(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년05월27일
(11) 등록번호 10-0899471
(24) 등록일자 2009년05월19일

(51) Int. Cl.
*G06F 1/00* (2006.01) *G06F 12/00* (2006.01)
*G06F 17/00* (2006.01)
(21) 출원번호 10-2003-7010175
(22) 출원일자 2003년07월31일
심사청구일자 2007년01월31일
번역문제출일자 2003년07월31일
(65) 공개번호 10-2003-0071878
(43) 공개일자 2003년09월06일
(86) 국제출원번호 PCT/CA2002/000106
국제출원일자 2002년01월31일
(87) 국제공개번호 WO 2002/61550
국제공개일자 2002년08월08일
(30) 우선권주장
09/775,205 2001년02월01일 미국(US)
(56) 선행기술조사문헌
WO2000036566 A1
*(뒷면에 계속)*
전체 청구항 수 : 총 4 항

(73) 특허권자
**쓰리엠 이노베이티브 프로퍼티즈 컴파니**
미국 55133-3427 미네소타주 세인트 폴 피.오.박스 33427 쓰리엠 센터
(72) 발명자
**보트,알란**
캐나다케이1제이7이9온타리오오타와오리올드라이브61
**리드,브라이언**
캐나다케이2에스1이1온타리오스티츠빌스노위오울트래일14
(74) 대리인
**백만기, 이중희, 주성민**

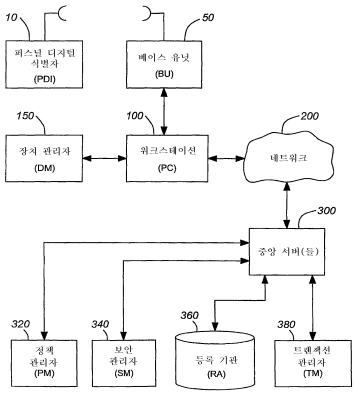
심사관 : 박상현

# (54) 컴퓨터 네트워크 보안 방법 및 시스템과 그에 사용된네트워크 구성 요소들에의 액세스를 제어하기 위한 퍼스널식별 장치

## *(57) 요 약*

향상된 컴퓨터 네트워크 보안 시스템과 방법, 및 네트워크 액세스를 제어하기 위해 사용되는 퍼스널 식별 장치가 개시된다. 새로운 유저는 휴대용 퍼스널 디지털 식별 장치에 등록되고, 유저의 생체 인식용 입력이 저장 장치에 수신되어 저장된다. 또한, 개인 키가 생성되어 저장 장치에 안전하게 유지된다. 퍼스널 디지털 식별 장치가 워크스테이션 근방의 엔벨로프 영역 내에 있을 때, 워크스테이션과 연관된 베이스 유닛으로부터의 제1 신호가 퍼스널 디지털 식별 장치에게 송신되고, 퍼스널 디지털 식별 장치는 베이스 유닛과 퍼스널 디지털 식별 장치 사이의 통신을 수립하는 응답 신호를 자동적으로 송신한다. 디지털 방식으로 생체 인식적으로 서명된 챌린지 응답 메시지가 퍼스널 디지털 식별 장치에 의해 생성되어 송신된다.

*대 표 도* - 도1



(56) 선행기술조사문헌
WO9926188 A1
KR1020010023602 A
KR1020010024318 A
KR1020010086236 A
KR1020010052103 A
EP1045346 A
US 5229764 A

## *특허청구의 범위*

**청구항 1**

컴퓨터 네트워크에 대한 액세스를 제어하기 위한 퍼스널 디지털 식별 장치로서,

상기 네트워크는 복수의 워크스테이션들을 포함하고, 상기 복수의 워크스테이션들 각각은 그와 연관되어 있는 베이스 유닛을 갖고, 상기 베이스 유닛은 상기 퍼스널 디지털 식별 장치와 무선 통신을 하도록 구성되고, 상기 네트워크는 보안 관리자 컴포넌트와 네트워크 저장 장치를 사용하는 중앙 서버를 더 포함하고, 상기 보안 관리자 컴포넌트는 개인 키 및 대응하는 공개 키와 연관되고, 상기 네트워크 저장 장치는 상기 퍼스널 디지털 식별 장치에 의해 보유된 개인 키에 대응하는 공개 키를 포함하고,

상기 퍼스널 디지털 식별 장치는,

등록된 유저에 의해 착용되거나 및/또는 휴대될 수 있도록 경량으로 구성되고,

(a) 상기 베이스 유닛과 통신하기 위한 송수신기를 포함한 무선 통신 컴포넌트;

(b) 유저의 생체 인식용 입력을 획득하여 그것의 디지털 표현을 생성하기 위한 생체 인식용 포착 컴포넌트;

(c) 상기 송수신기 및 상기 생체 인식용 포착 컴포넌트와 통신하도록 구성되고,

(i) 상기 디지털 표현으로부터 유도된 템플릿이 상기 생체 인식용 포착 컴포넌트에 의해 이전에 생성된 유저의 생체 인식용 디지털 표현으로부터 유도된 마스터 템플릿과 정합하는지를 평가하고, 정합하는 것으로 판정되면 정합 신호를 생성하고,

(ii) 상기 퍼스널 디지털 식별 장치에 의해 보유되는 상기 개인 키와 상기 개인 키에 대응하는 공개 키를 생성하고, 상기 송수신기에 의한 송신을 위해 상기 생성된 공개 키를 출력하고,

(iii) 상기 개인 키를 사용하여 디지털 서명을 생성하고,

(iv) 상기 보안 관리자 컴포넌트와 연관된 상기 개인 키에 대한 상기 공개 키를 사용하여, 상기 보안 관리자로부터 수신된 암호화된 메시지의 소스가 상기 보안 관리자 컴포넌트라는 것을 검증하는

동작들을 수행하는 프로세서;

(d) 유저의 생체 인식용의 상기 마스터 템플릿, 상기 보안 관리자 컴포넌트와 연관된 상기 생성된 개인 키 및 상기 개인 키에 대한 상기 공개 키를 포함하는 보안 저장 장치;

(e) 전원; 및

(f) 하우징

을 포함하고,

상기 퍼스널 디지털 식별 장치는, 상기 보안 관리자 컴포넌트로부터 수신된 챌린지 메시지에 응답하여 상기 정합 신호를 생성한 다음에, 상기 생성된 개인 키를 사용하여 디지털 서명된 챌린지 응답 메시지를 생성하고, 상기 응답 메시지를 송신하도록 구성되고, 상기 퍼스널 디지털 식별 장치는, 유저의 생체 인식용의 상기 마스터 템플릿과 상기 개인 키 중 어느 것도 전송되지 않도록 구성되며,

상기 퍼스널 디지털 식별 장치와 연관된 유저의 현재의 로그-인 세션 동안, 정책 관리자 컴포넌트는, 제2 퍼스널 디지털 식별 장치가 엔벨로프 내의 위치에서 검출되면, 상기 제2 퍼스널 디지털 식별 장치에 등록된 유저가 생체 인식적으로 확인되어 현재의 로그-인 세션의 데이터를 볼 수 있도록 허가될 때까지, 상기 워크스테이션들 중 적어도 하나에게 각자의 스크린을 블랭킹하도록(blank out) 지시하는 퍼스널 디지털 식별 장치.

**청구항 2**

제1항에 있어서,

상기 생체 인식용 포착 컴포넌트는 트랜스듀서를 포함하는 퍼스널 디지털 식별 장치.

**청구항 3**

삭제

**청구항 4**

제1항에 있어서,

상기 보안 저장 장치 내에 보유된 모든 데이터는 그 자체로는 상기 유저의 식별이 불가능한 퍼스널 디지털 식별 장치.

**청구항 5**

삭제

**청구항 6**

삭제

**청구항 7**

삭제

**청구항 8**

삭제

**청구항 9**

워크스테이션을 포함하는 네트워크 액세스 포인트에서 컴퓨터 네트워크에 대한 액세스를 제어하기 위한 보안 시스템으로서,

A. 퍼스널 디지털 식별 장치 - 상기 퍼스널 디지털 식별 장치는,

(a) 송수신기를 포함한 무선 통신 컴포넌트;

(b) 유저의 생체 인식용 입력을 획득하여 그것의 디지털 표현을 생성하기 위한 생체 인식용 포착 컴포넌트;

(c) 상기 송수신기 및 상기 생체 인식용 포착 컴포넌트와 통신하도록 구성되고,

(i) 상기 디지털 표현으로부터 유도된 템플릿이 상기 생체 인식용 포착 컴포넌트에 의해 이전에 생성된 유저의 생체 인식용 디지털 표현으로부터 유도된 마스터 템플릿과 정합하는지를 평가하고, 정합하는 것으로 판정되면 정합 신호를 생성하고,

(ii) 상기 퍼스널 디지털 식별 장치에 의해 보유될 개인 키와 상기 개인 키에 대응하는 공개 키를 생성하고, 상기 송수신기에 의한 송신을 위해 상기 생성된 공개 키를 출력하고,

(iii) 상기 개인 키를 사용하여 디지털 서명을 생성하고,

(iv) 상기 보안 관리자 컴포넌트와 연관된 개인 키에 대한 공개 키를 사용하여, 수신된 암호화된 메시지가 보안 관리자 컴포넌트로부터 온 것임을 검증하는

동작들을 수행하는 프로세서;

(d) 유저의 생체 인식용의 상기 마스터 템플릿, 상기 보안 관리자 컴포넌트와 연관된 상기 생성된 개인 키 및 상기 개인 키에 대한 상기 공개 키를 포함하는 보안 저장 장치

를 포함하고,

상기 퍼스널 디지털 식별 장치는, 상기 보안 관리자 컴포넌트로부터 수신된 챌린지에 응답하여 상기 정합 신호를 생성한 다음에, 상기 생성된 개인 키를 사용하여 디지털 서명된 챌린지 응답 메시지를 생성하고, 상기 응답 메시지를 송신하도록 구성되고, 상기 퍼스널 디지털 식별 장치는, 유저의 생체 인식용의 상기 마스터 템플릿과 상기 개인 키 중 어느 것도 전송되지 않도록 구성됨 -;

B. 상기 워크스테이션과 연관되고, 상기 퍼스널 디지털 식별 장치와의 무선 통신을 시작하고 유지하도록 구성된 베이스 유닛 - 상기 통신은 상기 워크스테이션과 연관된 엔벨로프에 의해 정의된 영역에 걸쳐 이루어지고, 상기

퍼스널 디지털 식별 장치와 연관된 유저의 현재의 로그-인 세션 동안, 정책 관리자 컴포넌트는, 제2 퍼스널 디지털 식별 장치가 상기 엔벨로프 내의 위치에서 검출되면, 상기 제2 퍼스널 디지털 식별 장치에 등록된 유저가 생체 인식적으로 확인될 때까지, 상기 워크스테이션에게 스크린을 블랭킹하도록 지시함 -; 및

C. 네트워크 저장 장치를 액세스하고, 상기 유저를 인증하기 위해 상기 보안 관리자 컴포넌트와 상기 퍼스널 디지털 식별 장치를 이용하는 중앙 서버 - 상기 네트워크 저장 장치는 상기 퍼스널 디지털 식별 장치에 의해 생성된 상기 개인 키에 대응하는 공개 키를 포함함 -

를 포함하는 보안 시스템.

