(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년05월19일
(11) 등록번호 10-0898055
(24) 등록일자 2009년05월11일

(51) Int. Cl.
H04W 12/08 (2009.01) *H04W 8/24* (2009.01)
(21) 출원번호 10-2008-0129038
(22) 출원일자 2008년12월18일
심사청구일자 2008년12월18일
(56) 선행기술조사문헌
KR1020040023089 A
KR1020020072240 A

(73) 특허권자
주식회사 스마트카드연구소
서울 구로구 구로동 182-13 대륭포스트타워 2차 1201,1202,1203
(72) 발명자
김운
서울특별시 송파구 오금동 55-8 반석블레스빌아파트 304호
김형석
서울특별시 구로구 구로동 1130-6번지 708호
(뒷면에 계속)
(74) 대리인
특허법인지명

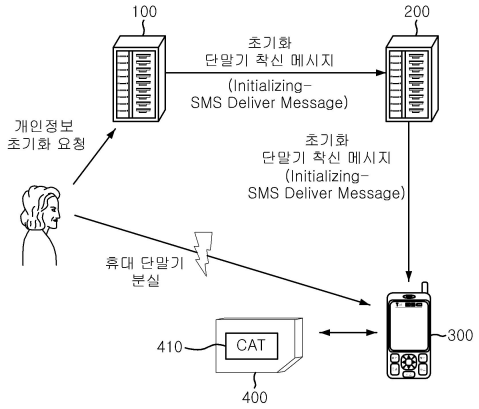
전체 청구항 수 : 총 15 항 심사관 : 문성돈

(54) ＵＩＣＣ의 개인 정보 보호 시스템 및 방법

(57) 요 약

본 발명은 UICC의 개인 정보 보호 시스템 및 방법에 관한 것으로, 특정 UICC(Universal IC Card)의 개인정보 초기화 요청에 따라 상기 UICC에 저장된 개인 정보를 초기화하는 초기화 명령어가 포함되고 상기 UICC에 할당된 전화번호를 수신번호로 하는 초기화 단말기 착신 메시지(Initializing_SMS Deliver Message)를 생성하는 초기화 관리 서버 및 상기 초기화 관리 서버로부터 전송된 상기 초기화 단말기 착신 메시지를 상기 UICC에 할당된 전화번호로 전송하는 단문 메시지 센터(SMSC : Short Message Service Center)를 포함하여 구성되는 것을 특징으로 한다.

대 표 도 - 도1



(72) 발명자

김대철

서울특별시 송파구 오금동 55-8 반석블레스빌아파트 304호

신남호

서울특별시 관악구 신림동 1659-7

특허청구의 범위

청구항 1

특정 UICC(Universal IC Card)의 개인정보 초기화 요청에 따라 상기 UICC에 저장된 개인 정보를 초기화하는 초기화 명령어가 포함되고 상기 UICC에 할당된 전화번호를 수신번호로 하는 초기화 단말기 착신 메시지(Initializing_SMS Deliver Message)를 생성하는 초기화 관리 서버; 및

상기 초기화 관리 서버로부터 전송된 상기 초기화 단말기 착신 메시지를 상기 UICC에 할당된 전화번호로 전송하는 단문 메시지 센터(SMSC : Short Message Service Center);를 포함하여 구성되는 것을 특징으로 하는 UICC의 개인 정보 보호 시스템.

청구항 2

단문 메시지(Short Message Service)를 수신하는 휴대 단말기; 및

상기 휴대 단말기에 장착되고 사용자의 개인 정보를 저장하는 UICC(Universal IC Card);를 포함하여 구성되되,

상기 휴대 단말기는, 개인정보 초기화 요청에 따라 상기 UICC에 저장된 상기 개인 정보를 초기화하는 초기화 명령어를 포함하는 초기화 단말기 착신 메시지(Initializing_SMS Deliver Message)를 수신한 경우, 상기 초기화 단말기 착신 메시지를 상기 UICC로 전송하는 UICC 메시지 전송모듈을 포함하고,

상기 UICC는, 상기 초기화 단말기 착신 메시지를 전송받은 경우 상기 초기화 단말기 착신 메시지로부터 상기 초기화 명령어를 추출하고, 상기 초기화 명령어에 따라 상기 UICC에 저장된 상기 개인 정보를 초기화시키는 초기화 카드 애플리케이션 툴킷(Card Application Toolkit : CAT)을 포함하는 것을 특징으로 하는 UICC의 개인 정보 보호 시스템.

