(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0050152
(43) 공개일자 2009년05월20일

(51) Int. Cl.
H04L 9/32 (2006.01) *G06F 12/16* (2006.01)
H04B 1/40 (2006.01)
(21) 출원번호 10-2007-0116430
(22) 출원일자 2007년11월15일
심사청구일자 2007년11월15일

(71) 출원인
한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자
한진희
대전 유성구 신성동 125-12 금남빌라 202호
전성익
대전 유성구 어은동 한빛아파트 107동 704호
(74) 대리인
유미특허법인

전체 청구항 수 : 총 8 항

(54) 단말기의 정보 관리 장치 및 그 방법

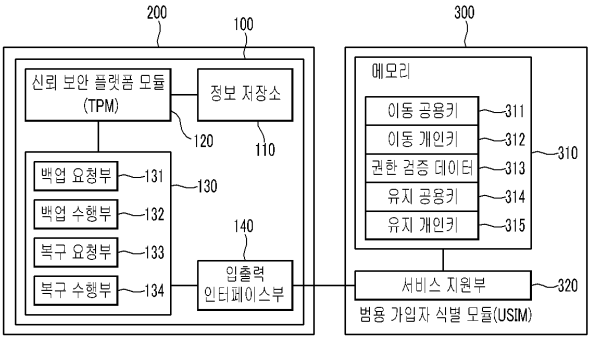
(57) 요 약

본 발명은 단말기의 정보 관리 장치 및 그 방법에 관한 것이다.

본 발명에서는, 단말기에 저장된 정보를 보안할 수 있는 적어도 하나의 키(Key) 및 데이터를 정보 저장소에 저장한다. 그리고, 사용자의 요청 사항이나, 단말기의 변경, 분실 및 고장 등에 대비하기 위해, 정보 저장소에 저장된 키 및 데이터를 단말기에 탈부착 되는 백업 장치 중 하나인 범용 가입자 식별 모듈(USIM)로 이동 저장시킨다. 이후, 사용자의 요청 사항에 따라, 백업 장치로 이동 저장시킨 키 또는 데이터를 소정의 인증 절차를 거쳐 백업 장치로부터 제공 받는다. 그리고, 제공 받은 키 또는 데이터를 정보 저장소에 저장한다.

이를 통해, 단말기 사용자 및 관계자에게 보다 안전하고 편리한 정보 관리 서비스를 제공한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	2006-S-041-02
부처명	정보통신부 및 정보통신연구진흥원
연구사업명	IT성장동력기술개발사업
연구과제명	차세대 모바일 단말기의 보안 및 신뢰 서비스를 위한 공통보안 핵심 모듈 개발
주관기관	한국전자통신연구원
연구기간	2007.03.01~2008.02.28

특허청구의 범위

청구항 1

단말기의 정보 관리 장치에 있어서,

적어도 하나의 키(Key) 및 데이터가 저장되는 정보 저장소;

상기 정보 저장소에 저장된 키 및 데이터 중 적어도 하나를 이용하여 상기 단말기에 저장되는 정보를 보안하는 정보 보안 칩; 및

상기 정보 저장소에 저장된 키 및 데이터 중 적어도 하나를 상기 단말기에 탈부착 되는 백업 장치로 이동 저장시키며, 상기 이동 저장시킨 키 및 데이터 중 적어도 하나를 상기 백업 장치로부터 제공 받아 상기 정보 저장소에 저장하는 정보 관리기

를 포함하는 단말기의 정보 관리 장치.

청구항 2

제1 항에 있어서,

상기 정보 관리기는,

상기 정보 저장소에 저장된 키 및 데이터 중 적어도 하나를 상기 백업 장치로 이동 저장하길 요청하는 메시지인 백업 요청 메시지를 생성하며, 상기 생성된 백업 요청 메시지를 상기 백업 장치로 전송하는 백업 요청부;

상기 전송된 백업 요청 메시지에 따라, 상기 백업 장치로부터 제공되는 적어도 하나의 키 및 권한 검증 데이터를 이용하여 상기 저장된 키 및 데이터를 암호화하며, 상기 암호화된 결과 값을 상기 백업 장치로 전송하는 백업 수행부;

상기 백업 장치로 이동 저장시킨 키 및 데이터 중 적어도 하나를 제공 받길 요청하는 메시지인 복구 요청 메시지를 생성하며, 상기 생성된 복구 요청 메시지를 상기 백업 장치로 전송하는 복구 요청부; 및

상기 전송된 복구 요청 메시지에 따라, 상기 백업 장치로부터 제공되는 적어도 하나의 키 및 데이터를 상기 정보 저장소에 저장하는 복구 수행부

를 포함하는 단말기의 정보 관리 장치.

청구항 3

제2 항에 있어서,

상기 백업 장치는,

상기 이동 저장시킨 키 및 데이터가 저장되는 메모리; 및

상기 전송된 백업 요청 메시지에 따라, 상기 메모리에 저장된 키 및 데이터 중 적어도 하나를 상기 정보 관리기로 제공하며, 상기 정보 관리기로부터 수신되는 적어도 하나의 키 및 데이터를 상기 메모리에 저장하는 서비스 지원부

를 포함하는 단말기의 정보 관리 장치.

