(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0022904
(43) 공개일자 2025년02월17일

(51) 국제특허분류(Int. Cl.)
G06F 21/44 (2013.01) *G06F 21/45* (2013.01)
H04L 9/32 (2006.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
G06F 21/44 (2013.01)
G06F 21/45 (2013.01)
(21) 출원번호 10-2025-7003799(분할)
(22) 출원일자(국제) 2019년07월01일
심사청구일자 2025년02월06일
(62) 원출원 특허 10-2021-7000183
원출원일자(국제) 2019년07월01일
심사청구일자 2022년06월27일
(85) 번역문제출일자 2025년02월06일
(86) 국제출원번호 PCT/US2019/040064
(87) 국제공개번호 WO 2020/014024
국제공개일자 2020년01월16일
(30) 우선권주장
16/029,559 2018년07월07일 미국(US)

(71) 출원인
인테그리티 시큐리티 서비시즈 엘엘씨
미국 캘리포니아주 93101, 산타 바바라, 웨스트 솔라 스트리트 30
(72) 발명자
메이어, 알란 티.
미국 캘리포니아주 93101, 산타 바바라, 웨스트 솔라 스트리트 30, 인테그리티 시큐리티 서비시즈 엘엘씨 내
포웰, 그레고리 에이.
미국 캘리포니아주 93101, 산타 바바라, 웨스트 솔라 스트리트 30, 인테그리티 시큐리티 서비시즈 엘엘씨 내
(74) 대리인
김동완

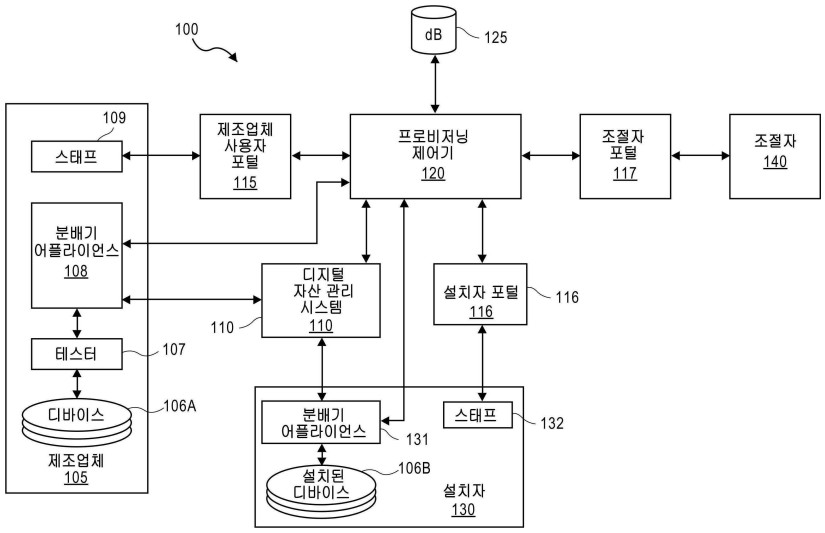
전체 청구항 수 : 총 33 항

(54) 발명의 명칭 **확장 가능한 인증서 관리 시스템 구축물**

(57) 요 약

확장 가능한 인증서 관리 시스템 아키텍처. 예시적인 시스템은 등록 권한을 실행하고 등록 권한에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼(예를 들어 VM)을 포함할 수 있다. 시스템은 등재 인증 권한을 실행하고 등재 인증 권한에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼을 또한 포함할 수 있다. 가명 인증 권한을 실행하고 가명 인증 권한에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼을 더욱 포함할 수 있다. 또한 첫 번째 및 두 번째 연결 권한을 실행하고 연결 권한에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼을 포함할 수 있다.

대 표 도



(52) CPC특허분류
H04L 63/0414 (2013.01)
H04L 63/062 (2013.01)
H04L 63/0823 (2013.01)
H04L 9/3268 (2013.01)
H04L 2209/42 (2013.01)

명 세 서

청구범위

청구항 1

등록 권한 응용프로그램을 실행하고 등록 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 하나 이상의 등록 권한 컴퓨터 엔진에 통신적으로 연결된 하나 이상의 응용프로그램 플랫폼;

가명 인증 권한 응용프로그램은 등록 권한 응용프로그램에 디지털 자산을 생성하고 조건부로 전송하도록 작동 가능 하고, 가명 인증 권한 응용프로그램을 실행하고 가명 인증 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 하나 이상의 가명 인증 권한 컴퓨터 엔진에 통신적으로 연결된 하나 이상의 응용프로그램 플랫폼; 및

하나 이상의 로드 밸런서는 하나 이상의 컴퓨터 엔진의 상태 측정에 따라 하나 이상의 요청을 하나 이상의 컴퓨터 엔진에 분산하도록 형상화되고, 하나 이상의 등록 권한 컴퓨터 엔진 중 하나 이상의 컴퓨터 엔진과 하나 이상의 가명 인증 권한 컴퓨터 엔진에 통신적으로 연결된 하나 이상의 로드 밸런서;

를 포함하는 프로비저닝 컨트롤러에 인증서를 안전하게 제공하기 위한 확장 가능한 인증서 관리 시스템에 있어서,

상기 확장 가능한 인증서 관리 시스템은 복수의 컴퓨터화된 장치 중 각 컴퓨터화된 장치에 하나 이상의 인증서 로드를 할당하도록 형상화 되고, 하나 이상의 인증서 로드는 시간 기간 동안 각각의 컴퓨터화된 장치에 저장될 디지털 자산의 수를 나타내며,

하나 이상의 인증서 로드는 각 컴퓨터화된 장치가 시간 기간 동안 다른 컴퓨터화된 장치와 다른 수의 디지털 자산을 저장할 수 있도록 할당 가능함를 특징으로 하는 인증서 관리 시스템.

청구항 2

제1항에 있어서,

상기 상태 측정은 적어도 하나의 컴퓨터 엔진의 작동 온도, 적어도 하나의 컴퓨터 엔진의 인클로저 내부의 습도 수준, CPU 용량, 저장 용량, 적어도 하나의 컴퓨터 엔진의 재시작 또는 재부팅 빈도, 적어도 하나의 컴퓨터 엔진의 가장 최근 재시작 이후의 시간, 일정 기간 동안 적어도 하나의 컴퓨터 엔진의 디스크 오류 또는 메모리 오류 수, 적어도 하나의 컴퓨터 엔진의 예약된 유지 관리 이벤트까지의 시간, 적어도 하나의 컴퓨터 엔진이 백업 전원 공급 장치에서 실행 중이라는 표시, 또는 적어도 하나의 컴퓨터 엔진의 전원 공급 장치에 대한 마지막 정전 또는 전압 감소 이후의 기간에서 선택된 적어도 하나를 포함함을 특징으로 하는 인증서 관리 시스템.

청구항 3

제1항에 있어서, 상기 인증서관리 시스템은 등록 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼과 가명 인증 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼에 작동 가능하게 연결된 하나 이상의 데이터베이스를 더욱 포함함을 특징으로 하는 인증서 관리 시스템.

청구항 4

제1항에 있어서, 등록 권한 응용프로그램과 가명 인증 권한 응용프로그램은 각각 서로 독립적으로 확장되도록 작동 가능함을 특징으로 하는 인증서 관리 시스템.

청구항 5

제1항에 있어서,

등록 인증 권한 응용프로그램을 실행하고 등록 인증 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 하나 이상의 등록 인증 권한 컴퓨터 엔진에 통신적으로 연결된 하나 이상의 응용프로그램 플랫폼을 더욱 포함하고,

등록 인증 권한 응용프로그램은 등록 인증서를 생성하고 등록 권한 응용프로그램에 조건부로 전송하도록 작동할

수 있으며,

등록 인증 권한 응용프로그램은 등록 권한 응용프로그램에서 등록 인증서에 대한 요청을 수신한 것에 대한 응답으로 등록 인증서를 생성하도록 작동할 수 있음을 특징으로 하는 인증서 관리 시스템.

청구항 6

제1항에 있어서, 등록 권한 응용프로그램과 가명 인증 권한 응용프로그램 각각이 복수의 메시지 큐를 포함하는 메시지 큐 서비스를 통해 서로 통신적으로 연결됨을 특징으로 하는 인증서 관리 시스템.

청구항 7

제5항에 있어서,

등록 인증 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼은 등록 인증 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 하나 이상의 등록 인증 권한 컴퓨터 엔진에 제1 복수의 메시지 큐를 통해 통신적으로 연결된 하나 이상의 가상 머신 임을 특징으로 하는 인증서 관리 시스템.

청구항 8

제7항에 있어서,

제1 복수의 메시지 큐는

등록 인증 권한 응용프로그램을 실행하는 하나 이상의 가상 머신에 전달할 메시지를 큐잉하기 위한 제1 메시지 큐; 및

등록 인증 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 하나 이상의 등록 인증 권한 컴퓨터 엔진에 전달할 메시지를 큐잉하기 위한 제2 메시지 큐를 포함함을 특징으로 하는 인증서 관리 시스템.

청구항 9

제7항에 있어서,

제1 복수의 메시지 큐는

등록 인증 권한 응용프로그램을 실행하는 하나 이상의 가상 머신에 전달되고 해당 가상 머신에서 전송되는 메시지를 큐잉하기 위한 제1 양방향 메시지 큐; 및

등록 인증 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 하나 이상의 등록 인증 권한 컴퓨터 엔진으로 전달되고 이로부터 전송되는 메시지를 큐잉하기 위한 제2 양방향 메시지 큐를 포함함을 특징으로 하는 인증서 관리 시스템.

청구항 10

제5항에 있어서,

등록 인증 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼은 하나 이상의 로드 밸런서의 제1 로드 밸런서에 의해 등록 인증 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 하나 이상의 등록 인증 권한 컴퓨터 엔진에 통신적으로 연결됨을 특징으로 하는 인증서 관리 시스템.

청구항 11

제10항에 있어서,

제1 로드 밸런서는 로드 밸런서 가상 머신과 로드 밸런서 서버 중 하나 이상을 포함하고; 로드 밸런서 가상 머신과 로드 밸런서 서버는 각각 다수의 응용프로그램 플랫폼과 다수의 컴퓨터 엔진에 걸쳐 워크로드를 분산하도록 형상화됨을 특징으로 하는 인증서 관리 시스템.

청구항 12

제11항에 있어서, 로드 밸런서 가상 머신과 로드 밸런서 서버는 각각 라운드 로빈 기술을 사용하여 다수의 응용프로그램 플랫폼과 다수의 컴퓨터 엔진에 걸쳐 워크로드를 분산하도록 형상화됨을 특징으로 하는 인증서 관리

시스템.

청구항 13

제11항에 있어서, 로드 밸런서 가상 머신과 로드 밸런서 서버는 각각 다수의 응용프로그램 플랫폼과 다수의 컴퓨터 엔진 각각에서 보고된 해당 워크로드에 따라 다수의 응용프로그램 플랫폼과 다수의 컴퓨터 엔진에 걸쳐 워크로드를 분산하도록 형상화됨을 특징으로 하는 인증서 관리 시스템.

청구항 14

제1항에 있어서, 인증서 관리 시스템은 컴퓨터화된 장치와 관련된 인증서 활동에 관한 정보를 프로비저닝 컨트롤러에 전송하여 로그에 저장하도록 추가로 작동함을 특징으로 하는 인증서 관리 시스템.

청구항 15

제5항에 있어서, 등록 인증서에 대한 요청을 등록 권한 응용프로그램에 전송하기 전에 컴퓨터화된 장치를 인증하도록 작동할 수 있는 프로비저닝 컨트롤러를 추가로 포함함을 특징으로 하는 인증서 관리 시스템.

청구항 16

제5항에 있어서, 등록 인증서는 공개 키 인증서 소지자를 복수의 컴퓨터화된 장치를 포함하는 생태계의 승인된 참여자로 식별하는 공개 키 인증서이고, 생태계의 각 승인된 참여자는 복수의 컴퓨터화된 장치와의 통신을 가능하게 하는 하나 이상의 디지털 자산을 수신할 수 있음을 특징으로 하는 인증서 관리 시스템.

청구항 17

등록 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 하나 이상의 등록 권한 컴퓨터 엔진에 통신적으로 연결된 등록 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 단계;

가명 인증 권한 응용프로그램은 디지털 자산을 생성하고 등록 권한 응용프로그램에 조건부로 전송하고, 가명 인증 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 하나 이상의 가명 인증 권한 컴퓨터 엔진에 통신적으로 연결된 가명 인증 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 단계;

및

하나 이상의 인증서 로드는 시간 기간 동안 각 컴퓨터화된 장치에 저장될 디지털 자산의 수를 나타내며, 다수의 컴퓨터화된 장치의 각 컴퓨터화된 장치에 하나 이상의 인증서 로드를 할당하는 단계; 를 포함하는 인증서의 보안 제공 방법에 있어서,

인증서 로드는 각 컴퓨터화된 장치가 시간 기간 동안 다른 컴퓨터화된 장치와 다른 수의 디지털 자산을 저장할 수 있도록 할당할 수 있으며,

하나 이상의 등록 권한 컴퓨터 엔진의 하나 이상의 컴퓨터 엔진과 하나 이상의 가명 인증 권한 컴퓨터 엔진에 통신적으로 연결된 하나 이상의 로드 밸런서는 하나 이상의 컴퓨터 엔진의 상태 측정을 기반으로 하나 이상의 컴퓨터 엔진에 하나 이상의 요청을 배포하는 작업을 수행함을 특징으로 하는 인증서의 보안 제공 방법.

청구항 18

제17항에 있어서, 상기 상태 측정은 적어도 하나의 컴퓨터 엔진의 작동 온도, 적어도 하나의 컴퓨터 엔진의 인클로저 내부의 습도 수준, CPU 용량, 저장 용량, 상기 적어도 하나의 컴퓨터 엔진의 재시작 또는 재부팅 빈도, 적어도 하나의 컴퓨터 엔진의 가장 최근 재시작 이후의 시간, 적어도 하나의 컴퓨터 엔진의 일정 기간 동안의 디스크 오류 또는 메모리 오류의 수, 적어도 하나의 컴퓨터 엔진의 예약된 유지 관리 이벤트까지의 시간, 적어도 하나의 컴퓨터 엔진이 백업 전원 공급 장치에서 실행 중이라는 표시, 또는 적어도 하나의 컴퓨터 엔진의 전원 공급 장치에 대한 마지막 정전 또는 전압 감소 이후의 기간. 선택된 적어도 하나를 포함함을 특징으로 하는 인증서의 보안 제공 방법.

청구항 19

제17항에 있어서,

등록 인증 권한 응용프로그램은 등록 인증서를 생성하고 등록 권한 응용프로그램에 조건부로 전송하고, 등록 인증 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 하나 이상의 등록 인증 권한 컴퓨터 엔진에 통신적으로 연결된 등록 인증 권한 응용프로그램에서 요청한 암호화 계산을 수행하는 단계; 및

등록 권한 응용프로그램에서 등록 인증서에 대한 요청을 수신한 것에 대한 응답으로 등록 인증서를 생성하는 단계;

를 더욱 포함함을 특징으로 하는 인증서의 보안 제공 방법.

청구항 20

제17항에 있어서,

컴퓨터화된 장치와 관련된 인증서 활동에 대한 정보를 로그에 저장하기 위하여. 프로비저닝 컨트롤러에 전송하는 단계; 를 더욱 포함하는 인증서의 보안 제공 방법.

청구항 21

제17항에 있어서, 등록 인증서에 대한 요청을 등록 권한 응용프로그램에 전송하기 전에 컴퓨터화된 장치를 인증하는 단계; 를 더욱 포함하는 인증서의 보안 제공 방법.

청구항 22

제17항에 있어서, 등록 인증서는 다수의 컴퓨터화 장치를 포함하는 생태계에서 공인 참여자로서 공개 키 인증서 보유자를 식별하는 공개 키 인증서이고, 생태계의 각 공인 참여자는 다수의 컴퓨터화 장치와의 통신을 가능하게 하는 하나 이상의 디지털 자산을 수신함을 특징으로 하는 인증서의 보안 제공 방법.

청구항 23

프로세서의 실행에 응답하여 작업을 수행하도록 하는 복수의 명령어를 포함하는 인증서를 보안 제공하기 위한 비일시적 컴퓨터 판독 저장 매체에 있어서,

상기 프로세서는

등록 권한 응용프로그램에서 요청한 암호화 계산 수행하고;

가명 인증 권한 응용프로그램은 디지털 자산을 생성하고 등록 권한 응용프로그램에 조건부로 전송하고, 가명 인증 권한 응용프로그램에서 요청한 암호화 계산 수행하고; 및

하나 이상의 인증서 로드는 시간 기간 동안 각 컴퓨터화된 장치에 저장될 디지털 자산의 수를 나타내며, 다수의 컴퓨터화된 장치의 각 컴퓨터화된 장치에 하나 이상의 인증서 로드를 할당하고,

하나의 인증서 로드는 할당 가능하므로 각 컴퓨터화된 장치는 시간 기간 동안 다른 컴퓨터화된 장치와 다른 수의 디지털 자산을 저장할 수 있으며, 하나 이상의 인증서 로드는 시간 기간 동안 각 컴퓨터화된 장치에 저장될 디지털 자산의 수를 나타내며,

하나 이상의 컴퓨터 엔진에 통신적으로 연결된 하나 이상의 로드 밸런서는 하나 이상의 컴퓨터 엔진의 상태 측정을 기반으로 하나 이상의 컴퓨터 엔진에 적어도 하나의 요청을 배포하는 작업을 수행하고,

하나 이상의 컴퓨터 엔진은 등록 권한 응용프로그램과 가명 인증 권한 응용프로그램 중 하나에서 요청한 암호화 계산 중 적어도 하나를 수행하도록

유도하는 비일시적 컴퓨터 판독 저장 매체.

청구항 24

제 23항에 있어서, 상기 상태 측정은 하나 이상의 컴퓨터 엔진의 작동 온도, 하나 이상의 컴퓨터 엔진의 인클로저 내부의 습도 수준, CPU 용량, 저장 용량, 하나 이상의 컴퓨터 엔진의 재시작 또는 재부팅 빈도, 하나 이상의 컴퓨터 엔진의 가장 최근 재시작 이후의 시간, 일정 기간 동안 하나 이상의 컴퓨터 엔진의 디스크 오류 또는 메모리 오류 수, 하나 이상의 컴퓨터 엔진의 예약된 유지 관리 이벤트까지의 시간, 하나 이상의 컴퓨터 엔진이 백업 전원 공급 장치에서 실행 중이라는 표시, 또는 하나 이상의 컴퓨터 엔진의 전원 공급 장치에 대한 마지막 정

전 또는 전압 감소 이후의 기간에 선택된 하나 이상을 포함함을 특징으로 하는 비일시적 컴퓨터 판독 저장 매체.

청구항 25

제 23항에 있어서,

등록 인증 권한 응용프로그램은 등록 인증서를 생성하고 등록 권한 응용프로그램에 조건부로 전송하고, 등록 인증 권한 응용프로그램에서 요청한 암호화 계산 수행; 및

등록 권한 응용프로그램에서 등록 인증서에 대한 요청을 수신한 것에 대한 응답으로 등록 인증서 생성; 을 더욱 유도함을 특징으로 하는 비일시적 컴퓨터 판독 저장 매체.

청구항 26

제 23항에 있어서, 컴퓨터화된 장치와 관련된 인증서 활동에 대한 정보를 로그에 저장하기 위하여 프로비저닝 컨트롤러에 전송; 을 더욱 유도함을 특징으로 하는 비일시적 컴퓨터 판독 저장 매체.

청구항 27

제 25항에 있어서, 등록 인증서에 대한 요청을 등록 권한 응용프로그램에 전송하기 전에 컴퓨터화된 장치를 인증; 을 더욱 유도함을 특징으로 하는 비일시적 컴퓨터 판독 저장 매체.

청구항 28

제 1항에 있어서, 인증서 로드는 가입자가 할당 가능함을 특징으로 하는 인증서 관리시스템.

청구항 29

제 17항에 있어서, 인증서 로드는 가입자에 의해 할당 가능함을 특징으로 하는 인증서의 보안 제공 방법.

청구항 30

제 23항에 있어서, 인증서 로드는 가입자에 의해 할당 가능함을 특징으로 하는 비일시적 컴퓨터 판독 저장 매체.

청구항 31

제 1항에 있어서, 확장 가능한 인증서 관리 시스템은 시간 기간 동안 사용 가능한 디지털 자산 수를 나타내는 가입자당 디지털 자산 사용량을 할당함을 특징으로 하는 인증서 관리시스템.

청구항 32

제 17항에 있어서, 더 나아가 시간 기간 동안 사용 가능한 디지털 자산의 수를 나타내는 가입자당 디지털 자산 사용량의 할당을 포함함을 특징으로 하는 인증서의 보안 제공 방법.

청구항 33

제 23항에 있어서, 프로세서는 시간 기간 동안 사용 가능한 디지털 자산의 수를 나타내는 가입자당 디지털 자산 사용량을 할당하는 것을 더 포함하는 작업을 수행하도록 유도함을 특징으로 하는 비일시적 컴퓨터 판독 저장 매체.

발명의 설명

기 술 분 야

[0001] 본 출원은 2016년 11월 14일에 출원된 미국 잠정 특허출원 제62/421,878호, 2016년 11월 14일에 출원된 미국 잠정 특허출원 제62/421,852호, 2017년 4월 20일에 출원된 미국 잠정 특허출원 제62/487,909호의 우선권을 주장하는 2017년 11월 14일자로 출원된 미국 특허출원 15/812,510호의 부분 계속 출원으로 이들 모두는 전체적으로 본 출원에 참고 문헌으로 인용된다.

[0002] 본 발명은 컴퓨터화 디바이스의 보안 프로비저닝을 위한 시스템, 디바이스 및 방법에 관한 것이다.

배 경 기 술

[0003] 컴퓨터가 점점 더 소형화되고 상품화됨에 따라 제조업체는 하나 이상의 내장된 컴퓨터 또는 프로세서를 포함하는 점점 더 다양한 디바이스를 생산하고 있다. 컴퓨터화 디바이스의 컴퓨터는 디바이스의 작동을 제어하고 데이터를 수집 저장 및 공유하며 다른 컴퓨터 및 다른 컴퓨터화 디바이스와 통신할 수 있다. 또한 자체 소프트웨어를 업데이트한다.

[0004] 사물 인터넷(IoT)은 내장형 프로세서, 전자기기, 소프트웨어, 데이터, 센서, 액추에이터 및/또는 네트워크 연결을 지닌 컴퓨터화 물리적 디바이스의 네트워크로서 이러한 디바이스는 인터넷, 셀룰러 네트워크 및 기타 무선 네트워크를 포함하는 디지털 네트워크를 통해 데이터를 연결하고 교환할 수 있게 한다. 일반적으로 각 "사물"은 내장형 컴퓨터 시스템을 통해 고유하게 식별될 수 있으며 기존 인터넷 인프라 내에서 상호 운용될 수 있다.

[0005] IoT의 의미에서 "사물"은 소비자 가전제품, 비즈니스 및 기업 환경에서 사용되는 기업용 디바이스, 제조 기계, 농기구, 주택 및 건물의 에너지 소모 디바이스(스위치, 전원 콘센트, 가전 제품, 조명 시스템, 전구, 텔레비전, 차고 문 개폐기, 스프링클러 시스템, 보안 시스템 등), 의료 및 건강관리 디바이스, 인프라 관리 디바이스, 로봇, 드론, 운송 디바이스 및 차량 등과 같은 다양한 컴퓨터화 디바이스를 의미할 수 있다.

[0006] 예를 들어 전부는 아니지만 대부분의 현대식 차량 및 운송 기계(예를 들어, 자동차, 트럭, 항공기, 기차, 선박, 오토바이, 스쿠터 등)는 서브 시스템에 여러 개의 내장형 프로세서 또는 내장형 컴퓨터를 포함하며 일부 측면에서는 컴퓨터로 제어된다. 유사하게 점점 더 많은 현대 교통 인프라 디바이스(예: 신호등, 교통 카메라, 교통 센서, 교량 모니터, 교량 제어 시스템 등)에는 적어도 하나의 내장형 프로세서 또는 내장형 컴퓨터 시스템이 포함되어 있으며 일부 측면에서는 컴퓨터로 제어된다.

[0007] 운송 네트워크의 이러한 컴퓨터 제어 엘레멘트는 일반적으로 상호 통신하여 다양한 유형의 정보를 전후로 전달한다. 또한 안전하고 정확하며 효율적이고 신뢰할 수 있는 작동을 위해 일반적으로 서로 통신하여 다양한 유형의 정보를 주고 받으며 차량-대-차량(V2V, 자동차 대 자동차, C2C라고도 함) 통신 및/또는 차량 대 인프라(V2I, 자동차 대 인프라, C2I 라고도 함) 통신을 통해 다른 차량으로부터/차량에 주거나/받는 정보에 응답하거나 반응하며 작동을 변경하거나 의존한다.

[0008] 컴퓨터화 디바이스의 컴퓨터는 소프트웨어 및/또는 펌웨어 및 데이터에 따라 작동한다. 안전하고 적절한 작동을 보장하기 위해 컴퓨터화 디바이스는 적절한 소프트웨어, 펌웨어, 실행 가능 명령어, 디지털 인증서(예: 공개 키 인증서), 암호화 키 등(이하 총칭하여 "디지털 자산" 또는 "소프트웨어"라고 함)에 의해 제조자가 의도한 대로 적절하게 초기화되고 업데이트 되어야 한다. 이를 통해 IoT는 인증되고 정상으로 알려진 소프트웨어 및 데이터를 실행하는 디바이스로만 구성된다.

[0009] 그러나 권한이 없는 사람이나 조직(예를 들어 해커)이 컴퓨터화 디바이스의 소프트웨어를 교체하거나 변경할 때 문제가 발생한다. 이전 소프트웨어, 테스트되지 않은 소프트웨어, 승인되지 않은 소프트웨어 및/또는 알려진 버그가 있는 소프트웨어가 컴퓨터화 디바이스에 설치된 경우에도 문제가 발생한다.

[0010] 따라서 컴퓨터화 디바이스에서 디지털 자산을 안전하게 프로비저닝 하기 위한 개선된 시스템, 방법 및 기술을 제공하여 오류가 발생하거나 오작동하거나 테스트되지 않았거나 악의적으로 변경되거나 또는 기타 적절하지 않은 소프트웨어 및 데이터를 사용하여 작동하는 것으로부터 컴퓨터화 디바이스를 보호한다.

발명의 내용

과제의 해결 수단

[0011] 본 명세서에는 보안 자격 증명 및 디지털 인증서와 같은 특정 유형의 디지털 자산을 안전하게 생성하고 제공하기 위한 시스템, 방법 및 디바이스를 개시한다. 다양한 실시형태에서 시스템, 방법 및 디바이스는 확장 가능한 인증서 관리 시스템(CMS)을 사용하여 보안 자격 증명 및 공개 키 인증서와 같은 특정 유형의 디지털 자산을 생성하고 제공한다. 일부 실시형태에서 CMS는 이러한 인증서에 대한 요청에 응답하여 등재 인증서 및 가명 인증서와 같은 인증서를 제공한다.

[0012] 다양한 실시형태에서 CMS는 등록 권한, 하나 이상의 연결 권한, 가명 인증 권한 및 등록 인증 권한을 포함하는 확장 가능한 아키텍처를 지닌다. 예시적인 CMS는 등록 권한 응용프로그램을 실행하고 등록 권한 응용프로그램에

의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결되는 하나 이상의 응용프로그램 플랫폼을 포함할 수 있다.

[0013] 하나 이상의 응용프로그램 플랫폼은 하나 이상의 가상 머신(VM) 또는 하나 이상의 하드웨어 플랫폼(예를 들어 서버, 컴퓨터 또는 소프트웨어 응용프로그램을 호스팅하고 실행할 수 있는 다른 컴퓨터 하드웨어)을 포함할 수 있다.

[0014] 또한 시스템은 등재 인증 권한을 실행하고 등재 인증 권한에서 요구하는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 VM을 포함할 수 있다. 등재 인증 권한 응용프로그램은 등재 인증서를 생성하고 조건부로 등재 권한 응용프로그램에 전송하도록 작동할 수 있다.

[0015] 예시적인 CMS는 가명 인증 권한 응용프로그램을 실행하고 가명 인증 권한에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 VM을 더욱 포함할 수 있다. 가명 인증 권한 응용프로그램은 가명 인증서를 생성하고 조건부로 등록 권한 응용프로그램에 전송하도록 작동할 수 있다.

