(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0042232
(43) 공개일자 2013년04월26일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04W 12/04* (2009.01)
(21) 출원번호 10-2011-0106410
(22) 출원일자 2011년10월18일
심사청구일자 2011년10월18일

(71) 출원인
에스케이씨앤씨 주식회사
경기도 성남시 분당구 성남대로331번길 8, SKu타워 (정자동)
(72) 발명자
전영환
경기도 화성시 반송동 19 시범한빛마을KCC스위첸 212동 303호
제윤호
서울특별시 강남구 강남대로112길 35, 501호 (논현동)
조승진
서울특별시 강남구 도곡동 렉슬아파트 102동 2003호
(74) 대리인
양성환, 한지나

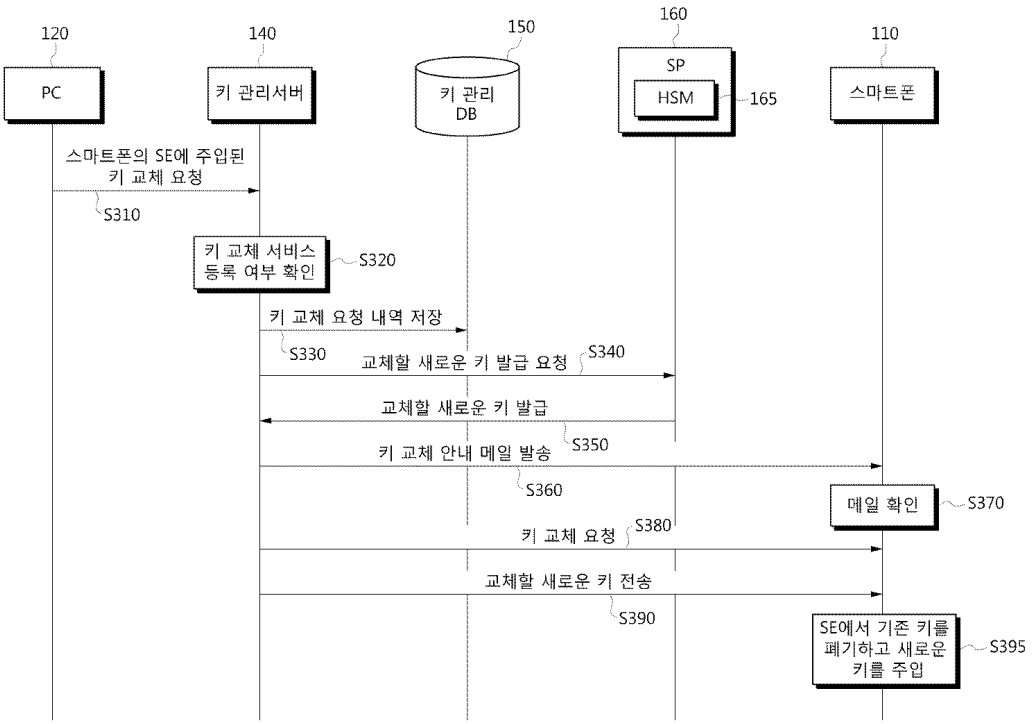
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **모바일 단말기의 S E 키 교체 방법 및 시스템**

(57) 요 약

모바일 단말기의 S E 키 교체 방법 및 시스템이 제공된다. 본 실시예에 따른 SE 키 교체 방법은, 모바일 단말기에 장착된 SE에 주입된 키의 교체를 요청받으면, 교체 요청된 키를 발급한 서비스 제공자에 새로운 키를 요청하여 모바일 단말기에 전달한다. 이에 의해, 사용자의 요청에 의해 SE에 주입된 키를 온-라인으로 교체할 수 있게 되어, 키 노출 등의 이유로 SE 주입된 키 교체가 필요한 경우 사용자가 키 주입 장치가 마련된 기관에 직접 방문하지 않고서도 SE 키 교체가 가능해져, 사용자의 불편을 해소할 수 있게 된다.

대 표 도



특허청구의 범위

청구항 1

모바일 단말기에 장착된 SE(Secure Element)에 주입된 키의 교체를 요청받는 단계;

교체 요청된 키를 발급한 서비스 제공자에 새로운 키를 요청하여 수신하는 단계; 및

상기 수신단계를 통해 수신된 새로운 키를 상기 모바일 단말기에 전달하는 단계;를 포함하는 것을 특징으로 하는 SE 키 교체 방법.

청구항 2

제 1항에 있어서,

상기 전달단계는,

상기 모바일 단말기에 키 교체 안내를 전송하는 단계; 및

상기 키 교체 안내에 대한 응답으로 상기 모바일 단말기로부터 키 교체 요청이 수신되면, 상기 새로운 키를 상기 모바일 단말기에 전달하는 단계;를 포함하는 것을 특징으로 하는 SE 키 교체 방법.

청구항 3

제 1항에 있어서,

상기 전달단계는,

상기 수신단계를 통해 수신된 새로운 키를 상기 모바일 단말기에 푸시 방식으로 전달하는 것을 특징으로 하는 SE 키 교체 방법.