청구항 4

제3 항에 있어서,

상기 서비스 지원부는,

상기 전송된 복구 요청 메시지에 따라, 소정의 사용자 인증 절차를 수행하며, 상기 수행된 결과를 토대로 상기 메모리에 저장된 키 및 데이터 중 어느 하나를 상기 정보 관리기로 제공하는 단말기의 정보 관리 장치.

청구항 5

제1 항 내지 제4 항 중 어느 한 항에 있어서,

상기 백업 장치는, 범용 가입자 식별 모듈인 단말기의 정보 관리 장치.

청구항 6

단말기에 저장된 정보를 보안하는 적어도 하나의 키(Key) 및 데이터를 정보 저장소에 저장하는 단계;

상기 저장된 키를 상기 단말기에 탈부착 되는 백업 장치로 이동 저장하길 요청하는 메시지인 백업 요청 메시지를 생성한 후, 상기 생성된 백업 요청 메시지를 상기 백업 장치로 전송하는 단계;

상기 전송된 백업 요청 메시지에 따라, 상기 백업 장치로부터 제공되는 적어도 하나의 키 및 권한 검증 데이터를 이용하여 상기 저장된 키를 암호화하는 단계; 및

상기 암호화된 결과 값과 사전 생성한 일회용 키를 상기 백업 장치로 전송하는 단계

를 포함하는 단말기의 정보 관리 방법.

청구항 7

제6 항에 있어서,

상기 저장된 데이터를 상기 백업 장치로 이동 저장하길 요청하는 메시지인 백업 요청 메시지를 생성한 후, 상기 생성된 백업 요청 메시지를 상기 백업 장치로 전송하는 단계;

상기 전송된 백업 요청 메시지에 따라, 상기 백업 장치로부터 제공되는 적어도 하나의 키를 상기 정보 저장소에 저장하는 단계;

상기 저장된 키를 소정의 형태로 변환한 후, 상기 변환된 결과 값 및, 난수 또는 사용 인가 정보로부터 생성된 문자열에 대해 소정의 연산을 수행하는 단계;

상기 수행된 결과 값을 상기 백업 장치로부터 제공 받은 키를 이용하여 암호화한 후, 상기 암호화된 결과 값과 상기 생성된 문자열을 상기 백업 장치로 전송하는 단계

를 더 포함하는 단말기의 정보 관리 방법.

청구항 8

제6 항에 있어서,

상기 백업 장치에 저장된 적어도 하나의 키 및 데이터를 제공 받길 요청하는 메시지인 복구 요청 메시지를 생성한 후, 상기 생성된 복구 요청 메시지를 상기 백업 장치로 전송하는 단계; 및

상기 전송된 복구 요청 메시지에 따라, 상기 백업 장치로부터 제공되는 키 및 데이터 중 적어도 하나를 상기 정보 저장소에 저장하는 단계

를 더 포함하는 단말기의 정보 관리 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 단말기의 정보 관리 장치 및 그 방법에 관한 것으로서, 보다 상세하게는 범용 가입자 식별 모듈을 이용하여 단말기의 정보를 관리하는 장치 및 그 방법에 관한 것이다.

<2> 본 발명은 정보통신부 및 정보통신연구진흥원의 IT성장동력기술개발사업의 일환으로 수행한 연구로부터 도출된 것이다[과제관리번호: 2006-S-041-02, 과제명: 차세대 모바일 단말기의 보안 및 신뢰 서비스를 위한 공통 보안 핵심 모듈 개발].

배 경 기 술

<3> 최근 들어, 컴퓨터 시스템을 포함한 각종 단말기 등에 대한 보안 위협이 급증하면서, 그 해결 방안을 다양한 각도에서 검색 및 개발하고 있다. 이중, 소프트웨어적인 보안 방식이 대다수를 이루는데, 이는 그 특성상 여러 문

제점들이 발견되고 있다.

<4> 실제로 소프트웨어적인 보안 방식은 예를 들어, 사용자가 자신이 가지고 있던 데이터 저장소를 분실하게 되면, 분실된 저장소에 저장되어 있던 개인적인 데이터는 고스란히 유출된다. 또한, 기존의 보안 방식은 암호화 키가 쉽게 외부에 노출될 수 있기 때문에, 해킹의 위협시 아무런 보호 기능을 하지 못한다.

<5> 이로 인해, 각종 문제점들을 해결하기 위한 방안으로서 하드웨어를 사용한 보안 방식이 제안되고 있다. 그 중 하나가 바로 TCG(Trusted Computing Group, 이하 'TCG'라 함)의 TPM(Trusted Platform Module : 신뢰할 수 있는 플랫폼 모듈, 이하 'TPM'이라 함) 칩이다.

<6> 구체적으로, TPM 칩은 CPU 프로세서와는 달리 단순히 키 값이나 패스워드, 디지털 인증서 등을 저장할 수 있는 저장 공간을 제공함과 동시에, 암호화 엔진을 제공한다. 즉, 각각의 TPM 칩은 제조될 때 고유의 키인 EK(Endorsement Key) 및 SRK(Storage Root Key)가 할당되는데, 이 키 값들은 칩 외부로 나가지 못하게 되어 있다.

<7> 따라서, TPM 칩은 그 특성상 기존의 소프트웨어적인 보안 방식이 가지는 여러 취약점들을 보안할 수 있어, 근래 들어 사용자 및 관계자들에게 각광받고 있는 추세이다.

