(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년03월20일
(11) 등록번호 10-1504855
(24) 등록일자 2015년03월16일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2013-7017753
(22) 출원일자(국제) 2011년12월05일
심사청구일자 2013년07월05일
(85) 번역문제출일자 2013년07월05일
(65) 공개번호 10-2013-0093676
(43) 공개일자 2013년08월22일
(86) 국제출원번호 PCT/EP2011/071778
(87) 국제공개번호 WO 2012/076480
국제공개일자 2012년06월14일
(30) 우선권주장
10306359.0 2010년12월06일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
JP2010532107 A
JP2010501092 A
US20080261561 A1
전체 청구항 수 : 총 3 항

(73) 특허권자
제말토 에스에이
프랑스, 92190 므동, 루 드 라 브레리 6
(72) 발명자
메리엔, 리오넬
캐나다 에이치4케이1와이3 큐씨 퀘벡 뤼 리모게스 몬트리얼
베라르, 자비에
프랑스 에프-13950 까돌리브 루뜨 뒤 스따드
(74) 대리인
양영준, 전경석, 백만기

심사관 : 손영태

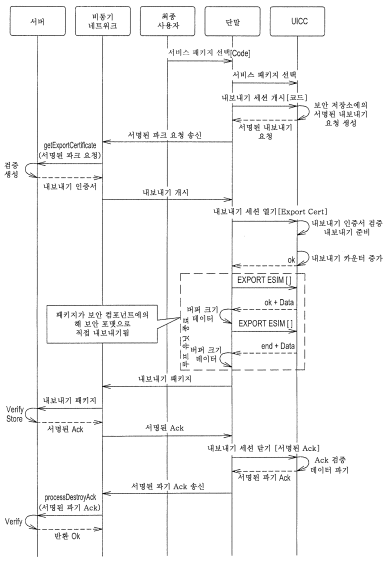
(54) 발명의 명칭 **단말에 포함된 UICC에 포함된 데이터를 보안 서버 상에 내보내기 위한 방법**

(57) 요 약

본 발명은 단말에 포함된 UICC에 포함된 데이터를 보안 서버 상에 내보내기 위한 방법을 제안한다. 방법은, 내보내기 요청 시에, UICC에 의해 내보내기 요청에 서명하는 단계 - 서명된 내보내기 요청은 단말에 의해 서버에 전송됨 - ; 서버의 레벨에서, UICC의 신원과 서명을 비교함으로써, 서명된 내보내기 요청을 검증하는 단계; 검증

(뒷면에 계속)

대 표 도 - 도1



이 긍정적인 경우, 서버에 의해, 서명된 내보내기 인증서(export certificate)를 단말을 경유하여 UICC에 송신하는 단계; UICC에서 내보내기 인증서를 검증하고, 긍정적인 경우, 데이터를 포함하는 내보내기 패키지를 준비하는 단계 - 내보내기 패키지는 UICC에 의해 서명되고 암호화됨 - ; 내보내기 패키지를 단말에 송신하고, UICC 내에서, 내보내진 데이터를 "사용불가능"으로 설정하는 단계; 내보내기 패키지를 단말로부터 서버로 전송하는 단계; 서버의 레벨에서 패키지를 수신하고 서명을 검증하는 단계; 확인 메시지에 서명하고, 확인 메시지를 단말을 경유하여 UICC에 전송하는 단계; UICC에서, 확인 메시지를 검증하고, 서버의 서명이 인식되는 경우에는, 내보내진 데이터를 파기하고, 서명된 확인 메시지를 단말을 경유하여 서버에 송신하는 단계; 및 서버 내에서 확인 메시지의 서명을 검증하고, 서명이 인식되는 경우에는 데이터를 새로운 단말 또는 UICC로의 이전에 이용가능해지게 하는 단계를 포함한다.

특허청구의 범위

청구항 1

단말에 포함된 UICC 상에 포함된 데이터를 보안 서버에 전송하기 위한 방법으로서,

전송 요청 시에, 상기 UICC가 상기 전송 요청에 서명하는 단계 - 상기 서명된 전송 요청은 상기 단말에 의해 상기 서버에 전송됨 - ;

상기 서버의 레벨에서, 상기 UICC의 신원(identity)과 서명을 비교함으로써, 상기 서버가 상기 서명된 전송 요청을 검증하는 단계;

상기 검증이 성공적인 경우, 상기 서버에 의해, 서명된 전송 인증서를 상기 단말을 경유하여 상기 UICC에 송신하는 단계;