청구항 4

제 3항에 있어서,

상기 모바일 단말기는,

새로운 키가 수신되면, 상기 SE에 주입되어 있는 키를 즉시 폐기하고 새로운 키를 주입하는 것을 특징으로 하는 SE 키 교체 방법.

청구항 5

제 4항에 있어서,

상기 모바일 단말기는,

푸시 알림을 확인한 사용자가 키 교체를 명령한 경우, 상기 SE에 이미 발급된 키를 즉시 폐기하고 새로운 키를 주입하는 것을 특징으로 하는 SE 키 교체 방법.

청구항 6

제 1항에 있어서,

상기 요청단계에서의 교체 요청 내역을 저장하는 단계;를 더 포함하는 것을 특징으로 하는 SE 키 교체 방법.

청구항 7

제 1항에 있어서,

상기 요청단계는,

특정 서비스에 이용되는 키의 교체를 요청받고,

상기 수신단계는,

상기 특정 서비스를 제공하는 서비스 제공자에 새로운 키를 요청하여 수신하는 것을 특징으로 하는 SE 키 교체 방법.

청구항 8

제 1항에 있어서,

상기 모바일 단말기가 온-라인으로 키 교체 서비스를 제공받을 수 있도록 등록된 모바일 단말기인지 확인하는 단계;를 더 포함하고,

상기 수신단계는,

상기 모바일 단말기가 등록된 것으로 확인되면 수행되는 것을 특징으로 하는 SE 키 교체 방법.

청구항 9

제 1항에 있어서,

상기 요청단계는,

상기 모바일 단말기와 분리된 다른 단말기로부터 상기 키의 교체를 요청받는 것을 특징으로 하는 SE 키 교체 방법.

청구항 10

제 1항에 있어서,

상기 요청단계, 상기 수신단계 및 상기 전달단계는,

상기 SE에 주입된 키가 노출된 경우에 수행되는 것을 특징으로 하는 SE 키 교체 방법.

청구항 11

제 1항에 있어서,

상기 요청단계, 상기 수신단계 및 상기 전달단계는,

상기 모바일 단말기, 상기 SE 및 상기 서비스 제공자 중 적어도 하나에 대한 테스트 중에 수행되는 것을 특징으로 하는 SE 키 교체 방법.

청구항 12

제 1항에 있어서,

상기 모바일 단말기에 장착된 SE에 추가 주입할 키를 요청받는 단계;

추가 주입된 키를 발급하는 서비스 제공자에 키를 요청하여 수신하는 단계; 및

상기 수신단계를 통해 수신된 키를 상기 모바일 단말기에 전달하는 단계;를 더 포함하는 것을 특징으로 하는 SE 키 교체 방법.

청구항 13

모바일 단말기에 장착된 SE(Secure Element)에 주입된 키의 교체를 요청받는 통신 인터페이스;

상기 통신 인터페이스를 통해, 교체 요청된 키를 발급한 서비스 제공자에 새로운 키를 요청하여 수신하여 상기 모바일 단말기에 전달하는 제어부;를 포함하는 것을 특징으로 하는 키 관리 서버.

청구항 14

장착된 SE(Secure Element)에 주입된 키의 교체를 요청하는 단계;

상기 요청에 대한 응답으로 새로운 키를 수신하는 단계;

상기 SE에 주입되어 있는 키를 폐기하는 단계; 및

수신된 새로운 키를 상기 SE에 주입하는 단계;를 포함하는 것을 특징으로 하는 SE 키 교체 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 키 교체 방법 및 시스템에 관한 것으로, 더욱 상세하게는 모바일 단말기에 장착된 SE(Secure Element)에 주입된 키를 교체하는 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 모바일 단말기에 장착되는 SE는 통신, 금융, 인증, 결제, 정보관리 등의 서비스를 위한 애플릿과 키가 주입되어 있는 소자로, 형태에 따라 USIM(Universal Subscriber Identity Module), Embedded SE, Secure MC(Secure Memory Card)로 구분될 수 있다.

[0003] USIM은 사용자 정보를 탑재한 SIM(Subscriber Identity Module) 카드와 UICC(Universal IC Card)가 결합된 것으로 현재 가장 많이 활용되는 형태이다.

[0004] Embedded SE는 모바일 단말기의 기판 위에 하나의 부품으로 직접 탑재되는 형태의 SE이다.

[0005] Secure MC는 모바일 단말기에 장착 가능한 외장형 메모리 카드(Micro SD 카드, Micro MMC 카드 등)에 SE를 탑재한 형태이다.

[0006] 이와 같은 SE에 필요한 키를 주입하는 시스템을 도 1에 도시하였다. 도 1에 도시된 바와 같이, 키 주입 장치(20)는 HSM(H/w Secure Mobule)에 의해 생성된 키들을 다양한 SE들(30-1 내지 30-m)에 각각 주입하는 방식에 의한 키 주입이 일반적으로 이용되고 있다.

[0007] 도 1에 도시된 시스템에 의해 SE들(30-1 내지 30-m)에 주입된 키를 교체하는 데에는, 많은 제약과 불편이 따른다. 구체적으로, USIM이나 Secure MC에 주입된 키 교체를 위해서는 USIM이나 Secure MC를 키 주입 장치(20)에 직접 장착하여야 하고, Embedded SE에 주입된 키 교체를 위해서는 Embedded SE가 탑재된 모바일 단말기를 키 주입 장치(20)에 직접 연결하여야 하는 제약으로 인해, 어느 경우이든 SE 사용자가 키 주입 장치(20)가 있는 통신/금융 기관 등을 방문하여야 하는 불편이 따른다.

