보 처리 프로그램.

청구항 25.

제 24항에 있어서,

상기 기억 기능에 기억하는 기기 인증 정보의 암호화, 및 복호화에 사용하는 암호 키를. 상기 암호 키의 사용시에 상기 단말 기기에 고유한 정보를 이용하여 생성하는 키 생성 기능을 컴퓨터에서 실현하는 것을 특징으로 하는 기기 인증 정보 처리 프로그램.

청구항 26.

제 25항에 있어서,

상기 생성한 암호 키를. 상기 암호 키의 사용 후의 소정 기간 내에 소거하는 키 소거 기능을 컴퓨터에서 실현하는 것을 특징으로 하는 기기 인증 정보 처리 프로그램.

청구항 27.

제 22항에 있어서,

상기 제공 서버로부터 상기 기기 인증 정보를 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 기능과.

상기 생성한 기기 인증 정보를. 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 기능과.

상기 취득한 변환치와. 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 기능을 컴퓨터에서 실현하는 것을 특징으로 하는 기기 인증 정보 처리 프로그램.

청구항 28.

제 27항에 있어서,

상기 생성한 기기 인증 정보를 다른 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 기능과.

상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 기능을 컴퓨터에서 실현하는 것을 특징으로 하는 기기 인증 정보 처리 프로그램.

청구항 29.

제 22항에 있어서,

상기 생성한 기기 인증 정보를 소정의 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 기능과.

상기 산출한 변환치를 상기 제공 서버에 제공하는 변환치 제공 기능을 컴퓨터에서 실현하는 것을 특징으로 하는 기기 인증 정보 처리 프로그램.

청구항 30.

제 22항에 있어서,

상기 취득한 원 정보를 기억하는 기억 기능을 컴퓨터에서 실현하고,

상기 기기 인증 정보 송신 기능은. 상기 기억한 원 정보로부터 기기 인증 정보를 생성하여 상기 기기 인증 서버에 송신하는 것을 특징으로 하는 기기 인증 정보 처리 프로그램.

청구항 31.

제공 서버로부터 제공되는, 기기 인증 정보를 생성하는 기초가 되는 원 정보를 취득하는 원 정보 취득 기능과.

상기 취득한 원 정보로부터 기기 인증 정보를 생성하는 생성 기능과.

기기 인증시에. 상기 생성한 기기 인증 정보를 기기 인증 서버에 송신하는 기기 인증 정보 송신 기능을 컴퓨터에서 실현하는 것을 특징으로 하는 기기 인증 정보 처리 프로그램을 기억한 컴퓨터가 판독 가능한 기억 매체.

청구항 32.

단말 기기에 기기 인증 정보를 생성하는 기초가 되는 원 정보를 제공하는 원 정보 제공 수단과.

상기 기기 인증 정보, 또는 상기 원 정보를. 상기 단말 기기의 기기 인증을 행하는 기기 인증 서버에 제공하는 기기 인증 정보 제공 수단과.

상기 단말 기기로부터. 상기 원 정보로부터 생성된 기기 인증 정보의 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 수단과.

상기 기기 인증 정보를 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 수단과.

상기 취득한 변환치와 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 수단을 구비한 것을 특징으로 하는 제공 서버.

청구항 33.

제 32항에 있어서,

상기 판단 수단에서 출력된 판단 결과를. 상기 원 정보의 조립 주체에 송신하는 판단 결과 송신 수단을 구비하는 것을 특징으로 하는 제공 서버.

청구항 34.

원 정보 제공 수단과. 기기 인증 정보 제공 수단과. 변환치 취득 수단과. 변환치 산출 수단과. 판단 수단을 구비한 컴퓨터에 있어서,

단말 기기에 기기 인증 정보를 생성하는 기초가 되는 원 정보를. 상기 원 정보 제공 수단에서 제공하는 원 정보 제공 스텝과.

상기 기기 인증 정보, 또는 상기 원 정보를. 상기 기기 인증 정보 제공 수단에서 상기 단말 기기의 기기 인증을 행하는 기기 인증 서버에 제공하는 기기 인증 정보 제공 스텝과.

상기 변환치 취득 수단에서. 상기 단말 기기로부터. 상기 원 정보로부터 생성된 기기 인증 정보의, 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 스텝과.

상기 변환치 산출 수단에서. 상기 기기 인증 정보를 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 스텝과.

상기 판단 수단에서. 상기 취득한 변환치와 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 스텝으로 구성된 것을 특징으로 하는 기기 인증 정보 제공 방법.

청구항 35.

제 34항에 있어서,

상기 컴퓨터는. 판단 결과 송신 수단을 구비하고,

상기 판단 수단에서 출력된 판단 결과를. 상기 판단 결과 송신 수단에서 상기 원 정보의 조립 주체에 송신하는 판단 결과 송신 스텝을 구비한 것을 특징으로 하는 기기 인증 정보 제공 방법.

청구항 36.

단말 기기에 기기 인증 정보를 생성하는 기초가 되는 원 정보를 제공하는 원 정보 제공 기능과.

상기 기기 인증 정보, 또는 상기 원 정보를. 상기 단말 기기의 기기 인증을 행하는 기기 인증 서버에 제공하는 기기 인증 정보 제공 기능과.

상기 단말 기기로부터. 상기 원 정보로부터 생성된 기기 인증 정보의, 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 기능과.

상기 기기 인증 정보를 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 기능과.

상기 취득한 변환치와 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 기능을 컴퓨터에서 실현하는 것을 특징으로 하는 기기 인증 정보 제공 프로그램.

청구항 37.

제 36항에 있어서,

상기 판단 기능에서 출력된 판단 결과를. 상기 원 정보의 조립 주체에 송신하는 판단 결과 송신 기능을 컴퓨터에서 실현하는 것을 특징으로 하는 기기 인증 정보 제공 프로그램.

청구항 38.

단말 기기에 기기 인증 정보를 생성하는 기초가 되는 원 정보를 제공하는 원 정보 제공 기능과.

상기 기기 인증 정보, 또는 상기 원 정보를. 상기 단말 기기의 기기 인증을 행하는 기기 인증 서버에 제공하는 기기 인증 정보 제공 기능과.

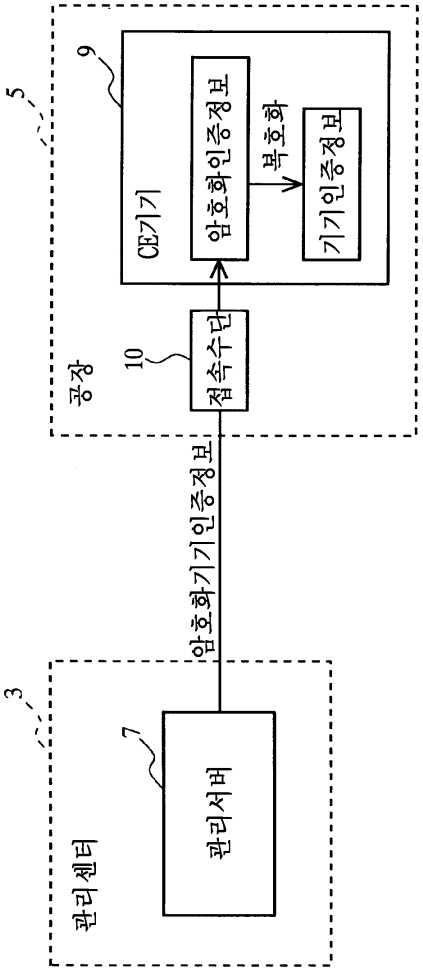
상기 단말 기기로부터. 상기 원 정보로부터 생성된 기기 인증 정보의, 소정의 일방향성 함수로 변환한 변환치를 취득하는 변환치 취득 기능과.

상기 기기 인증 정보를 상기 일방향성 함수로 변환하여 변환치를 산출하는 변환치 산출 기능과.