**청구항 10**

삭제

**청구항 11**

삭제

**청구항 12**

삭제

**청구항 13**

삭제

**청구항 14**

삭제

**청구항 15**

삭제

**청구항 16**

삭제

**청구항 17**

삭제

**청구항 18**

삭제

**청구항 19**

삭제

**청구항 20**

삭제

**청구항 21**

삭제

**청구항 22**

삭제

## *명 세 서*

## 기 술 분 야

<1> 본 발명은 컴퓨터 네트워크 보안용 수단에 관한 것으로, 특히, 컴퓨터 네트워크의 구성 요소들에 대한 개개인의 액세스의 범위를 제어하기 위해 컴퓨터 네트워크에 구비되어 그 개개의 소지자를 안전하게 인증하기 위해 사용되는 디지털 퍼스널 식별 장치에 관한 것이다.

## 배 경 기 술

<2> 전자 정보의 보호에 대해 세계적인 관심이 증대되고 있다. 그 정보가 지적 재산에 관한 것이든지, 중대한 운영 데이터이거나 혹은 개인적인 정보이거나 간에, 그러한 정보의 의도된 바 없는 노출은, 전세계적인 경쟁 관계, 데이터 프라이버시 이슈들에 관한 공중의 인식과 새로운 법률 제정에 기인하여, 그 손해가 증가하고 있다. 이 문제들은, 사실상 임의의 위치로부터의 데이터에 대한 액세스 및 많은 액세스 장치에 대한 액세스를 가능하게 해주는 널리 퍼져 있는 네트워크 기술에 의해 더욱 심각해졌다. 예를 들어, 미국 내의 보건 산업계와 같은 일부 산업들에 영향을 끼치는 규제 요건들은 (미국에서는, 보건 기구들이 개인적으로 식별 가능한 건강 정보의 보안 및 프라이버시를 보장하기 위해 모든 합리적인 조치들을 취하도록 보장하기 위해 규칙들이 채택되어 있음), 컴퓨터 네트워크의 각 예상 유저가 민감하거나 혹은 기밀로 여겨질 수 있는 네트워크나 혹은 그 내부의 데이터를 액세스하는 것을 허가하기 전에, 그 개개의 예상 유저를 인증할 수 있을 필요성을 증가시키고 있다.

<3> 네트워크의 각 구성 요소, 및 그러한 구성 요소들 간의 각 경로는 공격의 (즉, 인증되지 않은 엔티티에 의한 데이터 액세스를 허가하는) 주체가 될 수 있다. 또한, 네트워크를 거쳐 기밀의 데이터를 액세스하는 능력은 개인이 네트워크로 로그인할 것을 반드시 필요로 하지는 않는데, 그 이유는, 네트워크 컴퓨터 스크린의 가시 거리 내의 허가되지 않은 관측자가, 스크린이 데이터를 표시할 때 스크린을 봄으로써 간단히 기밀의 데이터를 액세스할 수 있기 때문이다. 따라서, 데이터 액세스를 방지하기 위해 유저 인증을 목표로 하는 데이터 액세스 방지 달성을 위한 보통의 방법들은 허가되지 않은 네트워크 유저들의 문제만을 해결할 수 있을 뿐, 결코 네트워크를 사용을 통해 액세스하려고 하지 않는 허가되지 않은 관측자들의 문제를 해결할 수 없다.

<4> 암호 기법이 종종 네트워크 시스템 내에서 보안 조치로서 채택되고 이 암호 기법은 개인 키와 공개 키를 사용한다. "개인 키"와 "공개 키"란 용어는 당해 분야에 잘 알려져 있고, 암호화를 위해 하나의 키가 사용되고 복호화를 위해 다른 한 키가 사용되는 비대칭 암호 기법에 사용되며, 이 키들 중 하나, 즉 개인 키는 유저가 가지고 있어서 절대 드러나거나 전달되지 않는다. 비대칭 암호 기법은, 암호화 및 복호화 모두를 위해 공유 키가 사용되는 대칭 암호 기법에 비해 더 높은 레벨의 보안성을 제공하는 것으로 여겨진다 (공유라는 점은 불안전성의 요소를 도입함). 다른 측에 메시지를 보내기 위해 비대칭 암호 기법을 사용하면, PKI(Public Key Infrastructure)를 사용하여 그 다른 측의 공개 키의 위치가 결정되고 이를 사용하여 메시지를 암호화한 후, 대응하는 개인 키를 가진 사람 (즉, 메시지를 생성하기 위한 다른 관계자임)만이 그 메시지를 복호화할 수 있다.

<5> 디지털 서명(digital signature)이란 용어도 당해 분야에 널리 알려져 있는데, 개인 키를 사용하여 암호화된 메시지 다이제스트를 일컬으며, 메시지 다이제스트는 문서나 트랜잭션을 생성하기 위해 사용될 수 없는 서명된 문서 또는 트랜잭션의 압축된 형태이며, 이것은 문서 내의 작은 변화에도 매우 민감하다. 디지털 서명은, 대응하는 공개 키로 복호화함으로써 메시지 다이제스트를 복원하고, 이 메시지 다이제스트를, 서명되었다고 칭해졌던 문서로부터 검증기에 의해 계산된 것과 비교함으로써 확인된다. 이 기술은, 일측이 그들의 메시지 다이제스트를 암호화하고 리턴하는 능력에 의해 특별한 개인 키를 갖는 것을 입증하는 인증 프로세스의 일부로서 사용될 수 있다. 이 경우, 메시지의 특정 콘텐츠들은 중요하지 않고, 메시지 다이제스트는 인증이 완료된 후에는 무시될 수 있다. 더 통상적으로, 암호화된 메시지 다이제스트는, 특별한 키의 소지자가 그 메시지와 관련한 트랜잭션에 연관되었다는 것을 입증하기 위해, 그리고 물리적인 서명이 문서 내에 그 소유자의 참여를 나타내기 위해 사용되는 것과 마찬가지로, 메시지에 동의를 표시하기 위해 보통 사용된다. 이 경우, 암호화된 형태의 다이제스트는 보안 사이트에 보류되어야 한다. 디지털 서명의 두 형태들이 본 발명의 일부로서 사용된다.

<6> 유저 식별 시스템들은 패스워드, 스마트 카드, 생체 인식, 및/또는 PKI(Public Key Infrastructure) 보안 조치들을 자주 사용하고, 그들이 인증 프로세스의 보안 부분들에 집중하는 동안 공지의 시스템들은 다른 공격 가도에 열려있다. 예를 들어, 소프트웨어 뿐인 시스템들은 유저가 알고 있는 그 무엇, 가령 꽤 쉽게 도난당하고 노출될 수 있는, 혹은 허가되지 않은 사람에 의해 포착되어 사용될 수 있는 유저 이름과 패스워드에 의존한다. 토큰이 분실되거나 도난당할 수 있기 때문에, 가령 스마트 카드와 같은 토큰들 (즉, 유저가 갖고 있는 것)에 기초한 보안 수단도, 마찬가지로 취약하므로, 허가된 유저가 실제로 존재하는지를 보장하지 않는다.

<7> 생체 인식 식별자들 (유저 자신의 것)에 기초한 보안 수단도 허가되지 않은 개입에 똑같이 취약할 수 있다. 예

를 들어, (제시된 생체를 캡쳐하는 생체 인식 트랜스듀서와 로컬 컴퓨터 사이, 그리고 로컬 컴퓨터와 제시된 생체에 비교되는 검증 데이터를 포함하는 검증 중앙 서버 사이의) 원격 검증을 위해 연결될 통신 채널들의 어느 일측 (또는 양측)을 통해 중요한 생체 인식 데이터를 전송할 필요성 때문에, 보안상 취약성을 초래한다. 그러므로, 생체 인식 식별자가 다루어지고 처리되는 방식은, 생체 인식 식별자가 보안 척도로서 유효하게 기능한다면, 더욱 중요하다.

<8> 컴퓨터 네트워크가 허가되지 않은 침입을 받게 되는 잠재적인 실패의 포인트들을 식별할 뿐만 아니라, 포괄적인 방식으로 그러한 취약한 영역들을 해결하고 감소시키기 위한 수단을 개발할 필요가 있다. 보안 파괴는 다음과 같은 것을 포함한 여러가지 다양한 형태로 발생할 수 있다. 즉, 재생(이전의 응답 엘리먼트가 캡쳐되어 거짓 응답을 불쑥 끼워넣기 위해 사용되는 상황을 일컬음), 기웃거리고 서성대기(snooping: 허가되지 않은 관측자를 일컬음), 위장 (spoofing: 남의 이름을 사칭하는 자가 자신을 삽입하고, 관리자가 그것이 마치 네트워크의 진정한 엘리먼트인양 수신 및 송신 모두를 관리하는 상황을 일컬음), 및/또는 테일게이팅(tailgating: 허가된 유저에 의해 액세스가 포기될 때 허가된 액세스 시퀀스와 결합하여 획득된 비인가된 액세스의 상황을 일컬음) 등이 있을 수 있다.

<9> 식별/검증 프로세스 동안 시간 갭 및/또는 일방 검증 체크에 의해 유발된 취약성을 피하는 것이 중요하다. 여기에서 발명자는 무언가의 타입의 보안 파괴를 방지하기 위해, 실시간으로 행해지는 검증 체크 프로세스들에 대한 필요성과, 중앙 검증 기관과 검증될 로컬 엔티티와의 사이의 상호 검증에 대한 필요성을 깨달았다.

<10> 또한, 네트워크에 대한 상이한 레벨들의 액세스 (예를 들어, 전체 액세스와 제한된 액세스)에 대한 권한을 가진 사람들을 자동적으로 그리고 효과적으로 감시하고 제어하고 이들에 대한 감사 추적을 하는 수단에 대한 필요성도 있다.

<11> <발명의 개요>

<12> 본 발명에 따르면, 특별한 네트워크 액세스 포인트에서 개인의 식별자 및 존재를 모두 실시간으로 인증하기 위한, 개선된 네트워크 보안 시스템, 방법, 및 네트워크 액세스 제어용 퍼스널 식별 장치가 제공된다. 생체 인식 검증과 암호화가 동시에 존재하는 애플리케이션이, 네트워크 상에 저장된 데이터에 대한 안전한 액세스를 설정하고 네트워크를 통한 안전한 트랜잭션을 수행하기 위해 사용되는 인증된 디지털 서명을 제공하기 위해 휴대가능한 퍼스널 디지털 식별 장치의 보드 상에 탑재되어 제공된다.