[0008] 이와 같은 제약과 불편으로 인해, SE에 주입된 키를 교체하여야 할 필요가 발생하면, 새로운 키를 주입한 SE를 사용자에게 새로 발송하고 있는 실정이다. 그나마 이와 같은 처리도 USIM이나 Secure MC에만 해당될 뿐이며, Embedded SE의 경우는 적용이 불가능한 문제가 있다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은, 사용자의 요청에 의해 온-라인으로 SE에 주입된 키를 교체할 수 있는 방법 및 시스템을 제공함에 있다.

과제의 해결 수단

[0010] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른, SE 키 교체 방법은, 모바일 단말기에 장착된 SE(Secure Element)에 주입된 키의 교체를 요청받는 단계; 교체 요청된 키를 발급한 서비스 제공자에 새로운 키를 요청하여 수신하는 단계; 및 상기 수신단계를 통해 수신된 새로운 키를 상기 모바일 단말기에 전달하는 단계;를 포함한다.

[0011] 그리고, 상기 전달단계는, 상기 모바일 단말기에 키 교체 안내를 전송하는 단계; 및 상기 키 교체 안내에 대한 응답으로 상기 모바일 단말기로부터 키 교체 요청이 수신되면, 상기 새로운 키를 상기 모바일 단말기에 전달하는 단계;를 포함할 수 있다.

[0012] 또한, 상기 전달단계는, 상기 수신단계를 통해 수신된 새로운 키를 상기 모바일 단말기에 푸시 방식으로 전달할 수 있다.

[0013] 그리고, 상기 모바일 단말기는, 새로운 키가 수신되면, 상기 SE에 주입되어 있는 키를 즉시 폐기하고 새로운 키를 주입할 수 있다.

[0014] 또한, 상기 모바일 단말기는, 푸시 알림을 확인한 사용자가 키 교체를 명령한 경우, 상기 SE에 이미 발급된 키를 즉시 폐기하고 새로운 키를 주입할 수 있다.

[0015] 그리고, 본 실시예에 따른 SE 키 교체 방법은, 상기 요청단계에서의 교체 요청 내역을 저장하는 단계;를 더 포함할 수 있다.

[0016] 또한, 상기 요청단계는, 특정 서비스에 이용되는 키의 교체를 요청받고, 상기 수신단계는, 상기 특정 서비스를 제공하는 서비스 제공자에 새로운 키를 요청하여 수신할 수 있다.

[0017] 그리고, 본 실시예에 따른 SE 키 교체 방법은, 상기 모바일 단말기가 온-라인으로 키 교체 서비스를 제공받을 수 있도록 등록된 모바일 단말기인지 확인하는 단계;를 더 포함하고, 상기 수신단계는, 상기 모바일 단말기가 등록된 것으로 확인되면 수행될 수 있다.

[0018] 또한, 상기 요청단계는, 상기 모바일 단말기와 분리된 다른 단말기로부터 상기 키의 교체를 요청받을 수 있다.

[0019] 그리고, 상기 요청단계, 상기 수신단계 및 상기 전달단계는, 상기 SE에 주입된 키가 노출된 경우에 수행될 수 있다.

[0020] 또한, 상기 요청단계, 상기 수신단계 및 상기 전달단계는, 상기 모바일 단말기, 상기 SE 및 상기 서비스 제공자 중 적어도 하나에 대한 테스트 중에 수행될 수 있다.

[0021] 그리고, 본 실시예에 따른 SE 키 교체 방법은, 상기 모바일 단말기에 장착된 SE에 추가 주입할 키를 요청받는 단계; 추가 주입된 키를 발급하는 서비스 제공자에 키를 요청하여 수신하는 단계; 및 상기 수신단계를 통해 수신된 키를 상기 모바일 단말기에 전달하는 단계;를 더 포함할 수 있다.

[0022] 한편, 본 발명의 다른 실시예에 따른, 키 관리 서버는, 모바일 단말기에 장착된 SE(Secure Element)에 주입된 키의 교체를 요청받는 통신 인터페이스; 상기 통신 인터페이스를 통해, 교체 요청된 키를 발급한 서비스 제공자에 새로운 키를 요청하여 수신하여 상기 모바일 단말기에 전달하는 제어부;를 포함한다.

[0023] 한편, 본 발명의 다른 실시예에 따른, SE 키 교체 방법은, 장착된 SE(Secure Element)에 주입된 키의 교체를 요청하는 단계; 상기 요청에 대한 응답으로 새로운 키를 수신하는 단계; 상기 SE에 주입되어 있는 키를 폐기하는 단계; 및 수신된 새로운 키를 상기 SE에 주입하는 단계;를 포함한다.

발명의 효과

[0024] 이상 설명한 바와 같이, 본 발명에 따르면, 사용자의 요청에 의해 SE에 주입된 키를 온-라인으로 교체할 수 있게 되어, 키 노출 등의 이유로 SE 주입된 키 교체가 필요한 경우 사용자가 키 주입 장치가 마련된 기관에 직접 방문하지 않고서도 SE 키 교체가 가능해져, 사용자의 불편을 해소할 수 있게 된다.