[0016] CMS 시스템은 첫 번째 및 두 번째 연결 권한을 실행하고 첫 번째 및 두 번째 연결 권한에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 VM을 또한 포함할 수 있다. 첫 번째 연결 권한 응용프로그램 및 두 번째 연결 권한 응용프로그램은 연결 값을 생성하고 조건부로 등록 권한 응용프로그램에 전송하도록 작동 가능하다.

[0017] 일부 실시형태에서 프로비저닝 제어기에 인증서를 보안 제공하기 위한 확장 가능한 CMS는 등록 권한 응용프로그램을 실행하고 등록 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼; 등재 인증 권한 응용프로그램을 실행하고 등재 인증 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결되고, 또한 등재 인증 권한 응용프로그램은 등재 인증서를 생성하고 등록 권한 응용프로그램에 조건부로 전송하도록 작동 가능한 하나 이상의 응용프로그램 플랫폼; 가명 인증 권한 응용프로그램을 실행하고 가명 인증 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결되고, 또한 가명 인증 권한 응용프로그램은 가명 인증서를 생성하고 등록 권한 응용프로그램에 조건부로 전송하도록 작동 가능한 하나 이상의 응용프로그램 플랫폼; 첫 번째 연결 권한 응용프로그램을 실행하고 첫 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼; 및 두 번째 연결 권한 응용프로그램을 실행하고 두 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결되고, 또한 첫 번째 연결 권한 응용프로그램 및 두 번째 연결 권한 응용프로그램은 연결 값을 생성하고 등록 권한 응용프로그램에 조건부로 전송하도록 작동 가능한 하나 이상의 응용프로그램 플랫폼;을 포함한다.

[0018] 또 다른 실시형태에서 CMS는 등록 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼, 등재 인증 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼, 가명 인증 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼, 첫 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼 및 두 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼에 작동 가능하게 연결된 하나 이상의 데이터베이스를 더욱 포함할 수 있다.

[0019] 또 다른 실시형태에서 각각의 등록 권한 응용프로그램, 등재 인증 권한 응용프로그램, 가명 인증 권한 응용프로그램, 첫 번째 연결 권한 응용프로그램, 두 번째 연결 권한 응용프로그램 및 하나 이상의 데이터베이스는 서로 독립적으로 확장되도록 작동 가능하다.

[0020] 또 다른 실시형태에서 등재 인증 권한 응용프로그램은 등록 권한 응용프로그램으로부터 등재 인증서에 대한 요청을 수신하는 것에 응답하여 등재 인증서를 생성하도록 작동 가능하고, 등재 인증 권한 응용프로그램은 등록 권한 응용프로그램으로부터 가명 인증서에 대한 요청을 수신하는 것에 응답하여 가명 인증서를 생성하도록 작동 가능하고, 첫 번째 연결 권한 응용프로그램 및 두 번째 연결 권한 응용프로그램은 등록 권한 응용프로그램으로부터 연결 값에 대한 요청을 수신하는 것에 응답하여 연결 값을 생성하도록 작동 가능하다.

[0021] 일부 실시형태에서 등록 권한 응용프로그램, 등재 인증 권한 응용프로그램, 가명 인증 권한 응용프로그램, 첫 번째 연결 권한 응용프로그램 및 두 번째 연결 권한 응용프로그램 각각은 다수의 메시지 큐를 포함하는 메시지 큐 서비스에 의해 서로 통신 가능하게 연결될 수 있다.

[0022] 특정 실시형태에서

[0023] 등재 인증 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼은 첫 번째 다수의 메시지 큐에 의해 등재 인증 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 가상 머신이고;

[0024] 첫 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼은 두 번째 다수의 메시지 큐에 의해 첫 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 가상 머신이고; 및

[0025] 두 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼은 세 번째 다수의 메시지 큐에 의해 두 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 가상 머신이다.

[0026] 첫 번째, 두 번째 및 세 번째 다수의 메시지 큐를 지닌 일부 실시형태에 따르면

[0027] 첫 번째 다수의 메시지 큐는 등재 인증 권한 응용프로그램을 실행하는 하나 이상의 가상 머신에 전달될 메시지를 큐 하기 위한 첫 번째 메시지 큐; 및 등재 인증 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진으로 전달될 메시지를 큐 하기 위한 두 번째 메시지 큐;를 포함하고

[0028] 두 번째 다수의 메시지 큐는 첫 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 가상 머신에 전달될 메시지를 큐 하기 위한 세 번째 메시지 큐; 및 첫 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진으로 전달될 메시지를 큐 하기 위한 네 번째 메시지 큐;를 포함하고,

[0029] 세 번째 다수의 메시지 큐는 두 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 가상 머신에 전달될 메시지를 큐 하기 위한 다섯 번째 메시지 큐; 및 두 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진으로 전달될 메시지를 큐 하기 위한 여섯 번째 메시지 큐;를 포함한다.

[0030] 첫 번째, 두 번째 및 세 번째 다수의 메시지 큐를 지닌 또 다른 실시형태에서

[0031] 첫 번째 다수의 메시지 큐는 등재 인증 권한 응용프로그램을 실행하는 하나 이상의 가상 머신으로 전달되고 머신으로부터 전송될 메시지를 큐 하기 위한 첫 번째 양방향 메시지 큐; 등재 인증 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진으로 전달되고 컴퓨터 엔진으로부터 전송될 메시지를 큐 하기 위한 두 번째 양방향 메시지 큐;를 포함하고,

[0032] 두 번째 다수의 메시지 큐는 첫 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 가상 머신으로 전달되고 머신으로부터 전송될 메시지를 큐 하기 위한 세 번째 양방향 메시지 큐; 및 첫 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진으로 전달되고 컴퓨터 엔진으로부터 전송될 메시지를 큐 하기 위한 네 번째 양방향 메시지 큐;를 포함하고, 및

[0033] 세 번째 다수의 메시지 큐는 두 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 가상 머신으로 전달되고 머신으로부터 전송될 메시지를 큐 하기 위한 다섯 번째 양방향 메시지 큐; 및 두 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진으로 전달되고 컴퓨터 엔진으로부터 전송될 메시지를 큐 하기 위한 여섯 번째 양방향 메시지 큐;를 포함한다.

[0034] CMS의 또 다른 실시형태에서

[0035] 등재 인증 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼은 첫 번째 로드 밸런서에 의해 등재 인증 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결되고;

[0036] 첫 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼은 두 번째 로드 밸런서에 의해 첫 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결되고; 및

[0037] 두 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼 세 번째 로드 밸런서에 의해 두 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된다.

[0038] 첫 번째, 두 번째 및 세 번째 로드 밸런서를 포함하는 CMS의 특정 실시형태에서 각각의 로드 밸런서는 로드 밸런서 가상 머신 및 로드 밸런서 서버 중 하나 이상을 포함할 수 있으며; 로드 밸런서 가상 머신 및 로드 밸런서

서버는 다수의 응용프로그램 플랫폼 및 다수의 컴퓨터 엔진에 걸쳐 작업로드를 분배시키도록 각각 형상화 된다.

[0039] 로드 밸런서 가상 머신 및 로드 밸런서 서버를 지닌 다른 실시형태에서 로드 밸런서 가상 머신 및 로드 밸런서 서버는 라운드 로빈 기술을 사용하여 다수의 응용프로그램 플랫폼 및 다수의 컴퓨터 엔진에 걸쳐 작업로드를 분배시키도록 각각 형상화 된다.

[0040] 로드 밸런서 가상 머신 및 로드 밸런서 서버를 포함하는 또 다른 실시형태에서 로드 밸런서 가상 머신 및 로드 밸런서 서버는 각각의 다수 응용프로그램 플랫폼 및 각각의 다수 컴퓨터 엔진에 의해 리포트된 개별 작업로드를 기반으로 하여 다수의 응용프로그램 플랫폼 및 다수의 컴퓨터 엔진에 걸쳐 작업로드를 분배시키도록 각각 형상화된다.

[0041] 다양한 실시형태에서 프로비저닝 제어기는 컴퓨터화 디바이스를 대신하여 등재 인증서에 대한 요청을 등록 권한 응용프로그램에 전송하고; 등록 권한 응용프로그램으로부터 등재 인증 권한 응용프로그램에 의해 생성될 수 있는 등재 인증서를 수신하고; 컴퓨터화 디바이스에 등재 인증서를 전송하고; 컴퓨터화 디바이스를 대신하여 다수의 가명 인증서에 대한 요청을 등록 권한 응용프로그램에 전송하고; 등록 권한 응용프로그램으로부터 가명 인증 권한 응용프로그램에 의해 생성될 수 있는 다수의 가명 인증서를 수신하고; 컴퓨터화 디바이스로 다수의 가명 인증서를 전송하고; 컴퓨터화 디바이스와 관련된 로그를 생성 및 유지하고; 컴퓨터화 디바이스의 인증서 활동에 관한 정보를 저장하도록 작동 가능하다.

[0042] 프로비저닝 제어기가 로그를 생성하고 유지하도록 작동 가능한 일부 실시형태에서 프로비저닝 제어기는 로그에 저장하기 위해 컴퓨터화 디바이스와 관련된 인증서 활동에 관한 정보를 프로비저닝 제어기로 전송하도록 더욱 작동 가능하다.

[0043] 프로비저닝 제어기가 등록 권한 응용프로그램에 등재 인증서에 대한 요청을 전송하도록 작동 가능한 특정 실시형태에서 프로비저닝 제어기는 등재 인증서에 대한 요청을 등록 권한 응용프로그램에 전송하기 이전에 컴퓨터화 디바이스를 인증하도록 더욱 작동 가능하다.

[0044] 또 다른 실시형태에서 등재 인증서는 다수의 컴퓨터화 디바이스를 포함하는 생태계 내에서 공개 키 인증서의 소유자를 권한 있는 참여자로서 식별하는 공개 키 인증서일 수 있으며, 생태계 내의 각각의 권한 있는 참여자는 다수의 컴퓨터화 디바이스와의 통신을 가능하게 하는 하나 이상의 가명 인증서를 수신할 수 있다.

[0045] 일부 실시형태에서 하나 이상의 컴퓨터화 디바이스를 프로비저닝 하기 위한 시스템은 컴퓨터화 디바이스에 통신 가능하게 연결되고 디지털 자산을 수신하고 디지털 자산을 컴퓨터화 디바이스에 로드하도록 작동 가능한 분배기 어플라이언스; 첫 번째 보안 통신 채널을 통해 분배기 어플라이언스에 연결되고 디지털 자산을 생성하며 조건부로 분배기 어플라이언스에 전송하도록 작동 가능한 디지털 자산 관리 시스템; 및 두 번째 보안 통신 채널을 통해 분배기 어플라이언스에 연결되고 세 번째 보안 통신 채널을 통해 디지털 자산 관리 시스템에 연결되며, 디지털 자산 관리 시스템이 디지털 자산을 분배기 어플라이언스에 전송하도록 지시할 수 있는 프로비저닝 제어기;를 포함한다.

[0046] 컴퓨터화 디바이스는 디지털 자산이 컴퓨터화 디바이스에 로딩되기 전에는 디지털 자산이 존재하지 않기 때문에 기능하지 않거나 부분적으로만 기능할 수 있다. 디지털 자산은 디지털 인증서, 암호화 키 및 실행 가능한 소프트웨어 중 적어도 하나일 수 있다. 특정 실시형태에서 시스템은 확장 가능한 CMS와 상호 작용하거나 자격증명을 수신할 수 있다.

[0047] 다양한 실시형태에서 시스템은 네 번째 보안 통신 채널을 통해 디지털 자산 관리 시스템에 접속되고 분배기 어플라이언스가 연결 해제된 후 컴퓨터화 디바이스에 통신 가능하게 접속되며 두 번째 디지털 자산을 수신하고 컴퓨터화 디바이스에 두 번째 디지털 자산을 로딩하도록 작동 가능한 두 번째 분배기 어플라이언스를 더욱 포함하며 프로비저닝 제어기는 디지털 자산 관리 시스템이 디지털 자산을 분배기 어플라이언스에 전송하도록 지시하는 것이 더욱 작동 가능하다.

[0048] 컴퓨터화 디바이스는 두 번째 디지털 자산이 컴퓨터화 디바이스에 로딩된 후에 완전히 기능할 수 있다.

[0049] 다양한 실시형태에서 디지털 자산 관리 시스템은

[0050] 등록(registration) 권한 응용프로그램을 실행하고 등록 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼;

[0051] 등재(enrollment) 인증 권한 응용프로그램을 실행하고 등재 인증 권한 응용프로그램에 의해 요구되는 암호화 연

산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼;

[0052] 가명(pseudonym) 인증 권한 응용프로그램을 실행하고 가명 인증 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼;

[0053] 첫 번째 연결 권한 응용프로그램을 실행하고 첫 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼; 및

[0054] 두 번째 연결 권한 응용프로그램을 실행하고 두 번째 연결 권한 응용프로그램에 의해 요구되는 암호화 연산을 수행하는 하나 이상의 컴퓨터 엔진에 통신 가능하게 연결된 하나 이상의 응용프로그램 플랫폼;

[0055] 을 더욱 포함한다.

[0056] 또 다른 실시형태에서디지털 자산 관리 시스템은 등록 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼에 작동 가능하게 연결된 하나 이상의 데이터베이스, 등재 인증 권한을 실행하는 하나 이상의 응용프로그램 플랫폼, 가명 인증 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼, 첫 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼 및 두 번째 연결 권한 응용프로그램을 실행하는 하나 이상의 응용프로그램 플랫폼을 더욱 포함한다.

[0057] 또 다른 실시형태에서 시스템은 프로비저닝 제어기에 작동 가능하게 연결되고 컴퓨터화 디바이스의 제조자를 인증하고 제조자가 컴퓨터화 디바이스의 프로비저닝을 관리할 수 있게 하는 포털 및/또는 프로비저닝 제어기에 작동 가능하게 연결되고 컴퓨터화 디바이스의 설치자를 인증하고 설치자가 컴퓨터화 디바이스의 프로비저닝을 관리할 수 있게 하는 포털 및/또는 프로비저닝 제어기에 작동 가능하게 연결되고 컴퓨터화 디바이스의 조절자를 인증하고 조절자가 컴퓨터화 디바이스의 프로비저닝을 조절할 수 있게 하는 포털을 더욱 포함한다.

[0058] 또 다른 실시형태에서 프로비저닝 제어기는 컴퓨터화 디바이스에 로딩하기 위해 분배기 어플라이언스에 디지털 자산(예를 들면 실행 가능한 소프트웨어 이미지)을 전송할 수 있도록 더욱 작동 가능하다. 또 다른 실시형태에서 프로비저닝 제어기는 디지털 디바이스와 연관되고 디지털 디바이스에 대한 프로비저닝 활동에 관한 정보를 저장하는 로그를 생성 및 유지하도록 더욱 작동 가능하며, 분배기 어플라이언스는 디지털 디바이스에 관련된 프로비저닝 활동에 관한 정보를 로그 내에 저장하기 위해 프로비저닝 제어기에 전송할 수 있도록 더욱 작동 가능하다.

[0059] 또 다른 실시형태에서 프로비저닝 제어기는 디지털 자산 관리 시스템이 디지털 자산을 전송하도록 지시하기 전에 디지털 디바이스를 인증하도록 더욱 작동 가능하다.

도면의 간단한 설명

[0060] 첨부된 도면은 본 명세서에 통합되어 본 명세서의 일부를 구성하고 본 발명의 실시형태를 나타내며 발명의 상세한 설명과 함께 본 발명의 원리를 설명하는 역할을 한다.

도 1은 본 발명의 실시형태와 일치하는 보안 프로비저닝을 위한 시스템의 실시예를 나타내는 블록도이다.

도 2는 본 발명의 실시형태와 일치하는 컴퓨터화 디바이스의 보안 프로비저닝을 위한 프로세스의 실시예를 나타내는 스윔 레인 다이어그램이다.

도 3은 본 발명의 실시형태와 일치하는 컴퓨터화 디바이스의 보안 프로비저닝을 위한 프로세스의 또 다른 실시예를 나타내는 스윔 레인 다이어그램이다.

도 4a는 본 발명의 실시형태와 일치하는 메시지 큐를 지닌 확장 가능한 보안 디지털 자산 관리 시스템을 구현하기 위한 시스템 실시예의 블록도 첫 번째 부분이다.

도 4b는 본 발명의 실시형태와 일치하는 메시지 큐를 지닌 확장 가능한 보안 인증서 관리 시스템을 구현하기 위한 시스템 실시예의 블록도 두 번째 부분이다.

도 5a는 본 발명의 실시형태와 일치하는 인증서와 같은 자격증명을 보안 제공하기 위한 프로세스의 실시예를 나타내는 스윔 레인 다이어그램의 첫 번째 부분이다.

도 5b는 본 발명의 실시형태와 일치하는 인증서와 같은 자격증명을 보안 제공하기 위한 프로세스의 실시예를 나타내는 스윔 레인 다이어그램의 두 번째 부분이다.

도 6a는 본 발명의 실시형태와 일치하는 양방향 메시지 큐를 지닌 확장 가능한 보안 인증서 관리 시스템을 구현

하기 위한 시스템 실시예의 블록도 첫 번째 부분이다.

도 6b는 본 발명의 실시형태와 일치하는 양방향 메시지 큐를 지닌 확장 가능한 인증서 관리 시스템을 구현하기 위한 시스템 실시예의 블록도 두 번째 부분이다.

도 7a는 본 발명의 실시형태와 일치하는 로드 밸런서를 지닌 확장 가능한 보안 인증서 관리 시스템을 구현하기 위한 시스템 실시예의 블록도 첫 번째 부분이다.

도 7b는 본 발명의 실시형태와 일치하는 로드 밸런서를 지닌 확장 가능한 보안 인증서 관리 시스템을 구현하기 위한 시스템 실시예의 블록도 두 번째 부분이다.

도 8은 본 발명의 실시형태와 일치하는 라운드 로빈 요청으로 확장 가능한 보안 인증서 관리 시스템을 구현하기 위한 시스템 실시예의 블록도이다.

도 9는 본 발명의 실시형태와 일치하는 작업로드에 기반한 요청으로 확장 가능한 보안 인증서 관리 시스템을 구현하기 위한 시스템 실시예의 블록도이다.

도 10a는 본 발명의 실시형태와 일치하는 메시지 큐를 지닌 확장 가능한 보안 디지털 자산 관리 시스템을 구현하기 위한 시스템 실시예의 블록도 첫 번째 부분이다.

도 10b는 본 발명의 실시형태와 일치하는 메시지 큐를 지닌 확장 가능한 보안 인증서 관리 시스템을 구현하기 위한 시스템 실시예의 블록도 두 번째 부분이다.

도 11은 본 발명의 실시형태와 일치하는 호스팅 시스템 및 방법에 사용될 수 있는 컴퓨터 시스템 실시예의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0061] 이제 본 발명의 다양한 실시형태가 상세하게 설명되며 그 실시예는 첨부된 도면에 도시되어 있다. 편의를 위해 동일한 참조 번호가 동일하거나 유사한 부분을 나타내기 위해 도면 전체에 걸쳐 사용된다.

[0062] 현장에서 안전하고 적절한 작동을 보장하기 위해 차량에 사용되는 전자 제어 유니트(ECU)와 같은 내장형 디바이스는 보안 자산과 같은 디지털 자산을 프로비저닝 함으로써 제조 과정에서 적절하게 초기화 시킬 필요가 있다. 디지털 자산에는 다양한 암호화 키, 고유 식별자, 디지털 인증서 및 소프트웨어가 포함될 수 있다.

[0063] 대부분의 경우 이러한 디지털 자산 및 제조업체의 출처는 지리적으로 서로 다르게 위치하여 있으며 일반적으로 보안되지 않은 인터넷 통신을 통해 상호 연결된다. 따라서 이러한 디지털 자산의 출처로부터 디바이스까지 엔드-투-엔드 보안 채널을 만들어 악의적인 당사자 또는 우연히 디지털 자산에 접속하거나 수정할 수 없게 하는 것이 바람직하다.

[0064] TLS/SSL과 같은 엔드-투-엔드 보호를 위한 종래의 네트워크 보안 프로토콜에는 미리 공유된 키 또는 특정 비밀 보안 자료가 모든 통신 당사자에게 미리 존재해야 한다는 단점이 있다. 이는 디지털 자산을 프로비저닝 하기 위해 일부 초기 비밀 자료가 미리 존재해야 하는 주기적인 기술적 문제를 야기한다. 이 문제는 초기 비밀 자료를 어떻게 보호하는지를 포함한다. 이 문제는 물류를 단순화하기 위해 일반적으로 초기 소프트웨어의 단일 버전을 제조 과정에서 컴퓨터화 디바이스에 로딩시키기 때문에 컴퓨터화 디바이스에 특히 민감하다.

[0065] 초기 소프트웨어에 초기 보안 자료가 포함되어야 하는 경우 전반적 비밀이 필요하다. 결과적으로 동일한 전반적 비밀을 공유하기 때문에 초기 보안 자료를 손상시키면 모든 디바이스에 프로비저닝 되는 모든 디지털 자산을 손상시킬 수 있다. 본 명세서의 내용과 일치하는 시스템, 방법 및 디바이스는 종래의 프로비저닝 시스템의 이러한 문제점 및 다른 문제점을 해결한다.

[0066] 프로비저닝은 일반적으로 적절한 데이터 및 소프트웨어로 컴퓨터화 디바이스를 제조하기 위해 취해지는 일련의 작업을 의미한다. 또한 작동 환경에 디바이스를 올바르게 설치하여 작동 준비 상태로 만드는 일련의 작업을 포함할 수도 있다. 작업에는 적절한 디지털 자산(예를 들면 운영 체제, 디바이스 드라이버, 미들웨어, 응용프로그램, 디지털 인증서 등)을 디바이스의 디지털 저장소(예를 들면 메모리)에 로딩하는 것과 (필요한 경우) 디바이스에 특정 디지털 자산을 적절하게 커스터마이징 및 형상화하는 것을 포함하며 이 디지털 자산은 특정 디바이스에 고유할 수 있다. 이러한 작업은 컴퓨터화 디바이스가 합법적인 디바이스 제조업체가 만든 합법적인 디바이스며 복제품이나 모조품 디바이스가 아닌지 확인하는 것 또한 포함한다.

[0067] 작업은 디바이스를 작동 환경에 올바르게 설치하고 적절하게 작동하는지 검증하기 위해 디바이스를 테스트하는

것 또한 포함한다. 정상 작동이 확인된 디바이스만 보안 프로비저닝 하는 능력은 한 제조업체가 디바이스를 제조한 이후에 다른 제조업체에 의해 대형 시스템이나 디바이스에 설치될 수 있다는 점에서 복잡하다. 예를 들어 부품 제조 업체가 만든 차량 탑재 장치(OBU)가 자동차 제조업체가 만든 자동차에 설치될 수 있다. 부적절하게 설치된 디바이스는 제대로 작동하지 않을 수 있다.

[0068] 본 발명에 따른 다양한 실시형태에서 IoT 디바이스를 포함하는 컴퓨터화 디바이스의 보안 프로비저닝을 제공한다. 이러한 실시형태에서 컴퓨터화 디바이스가 사용하는 디지털 자산의 악의적, 부주의, 과실에 의한 변조, 변경, 업데이트 또는 유출을 방지 또는 금지한다. 또한 컴퓨터화 디바이스 및 이들 소프트웨어의 부적절한 설치를 방지 또는 금지한다.

[0069] 본 발명에 따른 다양한 실시형태에서 또한 나중에 발견된 문제를 분석하고 해결하는 데 사용될 수 있는 보안 프로비저닝 프로세스의 감사 로그, 기록, 리포트 등을 생성할 수 있다.

[0070] 본 발명과 일치하는 다양한 실시형태에서 디바이스 및 시스템 제조업체에 대한 서비스로서 제공될 수 있는 보안 프로비저닝 및 관리 플랫폼을 제공할 수 있다.

[0071] 도 1은 본 발명의 실시형태와 일치하는 컴퓨터화 디바이스의 보안 프로비저닝을 위한 시스템(100)의 실시예를 나타내는 블록도이다.

[0072] 도 1의 실시예에 나타난 바와 같이 시스템(100)은 프로비저닝 제어기(120)를 포함한다. 프로비저닝 제어기(120)는 디지털 보안 자산을 안전하게 생성 및 저장하고 다양한 암호화 및 민감한 연산을 안전하게 수행하는 내장된 하드웨어 보안 모듈(HSM)을 지니는 서버 컴퓨터(예를 들면 적어도 하나의 프로세서 및 관련 메모리를 구비함)로서 구현될 수 있다. HSM은 암호화 키와 같은 디지털 보안 자산 및 기타 민감한 데이터를 침입자가 접근할 수 없도록 보호한다.

[0073] 다양한 실시형태에서 프로비저닝 제어기(120)는 시스템(100)의 사용자를 인증하고 보안 통신하는 기능을 하고; 하나 이상의 분배기 어플라이언스(108, 131)와 보안 통신하며 관리하고; 디지털 자산 관리 시스템(DAMS)(110)과 보안 통신하며 작동을 지시하고; 프로비저닝 기록을 생성 및 저장하고; 프로비저닝 기록을 생성, 저장 및 배포하고; 감사 로그를 생성, 저장 및 배포하고; DAMS(110) 및 분배기 어플라이언스(108, 131)의 엘레멘트를 암호화 방식으로 결합시키기 위해 인증서를 생성 및 배포하고; 신뢰를 상실하게 되면 필요에 따라 사용자 및 관리 디바이스를 해지하고; 및 비즈니스 연속성 및 재해 복구를 위해 오프 사이트 저장을 위한 중요 키 및 데이터의 보안 암호화된 백업을 생성 및 배포한다.

[0074] 도 1의 실시예에 나타난 바와 같이 프로비저닝 제어기(120)는 디바이스(106a, 106b)(종합적으로 106으로 지칭될 수 있음)를 보안 프로비저닝 하는 것과 관련된 데이터, 정보 및 디지털 자산을 저장할 수 있는 데이터베이스(125)에 통신 가능하게 연결된다.

[0075] 또한 프로비저닝 제어기(120)는 예를 들면 서버 또는 프로비저닝 제어기(120)에 대한 인터페이스로서 구현될 수 있는 제조업체의 사용자 포털(115)에 보안 통신 가능하게 연결된다.

[0076] 다양한 실시형태에서 디바이스 제조업체(105)의 스태프(109)는 프로비저닝 제어기(120) 및 DAMS(110)에 인터페이스 되고 그들의 디바이스 프로비저닝 활동을 관리하기 위하여 제조업체의 사용자 포털(115)을 사용할 수 있다. 다양한 실시형태에서 제조업체의 사용자 포털(115)은 사용자 이름, 비밀번호, 2-요인 식별 데이터, 안면 인식 이미지, 지문 등과 같은 스태프 사용자(109)로부터의 식별 정보를 수집하고 식별 정보를 프로비저닝 제어기(120)에 제공한다.

[0077] 프로비저닝 제어기(120)는 스태프(109)가 보안 프로비저닝 시스템(100)에 접근하는 것을 허용하기 전에 스태프(109)를 인증한다. 예를 들면 프로비저닝 제어기(120)는 스태프 사용자(109)와 관련되고 이전에 검증되어 데이터베이스(125)에 저장된 식별 정보를 조회하고 저장된 식별 정보를 제조자의 사용자 포털(115)에 의해 수집된 식별 정보와 비교한다.

[0078] 대안적으로 프로비저닝 제어기(120) 또는 DAMS 사용자 포털(115)은 스태프(109)가 시스템(100)을 사용할 권한이 있는지를 결정하는 사용자의 기업 식별 및 인증 시스템과 통합될 수 있다.

[0079] 다양한 실시형태에서 프로비저닝 제어기(120) 또는 DAMS 사용자 포털(115)은 성공적으로 인증된 스태프(109)에게 역할을 부여하여 시스템(100) 내에서 그들의 작업을 제한한다. 일부 실시형태에서 프로비저닝 제어기(120)는 두 세트의 식별 정보가 일치하는 경우에만 접근을 허용한다.

[0080] 이와 유사하게 프로비저닝 제어기(120)는 예를 들면 서버 또는 프로비저닝 제어기(120)에 대한 인터페이스로서 구현될 수 있는 설치자 사용자 포털(116)에 통신 가능하게 연결된다.