<8> TCG는 지난 2003년에 결성된 일종의 컨소시엄으로서, 그 동안 컴퓨터, 휴대폰 및 PDA 등에 사용될 보안 규격을 마련해 공개하고 있다. 그 예로, 단말기에 장착된 TPM 칩이 동작하지 않거나, 또는 단말기 분실 및 변경시 요구되는 중요 데이터의 백업, 이동 매커니즘을 위한 기능 및 명령어 등을 정의하고 있다.

<9> 그러나, TCG에서 정의한 규격은 정보 보안에 있어서 플랫폼(Platform)이나 TPM 칩 제조사의 참여를 필수적으로 요구하며, 일부 기능에 대해서는 선택 사항으로 규정하고 있어, 현재 일부 칩 제조업체에서는 그 일부 기능을 처음부터 배제하고 제공하지 않는 경우도 있다.

<10> 따라서, 각종 단말기에 저장된 개인적인 정보 보안 및 관리에 있어, 사용자 및 관계자들에게 기존 방식보다 향상된 안정성 및 편의성을 제공할 수 있는 방안이 현실적으로 요구되고 있는 실정이다.

발명의 내용

해결 하고자하는 과제

<11> 본 발명이 이루고자 하는 기술적 과제는 단말기의 정보 보안을 위해 사용하는 키 및 데이터를 백업 장치로 백업(Back-up)시키며, 백업된 키 및 데이터를 백업 장치로부터 제공 받아 단말기에 저장할 수 있는 장치 및 그 방법을 제공하기 위한 것이다.

과제 해결수단

<12> 이러한 목적을 달성하기 위한 본 발명의 특징에 따른 단말기의 정보 관리 장치는, 적어도 하나의 키(Key) 및 데이터가 저장되는 정보 저장소; 상기 정보 저장소에 저장된 키 및 데이터 중 적어도 하나를 이용하여 상기 단말기에 저장되는 정보를 보안하는 정보 보안 칩; 및 상기 정보 저장소에 저장된 키 및 데이터 중 적어도 하나를 상기 단말기에 탈부착 되는 백업 장치로 이동 저장시키며, 상기 이동 저장시킨 키 및 데이터 중 적어도 하나를 상기 백업 장치로부터 제공 받아 상기 정보 저장소에 저장하는 정보 관리기를 포함한다.

<13> 또한, 본 발명의 다른 특징에 따른 단말기의 정보 관리 방법은, 단말기에 저장된 정보를 보안하는 적어도 하나의 키(Key) 및 데이터를 정보 저장소에 저장하는 단계; 상기 저장된 키를 상기 단말기에 탈부착 되는 백업 장치로 이동 저장하길 요청하는 메시지인 백업 요청 메시지를 생성한 후, 상기 생성된 백업 요청 메시지를 상기 백업 장치로 전송하는 단계; 상기 전송된 백업 요청 메시지에 따라, 상기 백업 장치로부터 제공되는 적어도 하나의 키 및 권한 검증 데이터를 이용하여 상기 저장된 키를 암호화하는 단계; 및 상기 암호화된 결과 값과 사전 생성한 일회용 키를 상기 백업 장치로 전송하는 단계를 포함한다.

효 과

<14> 본 발명에 따르면, 단말기의 정보 보안을 위해 사용하는 키 및 데이터를 단말기에 탈부착 되는 백업 장치, USIM으로 백업시키거나, 백업된 키 및 데이터를 USIM으로부터 제공 받아 단말기에 저장한다. 이를 통해, 단말기 사용자 및 관계자에게 보다 안전하고 편리한 정보 관리 서비스를 제공할 수 있다.

발명의 실시를 위한 구체적인 내용

<15> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시 예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

<16> 명세서 전체에서, 어떤 부분이 어떤 구성 요소를 "포함" 한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

<17> 또한, 이하 본 발명의 실시 예에서는 보안 칩 중의 하나인 TPM(Trusted Platform Module)에 저장된 정보를 관리하는 것에 대해 설명한다. 하지만, 본 발명이 이에 한정되는 것은 아니며, 경우에 따라서는 단말기 내 다른 메모리 또는 모듈 등에 저장된 정보를 관리하는 것에 대해 적용할 수 있다.

<18> 또한, 이하 본 발명의 실시 예에서는 설명의 편의를 위하여 보안 칩에 저장된 정보를 단말기에 탈부착 되는 백업 장치로 이동 저장시키는 것을 '백업'이라 명명하며, 백업된 정보를 백업 장치로부터 제공 받아 저장시키는 것을 '복구'라 명명한다.

<19> 먼저, 본 발명의 실시 예에 따른 단말기의 정보 관리 장치에 대해 알아본다.

<20> 도 1은 본 발명의 실시 예에 따른 단말기의 정보 관리 장치를 도시한 도면이다.

<21> 도 1에 도시된 바와 같이, 본 발명의 실시 예에 따른 정보 관리 장치(100)는 단말기(200) 내에 포함되며, 정보 저장소(Protected storage, 110), 신뢰 보안 플랫폼 모듈(Trusted Platform Module, 120), 정보 관리기(130) 및 입출력 인터페이스부(140)를 포함한다.