[0025] 뿐만 아니라, SE를 계속하여 사용 가능하므로, SE 발급 남발에 의한 자원 낭비를 막을 수 있다.

[0026] 또한, 본 발명에 따르면, 사용자의 요청으로 온-라인을 통해 SE에 새로운 키를 추가로 주입할 수 있게 되어, 새로운 서비스 추가시에 필요한 키 주입이 서비스 제공 기관 방문 없이도 가능하여, 사용자의 편의를 더욱 도모할 수 있게 된다.

도면의 간단한 설명

[0027] 도 1은 SE에 키를 주입하는 기존의 시스템을 도시한 도면,

도 2는 본 발명이 적용가능한 SE 키 교체 시스템을 도시한 도면,

도 3은 본 발명의 일 실시예에 따른 SE 키 교체방법의 설명에 제공되는 도면,

도 4는 본 발명의 다른 실시예에 따른 SE 키 교체방법의 설명에 제공되는 도면, 그리고,

도 5는, 도 1에 도시된 키 관리 서버의 블럭도이다.

발명을 실시하기 위한 구체적인 내용

[0028] 이하에서는 도면을 참조하여 본 발명을 보다 상세하게 설명한다.

[0029] 도 2는 본 발명이 적용가능한 SE(Secure Element) 키 교체 시스템을 도시한 도면이다. SE 키 교체 시스템은, 사용자의 요청이 있는 경우 사용자의 스마트폰에 장착된 SE에 주입된 키를 새로운 키로 교체하는 시스템이다.

[0030] 이와 같은 기능을 수행하는 SE 키 교체 시스템은, 도 2에 도시된 바와 같이, 스마트폰(110), PC(Personal Computer)(120), 푸시 서버(130), 키 관리 서버(140), 키 관리 DB(DataBase)(150) 및 SP(Service Provider)들(160-1 내지 160-n)이 상호 통신가능하도록 연결되어 구축된다.

[0031] 스마트폰(110)은 모바일 단말기의 일종으로 SE(112)가 장착된다. 스마트폰(110)에 장착되는 SE(112)의 형태에 대한 제한은 없다. 즉, USIM, Embedded SE 및 Secure MC는 물론 이와 다른 형태의 SE도 스마트폰(110)에 장착되어 사용가능하다.

[0032] 프로세서(111)에 의해 구동되는 OTA 프록시(On The Air Proxy)(111a)에 의해 스마트폰(110)은 SE(112)에 인터페이스 가능하다.

[0033] PC(120)는 스마트폰(110)의 사용자가 SE(112)에 주입된 키를 교체하여 줄 것을 키 관리 서버(140)에 요청하는데 이용되는 수단이다.

[0034] 키 관리 서버(140)는 스마트폰(110)의 SE(112)에 주입된 키를 교체하는데 필요한 절차를 수행하는 서버이다.

[0035] 키 관리 DB(150)는 키 교체와 관련한 사항들이 저장되어 있는 DB이고, 푸시 서버(130)는 스마트폰(110)에 키 교체를 위한 푸시 메세지를 전송하는 서버이다.

[0036] SP들(160-1 내지 160-n)은 스마트폰(110)에 통신, 금융, 인증, 결제 등의 다양한 서비스를 제공함은 물론, 서비스에 필요한 키를 생성하는 HSM들(165-1 내지 165-n)을 구비하고 있다.

[0037] 이하에서는, 도 2에 도시된 SE 키 교체 시스템에 의해 사용자의 스마트 폰(110)에 장착된 SE(112)에 주입되어 있는 키를 새로운 키로 교체하는 과정에 대해 상세히 설명한다.

[0038] 도 3은 본 발명의 일 실시예에 따른 SE 키 교체방법의 설명에 제공되는 도면이다.

[0039] 도 3에 도시된 바와 같이, PC(120)는 스마트폰(110)의 SE(112)에 주입된 키 교체를 키 관리 서버(140)에 요청한다(S310). S310단계에서의 키 교체 요청은 PC(120)를 통해 사용자가 입력한다. 한편, 스마트폰(110)은 S/N이나 전화번호 등으로 특정하고, SE(112)는 S/N으로 특정하는 것이 가능하다.

[0040] 한편, 스마트폰(110)의 SE(112)에는 다수의 키들이 주입되어 있을 수 있다. 이 경우, 스마트폰(110)의 사용자는 교체가 필요한 '키'를 직접 지정할 수 있음은 물론 교체가 필요한 키를 이용하는 '서비스'를 지정할 수도 있다. 서비스가 지정된 경우에는, 그 서비스를 위해 이용되는 키가 지정된 것으로 취급하고 다음 절차들을 수행할 수 있다.

[0041] S310단계를 통해 키 교체 요청을 수신한 키 관리 서버(140)는 사용자의 스마트폰(110)이 키 교체 서비스에 사전 등록되어 있는지 여부를 확인한다(S320). S320단계에서 확인되는 키 교체 서비스란 온-라인을 통한 키 교체를 제공하는 서비스를 말한다.