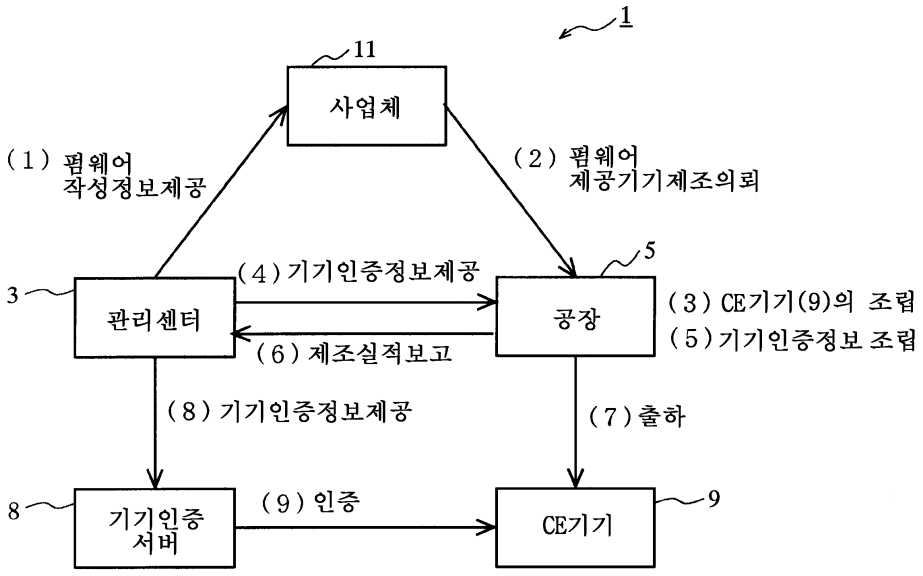
상기 취득한 변환치와 상기 산출한 변환치의 동일성을 판단하고, 그 판단 결과를 출력하는 판단 기능을 컴퓨터에서 실현하는 것을 특징으로 하는 기기 인증 정보 제공 프로그램을 기억한 컴퓨터가 판독 가능한 기억 매체.

도면

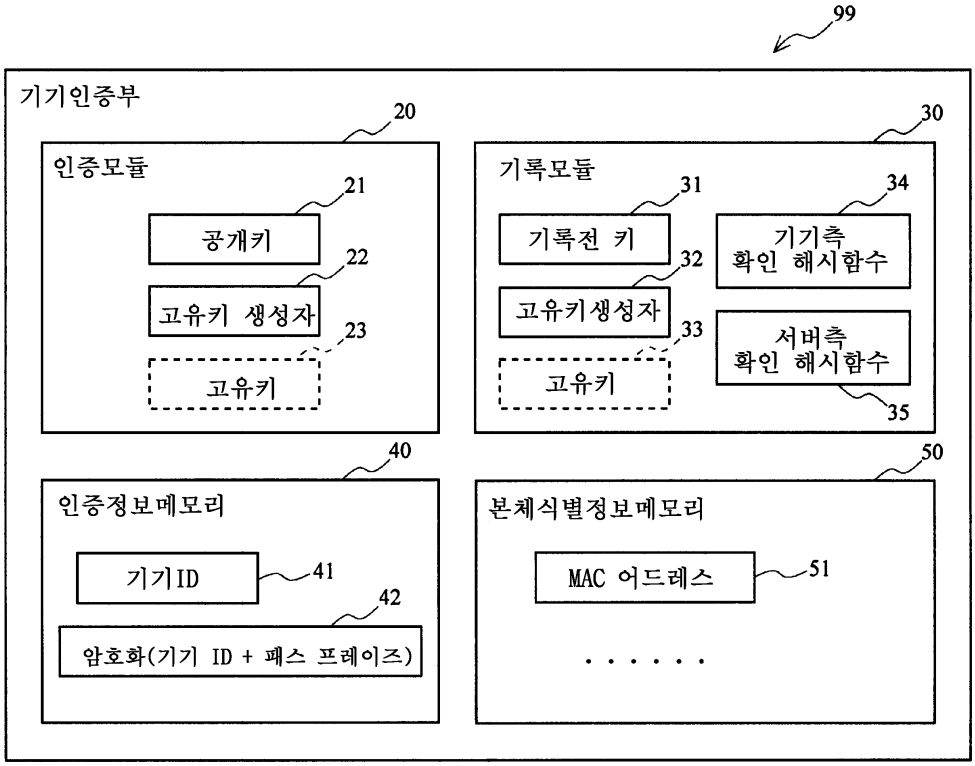
도면1


5
9
CE기기
암호화인증정보
복호화
기기인증정보
공장
10
접속수단
암호화기기인증정보
3
7
관리서버
관리센터

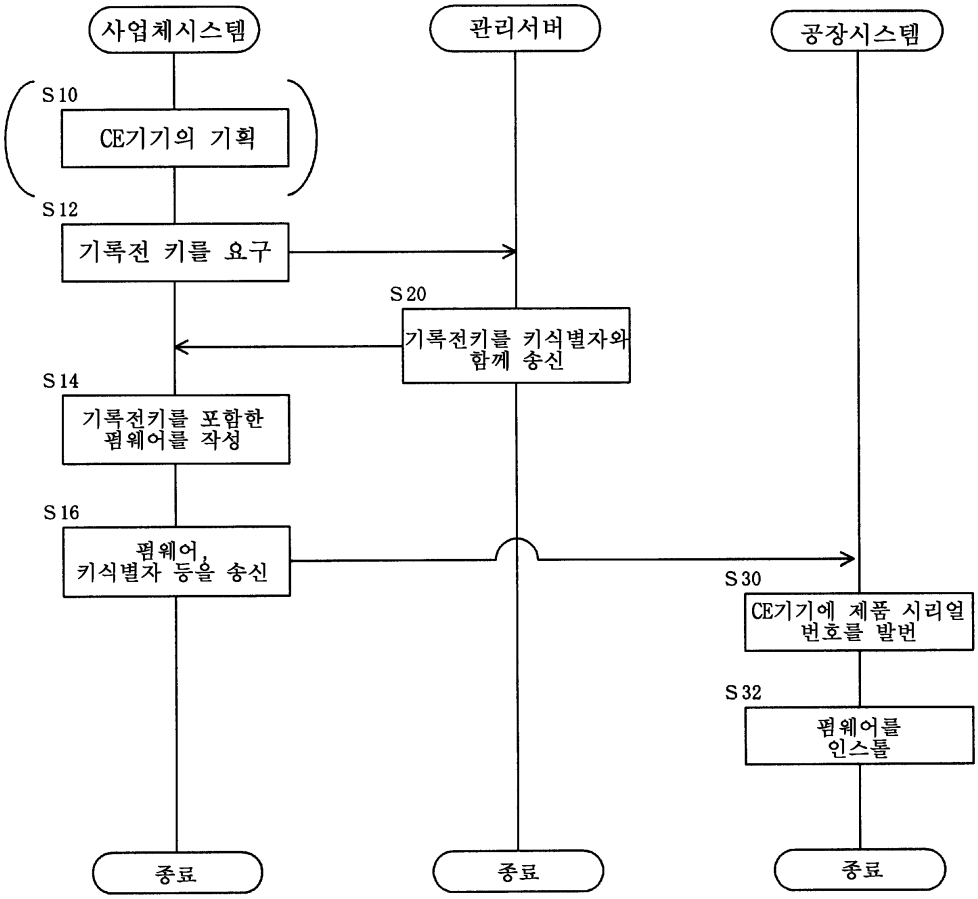
도면2


1
11
사업체
(1) 펌웨어 작성정보제공
(2) 펌웨어 제공기기제조의뢰
3
관리센터
(4) 기기인증정보제공
(6) 제조실적보고
5
공장
(3) CE기기(9)의 조립
(5) 기기인증정보 조립
(8) 기기인증정보제공
(7) 출하
8
기기인증 서버
(9) 인증
9
CE기기

