(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년09월02일
(11) 등록번호 10-1436872
(24) 등록일자 2014년08월27일

(51) 국제특허분류(Int. Cl.)
H04W 8/30 (2009.01) *H04W 12/08* (2009.01)
(21) 출원번호 10-2012-0137052
(22) 출원일자 2012년11월29일
심사청구일자 2012년11월29일
(65) 공개번호 10-2014-0069596
(43) 공개일자 2014년06월10일
(56) 선행기술조사문헌
KR1020050092420 A*
KR1020100011456 A*
KR1020110116095 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
에스케이씨앤씨 주식회사
경기도 성남시 분당구 성남대로343번길 9 (정자동, 에스케이유타워)
(72) 발명자
전미숙
서울 중랑구 용마산로 566, (망우동)
강경구
경기 용인시 수지구 정든로 22, 905동 1501호 (죽전동, 도담마을죽전파크빌)
(74) 대리인
특허법인 에이치엠피

전체 청구항 수 : 총 17 항 심사관 : 이종익

(54) 발명의 명칭 **보안 요소 정보 관리 방법 및 시스템**

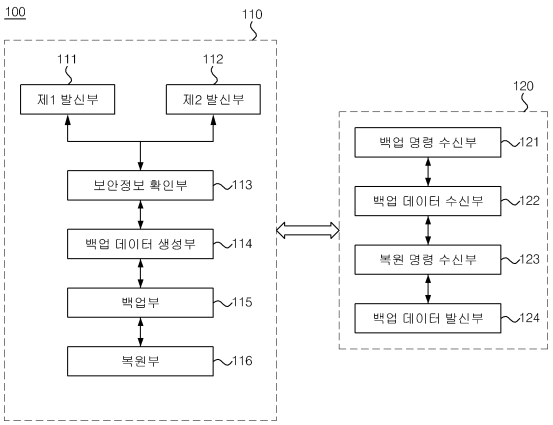
(57) 요 약

본 발명은 보안 요소 정보 관리 방법 및 시스템에 관한 것으로, 보다 상세하게는 단말기 내 보안 요소(SE; Secure Element)의 보안정보를 보안 서버(TSM; Trusted Service Manager)로 안전하게 백업한 후, 상기 단말기 또는 타 단말기 내 보안 요소로 백업한 보안정보를 안전하게 복원하는 방법 및 시스템에 관한 것이다.

이러한 목적을 달성하기 위하여 본 발명의 일 실시예에 따른 보안 요소 정보 관리 방법은 보안정보를 확인하는 단계, 백업 데이터를 생성하는 단계, 백업 데이터를 보안 서버로 전송하는 단계 및 백업 데이터를 상기 보안 요소 또는 타 보안 요소에 복원하는 단계를 포함한다.

상기 보안정보를 확인하는 단계는 보안 요소의 보안정보에 대한 백업 명령에 응답하여 상기 보안 요소에 저장된 보안정보를 확인한다. 상기 백업 데이터를 생성하는 단계는 상기 확인된 보안정보 중 적어도 일부를 이용하여 백업 데이터를 생성한다. 상기 백업 데이터를 보안 서버로 전송하는 단계는 보안 서버와 보안 요소 사이의 보안 채널을 설정하고, 상기 설정된 채널을 통해 상기 백업 데이터를 상기 보안 요소로부터 상기 보안 서버로 전송하여 저장하도록 한다. 상기 백업 데이터를 상기 보안 요소 또는 타 보안 요소에 복원하는 단계는 상기 보안정보에 대한 복원 명령에 응답하여 상기 백업 데이터를 복원한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

보안 요소(SE; Secure Element)의 보안정보에 대한 백업(Backup) 명령에 응답하여 상기 보안 요소에 저장된 보안정보를 확인하는 단계;

상기 확인된 보안정보에 포함되는 결제수단에 대하여 사용 정지 설정을 요청하는 명령을 발신하는 단계;

상기 확인된 보안정보 중 적어도 일부를 이용하여 백업 데이터를 생성하는 단계;

보안 서버(TSM; Trusted Service Manager)와 보안 요소 사이의 보안 채널(secure channel)을 설정하고, 상기 설정된 채널을 통해 상기 백업 데이터를 상기 보안 요소로부터 상기 보안 서버로 전송하여 저장하도록 하는 단계;

상기 보안정보에 대한 복원(Restore) 명령에 응답하여 상기 보안 서버의 백업 데이터를 상기 보안 요소 또는 타 보안 요소에 복원하는 단계; 및

상기 복원된 보안정보에 포함되는 결제수단에 대하여 사용 가능 설정을 요청하는 명령을 발신하는 단계;

를 포함하는 보안 요소 정보 관리 방법.

청구항 2

제1항에 있어서,

상기 백업 데이터를 생성하는 단계는

상기 확인된 보안정보를 카테고리로 분류하고,

상기 분류된 카테고리 별 백업방법에 따라 상기 백업 데이터를 생성하는 것

을 특징으로 하는 보안 요소 정보 관리 방법.

청구항 3

제2항에 있어서

상기 백업 데이터를 생성하는 단계는

상기 확인된 보안정보 중 카드 애플릿 카테고리로 분류된 정보들의 카드 애플릿 정보를 포함하는 카드 애플릿 설치 목록을 백업 데이터로 생성하고,

상기 복원하는 단계는

상기 백업 데이터에 포함된 상기 카드 애플릿 설치 목록을 기초로 상기 보안 요소 또는 상기 타 보안 요소에 상기 카드 애플릿을 설치할 수 있도록 제어하는 것

을 특징으로 하는 보안 요소 정보 관리 방법.

청구항 4

제3항에 있어서,

상기 복원하는 단계는

상기 카드 애플릿 설치 목록에 포함된 카드 정보를 디스플레이 화면에 표시하고, 사용자의 선택 입력에 응답하여 선택된 카드 애플릿을 상기 보안 요소 또는 상기 타 보안 요소에 설치하는 것

을 특징으로 하는 보안 요소 정보 관리 방법.

청구항 5

제2항에 있어서,

상기 백업 데이터를 생성하는 단계는

상기 확인된 보안정보 중 수치 데이터 카테고리로 분류된 정보들의 수치 데이터를 백업 데이터로 생성하고,

상기 복원하는 단계는

상기 백업 데이터에 포함된 상기 수치 데이터를 상기 보안 요소 또는 상기 타 보안 요소에 저장하는 것

을 특징으로 하는 보안 요소 정보 관리 방법.

청구항 6

제1항에 있어서,

상기 백업 데이터를 생성하는 단계는

상기 보안정보 중 적어도 일부를 이용하여 생성한 데이터를 사용자 단말기의 고유 정보를 이용하여 암호화하여 백업 데이터를 생성하는 것

을 특징으로 하는 보안 요소 정보 관리 방법.

청구항 7

삭제

청구항 8

제1항에 있어서,

상기 보안 요소는 내장형 보안 요소(embedded SE)인 것을 특징으로 하는 보안 요소 정보 관리 방법.

청구항 9

사용자 단말기의 보안 요소(SE; Secure Element)에 저장된 보안정보에 대한 백업 명령을 수신하는 단계;

상기 보안정보에 포함되는 결제수단에 대하여 사용 정지 설정을 요청하는 명령을 수신하고, 상기 보안정보에 포함되는 결제수단을 사용 정지시키는 단계;

상기 사용자 단말기의 보안 요소와 보안 채널(secure channel)을 설정하고, 상기 설정된 채널을 통해 상기 보안정보 중 적어도 일부의 백업 데이터를 수신하는 단계;

상기 보안정보에 대한 복원(Restore) 명령을 수신하는 단계;

상기 복원 명령에 응답하여 상기 백업 데이터를 상기 사용자 단말기 또는 다른 사용자 단말기의 보안 요소로 보내는 단계; 및

상기 보안정보에 포함되는 결제수단에 대하여 사용 가능 설정을 요청하는 명령을 수신하고 상기 사용 정지된 상기 보안 정보에 포함되는 결제수단의 사용 정지를 해제시키는 단계;

를 포함하는 보안 요소 정보 관리 방법.