[0042] 만약, 스마트폰(110)이 키 교체 서비스에 사전 등록되어 있지 않은 경우라면, S310단계에서의 요청은 폐기되고, S320단계 이후의 절차는 수행되지 않는다.

[0043] 스마트폰(110)이 키 교체 서비스에 사전 등록되어 있다면, 키 관리 서버(140)는 S310단계에서 수신한 키 교체 요청 내역을 키 관리 DB(150)에 저장한다(S330).

[0044] S330단계에서는 키 교체 요청 내역을 스마트폰(110) 또는 SE(112) 별로 구분하여 저장하여, 추후 키 교체 요청 내역을 스마트폰(110) 또는 SE(112) 별로 제공가능하도록 할 수 있다.

[0045] 이후, 키 관리 서버(140)는 SP(160)에 교체할 새로운 키 발급을 요청한다(S340). S340단계에서의 키 발급 요청은, S310단계에서 교체 요청된 키를 발급하였던 SP에게 행한다.

[0046] 즉, 교체 요청된 키를 발급하였던 SP가 SP-1(160-1)인 경우 키 관리 서버(140)는 SP-1(160-1)에 새로운 키 발급을 요청하고, 교체 요청된 키를 발급하였던 SP가 SP-3(160-3)인 경우 키 관리 서버(140)는 SP-3(160-3)에 새로운 키 발급을 요청한다.

[0047] S340단계를 통해 키 발급을 요청받은 SP(160)는 HSM(165)을 통해 새로운 키를 생성하여 키 관리 서버(140)로 발급한다(S350).

[0048] S350단계를 통해 SP(160)로부터 새로운 키를 발급받은 키 관리 서버(140)는 스마트폰(110)으로 키 교체 안내 메일을 발송한다(S360). 키 교체 안내 메일은, 교체할 새로운 키가 발급 완료되었으니 키 교체를 요청할 것을 유도하기 위한 내용이 수록되어 있는 메일이다.

[0049] S360단계에서의 키 교체 안내 메일은, 메일 형식이 아닌, SMS(Short Message Service)나 MMS(Multimedia Messaging Service) 메세지로 발송될 수도 있다.

[0050] S360단계를 통해 수신된 키 교체 안내 메일이 스마트폰(110)의 사용자에 의해 확인되어(S370), 스마트폰(110)이 키 관리 서버(140)에 키 교체를 요청하면(S380), 키 관리 서버(140)는 S350단계를 통해 SP(160)로부터 발급받은 교체할 새로운 키를 스마트폰(110)으로 전송한다(S390).

[0051] 그러면, 스마트폰(110)은 SE(112)에 이미 주입되어 있는 기존 키를 폐기한 후, S390단계를 통해 수신된 새로운 키를 주입하며(S395), 이에 의해 스마트폰(110)의 SE(112)에 주입된 키의 교체가 완료된다.

[0052] 이하에서는, 도 2에 도시된 SE 키 교체 시스템에 의해 사용자의 스마트 폰(110)에 장착된 SE(112)에 주입되어 있는 키를 새로운 키로 교체하는 또 다른 방법에 대해, 도 4를 참조하여 상세히 설명한다.

[0053] 도 4는 본 발명의 다른 실시예에 따른 SE 키 교체방법의 설명에 제공되는 도면이다. 도 4에 도시된 S410 단계 내지 S450단계에 대한 상세한 설명은 도 3에 도시된 S310 단계 내지 S350단계에 대한 상세한 설명과 동일하므로 생략하고, 이하에서는 S450단계 이후에 대해서만 설명한다.

[0054] S450단계를 통해 SP(160)로부터 새로운 키를 발급받은 키 관리 서버(140)는 발급받은 새로운 키를 푸시 서버(130)로 전달한다(S460). 그러면, 푸시 서버(130)는 S460단계를 통해 전달받은 새로운 키를 푸시 방식으로 스마트폰(110)에 전송한다(S470).

[0055] 이후, 스마트폰(110)은 SE(112)에 이미 주입되어 있는 기존 키를 폐기한 후, S470단계를 통해 푸시된 새로운 키

를 주입하며(S480), 이에 의해 스마트폰(110)의 SE(112)에 주입된 키의 교체가 완료된다.

[0056] S480단계는, 1) 사용자의 확인 절차 없이 푸시 서버(130)로부터 새로운 키를 푸시 받은 즉시 수행될 수 있음은 물론, 2) 푸시 알림을 통해 사용자의 확인을 거친 후에(즉, 푸시 알림을 확인한 사용자가 키 교체를 명령한 후에), 수행되도록 구현하는 것도 가능하다.

[0057] 지금까지, SE 키 교체 시스템에 대한 바람직한 실시예들에 대해 바람직한 실시예들을 들어 상세히 설명하였다.

[0058] 위 실시예에 따른 SE 키 교체는 스마트폰(110)의 SE(112)에 주입된 키가 노출된 경우, 스마트폰(110), SE(112), 서비스 제공자(160) 중 적어도 하나를 개발하는 중에 테스트하는 경우 등에 수행되는 경우 유용하다.