<22> 그리고, 정보 관리기(130)는 백업 요청부(131), 백업 수행부(132), 복구 요청부(133) 및 복구 수행부(134)를 포함한다.

<23> 또한, 본 발명의 실시 예에 따른 USIM(Universal Subscriber Identity Module : 범용 가입자 식별 모듈, 이하 'USIM'이라 함, 300)은 단말기(200)에 탈부착 되는 백업 장치 중 하나로서, 메모리(310) 및 서비스 지원부(320)를 포함한다.

<24> 참고로, 서비스 지원부(320)는 신뢰 보안 플랫폼 모듈(120)과 관련된 키 및 데이터를 백업하거나 복구하는 카드 애플릿(Card Applet)이다.

<25> 구체적으로, 정보 저장소(110)는 고유 키인 SRK(Storage Root Key, 이하 'SRK'라 함)를 중심으로 계층 구조를 이루는 적어도 하나의 키(Key) 및 데이터(Secret data)가 함께 저장된다.

<26> 신뢰 보안 플랫폼 모듈(120)은 정보 보호시 사용하는 적어도 하나의 키 및 데이터(예를 들어, 패스워드 및 디지털 인증서 등)를 정보 저장소(110)에 저장 및 관리한다.

<27> 정보 관리기(130)는 신뢰 보안 플랫폼 모듈(120)이 정보 저장소(110)에 저장한 키 및 데이터를 USIM(300)으로 백업시키며, 백업된 정보를 USIM(300)으로부터 제공 받아 정보 저장소(110)에 저장시킨다.

<28> 구체적으로, 정보 관리기(130)의 백업 요청부(131)는 정보 저장소(110)에 저장된 적어도 하나의 키를 USIM(300)으로 이동 저장, 즉 백업(Back-up)하길 요청하는 메시지(이하 '백업 요청 메시지'라 함)를 생성한 후, 생성된 백업 요청 메시지를 USIM(300)으로 전송한다.

<29> 참고로, 본 발명의 실시 예에 따른 정보 관리 장치(100)는 APDU(Application Protocol Data Unit, 이하 'APDU'라 함) 형태로 메시지를 생성하여 USIM(300)으로 전송한다. 그리고, USIM(300) 역시 수신된 메시지에 대한 응답 메시지를 APDU 형태로 생성하여 정보 관리 장치(100)로 전송한다.

<30> 백업 수행부(132)는 전송한 백업 요청 메시지에 따라, USIM(300)으로부터 제공되는 데이터(키 및 권한 검증 데이터 등)를 이용하여 백업하고자 하는 키를 소정의 형태로 변환한다. 그리고, 변환된 키 및 자체적으로 생성한 일회용 키(One-time pad)에 대해 비 등가 연산(예를 들어, Exclusive-or operation 등)을 수행한다.

<31> 이어, 백업 수행부(132)는 수행된 결과 값을 앞서 USIM(300)으로부터 제공 받은 데이터(키)를 통해 암호화한 후, 암호화된 최종적인 결과 값 및 앞서 생성된 일회용 키를 USIM(300)으로 송신한다.

<32> 복구 요청부(133)는 USIM(300)으로 백업시킨 적어도 하나의 키를 단말기(200)로 이동 저장, 즉 복구하길 요청하는 메시지(이하 '복구 요청 메시지'라 함)를 생성한 후, 생성된 복구 요청 메시지를 USIM(300)으로 전송한다.

<33> 복구 수행부(134)는 전송한 복구 요청 메시지에 따라, USIM(300)으로부터 제공 받는 데이터를 소정 형태로 변환한 후, 변환된 결과 값 내의 적어도 하나의 키를 신뢰 보안 플랫폼 모듈(120)을 통해 정보 저장소(110)에 저장한다.

<34> 입출력 인터페이스부(140)는 정보 관리 장치(100) 및 USIM(300)간의 데이터 송수신을 지원한다.

<35> 다음, USIM(300)은 단말기(200)로부터 적어도 하나의 키 및 데이터를 백업 받아 메모리(310)에 저장시키며, 메모리(310)에 저장된 키 및 데이터를 사용자의 요청 사항에 따라 단말기(200)로 제공한다.

<36> 구체적으로, USIM(300)의 메모리(310)는 단말기(200)로부터 백업 받은 키 및 데이터 뿐만 아니라, 이동 공용 키(Migration Public Key, 311), 이동 개인 키(Migration Private Key, 312), 권한 검증 데이터(Authorization Data, 313), 유지 공용 키(Maintenance Public Key, 314) 및 유지 개인 키(Maintenance Private Key, 315) 값이 저장된다.

<37> 서비스 지원부(320)는 정보 관리기(130)로부터 백업 요청 메시지가 수신되면, 메모리(310)에 저장된 정보 중 이동 공용 키 및 권한 검증 데이터를 APDU 형태로 변환하여 정보 관리기(130)로 제공한다. 그리고, 제공된 정보에 따라 해당 단말기로부터 백업되는 키 및 데이터를 메모리(310)에 저장한다.

<38> 또한, 서비스 지원부(320)는 정보 관리기(130)로부터 복구 요청 메시지가 수신되면, 소정의 사용자 인증 절차(예를 들어, 비밀번호 일치 등)를 수행한다.