청구항 10

보안 요소(SE; Secure Element)의 보안정보에 대한 백업(Backup) 명령에 응답하여 상기 보안 요소에 저장된 보안정보를 확인하는 단계;

상기 확인된 보안정보에 포함되는 결제수단에 대하여 사용 정지 설정을 요청하는 명령을 발신하는 단계;

상기 확인된 보안정보 중 적어도 일부를 이용하여 백업 데이터를 생성하는 단계;

보안 서버(TSM; Trusted Service Manager)와 보안 요소 사이의 보안 채널(secure channel)을 설정하고, 상기 설정된 채널을 통해 상기 백업 데이터를 상기 보안 요소로부터 상기 보안 서버로 전송하여 저장하도록 하는 단계;

상기 보안정보에 대한 복원(Restore) 명령에 응답하여 상기 보안 서버의 백업 데이터를 상기 보안 요소 또는 타 보안 요소에 복원하는 단계; 및

상기 복원된 보안정보에 포함되는 결제수단에 대하여 사용 가능 설정을 요청하는 명령을 발신하는 단계;

를 포함하는 방법을 실행하기 위한 프로그램이 기록되어 있는 것을 특징으로 하는 컴퓨터에서 판독 가능한 기록매체.

청구항 11

보안 요소(SE; Secure Element)의 보안정보에 대한 백업(Backup) 명령에 응답하여 상기 보안 요소에 저장된 보안정보를 확인하는 보안정보 확인부;

상기 확인된 보안정보에 포함되는 결제수단에 대하여 사용 정지 설정을 요청하는 명령을 발신하는 제1 발신부;

상기 확인된 보안정보 중 적어도 일부를 이용하여 백업 데이터를 생성하는 백업 데이터 생성부;

보안 서버(TSM; Trusted Service Manager)와 보안 요소 사이의 보안 채널(secure channel)을 설정하고, 상기 설정된 채널을 통해 상기 백업 데이터를 상기 보안 요소로부터 상기 보안 서버로 전송하여 저장하도록 하는 백업부;

상기 보안정보에 대한 복원(Restore) 명령에 응답하여 상기 보안 서버의 백업 데이터를 상기 보안 요소 또는 타 보안 요소에 복원하는 복원부; 및

상기 복원된 보안정보에 포함되는 결제수단에 대하여 사용 가능 설정을 요청하는 명령을 발신하는 제2 발신부;

를 포함하는 보안 요소 정보 관리 시스템.

청구항 12

제11항에 있어서,

상기 백업 데이터 생성부는

상기 확인된 보안정보를 카테고리로 분류하고,

상기 분류된 카테고리 별 백업방법에 따라 상기 백업 데이터를 생성하는 것

을 특징으로 하는 보안 요소 정보 관리 시스템.

청구항 13

제12항에 있어서

상기 백업 데이터 생성부는

상기 확인된 보안정보 중 카드 애플릿 카테고리로 분류된 정보들의 카드 애플릿 정보를 포함하는 카드 애플릿 설치 목록을 백업 데이터로 생성하고,

상기 복원부는

상기 백업 데이터에 포함된 상기 카드 애플릿 설치 목록을 기초로 상기 보안 요소 또는 상기 타 보안 요소에 상기 카드 애플릿을 설치할 수 있도록 제어하는 것

을 특징으로 하는 보안 요소 정보 관리 시스템.

청구항 14

제13항에 있어서,

상기 복원부는

상기 카드 애플릿 설치 목록에 포함된 카드 정보를 디스플레이 화면에 표시하고, 사용자의 선택 입력에 응답하여 선택된 카드 애플릿을 상기 보안 요소 또는 상기 타 보안 요소에 설치하는 것

을 특징으로 하는 보안 요소 정보 관리 시스템.

청구항 15

제12항에 있어서,

상기 백업 데이터 생성부는

상기 확인된 보안정보 중 수치 데이터 카테고리로 분류된 정보들의 수치 데이터를 백업 데이터로 생성하고,

상기 복원부는

상기 백업 데이터에 포함된 상기 수치 데이터를 상기 보안 요소 또는 상기 타 보안 요소에 저장하는 것

을 특징으로 하는 보안 요소 정보 관리 시스템.

청구항 16

제11항에 있어서,

상기 백업 데이터 생성부는

상기 보안정보 중 적어도 일부를 이용하여 생성한 데이터를 사용자 단말기의 고유 정보를 이용하여 암호화하여 백업 데이터를 생성하는 것

을 특징으로 하는 보안 요소 정보 관리 시스템.

청구항 17

삭제

청구항 18

제11항에 있어서,

상기 보안 요소는 내장형 보안 요소(embedded SE)인 것을 특징으로 하는 보안 요소 정보 관리 시스템.

청구항 19

사용자 단말기의 보안 요소(SE; Secure Element)에 저장된 보안정보에 대한 백업 명령을 수신하는 백업 명령 수신부;

상기 사용자 단말기의 보안 요소와 보안 채널(secure channel)을 설정하고, 상기 설정된 채널을 통해 상기 보안정보 중 적어도 일부의 백업 데이터를 수신하는 백업 데이터 수신부;

상기 보안정보에 대한 복원(Restore) 명령을 수신하는 복원 명령 수신부; 및

상기 복원 명령에 응답하여 상기 백업 데이터를 상기 사용자 단말기 또는 다른 사용자 단말기의 보안 요소로 보내는 백업 데이터 발신부;

를 포함하고,

상기 보안정보에 포함되는 결제수단에 대하여 사용 정지 설정을 요청하는 명령이 수신되면 상기 보안정보에 포함되는 결제수단을 사용 정지시키고,

상기 보안정보에 포함되는 결제수단에 대하여 사용 가능 설정을 요청하는 명령이 수신되면 상기 사용 정지된 상기 보안 정보에 포함되는 결제수단의 사용 정지를 해제시키는

보안 요소 정보 관리 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 보안 요소 정보 관리 방법 및 시스템에 관한 것으로, 보다 상세하게는 단말기 내 보안 요소(SE;

Secure Element) 보안정보를 보안 서버(TSM; Trusted Service Manager)로 안전하게 백업한 후, 상기 단말기 또는 타 단말기 내 보안 요소로 백업한 보안정보를 안전하게 복원하는 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 현대 스마트폰의 보급이 확산되면서 휴대폰 안에 있는 보안 요소(SE; Secure Element)에 신용카드 기능을 추가함으로써 통신과 금융이 융합된 모바일 결제 서비스가 많이 사용화되었다.

[0003] 이러한 모바일 결제 서비스는 통신 서비스와 금융 서비스가 융합되어 서비스가 제공되기 때문에, 통신 서비스 제공자와 금융 서비스 제공자 사이에 정보를 안전하게 전달하고 관리하는 중계자가 필요하며, 이 중계자 역할을 하는 것이 신뢰받는 서비스 관리자(TSM; Trusted Service Manager)이다.

[0004] 또한, 모바일 결제 서비스에 있어서 통신 서비스 제공자나 금융 서비스 제공자는 USIM(유심) 및 SD메모리(외장형 메모리)와 같은 보안 요소 내에 고객 정보를 저장하여 고객을 관리하는데, 상기 보안 요소 내에는 고객 정보가 포함되어 있으므로, 보안이 중요시 되어야 하고, 이러한 보안 요소를 관리하는 것이 신뢰받는 서비스 관리자(TSM)이다.

[0005] 즉, 신뢰받는 서비스 관리자는 개인의 결제와 직접적으로 관련된 금융 정보를 단말기 내 보안 요소(Secure Element)에 저장하여 관리하기 때문에 신뢰받는 서비스 관리자의 역할이 매우 중요 시 된다.