청구항 3

개인정보 초기화 요청에 따라 특정 UICC(Universal IC Card)에 저장된 개인 정보를 초기화하는 초기화 명령어가 포함되고 상기 UICC에 할당된 전화번호를 수신번호로 하는 초기화 단말기 착신 메시지(Initializing_SMS Deliver Message)를 생성하는 초기화 관리 서버;

상기 초기화 관리 서버로부터 전송된 상기 초기화 단말기 착신 메시지를 상기 UICC에 할당된 전화번호로 전송하는 단문 메시지 센터(SMSC : Short Message Service Center);

상기 초기화 단말기 착신 메시지를 수신하는 휴대 단말기; 및

상기 휴대 단말기에 장착되어 상기 초기화 단말기 착신 메시지를 전송받는 상기 UICC;를 포함하여 구성되되,

상기 UICC는, 상기 초기화 단말기 착신 메시지를 전송받은 경우 상기 초기화 단말기 착신 메시지로부터 상기 초기화 명령어를 추출하고, 상기 초기화 명령어에 따라 상기 UICC에 저장된 상기 개인 정보를 초기화시키는 초기화 카드 애플리케이션 툴킷(Card Application Toolkit : CAT)을 포함하는 것을 특징으로 하는 UICC의 개인 정보 보호 시스템.

청구항 4

제 2 항 또는 제 3 항에 있어서, 상기 초기화 단말기 착신 메시지는,

Command Packet Identifier(CPI) 필드, Command Packet Length(CPL) 필드, Command Header Identifier(CHI) 필드, Command Header Length(CHL) 필드, Security Parameter Indicator(SPI) 필드, Ciphering Key Identifier(KIC) 필드, Key Identifier(KID) 필드, Toolkit Application Reference(TAR) 필드, Counter(CNTR) 필드, Padding counter(PCNTR) 필드 및 Secured Data 필드와 Redundancy Check(RC) 필드, Cryptographic Checksum(CC) 필드 또는 Digital Signature(DS) 필드 중 어느 하나로 구성되는 단문 메시지이고,

상기 Toolkit Application Reference(TAR) 필드에서 상기 초기화 카드 애플리케이션 툴킷을 지정하고,

상기 Secure Data 필드가 상기 초기화 카드 애플리케이션 툴킷을 실행시키는 실행 명령어를 포함하는 것을 특징으로 하는 UICC의 개인 정보 보호 시스템.

청구항 5

제 1 항 내지 제 3 항 중 어느 한 항에 있어서, 상기 개인 정보는,

주소록, 통화정보, SMS, MMS, 사진 또는 개인 일정 중 적어도 어느 하나인 것을 특징으로 하는 UICC의 개인 정보 보호 시스템.

청구항 6

제 5 항에 있어서, 상기 초기화 단말기 착신 메시지는,

상기 개인 정보 중에서 초기화할 카테고리에 대한 데이터를 더 포함하는 것을 특징으로 하는 UICC의 개인 정보 보호 시스템.

청구항 7

제 3 항에 있어서,

상기 UICC는, 상기 UICC에 저장된 상기 개인 정보를 초기화시키기 전에 상기 개인 정보를 전송하는 개인 정보 전송모듈을 더 포함하고,

상기 개인 정보 보호 시스템은, 통신망을 통해 전송된 상기 개인 정보를 수신하여 백업시키는 백업 서버;를 더 포함하여 구성되는 것을 특징으로 하는 UICC의 개인 정보 보호 시스템.

청구항 8

제 7 항에 있어서, 상기 백업 서버는,

사용자의 요청이 있는 경우 상기 백업 서버에 백업된 상기 개인 정보를 상기 UICC 또는 상기 UICC가 아닌 타 UICC에 전송하여 주는 개인정보 복구모듈을 더 포함하는 것을 특징으로 하는 UICC의 개인 정보 보호 시스템.

청구항 9

제 3 항에 있어서, 상기 UICC는,

상기 초기화 카드 애플리케이션 툴킷을 실행시켜 상기 UICC를 초기화한 후에, 상기 개인정보 초기화 요청에 따른 실행결과를 상기 초기화 관리 서버로 전송하는 실행결과 전송모듈을 더 포함하는 것을 특징으로 하는 UICC의 개인 정보 보호 시스템.

청구항 10

제 2 항 또는 제 3 항에 있어서, 상기 휴대 단말기는,

상기 초기화 카드 애플리케이션 툴킷이 실행된 후에, 상기 개인 정보가 초기화되어 상기 UICC에 저장된 상기 개인 정보가 없다는 메시지를 디스플레이하는 디스플레이모듈을 더 포함하는 것을 특징으로 하는 UICC의 개인 정보 보호 시스템.