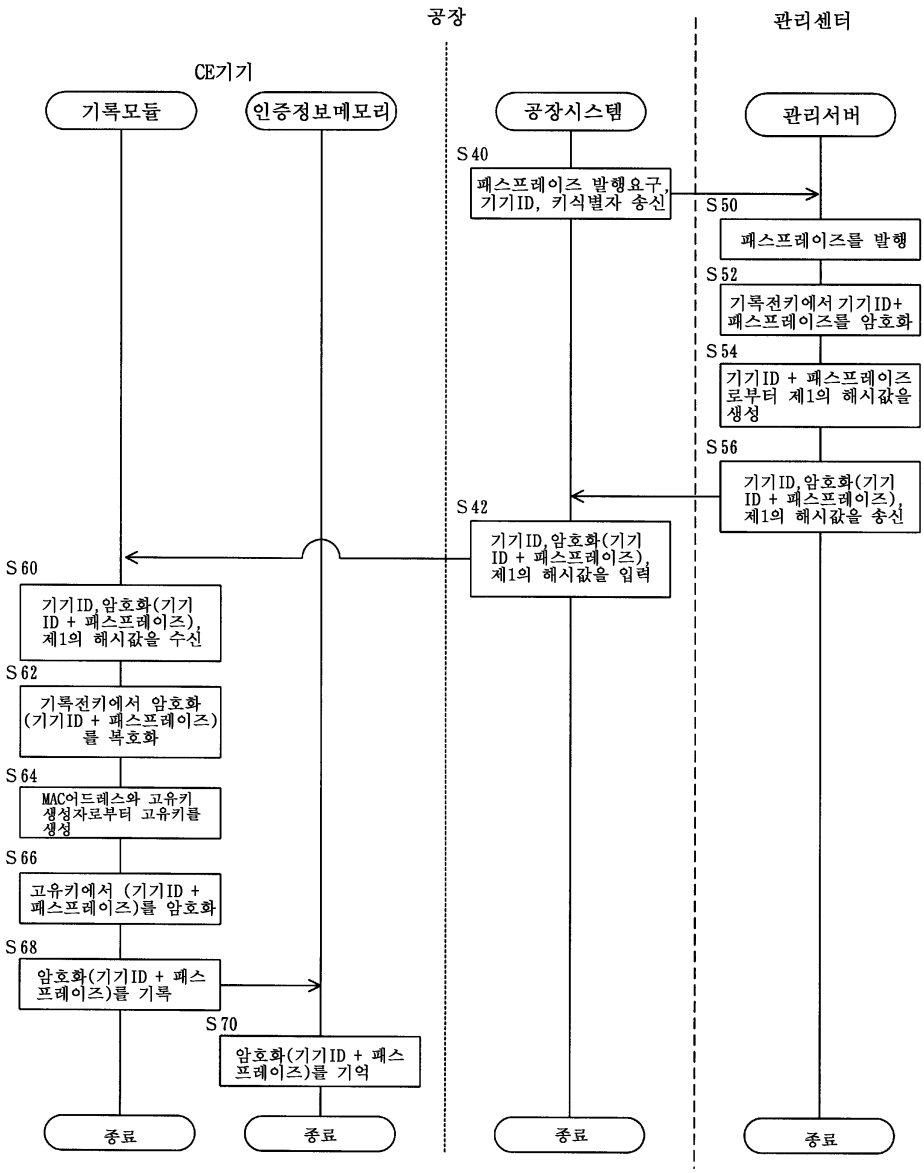
도면3


99
기기인증부
20
인증모듈
21
공개키
22
고유키 생성자
23
고유키
30
기록모듈
31
기록전 키
32
고유키생성자
33
고유키
34
기기측
확인 해시함수
서버측
확인 해시함수
35
40
인증정보메모리
기기ID
41
42
암호화(기기 ID + 패스 프레이즈)
50
본체식별정보메모리
MAC 어드레스
51
. . . . . .

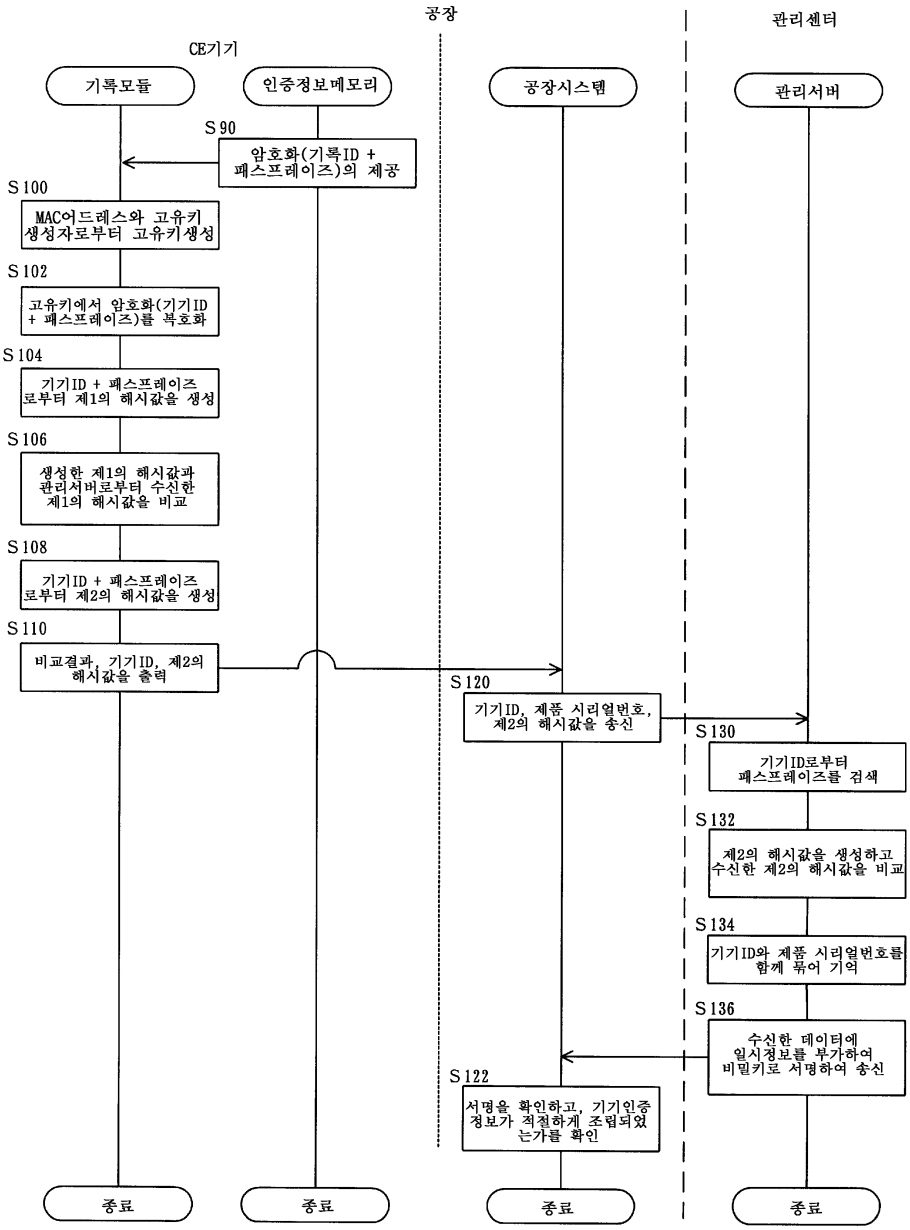
도면4


사업체시스템
관리서버
공장시스템
S10
CE기기의 기획
S12
기록전 키를 요구
S20
기록전키를 키식별자와 함께 송신
S14
기록전키를 포함한 펌웨어를 작성
S16
펌웨어, 키식별자 등을 송신
S30
CE기기에 제품 시리얼 번호를 발번
S32
펌웨어를 인스톨
종료
종료
종료