[0006] 한편 이러한 중요 고객 정보를 담고 있는 보안 요소에는 외장형 보안 요소인 USIM 및 SD메모리 또는 단말기 내 장착되는 보안 요소로 내장형 보안 요소(Embedded SE)가 있는데, 이러한 보안 요소 내 중요 정보를 백업하는 방법은 현재 어느 기술에서도 찾아볼 수 없으며, 종래에는 단말기 교체 또는 외장 메모리 교체 시 보안 요소 내 정보를 다 날려버리게 되어, 정보를 새로 설치해야 하는 불편함이 있었다.

[0007] 한편, 한국등록특허 제1107850호 "전송 방법, 전송 시스템, 신뢰받는 서비스 관리자, 컴퓨터 판독가능 매체 및 모바일 폰"에서는 신뢰받는 서비스 관리자를 통해 액세스 키에 의한 미승인 액세스에 대비하여 보호되는 다수의 메모리 섹터를 포함하는 메모리 디바이스가 장착된 모바일 폰에 서비스 제공자로부터의 서비스 또는 애플리케이션을 전송하는 시스템 및 방법을 제시한다.

[0008] 하지만, 위 선행기술은 신뢰받는 서비스 관리자가 보안 요소에 카드 정보 및 보안, 결제 관련 어플리케이션을 설치하기 위한 기능만 기재하고 있기 때문에, 종래의 보안 요소 교체 및 단말기 교체 시 보안 요소 내 정보의 리셋 또는 정보를 새로 설치해야 하는 문제는 해결하지 못하고 있다.

[0009] 이에 단말기의 교체 또는 보안 요소 교체 및 업데이트가 이루어져도 보안 요소 내 정보를 안전하게 백업하여 정보를 보관하는 기술이 요구된다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) 한국등록특허 제1107850호

발명의 내용

해결하려는 과제

[0011] 본 발명은 보안 요소 정보 관리 방법 및 시스템을 제공하는 것을 목적으로 한다.

[0012] 본 발명은 보안 요소의 보안정보를 보다 안전하게 백업 및 복원하는 것을 목적으로 한다.

[0013] 본 발명은 단말기 내 보안 요소 보안정보를 보안 서버로 안전하게 백업한 후, 상기 단말기 또는 타 단말기 내 보안 요소로 백업한 보안정보를 안전하게 복원하는 것을 목적으로 한다.

[0014] 본 발명은 복수개의 카드 정보를 통합 관리하는 것을 목적으로 한다.

과제의 해결 수단

[0015] 이러한 목적을 달성하기 위하여 본 발명의 일 실시예에 따른 보안 요소 정보 관리 방법은 보안정보를 확인하는

단계, 백업 데이터를 생성하는 단계, 백업 데이터를 보안 서버로 전송하는 단계 및 백업 데이터를 상기 보안 요소 또는 타 보안 요소에 복원하는 단계를 포함한다.

[0016] 상기 보안정보를 확인하는 단계는 보안 요소의 보안정보에 대한 백업 명령에 응답하여 상기 보안 요소에 저장된 보안정보를 확인한다. 상기 백업 데이터를 생성하는 단계는 상기 확인된 보안정보 중 적어도 일부를 이용하여 백업 데이터를 생성한다. 상기 백업 데이터를 보안 서버로 전송하는 단계는 보안 서버와 보안 요소 사이의 보안 채널을 설정하고, 상기 설정된 채널을 통해 상기 백업 데이터를 상기 보안 요소로부터 상기 보안 서버로 전송하여 저장하도록 한다. 상기 백업 데이터를 상기 보안 요소 또는 타 보안 요소에 복원하는 단계는 상기 보안정보에 대한 복원 명령에 응답하여 상기 백업 데이터를 복원한다.

[0017] 또한, 상기 백업 데이터를 생성하는 단계는 상기 확인된 보안정보를 카테고리로 분류하고, 카드 애플릿 카테고리로 분류된 정보에서는 카드 애플릿 설치 목록을 추출하여 이를 암호화하여 백업 데이터를 생성하고, 수치 데이터 카테고리로 분류된 정보에서는 수치 데이터를 추출하여 이를 암호화하여 백업 데이터를 생성한다.

[0018] 또한, 상기 백업 데이터를 생성하는 단계는 보안정보 중 적어도 일부를 이용하여 생성한 데이터를 사용자 단말기의 고유 정보를 이용하여 암호화하여 백업 데이터를 생성한다.

[0019] 또한, 사용자 단말기의 보안 요소에 저장된 보안정보에 대한 백업 명령을 수신하는 단계, 상기 사용자 단말기의 보안 요소와 보안 채널을 설정하고, 상기 설정된 채널을 통해 상기 보안정보 중 적어도 일부의 백업 데이터를 수신하는 단계, 상기 보안정보에 대한 복원 명령을 수신하는 단계 및 상기 복원 명령에 응답하여 상기 백업 데이터를 상기 사용자 단말기 또는 다른 사용자 단말기의 보안 요소로 보내는 단계를 더 포함한다.

[0020] 한편, 본 발명의 일 실시예에 따른 보안 요소 정보 관리 시스템은 보안정보 확인부, 백업 데이터 생성부, 백업부 및 복원부를 포함한다.

[0021] 상기 보안정보 확인부는 보안 요소의 보안정보에 대한 백업 명령에 응답하여 상기 보안 요소에 저장된 보안정보를 확인한다. 상기 백업 데이터 생성부는 상기 확인된 보안정보 중 적어도 일부를 이용하여 백업 데이터를 생성한다. 상기 백업부는 보안 서버와 보안 요소 사이의 보안 채널을 설정하고, 상기 설정된 채널을 통해 상기 백업 데이터를 상기 보안 요소로부터 상기 보안 서버로 전송하여 저장하도록 한다. 상기 복원부는 상기 보안정보에 대한 복원 명령에 응답하여 상기 백업 데이터를 복원한다.

[0022] 또한, 상기 백업 데이터 생성부는 상기 확인된 보안정보를 카테고리로 분류하고, 카드 애플릿 카테고리로 분류된 정보에서는 카드 애플릿 설치 목록을 추출하여 이를 암호화하여 백업 데이터를 생성하고, 수치 데이터 카테고리로 분류된 정보에서는 수치 데이터를 추출하여 이를 암호화하여 백업 데이터를 생성한다.

[0023] 또한, 상기 백업 데이터 생성부는 보안정보 중 적어도 일부를 이용하여 생성한 데이터를 사용자 단말기의 고유 정보를 이용하여 암호화하여 백업데이터를 생성한다.

[0024] 또한, 사용자 단말기의 보안 요소에 저장된 보안정보에 대한 백업 명령을 수신하는 백업 명령 수신부, 상기 사용자 단말기의 보안 요소와 보안 채널을 설정하고, 상기 설정된 채널을 통해 상기 보안정보 중 적어도 일부의 백업 데이터를 수신하는 백업 데이터 수신부, 상기 보안정보에 대한 복원 명령을 수신하는 복원 명령 수신부 및 상기 복원 명령에 응답하여 상기 백업 데이터를 상기 사용자 단말기 또는 다른 사용자 단말기의 보안 요소로 보내는 백업 데이터 발신부를 더 포함한다.

발명의 효과

[0025] 본 발명은 보안 요소 보안정보를 보다 안전하게 백업 및 복원할 수 있는 효과가 있다.

[0026] 본 발명은 단말기 내 보안 요소 보안정보를 보안 서버로 안전하게 백업한 후, 상기 단말기 또는 타 단말기 내 보안 요소로 백업한 보안정보를 안전하게 복원할 수 있는 효과가 있다.

[0027] 본 발명은 복수개의 카드 정보를 통합 관리 할 수 있는 효과가 있다.

[0028] 본 발명은 보안 요소와 보안 서버 사이에 보안 채널을 통해 백업 데이터를 전송함으로써, 백업 데이터의 분실 또는 손상에 대한 안전성을 보장할 수 있다..