청구항 11

초기화 관리 서버, 단문 메시지 센터(SMSC : Short Message Service Center), 휴대 단말기 및 상기 휴대 단말기에 장착되는 특정 UICC(Universal IC Card)를 포함하여 구성되는 UICC의 개인 정보 보호 방법에 있어서,

상기 초기화 관리 서버가 상기 UICC(Universal IC Card)의 개인정보 초기화 요청에 따라 상기 UICC에 저장된 개인 정보를 초기화하는 초기화 명령어가 포함되고 상기 UICC에 할당된 전화번호를 수신번호로 하는 초기화 단말기 착신 메시지를 생성하는 제 1 단계;

상기 초기화 관리 서버가 상기 초기화 단말기 착신 메시지를 상기 단문 메시지 센터로 송신하는 제 2 단계;

상기 단문 메시지 센터가 상기 초기화 단말기 착신 메시지를 수신하여 상기 휴대 단말기로 송신하는 제 3 단계;

상기 휴대 단말기가 상기 초기화 단말기 착신 메시지를 상기 UICC로 전송하는 제 4 단계; 및

상기 UICC가 상기 초기화 단말기 착신 메시지를 수신하고 상기 UICC에 저장된 초기화 카드 애플리케이션 툴킷

(Card Application Toolkit : CAT)을 실행시켜 상기 UICC에 저장된 상기 개인 정보를 초기화시키는 제 5 단계;를 수행하는 것을 특징으로 하는 UICC의 개인 정보 보호 방법.

청구항 12

제 11 항에 있어서, 상기 초기화 단말기 착신 메시지는,

Command Packet Identifier(CPI) 필드, Command Packet Length(CPL) 필드, Command Header Identifier(CHI) 필드, Command Header Length(CHL) 필드, Security Parameter Indicator(SPI) 필드, Ciphering Key Identifier(KIC) 필드, Key Identifier(KID) 필드, Toolkit Application Reference(TAR) 필드, Counter(CNTR) 필드, Padding counter(PCNTR) 필드 및 Secured Data 필드와 Redundancy Check(RC) 필드, Cryptographic Checksum(CC) 필드 또는 Digital Signature(DS) 필드 중 어느 하나로 구성되는 단문 메시지이고,

상기 Toolkit Application Reference(TAR) 필드에서 상기 초기화 카드 애플리케이션 툴킷을 지정하고,

상기 Secure Data 필드가 상기 초기화 카드 애플리케이션 툴킷을 실행시키는 실행 명령어를 포함하는 것을 특징으로 하는 UICC의 개인 정보 보호 방법.

청구항 13

제 11 항에 있어서, 상기 제 5 단계는,

상기 UICC가 상기 초기화 카드 애플리케이션 툴킷을 실행시키기 전에 상기 UICC에 저장된 상기 개인 정보를 백업 서버로 전송하는 제 1 부단계; 및

상기 백업 서버가 상기 개인 정보를 백업시켜 저장하는 제 2 부단계;를 더 수행하는 것을 특징으로 하는 UICC의 개인 정보 보호 방법.

청구항 14

제 11 항에 있어서, 상기 제 5 단계 이후에,

상기 UICC가 상기 개인정보 초기화 요청에 따른 실행 결과를 상기 초기화 관리 서버로 전송하는 제 6 단계;를 더 수행하는 것을 특징으로 하는 UICC의 개인 정보 보호 방법.

청구항 15

제 13 항에 있어서, 상기 제 5 단계 이후에,

상기 백업 서버는 사용자의 요청이 있는 경우 상기 백업 서버에 저장된 상기 개인 정보를 상기 UICC 또는 상기 UICC가 아닌 타 UICC에 전송하는 제 3 부단계;를 더 수행하는 것을 특징으로 하는 UICC의 개인 정보 보호 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 UICC의 개인 정보 보호 시스템 및 방법에 관한 것으로, 특히 개인정보 초기화 요청에 따라 UICC에 저장된 개인 정보를 초기화함으로써, UICC에 저장된 개인 정보를 보호할 수 있는 UICC의 개인 정보 보호 시스템 및 방법에 관한 것이다.