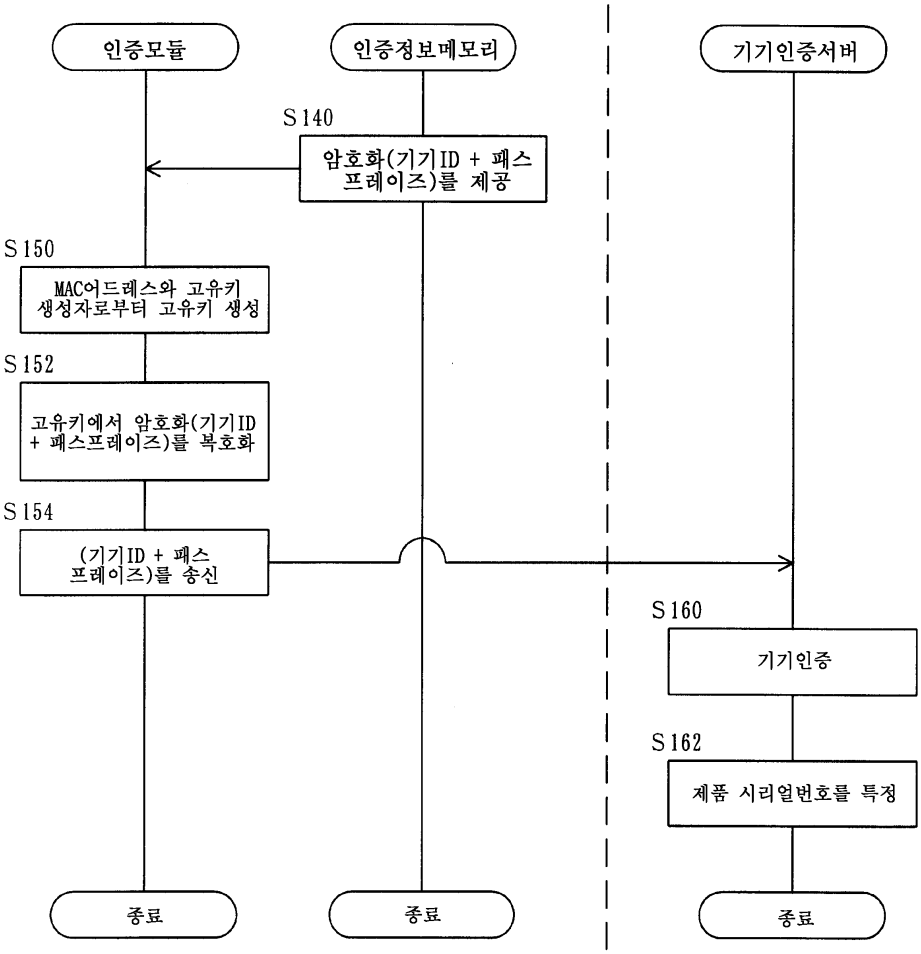
도면5


공장
관리센터
CE기기
기록모듈
인증정보메모리
공장시스템
관리서버
S40
패스프레이즈 발행요구, 기기ID, 키식별자 송신
S50
패스프레이즈를 발행
S52
기록전키에서 기기ID+패스프레이즈를 암호화
S54
기기ID + 패스프레이즈로부터 제1의 해시값을 생성
S56
기기ID,암호화(기기ID + 패스프레이즈), 제1의 해시값을 송신
S42
기기ID,암호화(기기ID + 패스프레이즈), 제1의 해시값을 입력
S60
기기ID,암호화(기기ID + 패스프레이즈), 제1의 해시값을 수신
S62
기록전키에서 암호화(기기ID + 패스프레이즈)를 복호화
S64
MAC어드레스와 고유키 생성자로부터 고유키를 생성
S66
고유키에서 (기기ID + 패스프레이즈)를 암호화
S68
암호화(기기ID + 패스프레이즈)를 기록
S70
암호화(기기ID + 패스프레이즈)를 기억
종료
종료
종료
종료

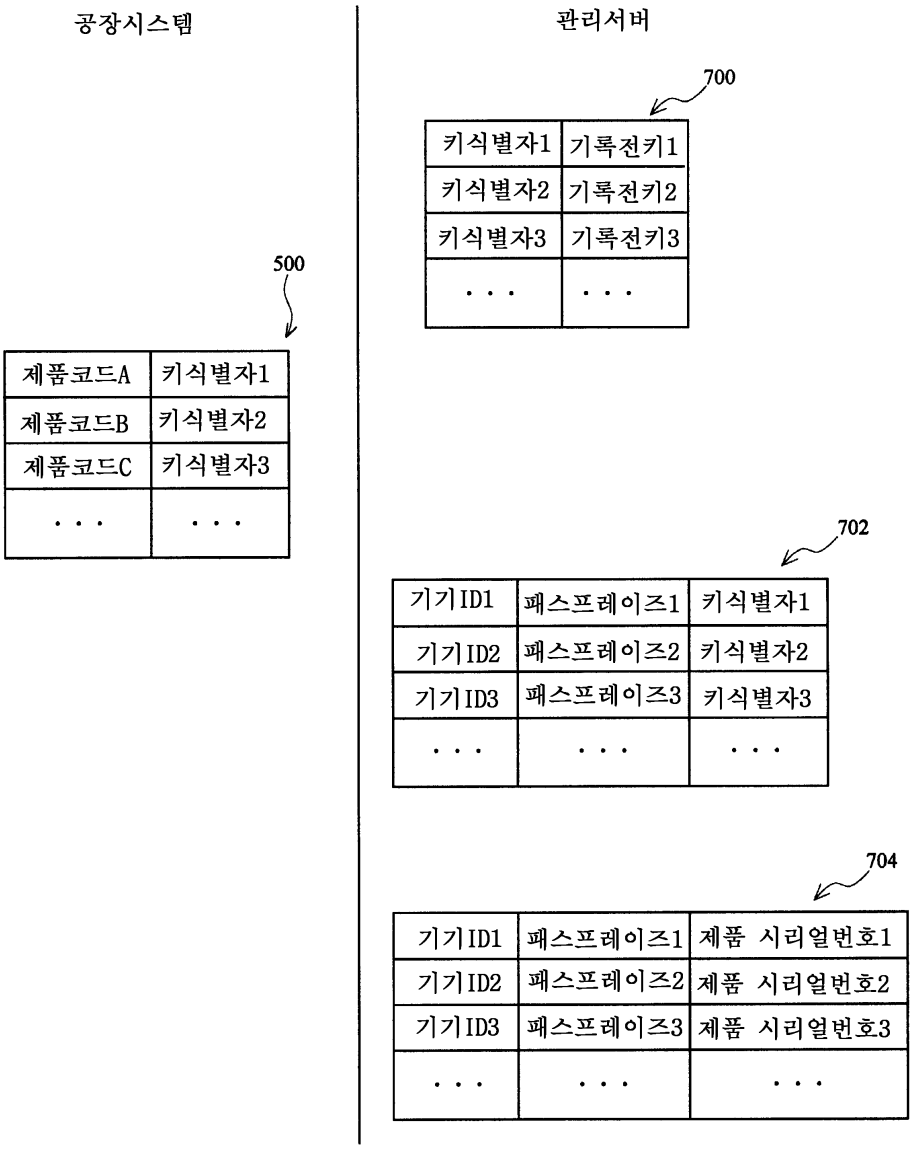
도면6


공장
관리센터
CE기기
기록모듈
인증정보메모리
공장시스템
관리서버
S90
암호화(기록ID + 패스프레이즈)의 제공
S100
MAC어드레스와 고유키 생성자로부터 고유키생성
S102
고유키에서 암호화(기기ID + 패스프레이즈)를 복호화
S104
기기ID + 패스프레이즈로부터 제1의 해시값을 생성
S106
생성한 제1의 해시값과 관리서버로부터 수신한 제1의 해시값을 비교
S108
기기ID + 패스프레이즈로부터 제2의 해시값을 생성
S110
비교결과, 기기ID, 제2의 해시값을 출력
S120
기기ID, 제품 시리얼번호, 제2의 해시값을 송신
S130
기기ID로부터 패스프레이즈를 검색
S132
제2의 해시값을 생성하고 수신한 제2의 해시값을 비교
S134
기기ID와 제품 시리얼번호를 함께 묶어 기억
S136
수신한 데이터에 일시정보를 부가하여 비밀키로 서명하여 송신
S122
서명을 확인하고, 기기인증 정보가 적절하게 조립되었는가를 확인
종료
종료
종료
종료