[0081] 다양한 실시형태에서 디바이스 설치자의 스태프(132)는 프로비저닝 제어기(120) 및 DAMS(110)와 인터페이스 되고 그들의 디바이스 설치 및 프로비저닝 활동을 관리하기 위하여 제조업체의 사용자 포털(116)을 사용할 수 있다. 프로비저닝 제어기(120)는 스태프(132)를 허용하기 전에 스태프(132)를 인증하고 이들에게 역할을 부여하여 스태프(132)가 보안 프로비저닝 시스템(100)에 접근하여 시스템 상에서 권한 있는 기능을 수행할 수 있게 한다.

[0082] 이와 유사하게 프로비저닝 제어기(120)는 예를 들면 서버 또는 프로비저닝 제어기(120)에 대한 인터페이스로서 구현될 수 있는 조절자 포털(117)에 통신 가능하게 연결된다. 다양한 실시형태에서 일단 프로비저닝 제어기(120)에 의해 인증 된 조절자(140)는 조절자 포털(117)을 사용하여 프로비저닝 제어기(120)와 인터페이스하고 제조자(104), 설치자(130), 디바이스(106) 및/또는 디바이스(106)에 설치된 소프트웨어/디지털 자산의 검토와 승인을 관리한다.

[0083] 프로비저닝 제어기(120)는 조절자(140)의 보안 프로비저닝 시스템(100)으로 접근을 허용하기 전에 조절자(140)를 인증한다. 시스템(100)의 일부 실시형태에서 조절자(140) 및 조절자 포털(117)은 선택적이다.

[0084] 프로비저닝 제어기(120)는 DAMS(110)에 또한 통신 가능하게 연결된다. 다양한 실시형태에서 DAMS(110)는 서버, 디바이스 또는 보안 어플라이언스 및/또는 서버 시스템으로 구현될 수 있다. DAMS(110)는 분배기 어플라이언스(108, 131) 또는 다른 보안 및 인증된 연결을 통해 프로비저닝 말단 엔티티 디바이스로부터 공개 키를 보안 검색하고 디바이스(106)에 설치된 디지털 인증서 및 관련 데이터를 보안 공급한다.

[0085] 또한 DAMS(110)는 분배기 어플라이언스(108, 131)를 통해 컴퓨터화 디바이스(106)의 프로비저닝, 설치, 기능 등에 관한 상태 정보를 제조사(105) 및 설치자(130)로부터 보안 수신한다. 또한 DAMS(110)는 도 1에 나타난 바와 같이 단일 사이트 또는 다중 사이트에서 이러한 프로비저닝을 수행한다. 도 2에 의해 보다 상세하게 설명된 바와 같이 DAMS(110)는 다음 주요 엘레멘트를 포함한다: 루트 인증 권한(CA), 정책 생성기, CRL 생성기, 오작동 권한, 중간 CA, 등재 CA, 연결 권한, 가명 CA 및 등록 권한 등이다.

[0086] DAMS(110)는 William Whyte 등, "V2V 통신을 위한 보안 자격증명 관리 시스템", 2013 IEEE Vehicular Networking Conference, 2013년 12월자 논문에 개시된 새로운 기능을 추가하고 컴포넌트 및 기능을 향상시킨다. 다양한 실시형태에서 DAMS(110)는 다단계 프로그래밍 및 유연한 관리(예를 들면 조절자(140)의 포함을 허용)를 포함한다. DAMS(110)의 다양한 실시형태는 단일 DAMS(110)가 서로 다른 이용자에게 상이한 레벨의 프로비저닝을 또한 제공할 수 있게 한다.

[0087] DAMS(110) 다양한 실시형태는 서로 다른 인증서의 로딩(예를 들면 종래의 시스템에서와 같이 3년 대신에 1주일) 뿐만 아니라 일정 기간(예를 들면 주 당) 동안 서로 다른 디지털 인증서 사용을 할당하도록 이용자를 허용하는 것이 가능하다. DAMS(110)의 다양한 실시형태는 또한 특정 제조업체의 컴퓨터화 디바이스(106)(예를 들면 OEM의 차량)가 제조업체의 영역 내에 머물 수 있도록 이용자 특정 URL을 제공한다(예를 들면 그들의 URL은 그들의 명칭을 나타낸다).

[0088] 도시된 바와 같이 프로비저닝 제어기(120)는 분배기 어플라이언스(108, 131)에 또한 통신 가능하게 연결된다. 다양한 실시형태에서 분배기 어플라이언스(108, 131)는 회사 구내에 설치된 독립형 보안 어플라이언스(도시됨) 또는 이들 사이의 웹 또는 클라우드 서비스로 구현된다.

[0089] 다양한 실시형태에서 분배기 어플라이언스(108, 131)는 바람직하게는 인터넷이 아닌 전용의 통신 채널을 통해 DAMS(110) 및 프로비저닝 제어기(120)를 통해 디지털 자산 및 다른 정보를 보안 송수신하는 신뢰할 수 있는 엔드 포인트 디바이스로서 실현된다. 나타난 바와 같이 분배기 어플라이언스(108, 131)는 디바이스(106a, 106b)로 디지털 자산을 다운로드하고 디바이스로부터 데이터를 수신하기 위해 디바이스(106a, 106b)와 직접 또는 간접적으로 연결된다.

[0090] 다양한 실시형태에서 분배기 어플라이언스(108, 131)는 하드웨어 보안 모듈(HSM), 강화된 운영체제(OS), 방화벽 및 내부 호스트 침입 탐지/방지 시스템을 지닌 서버 컴퓨터(예를 들면 적어도 하나의 프로세서 및 관련 메모리를 지님)를 포함하는 박스로서 구현될 수 있다.

[0091] 분배기 어플라이언스는 신뢰할 수 없는 환경에서 작동하도록 특이적으로 설계되었으나 여전히 신뢰할 수 있고 안정적인 작동을 제공할 수 있다. 분배기 어플라이언스는 자신과 보안 프로비저닝 제어기(120) 및 DAMS(110) 사이에 보안 통신 채널을 지닌다. 이 채널은 분배기 어플라이언스를 제어하고 프로비저닝 관련 데이터 및 로그 정

보를 전송 및 검색하는 데 사용된다.

[0092] 분배기 어플라이언스는 디바이스(106)를 프로그래밍하거나 프로비저닝 하는 데 사용되는 테스터(107)에 대한 보안 통신 채널을 또한 지닌다. 이 채널은 프로비저닝 데이터 및 로그 데이터가 제조 지역의 통신 네트워크 상에 유출되거나 변경되는 것을 방지한다. 분배기 어플라이언스(108)는 프로비저닝 데이터가 제3자(불량 테스터(107) 포함)에 의해 손상되거나 변경되지 않도록 프로그래밍 될 디바이스(106)와 직통으로 보안 통신 채널을 또한 수립한다.

[0093] 다양한 실시형태에서 분배기 어플라이언스는 공개 키 및 마이크로프로세서 시리얼 넘버와 같은 다른 데이터를 프로비저닝 될 디바이스(106)로부터 수집한다. 이 정보를 프로비저닝 제어기(120) 및/또는 DAMS(110)로 전송한다. 또한 디바이스(106)에 프로그래밍 하기 위하여 프로비저닝 제어기(120) 및/또는 DAMS(110)로부터 데이터, 명령어 및 기타 정보를 수신한다. 자신의 로그 데이터를 반송하고 테스터(107)로부터 프로비저닝 조절자(120) 및/또는 DAMS(110)로 데이터를 반송한다.

[0094] 디바이스 제조업체(105)와 관련하여 나타난 바와 같이 분배기 어플라이언스(108)는 테스터(107)(예를 들면 컴퓨터화 제조 장치, 제품 테스트 디바이스 등)에 통신 가능하게 연결되며 OBU 디바이스와 같은 제조업체(105)에 의해 생산된 디바이스(106a)를 차례로 연결한다. 제조업체(105)는 컴퓨터화 디바이스(106a)를 제조 및/또는 시장에 공급하는 공장을 포함하거나 공장일 수 있다.

[0095] 많은 가능한 실시예 중 하나로서 컴퓨터화 디바이스(106a)는 차량 내에 나중에 설치되는 차량탑재장치(OBU)의 일부로서 통합된 전화통신을 위한 셀룰러 모뎀에 사용되는 내장형 범용 집적 회로 카드(eUICC)일 수 있다. 이는 자동차와 교통 인프라 디바이스 간의 통신에 사용된다. 또한 다른 차량 및 도로변 장치(RSU)와의 통신을 위해 OBU에 설치된 V2V 보안 마이크로프로세서일 수도 있다. 이러한 새롭게 제조된 디바이스(106a)는 적절히 작동하기 위해 DAMS(110)로부터의 디지털 인증서와 같은 디지털 자산으로 적절하게 프로비저닝 되어야 한다.

[0096] 제조업체(105)의 스태프(109)는 사용자 포털(115)을 사용하여 프로비저닝 제어기(120)와 상호 작용하고 DAMS(110)에 의해 제품 프로비저닝 활동을 관리할 수 있다.

[0097] 설치자(130)와 관련하여 나타난 바와 같이 분배기 어플라이언스(131)는 대안적으로 디바이스(106b)가 작동 환경에 설치되는 동안 또는 이후에 디바이스(106b)에 직접 통신 가능하게 연결될 수 있다. 설치자(130)는 컴퓨터화 디바이스(106b)를 그들의 작동 환경에 설치하는(예를 들면 OBU를 자동차에 설치한다) 공장 또는 점포이거나 이들을 포함할 수 있다.

[0098]

[0099] 설치시에 컴퓨터화 디바이스(106b)는 적절하게 작동하기 위해 DAMS(110)로부터의 추가적인 디지털 인증서와 같은 디지털 자산이 적절하게 프로비저닝 되어야 한다. 설치자(130)의 스태프(132)는 설치자 사용자 포털(116)을 사용하여 프로비저닝 제어기(120)와 상호 작용하고 DAMS(110)에 의해 제품 프로비저닝 활동을 관리할 수 있다.

[0100] 다양한 실시형태에서 프로비저닝 제어기(120), 분배기 어플라이언스(108, 131 및 DAMS(110))는 그들 사이에 보안되고 비공개적으로 액세스 가능한 통신 링크 또는 채널을 지니며 다양한 실시형태에서 도 1에 나타난 모든 통신 연결은 안전하고 비공개적으로 액세스 가능한 통신 채널이어야 한다. 다양한 실시형태에서 이러한 보안 채널은 암호화되고 상호 인증되어 권한 없는 엔드 포인트가 이 보안 인프라 내에서 통신하지 못하게 한다.

[0101] 여러 보안 메커니즘을 사용하여 이러한 통신 채널을 보호할 수 있으므로 외부 계층이 손상되어도 내부 계층은 안전하게 유지된다. 예를 들어 상호 인증 TLS 터널은 전용 보안 통신 프로토콜과 같은 다른 프로토콜을 사용하여 내부 계층을 지닌 외부 계층으로 사용된다.

[0102] 시스템(100)을 포함하는 인프라 컴포넌트 사이의 이러한 보안 연결은 컴포넌트들 간의 민감한 통신을 보호하고 그들의 정확한 작동을 보장하는데 사용된다. 이러한 보안 경로를 사용하여 프로비저닝 제어기(120) 및 DAMS(110)는 전송 중에 손상되거나 변경될 염려없이 컴포넌트 간에 디지털 데이터를 전송한다. 명령 및 제어 정보 또한 이러한 채널을 통해 전달된다.

[0103] 예를 들면 프로비저닝 제어기(120)는 특정 디지털 자산 및 데이터가 전송되는 분배기 어플라이언스(108, 131)를 제어할 수 있다. 또한 프로비저닝 하고 있는 제조 라인 상의 디바이스(106)에 이러한 데이터를 미터 아웃(meter out)하는 것을 분배기 어플라이언스(108, 131)에 지시할 수도 있다.

[0104] 또한 분배기 어플라이언스(108, 131)는 정보가 전송 중에 손상되거나 변경될 것이라는 우려 없이 프로비저닝 제

어기(120)에 정보를 다시 리포트할 수 있다. 예를 들면 보안 프로비저닝 제어기(120)는 임의의 유형의 디지털 자산(예를 들면 인증서, 소프트웨어, 퓨즈 콘텐츠 등)으로 최대 10,000 개의 디바이스를 프로비저닝 하도록 분배기 어플라이언스(108, 131)를 프로그래밍할 수 있다. 분배기 어플라이언스(108, 131)는 프로비저닝 중인 디바이스를 카운트할 수 있으며 한계에 도달하면 프로비저닝 제어기(120)에 리포트 한다.

[0105] 다양한 실시형태에서 프로비저닝 제어기(120)에 의해 관리되는 디바이스(예를 들어 108, 110, 131, 115, 116, 117)는 프로비저닝 제어기(120)와 정기적으로 통신하지 않는 경우 작동을 중단하게 하는 기능을 포함하며 따라서 도난당한 경우 쓸모없게 된다. 이러한 기능은 분실/도난된 디바이스가 계속해서 작동하고 적절한 제조 환경에 있는 것처럼 디바이스(106)를 프로비저닝 하는 것을 방지한다.

[0106] 계속해서 도 1에 나타난 실시예를 참조하면 작동 중에 제조업체(105)에 위치한 분배기 어플라이언스(108)는 DAMS(110)로부터 디지털 자산을 보안 수신하고 이를 디바이스(106a)의 테스터(107)에 공급한다. 각각의 디바이스(106a)가 제조업체(105)에 의해 제조됨에 따라 테스터(107)는 디바이스(106a)와 통신하여 디바이스(106a)로부터 고유 식별 번호 및 상태와 같은 정보를 얻고 디지털 인증서와 같은 디지털 자산을 디바이스에 다운로드하거나 설치한다.

[0107] 또한 테스터(107)는 예를 들면 프로비저닝 상태와 같은 정보를 디바이스(106a)로부터 분배기 어플라이언스(108)로 제공할 수 있으며, 이는 그 정보를 DAMS(110) 및/또는 프로비저닝 제어기(120)에 안전하게 전달한다.

[0108] 일부 실시형태에서 테스터(107)는 분배기 어플라이언스(108)와 디바이스(106a) 사이에서 데이터를 안전하게 전송하는 소프트웨어 전송 계층 보안(TLS) 에이전트를 포함한다. 이는 각각의 디바이스(106a)와 관련된 임시 키를 사용하여 분배기 어플라이언스(108) 및 테스터(107)를 통해 DAMS(110)와 디바이스(106a) 사이에 보안 암호화 통신 경로를 생성한다.

[0109] 초기에 프로비저닝된 후 제조자(105)는 디바이스(106b)를 설치하는 설치자(130)에게 디바이스(106a)를 배송한다. 다양한 실시형태에서 초기 프로비저닝 전에 디바이스(106a)는 기능하지 않는다; 제조자(105)에 의한 초기 프로비저닝 후에 디바이스(106a)는 부분적으로 기능할 수 있으나 아직 완전히 기능하지는 않는다. 이러한 실시형태에서 초기 프로비저닝은 설치 및 완전히 작동하기 위해 요구되는 추가적인 최종 프로비저닝에 필요한 범위 까지만 디바이스가 기능하게 한다.

[0110] 설치자(130)는 디바이스(106b)를 작동 환경에 설치하고 설치자(130)의 스태프 멤버(132)는 설치자 포털(116)을 통해 그 사실을 프로비저닝 제어기(120)에 통지한다. 이 통지는 설치가 적절하게 완료되었음을 증명하며 디바이스(106b)를 고유하게 식별하는 정보를 프로비저닝 제어기(120)에 포함하는 것이 바람직하다.

[0111]

[0113] *일부 실시형태에서 분배기 어플라이언스(131)는 상태 및 식별 정보에 대해 디바이스(106b)에 질의한 후에 프로비저닝 제어기(120)에 자동으로 통보할 수 있다. 설치자(130)가 설치자 포털(116)을 통해 디바이스(106b)를 적절하게 설치했음을 증명하는 다양한 실시형태에서 이러한 증명(attestation)은 프로비저닝 제어기(120)에 의해 데이터베이스(125)에 기록/저장될 수 있다. 증명은 무선 송신 전력 측정 또는 GPS 안테나 위치의 검증과 같은 각각의 특정 설치된 디바이스(106b)에 관련된 특정 테스트 데이터를 포함할 수 있다.

[0114] 설치 통지에 응답하여 프로비저닝 제어기(120)는 (i) 디바이스(106b)가 제조업체(105)에 의해 합법적으로 제조된 디바이스로서 데이터베이스(125)에 등재되는지, (ii) 디바이스(106b)가 제조업체(105)에 의해 성공적으로 초기 프로비저닝된 것으로 데이터베이스(125)에 등재되는지, 및 (iii) 설치자(130)가 권한 있는 설치자로서 데이터베이스(125)에 등재되는지 여부를 검증한다.

[0115] 이 검증이 성공적이면 제어기(120)는 디지털 자산(예를 들면 가명 인증서 (PC)) 및/또는 디바이스(106b)를 작동 가능하게 프로비저닝 하는 데 필요한 기타 정보를 전송하도록 DAMS(110)에 지시하여 디바이스(106b)는 그 작동 환경 내에 설치된 대로 적절하게 기능할 수 있다.

[0116] 다양한 실시형태에서 조절자(140)는 조절자 포털(117)을 통해 프로비저닝 제어기(120)와 상호 작용하여 설치자(130) 및/또는 제조업체(105)를 식별, 확인 및 관리한다. 따라서 권한 없는 설치자(예를 들면 해커)가 시스템(100)으로부터 인증된 디지털 자산을 획득할 수 없게 한다. 조절자(140)의 스태프 멤버는 프로비저닝 제어기(120)에 의해 인증될 수 있으며 그들의 행동이 고유하게 기록될 수 있도록 시스템(100)에 고유한 ID를 지닌다.

[0117] 다양한 실시형태에서 조절자(140)는 프로비저닝 제어기(120)에 질의하여 증명 리포트, 설치자 행위, 제조된 디바이스(106a)의 수량 및 신원, 설치되고 완전히 프로비저닝된 디바이스(106b)의 수량 및 신원 등과 같은 제어기(120)에 의해 기록된 정보의 사본 및 리포트를 획득하기 위해 조절자 포털(117)을 사용할 수 있다.

[0118] 다양한 실시형태에서 설치자(130)는 시스템(100)과 상호 작용하기 위해 프로비저닝 제어기(120)에 의해 권한 있는 것으로 인증되어야 한다. 예를 들면 권한을 부여받기 위해 설치자(130)는 타겟 환경(예를 들면 타겟 차량 또는 사이트 등) 내에 디바이스(106b)를 적절하게 설치할 것임을 나타내는 적절한 계약 문서에 서명해야 한다.

[0119] 예를 들면 설치자(130)는 조절자(140)에 의해 다른 계약 요소를 증명하도록 요구될 수 있다. 바람직하게는 각각의 설치자(130)는 그들의 작업이 프로비저닝 제어기(120)에 의해 고유하게 기록될 수 있도록 시스템(100) 내에 고유 ID를 지닌다.

[0120] 시스템(100)의 개시된 실시형태 및 그의 기능은 제조업체(105)에 의해 제조되고 권한 있는 설치자(130)에 의해 적절하게 설치 및 테스트된 디바이스(106) 만이 디바이스(106)를 작동시키기 위해 필요한 디지털 자산으로 완전히 프로비저닝 되는 것을 보장한다.

[0121] 프로비저닝 제어기(120)는 프로비저닝 프로세스의 각 단계에서 누군가의 의한 행동에 대한 광범위한 로그 및 리포트를 생성하여 기존 시스템에는 존재하지 않았던 중요한 감사 기능을 제공한다.

[0122]

[0123] 당업자는 도 1에 나타난 컴포넌트, 프로세스, 데이터, 작동 및 실시형태 세부 사항이 설명의 간결성과 명확성을 위해 제공된 실시예 임을 인식할 것이다. 이러한 실시예는 한정하려는 의도가 아니며 다양한 변형이 가능하기 때문에 본 발명의 원리를 벗어나지 않고 다른 컴포넌트, 프로세스, 실시형태 세부 사항 및 변형이 수행될 수 있다.

[0124] 예를 들어 단 하나의 제조자(105), 단 하나의 설치자(130) 및 단 하나의 조절자(140)만이 도 1에 도시되어 있으나 다른 실시형태는 이들 엔티티는 임의의 수를 지닐 수 있다. 다른 실시예로서 DAMS(110) 및 프로비저닝 제어기(120)가 별개의 디바이스로 도시되어 있으나 다른 실시형태에서 그 기능을 단일 디바이스 및 예를 들면 단일 서버로 결합할 수 있다.

[0125] 또 다른 실시예로서 포털(115-117)에 대해서도 동일하게 수행될 수 있다. 또 다른 실시예로서 2016년 11월 14일자로 출원되고 참고문헌으로 통합된 미국 잠정출원 제62/421,852호에 기술된 바와 같이 시스템(100)은 자산 관리 어플라이언스(AMA, 도시되지 않음)를 추가로 포함할 수 있다.

[0126] 이러한 실시형태에서 AMA는 프로비저닝 제어기(120) 및/또는 분배기 어플라이언스(108, 131) 및/또는 DAMS(110)에 통신 가능하게 연결될 수 있다. 다양한 실시형태에서 AMA는 생산 코디네이터가 제품(예를 들면 디바이스(106)) 변형과 구축을 쉽고 효율적으로 관리할 수 있게 하는 사용자 친화적 GUI 및 기능을 포함할 수 있다. 이를 통해 자산 소유자가 디지털 자산의 재고를 쉽고 효율적으로 관리할 수 있게 한다.

[0127] 도 2는 본 발명의 실시형태와 일치하는 컴퓨터화 디바이스를 안전하게 프로비저닝하기 위한 프로세스(200)의 실시예를 나타낸 스윔 레인 다이어그램이다. 다양한 실시형태에서 프로세스(200) 또는 작동의 일부 또는 전부는 범용 컴퓨터 시스템(하나 이상의 프로세서 또는 하나 이상의 컴퓨터 서브 시스템을 포함할 수 있음), 하드웨어 전용 시스템 또는 이들의 혼성화 시스템 상에서 실행되는 코드에 의해 수행될 수 있다.

[0128] 도 2의 상부에 나타난 바와 같이 프로세스(200)와 관련된 엔티티는 컴퓨터화 디바이스(106)의 제조업체(105), 제조업체(105)에 위치한 분배기 어플라이언스(108), 프로비저닝 제어기(120) 및 DAMS(110)를 포함한다. 다양한 실시형태에서 도 1과 관련되고 본 명세서 전체에 걸쳐 개시된 바와 같이 이들 엔티티는 서로 존재하고 통신한다.

[0129] 도 2의 실시예에 나타난 바와 같이 프로세스(200)는 프로비저닝 제어기(130)로부터 디지털 자산 프로비저닝 서비스를 요청하는 제조업체(105)(예를 들면 스태프 멤버(109))와 함께 단계 205에서 시작한다. 여기서 디지털 자산은 디바이스(106a)에 (예를 들면 사용되기 위해) 프로비저닝 되고 요청은 디지털 자산의 목적지인 디바이스(106a)를 식별할 수 있다. 요청은 예를 들면 신규 제품(106A)을 위한 프로비저닝 서비스를 요청하거나 기존 제품(106B)을 위한 신규 프로비저닝 서비스를 생성하는 제조자(105)일 수 있다.

[0130] 다양한 실시형태에서 이러한 작동은 예를 들면 사용자 포털(115)을 통해 프로비저닝 제어기(130)에 로그인하는 권한 있는 사용자를 포함할 수 있다. 일부 경우에 요청된 디지털 자산은 등재 인증서; 디바이스(106)를 작동시

킬 실행 가능 코드; 디지털 작동 파라미터; 등과 같은 보안 크리덴셜일 수 있다.

[0131] 등재 인증서는 모든 참가자가 유효한 등재 인증서를 공유해야 하는 생태계 내의 인증된 참가자로서 해당 소유자를 식별하는 공개키 인증서이다(예를 들면 USDOT의 V2X 생태계). 또한 권한 있는 참가자는 생태계 내의 디바이스(106)의 통신 및 작동을 가능하게 하는(예를 들면 USDOT의 V2X 생태계의 실시예에서 차량과 도로변 인프라 사이의 통신 및 작동을 가능하게 하는) 가명 인증서를 또한 수신할 수 있다.

[0132] 단계 210에서 프로비저닝 제어기(120)는 제조자(109)로부터의 사용자가 권한 있는 사용자인지 여부를 결정한다. 일부 실시형태에서 프로비저닝 제어기(120)는 프로비저닝 될 디바이스(106a)(예를 들면 제품)가 시스템(100)과 함께 사용하도록 승인되었는지 여부 또한 단계 210에서 결정한다. 특정 경우에서 승인된 디바이스의 목록은 도 1의 조절자에 의해 제공되고 이러한 결정을 내리기 위해 프로비저닝 제어기(120)에 의해 사용된다.

[0133] 사용자(및/또는 제품)가 권한을 지니지 않으면 프로비저닝 제어기(120)는 디지털 자산 프로비저닝 서비스에 대한 요청을 거부한다(도 2에 나타내지 않음). 한편 권한 있는 사용자가 (예를 들어 인증된 제품에 대해) 요청을 하는 경우(단계 210이 '예'인 경우), 예를 들면 DAMS(110)로 서비스 요청 명령을 전송함으로써(단계 215에서) 프로비저닝 제어기(120)는 DAMS(110)가 서비스 요청을 수행하도록 지시, 명령 또는 제어한다.

[0134] 단계 220에서 단계 215로부터의 요청을 수신함에 따라 DAMS(110)는 요청에 기초하여 디바이스(106a)에 서비스를 시작하도록 스스로를 형상화시킨다. 일부 실시형태에서 DAMS(110)는 분배기 어플라이언스(108)에 명령을 전송하여 분배기 어플라이언스(108)가 디바이스(106a)를 서비스하도록 형상화시킬 수 있다.

[0135] 단계 222에서 DAMS(110)는 단계 205에서 요청된 바와 같이 디바이스(106a)를 위한 디지털 자산을 생산, 생성, 계산 및/또는 검색한다. 다양한 실시형태에서 DAMS(110)는 공개 및 개인 키 쌍, 디바이스(106a)에 대한 등재 인증서 및 가명 인증서와 같은 요청된 디지털 보안 자산을 생산 또는 생성한다.

[0136] 작동 222의 대안적인 실시형태(도 2에 나타나지 않음)에서 DAMS(110)는 분배기 어플라이언스(108)로부터 디바이스(106a)와 관련된 디지털 자산 생성 정보를 요구하고 수신한다. 이러한 정보는 디바이스(106a)에 의해 생성되고 검색된 등재 및 가명 공개 키 및 디바이스(106a)를 고유하게 식별하는 데이터(예를 들면 마이크로프로세서 시리얼 넘버)를 포함한다. 이러한 실시형태에서 DAMS(110)는 등재 및 가명 공개 키를 사용하여 예를 들면 디바이스(106a)에 대한 등재 인증서 및 적절한 수의 가명 인증서와 같은 디지털 자산을 생성한다.

[0137] 단계 225에서 DAMS(110)는 단계 205에서 디지털 자산 서비스를 요청한 제조업체(105)의 분배기 어플라이언스(108)로 디지털 자산을 전송한다. 예를 들어 DAMS(110)는 공개 및 개인 키 쌍, 등재 인증서 및 가명 인증서를 제조자(105)의 분배기 어플라이언스(108)에 보안 전송한다.

[0138] 단계 226에서 DAMS(110)는 디지털 자산에 관한 로그 정보를 프로비저닝 제어기(120)에 전송한다. 다양한 실시형태에서 로그 정보는 요청자의 ID, 디지털 자산 ID, 분배기 어플라이언스 ID, 요청 및 전송 작업의 타임스탬프, 수신된 마이크로프로세서 시리얼 넘버와 같은 디지털 자산의 요청 및 전송을 설명하는 정보를 포함할 수 있다.

[0139] 일부 실시형태에서 로그 정보는 디지털 자산의 사본을 포함할 수 있다. 단계 227에서 프로비저닝 제어기(120)는 예를 들면 데이터베이스(125)에 로그 정보를 수신하여 저장한다. 프로비저닝 제어기(120)는 실제로 시스템(100)에서 발생하는 모든 활동의 감사 추적을 유지하며 이는 디바이스(106a)가 제조업체(105)에 의해 어떻게 구축되고 제공될 수 있는지에 관한 데이터와 같은 다양한 유형의 데이터를 수집할 수 있다. 이러한 데이터 및 로그 정보는 감사 목적 뿐만 아니라 비용 청구에 사용될 수 있다.