배 경 기 술

<2> 휴대 단말기를 분실할 경우, 사용자는 이동 통신사에 분실 신고를 하여 통화기능을 정지시킬 수 있다. 그러나 통화기능을 정지시킨 후에도 휴대 단말기 습득자는 휴대 단말기에 저장된 개인 정보를 열람할 수 있어, 휴대 단말기 사용자의 개인 정보가 노출될 위험이 있다. 특히 최근에는 휴대 단말기가 다양한 기능을 수행하면서 사진 앨범과 같은 프라이버시를 침해할 위험뿐만 아니라 뱅킹 서비스 등과 같은 금융 정보까지 습득자에게 노출되어 휴대 단말기를 분실할 경우 사용자에게 막대한 피해를 끼칠 수 있는 문제가 있다.

<3> 이러한 문제를 해결하기 위해 USIM 카드, SIM 카드, RUIM 카드 또는 UIM 카드 등의 UICC(Universal IC Card)

사용시 PIN(Personal Identification Number)을 사용할 수 있다. 사용자는 PIN을 입력하여 UICC의 인증을 거친 후에 휴대 단말기 및 UICC를 사용할 수 있다. 그러나 PIN 인증 방식은 번거롭고 전자 기기의 조작이 쉽지 않은 사용자들은 PIN을 설정하지 않거나, PIN을 설정하더라도 연속된 숫자 또는 타인이 쉽게 알 수 있는 특정번호로 설정하여 UICC에 저장된 개인 정보가 타인에게 노출될 위험이 여전히 존재한다.

발명의 내용

해결 하고자하는 과제

<4> 본 발명은 상기의 문제를 해결하기 위한 것으로, 개인정보 초기화 요청이 있는 경우 초기화 관리 서버가 UICC에 저장된 개인 정보를 초기화하는 초기화 명령어가 포함된 초기화 단말기 착신 메시지를 생성함으로써, 이를 수신한 초기화 카드 애플리케이션 툴킷이 UICC에 저장된 개인 정보를 초기화할 수 있는 UICC의 개인 정보 보호 시스템 및 방법을 제공하는 것을 목적으로 한다.

<5> 본 발명의 실시예에 따르면, 초기화 단말기 착신 메시지를 수신한 경우 초기화 카드 애플리케이션 툴킷이 상기 초기화 단말기 착신 메시지로부터 UICC에 저장된 개인 정보를 초기화하는 초기화 명령어를 추출하여 실행함으로써, 사용자가 휴대 단말기를 분실한 경우에 UICC에 저장된 개인 정보를 초기화하여 개인 정보가 제 3 자에게 노출되지 않도록 보호할 수 있는 UICC의 개인 정보 보호 시스템 및 방법을 제공하는 것을 목적으로 한다.

<6> 마지막으로, 본 발명의 다른 실시예에 따르면, UICC를 초기화하기 전에 초기화할 개인 정보를 통신망을 통해 수신하여 저장하고 사용자의 요청이 있는 경우 저장한 개인 정보를 전송하는 백업 서버를 더 포함함으로써, UICC에 저장된 개인 정보를 사용자가 원하는 경우 다시 얻을 수 있는 UICC의 개인 정보 보호 시스템 및 방법을 제공하는 것을 다른 목적으로 한다.

과제 해결수단

<7> 상기의 목적을 달성하기 위해 본 발명의 실시예에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 특정 UICC(Universal IC Card)의 개인정보 초기화 요청에 따라 상기 UICC에 저장된 개인 정보를 초기화하는 초기화 명령어가 포함되고 상기 UICC에 할당된 전화번호를 수신번호로 하는 초기화 단말기 착신 메시지(Initializing_SMS Deliver Message)를 생성하는 초기화 관리 서버; 및 상기 초기화 관리 서버로부터 전송된 상기 초기화 단말기 착신 메시지를 상기 UICC에 할당된 전화번호로 전송하는 단문 메시지 센터(SMSC : Short Message Service Center);를 포함하여 구성되는 것을 특징으로 한다.

<8> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 단문 메시지(Short Message Service)를 수신하는 휴대 단말기; 및 상기 휴대 단말기에 장착되고 사용자의 개인 정보를 저장하는 UICC(Universal IC Card);를 포함하여 구성되되, 상기 휴대 단말기는, 개인정보 초기화 요청에 따라 상기 UICC에 저장된 상기 개인정보를 초기화하는 초기화 명령어를 포함하는 초기화 단말기 착신 메시지(Initializing_SMS Deliver Message)를 수신한 경우, 상기 초기화 단말기 착신 메시지를 상기 UICC로 전송하는 UICC 메시지 전송모듈을 포함하고, 상기 UICC는, 상기 초기화 단말기 착신 메시지를 전송받은 경우 상기 초기화 단말기 착신 메시지로부터 상기 초기화 명령어를 추출하고, 상기 초기화 명령어에 따라 상기 UICC에 저장된 상기 개인 정보를 초기화시키는 초기화 카드 애플리케이션 툴킷(Card Application Toolkit : CAT)을 포함하는 것을 특징으로 한다.