상기 UICC에서 상기 UICC가 상기 전송 인증서를 검증하고, 상기 검증이 성공적인 경우, 상기 UICC가 상기 데이터를 포함하는 전송 패키지를 준비하는 단계 - 상기 전송 패키지는 상기 UICC에 의해 서명되고 암호화됨 - ;

상기 UICC가 상기 전송 패키지를 상기 단말에 송신하고, 상기 UICC 내에서, 전송된 데이터를 "사용불가능(unusable)"으로 설정하는 단계;

상기 단말이 상기 전송 패키지를 상기 단말로부터 상기 서버로 전송하는 단계;

상기 서버가 상기 서버의 레벨에서 상기 패키지를 수신하고 상기 서명을 검증하는 단계;

상기 서버가 확인 메시지(acknowledgment message)에 서명하고, 상기 확인 메시지를 상기 단말을 경유하여 상기 UICC에 전송하는 단계;

상기 UICC에서, 상기 UICC가 상기 확인 메시지를 검증하고, 상기 서버의 서명이 인식되는 경우에는, 전송된 데이터를 파기하고, 서명된 확인 메시지를 상기 단말을 경유하여 상기 서버에 송신하는 단계; 및

상기 서버가 상기 서버 내에서 상기 확인 메시지의 서명을 검증하고, 상기 서명이 인식되는 경우에는 상기 데이터를 전송을 위해 이용가능해지게 하는 단계

를 포함하는 방법.

청구항 2

제1항에 있어서,

상기 UICC는 상기 단말 내에 내장되는 방법.

청구항 3

제1항 또는 제2항에 있어서,

상기 전송 요청 전에, 전송될 데이터의 선택이 이루어지는 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 단말에 포함된 UICC(Universal Integrated Circuit Card)에 포함된 데이터를 보안 서버 상에 내보내기 위한 방법에 관한 것이다.

배 경 기 술

[0002] UICC와 같은 보안 요소는 Sim 애플리케이션을 내장하고 있다. 보안 요소는 예를 들어 이동 전화와 같은 단말 내에 고정되거나 고정되지 않게 설치될 수 있다. 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 모두에의 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 특징 모두를 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 전화기를 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 할때 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] 본 발명은 그러한 납땜된 UICC, 또는 UICC 내에 포함된 칩과 동일한 애플리케이션들을 포함하는 그러한 칩에도 적용된다. 디바이스에 완전히 링크되어 있지는 않지만 제거되도록 의도되지 않았거나 멀리 떨어진 단말 내에 위치되어 있거나 머신 내에 깊게 집적되어 있기 때문에 제거하기가 어려운 UICC들에 대해서도 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. 그러한 용접된 UICC, 또는 UICC와 동일한 애플리케이션을 포함하거나 포함하도록 설계된 칩들은 일반적으로 (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

해결하려는 과제

[0014] 본 발명은 보안 컴포넌트(UICC 칩)로부터 보안 저장소(secure vault)(예를 들어, 보안 서버)로 송신될 민감한 데이터(sensitive data)의 내보내기로서, 데이터의 복제(cloning)의 위험을 수반하지 않고, UICC와 보안 서버 간의 직접적인 데이터 링크도 수반하지 않는 내보내기에 관한 것이다. 더 구체적으로, 본 발명은 단말에 포함된 UICC에 포함된 데이터를 보안 서버 상에 내보내기 위한 방법에 관한 것이다.

[0015] 이동 단말, 예를 들어 이동 전화기, 무선 단말 또는 접속 단말과 같은 단말을 교체할 때, 사용자는 자신의 기존 단말에서 이용가능했던 서비스들을 계속 유지하는 기능을 원한다. 셀룰러 서비스 또는 뱅킹 서비스와 같은 이들 서비스는 단말의 UICC에 로드되는 키 및 민감한 데이터에 의존하고 있다.

[0016] 고전적인 SIM 카드와 같이, 보안 컴포넌트(UICC)가 제거가능하고, 새로운 단말이 그러한 제거가능한 컴포넌트를 지원한다면, 사용자는 단순히 보안 컴포넌트를 오래된 단말로부터 제거하여 그것을 새로운 단말에 삽입할 수 있다.

[0017] 그러나, UICC가 제거가능하지 않거나(내장형 UICC) 새로운 단말이 이러한 유형의 컴포넌트를 지원하지 않는다면, 그 서비스에 관련된 모든 키 및 데이터를 새로운 단말의 보안 컴포넌트에 옮길 방법이 필요하다.