<39> 그리고, 수행된 결과에 따라 메모리(320)에 저장된 데이터를 이동 개인 키(312)로 복호화한 후, 복호화된 결과 값을 정보 관리기(130)로부터 전달된 공용 키(Public key)를 이용하여 암호화한다. 그리고, 암호화된 결과 값 및 일회용 키를 정보 관리 장치(100)로 제공한다.

<40> 이처럼, 본 발명의 실시 예에 따른 정보 관리 장치(100)는 신뢰 보안 플랫폼 모듈(120)이 정보 보안을 위해 사용하는 키 및 데이터를 단말기(200)와 탈부착 되는 백업 장치 중 하나인 USIM(300)으로 백업시킨다. 그리고, 백업된 키 및 데이터를 USIM(300)으로부터 제공 받아 단말기(100) 내 해당 공간에 저장시킨다.

<41> 이를 통해, 본 발명의 실시 예에 따르면, 단말기 사용자 또는 신뢰 보안 플랫폼 모듈(TPM)을 제조하는 업체 및 관계자로 하여금 일반적인 보안 규격(예를 들어, TCG 규격 등)에 기술된 방식 보다 좀 더 편리하면서 안전한 정보 관리를 제공할 수 있다.

<42> 참고로, 본 발명의 실시 예에서는 정보 관리 장치(100)가 신뢰 보안 플랫폼 모듈(120, TPM)을 통해 정보 저장소(110)에 저장된 키 및 데이터만을 백업시키거나, 또는 복구하는 것에 대해 설명한다. 하지만, 앞서 언급한 바와 같이 본 발명이 이에 한정되는 것은 아니며, 경우에 따라서는 단말기 내 다른 메모리 또는 모듈 등에 저장된 각종 정보를 백업시키거나 복구할 수 있다.

<43> 그러면, 위에 기술된 구조로 이루어지는 정보 관리 장치를 토대로, 본 발명의 실시 예에 따른 정보 관리 방법에 대해 설명한다.

<44> 먼저, 본 발명의 실시 예에 따른 정보 관리 방법 중, 정보 저장소(110)에 저장된 키 및 데이터를 USIM(300)으로 백업시키는 과정에 대해 알아본다.

<45> 도 2는 도 1에 도시된 정보 관리 장치의 동작 과정 중, 백업 과정을 순차적으로 도시한 흐름도이다.

<46> 먼저, 정보 저장소(110)에 저장된 이동 가능한(Migratable) 키를 USIM(300)으로 백업시키는 과정에 대해 알아본다.

<47> 도 2에 도시되어 있듯이, 단말기 사용자가 정보 저장소(110)에 저장된 키 및 데이터 중 적어도 하나의 키를 백업(S210, S220) 시키고자 하면, 정보 관리 장치(100)의 백업 요청부(131)는 USIM(300)으로 백업 요청 메시지를 전송한다(S230).

<48> 그러면, USIM(300)의 서비스 지원부(320)는 수신된 백업 요청 메시지에 따라, 메모리(310)에 저장된 정보 중 이

동 공용 키 및 권한 검증 데이터를 APDU 형태로 변환하여 정보 관리기(130)로 제공한다(S231).

<49> 이후, 백업 수행부(132)는 USIM(300)으로부터 제공 받은 데이터(키 및 권한 검증 데이터 등)를 이용하여 백업하고자 하는 키를 소정의 형태로 변환한다(S232). 그리고, 변환된 키 및 자체적으로 생성한 일회용 키(One-time pad)에 대해 비 등가 연산(예를 들어, Exclusive-or operation 등)을 수행한다(S233).

<50> 이후, 백업 수행부(132)는 수행된 결과 값을 앞서 USIM(300)으로부터 제공 받은 데이터(키)를 통해 암호화(S234)한 후, 암호화된 최종적인 결과 값 및 앞서 생성한 일회용 키를 USIM(300)으로 송신한다(S235).

<51> 그러면, USIM(300)의 서비스 지원부(320)는 수신된 데이터를 메모리(310)에 저장한다(S236).

<52> 다음, 단말기(200)에 장착된 신뢰 보안 플랫폼 모듈(120)이 동작하지 않거나, 단말기의 분실 또는 변경 상황 등을 대비하기 위해, 정보 저장소(110)에 저장된 데이터를 USIM(300)으로 백업시키는 과정에 대해 알아본다.

<53> 도 2에 도시되어 있듯이, 단말기 사용자가 정보 저장소(110)에 저장된 데이터를 백업(S210, S220) 시키고자 하면, 정보 관리기(130)의 백업 요청부(131)는 USIM(300)으로 백업 요청 메시지를 전송한다(S240).

<54> 그러면, USIM(300)의 서비스 지원부(320)는 수신된 백업 요청 메시지에 따라, 메모리(310)에 저장된 유지 공용 키(314)를 읽어 들여 정보 관리기(130)로 제공한다(S241).

<55> 이후, 백업 수행부(132)는 USIM(300)으로부터 제공 받은 유지 공용 키(314)를 소정의 기능(TPM_LoadManuMaintPub)을 통해 신뢰 보안 플랫폼 모듈(120)이 관리하는 정보 저장소(110)에 저장한다(S242).

<56> 이후, 신뢰 보안 플랫폼 모듈(120)은 소정의 기능(TPM_CreateMaintenance- Archive)을 통해 정보 저장소(110)에 저장된 SRK 및 권한 검증 데이터 등을 소정의 형태로 변환하여 안전환 데이터 구조로 만든다(S243).