<9> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 개인정보 초기화 요청에 따라 특정 UICC(Universal IC Card)에 저장된 개인 정보를 초기화하는 초기화 명령어가 포함되고 상기 UICC에 할당된 전화번호를 수신번호로 하는 초기화 단말기 착신 메시지(Initializing_SMS Deliver Message)를 생성하는 초기화 관리 서버; 상기 초기화 관리 서버로부터 전송된 상기 초기화 단말기 착신 메시지를 상기 UICC에 할당된 전화번호로 전송하는 단문 메시지 센터(SMSC : Short Message Service Center); 상기 초기화 단말기 착신 메시지를 수신하는 휴대 단말기; 및 상기 휴대 단말기에 장착되어 상기 초기화 단말기 착신 메시지를 전송받는 상기 UICC;를 포함하여 구성되되, 상기 UICC는, 상기 초기화 단말기 착신 메시지를 전송받은 경우 상기 초기화 단말기 착신 메시지로부터 상기 초기화 명령어를 추출하고, 상기 초기화 명령어에 따라 상기 UICC에 저장된 상기 개인 정보를 초기화시키는 초기화 카드 애플리케이션 툴킷(Card Application Toolkit : CAT)을 포함하는 것을 특징으로 한다.

<10> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 상기 초기화 단말기 착신 메시지가 Command Packet Identifier(CPI) 필드, Command Packet Length(CPL) 필드, Command Header Identifier(CHI) 필드, Command Header Length(CHL) 필드, Security Parameter Indicator(SPI) 필드, Ciphering Key

Identifier(KIC) 필드, Key Identifier(KID) 필드, Toolkit Application Reference(TAR) 필드, Counter(CNTR) 필드, Padding counter(PCNTR) 필드 및 Secured Data 필드와 Redundancy Check(RC) 필드, Cryptographic Checksum(CC) 필드 또는 Digital Signature(DS) 필드 중 어느 하나로 구성되는 단문 메시지이고, 상기 Toolkit Application Reference(TAR) 필드에서 상기 초기화 카드 애플리케이션 툴킷을 지정하고, 상기 Secure Data 필드가 상기 초기화 카드 애플리케이션 툴킷을 실행시키는 실행 명령어를 포함하는 것을 특징으로 한다.

<11> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 상기 개인 정보가 주소록, 통화정보, SMS, MMS, 사진 또는 개인 일정 중 적어도 어느 하나인 것을 특징으로 한다.

<12> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 상기 초기화 단말기 착신 메시지가 상기 개인 정보 중에서 초기화할 카테고리에 대한 데이터를 더 포함하는 것을 특징으로 한다.

<13> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 상기 UICC가 상기 UICC에 저장된 상기 개인 정보를 초기화시키기 전에 상기 개인 정보를 전송하는 개인 정보 전송모듈을 더 포함하고, 상기 개인 정보 보호 시스템이 통신망을 통해 전송된 상기 개인 정보를 수신하여 백업시키는 백업 서버;를 더 포함하여 구성되는 것을 특징으로 한다.

<14> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 상기 백업 서버가 사용자의 요청이 있는 경우 상기 백업 서버에 백업된 상기 개인 정보를 상기 UICC 또는 상기 UICC가 아닌 타 UICC에 전송하여 주는 개인정보 복구모듈을 더 포함하는 것을 특징으로 한다.

<15> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 상기 UICC가 상기 초기화 카드 애플리케이션 툴킷을 실행시켜 상기 UICC를 초기화한 후에, 상기 개인정보 초기화 요청에 따른 실행결과를 상기 초기화 관리 서버로 전송하는 실행결과 전송모듈을 더 포함하는 것을 특징으로 한다.

<16> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 상기 휴대 단말기가 상기 초기화 카드 애플리케이션 툴킷이 실행된 후에, 상기 개인 정보가 초기화되어 상기 UICC에 저장된 상기 개인 정보가 없다는 메시지를 디스플레이하는 디스플레이모듈을 더 포함하는 것을 특징으로 한다.