[0018] 내장형 UICC의 경우에 발생하는 다른 문제는 오래된 단말과 새로운 단말이 때로는 동시에 이용가능하지 않다는 것이다. 사용자는 새로운 단말을 구입하기 전에 자신의 민감한(개인) 데이터 및 키를 안전하게 하기를 원한다.

[0019] 본 발명은 장래의 다른(또는 동일한) 단말에의 다운로드를 위해, 서비스에 관련된 키 및 데이터를 그 키 및 데이터가 복제될 수 없는 방식으로 보안 저장소에 안전하게 내보내는 방법을 제공한다.

[0020] 또한, 본 발명은 보안 저장소와 보안 컴포넌트 사이에 직접적인 IP 링크가 설정될 수 없을 수도 있다는 문제를 해결한다.

과제의 해결 수단

[0021] 이러한 목적을 위해, 본 발명은 단말에 포함된 UICC에 포함된 데이터를 보안 서버 상에 내보내기 위한 방법을 제안한다. 방법은:

[0022] 내보내기 요청 시에, UICC에 의해 내보내기 요청에 서명하는 단계 - 서명된 내보내기 요청은 단말에 의해 서버에 전송됨 - ;

[0023] 서버의 레벨에서, UICC의 신원(identity)과 서명을 비교함으로써, 서명된 내보내기 요청을 검증하는 단계;

[0024] 검증이 긍정적인 경우, 서버에 의해, 서명된 내보내기 인증서(export certificate)를 단말을 통해 UICC에 송신하는 단계;

[0025] UICC에서 내보내기 인증서를 검증하고, 긍정적인 경우 데이터를 포함하는 내보내기 패키지(export package)를 준비하는 단계 - 내보내기 패키지는 UICC에 의해 서명되고 암호화됨 - ;

[0026] 내보내기 패키지를 단말에 송신하고, UICC 내에서, 내보내진 데이터를 "사용불가능(unusable)"으로 설정하는 단계;

[0027] 내보내기 패키지를 단말로부터 서버로 전송하는 단계;

[0028] 서버의 레벨에서 패키지를 수신하고 서명을 검증하는 단계;

[0029] 확인 메시지(acknowledgment message)에 서명하고, 확인 메시지를 단말을 경유하여 UICC에 전송하는 단계;

[0030] UICC에서, 확인 메시지를 검증하고, 서버의 서명이 인식되는 경우에는, 내보내진 데이터를 파기하고, 서명된 확인 메시지를 단말을 경유하여 서버에 송신하는 단계; 및

[0031] 서버 내에서 확인 메시지의 서명을 검증하고, 서명이 인식되는 경우에는 데이터가 새로운 단말 또는 UICC로의 이전에 이용가능해지게 하는 단계

[0032] 를 포함한다.

[0033] UICC는 바람직하게는 단말 내에 내장되고, 내보내기 요청 전에, 내보내질 데이터의 선택이 이루어진다.

도면의 간단한 설명

[0034] 본 발명은 본 발명의 바람직한 실시예의 흐름도를 나타내는 도 1에 관한 이하의 설명을 읽으면 더 잘 이해될 것

이다.

발명을 실시하기 위한 구체적인 내용

[0035] 본 발명은 보안 컴포넌트(UICC)와, 예를 들어 원격 서버에 의해 구성된 보안 저장소 간의 비동기 접속을 통합한다.

[0036] 도 1에서, 단말의 최종 사용자는 먼저, 내보내질 데이터를 선택한다. 이러한 데이터는 예를 들어 사용자가 추후에 다른(또는 동일한) 단말로 이전할 수 있도록 안전하게 하기를 원하는 전화 번호 또는 개인 키이다.

[0037] 이것은 UICC 상에서 애플리케이션 id 또는 서비스 id를 선택함으로써 행해질 수 있다. 이것은 단말 상의 애플리케이션을 통해 사용자에 의해 행해질 수도 있고, 단말을 통해 자동으로 행해질 수도 있다. 이것은 최종 사용자에 의해 만들어진 내보내기 요청에 대응한다. 그러한 내보내기 요청은 원격 서버에 의해 또는 단말에 의해서도 만들어질 수 있다.

[0038] 선택적으로, UICC로부터 내보내질 데이터/서비스를 선택할 때, 사용자/단말은 데이터에의 액세스를 얻기 위해, UICC 또는 서비스를 향해 코드를 제공하거나 인증을 해야할 수 있다.

[0039] 다음으로, 단말은 "내보내기 세션 개시(INIT EXPORT SESSION)" 명령을 그에 송신함으로써, 보안 컴포넌트 상에서 내보내기 세션을 개시한다.