[0140] 단계 230에서 분배기 어플라이언스(108)는 DAMS(110)에 의해 전송된 디지털 자산(예를 들면 공개키 및 개인키 쌍, 등재 인증서 및 가명 인증서)을 수신하여 저장한다.

[0141] 단계 235에서 분배기 어플라이언스(108)는 분배기 어플라이언스(108)로부터 디바이스(106a)로 디지털 자산을 보안 전송하는데 사용될 수 있는 공개 키와 같은 디지털 보안 자산을 디바이스(106a)에 요청하고 수신한다. 다양한 유형의 디바이스(106a)는 아마도 디바이스(106)에 내장된 보안 프로세서를 사용하여 임시 키 쌍을 생성하는 능력을 지니며 공개 키는 임시 키 쌍의 일부일 수 있다.

[0142] 단계 240에서 분배기 어플라이언스(108)는 디지털 자산(예를 들어 등재 인증서)을 디바이스(106a)로 보안 전송하기 위해 디지털 보안 자산(예를 들어 공개 키)을 사용한다. 다양한 실시형태에서 분배기 어플라이언스(108)는 예를 들어 디바이스(106a)와의 가상 사설 네트워크(VPN)을 형성하기 위해 디바이스(106a)의 공개키를 사용할 수 있고 그 안의 디지털 자산을 보안 전송할 수 있다.

[0143] 다양한 실시형태에서 분배기 어플라이언스(108)는 디바이스(106a)에 접속될 수 있는 테스터(107)와의 통신을 보안하기 위해 테스터(107) 사이에 전송 계층 보안(TLS)을 사용할 수 있다. 디바이스(106a)에 직접적으로 보안 통신 하는 것이 바람직한 실시형태에서 시스템은 디바이스(106a) 상에 일시적인 공개 키 쌍을 생성할 수 있으며 분배기 어플라이언스(108)의 공개 키를 포함하는 분배기 어플라이언스(108)로부터의 인증서 및 공개 키를 사용하여 디바이스(106a)에 대한 보안 터널을 생성한다.

[0144] 이러한 실시형태에서 디바이스(106a)는 분배기 어플라이언스(108)가 그것에 전송하는 인증서를 검증하기 위해 시스템(100)의 루트 공개 키와 함께 특수 코드를 실행시킨다.

[0145] 디바이스(106a) 또는 테스터(107)와 분배기 어플라이언스(108) 사이에 보안 경로가 설정되면, 디바이스(106a)는 등재 및 가명 공개 키 쌍(예를 들어 V2X 생태계에 대한)을 생성하고 분배기 어플라이언스(108)로 공개 키 및 다른 데이터를 전송할 수 있으며 분배기 어플라이언스(108)는 이 데이터를 DAMS(110) 및 프로비저닝 제어기(120)로 전송할 수 있다.

[0146] 작동 222의 대안적인 실시형태에 관해 전술한 바와 같이 DAMS(110)는 수신 된 공개 키를 사용하여 등재 인증서 및 가명 인증서를 생성할 수 있다. 일부 실시형태에서 많은 수(예를 들어 3,000)의 가명 인증서가 존재할 수 있다.

[0147] 이러한 실시형태의 대안적인 실시예에서 DAMS(110)는 전술한 바와 같이 작동 225에서 이들 인증서를 분배기 어플라이언스(108)로 반송할 것이다. 일부 다른 실시형태에서 DAMS(110)는 프로비저닝이 수행되는 장소에 따라 분배기 어플라이언스(108) 대신에 분배기 어플라이언스(131)로 이들 인증서를 전송할 수 있다.

[0148] 일부 실시형태에서 분배기 어플라이언스(108)는 예를 들면 디바이스(106)가 자체의 무선 또는 유선 통신 기능을 지니며 적어도 부분적으로 작동하는 경우 디바이스(106)와 직접 통신할 수 있다. 다른 실시형태에서 분배기 어플라이언스(108)는 테스터(107)와 같은 중간 디바이스를 통해 디바이스(106)와 간접적으로 통신할 수 있다.

[0149] 디바이스(106a)는 디지털 자산을 수신하고 작동 중에 사용하기 위해 저장한다. 예를 들어 디바이스(106a)가 차량 탑재 장치(OBU) 또는 전자 제어 디바이스(ECU)이고 디지털 자산이 무선 네트워크에 연결하는 데 필요한 보안 자산(예를 들면 공개 키 인증서) 인 경우, 디지털 보안 자산은 OBU에 의해 저장된다.

[0150] OBU가 차량에 설치되고 활성화되면 무선 네트워크에 연결을 시도한다. 네트워크가 OBU를 네트워크에 연결되도록 허용하기 전에 OBU 인증을 시도한다. OBU는 제조업체(105)에서 분배기 어플라이언스(108)에 의해 제공되는 디지털 보안 자산을 지니는 경우에만 네트워크를 인증하고 연결할 수 있다.

[0151] 단계 245에서 분배기 어플라이언스(108)는 디바이스(106a)가 단계 240에서 전송된 디지털 자산을 성공적으로 수신 및 설치(예를 들어 저장)하였는지 여부를 나타내는 상태 정보를 디바이스(106a)로부터 수신 또는 접속한다.

[0152] 단계 250에서 분배기 어플라이언스(108)는 상태 정보를 프로비저닝 제어기(120)로 전송한다. 또한 단계 255에서 프로비저닝 제어기(120)는 단계 227에서 저장된 로그 정보와 관련된 상태 정보를 수신하고 저장한다. 따라서 프로비저닝 제어기(120)는 각각의 특정 디바이스(106)와 관련된 모든 시스템(100) 활동에 대한 감사 추적 또는 감사 로그를 계속한다.

[0153] 다양한 실시형태에서 감사 로그는 각각의 디바이스(106)에 대해 제조업체의 프로비저닝 성공 또는 실패(예를 들면 작동 235-245); 디지털 자산의 확인(및/또는 디지털 자산 자체의 복제); 암호화 유형; 등을 나타내는 정보를 포함한다.

[0154] 단계 270에서 디바이스(106a)가 디지털 자산으로 성공적으로 프로비저닝 된 경우, 제조업체(105)는 디바이스를 시장에 출시한다. 예를 들어 제조업체(105)는 디바이스(106a)를 그 작동 환경에 설치하는 회사(예를 들면 도 1의 설치자 회사(130))에 물리적으로 운송할 수 있다.

[0155] 일부 실시형태에서 디바이스(106a)는 이 시점에서 완전히 프로그래밍되거나 프로비저닝 될 수 있으며 완전한 기능으로 작동할 수 있다. 다른 실시형태에서 디바이스(106a)는 이 시점에서 부분적으로만 프로그래밍되거나 프로비저닝 될 수 있으며 완전한 기능으로 작동할 수 없거나 비기능적이다.

[0156] 도 2에 나타난 실시예는 단지 발명의 상세한 설명을 위한 것이며 범위를 한정하려는 것은 아니다. 또한 도시된 프로세스(200)는 특정 개시된 특정 실시형태와 일치하는 일부 신규하고 혁신적인 특징 설명의 명료성을 위해 다소 간략화된 실시예이지만 이러한 실시예로 한정하려는 의도가 아니며 다양한 변형이 가능하다.

[0157] 예를 들면 기능 및 작동이 특정 순서로 수행되는 것으로 나타났으나 개시된 순서는 단지 하나의 실시예이며 소

정의 개시된 실시형태와 일치하는 다양하고 상이한 작동 순서가 가능하다.

[0158] 또한 작동은 단지 발명의 상세한 설명을 위해 별개의 단계로 설명되며 일부 실시형태에서는 다수의 작동이 동시에 및/또는 단일 연산 또는 더 큰 작동의 일부로서 수행될 수 있다. 개시된 작동은 완전하거나 한정적이거나 절대적인 것은 아니며 다양한 작동을 수정, 삽입 또는 삭제할 수 있다.

[0159] 변형의 실시예로서 도 2는 단일 디지털 자산(예를 들면 단일 디지털 인증서)의 맥락에서 일반적으로 설명하였으나 시스템 및 프로세스는 다수의 디지털 자산(예를 들면 2 이상의 디지털 인증서)을 처리하는 것과 유사하게 기능할 것이다. 또 다른 실시예로서 디바이스(106a)가 보안 통신 능력을 지니지 않는 경우 작동(235 및 240)을 삭제할 수 있고 분배기 어플라이언스(108)는 암호화되지 않은 통신을 사용하여 디바이스(106b)와 통신할 수 있다.

[0160] 또 다른 실시예에 있어서 다양한 실시형태에서 프로비저닝 제어기(120) 또는 특수 서명 어플라이언스와 같은 위임된 권한은 분배기 어플라이언스(108)에 유사하게 전송하고 소프트웨어, 펌웨어, 퓨즈 블롭, 매니페스트 파일 등과 같은 디지털 자산을 포함하는 또 다른 또는 추가적인 디지털 자산을 디바이스(106b)에 로딩시킬 수 있다. 이와 같은 실시형태에서 프로비저닝 제어기(120)는 저장장치로부터 요구된 디지털 자산을 추가적 또는 대안적으로 검색, 획득, 접속 또는 접속의 지시를 한다.

[0161] 예를 들어(도 2에 나타내지 않음) 프로비저닝 제어기(120) 또는 그의 권한 있는 위임자는 디바이스(106a)에 로딩되어 디바이스에 의해 실행되는 실행 가능한 소프트웨어 이미지(예를 들면 데이터베이스(125)에 저장된 컴파일된 컴퓨터 프로그램)를 검색할 수 있다. 또한 실행 가능한 소프트웨어 이미지를 디바이스에 프로그래밍하기 위해 분배기 어플라이언스(10)에 전송한다.

[0162] 다양한 실시형태에서 프로비저닝 제어기(120)에 의해 접속되는 디지털 자산은 허가되지 않은 소프트웨어가 로딩될 수 없도록 디바이스(106a)의 제조업체(105)에 의해 보안 하에 공급, 배포 및/또는 인증된 소프트웨어 등으로만 구성된다. 일부 실시형태에서 프로비저닝 제어기(120)에 의해 검색된 디지털 자산은 도 1의 데이터베이스(125)와 같은 프로비저닝 제어기(120)와 연관된 저장장치 또는 데이터베이스에 저장될 수 있다.

[0163] 도 3은 본 발명의 실시형태와 일치하는 컴퓨터화 디바이스를 보안하에 프로비저닝 하기 위한 프로세스(200)의 실시예를 나타내는 스윔 레인 다이어그램이다. 다양한 실시형태에서 프로세스(300) 또는 도시된 작동 중 일부 또는 전부는 범용 컴퓨터 시스템(하나 이상의 프로세서 또는 하나 이상의 컴퓨터 서브 시스템을 포함할 수 있음) 상에서 실행되는 코드 또는 하드웨어-단독 시스템 또는 이들의 혼성화 시스템에 의해 수행될 수 있다.

[0164] 도 3의 상부에 나타난 바와 같이 프로세스(300)와 관련된 엔티티는 컴퓨터화 디바이스(106)의 설치자(130), 설치자(130)에 위치한 분배기 어플라이언스(131), 프로비저닝 제어기(120) 및 DAMS(110)를 포함한다. 다양한 실시형태에서 도 1과 관련되고 본 명세서 전체에 걸쳐 개시된 바와 같이 이들 엔티티는 서로 존재하고 통신한다.

[0165] 도 3의 실시예에 나타난 바와 같이 프로세스(300)는 제조업체(105)에 의해 제조 및 출시되거나 출하된(예를 들어 도 2의 작동 270 참조) 디바이스(106b)(예를 들어 OBU 또는 ECU)를 설치자(130)가 수신하는 단계 305에서 시작한다. 단계 310에서 설치자(130)는 더 큰 시스템과 같은 작동 환경에 디바이스(106b)를 설치한다.

[0166] 예를 들면 설치자(130)는 제조사(105)로부터 OBU를 구매하는 자동차 제조사일 수 있으며 설치자(130)는 OBU를 자동차에 설치할 수 있다. 다양한 실시형태에서 디바이스(106b)를 설치하는 것은 설치 후에 디바이스(106b)의 작동, 기능 등을 테스트하고 관련된 상태 데이터를 수집하는 것을 포함할 수 있다.

[0167] 일부 실시형태에서 디바이스(106b)는 단지 부분적으로 프로비저닝 되어 완전히 기능하지 않을 수 있다. 예를 들면 디바이스(106b)의 제조업체(105)는 등재 인증서만으로 디바이스(106b)를 프로비저닝 함으로써 디바이스(106b)는 다른 완전히 프로그래밍된 디바이스(106)와 통신하는 기능과 같은 완전한 기능을 획득하기 위해 가명 인증서와 같은 다른 디지털 인증서로 더욱 프로비저닝 되어야 한다.

[0168] 단계 315에서 설치자(130)(예를 들어 스태프 멤버(132))는 설치 상태 데이터를 프로비저닝 제어기(120)에 전송한다. 다양한 실시형태에서 설치 상태 데이터는 예를 들면 시리얼 넘버 또는 한 번 생성되면 결코 지워지지 않는 키 쌍 내의 공개 키와 같은 고정적이고 고유하게 식별되는 정보와 같은 설치된 디바이스의 불변(immutable) 식별자를 포함한다.

[0169] 설치 상태 데이터는 설치자(130)의 고유 식별자, 디바이스(106b)가 설치된 방법 및 시기를 나타내는 정보, 설치된 디바이스(106b)에서 수행된 테스트 결과에 대한 정보, 설치자(130)가 적용 가능한 사양, 계약 요건 및/또는 지침에 따라 디바이스(106b)를 설치하였음을 증명하는 정보 및 다른 유사한 정보를 또한 포함할 수 있다.

[0170] 단계 320에서 프로비저닝 제어기(120)는 설치자(130)로부터 사용자가 권한 있는 사용자인지 여부를 결정한다. 그렇지 않은 경우 프로비저닝 제어기(120)는 설치 상태 통신을 거부한다(도 3에 나타내지 않음). 한편 권한 있는 사용자가 요청을 하는 경우(단계 320이 '예') 프로비저닝 제어기(120)는 설치 상태 데이터 내에서 식별된 디바이스(106b)가 권한 있는 디바이스인지 여부를 결정한다(단계 325).

[0171] 일부 실시형태에서 프로비저닝 제어기(120)는 데이터베이스(125)에 이전에 저장된 정보에 대해 검증함으로써 디바이스(106b)가 권한 있는지를 결정한다. 1) 데이터베이스(125) 내에 디바이스(106b)에 대한 기록이 존재하는지; 2) 디바이스(106b)가 제조자(105)에서 성공적으로 프로비저닝 되었음을 기록이 나타내는지; 3) 디바이스(106b)가 단계 320에서 권한 있는 설치자로서 입증된 설치자(130)에게 송부되었음을 기록이 나타내는지; 를 검증한다.

[0172] 설치 상태 데이터 내에서 식별된 디바이스가 권한이 없으면 프로비저닝 제어기(120)는 설치 상태 통신을 거부한다(도 3에 나타내지 않음). 한편 설치 상태 데이터에서 식별된 디바이스(106b)가 권한이 있으면(단계 325가 '예') 프로비저닝 제어기(120)는 단계 330에서 디바이스(106b)와 관련된 로그 정보와 함께 설치 상태 데이터를 저장한다. 예를 들면 디바이스(106b)와 관련된 로그 정보는 도 2의 단계 227의 측면에서 설명된 바와 같이 데이터베이스(125)에 이미 저장된 것일 수 있다.

[0173] 단계 335에서 프로비저닝 제어기(120)는 예를 들면 설치자(130)가 지닌 디바이스(106b)를 프로비저닝 하라는 요청을 DAMS(110)에 전송함으로써 프로비저닝 요청을 수행하도록 DAMS(110)를 지시, 명령 또는 제어한다. 단계 340에서 단계 335로부터 요청을 수신하는 조건에 따라 DAMS(110)는 단계 335에서 요청된 디지털 자산을 생성 및/또는 검색한다.

[0174] 다양한 실시형태에서 DAMS(110)는 도 2와 관련하여 설명된 바와 같이 가명 인증서 또는 다른 공개 키 인증서와 같은 요청된 디지털 자산을 생산하거나 생성할 수 있다. 다양한 실시형태에서 DAMS(110) 또는 DAM(110) 대신에 프로비저닝 제어기(120)는 저장장치로부터 요청된 디지털 정보를 추가적으로 또는 선택적으로 검색, 획득 또는 접속한다. 정보는 디바이스(106b) 유형의 디바이스 내에서 사용하기 위해 데이터베이스(125) 내에 이미 저장된 실행 가능한 이미지와 같다.

[0175] 단계 345에서 DAMS(110)는 단계 315에서 설치 상태를 전송한 설치자(130)의 분배기 어플라이언스(131)로 디지털 자산을 전송한다. 예를 들어, DAMS(110)는 설치자(130)의 분배기 어플라이언스(131)로 가명 인증서를 보안 전송할 수 있다.

[0176] 단계 350에서 분배기 어플라이언스(131)는 도 2와 관련하여 설명된 바와 같이 작동 230-245와 동일하거나 유사한 작동을 수행한다. 단계 355에서 분배기 어플라이언스(131)는 상태 정보를 프로비저닝 제어기(120)로 전송한다. 또한 단계 360에서 프로비저닝 제어기(120)는 작동 227에서 저장된 상태 정보와 같은 디바이스(106b)와 관련하여 이전에 저장된 상태 정보를 수신하고 저장한다. 따라서 프로비저닝 제어기(120)는 각각의 특정 디바이스(106)와 관련된 모든 시스템(100) 작업에 대한 감사 추적 또는 감사 로그를 계속한다.

[0177]

[0178] 도 3에 도시된 프로세스(300)는 발명의 상세한 설명을 위한 실시예이며 그 범위를 한정하려는 것은 아니다. 또한 도시된 프로세스(300)는 개시된 특정 실시형태와 일치하는 특정 신규하고 혁신적인 특징 설명의 명료성을 위해 다소 간략화된 실시예이지만 다양한 변형이 가능하다. 예를 들면 기능 및 작동이 특정 순서로 수행되는 것으로 나타났으나 개시된 순서는 단지 하나의 실시예이며 소정의 개시된 실시형태와 일치하는 다양하고 상이한 작동 순서가 가능하다.

[0179] 또한 작동은 단지 발명의 상세한 설명을 위해 별개의 단계로 설명되며 일부 실시형태에서는 다수의 작동이 동시에 및/또는 단일 연산 또는 더 큰 작동의 일부로서 수행될 수 있다. 개시된 작동은 완전하거나 제한적이거나 절대적인 것은 아니며 다양한 작동을 수정, 삽입 또는 삭제할 수 있다.

[0180] 도 4a 및 4b는 함께 본 발명의 실시형태에 따라 확장 가능하고 보안된 인증서 관리 시스템(CMS)(400)을 구현하기 위한 예시적인 아키텍처의 블록도이다. 확장 가능한 CMS(400)의 다양한 실시형태는 매우 대용량의 디바이스 트랜잭션 및 인증서 생성 프로세스에 사용될 수 있다. 다양한 실시형태에서 확장 가능한 CMS(400)는 다수의 서버, 하드웨어 보안 모듈(HSM), 다수의 컴퓨터 또는 컴퓨터 엔진 및 다수의 응용프로그램 플랫폼을 사용하여 구현될 수 있다. 도 4a 및 4b에 나타난 예시적인 실시형태에서 응용프로그램 플랫폼은 각각 하나 이상의 가상 머신(VM)을 포함할 수 있다.

[0181] 추가적 또는 대안적인 실시형태에서 응용프로그램 플랫폼은 각각 예를 들어 응용프로그램 서버, 컴퓨터 또는 소프트웨어 응용프로그램을 호스팅하고 실행할 수 있는 다른 컴퓨터 하드웨어와 같은 하나 이상의 하드웨어 플랫폼을 포함할 수 있다.

[0182] 도 4a및 4b의 실시예에서 등재 인증 권한을 위한 응용프로그램 플랫폼(430)은 등재 인증 권한 응용프로그램을 실행하는 하나 이상의 VM일 수 있으며, 가명 인증 권한을 위한 응용프로그램 플랫폼(440)은 가명 인증 권한 응용프로그램을 호스팅하고 실행할 수 있는 하나 이상의 VM일 수 있다.

[0183] 유사하게 연결 권한 1에 대한 응용프로그램 플랫폼(450)은 연결 권한 1 응용프로그램을 호스팅하고 실행할 수 있도록 형상화된 하나 이상의 VM일 수 있으며, 연결 권한 2에 대한 응용프로그램 플랫폼(460)은 연결 권한 2 응용프로그램을 호스팅하고 실행할 수 있는 하나 이상의 VM일 수 있다. 확장 가능한 CMS(400)의 실시예는 사설 데이터 센터, Amazon의 아마존 웹 서비스(AWS)와 같은 클라우드 데이터 센터 또는 사설 및 클라우드 데이터 센터의 하이브리드에서 구현될 수 있다.

[0184] 일부 실시형태에서 확장 가능한 CMS(400)는 예를 들어 등재 인증서 및 가명 인증서와 같은 보안 인증서를 제조업체(105)의 분배기 어플라이언스(108)에 의해 사용되도록 제공할 수 있으며, 이는 도 1 및 본 명세서의 다른 부분에 개시된 바와 같이 기능할 수 있다. 특정 실시형태에서 확장 가능한 CMS(400)는 분배기 어플라이언스(108)에 인증서를 제공하기 위해 도 1과 관련하여 상기에 개시된 디지털 자산 관리 시스템(DAMS)(110)과 상호작용할 수 있다.

[0185] 도 4a의 실시예에 나타난 바와 같이 CMS(400)의 아키텍처는 개별 서버 내에서 바람직하게 구현되는 프라이머리 및 예비의 2 개 프로비저닝 제어기(120)를 포함할 수 있다. 2개의 프로비저닝 제어기(120)는 프라이머리 프로비저닝 제어기 내에 포함 된 객체, 데이터 등이 예비(세컨더리) 프로비저닝 제어기에 복사되거나 포함되는 기능을 포함한다.

[0186] 프라이머리 프로비저닝 제어기가 어떠한 이유로 오프라인 상태가 되면 예비 프로비저닝 제어기가 온라인 상태로 되어 프라이머리 프로비저닝 제어기를 대체할 수 있다. 이것은 프로비저닝 제어기(120)의 연속적 (또는 매우 높은) 이용 가능성을 제공한다. 다양한 실시형태에서 프라이머리 및 예비 프로비저닝 제어기는 도 1 및 본 명세서의 다른 부분에서 개시된 바와 같다.

[0187] 다양한 실시형태에서 프로비저닝 제어기(120)는 도 1의 프로비저닝 제어기(120)와 제조업체의 분배기 어플라이언스(108) 사이의 연결 및 통신과 관련하여 본 명세서에서 설명된 것과 동일하거나 유사한 방식으로 확장 가능한 CMS(400)에 접속할 수 있다. 일반적으로 프로비저닝 제어기(120)는 인프라 구조를 포함하는 시스템 엘레멘트를 관리하여 명시적으로 권한 있는 엘레멘트 만이 확장 가능한 CMS(400)에 참여하고 상호작용할 수 있다.

[0188] 다양한 실시형태에서 프로비저닝 제어기(120)는 사용자(예를 들면 제조업체(105) 또는 설치자(130))의 스태프 식별 및 인증 시스템을 통합하거나 권한 있는 사용자만이 확장 가능한 CMS(400)를 사용할 수 있도록 식별 및 인증을 위한 자체 기능을 제공할 수 있다.

[0189] 일부 실시형태에서 프로비저닝 제어기(120)는 예를 들면 프라이머리 및 예비 DLM 제어기와 같은 디바이스 수명주기 관리(DLM) 제어기일 수 있다. 다양한 실시형태에서 프로비저닝 제어기(120)는 컴포넌트 유형별로 CMS(400) 내에 존재하는 제어기일 수 있다. 예를 들어 도 4a 및 4b에서 프로비저닝 제어기(120)는 등록 권한(420), 등재 인증 권한(430), 가명 인증 권한(440) 및 연결 권한(450, 460)을 위해 존재하는 제어기의 세트 또는 쌍일 수 있다.

[0190] 도 4a 및 4b에 나타난 바와 같이 확장 가능한 CMS(400)의 아키텍처는 표현 상태 변경(REST) 웹 서비스로 구현된 등록 권한(405), 등록 권한(420), 등록 권한 컴퓨터 엔진(425), 등재 인증 권한(430), 등재 인증 권한 컴퓨터 엔진(435), 가명 인증 권한(440), 가명 인증 권한 컴퓨터 엔진(445), 연결 권한 1(450), 연결 권한 1 컴퓨터 엔진(455), 연결 권한 2(460), 연결 권한 2 컴퓨터 엔진(465), 메시지 큐(410, 411, 412, 413, 414, 415, 416, 417, 418, 419) 및 하나 이상의 데이터베이스(470)를 포함한다. 이러한 컴포넌트 각각은 다음 단락에서 설명된다.

[0191] 확장 가능한 CMS(400)의 아키텍처는 보안 기능으로부터 비-보안-관련 응용프로그램을 분리시킨다. 도 4a 및 4b의 실시예에 나타난 바와 같이 등록 권한(420), 등재 인증 권한(430), 가명 인증 권한(440) 및 연결 권한(450, 460)은 그들 자신의 전용 컴퓨터 엔진(425, 435, 445, 455, 465) 상에서 실행되는 VM 상에서 응용프로그램으로서 구동된다. 이들 전부는 비-보안-관련 응용프로그램 및 기능으로부터 분리되어 있다.

[0192] 이는 HSM의 성능이 느리거나 클라우드 서비스 제공 업체가 HSM을 공급할 수 없거나 HSM의 적절한 관리가 불확실한 기존 시스템에 비해 기술적 및 보안적 이점과 개선을 제공한다. 확장 가능한 CMS(400)에서 HSM이 필요로 하는 모든 암호화 작동은 컴퓨터 엔진(예를 들면 하나 이상의 컴퓨터 엔진 425, 435, 445, 455 및 465)에서 수행된다.

[0193] 도 4a 및 4b에 나타난 바와 같이 중요한 보안 기능을 서로 별도의 컴퓨터 엔진으로 분리함으로써 예를 들면 등록 권한(420), 등재 인증 권한(430), 가명 인증 권한(440) 및 연결 권한(450, 460)에 의해 수행되는 바와 같이 연산-집약적인 암호화 및 보안 기능(예를 들면 타원 곡선 버터플라이 확장 연산 또는 타원 곡선 디지털 서명)을 기존 등록 권한 시스템에 비해 유의미하게 빨리 수행할 수 있다.

[0194] 이러한 디자인은 "병목 현상" 응용프로그램을 필요에 따라 개별적으로 확장할 수 있도록 하여 트랜잭션 처리를 크게 향상시킨다. 이와 같이 본 명세서와 일치하는 실시형태는 기존 등록 권한 시스템과 관련된 병목 현상을 줄이기 위해 기술적으로 유리한 특정 시스템 아키텍처를 제공한다.

[0195] 예를 들면 등록 권한(405 및 420) 상에서 실행되는 등록 권한 응용프로그램을 확장해야 하는 경우 추가적인 VM을 부가할 수 있으며 이때 등록 권한 컴퓨터 엔진(425)의 보안 연산 기능에는 변경이 필요하지 않다. 대안적으로 보안 연산이 기능을 제한하는 경우 추가적인 보안 등록 권한 컴퓨터 엔진(425)이 부가될 수 있다.

[0196] CMS(400)의 다른 컴포넌트에서도 이와 동일한 다차원 확장이 적용된다. 이러한 기능은 기존 보안 자격 증명 관리 시스템(SCMS)에 비해 상당한 기능 향상과 확장성을 제공한다.

[0197] 도 4a 및 4b에 나타난 실시예에서 등록 권한(405)은 입력 메시지 큐(410, 411, 412, 413, 414, 415, 416, 417, 418 및 419)를 포함하는 메시지 서브 시스템 또는 메시지 큐 서비스에 의해 다른 컴포넌트에 연결되고 다른 컴포넌트는 서로 연결된다.

[0198] 도 4a 및 4b의 예시적인 실시형태에서 입력 메시지 큐(410, 411, 412, 413, 414, 415, 416, 417, 418 및 419)는 이러한 큐의 메시지가 한 방향으로(예를 들면 클라이언트에서 서버로) 전달된다는 점에서 하나의 방향이다. 이는 각 VM 및 컴퓨터 엔진에 대해 단일 입력 큐를 보유함으로써 단순성의 기술적 이점을 제공한다.

