



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2015년03월24일

(11) 등록번호 10-1505763

(24) 등록일자 2015년03월18일

(51) 국제특허분류(Int. Cl.)

H04W 8/20 (2009.01)

(21) 출원번호 10-2013-7016486

(22) 출원일자(국제) 2011년12월05일

심사청구일자 2013년06월25일

(85) 번역문제출일자 2013년06월25일

(65) 공개번호 10-2013-0097799

(43) 공개일자 2013년09월03일

(86) 국제출원번호 PCT/EP2011/071695

(87) 국제공개번호 WO 2012/076440

국제공개일자 2012년06월14일

(30) 우선권주장

10306359.0 2010년12월06일

유럽특허청(EPO)(EP)

(56) 선행기술조사문헌

KR100489783 B1\*

KR1020090056019 A\*

\*는 심사관에 의하여 인용된 문헌

(73) 특허권자

제말토 에스에이

프랑스, 92190 르동, 루 드 라 브레리 6

(72) 발명자

베르뉴, 파브리스

프랑스 에프-13710 휘보 슈망 드 메퇴이

이무샤, 프랑크

프랑스 에프-13390 오리올 레 쥐베에르 - 까르띠

에 뵙 드 주

루셀, 니콜라

프랑스 에프-13009 마르쎬이유 아브뉴 들 라 그랭

드 고르주

(74) 대리인

양영준, 전경석, 백만기

전체 청구항 수 : 총 6 항

심사관 : 이종익

(54) 발명의 명칭 자바 카드 애플리케이션의 데이터를 내보내고 가져오기 위한 방법

(57) 요약

본 발명은 UICC에 저장된 자바 카드 애플리케이션의 데이터를 호스트에 내보내기 위한 방법을 제안하는데, 이 방법은 자바 카드 API를 통해 애플리케이션에 이전 명령을 송신하는 단계; 데이터를 팩 내에 포맷화하는 단계 - 포맷화는 애플리케이션에 의해 실행됨 -; 및 팩을 호스트에 내보내는 단계를 포함한다. 호스트는 원격 서버 또는 다른 UICC일 수 있다. 본 발명은 또한 호스트에 저장된 자바 카드 애플리케이션의 데이터를 UICC에 가져오기 위한 대응하는 방법도 제안한다. 애플리케이션은 전자 지갑일 수 있고, 데이터는 신용카드에 관한 것일 수 있다.

**특허청구의 범위**

**청구항 1**

UICC에 저장된 자바 카드 애플리케이션(Javacard application)의 데이터를 호스트에 내보내기(exporting) 위한 방법으로서,

자바 카드 API를 통해 상기 애플리케이션에 이전 명령(transfer order)을 송신하는 단계;

상기 데이터를 팩(pack) 내에 포맷화하는 단계 - 상기 포맷화는 상기 애플리케이션에 의해 실행됨 -; 및

상기 팩을 상기 호스트에 내보내는 단계

를 포함하고,

상기 팩은 상기 UICC에 저장된 상기 자바 카드 애플리케이션과 동일한 애플리케이션에 의해 언팩(unpack)되는, 방법.

**청구항 2**

제1항에 있어서,

상기 호스트는 원격 서버인 방법.

**청구항 3**

제1항에 있어서,

상기 호스트는 다른 UICC인 방법.

**청구항 4**

제1항 또는 제2항에 있어서,

상기 호스트는 상기 UICC로부터 상기 팩을 다운로드하는 방법.

**청구항 5**

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 애플리케이션은 상기 팩을 상기 호스트에 내보내는 방법.

**청구항 6**

호스트에 저장된 자바 카드 애플리케이션의 데이터 팩을 UICC에 가져오기(importing) 위한 방법으로서,

자바 카드 API를 통해 데이터의 가져오기 명령을 애플리케이션에 송신하는 단계 - 상기 애플리케이션은 상기 UICC 상에 위치되어 있음 -; 및

상기 데이터를 언팩(unpacking)하는 단계 - 상기 언팩은 상기 애플리케이션에 의해 실행됨 -

를 포함하고,

상기 가져온(imported) 데이터 팩은 상기 UICC에 저장된 상기 애플리케이션과 동일한 애플리케이션에 의해 이미 포맷화(formatted)되어 있는 것인,

방법.