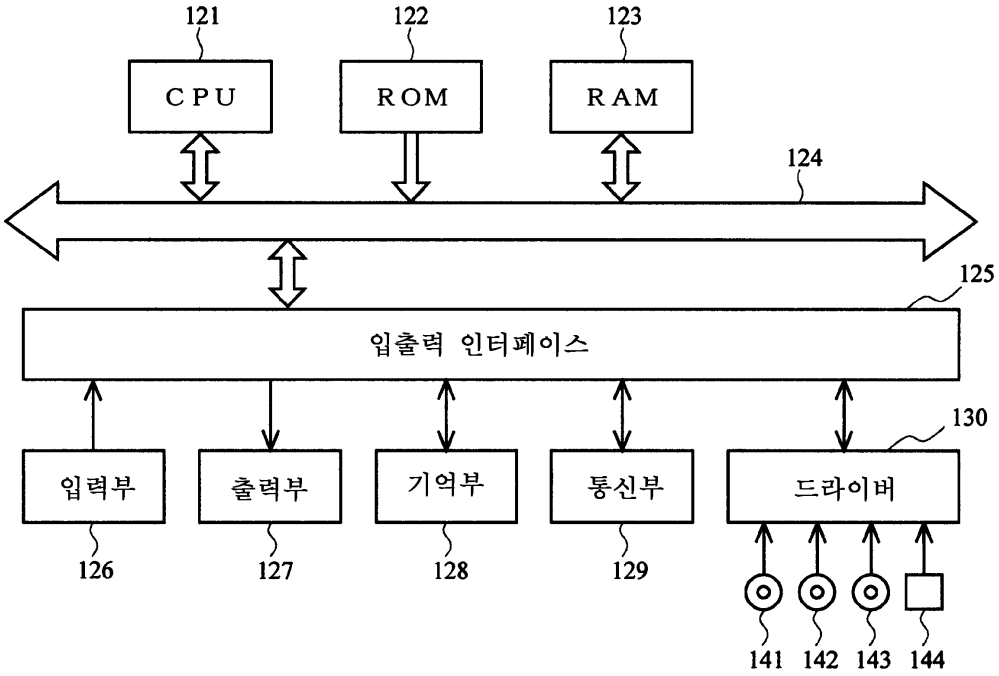
도면7


인증모듈
인증정보메모리
기기인증서버
S140
암호화(기기ID + 패스 프레이즈)를 제공
S150
MAC어드레스와 고유키 생성자로부터 고유키 생성
S152
고유키에서 암호화(기기ID + 패스프레이즈)를 복호화
S154
(기기ID + 패스 프레이즈)를 송신
S160
기기인증
S162
제품 시리얼번호를 특정
종료
종료
종료

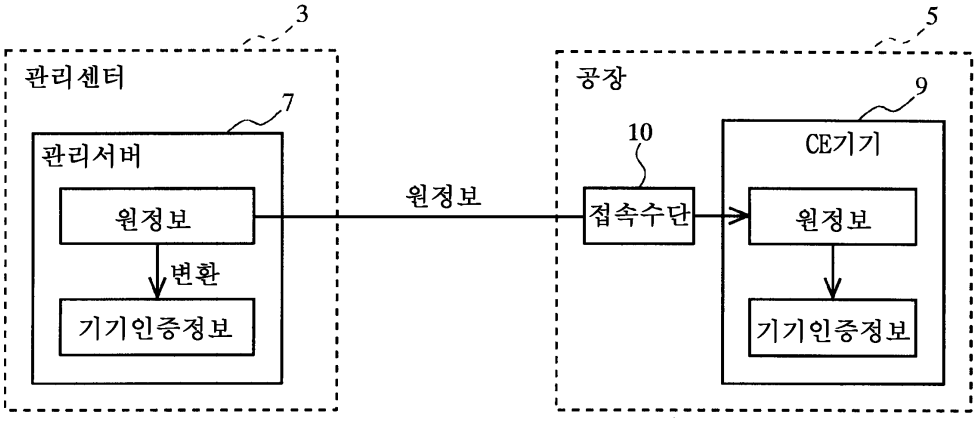
도면8


공장시스템
관리서버
700
키식별자1 기록전키1
키식별자2 기록전키2
키식별자3 기록전키3
500
제품코드A 키식별자1
제품코드B 키식별자2
제품코드C 키식별자3
702
기기ID1 패스프레이즈1 키식별자1
기기ID2 패스프레이즈2 키식별자2
기기ID3 패스프레이즈3 키식별자3
704
기기ID1 패스프레이즈1 제품 시리얼번호1
기기ID2 패스프레이즈2 제품 시리얼번호2
기기ID3 패스프레이즈3 제품 시리얼번호3

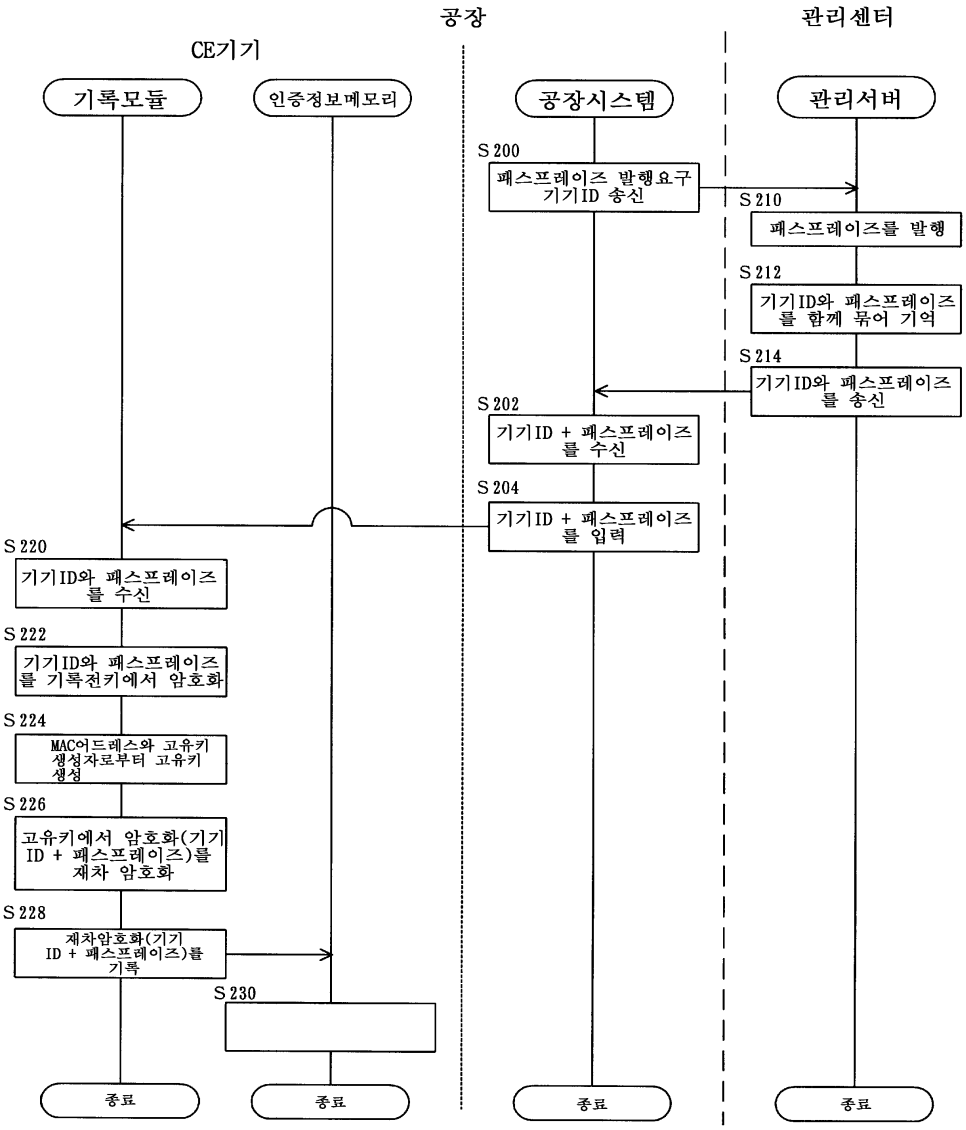
도면9


121
122
123
CPU
ROM
RAM
124
125
입출력 인터페이스
130
입력부
출력부
기억부
통신부
드라이버
126
127
128
129
141
142
143
144