<57> 그리고, 신뢰 보안 플랫폼 모듈(120)은 난수(Random number) 또는 사용 인가(Usage Authorization) 정보로부터 생성한 문자열(String)을 앞서 만든 안전한 데이터 구조와 함께 비 등가 연산(예를 들어, Exclusive-or operation 등) 시킨다(S244). 이어, 그 결과 값을 앞서 USIM(300)으로부터 제공 받은 유지 공용 키(314)로 암호화한다(S245).

<58> 이후, 백업 수행부(132)는 암호화된 최종 결과 값과, 난수 또는 사용 인가 정보로부터 생성한 문자열을 함께 APDU 형태로 변환하여 USIM(300)으로 전송한다(S246).

<59> 그러면, USIM(300)의 서비스 지원부(320)는 수신된 데이터를 메모리(310)에 저장한다(S247).

<60> 다음, 본 발명의 실시 예에 따른 정보 관리 방법 중, USIM(300)으로부터 키 및 데이터를 제공 받아 단말기(200)에 저장하는 과정에 대해 알아본다.

<61> 도 3은 도 1에 도시된 정보 관리 장치의 동작 과정 중 복구 과정을 순차적으로 도시한 흐름도이다.

<62> 먼저, USIM(300)으로부터 이동 가능한(Migratable) 키를 제공 받아 정보 저장소(110)에 저장하는 과정에 대해 알아본다.

<63> 도 3에 도시되어 있듯이, 단말기 사용자가 USIM(300)으로 백업시킨 적어도 하나의 키를 정보 관리 장치(100)의 정보 저장소(110)로 이동 저장, 즉 복구(S310, S320)하길 요청하면, 복구 요청부(133)는 복구 요청 메시지를 USIM(300)으로 전송한다(S330).

<64> 이때, 복구 요청 메시지는 이동 가능한 키(Migratable key)를 암호화할 수 있는 공용 키(Public key)를 포함한다.

<65> 그러면, USIM(300)의 서비스 지원부(320)는 소정의 사용자 인증 절차(예를 들어, 비밀번호 일치 등)를 수행한다(S331).

<66> 이후, 서비스 지원부(320)는 수행된 인증 절차에 따라 메모리(320)에 저장된 보호 데이터를 이동 개인 키(312)로 복호화(S332)한 후, 복호화된 결과 값을 복구 요청 메시지 내에 포함된 공용 키(Public key)를 이용하여 암호화한다(S333).

<67> 그리고, 서비스 지원부(320)는 암호화된 결과 값 및 일회용 키를 정보 관리 장치(100)로 제공한다(S334).

<68> 이후, 정보 관리 장치(100)의 복구 수행부(134)는 USIM(300)으로부터 제공 받은 데이터를 소정 형태로 변환한 후, 변환된 결과 값 내의 적어도 하나의 키를 신뢰 보안 플랫폼 모듈(120)을 통해 정보 저장소(110)에 저장한다

(S335).

<69> 이후, 복구 수행부(130)는 정보 저장소(110)에 해당 키가 성공적으로 저장되었음을 알리는 보고 메시지를 USIM(300)으로 전송(S336)하며, USIM(300)의 서비스 지원부(320)는 수신된 보고 메시지에 따라 메모리(310)에 저장된 이동(Migration) 관련 정보를 삭제한다(S337).

<70> 다음, 단말기의 분실 또는 변경 상황 등에 대비하기 위해 USIM(300)에 백업된 신뢰 보안 플랫폼 모듈(120)의 데이터를 정보 저장소(110)에 저장하는 과정에 대해 알아본다.

<71> 도 3에 도시되어 있듯이, 단말기 사용자가 USIM(300)으로 백업시킨 데이터를 정보 관리 장치(100)의 정보 저장소(110)로 이동 저장, 즉 복구(S310, S320)하길 요청하면, 복구 요청부(133)는 복구 요청 메시지를 USIM(300)으로 전송한다(S340).

<72> 이때, 복구 요청 메시지는 신뢰 보안 플랫폼 모듈(120)의 데이터를 암호화할 수 있는 공용 키(Public key)를 포함한다.

<73> 그러면, USIM(300)의 서비스 지원부(320)는 사용자 인증 절차에 따라 단말기 사용자에게 비밀 번호를 요청한다(S341). 그리고, 그 인증 결과에 따라 메모리(310)에 저장된 보호 데이터를 유지 개인 키(315)로 복호화한다(S342).

<74> 이후, 서비스 지원부(320)는 복호화된 결과 값을 복구 요청 메시지 내에 포함된 공용 키(Public key)를 이용하여 암호화한다(S343).

<75> 이후, 서비스 지원부(320)는 암호화된 결과 값을, 난수 또는 사용 인가 정보로부터 생성한 문자열과 함께 APDU 형태로 변환시켜 정보 관리 장치(100)로 전송한다(S344).

<76> 그러면, 정보 관리 장치(100)의 복구 수행부(134)는 수신된 메시지로부터 SRK, 권한 검증 데이터 및 신뢰 보안 플랫폼 모듈을 식별할 수 있는 고유 데이터 값(tpmproof)을 추출한 후, 추출된 값을 신뢰 보안 플랫폼 모듈(120)을 통해 정보 저장소(110)에 저장한다(S345).