[0029] 본 발명은 내장형 보안 요소(Embedded SE)의 보안정보뿐만 아니라 외장형 보안 요소(USIM, Micro-SD)의 보안정보도 안전하게 백업 및 복원 할 수 있는 효과가 있다.

도면의 간단한 설명

[0030] 도 1은 본 발명의 보안 요소 정보 관리 시스템의 개략적인 구성을 나타낸 도면이다.

도 2는 본 발명의 보안 요소 내 흐름을 나타낸 도면이다.

도 3은 본 발명의 일 실시예로 백업 데이터를 생성하는 과정을 나타낸 흐름도이다.

도 4는 본 발명의 일 실시예로 백업 데이터를 복원하는 과정을 나타낸 흐름도이다.

도 5는 본 발명의 보안 서버 내 흐름을 나타낸 도면이다.

도 6은 본 발명의 일 실시예에 따른 보안 요소의 타입 별 특성에 대해 나타낸 그림이다.

도 7은 본 발명의 일 실시예에 따라 보안 요소 내 보안정보를 확인한 경우를 나타낸 도면이다.

도 8은 본 발명의 일 실시예에 따라 디스플레이 화면에 표시되는 경우를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0031] 이하, 본 발명의 바람직한 실시예를 첨부된 도면들을 참조하여 상세히 설명한다. 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략하기로 한다. 또한 본 발명의 실시예들을 설명함에 있어 구체적인 수치는 실시예에 불과하다.

[0032] 본 발명은 모바일 결제 서비스에 이용되는 보안 요소 내에 저장된 정보를 관리하는 방법 및 시스템에 관한 기술을 제공한다.

[0033] 신뢰받는 서비스 관리자(TSM)는 개인의 결제와 직접적으로 관련된 금융 정보를 단말기 내 보안 요소(Secure Element)에 저장하여 관리한다.

[0034] 그러나 보안 요소 내에 저장된 정보는 종래에 따로 백업 할 방법이 없어서, 보안 요소의 업데이트 또는 단말기 교체 시 정보를 다시 설치해야 했다.

[0035] 본 발명에서는 이러한 문제점을 해결하기 위하여 단말기 내 보안 요소(SE; Secure Element) 보안정보를 이용하여 백업 데이터를 생성한 후 이를 보안 요소와 신뢰받는 서비스 관리자(TSM; Trusted Service Manager) 즉, 보안 서버 사이에 형성된 보안 채널(Secure Channel)을 통해 안전하게 백업한 후, 업데이트 또는 핸드폰 교체 시 상기 단말기 또는 타 단말기 내 보안 요소로 보안정보를 안전하게 복원하도록 하는 보안 요소 정보 관리 방법 및 시스템을 제시한다.

[0036] 신뢰받는 서비스 관리자(TSM; Trusted Service Manager)가 관리하는 보안 요소의 종류에는 크게 세가지로 USIM, 내장형 보안 요소(Embedded SE) 및 Micro-SD로 구분할 수 있으며, 이는 도 6을 참조하여 좀 더 자세하게 상기 보안 요소의 세가지 타입 별 장점 및 단점을 설명한다.

[0037] USIM은 가입자 인증 모듈로서 금융 서비스 제공 칩으로 확장 사용하는 형태이다. 보안 요소 제공자로는 이동통신 사업자가 가능하며, 기존 이동통신 사업자가 제공하는 기능을 사용할 수 있다는 장점이 있는 반면, 이동통신 사업자에 종속적인 모델이라는 단점이 있다.

[0038] 내장형 보안 요소(Embedded SE)는 단말기 자체에 보안 요소가 내장되어 들어가 있는 형태를 말하며, 보안 요소 제공자로는 핸드폰 제조사나 플랫폼 제공자(구글, 애플 등)가 가능하며, 이는 플랫폼 제공자가 사업의 중심이 될 수 있다는 장점이 있는 반면, 단말기와 일체형으로서, 휴대폰 교체 시 계속적인 사용이 어렵다는 단점이 있다.

[0039] Micro-SD(Secure Memory Card)는 USIM과 같이 단말기 내 탈부착이 가능한 저장 장치인 메모리 카드에 보안 요소가 들어가 있는 형태이다. 이는 보안 요소 제공자로 금융 서비스 제공자가 가능하며, 금융 서비스 제공자들이 쉽게 자신들의 보안 요소를 발급할 수 있는 장점이 있는 반면, 쉽게 탈부착이 가능하기 때문에 단말기와의 관계를 관리하기 어려움이 있다.

[0040] 이상 보안 요소의 종류에는 세가지 타입이 있으며, 본 발명에서 설명하는 보안 요소는 내장형 보안 요소(Embedded SE)인 것을 특징으로 하며, 이는 내장형 보안 요소(Embedded SE)에만 국한 되지 않고, USIM 및 Micro-SD와 같은 외장형 보안 요소에도 본 발명이 적용 가능하다.

[0041] 또한, 상기 신뢰받는 서비스 관리자(TSM; Trusted Service Manager)는 본 발명의 보안 서버(120)와 상응한다.

[0042] **<시스템에 대한 설명>**

[0043] 도 1은 본 발명의 보안 요소 정보 관리 시스템의 개략적인 구성을 나타낸 도면이다.

[0044] 도 1을 참조하면, 본 발명에 따른 보안 요소 정보 관리 시스템(100)은 보안 요소(110), 제1 발신부(111), 제2 발신부(112), 보안정보 확인부(113), 백업 데이터 생성부(114), 백업부(115), 복원부(116), 보안 서버(120), 백업 명령 수신부(121), 백업 데이터 수신부(122), 복원 명령 수신부(123) 및 백업 데이터 발신부(124)를 포함한다.

[0045] 보안 요소(110)는 Secure Element(SE)로 개인 정보, 애플릿 정보, 통신사 정보 및 보안 서버(120)에서 발급하는 금융 서비스 정보와 같은 다양한 정보를 저장하고 있다. 본 발명에서는 보안 요소에 저장된 정보를 이용해 백업 데이터를 생성하고, 상기 생성된 백업 데이터를 보안 서버(120)와 보안 요소(110) 사이에 설정된 보안 채널을 통하여 보안 서버(120)로 전송한다.

[0046] 보안정보 확인부(113)는 보안 요소의 보안정보에 대한 백업 명령에 응답하여 상기 보안 요소 내 보안정보를 확인한다. 상기 보안정보는 단말기에 설치된 카드 애플릿 정보, 충전식 카드(선불카드, 티머니 등)와 같은 카드의 잔액 정보, 적립카드의 마일리지 정보, 카드의 일련번호, 통신사 정보 등 보안 요소 내 저장된 모든 정보를 포함한다. 도 7은 본 발명의 일 실시예에 따라 보안 요소 내 보안정보를 확인한 경우를 나타낸 도면이다.

[0047] 상기 백업 명령은 사용자에 의해 수동적으로 요청된 백업 명령일 수도 있고, 보안 요소(110)의 업데이트 모듈이 보안 요소(110)의 업데이트를 감지하여 요청된 백업 명령일 수도 있다. 또는 보안 서버(120)에서 만약을 대비하여 요청된 백업 명령일 수도 있다.

[0048] 제1 발신부(111)는 보안정보 확인부(113)에서 확인된 보안정보에 포함되는 결제수단(카드)에 대하여 사용 정지 설정을 요청하는 명령을 발신한다. 이는 백업이 이루어 지는 동안 카드 사용의 기능을 정지시킴으로써 데이터를 안전하게 백업 및 복원하기 위함이다.

[0049] 제2 발신부(112) 단말기의 업그레이드 또는 단말기 교체가 이루어 진 후 보안 서버(120)로부터 백업 데이터를 복원이 완료된 후, 복원된 보안정보에 포함되는 결제수단에 대하여 사용 가능 설정을 요청하는 명령을 발신한다.