<13> 본 발명에 따른 보안 시스템은, 예를 들어 퍼스널 컴퓨터(PC)일 수 있는 워크스테이션을 포함하는 네트워크 액세스 포인트에서 컴퓨터 네트워크로의 액세스를 제어한다. 퍼스널 디지털 식별 장치는, (a) 송수신기를 포함한 무선 통신 컴포넌트; (b) 유저의 생체 인식용 입력을 받아서 그 디지털 표현을 생성하기 위한 생체 인식용 포착 컴포넌트; (c) 상기 송수신기 및 상기 생체 인식용 포착 컴포넌트와 통신하도록 구성되고, (i) 상기 디지털 표현으로부터 유도된 템플릿이 상기 생체 인식용 포착 컴포넌트에 의해 이전에 생성된 유저의 생체 인식용 디지털 표현으로부터 유도된 마스터 템플릿에 해당하는지를 평가하고, 그러한 해당성이 판정될 때 정합 신호를 생성하고, (ii) 상기 퍼스널 디지털 식별 장치에 의해 보유되는 상기 개인 키와 상기 개인 키에 대응하는 공개 키를 생성하고, 상기 송수신기에 의한 송신을 위해 상기 생성된 공개 키를 출력하고, (iii) 상기 개인 키를 사용하여 디지털 서명을 생성하고, (iv) 상기 보안 관리자 컴포넌트와 연관된 개인 키에 대한 공개 키를 사용하여, 수신된 암호화된 메시지가 상기 보안 관리자로부터 온 것임을 검증하는 동작들을 수행하는 프로세서; (d) 상기 유저의 생체 인식용 상기 마스터 템플릿, 상기 보안 관리자 컴포넌트와 연관된 상기 생성된 개인 키 및 상기 개인 키에 대한 상기 공개 키를 포함하는 보안 저장 장치를 포함한다. 퍼스널 디지털 식별 장치는, 상기 생성된 개인 키를 사용하여, 상기 보안 관리자 컴포넌트로부터 수신된 챌린지에 응답하여 상기 정합 신호를 생성한 다음에 디지털 서명된 챌린지 응답 메시지를 생성하고, 상기 응답 메시지를 송신하도록 구성된다. 상기 퍼스널 디지털 식별 장치는, 유저의 생체 인식용 상기 마스터 템플릿과 상기 개인 키 중 어느 것도 전송되는 것을 방지하도록 구성된다.

<14> 베이스 유닛은 상기 워크스테이션과 연관되고, 상기 퍼스널 디지털 식별 장치와의 무선 통신을 시작하고 유지하도록 구성된다. 상기 통신은 상기 워크스테이션과 연관된 엔벨로프에 의해 한정된 영역에 걸쳐 이루어지고, 상기 엔벨로프는, 관측자가 상기 워크스테이션의 스크린 상에 표시된 정보를 읽거나 이해할 수 있는 상기 워크스테이션 근방의 위치들을 포함하도록 구성되는 모양 및 영역을 갖는다.

<15> 보안 중앙 서버는 네트워크 저장 장치를 액세스하고, 상기 유저를 인증하기 위해 상기 보안 관리자 컴포넌트와 상기 퍼스널 디지털 식별 장치를 이용한다. 상기 네트워크 저장 장치는 상기 퍼스널 디지털 식별 장치에 의해

생성된 상기 개인 키에 대응하는 공개 키를 포함한다.

<16> 바람직하게, 베이스 유닛은 제1 신호를 상기 퍼스널 디지털 식별 장치에게 정기적으로 송신하고, 퍼스널 디지털 식별 장치는, 퍼스널 디지털 식별 장치가 엔벨로프 내에 있을 때, 제1 신호에 응답하여 응답 신호를 자동적으로 송신한다. 상기 시스템은 복수의 상기 퍼스널 디지털 식별 장치들과 복수의 워크스테이션들과 복수의 베이스 유닛들을 포함하고, 상기 베이스 유닛은 각각의 상기 워크스테이션과 연관되고, 각각의 상기 베이스 유닛은, 상기 베이스 유닛이 각각의 상기 퍼스널 디지털 식별 장치로부터의 응답 신호를 수신한 다음에, 상기 베이스 유닛의 연관 엔벨로프 내에 있는 각각의 상기 퍼스널 디지털 식별 장치에게 폴링 신호를 송신한다.

<17> 바람직하게, 상기 퍼스널 디지털 식별 장치의 상기 보안 저장 장치 내에 보유된 모든 데이터는 그 자체로는 상기 유저의 식별이 불가능하다. 상기 네트워크 저장 장치는, 상기 유저의 퍼스널 디지털 식별 장치가 상기 엔벨로프 내에 위치할 때, 상기 워크스테이션의 스크린 상에 표시되는 상기 유저를 식별할 수 있는 데이터를 포함한다.

<18> 바람직하게, 일단 유저가 워크스테이션에서 네트워크에 대한 액세스를 위해 인증되면, 유저의 네트워크를 통한 애플리케이션들에 대한 액세스는, 보안 관리자 컴포넌트에게 지시를 내리는 정책 관리자 컴포넌트에 의해 결정된다.

## *발명의 상세한 설명*

<25> 본 발명에 따른 바람직한 보안 시스템이 도 1에 도시된다. 바람직한 실시예에 있어서 퍼스널 컴퓨터들(PCs)인, 복수의 워크스테이션들(100)은, 글로벌 통신 네트워크, 광역 네트워크(WAN), 메트로 영역 네트워크(MAN) 혹은 근거리 네트워크(LAN) 중 임의의 하나인 네트워크를 통해 통신한다. 네트워크(200)에 액세스 포인트를 제공하는 이러한 각 PC(100)에는, PC의 통신 포트 (본 실시예에 있어서는 USB 포트임)에 접속된 베이스 유닛(BU) 장치(50), 및 가령 BU(50)와 보안 중앙 서버(300) 사이의 메시들을 중계하는 장치 관리자 (DM)(150) 소프트웨어 컴포넌트가 있다. 하나 또는 그 이상의 PDI 장치들(10)은, PDI가, PC(100) 및 그에 접속된 BU(50)와 연관된 선정된 검출 엔벨로프 내에 있을 때, BU(50)와 통신한다. PDI 장치(10)는 무선 통신 (본 실시예에서는 IR이 사용되지만, 다른 광학식 또는 RF 수단이 다른 가능한 대안적인 실시예들에서 사용될 수 있음)을 사용하여 BU(50)와 통신하고, PC(100)를 통해 네트워크에 액세스가 허가된 사람들에 의해 발행되고 소지되고 착용된다.

<26> BU(50)는 동일한 무선 통신 수단을 사용하여 PDI(10)와 통신하고, 검출 엔벨로프 내에 있는 임의의 그러한 PDI(10)와 자동적으로 통신을 시작한다. 이 검출 엔벨로프는 PC(100)의 디스플레이 스크린의 정면 쪽 영역과 측면에 걸쳐 연장되도록 설정되어 있고 스크린 상에 표시된 콘텐츠들을 읽고 이해할 수 있는 영역이다. BU(50)/PC(100) 쌍과 PDI(10) 사이의 통신 엔벨로프를 이와 같이 구성함으로써, 보안 시스템은 PDI(10)들을 착용한 사람들이 PC(100)의 유효 가시 거리 내로 들어 올 때, 모든 PDI들을 검출한다.

<27> PC(100)는, 보안 관리자(SM)(340), 정책 관리자(PM)(320) 및 트랜잭션 관리자(TM)(380) 애플리케이션들이 실행되고 있는 보안 중앙 서버(들)(300)과 네트워크(200)를 통해 통신한다. 트랜잭션 관리자(380)는 보안 중앙 서버(들)(300)과, 가령 장치 관리자(150) 및 PC(100) 상에서 또는 다른 네트워크 서버들 상에서 실행되는 임의의 관련 애플리케이션들을 포함한, 네트워크 상의 다른 장치들 사이의 모든 통신들을 관리한다. 보안 관리자(340)는 암호화와 디지털 서명에 관련된 모든 동작들을 지시한다. 정책 관리자(320)는 유저의 네트워크 상의 애플리케이션들이나 데이터의 액세스가 제한될 것인지를 판정하고, 제한할 것이라면, 보안 관리자(340)에게 유저의 액세스를 제한할 것을 지시한다. 등록 기관(RA) 컴포넌트(360)는 소프트웨어 컴포넌트 (즉, 등록 애플리케이션 일행) 및 보안 데이터베이스를 포함하고, 중앙 서버(300)를 통해 액세스된다.

<28> 도 2를 참조하면, PDI 장치(10)는 소량의 회로를 포함할 뿐이고, 간단하고, 가볍고, 착용 가능하다. PDI(10)는 생체 인식 컴포넌트(35)를 포함하는데, 본 발명에 있어서, 생체 인식 컴포넌트(35)는 고체 상태, 비-광학식 센서를 사용하여 유저의 손가락의 이미지를 채취하여 유저의 신원을 확인하는 지문 마이크로칩 트랜스듀서를 포함한다. 음성 특성, 홍채 패턴 및 얼굴 생김새와 같은 다른 타입의 생체 인식 센싱과 이들을 표시 신호로 변환하기 위한 트랜스듀서들은 적당한 다른 실시예에 사용 가능한 옵션이다. 마이크로프로세서(들)(20)는 유저의 생체 인식용 측정의 등록 및 검증을 처리하고, 디지털 서명을 생성 및 검증하고, 비대칭성 및/또는 대칭성 암호화를 실시하기 위해 제공된다. 보안 저장 장치(25)는 당해 분야에서 잘 알려져 있는 바와 같이, 암호 키들과 유저의 생체 인식용 템플릿만을 안전하게 저장하도록 제공된다. 다른 개인적 식별 가능한 데이터 (즉, 그 자체로 유저를 직접 혹은 간접적으로 식별하는 데이터)는 PDI(10) 상에 저장되지 않는데, 그 이유는 매우 능숙한 허가되지 않은 제3자가 어떤식으로든 보안 저장 장치에 침입하여 그 안에 저장된 데이터를 액세스할 수 있는 경우에

그 제3자가 유저의 아이덴티티와 유저의 생체 인식용 템플릿 둘다를 획득할 수 있기 때문이다. 무선 통신 송수신기(15)는 단거리 무선 통신을 (890㎚의 근적외선을 사용하여) 가능하게 한다. 충전 가능한 배터리(40)는 PDI(10)가 적당한 기간 (예를 들어 2주 혹은 그 이상) 동안 계속적으로 실행할 수 있도록 해주는 전력 관리 시스템을 제공한다. 각 PDI 장치(10)는 그에 할당된 전역적으로 고유한 식별자(ID) 넘버를 갖고, 따라서, 각 장치는 그의 ID 넘버로 식별 가능하다. 배터리 충전기(5)는 또한 PDI(10)의 배터리(40)를 재충전하기 위해 제공되고, 재충전 장치 홀더(받침대)(250)는 PC의 통신 포트에 접속한 통신 포트 커넥터(42)(예를 들어, USB 커넥터)에 의해 PDI(10)를 PC(100)에 직접 접속하기 위해 사용될 수 있는데, 이 직접 접속 (즉, PC(100)를 위해 BU(50)가 필요없거나 사용되지 않는 구속 모드)은, 예를 들면 홈 오피스와 같은 단지 한명의 유저가 존재할 것으로 예상되는 안전한 곳으로부터 네트워크에 대해 안전하게 로그-온하기에 유용하다. PDI가 장치 홀더에 대해 적당하게 위치될 때 PDI가 장치 홀더에 의해 안전하게 유지되도록, 장치 홀더는 PDI의 하우징과 협조하도록 구성된다.