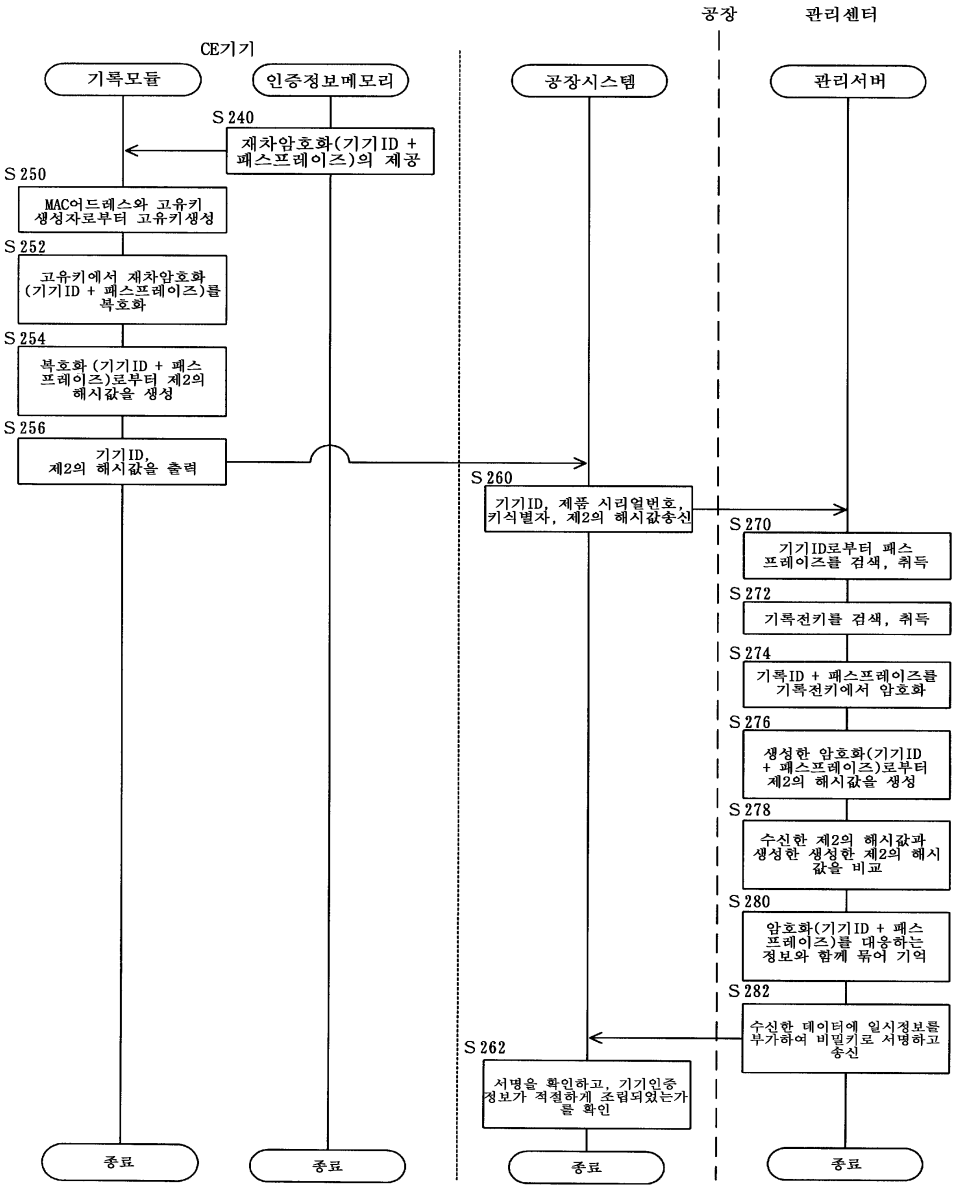
도면10


3
관리센터
7
관리서버
원정보
변환
기기인증정보
원정보
5
공장
10
접속수단
9
CE기기
원정보
기기인증정보

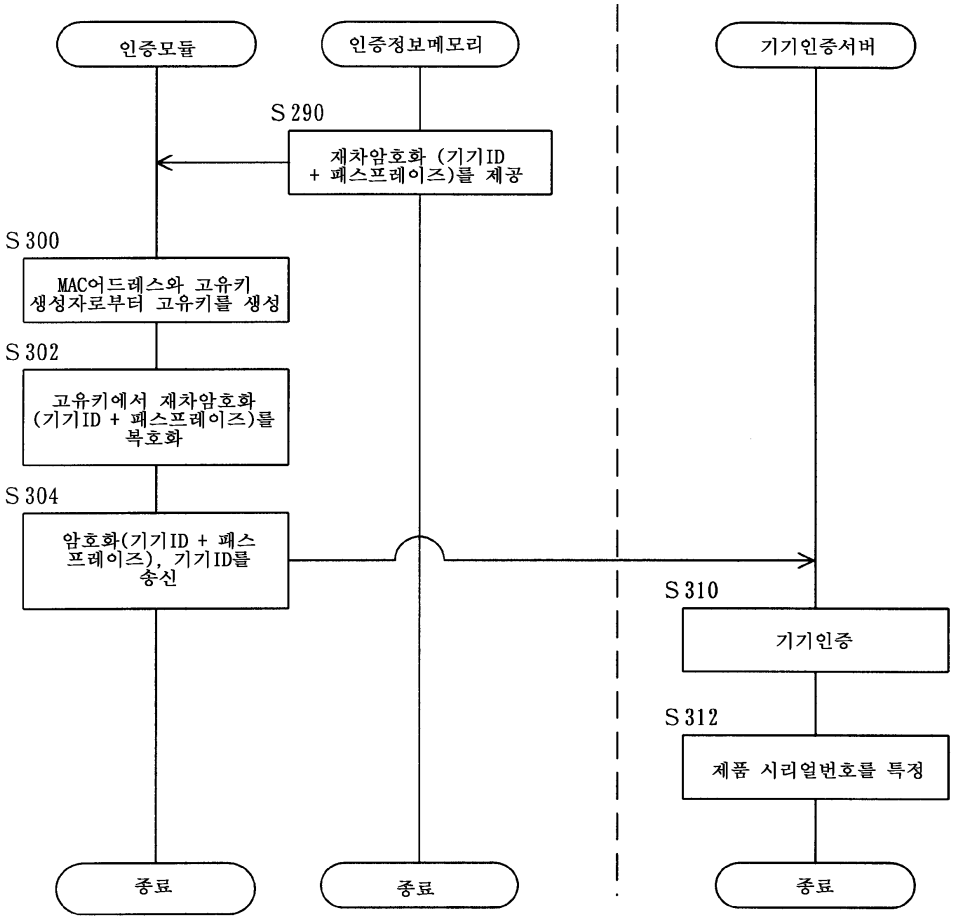
도면11


공장
관리센터
CE기기
기록모듈
인증정보메모리
공장시스템
관리서버
S200
패스프레이즈 발행요구 기기ID 송신
S210
패스프레이즈를 발행
S212
기기ID와 패스프레이즈를 함께 묶어 기억
S214
기기ID와 패스프레이즈를 송신
S202
기기ID + 패스프레이즈를 수신
S204
기기ID + 패스프레이즈를 입력
S220
기기ID와 패스프레이즈를 수신
S222
기기ID와 패스프레이즈를 기록전키에서 암호화
S224
MAC어드레스와 고유키 생성자로부터 고유키 생성
S226
고유키에서 암호화(기기ID + 패스프레이즈)를 재차 암호화
S228
재차암호화(기기ID + 패스프레이즈)를 기록
S230
종료
종료
종료
종료