**명세서**

**기술분야**

본 발명은 UICC(Universal Integrated Circuit Card)에 저장된 자바 카드 애플리케이션의 데이터를 호스트에 내보내기 위한 방법에 관한 것이다.

[0001]

**배경 기술**

- [0002] UICC는 전자 통신 영역에서 이용되는 보안 요소이다. UICC는 Sim 애플리케이션을 내장하고, 예를 들어 이동 전화와 같은 단말 내에 고정되거나 고정되지 않게 설치된다. 일부 경우들에서, 단말은 M2M(Machine to Machine) 애플리케이션을 위해 다른 머신과 통신하는 머신으로 구성된다.
- [0003] UICC는 스마트 카드의 형태일 수 있고, 아니면 예를 들어 PCT/SE2008/050380에 기술된 것과 같은 패키지 칩 또는 임의의 다른 형태를 포함하지만 그에 한정되지는 않는 임의의 다른 형태일 수 있다. 그것은 예를 들어 GSM 및 UMTS 네트워크 내의 이동 단말에서 이용될 수 있다. UICC는 모든 종류의 개인 데이터의 네트워크 인증, 무결성 및 보안을 보장한다.
- [0004] UICC는, GSM 네트워크에서는 주로 SIM 애플리케이션을 포함하고, UMTS 네트워크에서는 USIM 애플리케이션이다. UICC는 수 개의 다른 애플리케이션을 포함할 수 있어서, 동일한 스마트 카드가 GSM 및 UMTS 네트워크 양자 모두에 액세스를 제공할 수 있고, 또한 전화번호부 및 다른 애플리케이션의 저장소를 제공한다. 해당 액세스를 위해 준비된 이동 단말을 갖고서, USIM 애플리케이션을 이용하여 GSM 네트워크에 액세스하는 것도 가능하고, SIM 애플리케이션을 이용하여 UMTS 네트워크에 액세스하는 것도 가능하다. UMTS 릴리즈 5, 및 LTE와 같은 나중 단계의 네트워크에서는, IMS(IP Multimedia Subsystem)에서의 서비스를 위해 새로운 애플리케이션인 ISIM(IP multimedia Services Identity Module)이 요구된다. 전화번호부는 가입 정보 모듈의 일부분이 아니라 별개의 애플리케이션이다.
- [0005] CDMA 네트워크에서, UICC는 3GPP USIM 및 SIM 애플리케이션 외에, CSIM 애플리케이션을 포함한다. 3가지 특정 모듈을 갖는 카드는 R-UIM(removable user identity card)이라고 지칭된다. 따라서, R-UIM 카드는 CDMA, GSM 또는 UMTS 핸드셋에 삽입될 수 있으며, 3가지 경우 모두에서 제대로 작동할 것이다.
- [0006] 2G 네트워크에서, SIM 카드 및 SIM 애플리케이션은 함께 연계되어 있었으며, 따라서 "SIM 카드"는 바로 그 물리적 카드를 의미할 수도 있고, SIM 애플리케이션을 갖는 임의의 물리적 카드를 의미할 수도 있었다.