<29> 도 3을 참조하면, 베이스 유닛(BU)(50)은 또한 단거리 무선 통신을 (890㎚의 근적외선을 사용하여) 가능하게 하는 무선 송수신기(55)를 포함한다. 송수신기(55)와 BU(50)의 위치 설정은, 상술한 바와 같이, PC(100) 주위의 선정된 검출 엔벨로프 내의 임의의 PDI(10)로부터의 신호를 수신할 수 있도록 구성된다. 마이크로프로세서(들)(60)는 PDI(10) (또는 하나 이상의 PDI들이 BU의 무선 통신 범위 내에 있다면, 하나 이상의 PDI들)와 BU(50) 사이, 및 BU(50)와 호스트 PC(100) 사이의 통신을 관리한다. 통신 포트 커넥터(65) (예를 들어, USB 커넥터)는 BU(50)를 호스트 PC(100)에 접속하기 위해 제공된다.

<30> PDI(10)와 BU(50) 각각은 송수신기들(10, 55)의 동작을 각각 제어하는 하드웨어와 소프트웨어의 조합을 포함하여, 호스트 PC의 디스플레이 스크린 상의 데이터를 읽거나 이해하기에 충분하게 호스트 PC에 가까운 임의의 사람/PDI 쌍의 존재가 BU(50)에 의해 검출되도록, 이들은 연관된 PC(100)의 디스플레이 스크린을 읽기 위한 인간의 눈의 능력에 매우 근사한 시야 범위 및 각도 특성을 갖고 동작한다. 검출 엔벨로프의 모양과 사이즈는 제어 가능하고, 로컬 PC/워크스테이션 구성 또는 조직 요건들에 맞도록 BU 및 PDI에 적용되는 하드웨어와 소프트웨어 변화의 조합을 통해 변화될 수 있다. 당업자는 임의의 주어진 구성에 따라 그러한 변화를 용이하게 만들 수 있다. 통신 소프트웨어는, 선정된 검출 엔벨로프 내에 있는, 임의의 그리고 모든 PDIs(10)가 베이스 유닛(50)에 의해 포착될 수 있도록 해주고, 베이스 유닛은 각 PDI가 검출 엔벨로프 내에 있는 한, 대화 형태로 통신을 유지한다. 대화는 데이터의 암호화된 스트림들을 포함하고, 대화에 참여하려고 시도하는 임의의 다른 장치의 검출을 가능하게 하도록 구성된다. 유저가 간단히 등을 돌리거나 혹은 달리 PDI(10)와 BU(50) 사이의 광학식 경로를 방해할 때, 이 대화의 지속을 쉽게 하기 위하여, PDI와 BU 둘다에 단거리 무선-주파수(RF)파와 같은 비-방향성 통신 모드를 사용하는 제2 송수신기를 포함시키는 것이 가능하다. 이 모드는 대화를 시작하기 위해서 이용되지 않을 것이나, 단기간 동안 대화를 지속시킬 수 있다.

<31> 각 PDI(10)는 또한 PDI(10) 내에서 하나 이상의 공개/개인 키 쌍들의 생성과, 메시지의 암호화 및 복호화와 관련한 PDI(10) 상의 모든 후속 프로세싱을 관리하는 암호화 소프트웨어 컴포넌트를 포함한다. PDI(10)의 인증은 통신 프로토콜을 통해 확인되는데, 이에 따르면 보드상의 (즉, PDI 내에 포함된) 개인 키가 PDI에게 보내진 챌린지를 디지털 서명하기 위해 보안 관리자 컴포넌트(SM)(340)에 의해 사용되며, 보안 관리자 컴포넌트(SM)(340)는 네트워크의 중앙 서버(300) 상에서 실행된다. 중요하게, PDI(10)는 우선 보안 관리자의 보드 상의 공개 키를 사용하여 그로부터 수신된 메시지들의 소스로서 보안 관리자를 인증한다. PDI의 암호화 소프트웨어 모듈은, 외부 애플리케이션으로부터의 메시지에 기초하여, 보안 관리자에 의해 생성되고 PDI에게 전달되는 메시지에 서명하도록 구성된다. PDI가 그러한 메시지 다이제스트에 서명하기 전에, PDI는, 다이제스트를 생성하기 위해 사용된 보안 관리자의 키를 검증함으로써, 메시지 다이제스트가 실제로 보안 관리자로부터 온 것인지를 인증한다. 이것은 PDI가 서명되어야 할 것이 아닌 임의의 문서에 서명하도록 위장되는 것을 방지한다.

<32> 본 발명의 폐쇄형 시스템에 있어서, 암호화 인프라스트럭쳐는 비교적 단순하고, 단일 층의 계층에 의해 지원되는 공개 키들의 데이터베이스 레코드와, 디지털 서명의 온라인 검증을 제공하는 보안 서버를 포함한다.

<33> 생체 인식 소프트웨어 컴포넌트는 각 PDI(10)의 생체 인식용 포착 컴포넌트(35) 내에 포함된다. 이 소프트웨어 컴포넌트는 지문 마이크로칩(35)으로부터 수신된 생체 인식용 이미지의 디지털 표현을 템플릿으로 변환하고, 그 템플릿을, 유저가 보안 시스템에 등록할 때 캡쳐되고 저장되었던 유저의 생체 인식용 마스터 템플릿과 정합을 시도한다. 생체 인식 컴포넌트의 정합 알고리즘은 유저의 생체 인식용의 실시간 (즉, 라이브) 표현 입력으로부터 생성된 템플릿을 보안 메모리(25) 내의 PDI 상에 저장된 마스터 템플릿과 비교하여, 비교 결과를 포함한 디지털 서명된 메시지를 보안 관리자에게 전송하도록 출력한다. 임의의 주어진 시간에서, 정책 관리자 컴포넌트(320)에 의한 요구에 따라, 혹은 선정된 기간 동안에, PDI(10)는 유저의 생체 인식용 입력으로부터 유도된 새로

운 템플릿을, 실시간으로, 저장되어 있는 템플릿과 비교함으로써 유저를 검증할 수 있고, 이러한 검증은 모두 PDI(10) 보드 상에서 (즉, 단지 자체의 설비들만을 사용하여), 검증을 하기 위해 사용되는 저장된 데이터를 임의로 배포함이 없이, 수행된다.

<34> BU(50)로부터 정보를 수신하는 장치 관리자 소프트웨어 컴포넌트(DM)(150)를 포함하는 PC(100)는 중앙 서버(들)(300) 상에서 실행되는 트랜잭션 관리자 컴포넌트(TM)(380)와 통신한다. BU(50)는 PDI(10)와의 통신이 할당된 선정된 기간 동안 실패했을 때, BU(50)와 PDI(10) 간의 대화는 종료되고, TM(380)은 PDI(10)가 더 이상 선정된 검출 엔벨로프 내에 있지 않음을 정책 관리자 컴포넌트(PM)(320)에게 통보한다. TM(380)이 새로운 PDI(10)가 BU(50)에 의해 검출되었다는 통보를 수신할 때, TM(380)은 PC(100)에게 검출된 유저에 대한 로그-온 프로세스에 관한 상태 정보를 표시하도록 명령하고, 적정하다면, 인증된 유저가 시스템에 로그-온하도록 초대한다. 정책 관리자 세팅에 따라, 기존의 로그-인 세션의 일부로서 스크린 상에 현재 표시된 임의의 민감한 정보는 자동적으로 블랭킹될 수 있다. 스크린은, 새롭게 검출된 PDI 장치의 유저가 그 자신이 보안 관리자에 의해 생체 인식적으로 인증되고 정책 관리자가 그러한 유저들이 관측자로서 이 데이터를 볼 권리가 있다고 판정할 때까지, 복원되지 않는다.

<35> 또한, 검출된 PDI에 관해 통지되면, 트랜잭션 관리자 컴포넌트(380)는 PC(100)에게 (그의 디스플레이 상에) 검출된 유저의 가시적인 식별자, 예를 들면 유저의 이름이나, 혹은, 바람직하게는 등록 데이터베이스로부터 검색된 유저의 얼굴 이미지를 표시하도록 지시한다. 이것은 두개의 보안 체크를 제공한다. 첫째, 강력한 가시적인 통지는, 스크린의 가시 범위 내의 모든 사람들의 아이덴티티를 디스플레이 스크린과 작업하는 인증된 유저에게 통지하도록 제공되고, 이것은 유저가 인증되지 않은 데이터 액세스를 막도록 도와준다 (여기서, 유저는 누군가가 스크린 상에 표시된 정보를 읽을 수 있는 범위로 온 순간 즉시 알 수 있고, 그 사람이 누구인지를 알 수 있음). 둘째, 스크린에서 작업하는 사람은 스크린의 영역 내에 있는 모든 사람들의 이미지들을 스크린 상에서 볼 것을 기대할 것이고, 그런 사람의 이미지가 검출되지 않으면, 유저는 검출되지 않은 사람의 PDI가 결점이 있고, 충전, 수선, 또는 교체가 필요하다고 경계하게 된다. 옵션으로, 이러한 특성은, 사람/PDI 쌍이 그 워크스테이션을 지나갈 때 PDI에 등록된 사람의 이미지의 즉각적이고 자동적인 표시를 워크스테이션 수행원 (즉, 보안 요원)에게 제공하기 위해 (보안 상황에서 이렇게 표시된 이미지와 그 PDI를 착용한 사람은 동일하여야 함), 빌딩 내의 입구를 제어하기 위해 사용될 수 있다. 유사하게, 다른 사람이 로그 온하고 있는 동안 액세스 권한이 부여되지 않은 악의 있는 사람이 정보를 보려고 하면, 혹은 이들이 위장을 하고 보안 장소에 들어가려고 한다면, 이들의 이미지가 표시되지 않는다는 사실은 현재 정당한 유저들에게 즉각적으로 무언가가 잘못되었다는 것을 경고할 것이다.