<17> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 방법은, 초기화 관리 서버, 단문 메시지 센터(SMSC : Short Message Service Center), 휴대 단말기 및 상기 휴대 단말기에 장착되는 특정 UICC(Universal IC Card)를 포함하여 구성되는 UICC의 개인 정보 보호 방법에 있어서, 상기 초기화 관리 서버가 상기 UICC(Universal IC Card)의 개인정보 초기화 요청에 따라 상기 UICC에 저장된 개인 정보를 초기화하는 초기화 명령어가 포함되고 상기 UICC에 할당된 전화번호를 수신번호로 하는 초기화 단말기 착신 메시지를 생성하는 제 1 단계; 상기 초기화 관리 서버가 상기 초기화 단말기 착신 메시지를 상기 단문 메시지 센터로 송신하는 제 2 단계; 상기 단문 메시지 센터가 상기 초기화 단말기 착신 메시지를 수신하여 상기 휴대 단말기로 송신하는 제 3 단계; 상기 휴대 단말기가 상기 초기화 단말기 착신 메시지를 상기 UICC로 전송하는 제 4 단계; 및 상기 UICC가 상기 초기화 단말기 착신 메시지를 수신하고 상기 UICC에 저장된 초기화 카드 애플리케이션 툴킷(Card Application Toolkit : CAT)을 실행시켜 상기 UICC에 저장된 상기 개인 정보를 초기화시키는 제 5 단계;를 수행하는 것을 특징으로 한다.

<18> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 방법은, 제 5 단계가 상기 UICC가 상기 초기화 카드 애플리케이션 툴킷을 실행시키기 전에 상기 UICC에 저장된 상기 개인 정보를 백업 서버로 전송하는 제 1 부단계; 및 상기 백업 서버가 상기 개인 정보를 백업시켜 저장하는 제 2 부단계;를 더 수행하는 것을 특징으로 한다.

<19> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 방법은, 상기 제 5 단계 이후에, 상기 UICC가 상기 개인 정보 초기화 요청에 따른 실행 결과를 상기 초기화 관리 서버로 전송하는 제 6 단계;를 더 수행하는 것을 특징으로 한다.

<20> 본 발명의 다른 실시예에 따른 UICC의 개인 정보 보호 방법은, 상기 제 5 단계 이후에, 상기 백업 서버는 사용자의 요청이 있는 경우 상기 백업 서버에 저장된 상기 개인 정보를 상기 UICC 또는 상기 UICC가 아닌 타 UICC에 전송하는 제 3 부단계;를 더 수행하는 것을 특징으로 한다.

효 과

<21> 본 발명에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 개인정보 초기화 요청이 있는 경우 초기화 관리 서버가 UICC에 저장된 개인 정보를 초기화하는 초기화 명령어가 포함된 초기화 단말기 착신 메시지를 생성함으로써,

이를 수신한 초기화 카드 애플리케이션 툴킷이 UICC에 저장된 개인 정보를 초기화할 수 있는 효과를 제공한다.

<22> 본 발명에 따른 UICC의 개인 정보 보호 시스템 및 방법은, 초기화 단말기 착신 메시지를 수신한 경우 초기화 카드 애플리케이션 툴킷이 상기 초기화 단말기 착신 메시지로부터 UICC에 저장된 개인 정보를 초기화하는 초기화 명령어를 추출하여 실행함으로써, 사용자가 휴대 단말기를 분실한 경우에 UICC에 저장된 개인 정보를 초기화하여 개인 정보가 제 3 자에게 노출되지 않도록 보호할 수 있는 효과를 제공한다.

<23> 마지막으로, 본 발명에 따른 UICC의 개인 정보 보호 시스템 및 방법은, UICC를 초기화하기 전에 초기화할 개인 정보를 통신망을 통해 수신하여 저장하고 사용자의 요청이 있는 경우 저장한 개인 정보를 전송하는 백업 서버를 더 포함함으로써, UICC에 저장된 개인 정보를 사용자가 원하는 경우 다시 얻을 수 있는 효과를 제공한다.

발명의 실시를 위한 구체적인 내용

<24> 첨부한 도면을 참조하여 본 발명의 실시예를 상세히 설명하면 다음과 같다.

<25> 도 1에 도시된 바와 같이, 본 발명의 실시예에 따른 UICC의 개인 정보 보호 시스템은 초기화 관리 서버(100), 단문 메시지 센터(200), UICC(400)를 장착하는 휴대 단말기(300)를 포함하여 구성될 수 있다.