- [0007] UICC 스마트 카드는 CPU, ROM, RAM, EEPROM 및 I/O 회로로 구성된다. 초기 버전은 완전한 풀-사이즈(85×54 mm, ISO/IEC 7810 ID-1) 스마트 카드로 구성되었다. 곧, 소형의 전화를 위해 더 작은 버전의 카드에 대한 경쟁이 발생했다.
- [0008] 카드 슬롯이 표준화되어 있기 때문에, 가입자는 자신의 무선 계정 및 전화번호를 한 핸드셋으로부터 다른 핸드셋으로 쉽게 옮길 수 있다. 이것은 그의 전화번호부 및 문자 메시지도 이전할 것이다. 마찬가지로, 가입자는 통상적으로 새로운 사업자(carrier)의 UICC 카드를 자신의 기존의 핸드셋에 삽입함으로써 사업자를 변경할 수 있다. 그러나, 일부 사업자들(예를 들어, 미국에서)은 그들이 판매한 전화에 대해 SIM-잠금을 행하여, 경쟁 사업자의 카드가 이용되는 것을 방지하기 때문에, 이것이 항상 가능한 것은 아니다.
- [0009] ETSI 프레임워크와 글로벌 플랫폼(Global Platform)의 애플리케이션 관리 프레임워크의 통합이 UICC 구성에서 표준화되어 있다.
- [0010] UICC는 3GPP 및 ETSI에 의해 표준화되어 있다.
- [0011] UICC는 통상적으로, 예를 들어 사용자가 자신의 이동 단말을 변경하고자 할 때 이동 단말로부터 제거될 수 있다. 사용자는 자신의 UICC를 새로운 단말에 삽입한 후에, 자신의 애플리케이션, 연락처 및 자격증명(네트워크 운영자)에 여전히 액세스할 수 있을 것이다.
- [0012] 또한, UICC가 단말에 종속되도록 하기 위해 그것을 해당 단말에 납땜 또는 용접하는 것이 알려져 있다. 이것은 M2M(Machine to Machine) 애플리케이션에서 행해진다. SIM 또는 USIM 애플리케이션 및 파일을 포함하는 칩(보안 요소)이 단말 내에 포함될 때에도 동일한 목적이 달성된다. 칩은 예를 들어 단말 또는 머신의 마더보드에 납땜되며, e-UICC를 구성한다.
- [0013] 디바이스에 완전히 링크되어 있지는 않지만 제거되도록 의도되지 않았거나 멀리 떨어진 단말 내에 위치되어 있거나 머신 내에 깊게 집적되어 있기 때문에 제거하기가 어려운 UICC들에 대해서도, 그러한 납땜된 UICC, 또는 UICC 내에 포함된 칩과 동일한 애플리케이션들을 포함하는 그러한 칩에 대한 것과 유사한 것이 행해질 수 있다. UICC의 특수한 형태 인자(예를 들어, 매우 작아서 다루기 쉽지 않음)도 UICC가 사실상 단말 내에 포함되어 있다고 간주하는 이유가 될 수 있다. UICC가 개방되도록 의도되지 않은 머신 내에 집적될 때에도 마찬가지이다.
- [0014] 아래의 설명에서는, 용접된 UICC, 또는 UICC와 동일한 애플리케이션을 포함하거나 포함하도록 설계된 칩들은 일