[0059] 또한, 위 실시예에서 스마트폰(110)과 분리된 PC(120)를 통해 키 교체 요청이 이루어지는 것을 상정하였는데, 이는 보안을 더욱 강화하기 위한 것으로, 변형이 가능하다. 따라서, 키 교체 요청을 PC(120)가 아닌 스마트폰(110)에서 수행되는 것으로 변경하는 것이 가능하다.

[0060] 그리고, 스마트폰(110)은 모바일 단말기의 하나를 예시한 것으로, 본 발명은 스마트폰(110) 이외의 다른 모바일 단말기에 장착된 SE의 키를 교체하는 경우로 확장될 수 있음은 물론이다.

[0061] 한편, 위 실시예에서는, 스마트폰(110)의 SE(112)에 주입된 키를 교체하는 경우를 상정하였으나, SE(112)에 새로운 키를 주입하는 기능을 추가하는 것이 가능하다. 즉, 스마트폰(110)으로부터 이전에 주입되지 않은 새로운 키가 발급 요청된 경우, 키 관리 서버(140)가 요청된 키를 발급하는 SP에 키를 요청/수신하여 스마트폰(110)으로 전달하여 주는 것이 가능하다.

[0062] 도 5는, 도 1에 도시된 키 관리 서버(140)의 블럭도이다. 도 5에 도시된 바와 같이, 키 관리 서버(140)는, 통신 인터페이스(141), 제어부(142) 및 저장부(143)를 구비한다.

[0063] 통신 인터페이스(141)는 스마트폰(110), PC(120), 푸시 서버(130), 키 관리 DB(150) 및 SP들(160-1 내지 160-n)에 액세스하기 위한 통신 수단이다.

[0064] 저장부(133)는 키 관리 서버(140)가 동작하는데 필요한 프로그램과 데이터를 저장하는 수단이다. 도 1에 도시된 키 관리 DB(150)를 저장부(133)에 편입시키고, 키 관리 DB(150)를 생략하는 것이 가능하다.

[0065] 제어부(142)는 전술한 도 3과 도 4에 도시된 프로세스들 중, 키 관리 서버(140)에 의해 수행될 프로세스들을 수행한다.

[0066] 한편, 도 1에 도시된 푸시 서버(130)를 키 관리 서버(140))에 편입시키고, 푸시 서버(130)를 생략하는 것도 구현상 가능하다.

[0067] 본 실시예에 따른 장치와 방법의 기능을 수행하게 하는 컴퓨터 프로그램을 수록한 컴퓨터로 읽을 수 있는 기록매체에도 본 발명의 기술적 사상이 적용될 수 있음은 물론이다. 또한, 본 발명의 다양한 실시예에 따른 기술적 사상은 컴퓨터로 읽을 수 있는 기록매체에 기록된 컴퓨터로 읽을 수 있는 코드 형태로 구현될 수도 있다. 컴퓨터로 읽을 수 있는 기록매체는 컴퓨터에 의해 읽을 수 있고 데이터를 저장할 수 있는 어떤 데이터 저장 장치이더라도 가능하다. 예를 들어, 컴퓨터로 읽을 수 있는 기록매체는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광디스크, 하드 디스크 드라이브, 등이 될 수 있음은 물론이다. 또한, 컴퓨터로 읽을 수 있는 기록매체에 저장된 컴퓨터로 읽을 수 있는 코드 또는 프로그램은 컴퓨터간에 연결된 네트워크를 통해 전송될 수도 있다.

[0068] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

부호의 설명

[0069] 110 : 스마트폰 111 : 프로세서

111a : OTA 프록시(On The Air Proxy)

112 : SE(Secure Element) 120 : PC(Personal Computer)

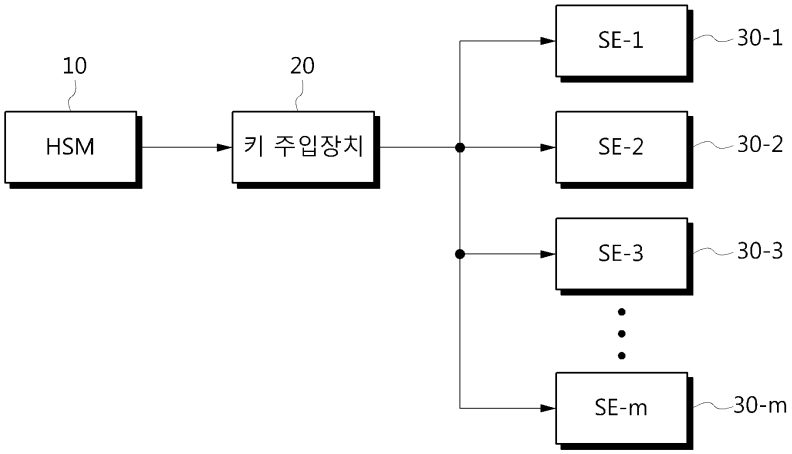
130 : 푸시 서버 140 : 키 관리 서버

150 : 키 관리 DB(DataBase)