[0040] 이에 응답하여, UICC는 "서명된 내보내기 요청(Signed Export request)"을 단말에 반환한다. 이 요청은 UICC에 의해 고유하게 식별되고 서명된다.

[0041] "서명된 내보내기 요청은" IP, 셀룰러, OTA 또는 OTI 네트워크와 같은 네트워크를 통해 서버에 비동기로 전송된다.

[0042] 수신 시에, 서버는 UICC의 신원과 서명을 비교함으로써, "서명된 내보내기 요청"을 검증한다. 본 발명은 어떠한 특정한 보안 방식도 요구하지 않지만, 서버가 UICC의 서명을 검증할 수 있을 것을 요구한다.

[0043] 그러면, 서버는 "내보내기 인증서(Export Certificate)"를 생성한다. 이 인증서는 서버에 의해 고유하게 서명되고, UICC를 고유하게 식별한다. 이 인증서로, 서버는 UICC가 진짜이며, 내보내기 프로세스가 개시될 수 있음을 확인한다.

[0044] "내보내기 인증서"는 단말에 의해 UICC에 비동기로 전송된다.

[0045] 다음으로, UICC는 "내보내기 인증서"를 검증한다. 본 발명은 특정한 보안 방식을 지정하지 않지만, UICC는 서버로부터의 서명을 검증하는 능력을 반드시 가져야 한다.

[0046] UICC는 "내보내기 카운터(Export Counter)"를 증가시킨다. 이 카운터는 UICC에 의해 유지된다.

[0047] UICC는 "내보내기 패키지"를 준비한다. 이 내보내기 패키지는 UICC에 의해 암호화되고 서명된다. 추가로, "내보내기 패키지"는 "내보내기 카운터"를 포함한다. 내보내기 패키지는 단말에 송신된다. (도면에 도시된 바와 같이) 단말과 UICC 간의 I/O 제한으로 인해 필요하다면, 내보내기 패키지는 복수의 커맨드를 통해 송신될 수 있다. 단말에 송신된 후, UICC 레벨에서 유지되어 있는 전송된 패키지의 이미지는 비활성으로 된다(패키지의 가능한 중복을 회피하기 위해).

[0048] 다음으로, "내보내기 패키지"는 서버에 비동기로 전송된다. 그것은 암호화되어 있으므로, 서버만이 그것을 읽을 수 있다.

[0049] 수신되고 나면, 서버는 내보내기 패키지를 복호화하고 검증한다. 각각의 UICC에 대해, 서버는 내보내기 카운터의 사본을 유지한다. 내보내기 패키지 내의 내보내기 카운터는 서버에 의해 유지되는 내보내기 카운터의 사본보다 높아야 하며, 그렇지 않으면 내보내기 패키지는 거부된다. 내보내기 패키지가 받아들여지고 나면, 서버는 자신의 내보내기 카운터의 사본을 내보내기 패키지 내의 값에 일치하도록 업데이트한다.

[0050] 다음으로, 서버는 서명된 Ack를 생성한다. 이 Ack는 서버에 의해 고유하게 서명되고, 내보내기 카운터의 값을 포함한다. 이 커맨드를 송신한 때, 수신된 패키지는 서버의 레벨에서 비활성으로 된다.

[0051] 서명된 Ack는 UICC에 비동기로(즉, 단말을 통해) 전송된다.

[0052] UICC는 수신된 서명된 Ack를 검증하고, 그것이 일치하면, 자신의 내보내진 데이터의 사본(이미지)을 파기한다.

[0053] 다음으로, UICC는 서명된 파기 Ack(Signed Destroy Ack)를 생성하고, 이것은 UICC에 의해 고유하게 서명되며, 내보내기 카운터의 값을 포함한다.

[0054] 서명된 파기 Ack는 비동기로 서버에 전송된다.

[0055] 다음으로, 서버는 서명된 파기 Ack를 검증한다. 그것이 일치하면, 내보내진 데이터는 나중에 새로운 단말 또는 동일한 단말 내의 다른 UICC로의 가져오기에 이용할 수 있게 된다.