반적으로 (이동식 UICC 또는 이동식 보안 요소와 대조적으로) 내장된 UICC 또는 내장된 보안 요소라고 지칭될 것이다. 이것은 제거가 어려운 UICC 또는 보안 요소에 대해서도 마찬가지일 것이다.

**발명의 내용**

**과제의 해결 수단**

- [0015] 본 발명은 UICC에서 실행되는 애플리케이션에게, 그것이 제거되거나, 아니면 직접적으로든 호스트(서버)를 통해서든 UICC 밖으로 내보내질 것(예를 들어 다른 UICC에 설치될 것)임을 통보하는 방법에 관한 것이다.
- [0016] 본 발명은 가입(subscription) 및 관련 애플리케이션이 원격 프로비저닝 시스템을 이용하여 UICC 카드에 다운로드될 수 있는 환경에서 이루어진다.
- [0017] 이러한 UICC 카드에는, 현재의 MNO 또는 제3자에 의해 다른 애플리케이션(교통 또는 बैं킹 애플리케이션)이 설치 및 관리될 수 있다.
- [0018] UICC 카드로부터 다른 UICC 카드로 모든 데이터, 특히 MNO 및 제3자 애플리케이션의 데이터를 옮겨야 할 필요가 있다.
- [0019] 이것은 전용의 솔루션을 통해 행해질 수 있다.
- [0020] 본 발명은 UICC(이동식 또는 내장식)로부터 호스트로 대응 데이터와 함께 내보내질 자바 카드 애플리케이션에 적용가능한 방법에 관한 것이며, 이 호스트는 예를 들어 다른 UICC이다.
- [0021] 본 발명은 UICC에 저장된 자바 카드 애플리케이션(Javacard application)의 데이터를 호스트에 내보내기 (exporting) 위한 방법을 제안하는데, 이 방법은:
- [0022] 자바 카드 API를 통해 애플리케이션에 이전 명령(transfer order)을 송신하는 단계;
- [0023] 데이터를 팩(pack) 내에 포맷화하는 단계 - 포맷화는 그 애플리케이션에 의해 실행됨 -; 및
- [0024] 팩을 호스트에 내보내는 단계
- [0025] 를 포함한다.
- [0026] 호스트는 팩이 예를 들어 다른 UICC에의 추후의 다운로드를 위해 내보내질 원격 서버일 수 있다.
- [0027] 호스트는 다른 UICC일 수 있다. 이 경우, 팩은 중간자 없이 제1 UICC로부터 제2 UICC로 직접 이전된다.
- [0028] 내보내기는 호스트에 의해(호스트가 데이터 팩을 검색해 옴), 또는 UICC에 의해(UICC가 데이터 팩을 보냄) 관리될 수 있다.
- [0029] 본 발명은 또한 호스트에 저장된 자바 카드 애플리케이션의 데이터 팩을 UICC에 가져오기(importing) 위한 방법을 제안하는데, 이 방법은:
- [0030] 자바 카드 API를 통해 데이터의 가져오기 명령을 애플리케이션에 송신하는 단계 - 애플리케이션은 UICC 상에 위치됨 -; 및
- [0031] 데이터를 언팩(unpacking)하는 단계 - 언팩은 그 애플리케이션에 의해 실행됨 -
- [0032] 를 포함한다.
- [0033] 애플리케이션 프로그래밍 인터페이스(API)는 소프트웨어 프로그램에 의해 구현되어 그 소프트웨어 프로그램이 다른 소프트웨어와 상호작용할 수 있게 해 주는 인터페이스이다. 그것은 사용자 인터페이스가 사람과 컴퓨터 사이의 상호작용을 용이하게 해 주는 것과 마찬가지로, 상이한 소프트웨어 프로그램들 사이의 상호작용을 용이하게 해 준다.

**발명을 실시하기 위한 구체적인 내용**

- [0034] 본 발명은 자바 카드 표준 API에 기반을 두는 어떠한 애플리케이션에 의해서도 이용될 수 있는 새로운 내보내기/가져오기 자바 카드 API를 정의할 것을 제안한다. 이러한 새로운 내보내기/가져오기 자바 카드 API는 애플리케이션에게 그것의 데이터를 내보내야 한다는 것을 알리기 위한 적어도 하나의 엔트리 포인트, 및 애플리케이션에게 데이터를 가져와야 한다는 것과 어떤 데이터인지를 알리기 위한 하나의 엔트리 포인트를 포함한다. 이러

한 엔트리 포인트들은 애플리케이션에 의해 구현되는 경우에 UICC의 운영 체제에 의해 호출된다. 이러한 새로운 API를 구현하는 애플리케이션은 (카드 제조사에는 독립적으로) 이러한 API를 제공하는 어떠한 자바 카드 호환 UICC 상이라도 설치될 수 있어서, 용이한 상호운영성(interoperability)을 보장한다. 내보내기를 위한 엔트리 포인트는 UICC에 저장된 애플리케이션의 데이터를 내보내는 기능에 대응하며, 이 UICC는 예를 들어 단말(예를 들어, 이동 단말 또는 머신) 내에 내장된다(제거가능하지 않음). 이동 단말은 예를 들어 이동 전화이다. 그러면, 애플리케이션의 데이터를 제1 UICC로부터 제2 UICC로 이전하는 것이 가능하며, 제2 UICC는 제1 UICC와 동일한 애플리케이션을 포함한다. 그러면, 제2 UICC는 제1 UICC와 동일한 환경에서, 즉 동일 데이터를 갖고서 이 애플리케이션으로 작업할 수 있을 것이다. 제1 및 제2 UICC가 동일한 UICC 제조사의 것일 필요는 없다.