[0199] 일부 실시형태에서 메시지 서비스는 예를 들어 Amazon 웹 서비스에서 제공하는 Amazon 심플 큐 서비스(SQS)와 같은 빠른 메시지 큐 서비스일 수 있다. 예를 들어 이러한 실시형태에 따르면 메시지 큐(410, 411, 412, 413, 414, 415, 416, 417, 418, 419)는 SQS 메시지 큐일 수 있다. 입력 메시지 큐(410, 411, 412, 413, 414, 415, 416, 417, 418, 419)를 사용하여 응용프로그램 VM과 컴퓨터 엔진을 서로 통신 방식으로 연결함으로써 필요에 따라 응용프로그램 VM과 컴퓨터 엔진은 독립적으로 확장 가능하다.

[0200] 즉 등록 권한(420), 등재 인증 권한(430), 가명 인증 권한(440) 및 연결 권한(450, 460)에 대한 각 응용프로그램 플랫폼은 각각의 입력 메시지 큐 세트, CMS(400)의 이들 컴포넌트 및 데이터베이스(470)를 통해 컴퓨터 엔진(425, 435, 445, 455, 465)과 통신 가능하게 연결되며 모두 서로 독립적으로 확장된다.

[0201] 상기에서 언급되고 도 4a 및 4b의 비 제한적인 실시예에 나타난 바와 같이 각각의 등록 권한(405, 420), 인증 권한(430, 440) 및 연결 권한(450, 460)은 자신의 가상 머신(VM)에서 응용프로그램으로 구현될 수 있다. 추가적 또는 대안적인 실시형태에서 하나 이상의 등록 권한(405, 420), 인증 권한(430, 440) 및 연결 권한(450, 460)은 하드웨어 플랫폼(예를 들면 서버 또는 컴퓨터 엔진) 상에서 실행될 수 있다. 응용프로그램 플랫폼(예를 들면 VM 또는 하드웨어 플랫폼) 상에서 실행되는 이러한 각 응용프로그램의 역할과 기능은 다음 단락에 개시되어 있다.

[0202] 다양한 실시형태에서 등록 권한(405)은 디지털 인증서 또는 다른 유형의 디지털 보안 자산에 대한 사용자 요청을 검증하고 디지털 인증서를 발급하기 위해 인증 권한(예를 들면 등재 인증 권한(430) 및 가명 인증 권한(440))을 활성화하는 프로비저닝 네트워크 내의 권한일 수 있다. 다양한 실시형태에서 등록 권한(405)은 공개키 인프라(PKI) 시스템 내에 알려진 등록 권한과 유사할 수 있다.

[0203] 다양한 실시형태에서 등록 권한(405)은 표현 상태 변경(REST) 웹 서비스로서 구현될 수 있다. 등록 권한(405)을 도 4a에 도시된 3 개의 적층된 직사각형으로 표시한 바와 같이 다양한 실시형태에서 동시에 등록 권한(405)을 실행해야 하는 다수의 경우가 있을 수 있다. 이것은 도 4a 및 4b의 다른 적층된 엘레멘트로 유사하게 표현된다.

[0204] CMS(400)의 등록 권한 기능은 REST 웹 서비스로 구현된 등록 권한(405)의 다중 인스턴스와 등록 권한(420)의 다중 인스턴스에 의해 그 기능이 수행될 수 있다는 점에서 비-중앙화 되어 있다. 등록 권한(405, 420)의 주요 역할은 서명하는 가명 인증 권한(440)이 특정 컴퓨터화 디바이스에서 종료되는 인증서를 알지 못하도록 유지하면

서 인증서 프로비저닝 요청을 승인하고 수행하는 것이다.

[0205] 등록 권한(405, 420)은 CMS(400) 내에서의 역할을 수행하기 위해 메시지 큐(414, 416 및 418)를 통해 가명 인증 권한(440), 연결 권한(450, 460)과 직접 상호 작용한다.

[0206] 직사각형의 좌측 하단에 나타나는 "DB" 화살표로 표시한 바와 같이 등록 권한(405)(및 "DB" 화살표로 표시한 도 4a 및 4b의 다른 컴포넌트)을 각각의 데이터베이스(470)에 접속시킬 수 있다. 단일 데이터베이스(470)가 도 4a에 나타나 있으나 CMS(400)는 데이터 저장 및 검색을 위해 데이터 저장소 또는 데이터베이스(470)의 집합을 이용할 수 있다는 것을 이해해야 한다.

[0207] 예를 들면 데이터베이스(470)는 하나 이상의 데이터베이스 논리 또는 물리적 유니트로 구성될 수 있으며 각각은 필요한 경우 데이터 분리를 가능하게 하는 하나 이상의 테이블을 지닌다. 본 명세서에서 사용되는 용어 "데이터베이스"는 하나 이상의 데이터베이스 또는 데이터 저장소를 의미한다. 특정 실시형태에서 다중 데이터베이스(470)의 사용은 "DB" 화살표로 도시된 도 4a 및 4b의 다른 컴포넌트들 사이의 데이터 분리를 허용한다. 예를 들어 다중 데이터베이스(470)의 이러한 사용은 등록 권한(405, 420), 인증 권한(430, 440) 및 연결 권한(450, 460) 간의 데이터 분리를 허용한다.

[0208] 바람직한 실시형태에서 데이터베이스(470)는 하나 이상의 빠른 액세스, 저-지연 데이터베이스의 집합이다. 일부 실시형태에서 데이터베이스(470)는 NoSQL 데이터베이스 또는 예를 들어 Amazon 웹 서비스에 의해 제공되는 DynamoDB 데이터 서비스와 같은 데이터베이스 서비스일 수 있다.

[0209] 다양한 실시형태에서 데이터베이스(470)에 저장된 데이터는 응용프로그램에 따라 상이하나 과거 발행된 인증서, 다양한 연결 권한 값, 인증서가 발행된 디바이스에 대한 데이터, 작업자 행위 등을 포함할 수 있다. 데이터는 암호화 되거나 암호화 되지 않거나 이들의 조합일 수 있다.

[0210] 다양한 실시형태에서 확장 가능한 CMS(400)는 등재 인증 권한(430) 및 가명 인증 권한(440)을 포함하며 이는 등록 권한(405)에 의해 생성된 디지털 인증서가 예를 들면 등재 디지털 인증서 및 가명 디지털 인증서와 같은 상이한 세그먼트로 분할되기 때문이다.

[0211] 등재 인증 권한(430)은 동시에 실행되는 등재 인증 권한(430)의 여러 인스턴스가 존재할 수 있으므로 CMS(400)의 비-중앙 컴포넌트다. 등재 인증 권한(430)에 대해 도 4a에서 3 개의 "적층된" 직사각형에 의해 예시된 바와 같이 일부 실시형태에서 동시에 실행되는 등재 인증 권한(430)의 다중 인스턴스가 존재할 수 있다.

[0212] 등재 인증 권한(430)은 등록 권한(420)으로부터 등재 인증서에 대한 요청을 수신할 수 있다. 등재 인증 권한(430)의 주요 역할은 예를 들면 도 1에 나타난 제조자의 분배기 어플라이언스(108)와 같은 최종 사용자 디바이스에 등재 인증서를 발급하는 등록 권한(420)으로부터의 요청을 수행하는 것이다. 도 5a를 참조하여 하기에 설명되는 바와 같이 등재 인증 권한(430)은 CMS(400) 내에서의 역할을 수행하기 위해 등록 권한(420)과 직접 상호 작용한다.

[0213] 가명 인증 권한(440)은 동시에 실행되는 가명 인증 권한(440)의 여러 인스턴스가 존재할 수 있다는 점에서 CMS(400)의 비-중앙 컴포넌트이다. 다시 말하지만, 가명 인증 권한(440)에 대해 도 4a에서 3 개의 "적층된" 직사각형에 의해 나타난 바와 같이 다양한 실시형태에서 동시에 병렬로 실행되는 가명 인증 권한(440)의 다중 인스턴스가 존재할 수 있다.

[0214] 가명 인증 권한(440)은 등록 권한(420)으로부터 가명 인증서에 대한 요청을 수신할 수 있다. 가명 인증 권한(440)의 주요 역할은 예를 들면 도 1에 나타난 제조자(105)의 분배기 어플라이언스(108)와 같은 최종 사용자 디바이스에 가명 인증서를 발급하는 등록 권한으로부터의 요청을 수행하는 것이다.

[0215] 특정 실시형태에서 가명 인증 권한(440)은 V2V 기능에 대한 단기 가명 인증서에 대한 요청을 수행한다. 도 5b를 참조하여 하기에 설명되는 바와 같이 가명 인증 권한(440)은 CMS(400) 내에서 그 기능을 수행하기 위해 등록 권한(420)과 직접 상호 작용한다.

[0216] 다양한 실시형태에서 도 4b에 나타난 연결 권한(450, 460)은 폐기 목적을 위해 인증서 요청자의 신원(즉 인증서 요청자 디바이스의 고유 식별자)을 발행된 가명 인증서에 연결한다. 즉 연결 권한 1(450) 및 연결 권한 2(460)는 발급된 가명 인증서에 대한 인증서 요청자 디바이스의 고유 식별자로서 각각의 연결 값을 제공한다.

[0217] 연결 권한 1(450) 및 연결 권한 2(460)는 등록 권한(420)으로부터 연결 값에 대한 요청을 수신한 후 요청된 연결 값을 등록 권한(420)에 제공할 수 있다. 도 5a를 참조하여 하기에 설명되는 바와 같이 연결 권한(450, 460)

은 연결 값에 대한 요청을 수행하기 위해 등록 권한(420)과 직접 상호 작용한다.

[0218] 다양한 실시형태에서 컴퓨터 엔진(425, 435, 445, 455, 465) 및 프로비저닝 제어기(120)는 HSM을 포함하며 이는 이들 컴포넌트가 해커로부터 부당하게 위협받지 않고 보안 연산을 수행할 수 있게 한다. 일부 실시형태에서 컴퓨터 엔진(425, 435, 445, 455 및 465)은 임베디드 HSM을 필요로 하지 않고 자체적으로 보안 연산을 수행하도록 설계될 수 있다. 이러한 실시형태에서 이들은 HSM을 구현한다.

[0219] 다양한 실시형태에서 상이한 HSM 버전이 CMS(400)에서 사용될 수 있다. 예를 들어 HSM은 하나 이상의 컴퓨터 엔진(425, 435, 445, 455 및 465) 내에 플러그인 카드로 설치된 임베디드 HSM을 포함할 수 있다. 이러한 예시적인 실시형태에서 임베디드 HSM은 주변 컴포넌트 상호연결(PCI) HSM 또는 PCI 익스프레스(PCIe) HSM과 같은 컴퓨터 엔진 중 하나 이상에 설치될 수 있다. 또한 예를 들어 CMS(400)의 HSM은 자체 인클로저의 컴퓨터 엔진과 분리된 외부, 네트워크-연결 또는 네트워크-접속 HSM을 포함할 수 있다.

[0220] 통상의 기술자는 도 4a 및 4b에 도시된 컴포넌트, 프로세스, 데이터, 작동 및 구현 세부사항이 설명의 간결성 및 명확성을 위해 제시된 예임을 인식할 것이다. 이러한 실시예는 범위를 제한하려는 것이 아니고 다양한 변형이 가능하며 본 발명의 원리를 벗어나지 않는 범위 내에서 다른 컴포넌트, 프로세스, 구현 세부사항 및 변형이 가능하다.

[0221] 도 5a 및 5b는 본 발명의 실시형태와 일치하는 인증서와 같은 자격 증명을 보안 제공하기 위한 프로세스(500)를 예시하는 스윔 레인 다이어그램이다. 다양한 실시형태에서 프로세스(500) 또는 도시된 작동의 일부 또는 전부는 범용 컴퓨터 시스템(하나 이상의 프로세서 또는 하나 이상의 컴퓨터 서브 시스템을 포함할 수 있음), 하드웨어 전용 시스템 또는 이들의 혼성화 시스템 상에서 실행되는 코드에 의해 수행될 수 있다.

[0222] 도 5a 및 5b의 상단에 나타난 바와 같이 프로세스(500)와 관련된 엔티티는 제조업체(105)에 위치한 분배기 어플라이언스(108), CMS 호스트의 등록 권한(420), 연결 권한(450, 460), 가명 인증 권한(440) 및 등재 인증 권한(430)을 포함한다. 다양한 실시형태에서 이러한 엔티티는 도 4a 및 4b와 관련하고 본 명세서 전반에 걸쳐 개시된 바와 같이 상호 통신한다.

[0223] 도 5a의 실시예에 나타난 바와 같이 프로세스(500)는 등재-관련 작동(505-535)에서 시작한다. 등재 인증 권한(430)의 주요한 역할은 예를 들어 분배기 어플라이언스(108)와 같은 최종 사용자 디바이스에 등재 인증서를 발행하는 등록 권한(420)으로부터의 요청을 수행하는 것이다. 등재-관련 작동(505)과 관련하여 하기에 개시되는 바와 같이 작동(505-535)에서 등재 인증 권한(430)은 요청된 등재 인증서를 분배기 어플라이언스(108)에 발행하기 위해 등록 권한(420)과 직접 상호 작용한다.

[0224] 단계 505에서 제조업체(105)의 분배기 어플라이언스(108)는 등록 권한(420)으로부터 등재 인증서를 요청하고, 여기서 등재 인증서는 디바이스(106a)에 프로비저닝(예를 들어 사용)될 것이며, 요청은 등재 인증서의 목적지인 해당 디바이스(106a)를 식별할 수 있다. 예를 들어 요청은 신규 디바이스(106A)(예를 들어 신규 제품)에 대한 등재 인증서를 요청하는 제조업체(105)의 분배기 어플라이언스(108)일 수 있다.

[0225] 도 2 상단에 언급한 바와 같이 등재 인증서는 모든 참가자가 유효한 등재 인증서를 공유해야 하는 생태계(예를 들면 USDOT의 V2X 생태계) 내의 권한 있는 참가자 자격을 지닌 소유자를 식별하는 공개 키 인증서이다. 권한 있는 참가자는 생태계 내에서 디바이스(106)의 통신 및 작동을 가능하게 하는 (예를 들어 USDOT의 V2X 생태계의 실시예에서 차량과 도로변 인프라 사이의 통신 및 작동을 가능하게 하는) 가명 인증서를 수신할 수도 있다.

[0226] 단계 510에서 등재 인증서에 대한 요청은 등록 권한(420)에서 수신된 후 등록 권한(420)으로부터 등재 인증 권한(430)으로 전송된다. 다양한 실시형태에서 이러한 작동은 등록 권한(420)이 서명 검증을 포함하여 요청을 해독 및 검증하는 단계, 승인되지 않은 디바이스 목록(예를 들면 블랙리스트)을 사용하여 등재 인증서의 목적지인 디바이스(예를 들면 디바이스(106a))의 폐기 상태를 확인하는 단계, 및 요청자(예를 들면 분배기 어플라이언스(108))가 등록 권한(420)으로부터 등재 인증서를 요청할 수 있는지 여부를 결정하는 단계를 포함한다.

[0227] 예를 들어 작동(510)은 제조자(105)로부터의 사용자가 권한 있는 사용자(예를 들면 스태프(109)의 일부)인지를 결정하는 단계를 포함할 수 있다. 일부 실시형태에서 등록 권한(420)은 또한 등재 인증서를 수신하기 위한 디바이스(106a)(예를 들어 제품)가 시스템(100)과 함께 사용하도록 승인되었는지 여부를 단계 510에서 결정할 수 있다. 일부 경우에 승인된 디바이스의 목록(예를 들어 화이트리스트)는 도 1의 조절자(140)에 의해 제공되고 이러한 결정을 위한 프로비저닝 제어기(120)를 사용할 수 있다.

[0228] 등재 인증서 요청이 검증된 후, 요청은 등록 권한(420)에서 등재 인증 권한(430)으로 전송된다. 이 요청은 등록

권한(420)에 의해 생성된 등재 인증서 생성 요청으로 전송될 수 있다.

[0229] 단계 515에서 등재 인증서에 대한 요청이 등재 인증 권한(430)에서 수신된다. 요청을 수신하는 것에 응답하여 단계 520에서 등재 인증 권한(430)은 요청된 등재 인증서를 생성하고 생성된 등재 인증서를 등록 권한(420)으로 다시 전송한다. 단계 525에서 등재 인증서는 등록 권한(420)에서 수신되고, 단계 530에서 등록 권한(420)은 등재 인증서를 분배기 어플라이언스(108)로 전송한다. 단계 535에서 분배기 어플라이언스는(108)는 등재 인증서를 수신한다. 이 시점에서 분배기 어플라이언스(108)는 디바이스가 등재 인증서를 사용할 수 있도록 등재 인증서를 디바이스(예를 들어 디바이스(106a))에 프로비저닝함으로써 등재-관련 작동이 완료된다.

[0230] 작동 540-599는 가명 인증서 프로비저닝과 관련이 있다. 단계 540에서 분배기 어플라이언스(108)는 등록 권한(420)으로부터 가명 인증서를 요청한다. 가명 인증서는 디바이스(106a)에 프로비저닝 될(예를 들어 사용될) 것이며, 요청은 가명 인증서에 대한 목적지인 디바이스(106a)를 식별할 수 있다.

[0231] 요청은 예를 들어 등재 인증서를 이전에 수신한 컴퓨터화 디바이스(예를 들어 등재된 디바이스(106A))에 대한 가명 인증서를 요청하는 제조업체(105)의 분배기 어플라이언스(108)일 수 있다. 가명 인증서에는 특정 분량(예를 들면 1주일 치, 1개월 치 또는 1년 치)의 공개 키 인증서가 포함된다.

[0232] 단계 545에서 가명 인증서에 대한 요청이 등록 권한(420)에서 수신되고, 그 후 가명 인증서의 프로비저닝을 시작한다.

[0233] 작동 550-570에서 연결 권한(450, 460)은 연결 값에 대한 요청을 수행하기 위해 등록 권한(420)과 직접 상호 작용한다. 단계 550에서 등록 권한(420)은 연결 권한 1(450)로 연결 값의 첫 번째 세트(LA1)에 대한 요청을 전송한다.

[0234] 단계 555에서 연결 값의 첫 번째 세트에 대한 요청을 수신하는 것에 응답하여 연결 권한 1(450)은 연결 값의 첫 번째 세트를 생성하고 등록 권한(420)에 전송한다. 단계 557에서 연결 값의 첫 번째 세트는 등록 권한(420)에서 수신된다. 단계 560에서 등록 권한(420)은 연결 값의 두 번째 세트(LA2)에 대한 요청을 연결 권한 2(460)에 전송한다.

[0235] 다음으로 도 5b에 나타난 바와 같이 단계 565에서 연결 값의 두 번째 세트에 대한 요청을 수신하는 것에 응답하여 연결 권한 2(460)는 연결 값의 두 번째 세트를 생성하고 등록 권한(420)에 전송한다. 연결 값의 두 번째 세트는 등록 권한(420)에서 수신된다.

[0236] 특정 실시형태에서 도 5a 및 5b에 나타난 연결 권한(450, 460)은 폐기 목적을 위해 인증서 요청자의 신원(즉 인증서 요청자 디바이스의 고유 식별자)을 발행된 가명 인증서에 연결할 수 있다. 즉 연결 권한 1(450) 및 연결 권한 2(460)는 각각 프로세스(500)의 일부로서 가명 인증 권한(440)에 의해 발행된 가명 인증서에 인증서 요청자 디바이스의 고유 식별자로서 연결 값의 첫 번째 및 두 번째 세트를 제공한다.

[0237] 연결 권한 1(450) 및 연결 권한 2(460)는 단계 550 및 단계 560에서 등록 권한(420)으로부터 전송된 연결 값의 요청을 수신하고 단계 555 및 단계 565에서 요청된 연결 값을 등록 권한(420)에 제공한다.

[0238] 비 제한적인 예시적인 실시형태에서 연결 값에 대한 요청 및 작동 550-570에서 교환된 요청에 대한 응답은 하기와 같이 헤더 및 페이로드 데이터 항목을 지닌 메시지를 포함할 수 있다.

[0239] # Registration Authority(RA)-> Linkage Authority-x(LA-x): Initial Linkage Seed Request {

[0240] header: {

[0241] msgID: mt.MSG_RA_LA_LINKAGE_SEED_REQUEST_MSG,

[0242] taskPosition: "Linkage Authority number 1 or 2"

[0243] },

[0244] payload: {

[0245] identifier: "Message identifier",

[0246] iMin: Number,

[0247] iMax: Number,

```
[0248]      jMax: Number
[0249]      }
[0250]    }
[0251]    # LA-x -> RA: Initial Linkage Seed Response {
[0252]      header: {
[0253]        msgID: mt.MSG_LA_RA_LINKAGE_SEED_RESPONSE_MSG,
[0254]        taskPosition: "Linkage Authority number 1 or 2"
[0255]      },
[0256]      payload: {
[0257]        identifier: "Incoming Message identifier",
[0258]        linkageChainIdentifier: "Linkage Chain ID -- HashedId8 of AES CCM Encrypted Linkage Seed",
[0259]        iMin: Number,
[0260]        iMax: Number,
[0261]        jMax: Number
[0262]      }
[0263]    }
[0264]    # RA -> LA-x:  PreLinkage Value Chain Request(Chunked 10 iRange at a time) {
[0265]      header: {
[0266]        msgID: mt.MSG_RA_LA_PRE_LINKAGE_VALUE_REQUEST_MSG,
[0267]        iRangeSegmentChunkSize: "set to 10",
[0268]        currentIRangeSegment: "Index of segment in total request",
[0269]        taskPosition: "Linkage Authority number 1 or 2"
[0270]      },
[0271]      payload: {
[0272]        identifier: "Incoming Message identifier",
[0273]        linkageChainId: "Linkage Chain ID to use to create P Linkage Values(PLVs)",
[0274]        iMin: Number,
[0275]        iMax: Number,
[0276]        jMax: Number
[0277]      }
[0278]    }
[0279]    # LA-x -> RA: PreLinkage Value Chain Response {
[0280]      header: {
[0281]        msgID: mt.MSG_LA_RA_PRE_LINKAGE_VALUE_RESPONSE_MSG,
[0282]        iRangeSegmentChunkSize: "set to 10",
[0283]        currentIRangeSegment: "Index of segment in total request",
```

[0284] taskPosition: "Linkage Authority number 1 or 2"

[0285] },

[0286] payload: {

[0287] identifier: "Incoming Message identifier",

[0288] preLinkageValues: Array of Encryped Prelinkage values for this segment of i,j tuples,

[0289] linkageChainIdentifier: "Linkage Chain ID to use to create P Linkage Values(PLVs)",

[0290] iMin: Number,

[0291] iMax: Number,

[0292] jMax: Number

[0293] }

[0294] }

[0295] 계속해서 도 5b를 참조하면 단계 575에서 등록 권한(420)은 가명 인증서에 대한 요청을 가명 인증 권한(430)에 전송한다. 이러한 요청은 등록 권한(420)에 의해 생성된 가명 인증서 생성 요청의 배치로서 전송될 수 있다.

[0296] 단계 580에서 가명 인증서에 대한 요청은 가명 인증 권한(430)에서 수신된다. 요청을 수신하는 것에 응답하여, 단계 585에서 가명 인증 권한(430)은 요청된 가명 인증서를 생성하고 생성된 가명 인증서를 등록 권한(420)으로 다시 전송한다. 단계 590에서 가명 인증서는 등록 권한(420)에서 수신된다.

[0297] 단계 595에서 분배기 어플라이언스(108)는 요청된 가명 인증서가 준비되었는지(즉 생성되고 이용 가능한지) 여부를 질의하기 위해 등록 권한(420)에 다중 요청을 전송할 수 있다. 특정 실시형태에서 작동 595의 질의는 작동 540에서 가명 인증서에 대한 요청이 전송된 후 언제든지 전송될 수 있다.

[0298] 예를 들면 작동 540에서 가명 인증서에 대한 요청을 등록 권한(420)에 전송 한 후 분배기 어플라이언스(108)는 요청된 가명 인증서가 준비 되었는지를 결정하기 위해 등록 권한(420)에 주기적으로 질의를 전송할 수 있다. 이러한 실시예에서 작동 595의 질의 중 하나 이상이 작동 545-590과 평행하게(즉 가명 인증서가 생성되는 동안) 전송될 수 있다.

[0299] 단계 598에서 가명 인증서가 준비되면 등록 권한(420)은 분배기 어플라이언스(108)로 가명 인증서를 전송한다. 단계 599에서 분배기 어플라이언스(108)는 가명 인증서를 수신한다. 이 시점에서 분배기 어플라이언스(108)는 디바이스가 가명 인증서를 사용할 수 있도록 가명 인증서를 디바이스(예를 들어 디바이스(106a)에 프로비저닝 할 수 있고 가명 인증서를 프로비저닝 하기 위한 작동이 완료된다.

[0300] 특정 비 제한적인 예시적 실시형태에서 가명 인증서에 대한 요청 및 작동 575-590에서 교환된 요청에 대한 응답은 하기와 같이 헤더 및 페이로드 데이터 항목을 지닌 메시지를 포함할 수 있다.

[0301] # Registration Authority(RA) -> Pseudonym Certificate Authority(PCA): Generate an individual Certificate {

[0302] header: {

[0303] msgID: mt.MSG_RA_PCA_CERT_REQUEST_MSG,

[0304] iRangeSegmentChunkSize: "set to 10"

[0305] },

[0306] payload: {

[0307] identifier: "hash of payload minus this field"

[0308] i: Number,

[0309] plv1: "Encrypted PLV from LA1",

[0310] plv2: "Encrypted PLV from LA2",

[0311] seedPublicKey: "Seed Verify Public key",

[0312] encryptKey: "Seed Encrypt Public key",

[0313] startSeconds: "start time for this certificate",

[0314] endSeconds: "end time for this certificate",

[0315] region: "requested region",

[0316] certRequestPermissions: "the cert request permissions from the enrollment cert(will be turned into app permissions)"

[0317] }

[0318] }

[0319] # PCA -> RA: Certificate Response

[0320] {

[0321] header: {

[0322] msgID: mt.MSG_PCA_RA_IDENTITY_CERT_RESPONSE_MSG

[0323] },

[0324] payload: {

[0325] data: "Signed and Encrypted SCMS certificate response",

[0326] identifier: "hash of original payload request"

[0327] }

[0328] }

[0329] 도 6a 및 6b는 양방향 메시지 큐(610, 611, 612, 613, 614, 615, 616, 617, 618, 619)를 사용하여 본 발명의 실시형태에 따른 확장 가능하고 보안적인 CMS(600)을 구현하기 위한 예시적인 아키텍처의 블록도이다.

[0330] 도 4a 및 4b를 참조하여 상기에서 개시된 CMS(400)와 같이 확장 가능한 CMS(600)의 다양한 실시형태는 매우 높은 볼륨의 디바이스 트랜잭션 및 인증서 생성 처리를 위해 사용될 수 있다. 일부 실시형태에서 확장 가능한 CMS(600)는 다중 서버, HSM, 다중 컴퓨터 또는 컴퓨터 엔진 및 다중 응용프로그램 플랫폼(예를 들면 VM 또는 하드웨어 플랫폼)을 사용하여 구현될 수 있다. 도 6a 및 6b에 나타난 예시적인 실시형태에서 응용프로그램 플랫폼은 각각 하나 이상의 가상 머신(VM)을 포함할 수 있다.

[0331] 추가적 또는 대안적인 실시형태에서 응용프로그램 플랫폼은 각각 예를 들어 서버, 컴퓨터, 또는 소프트웨어 응용프로그램을 실행할 수 있는 다른 컴퓨터 하드웨어와 같은 하나 이상의 하드웨어 플랫폼을 포함할 수 있다. 확장 가능한 CMS(600)의 예는 사설 데이터 센터, Amazon의 Amazon Web Services(AWS)와 같은 클라우드 데이터 센터 또는 사설 및 클라우드 데이터 센터의 혼성화에서 구현될 수 있다. 간결성을 위해 도 4a 및 4b와 비교하여 도 6a 및 6b 내에서 발생하는 차이점만이 하기에 개시되어 있다.