<36> 보안 관리자 컴포넌트(340)는 PDI(10)와, 가령 등록 기관 데이터베이스(360)와 같은 네트워크 보안 시스템의 다른 컴포넌트들 간에 발생하는 보안 프로세스들과 검증 및/또는 디지털 서명이 필요한 외부 애플리케이션에 의해 유저에게 보내진 메시지들 혹은 유저에 의해 외부 애플리케이션으로 보내진 메시지들을 관리한다. 보안 관리자는 디지털 서명들을 집적하는 챌린지/응답 메카니즘을 사용하여 PDI(10)를 인증하고, 이것에 의해 모든 그 이상의 동작들은 인증된 유저에 의해서만 취해질 수 있다. 보안 관리자는 또한 유저에게 전송될 임의의 문서나 혹은 트랜잭션(들)의 메시지 다이제스트와 모든 시스템 이벤트들의 공증된 로그(log)를 생성한다 (디지털 공증 프로세스는 당업계에 공지되어 있고, 서명된 문서에, 시간/날짜 및 믿을 수 있는 제3자 서명 둘 다를 첨부하여 사용됨). 또한, 보안 관리자는 애플리케이션에 따라, 데이터베이스로부터 추출된 데이터의 세세한 제어를 제공하기 위해 비즈니스 규칙들과 워크플로우를 적용하는 정책 관리자 컴포넌트(320)와 통신하고 상의할 수 있다. 이것은 애플리케이션이 다른 유저들에 대해 다른 수준의 보안성을 필요로 하는 상황에서 일어나는데, 즉, 매우 기밀한 데이터는 제한된 수의 유저들에게만 허가되는 것과 같이, 계층 분류에 기초하여, 유저들에게 데이터를 액세스하기 위한 다른 수준의 인증을 하는 경우에 발생한다.

<37> 보안 시스템은 새로운 유저를 등록하기 위한 구조적이고 엄격한 프로세스를 이용한다. 시스템이 새로운 유저들을 등록할 특권 (registrar privilege: 등록 특권)을 할당한 기존의 유저는, 네트워크에 로그인해야 하고, 등록 기관 컴포넌트(RA)(360)의 선단(front end)을 형성하는 등록 애플리케이션을 실행해야 한다. 등록될 새로운 유저를 아는 유저 (이하, 보증인이라 일컬음)는 동일한 BU(50)에 존재할 수 있다. 등록 기관 데이터베이스는 유저들, 그들의 역할 (예를 들면, 보증인) 및 새로운 유저들을 등록할 특권들에 관한 정보를 포함한다. 예를 들어, 어떤 상황에서는, 등록 특권을 가진 유저가 보증인의 역할을 할 수도 있다. 그런 다음 새로운 유저에 관한 어떤 기본적인 전기적 데이터, 예를 들면 새로운 유저의 이름(들), 주소, 생일, 신원을 증명하는데 사용되는 증명서의 넘버, 및 사람의 얼굴 이미지 등을 캡쳐하도록 구성될 수 있는 시스템에서는 그러한 이미지 등을 포함한 데이터가 입력된다. 그렇게 입력된 데이터는 RA 데이터베이스에만 저장되고, PDI(10)에는 저장되지 않는다.

그런 다음 유저는 PDI 장치를 들고, PC(100)의 BU(50)에 의해 PDI(10)가 포착되는 단계와, PDI가 새로운 유저에게 할당된 정확한 상태에 있음을 보장하기 위해 보안 관리자를 사용하여 PDI를 체크하는 단계를 통해 PDI의 성능이 검사되고, 그런 다음, 등록 프로세스가 하기와 같이 시작된다. 마이크로프로세서(들)(20)를 사용하여, PDI 장치 자체는 유저의 생체 인식용 템플릿과 하나 이상의 공개 및 개인 키들을 생성하고 이들을 내부에 저장한다. PDI는 일정하고 만족스러운 지문 템플릿을 얻을 때까지 새로운 유저의 지문을 샘플링한다. 결과적으로 구해진 지문 템플릿은 그 시스템의 임의의 외부 컴포넌트에는 전송되지 않고 PDI 장치 내의 보안 저장 장치 내에 저장된다. 지문에 관한 어떠한 생체 인식용 정보도 PDI 장치를 벗어나지 않는다. 그런 다음 PDI(10)는 등록 애플리케이션에 의해 하나 이상의 키쌍들을 생성하도록 지시되고, 이렇게 생성된 모든 개인 키(들)는 항상 PDI(10) 내에만 머물고, PDI(10) 밖으로 유출되지 않는다. 이렇게 생성된 공개 키는 중앙 서버(300)에 전달되고 RA 데이터베이스(360)에 저장된다. 보안 관리자는 또한 그 자신의 개인 키들을 보안 저장 장치 내에 보유하고, 이들 중 적어도 하나의 공개 키가 PDI에게 제공되어 PDI의 보안 저장 장치 내에 보유된다. 이러한 개인 및 공개 키들은, 그후, 새로운 유저의 PDI로부터 혹은 그에게 지향된 디지털 서명, 트랜잭션 및 챌린지를 검증하거나 생성하기 위해 PDI 및 SM에 의해 사용된다. 새로운 유저 등록 프로세스 동안, 보증인이 새로운 유저를 보증함을 증명하는 디지털 서명을 생성하기 위해, 보증인은 그의 PDI 장치 상의 지문 칩을 통해 그의 신원을 확인해 줄 것을 요구받을 수 있다.

<38> 현재 보안 시스템의 PDI들(10)은 암호화 프로세스들에 의해 공장 (그들의 제조처)과 사용처 (초기 배달 동안이나 장치 수선 동안 발생하는 이벤트들과 대조하여) 사이에서 탬퍼링(tampering)되는 것이 방지된다. 새롭게 제조된 PDI 장치들은 입수하는 기관에서 보안 관리자의 공개 키와 초기 발행 개인 키로 프로그래밍된다. 이 PDI 장치들이 입수 기관에 보내질 때, 그들의 고유 ID 넘버들의 리스트는 별도로 그리고 안전하게 그 기관에 통신된다. 새로운 유저를 등록하는 프로세스 동안, PDI는 초기에 발행된 개인 키 (그에 대한 공개 키를 보안 관리자가 갖고 있음)를 사용하여 보안 관리자에게 그 자신을 인증하고, 보안 관리자는 그의 개인 키를 사용하여 PDI에게 그 자신을 인증한다. 또한, PDI 장치의 고유의 ID 넘버는 보안 관리자에게 통신되고, 이 넘버는, 공장으로부터 수신된 PDI 장치 ID 넘버들의 리스트에 대해 정합된다. 이 프로토콜은 부정 장치들의 제조를 방지하고, 이 프로토콜은 공장에서 수선을 한 후에 그 기관으로 돌려보내진 PDI 장치들에 대해서도 사용된다.

<39> 로그-온과 다른 특권들은 주어진 네트워크 도메인 상에서 그 네트워크 도메인과 연관된 등록 기관에 등록된 PDI들에게만 가능하나, 각 PDI(10)도 고유의 ID 넘버를 가지기 때문에, 그의 등록시 원래 사용되었던 특정한 등록 기관과는 상관없이 보안 관리자에 의해 승인된다. 그러므로, PDI의 ID 넘버의 전역적인 특성은 다른 등록 기관들의 데이터베이스들을 공유함으로써 상이한 보안 시스템들 (즉, 다른 등록 기관들 하에서 운영되는 시스템들)의 통합을 가능하게 한다.

<40> 포착 (즉, PDI(10)가 범위 내에 있음이 BU(50)에 의해 검출됨) 및 로그-온 액세스를 위한 PDI의 후속 검증 동안 보안 시스템에 의해 수행되는 단계들이 도 4A 내지 도 4C의 플로우 챠트에 의해 설명된다. BU는 검출 엔벨로프 내에 있는 PC(100)/BU(50) 주위의 모든 지점들에 일정한 IR 신호를 송신한다. PDI가 그 엔벨로프 내에 들어오자마자, PDI는 BU의 이 IR 신호를 수신하고 그를 포착하려고 하는 BU에게 즉시 응답한다. 그런 다음, BU는 PDI를 폴링 루프에 추가한다. PDI가 그 시스템 상에 등록되어 있는지 아닌지 여부에 상관없이 범위 내에 있는 PDI는 BU에 의해 포착된다. 포착 단계는 낮은 프로세스 레벨에서 수행되는데, 이것에 의해 BU는 PDI를 감시하기 위한 폴링 루프에 새로운 PDI 장치를 추가하고, PDI의 고유의 ID 넘버를 식별하고 질문하는 중앙 보안 관리자에게 메시지를 보낸다. PDI가 그 시스템 상에 등록된 장치이고, 유저가 로그-온 특권을 갖고, 그리고 아무도 PC(100) (워크스테이션)에 로그-온하지 않았다면, 유저는 PC(100)에 로그-온하도록 초대될 것이다. PDI가 그 시스템 상에 등록된 장치이지만 누군가 이미 PC(100)에 로그-온하고 있으면, (정책 관리자에 의해 결정된) 임의의 민감한 정보가 즉시 블랭킹될 수 있고, 검출된 PDI와 연관된 유저의 가시적인 식별자가 PC(100) 상에 표시된다. 현재의 로그-인 세션과 연관된 데이터를 보기 위한 특권이 이 새로운 유저에게 있는지에 따라, 새로운 유저가 그 자신을 생체 인식 방식으로 인증하고 관측자로서 남아있도록 허가될 수 있다. 이것은, 마지막 단계에서, TM이 관측자의 존재를 기록하고, 네트워크 애플리케이션 또는 PC(100)에게, 유저를 로그-온하라는 것이 아닌, 스크린을 복원하라는 요청을 하게 될 것이라는 것을 제외하고는, 정상적인 로그-온의 나머지와 같은 프로세스를 통해 일어난다. 로그-온을 시도하거나 또는 관측자가 되려고 시도하는 유저에 대해, 그 다음 단계는, SM이, 그 안에서 무작위로 선택된 정보를 갖는, 그리고 SM 자신의 개인 키로 디지털 서명한 챌린지 메시지를 준비하는 것이다. 그런 다음 이 메시지는 PDI 장치에게 전송된다. 유저는 그의 손가락을 지문칩 상에 놓고 그의 신원을 확인함으로써, (옵션으로 그의 이름을 포함하는) 스크린 디스플레이에 의해 로그-온하도록 초대된다. PDI 장치는 우선, PDI 장치 상에 저장된 SM의 공개 키를 사용하여 메시지 상의 디지털 서명을 검증함으로써, 정당한 SM 프로세스로부터 메시지를 수신했음을 확인한다. 그런 다음 유저의 지문이 포착되고, 템플릿이 추출되

어 장치 상에 저장된 템플릿과 비교된다. 정합이 발견되면, 챌린지를 포함하고 유저가 생체 인식적으로 인증되었음을 확인하는 메시지가 SM에게 다시 보내진다. 이 메시지는 PDI 장치가 그의 보드 상의 개인 키를 사용하여 디지털 서명된 것이다. 확인 메시지는 등록 기관 내에 저장된 PDI 장치의 공개 키를 사용하여 SM에 의해 인증되고, 챌린지가 정확하게 돌아왔는지를 보장하기 위해 체크된다. 이것은 임의의 응답 공격에 대해 방어한다. PDI 장치가, 로그-온 액세스가 네트워크 상의 PC(100)에 허가되는, 싱글 사인-온(Single Sign-On: SSO) 프로세스를 위한 인증 수단으로서 사용되고 있다면, TM(380)은 PC(100) 상의 로그-온 컴포넌트에게 유저가 로그되도록 요청하는 메시지를 보낸다.