도면12


공장
관리센터
CE기기
기록모듈
인증정보메모리
공장시스템
관리서버
S 240
재차암호화(기기ID + 패스프레이즈)의 제공
S 250
MAC어드레스와 고유키 생성자로부터 고유키생성
S 252
고유키에서 재차암호화(기기ID + 패스프레이즈)를 복호화
S 254
복호화(기기ID + 패스프레이즈)로부터 제2의 해시값을 생성
S 256
기기ID, 제2의 해시값을 출력
S 260
기기ID, 제품 시리얼번호, 키식별자, 제2의 해시값송신
S 270
기기ID로부터 패스프레이즈를 검색, 취득
S 272
기록전키를 검색, 취득
S 274
기록ID + 패스프레이즈를 기록전키에서 암호화
S 276
생성한 암호화(기기ID + 패스프레이즈)로부터 제2의 해시값을 생성
S 278
수신한 제2의 해시값과 생성한 생성한 제2의 해시값을 비교
S 280
암호화(기기ID + 패스프레이즈)를 대응하는 정보와 함께 묶어 기억
S 282
수신한 데이터에 일시정보를 부가하여 비밀키로 서명하고 송신
S 262
서명을 확인하고, 기기인증 정보가 적절하게 조립되었는가를 확인
종료
종료
종료
종료

도면13


인증모듈
인증정보메모리
기기인증서버
S 290
재차암호화 (기기ID + 패스프레이즈)를 제공
S 300
MAC어드레스와 고유키 생성자로부터 고유키를 생성
S 302
고유키에서 재차암호화 (기기ID + 패스프레이즈)를 복호화
S 304
암호화(기기ID + 패스프레이즈), 기기ID를 송신
S 310
기기인증
S 312
제품 시리얼번호를 특정
종료
종료
종료

도면14

인증정보관리서버

706

키식별자1	기록전키1
키식별자2	기록전키2
키식별자3	기록전키3
. . .	. . .

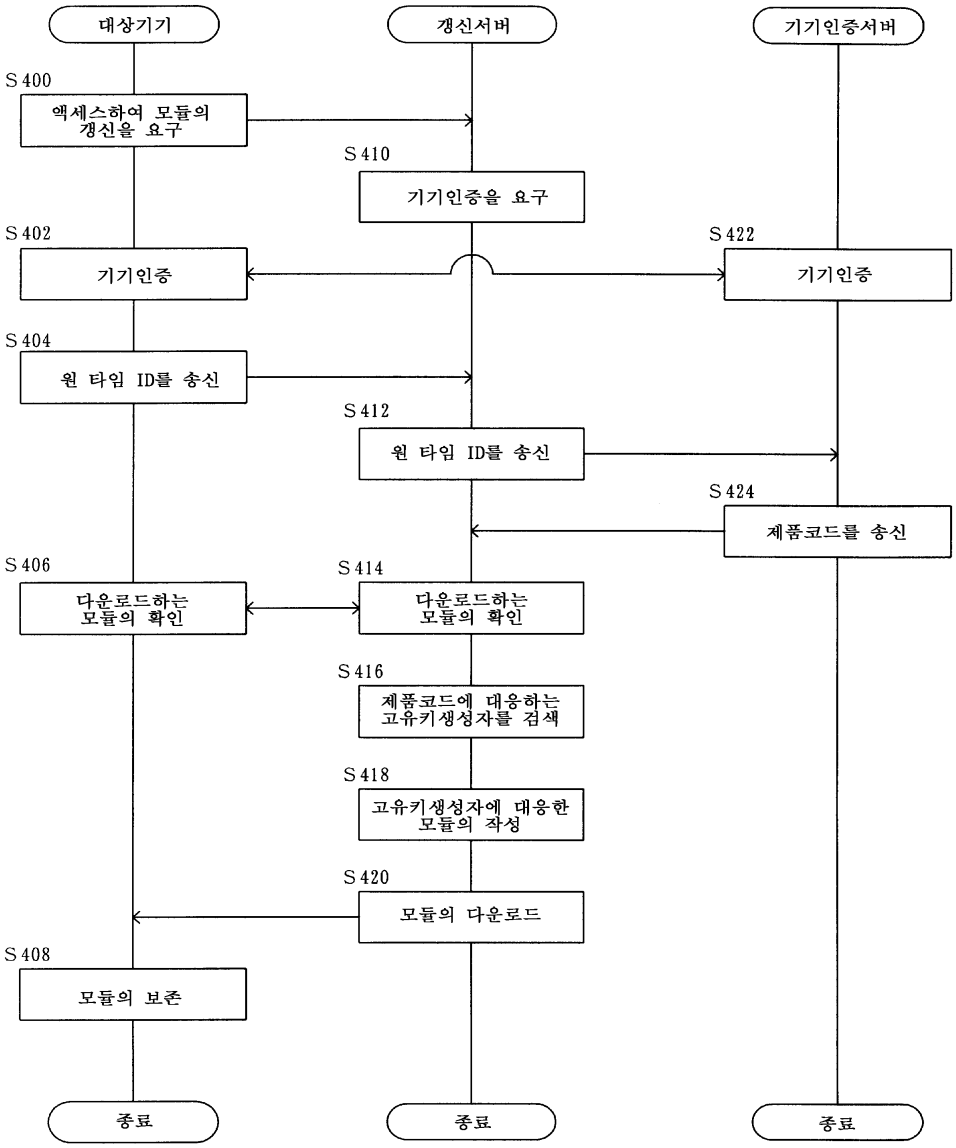
708

기기ID1	패스프레이즈1
기기ID2	패스프레이즈2
기기ID3	패스프레이즈3
. . .	. . .

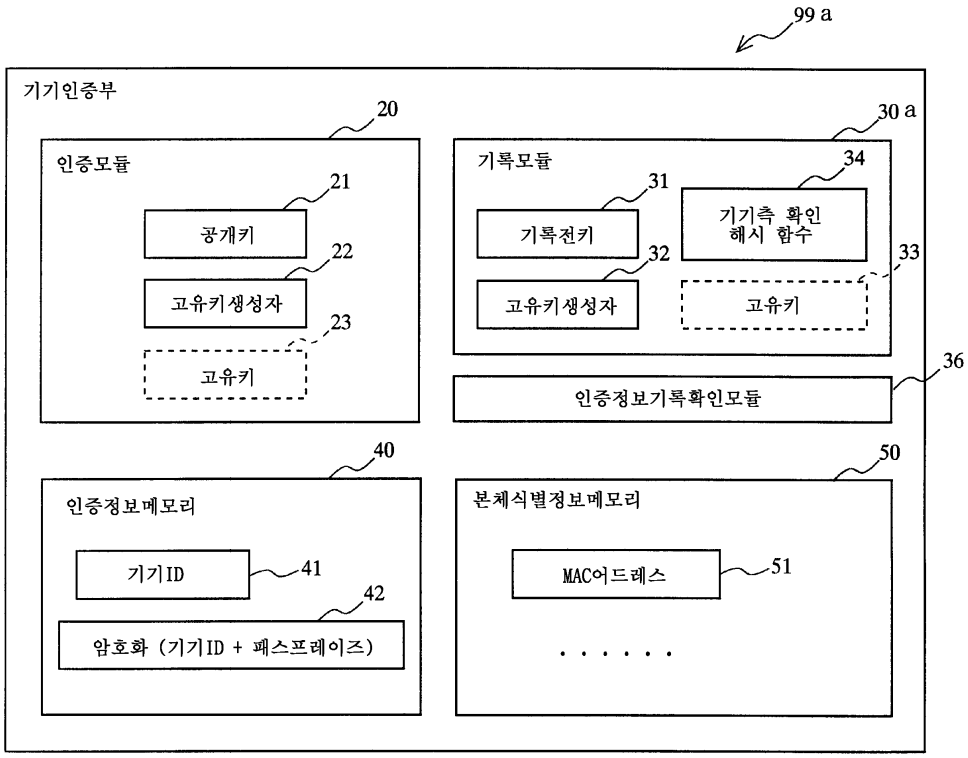
710

기기ID1	암호화 (기기ID1 + 패스프레이즈1)	제품 시리얼번호1	키식별자1
기기ID2	암호화 (기기ID2 + 패스프레이즈2)	제품 시리얼번호2	키식별자2
기기ID3	암호화 (기기ID3 + 패스프레이즈3)	제품 시리얼번호3	키식별자3
. . .	. . .	. . .	. . .