<26> 초기화 관리 서버(100)는 개인정보 초기화 요청이 있는 경우 초기화 단말기 착신 메시지(Initializing_SMS Deliver Message)를 생성하여 단문 메시지 센터(200)로 전송하는 기능을 수행한다. 초기화 관리 서버는 이동통신사 고객 서비스 센터와 연결되어 운영될 수 있으며, 이 경우는 사용자가 휴대 단말기 분실신고를 한 경우 자동으로 초기화 단말기 착신 메시지를 생성하여 전송할 수 있다. 별개의 서버로 운영될 수도 있다. 또한, 이동통신사 고객 서비스 센터와 별개의 서버로 운영될 수도 있는데, 이 경우 휴대 단말기 분실신고와는 별 사용자로부터 개인정보 초기화 요청이 있는 때에 초기화 단말기 착신 메시지를 생성하여 단문 메시지 센터로 전송할 수 있다.

<27> 초기화 단말기 착신 메시지는 특정 UICC(Universal IC Card)에 저장된 개인 정보를 초기화하는 초기화 명령어를 포함하고, UICC에 할당된 전화번호를 수신번호로 하는 메시지이다.

<28> 초기화 단말기 착신 메시지는 도 3에 도시된 바와 같이, Command Packet Identifier(CPI) 필드, Command Packet Length(CPL) 필드, Command Header Identifier(CHI) 필드, Command Header Length(CHL) 필드, Security Parameter Indicator(SPI) 필드, Ciphering Key Identifier(KIC) 필드, Key Identifier(KID) 필드, Toolkit Application Reference(TAR) 필드, Counter(CNTR) 필드, Padding counter(PCNTR) 필드 및 Secured Data 필드와 Redundancy Check(RC) 필드, Cryptographic Checksum(CC) 필드 또는 Digital Signature(DS) 필드 중 어느 하나로 구성되는 단문 메시지이다. 특히, Toolkit Application Reference(TAR) 필드에서는 실행할 초기화 카드 애플리케이션 툴킷(410)을 지정한다. 또한 Secure Data 필드는 초기화 카드 애플리케이션 툴킷(410)을 실행시키는 실행 명령어를 포함한다.

<29> UICC(400)에서 삭제하여 초기화할 개인 정보는 주소록, 통화정보, SMS, MMS, 사진 또는 개인 일정 중 적어도 어느 하나일 수 있고, 이때 초기화 단말기 착신 메시지는 상기 개인 정보 중에서 초기화할 카테고리에 대한 데이터를 더 포함할 수 있다. 예를 들면, 사용자가 개인 정보 중에서 SMS 및 MMS에 대한 데이터만을 삭제하도록 설정할 수 있고, 이 경우 초기화 단말기 착신 메시지는 이에 대한 데이터를 포함하고 초기화 카드 애플리케이션 툴킷은 SMS 및 MMS만을 UICC에서 삭제하여 초기화시킬 수 있다.

<30> 단문 메시지 센터(Short Message Service Center : SMSC)(200)는 초기화 관리 서버(100)로부터 전송된 초기화 단말기 착신 메시지를 UICC(400)에 할당된 전화번호로 전송하는 기능을 수행한다.

<31> 단문 메시지 센터(SMSC)는 일반적으로 Store and Forward Message Switch의 기능을 수행한다. 즉 휴대 단말기(Mobile Station : MS)와 휴대 단말기 간 또는 휴대 단말기와 SME(Short Message Entity)들 사이에 한정된 크기의 문자 형태로 전달하는 통신서비스로서 임의의 순간에 수신할 수 없는 착신 가입자에게 전송되는 단문을 그 가입자가 수신할 수 있을 때까지 저장(Store)하였다가 전달(Forward)하여 주고 통화중인 착신 가입자에게도 전달하여 주는 기능을 하는 시스템이다. 본원발명에서 단문 메시지 센터(200)는 통상적인 SMSC를 의미한다.

<32> 휴대 단말기(300)는 단문 메시지(Short Message Service)를 수신할 수 있는데, 특히 초기화 단말기 착신 메시지를 수신하는 기능을 수행한다.

<33> 도 2에 도시된 바와 같이, 휴대 단말기(300)는 UICC 메시지 전송모듈(310)을 더 포함하여 구성될 수 있다. UICC

메시지 전송모듈(310)은 초기화 단말기 착신 메시지(Initializing_SMS Deliver Message)를 수신한 경우, 초기화 단말기 착신 메시지를 UICC(400)로 전송하는 기능을 수행한다. 보다 구체적으로는 UICC(400)의 초기화 카드 애플리케이션 툴킷(410)으로 직접 전송한다.