[0332] 도 6a의 실시예에 나타난 바와 같이 CMS(600)의 아키텍처는 2 개의 프로비저닝 제어기(602)(프라이머리 및 예비)를 포함할 수 있으며 이는 별도의 서버에서 바람직하게 구현된다. 2 개의 프로비저닝 제어기(602)는 도 4a의 프로비저닝 제어기(102)와 유사한 기능을 포함한다. 따라서 프라이머리 프로비저닝 제어기 내에 포함된 객체, 데이터 등이 복사되거나 도 4a를 참고로 하여 상기에 개시된 장애 복구 목적을 위해 예비(세컨더리) 프로비저닝 제어기 내에 포함된다.

[0333] 특정 실시형태에서 프로비저닝 제어기(602)는 DLM 컨트롤러 예를 들면 프라이머리 및 예비 DLM 컨트롤러일 수 있다. 다양한 실시형태에서 프로비저닝 제어기(602)는 CMS(600)의 각 유형의 컴포넌트에 대해 존재하는 컨트롤러일 수 있다. 도 6a 및 6b의 실시예에서 프로비저닝 제어기(602)는 등록 권한(620), 등재 인증 권한(430), 가명 인증 권한(440) 및 연결 권한(450, 460)을 위해 존재하는 제어기의 쌍(예를 들면 프라이머리 및 예비)일 수

있다.

[0334]

[0335] 도 6a 및 6b에 나타난 바와 같이 확장 가능한 CMS(600)의 아키텍처는 REST 웹 서비스로 구현된 등록 권한(605), 등록 권한(620), 등록 권한 컴퓨터 엔진(625), 등재 인증 권한(630), 등재 인증 권한 컴퓨터 엔진(635), 가명 인증 권한(640), 가명 인증 권한 컴퓨터 엔진(645), 연결 권한 1(650), 연결 권한 1 컴퓨터 엔진(655), 연결 권한 2(660), 연결 권한 1 컴퓨터 엔진(665), 양방향 메시지 큐(610, 611, 612, 613, 614, 615, 616, 617, 618, 619) 및 데이터베이스(670)를 포함한다.

[0336] 확장 가능한 CMS(600)의 아키텍처는 보안 기능에서 비-보안-관련 응용프로그램을 유리하게 분리한다. 도 6a 및 6b의 비제한적인 실시예에서 등록 권한(620), 등재 인증 권한(630), 가명 인증 권한(640) 및 연결 권한(650, 660)은 그들 자신의 전용 컴퓨터 엔진(625, 635, 645, 655 및 665) 상에서 실행되는 VM상에서 응용프로그램으로서 구현된다. 이들 전부는 비-보안-관련 응용프로그램 및 기능에서 분리되어 있다.

[0337] 이는 HSM의 성능이 느리거나 클라우드 서비스 제공 업체가 HSM을 공급할 수 없거나 HSM의 적절한 관리가 불확실한 기존 시스템에 비해 기술적 및 보안적 이점과 개선을 제공한다. 확장 가능한 CMS(600)에서 HSM이 필요로 하는 모든 암호화 작동은 컴퓨터 엔진(예를 들면 하나 이상의 컴퓨터 엔진 625, 635, 645, 655 및 665)에서 수행된다. 즉 CMS(600)에서는 HSM이 필요로 하는 모든 암호화 작동이 컴퓨터 엔진에서 수행된다.

[0338] 도 6a 및 6b에 나타난 바와 같이 중요한 보안 기능을 서로 별도의 컴퓨터 엔진으로 분리함으로써 예를 들면 등록 권한(620), 등재 인증 권한(630), 가명 인증 권한(640) 및 연결 권한(650, 660)에 의해 수행되는 바와 같이 연산-집약적인 암호화 및 보안 기능 은 기존 등록 권한 시스템에 비해 유의미하게 빨리 수행된다. 이 설계는 "병목 현상" 응용프로그램을 필요에 따라 개별적으로 확장 가능하게 하여 트랜잭션 처리를 크게 향상시킨다.

[0339] 예를 들어 등록 권한(605 및 620) 상에서 실행되는 등록 권한 응용프로그램을 확장해야 하는 경우 추가적인 응용프로그램 플랫폼(예: VM 또는 하드웨어 플랫폼)을 부가할 수 있으며 이때 등록 권한 컴퓨터 엔진(625)의 보안 연산 기능에는 변경이 필요하지 않다. 또한 예를 들어 보안 연산이 기능을 제한하는 경우 추가적인 보안 등록 권한 컴퓨터 엔진(625)이 부가될 수 있다. 이러한 동일한 다차원 확장은 CMS(600)의 다른 컴포넌트에도 적용된다.

[0340] 도 6a 및 6b에 나타난 실시예에서 등록 권한(605)은 양방향 메시지 큐(610, 611, 612, 613, 614, 615, 616, 617)에 의해 다른 컴포넌트에 연결되고 다른 컴포넌트는 서로 연결된다. 도 6a 및 6b의 예시적인 실시형태에서 양방향 메시지 큐(610, 611, 612, 613, 614, 615, 616, 617, 618, 619)는 이러한 큐의 메시지가 2 방향(예를 들면 클라이언트와 서버 사이)으로 흐른다는 점에서 양방향이다. 이는 메시지 큐 내에서 보류중인 응답으로 부터 신규 요청을 분리하는 기술적 이점을 제공한다.

[0341] 양방향 메시지 큐(610, 611, 612, 613, 614, 615, 616, 617, 618, 619)를 사용하여 응용프로그램 플랫폼(예를 들면 VM 및/또는 하드웨어 플랫폼)과 컴퓨터 엔진을 서로 통신 가능하게 연결함으로써 응용프로그램 플랫폼(예를 들면 VM 및/또는 하드웨어 플랫폼)과 컴퓨터 엔진은 독립적으로 확장될 수 있다.

[0342] CMS(600)에서 등록 권한(620), 등재 인증 권한(630), 가명 인증 권한(640) 및 연결 권한(650, 660)을 위한 각각의 응용프로그램 플랫폼(예를 들면 VM 및/또는 하드웨어 플랫폼)은 양방향 메시지 큐의 각각의 세트를 통해 컴퓨터 엔진(625, 635, 645, 655 및 665)에 통신 가능하게 연결된다.

[0343] CMS(600)에서 등록 권한(605)(및 도 6a 및 6b 내에서 "DB" 화살표로 표시된 다른 컴포넌트)은 데이터베이스(670)에 연결될 수 있다. 바람직한 실시형태에서 데이터베이스(670)는 빠른 액세스, 저-지연 데이터베이스이다. 특정 실시형태에서 데이터베이스(670)는 NoSQL 데이터베이스 또는 예를 들어 Amazon 웹 서비스에 의해 제공되는 DynamoDB 데이터 서비스와 같은 데이터베이스 서비스일 수 있다.

[0344] 다양한 실시형태에서 데이터베이스(670)에 저장된 데이터는 응용프로그램에 따라 상이하나 과거 발행된 인증서, 다양한 연결 권한 값(예를 들면 연결 값), 인증서가 발급된 디바이스에 대한 데이터, 작업자 행위 등을 포함할 수 있다. 데이터는 암호화되거나 암호화되지 않거나 이들의 조합일 수 있다.

[0345] 다양한 실시형태에서 확장 가능한 CMS(600)는 등재 인증 권한(630) 및 가명 인증 권한(640)을 포함하며 이는 등록 권한(605)에 의해 생성된 디지털 인증서가 예를 들어 등재 디지털 인증서 및 가명 디지털 인증서와 같은 상이한 세그먼트로 분할되기 때문이다.

[0346] 등재 인증 권한(630)에 대해 도 6a에서 3 개의 "적층된" 직사각형으로 예시한 바와 같이 일부 실시형태에서 동시에 실행되는 등재 인증 권한(630)의 다중 인스턴스가 존재할 수 있다. 이것은 도 6a 및 도 6b의 다른 "적층된" 엘레멘트에 대해 유사하게 표현된다. 등재 인증 권한(630)은 등록 권한(620)으로부터 등재 인증서에 대한 다중 요청을 수신할 수 있다.

[0347] 다양한 실시형태에서 컴퓨터 엔진(625, 635, 645, 655 및 665) 및 프로비저닝 제어기(602)는 HSM을 포함하며 이는 이들 컴포넌트가 해커로부터 부당하게 위협받지 않고 보안적인 연산을 수행할 수 있게 한다. 일부 실시형태에서 컴퓨터 엔진(625, 635, 645, 655, 665)은 내장된 HSM 필요 없이 자체적으로 보안 연산을 수행하도록 설계될 수 있다. 이러한 실시형태에서 이들은 HSM을 구현한다.

[0348] 통상의 기술자는 도 6a 및 6b에 나타난 컴포넌트, 프로세스, 데이터, 작동 및 실시형태 세부 사항이 설명의 간결함과 명확성을 위해 제시된 실시예임을 인식할 것이다. 다른 컴포넌트, 프로세스, 실시형태 세부 사항 및 변형이 본 발명의 원리를 벗어나지 않고 사용될 수 있으며 이러한 실시예는 한정하려는 의도가 아니고 많은 변형이 가능하기 때문이다.

[0349] 도 7a및 7b는 본 발명의 실시형태와 일치하는 로드 밸런서(710, 711, 712, 713, 714, 715, 716, 717, 718, 719)를 사용하여 확장 가능하고 보안적인 CMS(700)을 구현하기 위한 예시적인 아키텍처의 블록도이다.

[0350] 도 4 및 도 6을 참조하여 상기에서 설명된 CMS(400 및 600)에서와 같이 확장 가능한 CMS(700)의 다양한 실시형태는 매우 큰 볼륨의 디바이스 트랜잭션 및 인증서 생성 처리를 위해 사용될 수 있다. 간결성을 위해 도 4 및 도 6과 비교하여 도 7a 및 7b 내에서 발생하는 차이점만이 하기에 개시되어 있다.

[0351] 도 7a 및 도 7b에 나타난 예시적인 실시형태에서 응용프로그램 플랫폼은 하나 이상의 가상 머신(VM)을 포함하는 것으로 묘사된다. 추가적 또는 대안적인 실시형태에서 응용프로그램 플랫폼은 각각 하나 이상의 하드웨어 플랫폼 예를 들면 응용프로그램 서버, 서버 팜, 클라우드 기반 서버, 응용프로그램 작동을 수행하도록 구성된 프로세서 또는 소프트웨어 응용프로그램을 실행할 수 있는 기타 컴퓨터 하드웨어를 포함할 수 있다.

[0352] 도 7a의 실시예에 나타난 바와 같이 CMS(700)의 아키텍처는 2 개의 프로비저닝 제어기(702)(프라이머리 및 예비)를 포함할 수 있으며 이는 바람직하게는 별도의 서버에서 구현된다. 2 개의 프로비저닝 제어기(702)는 각각 도 4a 및 도 6a의 프로비저닝 제어기(120 및 602)와 유사한 기능을 포함한다. 즉 프라이머리 프로비저닝 제어기에 포함된 객체, 데이터 등은 도 4a를 참조하여 설명한 바와 같이 장애 복구 목적을 위해 예비(세컨더리) 프로비저닝 제어기에 복사되거나 포함된다.

[0353] 도 7a 및 도 7b에 도시된 바와 같이 확장 가능한 CMS(700)의 아키텍처는 REST 웹 서비스로 구현된 등록 권한(705), 등록 권한(720), 등록 권한 컴퓨터 엔진(725), 등재 인증 권한(730), 등재 인증 권한 컴퓨터 엔진(735), 가명 인증 권한(740), 가명 인증 권한 컴퓨터 엔진(745), 연결 권한 1(750), 연결 권한 1 컴퓨터 엔진(755), 연결 권한 2(760), 연결 권한 2 컴퓨터 엔진(765), 로드 밸런서(710, 711, 712, 713, 714, 715, 716, 717, 718, 719) 및 데이터베이스(770)를 포함한다.

[0354] 도 4 및 도 6의 CMS(400) 및 CMS(600)와 마찬가지로 확장 가능한 CMS(700)의 아키텍처는 보안 기능에서 비보안 관련 응용프로그램을 유리하게 분리시킨다. 도 7a 및 도 7b의 비 제한적인 실시예에 나타난 바와 같이 등록 권한(720), 등재 인증 권한(730), 가명 인증 권한(740) 및 연결 권한(750, 760)은 자신의 전용 컴퓨터 엔진(725, 735, 745, 755 및 765) 상에서 실행되는 VM상에서 응용프로그램으로 구동된다. 이들 전부는 비-보안-관련 응용프로그램 및 기능에서 분리되어 있다.

[0355] 확장 가능한 CMS(700)에서 HSM을 필요로 하는 모든 암호화 작동은 컴퓨터 엔진(예: 하나 이상의 컴퓨터 엔진 725, 735, 745, 755 및 765)에서 수행된다. CMS(700)에서 HSM이 필요로 하는 모든 암호화 작동은 컴퓨터 엔진에서 수행된다.

[0356] 도 7a 및 7b에 나타난 바와 같이 중요한 보안 기능을 서로 별도의 컴퓨터 엔진으로 분리함으로써 예를 들면 등록 권한(720), 등재 인증 권한(730), 가명 인증 권한(740) 및 연결 권한(750, 760)에 의해 수행되는 연산-집약적인 암호화 및 보안 기능을 기존 등록 권한 솔루션 비해 유의미하게 빨리 수행할 수 있다. 이러한 디자인은 "병목 현상" 응용프로그램을 개별적으로 확장할 수 있도록 하여 서버의 처리 용량이나 스토리지 용량에 관계 없이 필요에 따라 트랜잭션 처리를 크게 향상시킨다.

[0357] 예를 들어 등록 권한(705 및 720)에서 실행되는 등록 권한 응용프로그램을 확장해야 하는 경우 추가적인 응용프로그램 플랫폼(예: VM 또는 하드웨어 플랫폼)을 부가할 수 있으며 이때 등록 권한 컴퓨터 엔진(725)의 보안 연

산 기능에는 변경이 필요하지 않다. 또한 예를 들어 보안 연산이 기능을 제한하는 경우 추가적인 보안 등록 권한 컴퓨터 엔진(725)이 부가될 수 있다. 이와 동일한 다차원 확장이 CMS(700)의 다른 컴포넌트에도 적용된다.

[0358] 도 7a 및 7b에 도시된 실시예에서 등록 권한(705)은 다른 컴포넌트에 연결되고, 다른 컴포넌트는 로드 밸런서(710, 711, 712, 713, 714, 715, 716, 717, 718)에 의해 서로 연결된다. 도 7a 및 7b의 예시적인 실시형태에서 로드 밸런서(710, 711, 712, 713, 714, 715, 716, 717, 718 및 719)는 (예를 들면 VM 상에서 실행되는) 가상 로드 밸런서 또는 전용 하드웨어를 통해 구현될 수 있다.

[0359] 도 7a 및 7b에 나타난 바와 같이 CMS(700)에서 각각의 로드 밸런서(710, 711, 712, 713, 714, 715, 716, 717, 718 및 719)는 유사한 유형의 VM 또는 컴퓨터 엔진 각각의 전면부에 삽입된다. 이는 하나의 또는 다수의 클라이언트가 단일 서버 엔드 포인트만 볼 수 있는 것과 로드 밸런서가 주어진 요청을 처리할 서버를 결정하는 이점을 제공한다.

[0360] 이러한 방식으로 로드 밸런서(710, 711, 712, 713, 714, 715, 716, 717, 718, 719)는 응용프로그램 플랫폼(예: VM 및/또는 하드웨어 플랫폼)과 컴퓨터 엔진을 서로 통신 가능하게 연결한다.

[0361] CMS(700)에서 등록 권한(720), 등재 인증 권한(730), 가명 인증 권한(740) 및 연결 권한(750, 760)에 대한 각각의 응용프로그램 플랫폼은 각각의 로드 밸런서 세트를 통해 컴퓨터 엔진(725, 735, 745, 755, 765)에 통신 가능하게 연결된다.

[0362] 다양한 실시형태에서 확장 가능한 CMS(700)는 등재 인증 권한(730) 및 가명 인증 권한(740)을 포함하며 이는 등록 권한(705)에 의해 생성된 디지털 인증서가 예를 들면 등재 디지털 인증서 및 가명 디지털 인증서의 상이한 세그먼트로 분할되기 때문이다.

[0363] 가명 인증 권한(740)에 대해 도 7a에서 3 개의 "적층된" 직사각형으로 도시한 바와 같이 다양한 실시형태에서 동시에 실행되는 가명 인증 권한(740)의 다중 인스턴스가 존재할 수 있다. 이것은 도 7a 및 7b의 다른 "적층된" 엘레멘트에 대해 유사하게 표현된다. 가명 인증 권한(740)은 등록 권한(720)으로부터 가명 인증서의 배치에 대한 다수의 요청(예를 들어 1주일 치, 1개월 치 또는 1년 치 가명 인증서 요청)을 수신할 수 있다.

[0364] 당업자는 도 7a 및 7b에 도시된 컴포넌트, 프로세스, 데이터, 작동 및 실시형태 세부 사항이 설명의 간결성과 명확성을 위해 제시된 실시예임을 인식할 수 있다. 다른 컴포넌트, 프로세스, 실시형태 세부 사항 및 변형이 본 발명의 원리를 벗어나지 않고 사용될 수 있으며 이러한 실시예는 한정하려는 의도가 아니고 많은 변형이 가능하기 때문이다.

[0365] 도 8은 본 발명의 실시형태와 일치하는 라운드 로빈 요청으로 확장 가능하고 보안적인 CMS를 구현하기 위한 시스템(800) 실시예의 블록도이다. 단순화를 위해 응용프로그램 플랫폼(예: VM 및/또는 하드웨어 플랫폼) 및 컴퓨터 엔진(825, 835, 845, 855)의 한 세트(820, 830, 840, 850) 만을 도 8에 나타내었다.

[0366] 도 8의 응용프로그램 플랫폼(820, 830, 840, 850) 및 컴퓨터 엔진(825, 835, 845, 855)은 도 7을 참고하여 상기에 개시된 임의의 등록 권한(720), 등재 인증 권한(730), 가명 인증 권한(740) 및 연결 권한(750, 760)을 구현하는 데 사용되는 응용프로그램 플랫폼 및 컴퓨터 엔진의 임의의 세트일 수 있다.

[0367] 도 7의 CMS(700)와 같이 시스템(800)에서 HSM을 필요로 하는 모든 암호화 작동은 컴퓨터 엔진에서 수행되고 응용프로그램 플랫폼 및 컴퓨터 엔진은 모두 독립적으로 확장된다.

[0368] 계속해서 도 8을 참조하면 라운드 로빈은 사용 가능한 각 서버(예를 들면 각각의 컴퓨터 엔진)의 정보를 사용하는 것을 의미한다. 시스템(800) 내에 전송된 라운드 로빈 요청은 사용 가능한 컴퓨터 엔진(예를 들면 컴퓨터 엔진(825, 835, 845, 855))의 정보를 사용하여 해당 컴퓨터 엔진 세트로 요청 및 메시지를 분배한다.

[0369] 시스템(800) 내에서 라운드 로빈 요청의 순서를 명확하게 설명하기 위해 응용프로그램 VM(850)에서 이용 가능한 컴퓨터 엔진(865, 875, 885, 895)의 확장된 세트를 나타내었다. 도 8의 실시예에서 "n" 개의 응용프로그램 플랫폼(예를 들면 VM 및/또는 하드웨어 플랫폼)이 존재하며 "m" 개의 컴퓨터 엔진을 사용할 수 있다.

[0370] 컴퓨터 엔진에 요청을 보내려 하는 클라이언트(예를 들면 응용프로그램 VM(895))는 도 8에 나타난 순서대로 수행한다. 나타난 바와 같이 응용프로그램 VM(895)의 첫 번째 요청은 CE1(컴퓨터 엔진(865))에 관한 것이다. 두 번째 요청은 CE2(컴퓨터 엔진(875))에 관한 것이다. 마지막 CE인 CEm(컴퓨터 엔진(895))에 도달하면 클라이언트(응용프로그램 VM(895))는 다시 CE1에서 시작한다.

[0371] 시스템(800)에서 모든 클라이언트(예를 들어 응용프로그램 플랫폼(820, 830, 840, 850))는 통신해야 하는 모든

서버(예를 들어 사용 가능한 컴퓨터 엔진 세트)를 인지하고 있다. 각 클라이언트는 각각의 서버에 라운드 로빈 요청을 수행하므로 모든 서버에 작업로드를 균등하게 분산하는 이점이 있다. 특정 실시예에서 도 7에 도시된 CMS(700)의 로드 밸런서(710, 711, 712, 713, 714, 715, 716, 717, 718, 719)는 컴퓨터 엔진에 작업로드를 균등하게 분배하기 위해 라운드 로빈 요청을 컴퓨터 엔진에 걸쳐 전송할 수 있다.

[0372] 도 9는 본 발명의 실시형태와 일치하는 작업로드에 기반한 요청으로 확장 가능하고 안전한 CMS를 구현하기 위한 시스템(900) 실시예의 블록도이다. 간결성을 위해 도 7 및 8과 비교하여 도 9에서 발생하는 차이점만이 하기에 개시되어 있다.

[0373] 도 8에서와 같이 단순화 및 명료화를 위해 응용프로그램 플랫폼(예: VM 및/또는 하드웨어 플랫폼) 및 컴퓨터 엔진(925, 935, 945, 955)의 한 세트(920, 930, 940, 950) 만을 도 9에 나타내었다. 도 9 내의 응용프로그램 플랫폼(예: VM 및/또는 하드웨어 플랫폼) 및 컴퓨터 엔진(925, 935, 945, 955)은 도 7을 참고하여 개시된 임의의 등록 권한(720), 등재 인증 권한(730), 가명 인증 권한(740) 및 연결 권한(750, 760)을 구현하기 위해 사용된다.

[0374] 도 7의 시스템(900)과 같이 시스템(900)에서 HSM을 필요로 하는 모든 암호화 작동은 컴퓨터 엔진에서 수행되고 응용프로그램 플랫폼(예를 들면 VM 및/또는 하드웨어 플랫폼) 및 컴퓨터 엔진은 모두 독립적으로 확장된다.

[0375] 계속해서 도 9를 참조하면 사용되는 개별 서버의 작업로드를 먼저 쿼리하는 지능을 추가함으로써 작업로드 분산 기술이 가능하다. 작업로드 분산 기술은 사용 가능한 개별 서버(예를 들면 개별 컴퓨터 엔진)의 작업로드에 대한 지식을 사용한다는 점에서 작업로드-기반이다.

[0376] 시스템(900)에서 전송된 요청은 사용 가능한 컴퓨터 엔진(예를 들면 컴퓨터 엔진(925, 935, 945, 955))에 대한 현재 작업로드의 정보를 사용하여 해당 컴퓨터 엔진 세트에 전송된 요청 및 메시지를 분배한다. 시스템(900)에서 컴퓨터 엔진 각각의 리포트된 개별 작업로드에 기반하여 요청이 컴퓨터 엔진으로 전송된다.

[0377] 시스템(900) 내에서 작업로드-기반 요청을 명확하게 설명하기 위해 응용프로그램 VM(950)에 각각의 작업로드를 리포트 하는 컴퓨터 엔진(965, 975, 985, 995)의 확장된 세트를 나타내었다. 도 9의 실시예에서 "m"은 응용프로그램 플랫폼의 수이고 "n"은 작업로드를 리포트 하는 컴퓨터 엔진의 수이다.

[0378] 도 9의 실시예에서 작업로드는 백분율로 리포트 되며 여기서 컴퓨터 엔진(975)에 대한 30 % 작업로드는 컴퓨터 엔진(975)이 현재 총 용량의 30 %로 실행되고 있음을 나타낸다. 이와 유사하게 컴퓨터 엔진(965, 985 및 995)에서 리포트 된 80 %의 작업로드는 이러한 컴퓨터 엔진이 현재 총 용량의 80 %로 각각 실행되고 있음을 나타낸다.

[0379] 특정 실시형태에서 특정 컴퓨터 엔진이 리포트 하는 현재의 작업로드는 해당 컴퓨터 엔진에 내장된 HSM의 작업로드를 나타낸다. 예를 들어 컴퓨터 엔진의 처리 용량이 암호화 작동을 수행하기 위한 HSM의 용량에 의해 제한되거나 한정되는 경우, 컴퓨터 엔진에서 리포트 하는 작업로드 백분율은 HSM의 현재 작업로드를 반영할 수 있다. 예를 들어 컴퓨터 엔진(975)에 의해 사용되는 HSM이 처리 용량의 30 %로 실행되고 있다면, 컴퓨터 엔진(975)은 전체 용량의 30 %로 실행되고 있다고 리포트 할 수 있다.

[0380] 일부 실시형태에서 작업로드 백분율은 서버(예: 컴퓨터 엔진)의 처리 용량, 통신 용량(예: 직접 통신 연결 또는 무선 모듈에 대한 가용 대역폭 측정) 및 스토리지/메모리 용량의 가중 측정일 수 있다. 실시예에서 처리, 통신 및 메모리 용량에 동일한 1/3 가중치가 주어질 수 있다.

[0381] 이러한 실시예에서 컴퓨터 엔진(975)이 중앙처리장치(CPU) 용량의 25 %, 통신 용량의 35 %, 사용 가능한 메모리 또는 스토리지의 30 %를 사용하는 경우에 컴퓨터 엔진(975)은 그의 작업로드가 30 %라고 리포트 한다.

[0382] 특정 실시형태에서 컴퓨터 엔진에 대한 환경 측정은 가중치가 부여되고 작업로드 측정과 결합하여 고려될 수 있다. 예를 들어 컴퓨터 엔진의 전체 상태 측정은 컴퓨터 엔진의 작업로드 측정과 함께 결정되고 리포트 될 수 있다.

[0383] 일부 실시예에서 주어진 컴퓨터 엔진에 대한 상태 측정은 컴퓨터 엔진의 작동 온도(예: 열 센서의 평균 온도 판독 값보다 높으면 CPU, 메모리 모듈 또는 디스크 드라이브가 열 종료 또는 오작동에 취약함을 나타낼 수 있음); 컴퓨터 엔진 인클로저 내부의 습도 수준; 재시작 또는 재부팅 빈도(예: 과열 또는 충돌); 최근 재시작 이후 시간; 최근 기간(예: 이전 일, 주 또는 월)의 여러 디스크 오류 또는 메모리 오류; 컴퓨터 엔진에 대한 예정된 유지 보수 이벤트(예: 소프트웨어 또는 펌웨어 업데이트, 결함을 지닌 하드웨어 컴포넌트 교체)까지의 시간; 컴퓨터 엔진이 백업 전원 공급장치에서 실행 중임을 나타내는 표시; 또는 컴퓨터 엔진의 전원 공급장치에 대한 최근

정전 또는 전압 감소 이후의 기간; 중 하나 이상의 함수일 수 있다.

[0384] 추가적 또는 대안적인 실시형태에서 컴퓨터 엔진에 대한 작업로드를 결정하기 위해 다른 가중치, 측정 값 및 메트릭이 사용될 수 있다. 예를 들어 암호화 작동을 수행하는 컴퓨터 엔진이 통신 또는 메모리 용량보다 CPU 용량에 의해 과거에 더 많은 제약을 받았다면 해당 컴퓨터 엔진의 전체 작업로드 백분율을 결정할 때 다른 용량보다 CPU 용량에 더 큰 가중치가 부여될 수 있다.

[0385] 시스템(900)에서 컴퓨터 엔진에 요청을 생성하고자 하는 클라이언트(예를 들어 응용프로그램 VM(995))는 컴퓨터 엔진에 의해 리포트 된 작업로드에 기반한다. 도 9의 실시예에서 응용프로그램 VM(995)으로부터의 다음 요청은 30 %의 비교적 낮은 작업로드에 기반한 CE2(컴퓨터 엔진(975))에 대한 것이다. 즉 컴퓨터 엔진(975)이 컴퓨터 엔진 세트(965, 975, 985, 995) 중 가장 낮은 작업로드를 지니기 때문이다.

[0386] 이후 요청이 응용프로그램 VM(995)에서 컴퓨터 엔진으로 전송될 때 현재 모두 동일한 80 % 작업로드를 리포트하므로 CE1(컴퓨터 엔진(965)), CE3(컴퓨터 엔진(985)) 또는 CEm(컴퓨터 엔진(995)) 중 하나가 사용될 수 있다.