<77> 참고로, 정보 저장소(110)에 저장된 키 및 데이터의 구조에 대한 표시 예가 첨부된 도 4이다.

<78> 도 4는 본 발명의 실시 예에 따라 정보 저장소에 저장된 키 및 데이터의 구조를 도시한 도면이다.

<79> 도 4에 도시되어 있듯이, 정보 저장소(110)에는 신뢰 보안 플랫폼 모듈(120)의 소유자가 소유권 획득(TakeOwnership) 과정을 수행하면 생성되는 고유 키인 SRK(401)가 루트(Root) 역할을 수행하며, SRK(401)를 중심으로 계층 구조를 이루는 서명 키(Signature key, 402), 보호 데이터(Secret data, 403) 및 저장 키(Storage key, 404)가 저장된다. 그리고, 저장 키(404)를 중심으로 적어도 하나의 다른 저장 키(405~400n)가 트리 형태로 저장된 구조를 이룬다.

<80> 구체적으로, 하나의 저장 키(404, 일명 부모 키)를 이용하여 적어도 하나의 다른 저장 키(405~408)를 암호화할 수 있으며, 특정 키(405)를 사용하고자 할 경우, 특정 키(405)와 그 키의 부모 키(404)를 모두 신뢰 보안 플랫폼 모듈(120)의 키 슬롯(Slot)으로 로딩한 후, 내부에서 복호화를 수행한다.

<81> 한편, 본 발명은 단말기(200)의 변경, 분실 및 고장 등에 대비하기 위해, USIM(300)의 메모리(310)에 제조사만이 소유할 수 있는 유지 공용 키 쌍(Maintenance key pair)을 저장시켜 제공한다.

<82> 일반적으로, 유지 공용 키 쌍은 오직 제조사만이 소유하고 사용할 수 있는 값으로 명시(TCG 규격)되어 있다. 하지만, 본 발명은 USIM(300) 그 자체가 제조사의 역할을 수행할 수 있도록, USIM(300)에 유지 공용 키 쌍을 저장시켜 제공한다.

<83> 또한, 유지 공용 키 쌍을 USIM(300)에 저장하기 위해서는 USIM 관리자의 PIN(Personal Identification Number : 개인 식별 번호)을 알아야 한다. 이는, 관리자만이 유지 공용 키 값을 USIM(300)에 저장시키거나, 읽어 올 수 있도록 함으로써, 물리적인 안정성을 제공하는 USIM을 통해 신뢰 보안 플랫폼 모듈(TPM)의 정보를 보다 안전하고 편리하게 관리할 수 있도록 한다.

<84> 이처럼, 본 발명의 실시 예에 따른 단말기의 정보 관리 장치는 제조업체나 관계자의 참여를 배제시켜 그로 인한 신뢰성 및 안전성 향상을 이룬다. 그리고, 단말기의 변경, 분실 및 고장 시에 USIM으로부터 정보 보안에 필요한 키 및 데이터를 제공 받아 복구 작업을 수행함으로써, 사용자 및 관계자로 하여금 서비스 만족도 증대를 이룰 수 있다.

<85> 이상에서 설명한 본 발명의 실시 예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시 예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시 예의 기재로부터 본 발명이 속하는 기술 분야의 전문가라면 쉽게 구현할 수 있는 것이다.

<86> 이상에서 본 발명의 실시 예에 대하여 상세하게 설명하였지만 본 발명의 권리 범위는 이에 한정되는 것은 아니고 다음의 청구 범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면의 간단한 설명

<87> 도 1은 본 발명의 실시 예에 따른 단말기의 정보 관리 장치를 도시한 도면이다.

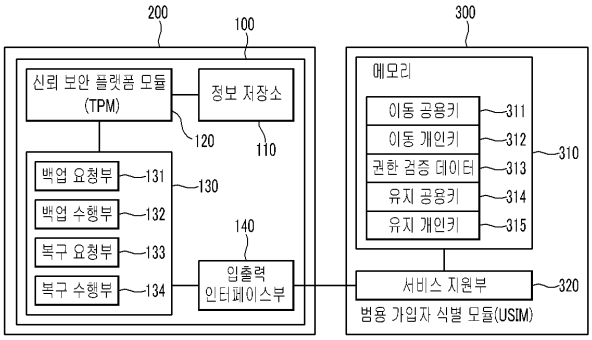
<88> 도 2는 도 1에 도시된 정보 관리 장치의 동작 과정 중, 백업 과정을 순차적으로 도시한 흐름도이다.

<89> 도 3은 도 1에 도시된 정보 관리 장치의 동작 과정 중, 복구 과정을 순차적으로 도시한 흐름도이다.