[0050] 백업 데이터 생성부(114)는 보안정보 확인부(113)에서 확인된 보안정보 중 적어도 일부를 이용하여 백업 데이터를 생성한다. 백업 데이터 생성부(114)는 확인된 보안정보를 이용하여 카드 애플릿 및 수치 데이터로 카테고리를 분류한다.

[0051] 백업 데이터 생성부(114)는 카드 애플릿으로 분류된 카테고리에서는 설치된 카드에 대한 카드 애플릿 설치 목록만을 추출하며(상기 추출된 설치 목록 정보는 카드 애플릿 정보를 포함함), 상기 추출된 목록을 사용자 단말기의 고유 정보 또는 사용자 식별 정보(또는 사용자가 따로 설정한 암호 등)를 이용해 암호화하여 백업 데이터를 생성한다.

[0052] 한편, 수치 데이터로 분류된 카테고리에서는 선불카드에서의 잔여 금액 또는 적립카드의 마일리지 누적 점수와 같은 수치 데이터를 추출한다. 이 때, 수치 데이터 외에 해당 카드의 특정 정보 또한 함께 추출한다. 이는 수치 데이터만 추출하여 백업 데이터로 생성했을 경우, 이를 복원 할 때, 상기 수치 데이터가 어떤 카드의 수치 정보인지 매칭시켜 복원하기 위해서이다. 이렇게 수치 데이터 및 해당 카드의 특정 정보를 추출한 후, 상기 추출된 데이터 및 해당 카드의 특정 정보를 사용자 단말기의 고유 정보 또는 사용자 식별 정보(또는 사용자가 따로 설정한 암호 등)를 이용해 암호화하여 백업 데이터를 생성한다.

[0053] 예를 들어, 백업 데이터 생성부(114)는 보안정보 확인부(113)에서 확인된 보안정보가 도 7과 같을 경우, 카드 애플릿 목록으로 카드명 A, B, C, D, E라는 정보를 추출하고, 상기 추출된 목록을 사용자 단말기의 고유 정보 또는 사용자 식별 정보(또는 사용자가 따로 설정한 암호 등)를 이용해 암호화하여 백업 데이터를 생성한다.

[0054] 한편, 수치 데이터로는 100만원, 50만원, 2000점을 추출하되, 이때 수치 데이터 뿐만 아니라 수치 데이터가 나타내는 해당 카드의 특성 정보도 함께 추출하므로, 카드 C는 100만원, 카드 D는 50만원, 카드 E는 2000점과 같은 정보가 추출된다. 상기 추출된 수치 데이터 및 해당 카드의 특정 정보를 사용자 단말기의 고유 정보 또는 사용자 식별 정보(또는 사용자가 따로 설정한 암호 등)를 이용해 암호화하여 백업 데이터를 생성한다.

[0055] 백업부(115)는 백업 데이터 생성부(114)에서 생성된 백업 데이터를 보안 요소(110)로부터 보안 서버(120)로 전

송하여 저장하도록 한다. 이때, 백업 데이터 전송은 보안 서버(120)와 보안 요소(110)사이에 설정된 보안 채널(Secure Channel)을 통해 전송하게 되며, 상기 보안 채널을 통해 전송함으로써 보안 요소의 보안정보를 백업 및 복원 시 데이터 분실 또는 손상되지 않도록 안전성을 보장한다.

[0056] 복원부(116)는 보안정보에 대한 복원 명령에 응답하여 상기 보안 서버(120)의 백업 데이터를 수신하여 데이터를 복원한다. 상기 복원 명령은 보안 요소(110)의 업데이트가 완료된 후 보안 요소(110)의 업데이트 모듈이 이를 감지하여 요청된 복원 명령일 수도 있고, 또는 단말기 교체 시 또는 보안 요소(110)의 업데이트 완료 후 사용자에 의해 수동적으로 요청된 복원 명령일 수도 있다. 또는 보안 요소(110)의 업데이트 완료를 감지하여 보안 서버(120)에서 요청된 복원 요청일 수도 있다.

[0057] 또한 백업 데이터의 복원 시 고려되어야 할 점은, 백업 데이터가 생성되었던 사용자 단말기의 보안 요소로 복원되는지 아니면 타 단말기의 보안 요소로 복원 되는지를 고려하여야 한다. 전자의 경우에는 사용자 단말기의 고유 정보로 암호화된 백업 데이터가 같은 단말기에서 복원이 이루어지므로 이상 없이 복원이 진행될 것이고, 후자의 경우는 단말기가 다르므로(단말기 교체된 경우) 사용자 단말기의 고유 정보로 암호화된 백업 데이터로는 복원되지 않을 것이다. 이러한 경우(타 보안 요소에서의 복원)를 대비하여, 백업 데이터를 암호화 할 때 사용자 단말기의 고유 정보를 이용하여 암호화하는 것 뿐만 아니라 사용자 식별 정보(또는 사용자가 따로 설정한 암호 등)를 이용해 암호화하는 것이다.

[0058] 즉 다시 말해, 보안 요소(110)의 보안정보를 이용해 백업 데이터를 생성하는 경우, 백업 데이터는 사용자 단말기의 고유 정보를 이용하여 암호화하여 백업 데이터를 생성 또는 사용자 식별 정보(또는 사용자가 따로 설정한 암호 등)를 이용해 암호화하여 백업 데이터를 생성한다.

[0059] 이때, 복원은 백업 데이터가 생성되었던 사용자 단말기 내 보안 요소에서 복원이 이루어지는 경우, 상기 사용자 단말기의 고유 정보를 이용하여 암호화된 백업 데이터로 복원이 수행되고, 타 단말기 (단말기 교체의 경우)내 보안 요소에서 복원이 이루어지는 경우, 사용자 식별 정보(또는 사용자가 따로 설정한 암호 등)를 이용하여 암호화된 백업 데이터로 복원이 수행된다.

[0060] 보안 서버(120)는 상기 설명 중 신뢰받는 서비스 관리자와 상응하는 것으로, 보안 요소(110)로부터 전송된 백업 데이터를 수신한다. 또한 복원 명령을 수신하면 상기 백업 데이터를 보안 요소(110)로 발신한다. 이때 보안 요소(110)는 백업 데이터 정보를 생성했던 사용자 단말기 내 보안 요소 일수도 있고, 또는 타 단말기 내 보안 요소(사용자가 휴대폰 교체 했을 경우) 일수도 있다.

[0061] 백업 명령 수신부(121) 사용자 또는 보안 요소(110)의 업데이트 모듈로부터 백업 명령을 수신한다. 다시 말해, 상기 백업 명령은 사용자에 의해 수동적으로 요청된 백업 명령일 수도 있고, 보안 요소(110)의 업데이트 모듈이 보안 요소(110)의 업데이트를 감지하여 요청된 백업 명령일 수도 있다. 또는 보안 서버(120) 자체적으로 만약을 대비하여 요청된 백업 명령일 수도 있다.

[0062] 백업 데이터 수신부(122) 보안 요소(110)의 백업부(115)로부터 전송된 보안 요소(110) 보안정보 중 적어도 일부의 백업 데이터를 수신하여 저장한다. 이때, 백업 데이터는 보안 서버(120)와 보안 요소(110)사이에 설정된 보안 채널(Secure Channel)을 통해 수신하며, 상기 백업 데이터를 보안 채널을 통해 수신함으로써, 백업 데이터의 분실 또는 손상에 대한 안전성을 보장할 수 있다..

[0063] 복원 명령 수신부(123)는 사용자 또는 보안 요소(110)의 업데이트 모듈로부터 복원 명령을 수신한다. 다시 말해, 복원 명령 수신부(123)는 보안 요소(110)의 업데이트가 완료된 후 보안 요소(110)의 업데이트 모듈이 이를 감지하여 요청한 복원 명령일 수도 있고, 또는 단말기 교체 시 또는 보안 요소(110)의 업데이트 완료 후 사용자에 의해 수동적으로 요청된 복원 명령일 수도 있다. 또는 보안 요소(110)의 업데이트 완료를 감지하여 보안 서버(120)에서 요청한 복원 요청일 수도 있다.