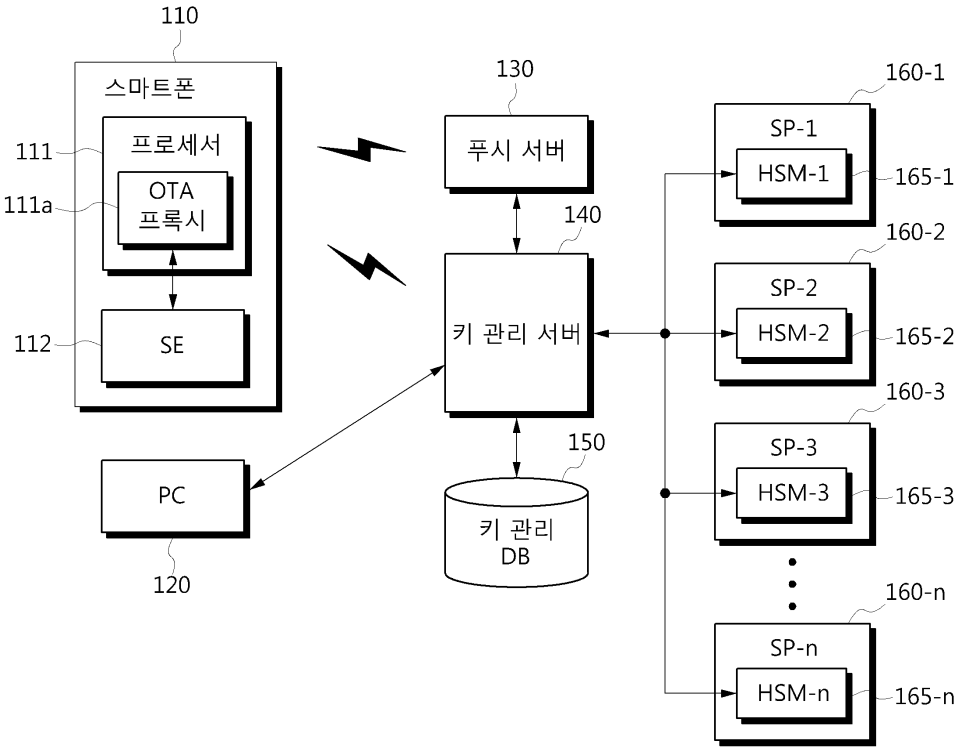
160, 160-1 내지 160-n : SP(Service Provider)