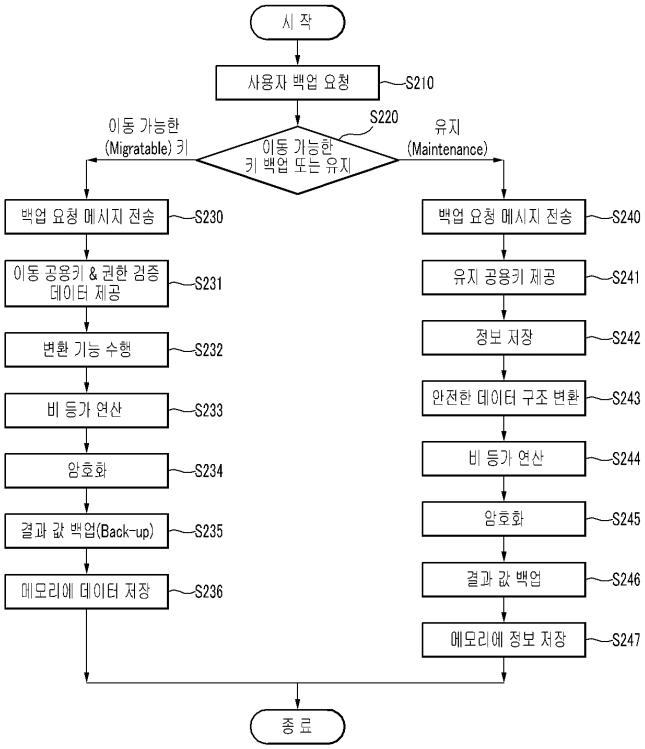
<90> 도 4는 본 발명의 실시 예에 따라 정보 저장소에 저장된 키 및 데이터의 구조를 도시한 도면이다.

도면

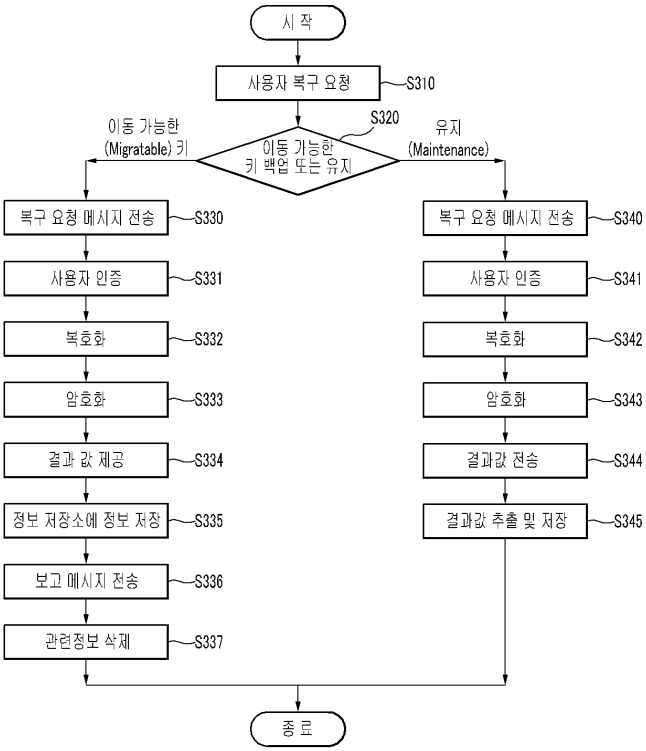
도면1



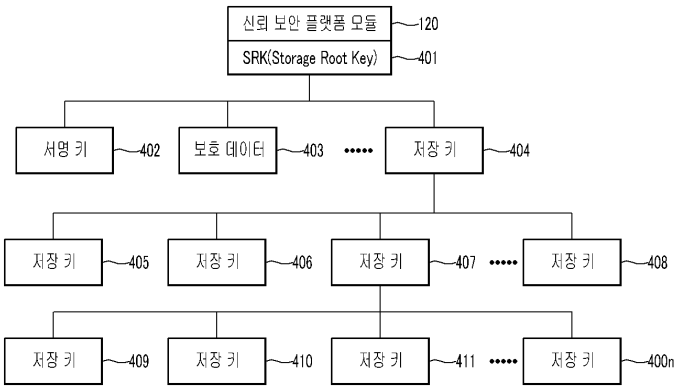
도면2


시 작
사용자 백업 요청
S210
S220
이동 가능한 키 백업 또는 유지
이동 가능한 (Migratable) 키
유지 (Maintenance)
백업 요청 메시지 전송
S230
이동 공용키 & 권한 검증 데이터 제공
S231
변환 기능 수행
S232
비 등가 연산
S233
암호화
S234
결과 값 백업(Back-up)
S235
메모리에 데이터 저장
S236
백업 요청 메시지 전송
S240
유지 공용키 제공
S241
정보 저장
S242
안전한 데이터 구조 변환
S243
비 등가 연산
S244
암호화
S245
결과 값 백업
S246
메모리에 정보 저장
S247
종 료

도면3


시 작
사용자 복구 요청
S310
S320
이동 가능한 키 백업 또는 유지
이동 가능한 (Migratable) 키
유지 (Maintenance)
복구 요청 메시지 전송
S330
사용자 인증
S331
복호화
S332
암호화
S333
결과 값 제공
S334
정보 저장소에 정보 저장
S335
보고 메시지 전송
S336
관련정보 삭제
S337
복구 요청 메시지 전송
S340
사용자 인증
S341
복호화
S342
암호화
S343
결과값 전송
S344
결과값 추출 및 저장
S345
종 료

도면4


신뢰 보안 플랫폼 모듈
120
SRK(Storage Root Key)
401
서명 키
402
보호 데이터
403
저장 키
404
저장 키
405
저장 키
406
저장 키
407
저장 키
408
저장 키
409
저장 키
410
저장 키
411
저장 키
400n