[0064] 백업 데이터 발신부(124)는 복원 명령 수신부(123)에서 수신한 복원 명령에 응답하여 백업 데이터를 보안 요소(110)으로 보낸다. 이때, 백업 데이터 발신부(124)는 백업 데이터를 보안 서버(120)와 보안 요소(110)사이에 설정된 보안 채널(Secure Channel)을 통해 보냄으로써, 백업 데이터의 분실 또는 손상에 대한 안전성을 보장할 수 있다.

[0065] **<방법에 대한 설명>**

[0066] 도 2는 본 발명의 보안 요소 정보 관리 방법의 전체 흐름도이며, 편의상 순서를 붙여 설명한다.

[0067] 1. 백업 명령 수신<S210>

[0068] 단계S210은 사용자 또는 보안 요소(110)의 업데이트 모듈로부터 백업 명령을 수신한다. 상기 백업 명령은 사용자에 의해 수동적으로 요청된 백업 명령일 수도 있고, 보안 요소(110)의 업데이트 모듈이 보안 요소(110)의 업데이트를 감지하여 요청된 백업 명령일 수도 있다. 또는 보안 서버(120) 자체적으로 만약을 대비하여 요청된 백업 명령일 수도 있다.

[0069] 2. 보안정보 확인<S220>

[0070] 단계S220은 보안정보 확인부(113)에서 단계S210에 응답하여 상기 보안 요소(110) 내 보안정보를 확인한다. 상기 보안정보는 단말기에 설치된 카드 애플릿의 정보, 충전식 카드(선불카드, 티머니 등)와 같은 카드의 잔액 정보, 적립카드의 마일리지 정보, 카드의 일련번호, 통신사 정보 등 보안 요소 내 저장된 모든 정보를 포함한다.

[0071] 3. 카드 사용 정지 설정 요청<S230>

[0072] 단계S230은 단계S220에서 보안 요소(110)내 보안정보가 확인되면, 제1 발신부(111)는 확인된 보안정보에 포함되는 결제수단(카드)에 대하여 사용 정지 설정을 요청하는 명령을 발신한다. 이는 백업이 이루어 지는 동안 카드 사용의 기능을 정지시킴으로써 데이터를 안전하게 백업 및 복원하기 위함이다.

[0073] 4. 백업 데이터 생성<S240>

[0074] 단계S240은 단계S230에서 카드 사용 정지 설정을 요청한 후 단계S220에서 확인된 보안정보 중 적어도 일부를 이용하여 백업 데이터를 생성한다. 이때 백업 데이터는 도 3의 도시된 단계를 거쳐 생성된다.

[0075] 단계S231은 카테고리를 분류하는 단계로, 단계S220에서 확인된 보안정보 중 적어도 일부를 이용하여 카드 애플릿 및 수치 데이터로 카테고리를 분류한다.

[0076] 단계S232는 카드 애플릿 설치 목록 추출 및 수치 데이터 추출 단계로, 카드 애플릿으로 분류된 카테고리에서는 설치된 카드에 대한 카드 애플릿 설치 목록만을 추출하고, 수치 데이터로 분류된 카테고리에서는 선불카드에서의 잔여 금액 또는 적립카드의 마일리지 누적 점수와 같은 수치 데이터를 추출한다. 이때, 수치 데이터는 단순한 수치 데이터뿐만 아니라 수치 데이터에 해당하는 카드의 특정 정보 또한 함께 추출한다. 이는 상기 수치 데이터의 복원 시 수치 데이터가 어떤 카드의 수치 정보인지를 매칭시켜 복원하기 위해서이다.

[0077] 단계S233은 단계S232에서 추출한 카드 애플릿 설치 목록 정보 및 수치 데이터(수치 데이터에 해당하는 카드의 특정 정보를 포함하는) 정보를 사용자 단말기의 고유 정보 또는 사용자 식별 정보(또는 사용자가 따로 설정한 암호 등)를 이용해 암호화한다.

[0078] 단계240은 단계 S233에서 암호화된 정보를 백업 데이터로 생성한다. 후에 사용자 단말기의 고유 정보를 이용해 암호화된 백업 데이터는 상기 사용자 단말기 내 보안 요소(110)에서 복원할 때 사용되고, 사용자 식별 정보(또는 사용자가 따로 설정한 암호 등)를 이용해 암호화된 백업 데이터는 타 단말기(단말기 교체의 경우)내 보안 요소에서 복원할 때 사용된다.

[0079] 5. 백업 데이터 전송<S250>

[0080] 단계S250은 단계S240에서 생성된 백업 데이터를 보안 요소(110)로부터 보안 서버(120)로 전송하여 저장하도록 한다. 이때, 백업 데이터 전송은 보안 서버(120)와 보안 요소(110)사이에 설정된 보안 채널(Secure Channel)을 통해 보안 서버(120)로 전송하며, 상기 백업 데이터를 보안 채널을 통해 전송함으로써, 백업 데이터의 분실 또는 손상에 대한 안전성을 보장할 수 있다

[0081] 단계S250가 완료된 후에는 단말기 교체, 보안 요소 교체 또는 보안 요소의 업데이트 등의 경우가 있을 수 있다.

[0082] 6. 복원 명령 수신<S260>

[0083] 단계S260은 복원 명령 수신부(123)에서 사용자 또는 보안 요소(110)의 업데이트 모듈로부터 복원 명령을 수신한다. 상기 복원 명령은 보안 요소(110)의 업데이트가 완료된 후 보안 요소(110)의 업데이트 모듈이 이를 감지하여 요청한 복원 명령일 수도 있고, 또는 단말기 교체 시 또는 보안 요소(110)의 업데이트 완료 후 사용자에 의해 수동적으로 요청된 복원 명령일 수도 있다. 또는 보안 요소(110)의 업데이트 완료를 이를 감지하여 보안 서버(120)에서 요청한 복원 요청일 수도 있다.

[0084] 7. 백업 데이터 복원<S270>

[0085] 단계S270은 단계S26에서 수신한 복원 명령에 응답하여, 백업 데이터를 보안 서버(120)와 보안 요소(110)사이에 설정된 보안 채널(Secure Channel)을 통해 수신한 후 복원을 수행한다. 이때, 복원의 경우는 단계S240에서 잠깐 설명했듯이 크게 두가지 경우로 구분할 수 있으며, 백업 데이터가 생성되었던 단말기 내 보안 요소에서의 복원 또는 타 단말기 내 보안 요소에서의 복원으로 구분할 수 있다.

[0086] 전자의 경우에는 사용자 단말기의 고유 정보를 이용해 암호화된 백업 데이터를 보안 서버(120)으로부터 수신해 복원을 수행한다. 반면 후자의 경우에는 사용자 식별 정보(또는 사용자가 따로 설정한 암호 등)를 이용해 암호화된 백업 데이터를 보안 서버(120)으로부터 수신해 복원을 수행한다.

[0087] 또한 단계S270은 도 4를 참조하여 좀 더 상세히 설명할 수 있다. 이때 도 4에 도시된 단계는 사용자 단말기 내 보안 요소에서의 복원 및 타 단말기 내 보안 요소에서의 복원에서 모두 적용 가능하다,

[0088] 단계S271은 보안 서버(120)로부터 백업 데이터를 수신한다. 즉, 상기 백업 데이터인 카드 애플릿 설치 목록 정보 및 수치 데이터(상기 수치 데이터에 해당하는 카드의 특정 정보를 포함하는) 정보를 수신한다.