<41> PC(100) 유저가 이미 PC(100) 상에 로그- 온되어 있고 특정한 네트워크 기반 애플리케이션 또는 애플리케이션들에 대한 액세스를 원하면, TM(380)은, 그 애플리케이션(들)을 실행하는 보안 서버와, SM을 통해, 그 자신을 상호 인증하고, 이 서버에게 유저가 로그-인했음을 알릴 것이다. 예를 들어 보건 영역에서는, 로그-온들의 공유를 허용하는 CCOW(Clinical Context Object Workgroup)이라고 불리는 PC들 상의 콘텍스트 관리를 위한 최근에 생겨난 표준이 있다. 그러면, TM(380)은, 등록 기관(360) 데이터베이스로부터 얻은 유저의 역할과 특권에 관한 정보를 사용하여, 정책 관리자에 의해 적당하다고 판정된 애플리케이션들과 데이터의 서브세트에만 유저의 액세스를 허가하기 위해, CCOW-인에이블드 애플리케이션들과 상호작용할 것이다. 일반적으로, 보안 관리자(340)와 정책 관리자(320)는, 유저의 로그-인 세션을 통해, 모든 네트워크 애플리케이션들과 데이터에 대한 보안 필터로서 함께 작용한다.

<42> PDI는 분실되었다거나 혹은 도난당한 것으로 보안 시스템에 기록되어 있을 수 있다. 이러한 상황에서, 일단 PDI가 포착되면, SM은 PDI를 인증하고, 그 결과, PDI가 분실된 것으로 리스트에 올라있는 것으로 판정한다. 또한, PDI를 포착한 BU가 보안 관리자에게 알려지면, 보안 관리자는 BU의 위치와 그 BU에 대한 PDI의 접근 둘다를 알게 된다. 그러면 PDI의 위치를 식별하는 이 정보는, 분실된 PDI가 검색될 수 있고, 그것이 만일 도난당했었다면 범인이 체포될 수 있도록 하기 위해, 지정된 유저(예를 들어, 관리자 또는 보안 요원)에게 통신된다.

<43> 유저의 로그-인 세션 동안, 로그-온에 이어, PDI 장치와 베이스 유닛은 PDI가 여전히 검출 엔벨로프 내에 있는지를 확인하기 위해 서로 통신하고, 이 대화는, 다른 (허가되지 않은) 장치가 통신 스트림 내로 메시지를 삽입하려고 하는 임의의 시도를 베이스 유닛이 검출할 수 있도록 보장하는 암호화 통신을 포함한다. 유저의 PDI가 제1 선정 기간 동안 BU와 통신을 중지하면, 예를 들어 유저가 무언가를 가지러 워크스테이션으로부터 멀어지면, 허가되지 않은 어떠한 사람이라도 허가된 유저 대신에 애플리케이션을 계속해서 사용할 수 없도록 보장하기 위해 선정된 로그-오프 프로세스를 수행하도록 워크스테이션에 명령한다. 이것은 일시적인 자동 로그-오프일 수 있는데, 이것에 의해, 만일 유저의 PDI가 짧은 제2 선정 기간 내에 검출되면, BU가 유저의 PDI와 통신할 능력을 상실했을 때에 유저가 있었던 포인트에서 애플리케이션의 동작의 재개를 지시할 것이다. 옵션으로, 시스템은 로그-인 세션 동안 유저에게 PDI와 함께 그의 존재를 생체 인식 방식으로 검증할 것을 요구하도록 구성될 수 있고, 이것은 무작위적으로, 경과 시간에 의해, 또는 특정 데이터나 애플리케이션들에 대한 유저의 액세스에 따른 정책 관리자(320)의 판정에 의해 촉발될 수 있다. 이것은, 유저가 로그-인 세션 전체 동안, PDI와 물리적으로 공존하고 있음을 보장한다.

<44> 도 4A 내지 4C의 플로우 챠트에 의해 설명된 바와 같이, 포착/검증 프로세스에서, 인증된 유저가 그 유저에게 할당된 PDI와 함께 있는지 그리고 보안 관리자와 정확하게 통신하고 있는지를 확실하게 하기 위해, 유저의 생체 인식 인증과 PDI, 유저 및 보안 관리자의 암호 검증 사이에, 공간 및 시간적으로, 타이트한 링크를 설정한다. 유저의 신원은, 상술한 바와 같이, 저장된 생체 인식용 템플릿을 실시간으로 생체 인식용 트랜스듀서 (예를 들어, 지문 마이크로칩)로부터 생성된 생체 인식용 템플릿과 비교함으로써, PDI 보드 상에서, 실시간으로 검증되는데, 이 프로세스를 통틀어, 저장된 생체 인식용 템플릿과 실시간으로 생체 인식용 트랜스듀서로부터 생성된 생체 인식용 템플릿은 모두 PDI 내에 보유된다. PDI와 보안 관리자는 챌린지/응답 프로토콜에 따라 통신된 디지털 서명을 사용하여 서로를 각각 검증하고, 보안 관리자는 PDI에 의해 실시간으로, 임의의 주어진 문서/트랜잭션 서명에 대해, 유저의 신원이, 디지털 서명된 메시지에 의해 통지된다.

<45> 애플리케이션을 사용하는 동안, 유저에게는 문서나 다른 형태의 트랜잭션 (예를 들어, 약 처방전)에 디지털 서명을 할 것이 요구될 수 있다. 문서/트랜잭션에 대한 디지털 서명을 만들기 위해 시스템에 의해 이루어지는 단계들은 도 5A 및 도 5B의 플로우 챠트에 의해 설명된다. 서명 프로세스는 애플리케이션에 의해 요청되는데, 이 애플리케이션은 서명될 문서/트랜잭션을 SM에게 전달한다. SM은 소스와 목적지 어드레스들, 문서/트랜잭션의 메시지 다이제스트, 시간 스탬프 및 랜덤 데이터를 포함하는 메시지를 생성한다. 그런 다음 이 메시지는 디지털 서명되어 PDI 장치에게 전달된다.

<46> PDI 장치는 먼저 SM의 서명을 검증하는데, 이것은 또 다른 프로세스가 PDI 장치의 서명 요청을 할 수 있는 가능성 및 메시지 다이제스트가 훼손되거나 대체될 수 있는 가능성을 제거한다. 서명 요청이 유저의 신원을 확인하기 위한 요건을 포함하면, 유저에게 현재 리뷰 중인 문서 또는 트랜잭션에 적극적으로 디지털 서명할 것을 요청하는 것은 애플리케이션의 책임이다. 그러면 유저는 그의 손가락을 지문 칩 위에 올려놓아야 한다. 그러면 PDI 장치는 유저가 그의 손가락을 장치 위에 올려 놓기를 기다린다. 손가락이 올려 놓여진 것이 검출되면, 이미지가 캡쳐되고, 처리되고, 저장된 템플릿과 비교된다. 템플릿이 제시된 손가락과 정합하면, 소스와 목적지 어드레스들, 원래의 문서/트랜잭션의 메시지 다이제스트, 및 랜덤 데이터를 포함하는 메시지가 생성된다. 그런 다음 이 메시지는 디지털 서명되고 BU에게 보내지는데, BU에서 이 메시지는 SM에게 전달된다. 손가락이 템플릿과 정합하면, 유저에게 특정 횟수의 시도가 허가된 후, 정합 실패를 나타내는 디지털 서명된 메시지가 SM에게 보내진다. SM은 PDI 장치의 고유 ID를 사용하여 PDI 장치의 공개 키를 검색하고, 메시지는 이 정보를 사용하여 검증된다. 여기서, 신원 인증의 결과가 인증을 요청한 애플리케이션에게 전달되고, 필요하다면, 디지털 서명된 메시지의 복사본이 보안 공증 서비스에 보내진다.

<47> 디지털 서명은 원래 문서/트랜잭션의 데이터가 그 후 변화되지 않았음을 보장하기 위해 사용될 수 있다. 신원의 생체 인식 검증을 포함하는 앞선 프로세스의 주어진 특성상, 서명을 거부하는 유저에 의한 어떠한 시도도 거절되도록 기능할 수도 있다.

<48> 본 발명의 보안 시스템은 특별한 네트워크 액세스 포인트에서 유저의 존재를 실시간으로 확실하게 인증하고, 네트워크 액세스 포인트와 선택된 네트워크 서버 사이의 안전한 암호화 경로를 셋업하고 감시한다. 또한 이 보안 시스템은 디지털 서명들을 수집하기 위한 신뢰성있는 수단을 제공한다.

<49> 상술한 바람직한 실시예에서 사용된 개개의 전자 및 처리 프로세싱 기능들을 당업자는 모두 잘 이해될 것이다. 당업자에 의해 다른 다양한 실시예들이 대신 도출될 수 있다는 것을 독자들은 이해할 수 있을 것이다. 전자 보안 시스템 및 통신 디자인 분야의 당업자들은 본 발명을 주어진 애플리케이션을 위한 적당한 실시 방법에 용이하게 응용할 수 있을 것이다.

<50> 끝으로, 예시적인 방식으로 본 명세서에 개시되고 설명된 특정 실시예는 하기의 청구범위에 의해 한정된 본 발명의 범위를 제한하지 않는다.

## *도면의 간단한 설명*

<19> 본 발명의 바람직한 실시예를 예시적인 방식으로 설명하는 첨부 도면들을 참조한다 (유사한 요소들에는 유사한 참조 부호를 병기한다).

<20> 도 1은 액세스 제어에 의해 통신 네트워크의 보안을 확보하기 위한 본 발명의 시스템의 대략적인 블럭도.

<21> 도 2는 본 발명에 따른 퍼스널 디지털 식별 장치(PDI)의 구성 요소들을 나타내는 개략적인 블럭도. 여기서 PDI는 안전한 단일-유저 위치로부터 네트워크를 액세스하기 위해 재충전 장치 홀더(받침대) 상에 위치한다.