[0387] 사용 가능한 각각의 컴퓨터 엔진이 동일하거나 유사한 작업로드를 리포트 하는 경우에는 순차적 요청을 사용하여 동일한 로드의 컴퓨터 엔진에 작업로드를 균등하게 분배시킬 수 있다. 즉 사용 가능한 각각의 컴퓨터 엔진이 실질적으로 동일하거나 균등한 작업로드를 리포트 하는 경우, 도 8을 참조하여 상기에서 설명한 요청이 사용될 수 있다. 시간이 지남에 따라 작업로드가 변경되면 클라이언트(응용프로그램 VM(995))는 사용 가능한 최소-로드 컴퓨터 엔진에 후속 요청을 전송한다.

[0388] 시스템(900)에서 모든 클라이언트(예를 들어 응용프로그램 플랫폼(920, 930, 940, 950))은 통신해야 하는 모든 서버(예를 들어 사용 가능한 컴퓨터 엔진 세트)의 작업로드를 알고있다. 각각의 클라이언트는 각 서버에 작업로드 쿼리를 제출하고 리포트 된 작업로드를 사용하여 모든 서버에 작업로드를 균등하게 분산할 수 있다. 특정 실시형태에서 도 7에 나타난 CMS(700)의 로드 밸런서(710, 711, 712, 713, 714, 715, 716, 717, 718, 719)는 컴퓨터 엔진에 작업로드-기반 요청을 전송하여 컴퓨터 엔진에 작업로드를 균등하게 분배시킬 수 있다.

[0389] 도 10a 및 10b는 본 발명의 실시형태에 따른 확장 가능하고 보안적인 인증서 관리 시스템(CMS)(400)을 구현하기 위한 예시적인 아키텍처의 블록도이다. 간결성을 위해 도 4a 및 4b와 비교하여 도 10a 및 10b 내에서 발생하는 차이점 만이 하기에 개시되어 있다.

[0390] 도 10a의 실시예에 나타난 바와 같이 CMS(1000)의 아키텍처는 별도의 서버에서 바람직하게 구현되는 2 개의 프로비저닝 제어기(1002)(프라이머리 및 예비)를 포함할 수 있다. 2 개의 프로비저닝 제어기(1002)는 각각 도 4a 및 6a의 프로비저닝 제어기(120 및 602)와 유사한 기능을 포함한다. 즉 프라이머리 프로비저닝 제어기에 포함된 객체, 데이터 등은 도 4a를 참조하여 개시한 바와 같이 장애 복구 목적을 위해 예비(세컨더리) 프로비저닝 제어기에 복사되거나 포함된다.

[0391] 도 10a 및 10b에 도시된 바와 같이 CMS(1000)의 아키텍처는 REST 웹 서비스로 구현된 등록 권한(1005), 등록 권한(1020), 컴퓨터 엔진(1025, 1035, 1045, 1050, 1060, 메시지 큐 1010, 1012, 1014, 1016, 1018) 및 데이터베이스(1070)를 포함한다.

[0392]

[0393] CMS(1000)의 실시예는 사설 데이터 센터, 클라우드 데이터 센터 또는 사설 및 클라우드 데이터 센터의 혼성화로 구현될 수 있다. CMS(1000)의 다양한 실시형태는 매우 높은 볼륨의 디바이스 트랜잭션 및 인증서 생성 처리에 사용될 수 있다. 다양한 실시형태에서 CMS(1000)는 다중 서버, HSM, 및 응용프로그램 플랫폼 역할을 하는 다중 컴퓨터 또는 컴퓨터 엔진을 사용하여 구현될 수 있다. 즉 도 10a 및 10b에 나타난 바와 같이 등록 권한, 인증 권한 및 연결 권한에 대해 기술된 응용프로그램은 소프트웨어 응용프로그램을 호스팅하고 실행할 수 있는 하나 이상의 컴퓨터 엔진을 각각 실행한다.

[0394] CMS(1000)은 응용프로그램을 호스팅하고 실행하기 위해 컴퓨터 엔진(1025, 1035, 1045, 1050, 1060)을 사용하는 차이점을 제외하고는 도 4a 및 4b를 참조하여 상기에 개시된 CMS(400)와 유사하다. 즉 CMS(1000) 아키텍처는 CMS(400) 아키텍처의 대안으로 등록 권한, 등재 인증 권한, 가명 인증 권한 및 연결 권한에 대한 응용프로그램이 자체의 전용 컴퓨터 엔진(1025, 1035, 1045, 1050 및 1060) 상에서 실행된다.

[0395] CMS(1000)에서 HSM을 필요로 하는 모든 암호화 작동은 관련 응용프로그램 또한 실행하는 컴퓨터 엔진(예: 컴퓨터 엔진 1025, 1035, 1045, 1050 및 1060)에서 수행된다. 유리하게는 컴퓨터 엔진(1025, 1035, 1045, 1050, 1060)에서 응용프로그램 및 암호화 작업을 실행함으로써 CMS(1000)의 아키텍처는 필요한 메시지 큐의 수를 감소

시킨다.

[0396] 도 10a 및 10b의 실시예에서 컴퓨터 엔진은 등록 권한 응용프로그램을 호스팅하고 실행하는 등록 권한 컴퓨터 엔진(1025), 등재 인증 권한 응용프로그램을 호스팅하고 실행하도록 작동 가능한 등재 인증 권한 컴퓨터 엔진(1035), 가명 인증 권한 응용프로그램을 호스팅하고 실행하도록 작동 가능한 가명 인증 권한 컴퓨터 엔진(1045), 연결 권한 1 응용프로그램을 호스팅하고 실행하는 연결 권한 1 컴퓨터 엔진(1050) 및 연결 권한 2 응용프로그램을 호스팅하고 실행하도록 작동 가능한 연결 권한 2(1060)를 포함한다.

[0397] 도 10a 및 10b에 나타난 바와 같이 등록 권한(1005)은 입력 메시지 큐(1010, 1012, 1014, 1016, 1018)를 포함하는 메시지 서브 시스템 또는 메시지 큐 서비스에 의해 다른 컴포넌트에 상호 연결된다.

[0398] 도 10a 및 10b의 예시적인 실시형태에서 입력 메시지 큐(1010, 1012, 1014, 1016, 1018)는 이들 큐의 메시지가 한 방향으로(예를 들어 클라이언트에서 서버로) 전달된다는 점에서 하나의 방향이다. 이는 각각의 컴퓨터 엔진에 대해 단일 입력 큐를 보유함으로써 단순성의 기술적 이점을 제공한다.

[0399] 입력 메시지 큐(1010, 1012, 1014, 1016, 1018)를 사용하여 컴퓨터 엔진을 서로 통신 가능하게 연결함으로써 필요에 따라 컴퓨터 엔진을 독립적으로 확장시킬 수 있다. 즉 등록 권한, 등재 인증 권한, 가명 인증 권한 및 연결 권한 응용프로그램에 대한 응용프로그램 플랫폼 역할을 하는 각각의 컴퓨터 엔진이 각각의 입력 메시지 큐를 통해 통신 가능하게 연결되므로 CMS(1000)의 이러한 컴포넌트와 데이터베이스(1070)는 모두 서로 독립적으로 확장된다.

[0400] 도 11은 본 발명의 실시형태와 일치하는 시스템 및 방법을 구현하기 위해 사용될 수 있는 컴퓨터 시스템(1100)을 포함하는 컴퓨터 환경(1101) 실시예의 블록도이다. 다른 컴포넌트 및/또는 배열 또한 사용될 수 있다.

[0401] 일부 실시형태에서 다른 것 보다도 프로비저닝 제어기(120), DAMS(110), 도 4 및 도 6 내지 도 10의 CMS 아키텍처의 컴퓨터 엔진 및 도 7의 로드 밸런서(710-719)와 같은 도 1 내지 도 10의 다양한 컴포넌트를 적어도 부분적으로 구현하기 위해 컴퓨터 시스템(1100)이 사용될 수 있다.

[0402] 일부 실시형태에서 컴퓨터 시스템(1100)과 유사한 일련의 컴퓨터 시스템은 네트워크(1135)를 통해 서로 통신할 수 있는 도 1 내지 도 10의 컴포넌트 중 하나를 구현하기 위해 특수 하드웨어로 각각 맞춤화 및/또는 특수 서버로 프로그래밍될 수 있다.

[0403]

[0404] 도 11에 나타난 실시예에서 컴퓨터 시스템(1100)은 CPU(1105), 메모리(1110), 입/출력(I/O) 디바이스(1125), 하드웨어 보안 모듈(HSM)(1140) 및 비휘발성 저장장치(1120)와 같은 다수의 컴포넌트를 포함한다. 시스템(1100)은 다양한 방식으로 구현될 수 있다. 예를 들어 통합 플랫폼(예를 들면 서버, 워크 스테이션, 개인용 컴퓨터, 랩톱 등)으로서의 실시형태는 CPU(1105), 메모리(1110), 비휘발성 저장장치(1120) 및 I/O 디바이스(1125)를 포함할 수 있다.

[0405] 이러한 구성에서 컴포넌트(1105, 1110, 1120 및 1125)는 로컬 데이터 버스를 통해 연결 및 통신할 수 있으며 외부 I/O 연결을 통해 데이터 저장소(1130)(예를 들면 별도의 데이터베이스 시스템으로 구현됨)에 액세스할 수 있다. I/O 컴포넌트(1125)는 직접 통신 연결(예: 유선 또는 로컬 Wi-Fi 연결), 근거리 통신망(LAN) 또는 광역 네트워크(WAN, 예를 들어 셀룰러 전화 네트워크 또는 인터넷)와 같은 네트워크 및/또는 다른 적절한 접속을 통해 외부 디바이스에 연결할 수 있다. 시스템(1100)은 독립형이거나 더 큰 시스템의 서브 시스템일 수도 있다.

[0406] CPU(1105)는 캘리포니아주 산타 클라라의 Intel™ 코퍼레이션에서 제조된 Core™ 제품군의 마이크로프로세서 또는 캘리포니아주 서니베일의 AMD™ 코퍼레이션에서 제조된 Athlon™ 제품군의 마이크로프로세서와 같은 하나 이상의 공지된 프로세서 또는 프로세싱 디바이스일 수 있다. 메모리(1110)는 본 발명의 실시형태와 관련된 소정의 기능, 방법 및 프로세스를 수행하기 위해 CPU(1105)에 의해 실행되거나 사용되는 명령어 및 정보를 저장하도록 형상화된 하나 이상의 고속 저장장치일 수 있다. 저장장치(1120)는 휘발성 또는 비휘발성, 자기, 반도체, 테이프, 광학 또는 다른 유형의 저장장치 또는 장기-저장을 위한 CD 및 DVD 및 고형상 디바이스와 같은 디바이스를 포함하는 컴퓨터 판독 가능 매체일 수 있다.

[0407] 예시된 실시형태에서 메모리(1110)는 스토리지(1120) 또는 원격 시스템(도시되지 않음)으로부터 로드된 하나 이상의 프로그램 또는 응용프로그램(1115)을 포함하며 이는 CPU(1105)에 의해 실행될 때 본 발명과 일치하는 다양한 작동 절차 프로세스 또는 방법을 수행한다.

[0408]

[0409] 대안적으로 CPU(1105)는 시스템(1100)으로부터 원격 위치한 하나 이상의 프로그램을 실행할 수 있다. 예를 들어 시스템(1100)은 네트워크(1135)를 통해 하나 이상의 원격 프로그램에 액세스할 수 있으며 이는 실행시 본 발명의 실시형태와 관련된 기능 및 프로세스를 수행한다.

[0410]

[0411] 하나의 실시형태에서 메모리(1110)는 프로비저닝 제어기(120), DAMS(110) 및/또는 분배기 어플라이언스(118, 131)에 대해 본 명세서에서 설명된 특수 기능 및 작동을 수행하기 위한 프로그램(1115)을 포함할 수 있다. 일부 실시형태에서 메모리(1110)는 또한 본 발명에 부수적인 기능을 제공하는 다른 방법 및 프로세스를 구현하는 다른 프로그램 또는 응용프로그램을 포함할 수 있다.

[0412] 메모리(1110)는 CPU(1105)에 의해 실행될 때 당업계에 공지된 다수의 기능을 수행하는 운영체제(나타내지 않음) 및/또는 본 발명과 관련되지 않은 다른 프로그램(나타내지 않음)으로 구성될 수 있다. 운영 체제는 Microsoft Windows™, Unix™, Linux™, Apple Computers™ 운영체제 또는 기타 운영체제일 수 있다. 운영체제의 선택과 운영체제의 사용은 본 발명에 중요하지 않다.

[0413] HSM(1140)은 디지털 보안 자산을 보안 생성 및 저장하고 다양한 암호화 및 민감한 연산을 보안 수행하는 자체 프로세서를 지닌 디바이스일 수 있다. HSM(1140)은 암호화 키와 같은 디지털 보안 자산 및 기타 민감한 데이터를 침입자가 액세스할 수 없도록 보호한다. 일부 실시형태에서 HSM은 컴퓨터 시스템(1100)에 직접 부착되는 플러그인 카드 또는 보드일 수 있다.

[0414] I/O 디바이스(1125)는 데이터를 시스템(1100)에 의해 수신 및/또는 송신될 수 있게 하는 하나 이상의 입력/출력 디바이스를 포함할 수 있다. 예를 들어 I/O 디바이스(1125)는 사용자로부터 데이터를 입력할 수 있는 키보드, 터치 스크린, 마우스 등과 같은 하나 이상의 입력 디바이스를 포함할 수 있다. 또한 I/O 디바이스(1125)는 데이터를 출력하고 사용자에게 제공할 수 있는 디스플레이 화면, CRT 모니터, LCD 모니터, 플라즈마 디스플레이, 프린터, 스피커 디바이스 등과 같은 하나 이상의 출력 디바이스를 포함할 수 있다.

[0415] 또한 I/O 디바이스(1125)는 컴퓨터 시스템(1100)이 예를 들어 다른 기계 및 디바이스와 디지털 방식으로 통신할 수 있게 하는 하나 이상의 디지털 및/또는 아날로그 통신 입력/출력 디바이스를 포함할 수 있다. 다른 구성 및/또는 입력 및/또는 출력 디바이스의 수는 I/O 디바이스(1125)에 통합될 수 있다.

[0416] 나타난 실시형태에서 시스템(1100)은 네트워크(1135)(예: 인터넷, 사설 네트워크, 가상 사설 네트워크, 셀룰러 네트워크 또는 기타 네트워크 또는 이들의 조합)에 연결되며, 이는 차례로 다양한 시스템 및 서버, 개인용 컴퓨터, 랩톱 컴퓨터, 클라이언트 디바이스 등과 같은 컴퓨터 기계에 연결될 수 있다. 일반적으로 시스템(1100)은 외부 기계 및 디바이스로부터 데이터를 입력하고 네트워크(1135)를 통해 외부 기계 및 디바이스로 데이터를 출력할 수 있다.

[0417] 도 11에 나타난 예시적인 실시형태에서 데이터 소스(1130)는 데이터베이스(125)와 같은 시스템(1100) 외부의 독립형 데이터베이스이다. 다른 실시형태에서 데이터 소스(1130)는 시스템(1100)에 의해 호스팅 될 수 있다. 다양한 실시형태에서 데이터는 소스(1130)는 본 발명에 따른 시스템 및 방법을 구현하는 데 사용되는 데이터를 관리하고 저장할 수 있다. 예를 들어 데이터 소스(1130)는 시스템(110)에 의해 프로비저닝 되는 각각의 디바이스(116)에 대한 상태 및 로그 정보를 포함하는 데이터 구조를 관리 및 저장할 수 있다.

[0418] 데이터 소스(1130)는 정보를 저장하고 시스템(1100)을 통해 액세스 및/또는 관리되는 하나 이상의 데이터베이스를 포함할 수 있다. 예를 들어 데이터베이스(1130)는 Oracle™ 데이터베이스, Sybase™ 데이터베이스 또는 다른 관계형 데이터베이스일 수 있다. 그러나 본 발명과 일치하는 시스템 및 방법은 별도의 데이터 구조 또는 데이터베이스로 심지어 데이터베이스 또는 데이터 구조의 사용으로 제한되지 않는다.

[0419] 당업자는 도 11 내의 시스템 컴포넌트 및 실시형태 세부 사항이 설명의 간결성과 명확성을 위해 제시된 실시예임을 인식할 것이다. 다른 컴포넌트 및 실시형태 세부 사항을 사용할 수 있다.

[0420] 전술한 실시예는 설명의 명확성을 위해 OBU, ECU 및 RSU와 같은 컴퓨터화 디바이스의 특정 실시예를 사용하였으나 본 발명은 이러한 특정 실시예에 한정되지 않는다. 본 발명과 일치하는 다양한 실시형태는 의료 기기(예를 들어 투석기, 주입 펌프 등); 로봇; 드론; 자율 주행 차량; 및 무선 통신 모듈(예: 내장 범용 집적 회로 카드(eUICC)) 등과 같은 다양한 컴퓨터화 디바이스와 함께 사용될 수 있다.

[0421] 본 명세서에 개시된 응용프로그램의 다양한 작동은 하나 이상의 VM에 의해 적어도 부분적으로 수행될 수 있다. 추가적 또는 대안적인 실시형태에서 본 명세서에 개시된 응용프로그램의 작동은 관련 작동을 수행하도록 (예를 들어 소프트웨어에 의해) 일시적으로 형상화 되거나 영구적으로 형상화 되는 하나 이상의 프로세서에 의해 적어도 부분적으로 수행될 수 있다. 일시적 또는 영구적으로 형상화 되는지 관계 없이 이러한 프로세서는 본 명세서에 개시된 하나 이상의 응용프로그램 작동, 기능 및 역할을 수행하도록 작동하는 프로세서-구현 모듈을 구성할 수 있다. 본 명세서에서 사용되는 용어 '프로세서 구현 모듈'은 하나 이상의 프로세서를 사용하여 구현된 하드웨어 모듈을 의미한다.

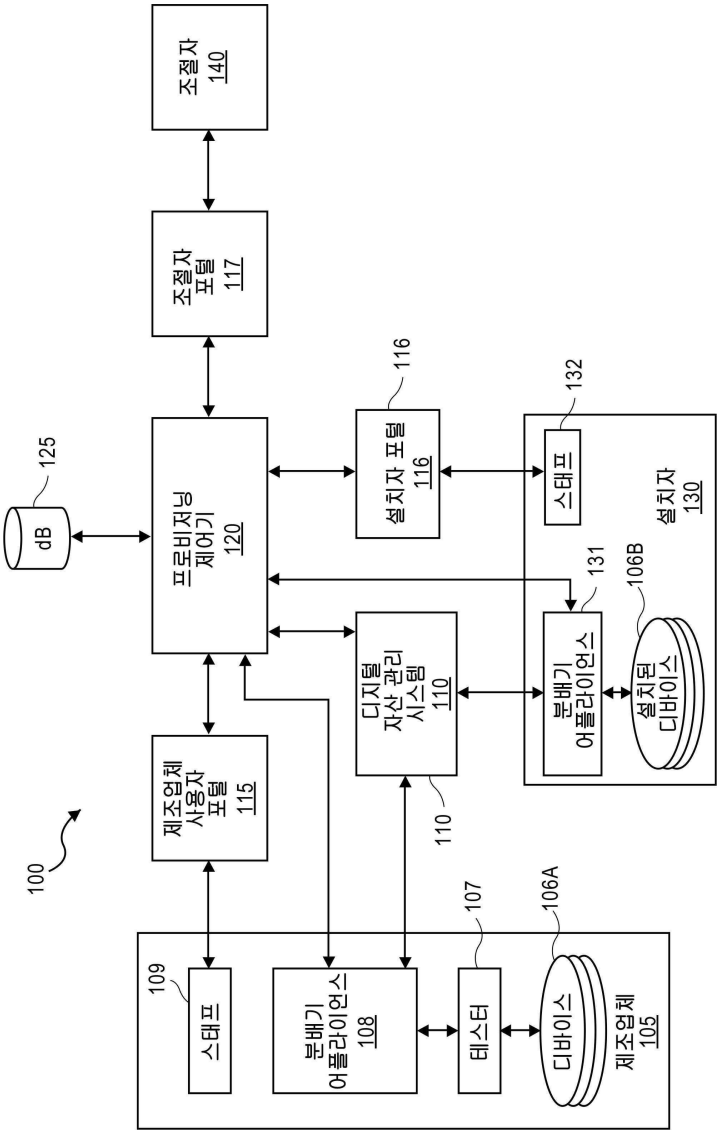
[0422] 유사하게 본 명세서에 개시된 방법은 하드웨어의 실시예인 특정 프로세서 또는 프로세서로 적어도 부분적으로 프로세서-구현될 수 있다. 예를 들어 방법의 작동 중 적어도 일부는 하나 이상의 프로세서 또는 프로세서-구현 모듈에 의해 수행될 수 있다. 또한 하나 이상의 프로세서는 '클라우드 컴퓨터' 환경에서 또는 '서비스로서의 소프트웨어(SaaS)'로 관련 작동의 성능을 지원하기 위해 작동할 수도 있다. 예를 들어 작동 중 적어도 일부는 컴퓨터 그룹(프로세서를 포함하는 머신의 실시예로서)에 의해 수행될 수 있으며 이러한 작동은 네트워크(예: 인터넷) 및 하나 이상의 적절한 인터페이스(예: API)를 통해 액세스 가능하다.

[0423] 특정 작업의 성능은 단일 컴퓨터 내에 존재할 뿐만 아니라 다수의 컴퓨터에 분배되어 프로세서 간에 분산될 수 있다. 일부 예시적인 실시형태에서 프로세서 또는 프로세서-구현 모듈은 단일 지리적 위치(예를 들어 사무실 환경, 제조 환경 또는 서버 팜 내)에 위치할 수 있다. 다른 예시적인 실시형태에서 프로세서 또는 프로세서-구현 모듈은 다수의 지리적 위치에 걸쳐 분산될 수 있다.

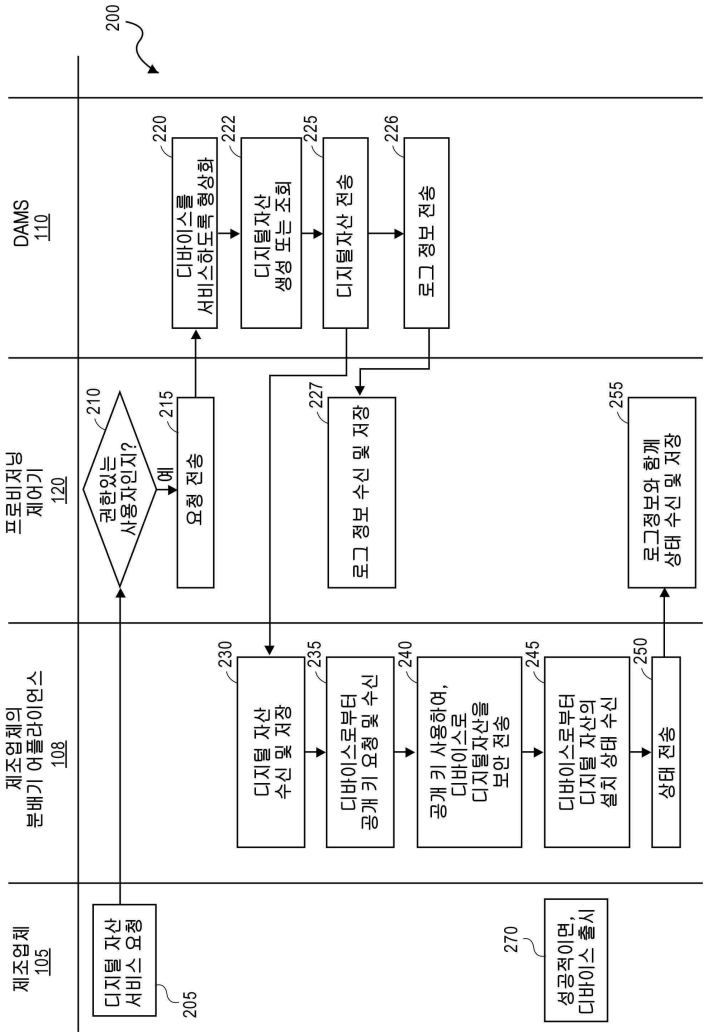
[0424] 본 발명의 또 다른 실시형태는 본 명세서에 개시된 본 발명의 명세서 및 실시를 고려함으로써 당업자에게 명백할 것이다. 명세서 및 실시예는 단지 예시적인 것으로 간주되며 본 발명의 진정한 범위는 하기 특허청구범위에 의해 표현된다.