[0089] 단계S272는 수치 데이터를 복원하는 단계로, 단계S271에서 수신한 백업 데이터의 카드 애플릿 설치 목록 정보를 기반으로 수치데이터를 복원할 수 있다. 상기 수치 데이터에는 수치 데이터 외에 수치에 해당하는 카드에 대한 특성 정보 또한 함께 포함하고 있기 때문에, 카드 애플릿 설치 목록을 기반으로 해당 카드의 수치 데이터를 복원 할 수 있다.

[0090] 단계273은 단계S272에서 복원된 데이터를 기반으로 제2 발신부(112)에서는 상기 복원된 보안정보에 포함되는 결제수단(카드)에 대한 사용 가능 설정을 요청하는 명령을 보안 서버(120)로 발신한다.

[0091] 단계S274는 카드 애플릿 설치 목록에 포함된 카드 정보를 디스플레이 화면에 표시한다. 다시 말해, 단계S274는 단계S272에서 수치 데이터의 복원이 이루어진 카드 정보를 포함한 설치 목록 카드 정보를 디스플레이 화면에 표시한다. 도 8은 상기 디스플레이 화면에 표시되는 일 실시 예를 나타낸다.

[0092] 단계S275는 카드 애플릿 설치 단계로, 단계S274에서 디스플레이 화면에 보여지는 다수 카드 정보 중에서 사용자가 필요한 카드만 선택함으로써, 사용자 입력에 응답하여 보안 서버(120)는 보안 요소(110)로 상기 사용자가 선택한 카드 정보에 대해 서비스 발급(신용카드와 같은 금융 서비스 등)을 하며, 보안 요소(110)는 이를 설치한다.

[0093] 지금까지 도 2 내지 도 4를 참조하여 설명한 단계는 일 실시 예에 따라 본 발명의 보안 요소(110) 측면에서의 흐름을 설명한 것이며, 도 5를 참조하여 설명하는 이하 설명은 일 실시 예에 따라 본 발명의 보안 서버(120) 측면에서의 흐름을 설명한다.

[0094] 단계S510은 백업 명령을 수신하는 단계로, 상기 백업 명령은 사용자에 의해 수동적으로 요청된 백업 명령일 수도 있고, 보안 요소(110)의 업데이트 모듈이 보안 요소(110)의 업데이트를 감지하여 요청된 백업 명령일 수도 있다. 또는 보안 서버(120)에서 만약을 대비하여 요청된 백업 명령일 수도 있다.

[0095] 단계S520은 카드 사용 정지 설정에 응답하는 단계로, 단계S230에서 제1 발신부(111)로부터 발신된 카드 사용 정지 설정 요청을 수신하여 보안 요소(110)에서 확인된 보안정보에 포함되는 결제수단을 사용하지 못하도록 서비스에 락(Lock)을 건다.

[0096] 단계S530은 백업 데이터를 수신하는 단계로, 단계S250에서 보안 요소(110)의 백업부(115)로부터 발신된 백업 데이터를 수신한다. 상기 백업 데이터는 보안 서버(120)와 보안 요소(110)사이에 설정된 보안 채널(Secure Channel)을 통해 수신된다.

[0097] 단계 S540은 복원 명령을 수신하는 단계로, 상기 복원 명령은 보안 요소(110)의 업데이트가 완료된 후 보안 요소(110)의 업데이트 모듈이 감지한 복원 명령일 수도 있고, 사용자에 의해 수동적으로 요청된 복원 명령일 수도 있다.

[0098] 단계S550은 백업 데이터를 발신하는 단계로, 단계S540에서 수신한 복원 명령에 응답하여, 백업 데이터를 보안 요소(110)으로 발신한다. 이 때, 백업 데이터는 보안 서버(120)와 보안 요소(110)사이에 설정된 보안 채널(Secure Channel)을 통해 발신한다. 또한, 보안 서버(120)에서의 백업 데이터는 상기 백업 데이터가 생성 되었던 사용자 단말기 내 보안 요소(110)로 발신할 수도 있고, 타 단말기 내 보안 요소로 발신할 수도 있다.

[0099] 단계S560은 카드 사용 가능 설정에 응답하는 단계로, 단계S550에서 백업 데이터가 보안 요소(110)로 발신되면, 보안 요소(110)의 복원부(116)에서 상기 백업 데이터를 수신하여 복원을 진행하게 되는데, 이때, 단계273에서

보안요소(110)의 제2 발신부(112)에서는 수신한 백업 데이터를 기반으로 상기 복원된 보안정보에 포함되는 결제수단에 대하여 사용 가능 설정을 요청하는 명령을 발신한다. 이에 보안 요소(120)은 사용 가능 설정 요청에 응답하여 복원된 보안정보에 포함되는 결제수단을 사용할 수 있도록 언락(Unlock)하며, 이는 단계S520에서 락(Lock)된 결제 카드의 서비스를 재 활성화시킨다.

[0100] 단계S570은 서비스를 발급하는 단계로, 단계S275에서 사용자가 카드를 선택하여 설치하면, 보안 서버(120)에서는 상기 사용자가 선택한 카드에 대한 서비스를 보안 요소(110)로 발급한다.

[0101] 본 발명의 일 실시 예에 따른 보안 요소 정보 관리 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0102] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0103] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0104] 100: 보안 요소 정보 관리 시스템

110: 보안 요소(SE; Secure Element)

111: 제1 발신부 112: 제2 발신부

113: 보안정보 확인부 114: 백업 데이터 생성부

115: 백업부 116: 복원부

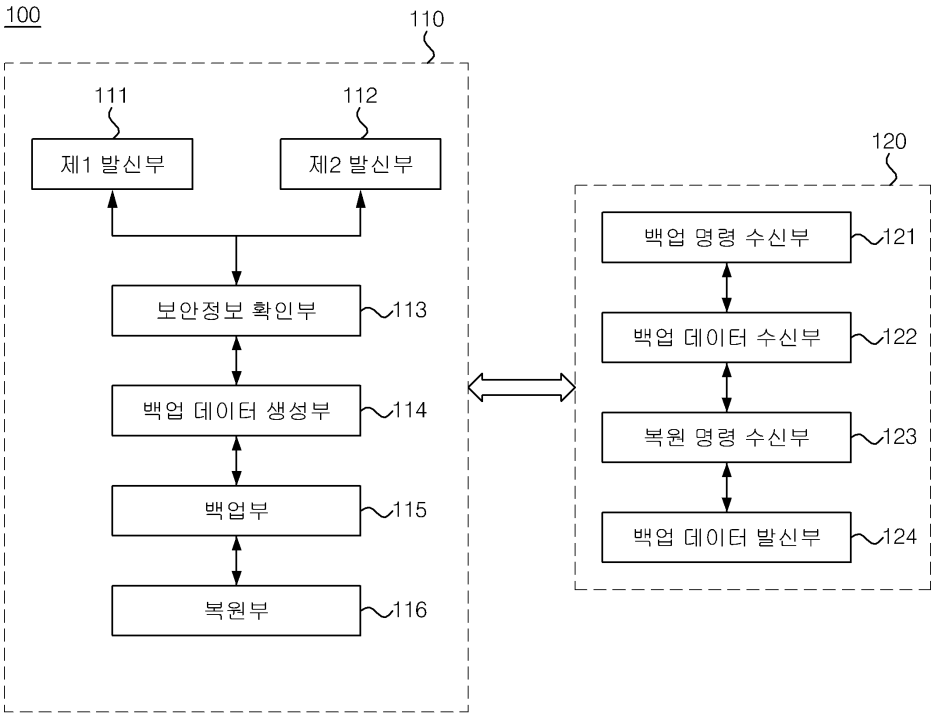
120: 보안 서버(TSM; Trusted Service Manager)