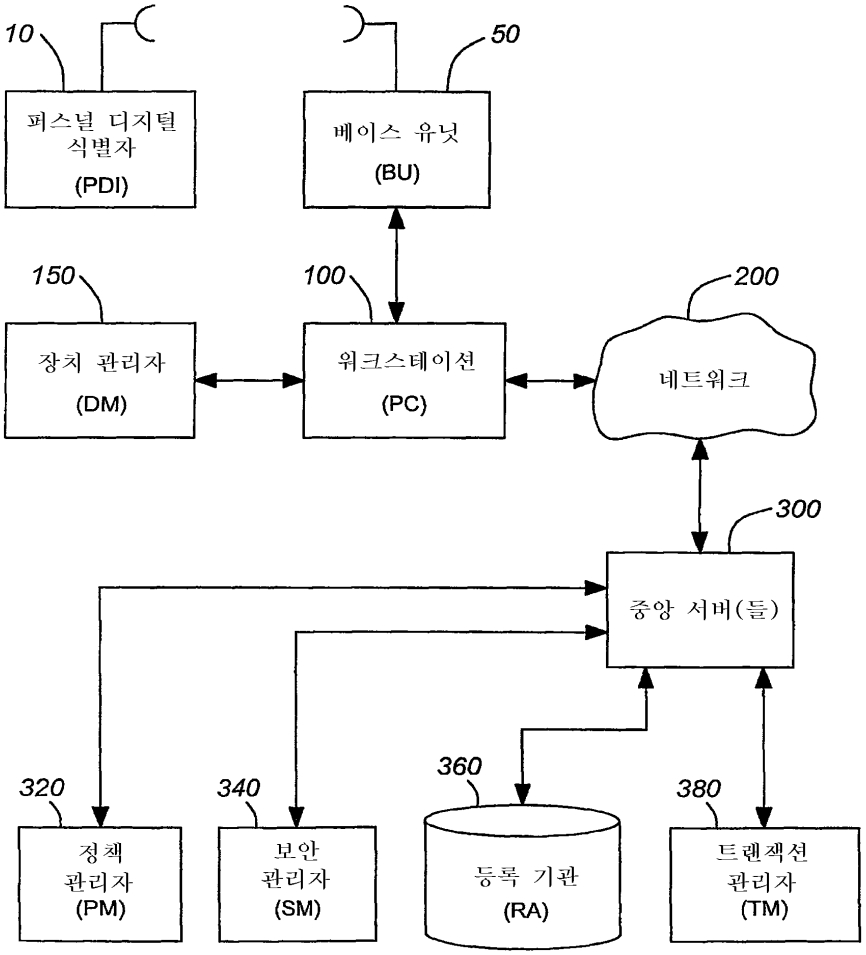
<22> 도 3은 본 발명의 보안 시스템의 베이스 유닛(BU)의 구성 요소들을 나타내는 블럭도.

<23> 도 4A, 4B, 및 4C는 본 발명에 따른 유저 획득 및 로그-온 프로세스를 설명하는 플로우 챠트.

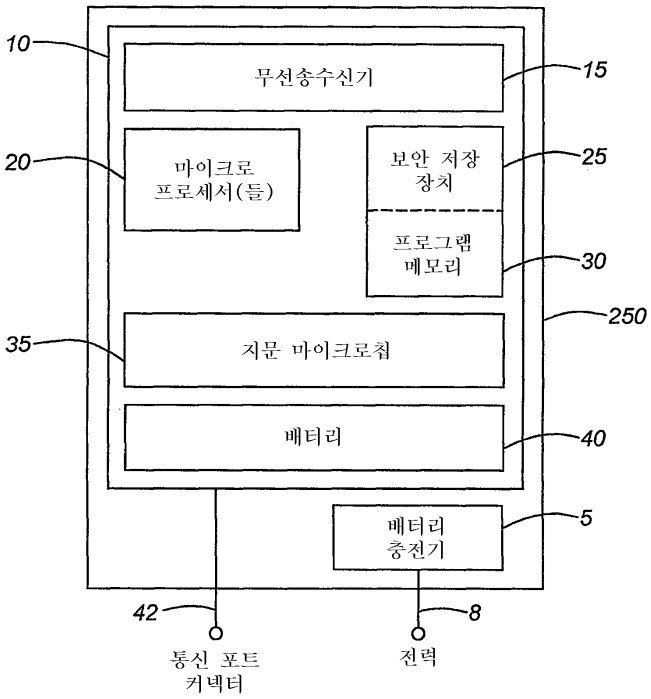
<24> 도 5A 및 5B는 디지털 서명을 생성하기 위한 본 발명의 바람직한 실시예의 보안 시스템에 의해 사용되는 프로세스를 설명하는 플로우 챠트.

## 도면

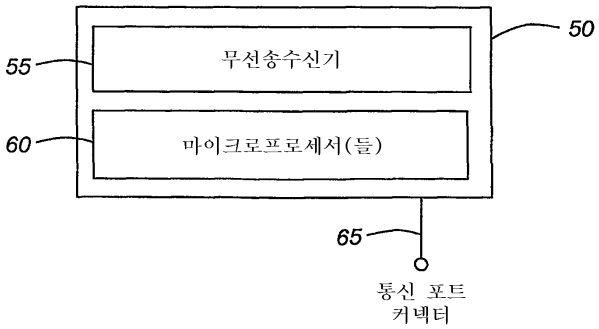
### 도면1


10
퍼스널 디지털 식별자 (PDI)
50
베이스 유닛 (BU)
150
장치 관리자 (DM)
100
워크스테이션 (PC)
200
네트워크
300
중앙 서버(들)
320
정책 관리자 (PM)
340
보안 관리자 (SM)
360
등록 기관 (RA)
380
트랜잭션 관리자 (TM)

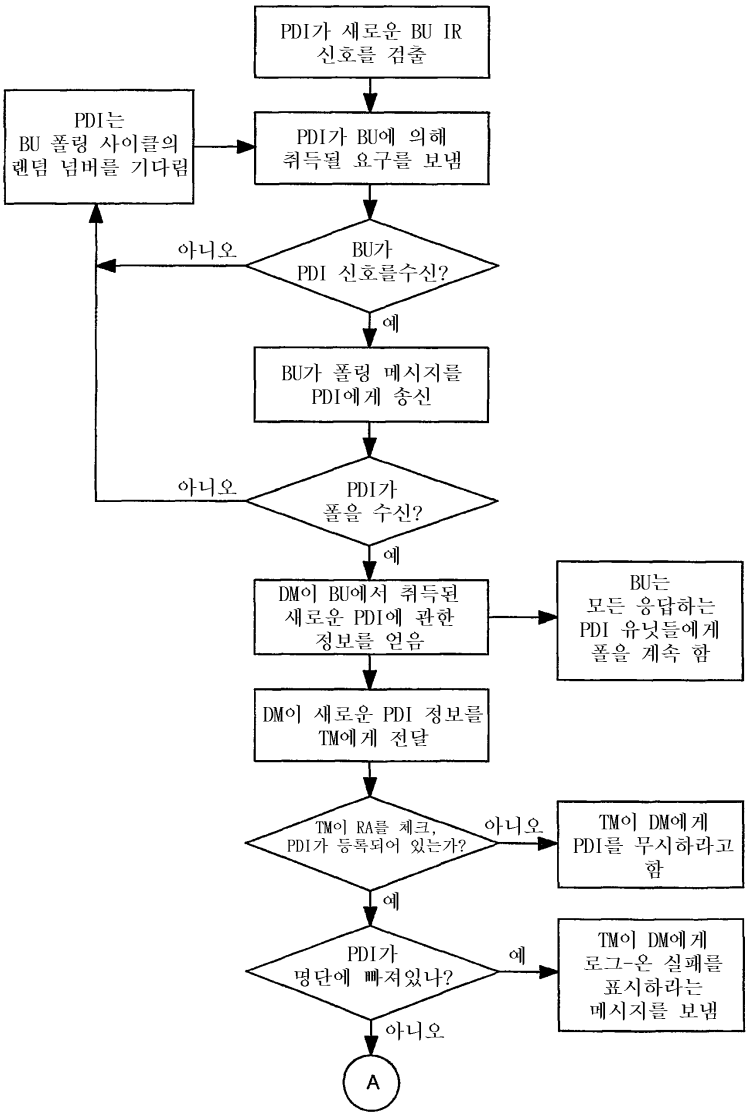
도면2


10
무선송수신기
15
20
마이크로
프로세서(들)
보안 저장
장치
25
프로그램
메모리
30
250
35
지문 마이크로칩
배터리
40
배터리
충전기
5
42
8
통신 포트
커넥터
전력