[0035] 이러한 이벤트에 의해 트리거될 때, 애플리케이션은 백업, 통보, 또는 애플리케이션에 관련된 비밀 사용자 데이터의 이동성을 유지하기 위해 원격 서버와의 사이에서 요구되는 것(예를 들어, 전자 지갑 신용 카드의 백업)을 위해, 필요한 조치를 취한다.

[0036] 데이터가 하나의 UICC 카드로부터 다른 UICC 카드로 옮겨져야 할 때, 이러한 API를 구현하는 UICC 상의 모든 애플리케이션은 그 데이터가 해당 UICC로부터 삭제되고 (예를 들어 다른 UICC 카드로) 내보내질 것임을 통보받는 것이 바람직하다.

[0037] UICC에 저장된 자바 카드 애플리케이션의 데이터를 호스트에 내보내기 위한 방법은 첫번째로 이전 명령을 자바 카드 API를 통해 이 애플리케이션에 송신하는 단계를 포함한다. 이러한 명령의 송신은 예를 들어 단말의 GUI의 메뉴에서의 사용자 동작 후에 UICC의 OS에 의해 행해질 수 있다.

[0038] 그러면, 애플리케이션 자신이 이 애플리케이션에 링크된 데이터의 팩을 포맷화한다. 다음으로, 팩은 IP 또는 링크를 통해 호스트로, 예를 들어 원격 서버로 내보내질 준비가 된다. 팩은 예를 들어 NFC 또는 블루투스를 통해 다른 UICC에 직접 이전될 수도 있다.

[0039] 호스트가 UICC로부터 팩을 검색해오는 주도권을 가질 수도 있고, UICC 스스로가 데이터 팩을 내보내기로 결정할 수 있다.

[0040] 데이터 팩은 바람직하게는 암호화되어 호스트에 송신된다.

[0041] 호스트에 설치되고 나면, 내보내진 팩은 다른 UICC에 설치되도록 검색될 수 있다. 이와 관련하여, 본 발명은 데이터의 가져오기 명령을 UICC 상에 위치되어 있는 동일 애플리케이션에 내보내기/가져오기 자바 카드 API를 통해 송신하고, 데이터를 언팩하는 것(언팩은 그 애플리케이션에 의해 실행됨)을 제안한다.

[0042] 제1 UICC 내에서 데이터 팩의 포맷화를 실행한 애플리케이션이 제2 UICC 내에서 데이터 팩을 언팩하는 애플리케이션과 동일하므로, 제2 UICC의 수준에서 동일한 환경이 획득된다.

[0043] 제1 UICC 상의 데이터 및 애플리케이션은 일단 내보내지고 나면 삭제되어, 애플리케이션 및 데이터의 중복을 회피한다.

[0044] 본 발명에 의해, UICC 내에 내장된 한 애플리케이션 또는 모든 애플리케이션은 통보받은 대로, 사용자 자격증명 및 이전가능한 데이터를 원격 서버에 백업할 수 있을 것이다.

[0045] 애플리케이션은 어느 데이터가 내보내져야 할지 및 그들이 어떻게 보안되는지를 스스로 책임질 수 있다.

[0046] 바람직하게는, 본 발명은 예를 들어 애플리케이션(예를 들어, बैंक 애플리케이션)의 데이터를 제1 단말 내에 포함된 제1 UICC로부터 제2 단말 내에 포함된 제2 UICC에 이전하기 위해, 내장형 UICC에 적용된다. बैंक 애플리케이션은 이러한 제2 UICC로의 데이터의 이전이 발생할 때 이미 제2 UICC 내에 설치되어 있을 수도 있고, 아니면 추후에 설치될 수도 있다.