121: 백업 명령 수신부 122: 백업 데이터 수신부

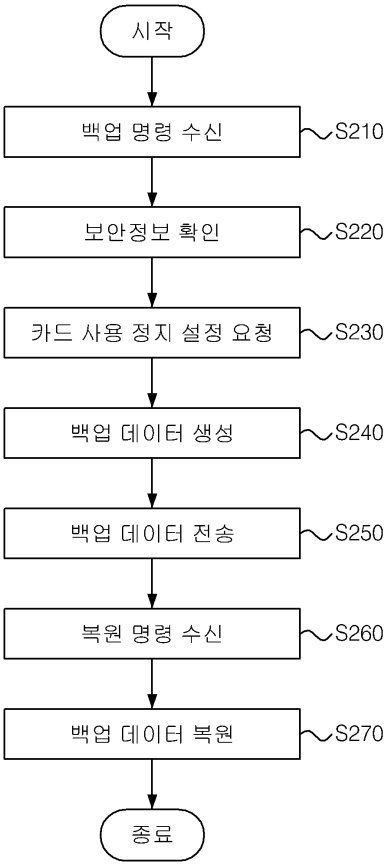
123: 복원 명령 수신부 124: 백업 데이터 발신부

도면

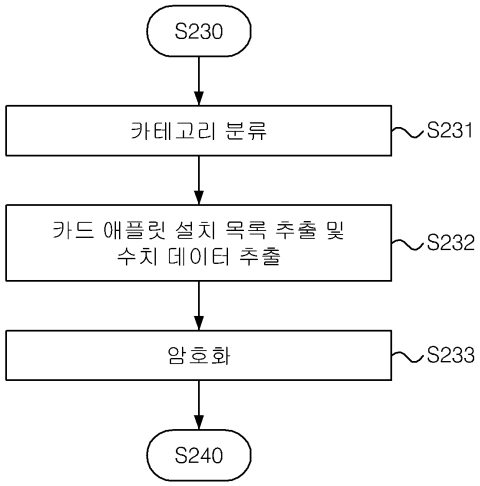
도면1


100
110
111
112
제1 발신부
제2 발신부
보안정보 확인부
113
백업 데이터 생성부
114
백업부
115
복원부
116
120
백업 명령 수신부
121
백업 데이터 수신부
122
복원 명령 수신부
123
백업 데이터 발신부
124

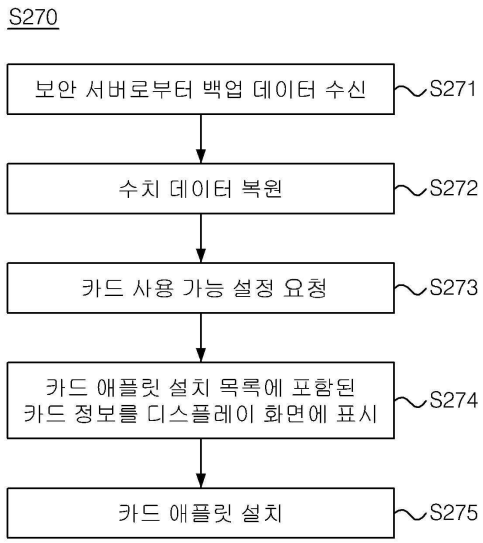
도면2


시작
백업 명령 수신
S210
보안정보 확인
S220
카드 사용 정지 설정 요청
S230
백업 데이터 생성
S240
백업 데이터 전송
S250
복원 명령 수신
S260
백업 데이터 복원
S270
종료

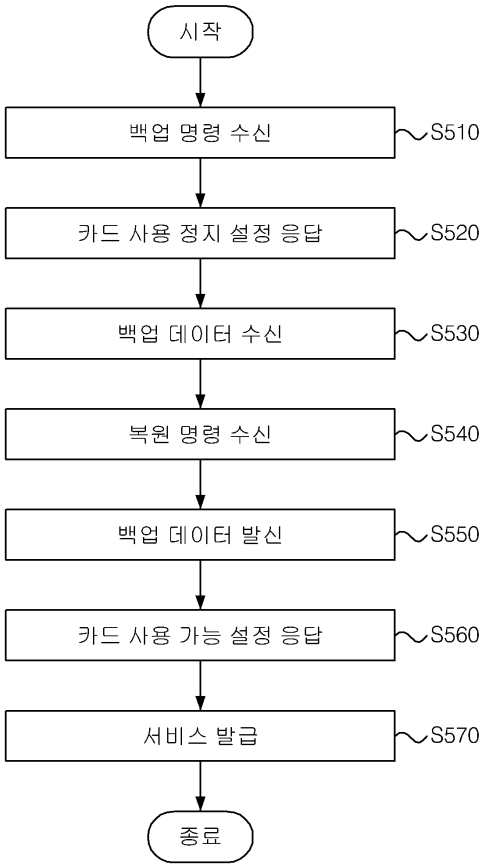
도면3


S230
카테고리 분류
S231
카드 애플릿 설치 목록 추출 및
수치 데이터 추출
S232
암호화
S233
S240

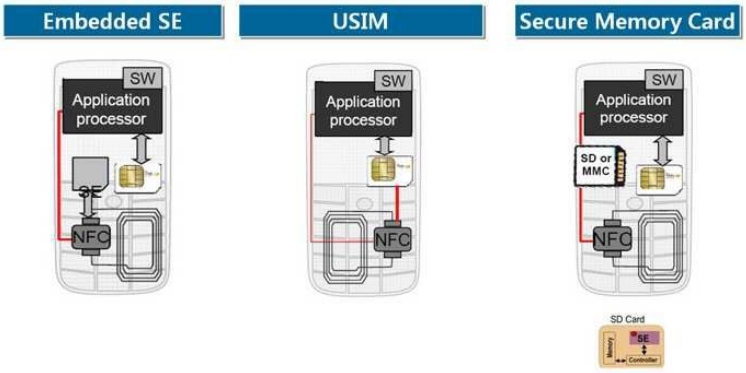
도면4


S270
보안 서버로부터 백업 데이터 수신
S271
수치 데이터 복원
S272
카드 사용 가능 설정 요청
S273
카드 애플릿 설치 목록에 포함된
카드 정보를 디스플레이 화면에 표시
S274
카드 애플릿 설치
S275

도면5


시작
백업 명령 수신
S510
카드 사용 정지 설정 응답
S520
백업 데이터 수신
S530
복원 명령 수신
S540
백업 데이터 발신
S550
카드 사용 가능 설정 응답
S560
서비스 발급
S570
종료

도면6



[핸드폰 내 Secure Element 세가지 타입]

항목	Embedded SE	USIM	Secure Memory Card
Secure Element 제공자	핸드폰 제조사나, 플랫폼 제공자 (e.g. 구글, 애플 등) 가능	이동통신 사업자	금융 서비스 제공자도 가능
OTA Channel	OTA Proxy만 가능	OTA Proxy/BIP/SMS-PP	OTA Proxy만 가능
단점	핸드폰과 일체형으로서, 핸드폰 교체시 계속적 사용 어려움	이동통신 사업자에 종속적인 서비스 모델	쉬운 탈부착이 가능하기 때문에, 핸드폰과의 관계를 관리하기 어려움
장점	플랫폼 제공자가 사업의 중심이 될 수 있음.	기존 이동통신 사업자가 제공하는 기능을 사용할 수 있음	금융 서비스 제공자들이 쉽게 자신들의 Secure Element를 발급할 수 있음.

도면7

카드명	종류	업체	카드 번호	금액	• • •
A	신용	우리은행	1234-5678-7890-3214	-	• • •
B	신용	국민은행	2486-6842-4546-8462	-	• • •
C	선불	우리은행	7531-1591-7586-9631	100만원	• • •
D	선불	신한은행	0108-5487-7706-8506	50만원	• • •
E	적립	미샤	4518-4244-0014-8003	2000점	• • •
⋮	⋮	⋮	⋮	⋮	⋱

도면8

A 우리은행	설치
B 국민은행	설치
C 우리은행	설치
D 신한은행	설치
E 미샤	설치
⋮	