도면

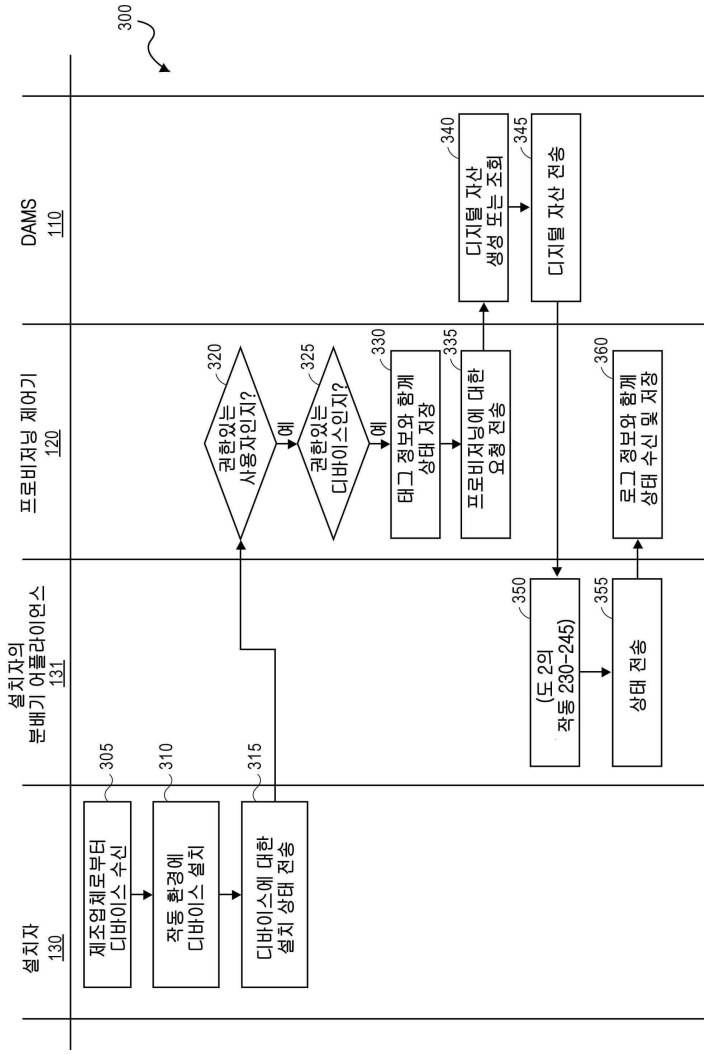
도면1


조절자
140
조절자
포털
117
프로비저닝
제어기
120
dB
125
제조업체
사용자
포털
115
100
설치자 포털
116
116
디지털
자산 관리
시스템
110
110
132
스태프
131
분배기
어플라이언스
106B
설치된
디바이스
설치자
130
107
106A
109
스태프
분배기
어플라이언스
108
테스터
디바이스
제조업체
105

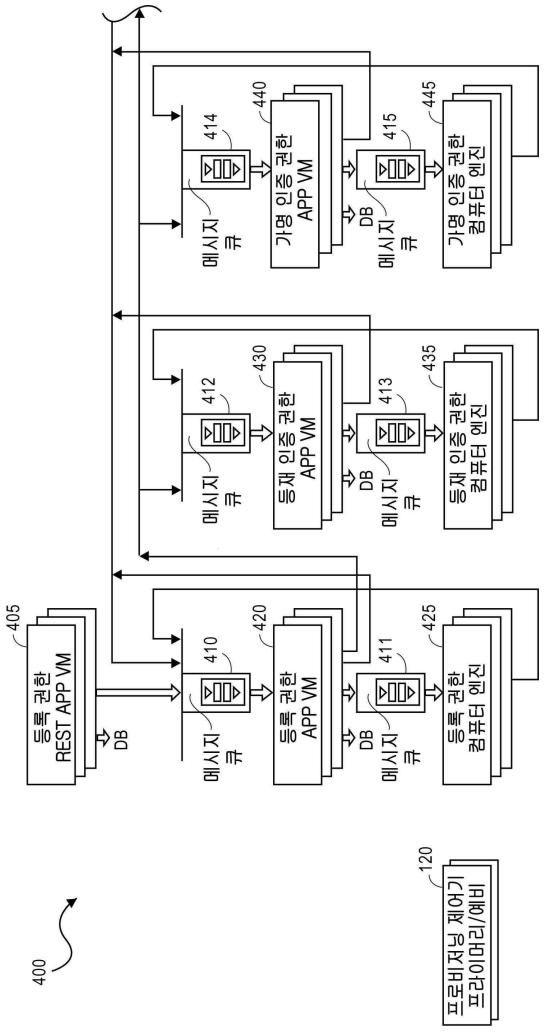
도면2


200
제조업체
105
디지털 자산
서비스 요청
205
제조업체의
분배기 어플라이언스
108
디지털 자산
수신 및 저장
230
디바이스로부터
공개 키 요청 및 수신
235
공개 키 사용하여,
디바이스로
디지털자산을
보안 전송
240
디바이스로부터
디지털 자산의
설치 상태 수신
245
상태 전송
250
프로비저닝
제어기
120
권한있는
사용자인지?
210
예
요청 전송
215
로그 정보 수신 및 저장
227
로그정보와 함께
상태 수신 및 저장
255
DAMS
110
디바이스를
서비스하도록 형상화
220
디지털자산
생성 또는 조회
222
디지털자산 전송
225
로그 정보 전송
226
성공적이면,
디바이스 출시
270

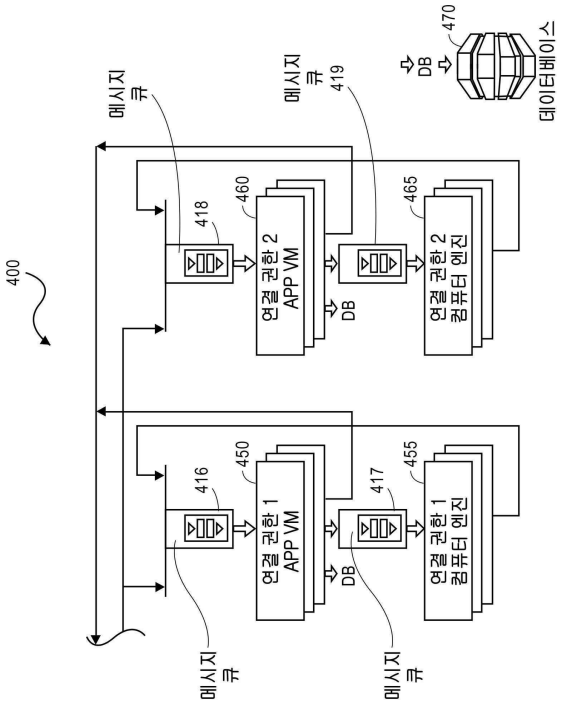
도면3


300
DAMS
110
프로비저닝 제어기
120
설치자의
분배기 어플라이언스
131
설치자
130
제조업체로부터
디바이스 수신
305
작동 환경에
디바이스 설치
310
디바이스에 대한
설치 상태 전송
315
권한있는
사용자인지?
320
예
권한있는
디바이스인지?
325
예
태그 정보와 함께
상태 저장
330
프로비저닝에 대한
요청 전송
335
디지털 자산
생성 또는 조회
340
디지털 자산 전송
345
(도 2의
작동 230-245)
350
상태 전송
355
로그 정보와 함께
상태 수신 및 저장
360

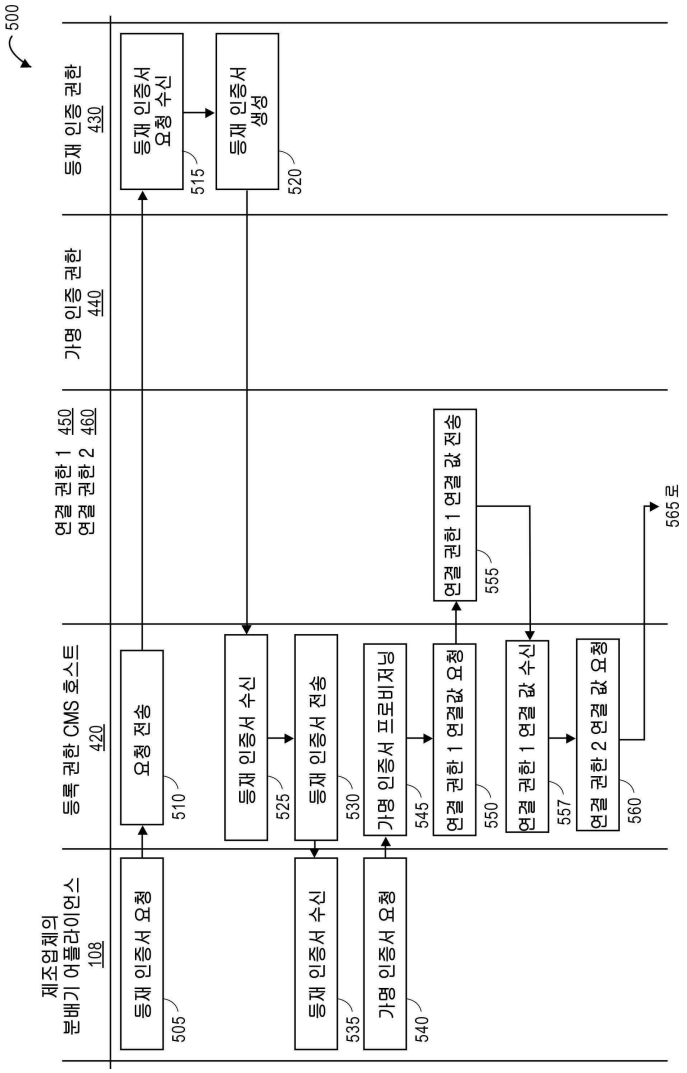
도면4a


400
405
등록 권한
REST APP VM
DB
410
메시지
큐
420
등록 권한
APP VM
DB
411
메시지
큐
425
등록 권한
컴퓨터 엔진
412
메시지
큐
430
등재 인증 권한
APP VM
DB
413
메시지
큐
435
등재 인증 권한
컴퓨터 엔진
414
메시지
큐
440
가명 인증 권한
APP VM
DB
415
메시지
큐
445
가명 인증 권한
컴퓨터 엔진
120
프로비저닝 제어기
프라이머리/예비

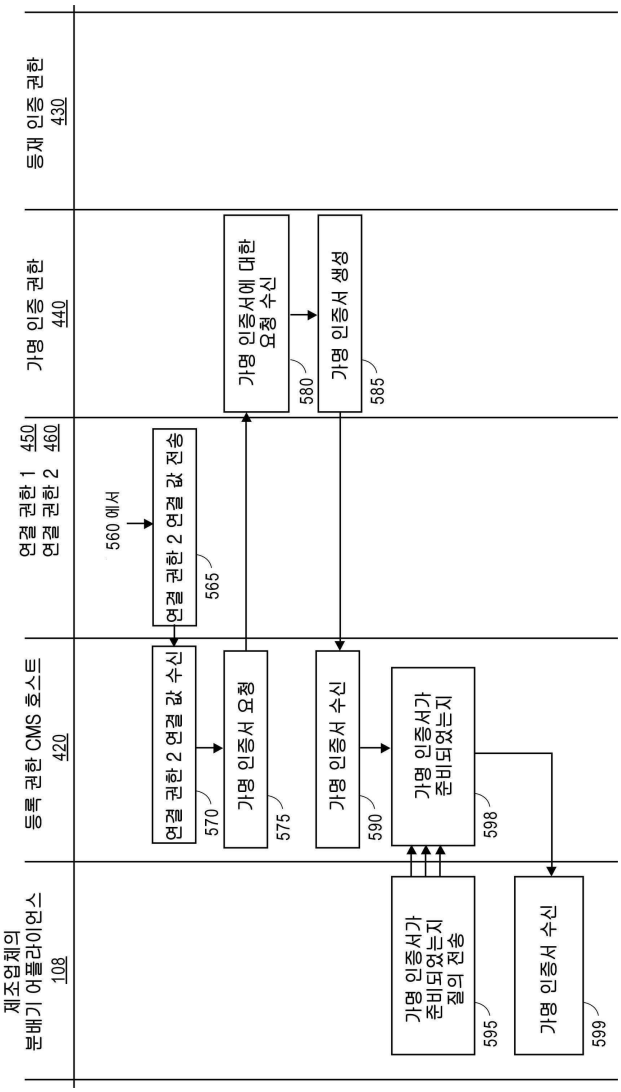
도면4b


400
메시지 큐
418
460
연결 권한 2 APP VM
DB
메시지 큐
419
465
연결 권한 2 컴퓨터 엔진
DB
470
데이터베이스
416
450
연결 권한 1 APP VM
메시지 큐
417
455
연결 권한 1 컴퓨터 엔진
DB
메시지 큐

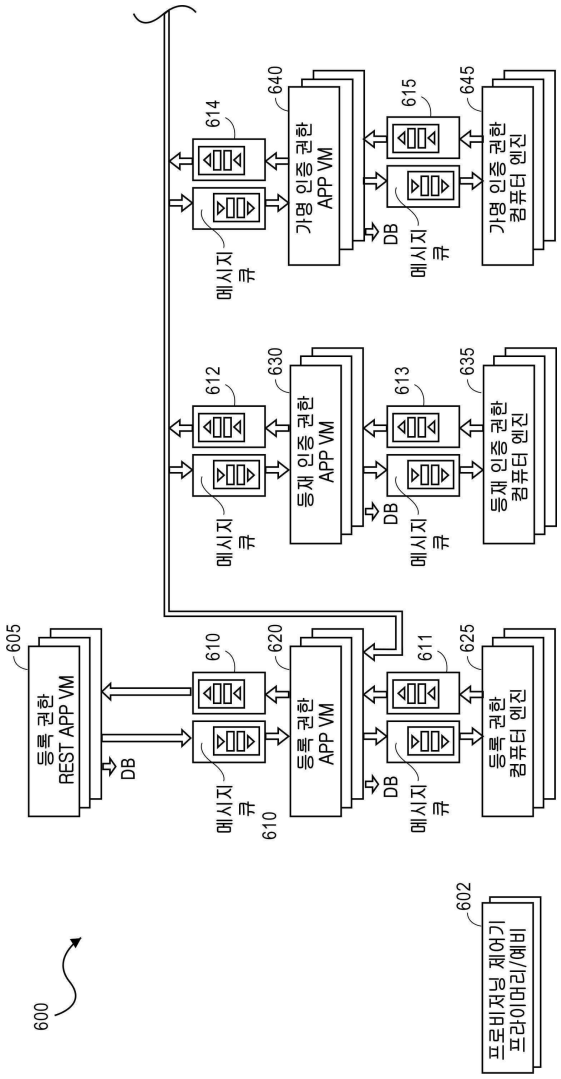
도면5a


500
제조업체의 분배기 어플라이언스 108
등록 권한 CMS 호스트 420
연결 권한 1 450
연결 권한 2 460
가명 인증 권한 440
등재 인증 권한 430
등재 인증서 요청
505
요청 전송
510
등재 인증서 요청 수신
515
등재 인증서 생성
520
등재 인증서 수신
525
등재 인증서 전송
530
등재 인증서 수신
535
가명 인증서 요청
540
가명 인증서 프로비저닝
545
연결 권한 1 연결값 요청
550
연결 권한 1 연결 값 전송
555
연결 권한 1 연결 값 수신
557
연결 권한 2 연결 값 요청
560
565로

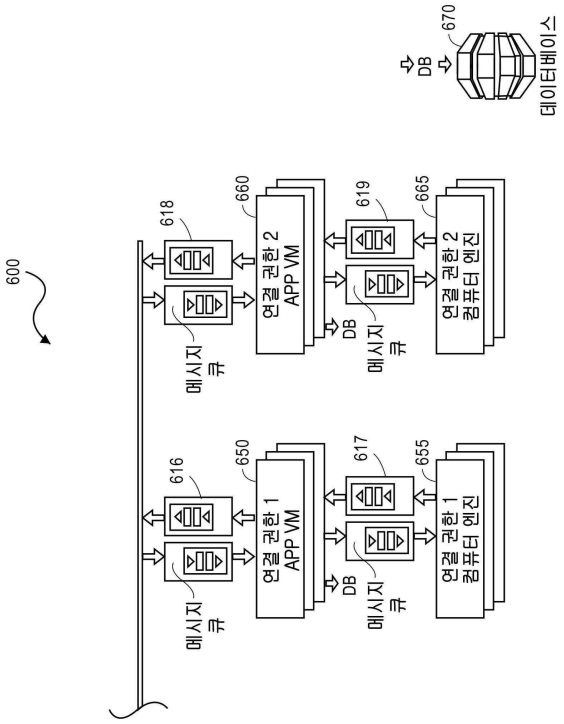
도면5b


제조업체의
분배기 어플라이언스
108
등록 권한 CMS 호스트
420
연결 권한 1
450
연결 권한 2
460
가명 인증 권한
440
등재 인증 권한
430
560 에서
연결 권한 2 연결 값 전송
565
연결 권한 2 연결 값 수신
570
가명 인증서 요청
575
가명 인증서에 대한
요청 수신
580
가명 인증서 수신
590
가명 인증서 생성
585
가명 인증서가
준비되었는지
598
가명 인증서가
준비되었는지
질의 전송
595
가명 인증서 수신
599

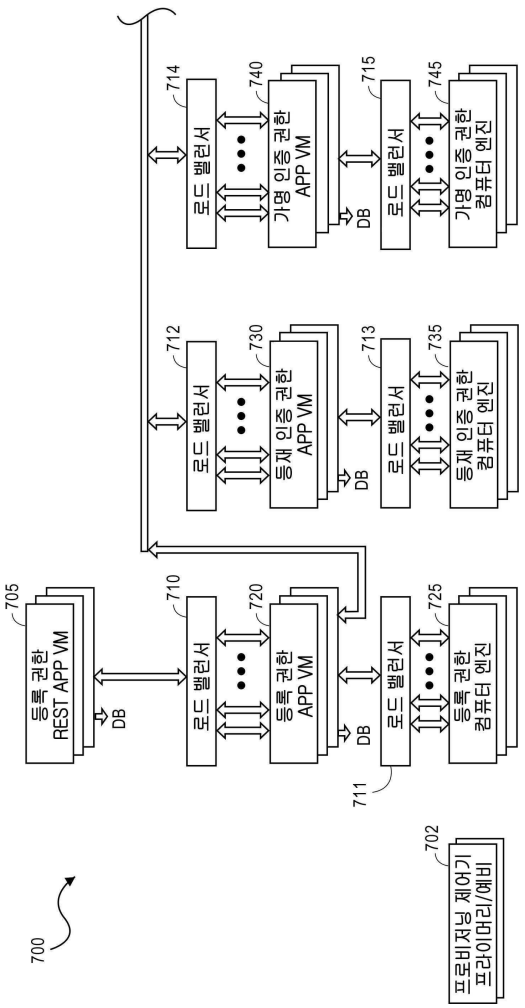
도면6a


600
602
프로비저닝 제어기
프라이머리/예비
605
등록 권한
REST APP VM
610
611
620
625
등록 권한
APP VM
등록 권한
컴퓨터 엔진
612
613
630
635
등재 인증 권한
APP VM
등재 인증 권한
컴퓨터 엔진
614
615
640
645
가명 인증 권한
APP VM
가명 인증 권한
컴퓨터 엔진
DB
메시지
큐

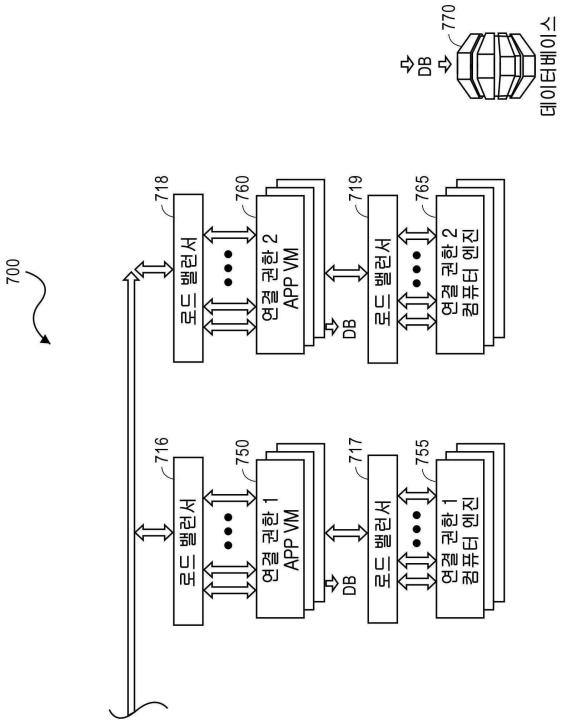
도면6b


600
618
660
연결 권한 2
APP VM
메시지
큐
619
665
연결 권한 2
컴퓨터 엔진
DB
메시지
큐
616
650
연결 권한 1
APP VM
메시지
큐
617
655
연결 권한 1
컴퓨터 엔진
DB
메시지
큐
670
DB
데이터베이스

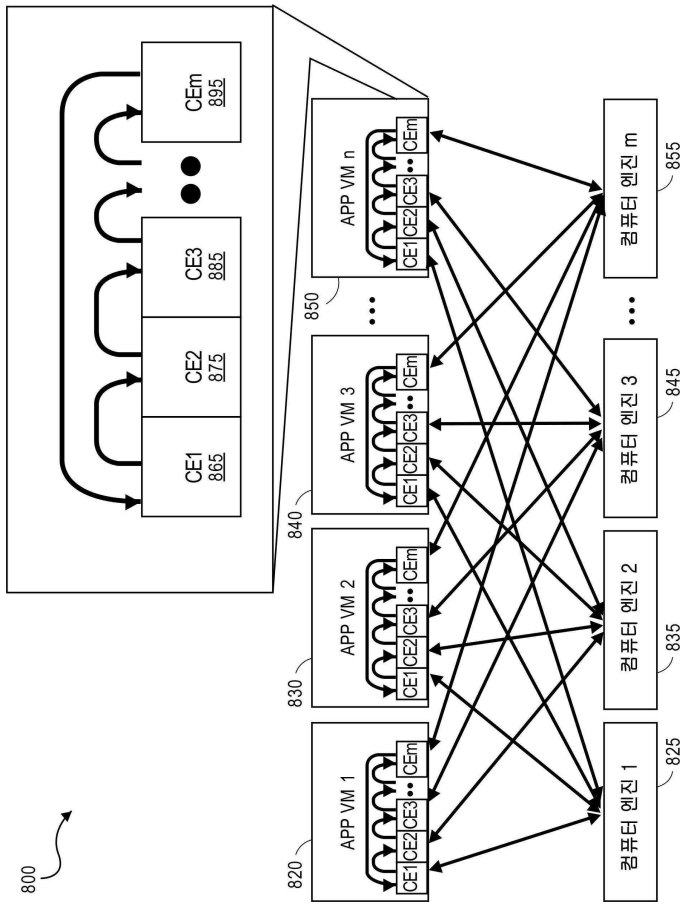
도면7a


700
705
등록 권한
REST APP VM
DB
710
로드 밸런서
720
등록 권한
APP VM
DB
711
로드 밸런서
725
등록 권한
컴퓨터 엔진
712
로드 밸런서
730
등재 인증 권한
APP VM
DB
713
로드 밸런서
735
등재 인증 권한
컴퓨터 엔진
714
로드 밸런서
740
가명 인증 권한
APP VM
DB
715
로드 밸런서
745
가명 인증 권한
컴퓨터 엔진
702
프로비저닝 제어기
프라이머리/예비

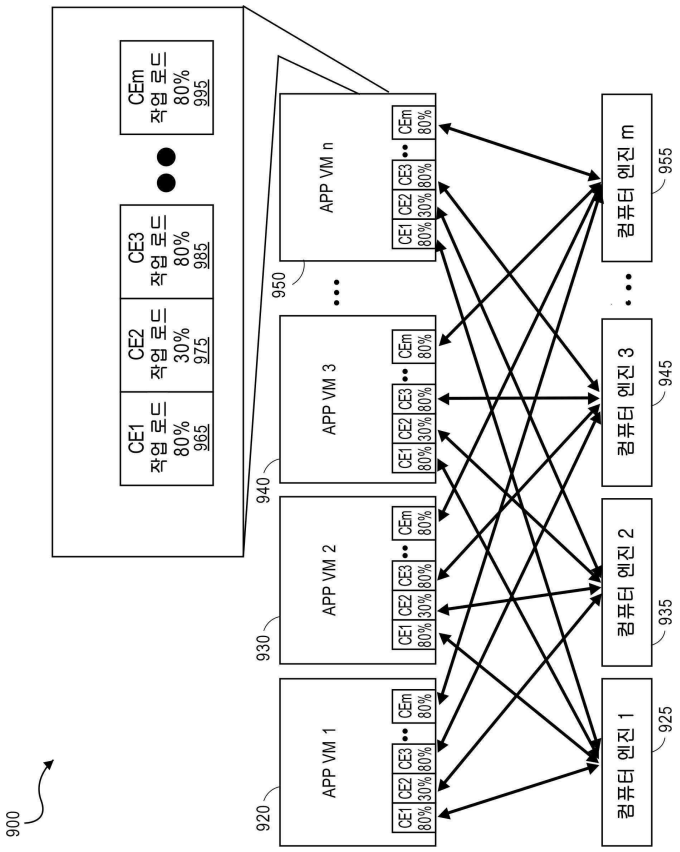
도면7b


700
718
로드 밸런서
760
연결 권한 2
APP VM
719
로드 밸런서
765
연결 권한 2
컴퓨터 엔진
DB
770
데이터베이스
716
로드 밸런서
750
연결 권한 1
APP VM
717
로드 밸런서
755
연결 권한 1
컴퓨터 엔진
DB

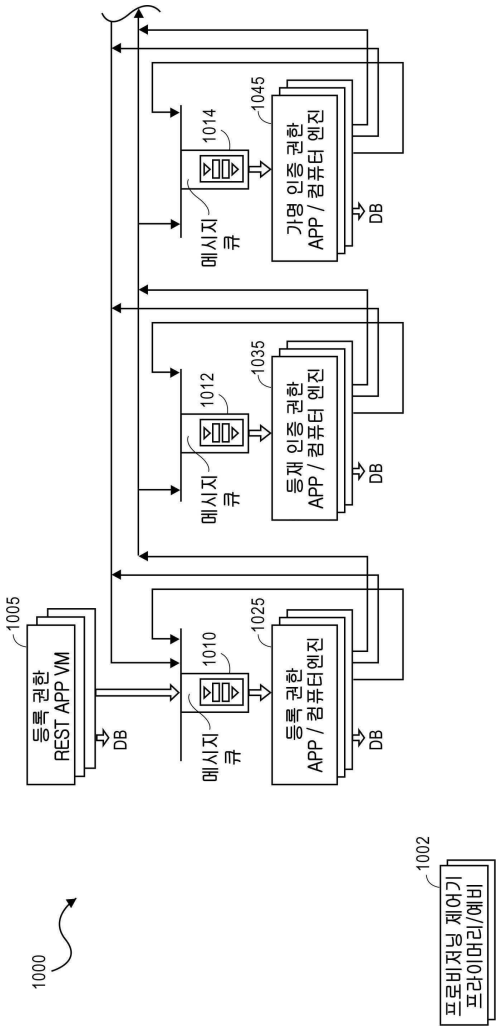
도면8


800
820
APP VM 1
CE1
CE2
CE3
CEm
830
APP VM 2
840
APP VM 3
850
APP VM n
CE1 865
CE2 875
CE3 885
CEm 895
825
컴퓨터 엔진 1
835
컴퓨터 엔진 2
845
컴퓨터 엔진 3
855
컴퓨터 엔진 m

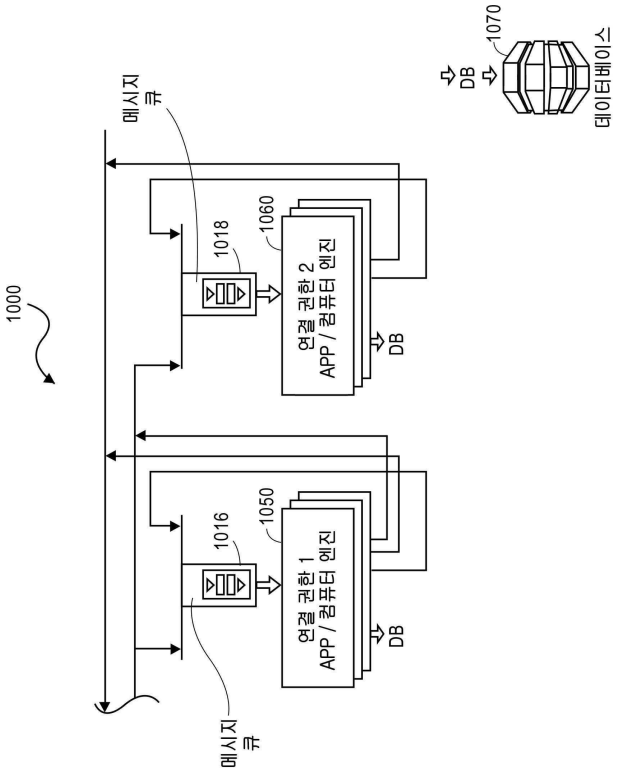
도면9


900
920
APP VM 1
CE1 80%
CE2 30%
CE3 80%
CEm 80%
930
APP VM 2
940
APP VM 3
950
APP VM n
925
935
945
955
컴퓨터 엔진 1
컴퓨터 엔진 2
컴퓨터 엔진 3
컴퓨터 엔진 m
CE1 작업 로드 80% 965
CE2 작업 로드 30% 975
CE3 작업 로드 80% 985
CEm 작업 로드 80% 995

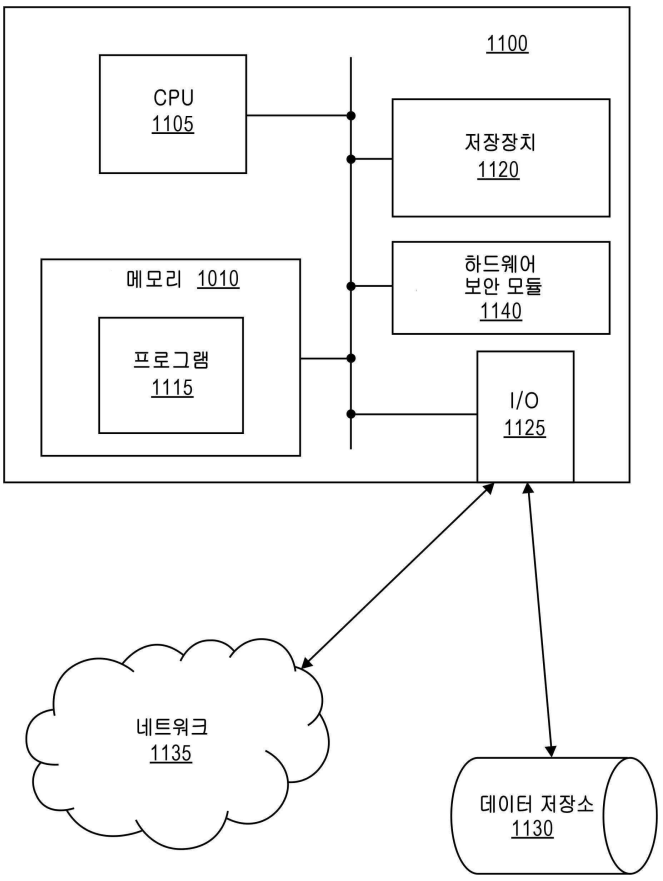
도면10a


1000
1002
프로비저닝 제어기
프라이머리/예비
1005
등록 권한
REST APP VM
DB
1010
메시지
큐
1025
등록 권한
APP / 컴퓨터엔진
DB
1012
메시지
큐
1035
등재 인증 권한
APP / 컴퓨터 엔진
DB
1014
메시지
큐
1045
가명 인증 권한
APP / 컴퓨터 엔진
DB

도면10b


1000
메시지 큐
1018
1060
연결 권한 2
APP / 컴퓨터 엔진
DB
1016
1050
연결 권한 1
APP / 컴퓨터 엔진
DB
메시지 큐
DB
1070
데이터베이스

도면11


1100
CPU
1105
저장장치
1120
메모리 1010
프로그램
1115
하드웨어
보안 모듈
1140
I/O
1125
네트워크
1135
데이터 저장소
1130