[0056] 본 발명의 이점은 아래와 같다:

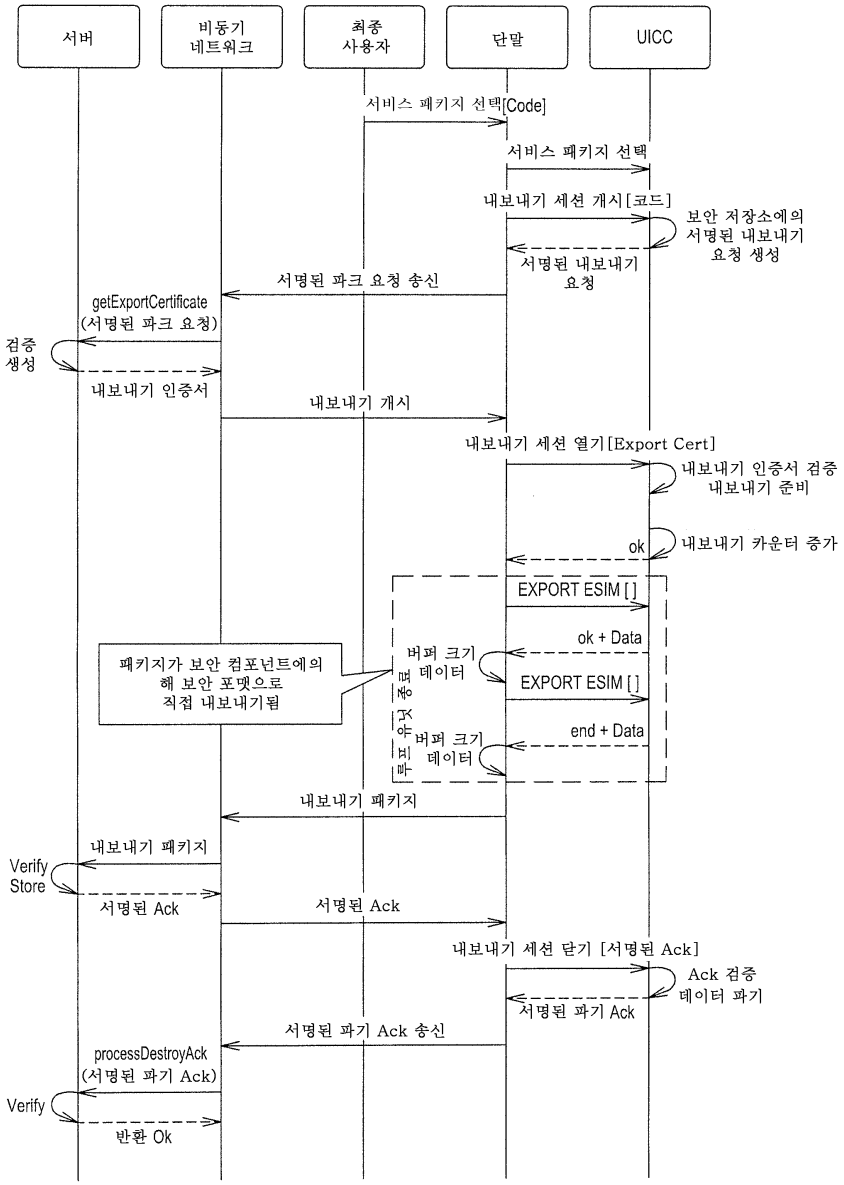
[0057] - 프로세스의 모든 지점에서, 본 발명은 프로세스를 차단하고 복귀(rollback)시키는 양호한 방법을 제공한다. 그러므로, 데이터를 상실할 위험이 없다.

[0058] - 모든 프로세스가 비동기 접속을 통해 행해질 수 있다(예를 들어, 이메일). UICC가 서버에 직접 접속될 필요가 없다.

[0059] - 복제된 정보를 갖는 것이 불가능하다. 데이터는 UICC 내에서 파기되었다는 확인 후에만 서버에서 이용가능하다.

도면

도면1


서버
비동기 네트워크
최종 사용자
단말
UICC
서비스 패키지 선택[Code]
서비스 패키지 선택
내보내기 세션 개시[코드]
보안 저장소에의 서명된 내보내기 요청 생성
서명된 내보내기 요청
서명된 파크 요청 송신
getExportCertificate (서명된 파크 요청)
검증 생성
내보내기 인증서
내보내기 개시
내보내기 세션 열기[Export Cert]
내보내기 인증서 검증 내보내기 준비
ok
내보내기 카운터 증가
EXPORT ESIM [ ]
ok + Data
버퍼 크기 데이터
EXPORT ESIM [ ]
end + Data
버퍼 크기 데이터
패키지가 보안 컴포넌트에의해 보안 포맷으로 직접 내보내기됨
내보내기 패키지
내보내기 패키지
Verify Store
서명된 Ack
서명된 Ack
내보내기 세션 닫기 [서명된 Ack]
Ack 검증 데이터 파기
서명된 파기 Ack
서명된 파기 Ack 송신
processDestroyAck (서명된 파기 Ack)
Verify
반환 Ok