도면

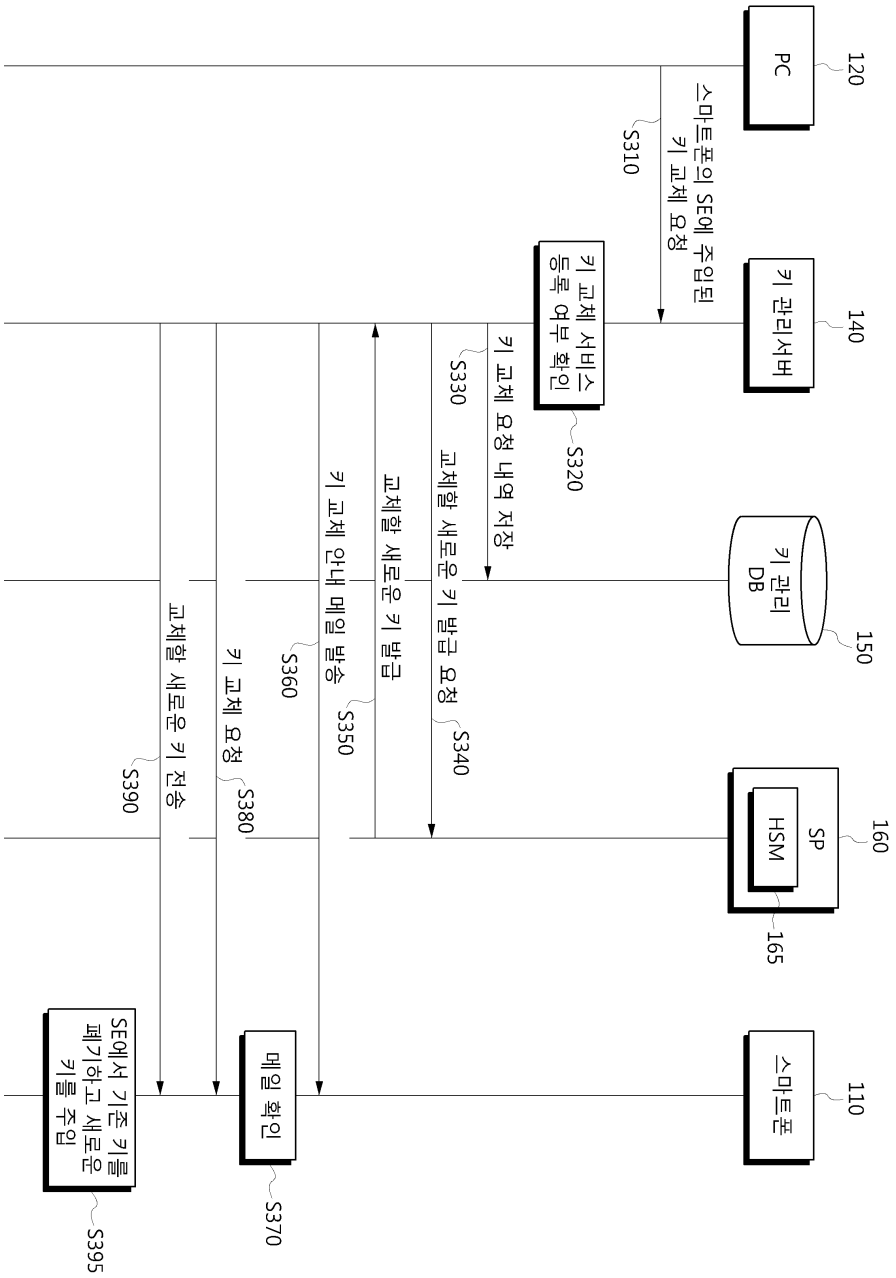
도면1



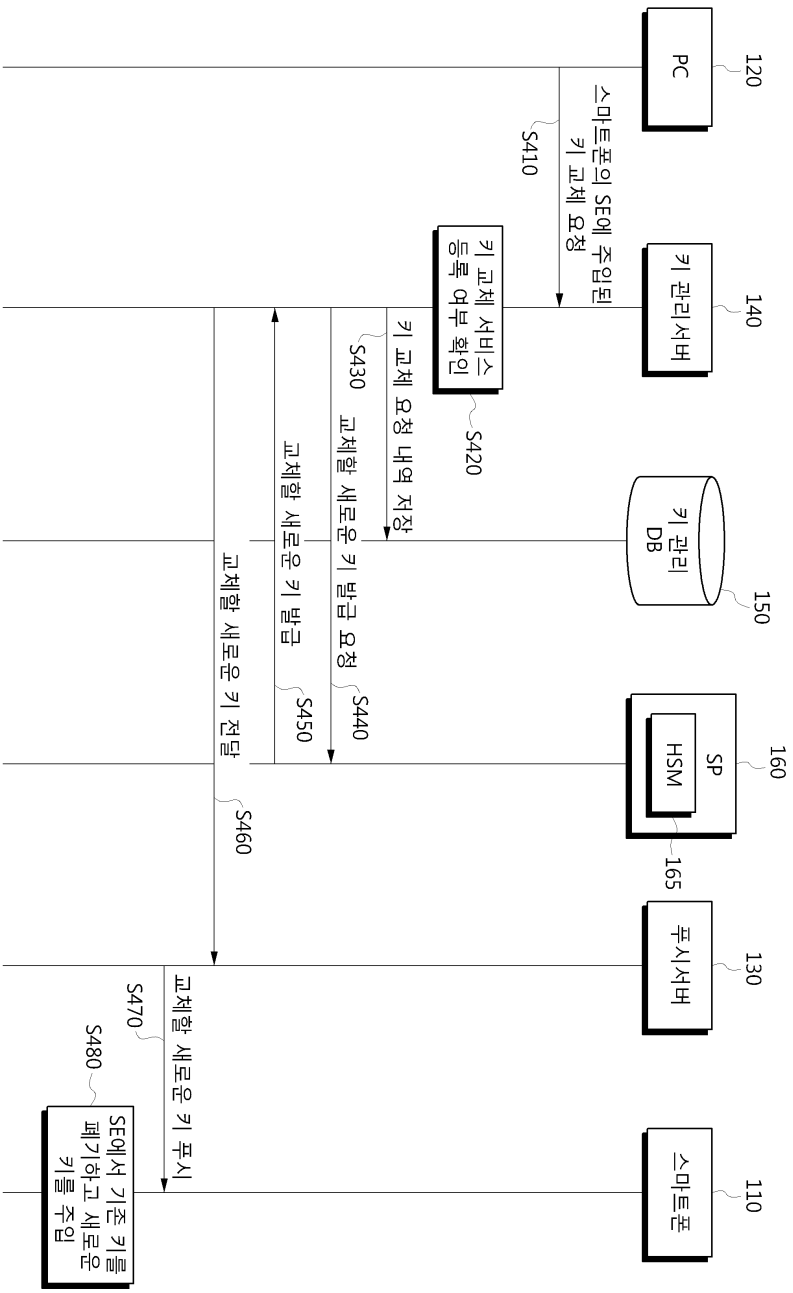
도면2



도면3


PC
120
스마트폰의 SE에 주입된 키 교체 요청
S310
키 관리서버
140
키 교체 서비스 등록 여부 확인
S320
키 교체 요청 내역 저장
S330
키 관리 DB
150
교체할 새로운 키 발급 요청
S340
SP
HSM
160
165
교체할 새로운 키 발급
키 교체 안내 메일 발송
S350
S360
스마트폰
110
키 교체 요청
S380
메일 확인
S370
교체할 새로운 키 전송
S390
SE에서 기존 키를 폐기하고 새로운 키를 주입
S395

도면4


PC
120
스마트폰의 SE에 주입된 키 교체 요청
S410
키 관리서버
140
키 교체 서비스 등록 여부 확인
S420
키 교체 요청 내역 저장
S430
키 관리 DB
150
교체할 새로운 키 발급 요청
S440
교체할 새로운 키 발급
S450
SP
HSM
160
165
교체할 새로운 키 전달
S460
푸시서버
130
교체할 새로운 키 푸시
S470
SE에서 기존 키를 폐기하고 새로운 키를 주입
S480
스마트폰
110

도면5