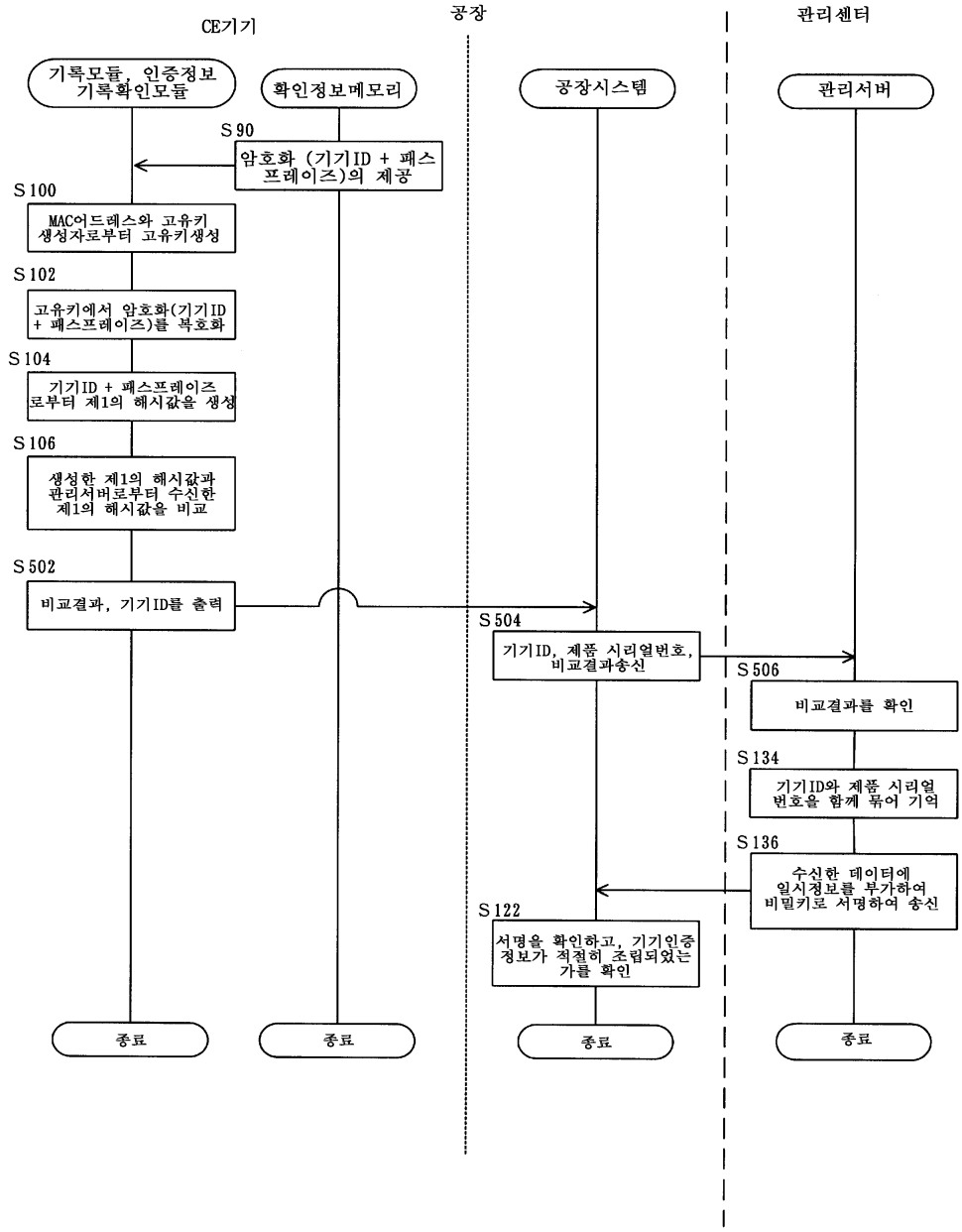
도면15


대상기기
갱신서버
기기인증서버
S400
액세스하여 모듈의 갱신을 요구
S410
기기인증을 요구
S402
기기인증
S422
기기인증
S404
원 타임 ID를 송신
S412
원 타임 ID를 송신
S424
제품코드를 송신
S406
다운로드하는 모듈의 확인
S414
다운로드하는 모듈의 확인
S416
제품코드에 대응하는 고유키생성자를 검색
S418
고유키생성자에 대응한 모듈의 작성
S420
모듈의 다운로드
S408
모듈의 보존
종료
종료
종료

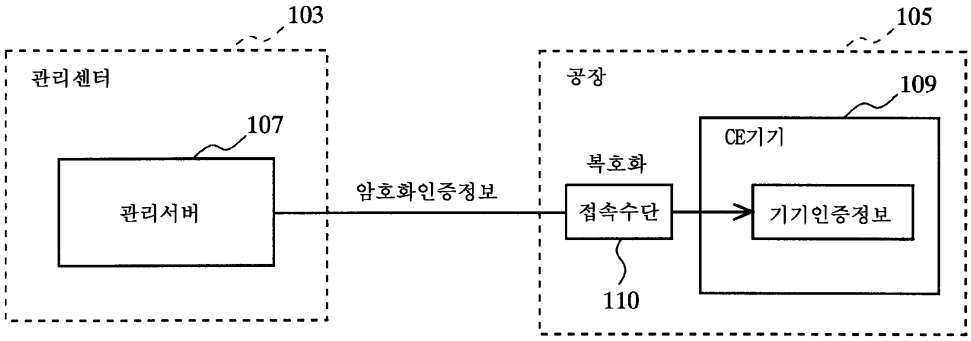
도면16


99 a
기기인증부
20
인증모듈
21
공개키
22
고유키생성자
23
고유키
30 a
기록모듈
31
기록전키
34
기기측 확인
해시 함수
32
고유키생성자
33
고유키
36
인증정보기록확인모듈
40
인증정보메모리
기기ID
41
42
암호화 (기기ID + 패스프레이즈)
50
본체식별정보메모리
MAC어드레스
51
. . . . . .

도면17


CE기기
공장
관리센터
기록모듈, 인증정보 기록확인모듈
확인정보메모리
공장시스템
관리서버
S90
암호화 (기기ID + 패스프레이즈)의 제공
S100
MAC어드레스와 고유키 생성자로부터 고유키생성
S102
고유키에서 암호화(기기ID + 패스프레이즈)를 복호화
S104
기기ID + 패스프레이즈로부터 제1의 해시값을 생성
S106
생성한 제1의 해시값과 관리서버로부터 수신한 제1의 해시값을 비교
S502
비교결과, 기기ID를 출력
S504
기기ID, 제품 시리얼번호, 비교결과송신
S506
비교결과를 확인
S134
기기ID와 제품 시리얼 번호을 함께 묶어 기억
S136
수신한 데이터에 일시정보를 부가하여 비밀키로 서명하여 송신
S122
서명을 확인하고, 기기인증 정보가 적절히 조립되었는 가를 확인
종료
종료
종료
종료

도면18


103
관리센터
107
관리서버
암호화인증정보
105
공장
109
CE기기
복호화
접속수단
기기인증정보
110