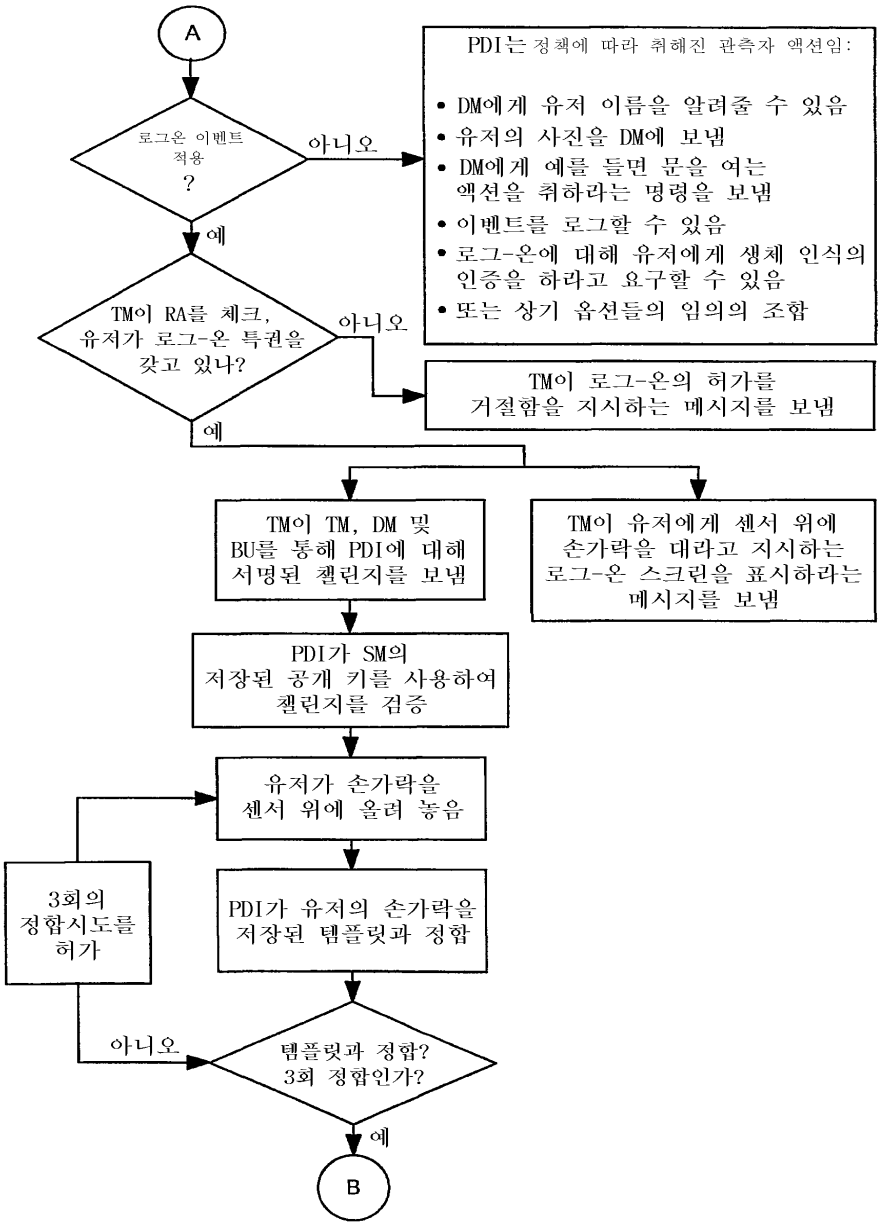
도면3


50
55
무선송수신기
60
마이크로프로세서(들)
65
통신 포트
커넥터

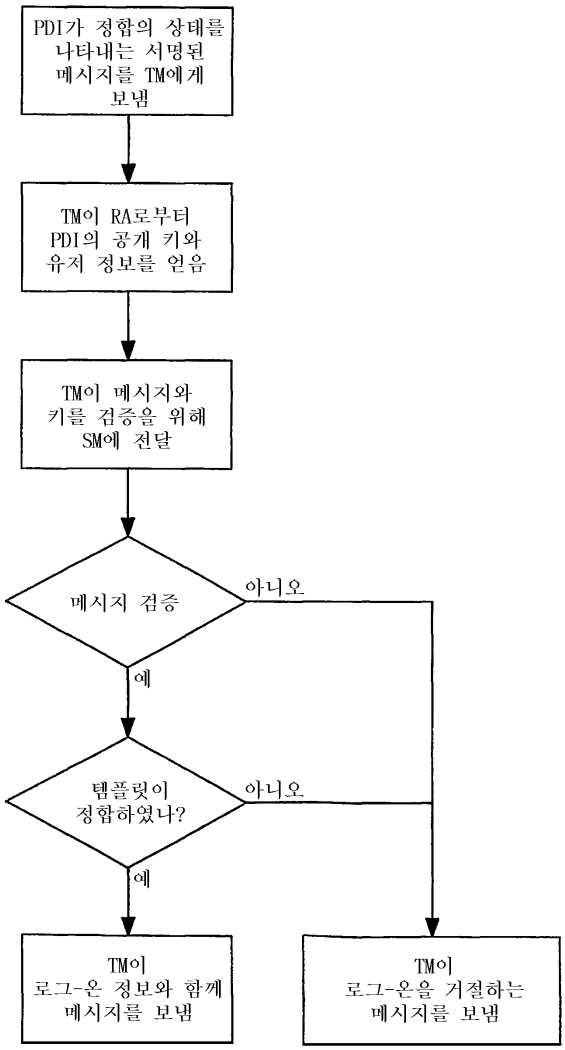
도면4A


PDI가 새로운 BU IR 신호를 검출
PDI는 BU 폴링 사이클의 랜덤 넘버를 기다림
PDI가 BU에 의해 취득될 요구를 보냄
BU가 PDI 신호를수신?
아니오
예
BU가 폴링 메시지를 PDI에게 송신
PDI가 폴을 수신?
아니오
예
DM이 BU에서 취득된 새로운 PDI에 관한 정보를 얻음
BU는 모든 응답하는 PDI 유닛들에게 폴을 계속 함
DM이 새로운 PDI 정보를 TM에게 전달
TM이 RA를 체크, PDI가 등록되어 있는가?
아니오
TM이 DM에게 PDI를 무시하라고 함
예
PDI가 명단에 빠져있나?
예
TM이 DM에게 로그-온 실패를 표시하라는 메시지를 보냄
아니오
A

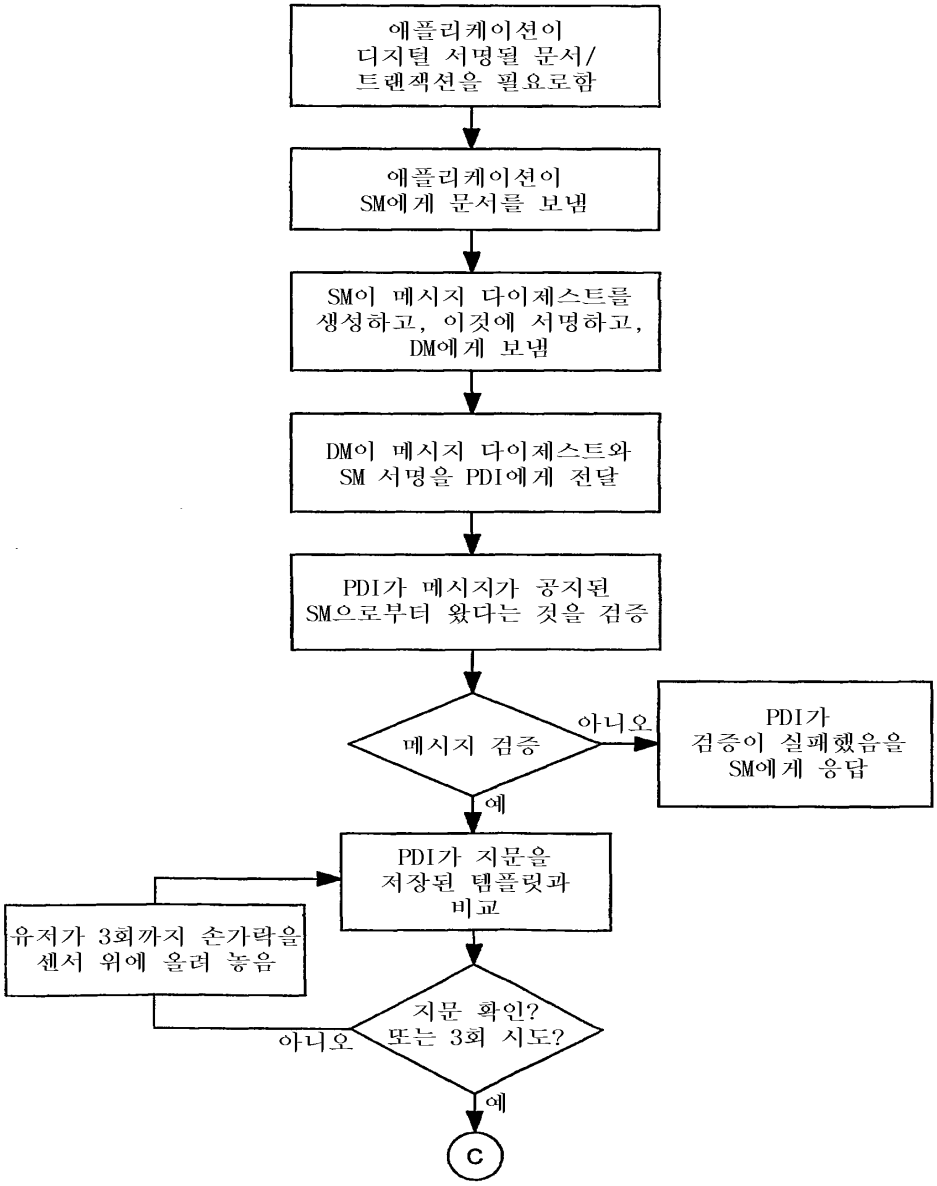
도면4B


A
로그온 이벤트 적용 ?
아니오
예
PDI는 정책에 따라 취해진 관측자 액션임:
• DM에게 유저 이름을 알려줄 수 있음
• 유저의 사진을 DM에 보냄
• DM에게 예를 들면 문을 여는 액션을 취하라는 명령을 보냄
• 이벤트를 로그할 수 있음
• 로그-온에 대해 유저에게 생체 인식의 인증을 하라고 요구할 수 있음
• 또는 상기 옵션들의 임의의 조합
TM이 RA를 체크, 유저가 로그-온 특권을 갖고 있나?
아니오
예
TM이 로그-온의 허가를 거절함을 지시하는 메시지를 보냄
TM이 TM, DM 및 BU를 통해 PDI에 대해 서명된 챌린지를 보냄
TM이 유저에게 센서 위에 손가락을 대라고 지시하는 로그-온 스크린을 표시하라는 메시지를 보냄
PDI가 SM의 저장된 공개 키를 사용하여 챌린지를 검증
유저가 손가락을 센서 위에 올려 놓음
3회의 정합시도를 허가
PDI가 유저의 손가락을 저장된 템플릿과 정합
아니오
템플릿과 정합? 3회 정합인가?
예
B

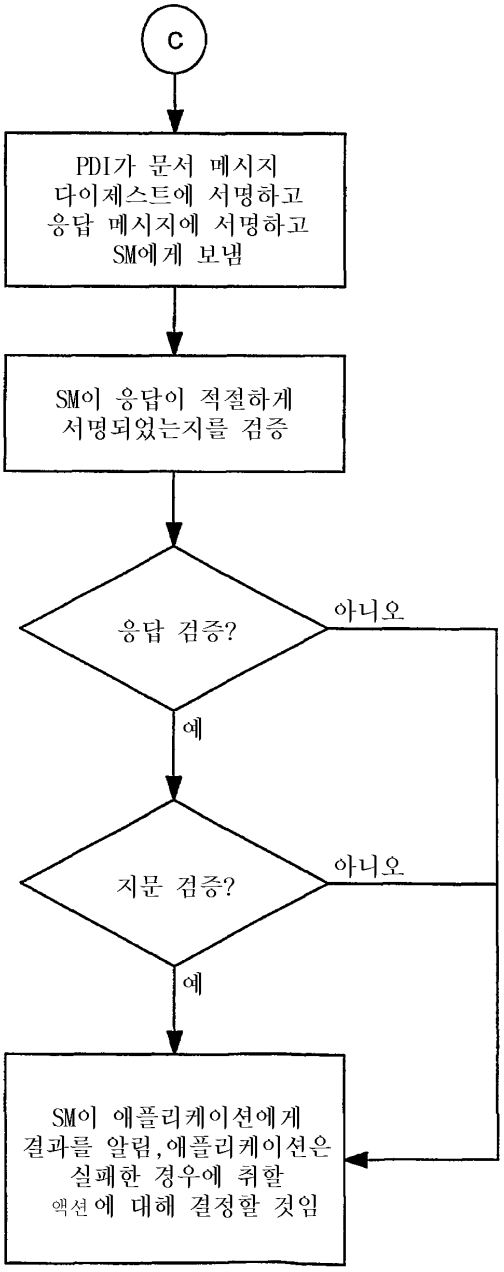
도면4C


PDI가 정합의 상태를 나타내는 서명된 메시지를 TM에게 보냄
TM이 RA로부터 PDI의 공개 키와 유지 정보를 얻음
TM이 메시지와 키를 검증을 위해 SM에 전달
메시지 검증
아니오
예
템플릿이 정합하였나?
아니오
예
TM이 로그-온 정보와 함께 메시지를 보냄
TM이 로그-온을 거절하는 메시지를 보냄

도면5A


애플리케이션이
디지털 서명될 문서/
트랜잭션을 필요로함
애플리케이션이
SM에게 문서를 보냄
SM이 메시지 다이제스트를
생성하고, 이것에 서명하고,
DM에게 보냄
DM이 메시지 다이제스트와
SM 서명을 PDI에게 전달
PDI가 메시지가 공지된
SM으로부터 왔다는 것을 검증
메시지 검증
아니오
PDI가
검증이 실패했음을
SM에게 응답
예
PDI가 지문을
저장된 템플릿과
비교
유저가 3회까지 손가락을
센서 위에 올려 놓음
지문 확인?
또는 3회 시도?
아니오
예
C

도면5B


C
PDI가 문서 메시지 다이제스트에 서명하고 응답 메시지에 서명하고 SM에게 보냄
SM이 응답이 적절하게 서명되었는지를 검증
응답 검증?
아니오
예
지문 검증?
아니오
예
SM이 애플리케이션에게 결과를 알림,애플리케이션은 실패한 경우에 취할 액션에 대해 결정할 것임