<34> 한편, 보다 바람직하게 휴대 단말기(300)는 디스플레이모듈을 더 포함하여 구성될 수 있다. 디스플레이모듈은 초기화 카드 애플리케이션 툴킷(410)이 실행된 후에, 개인 정보가 초기화되어 UICC(400)에 저장된 개인 정보가 없다는 메시지를 디스플레이하는 기능을 수행한다. 도 4에 도시된 바와 같이, 초기화 카드 애플리케이션 툴킷(410)이 실행되어 개인 정보가 삭제되어 초기화된 후 습득자가 주소록을 열람하고자 할 경우, 예를 들면 "해당 주소록이 비어 있습니다"와 같이 UICC(400)에 저장된 개인 정보가 없다는 메시지를 디스플레이할 수 있다.

<35> UICC(400)는 사용자의 개인 정보를 저장하고, 휴대 단말기(300)에 장착되어 초기화 단말기 착신 메시지를 전송받는 기능을 수행한다.

<36> UICC(400)는 'Universal IC Card' 의 약자로 휴대 인터넷의 안전한 네트워크 접속을 위한 가입자 인증 및 다양한 통신 및 금융 부가서비스를 제공하는 다기능 스마트카드로써 휴대 단말기에 장착된다. UICC(400)는 예를 들면, USIM 카드, SIM 카드, RUIM 카드 또는 UIM 카드가 있을 수 있다.

<37> UICC(400)는 초기화 카드 애플리케이션 툴킷(Card Application Toolkit : CAT)(410)을 포함한다.

<38> 카드 애플리케이션 툴킷(Card Application Toolkit : CAT)은 UICC에서 동작하는 애플릿으로, 예를 들면 SAT(SIM Application Toolkit), USAT(USIM Application Toolkit), UTK(UIM ToolKit) 애플릿 등을 말한다.

<39> 초기화 카드 애플리케이션 툴킷(410)은 휴대 단말기(300)로부터 초기화 단말기 착신 메시지를 전송받은 경우 초기화 단말기 착신 메시지로부터 초기화 명령어를 추출하고, 초기화 명령어에 따라 UICC(400)에 저장된 개인 정보를 초기화시키는 기능을 수행한다.

<40> 본 발명의 실시예에 따른 초기화 카드 애플리케이션 툴킷(410)은 초기화 단말기 착신 메시지를 수신한 경우 초기화 단말기 착신 메시지로부터 UICC(400)에 저장된 개인 정보를 초기화하는 초기화 명령어를 추출하여 실행함으로써, 사용자가 휴대 단말기를 분실한 경우에 UICC에 저장된 개인 정보를 초기화하여 개인 정보가 제 3 자에게 노출되지 않도록 보호할 수 있는 효과를 제공한다.

<41> 또한, UICC(400)는 실행결과 전송모듈을 더 포함하여 구성될 수 있다. 실행결과 전송모듈은 초기화 카드 애플리케이션 툴킷(410)을 실행시켜 UICC(400)를 초기화한 후에, 개인정보 초기화 요청에 따른 실행결과를 초기화 관리 서버(100)로 전송하는 기능을 수행한다.

<42> 한편 보다 바람직하게, 개인 정보 보호 시스템은 백업 서버(500)를 더 포함하여 구성될 수 있다. 백업 서버(500)는 통신망을 통해 전송된 개인 정보를 수신하여 백업하는 기능을 수행한다.

<43> 이때, UICC(400)는 UICC(400)에 저장된 개인 정보를 초기화시키기 전에 통신망을 통해 개인 정보를 백업 서버(500)로 전송하는 개인 정보 전송모듈(430)을 더 포함하여 구성될 수 있고, 백업 서버(500)는 개인정보 복구모듈(430)을 더 포함하여 구성될 수 있다. 개인정보 복구모듈(430)은 사용자의 요청이 있는 경우 백업 서버(500)에 백업 된 개인 정보를 UICC 또는 분실한 UICC가 아닌 타 UICC에 전송하여 주는 기능을 수행한다.

<44> 이러한 실시예에 따르면, UICC를 초기화하기 전에 초기화할 개인 정보를 통신망을 통해 수신하여 저장하고 사용자의 요청이 있는 경우 저장한 개인 정보를 전송함으로써 UICC에 저장된 개인 정보를 사용자가 원하는 경우 다시 얻을 수 있는 효과를 제공한다. 즉, 휴대 단말기 사용자는 휴대 단말기 또는 휴대 단말기에 장착된 UICC에 전화번호, 기념일 또는 계획 등과 같은 여러 가지 개인 정보를 저장하고, 이러한 개인 정보에 대해 별도로 저장하여 두지는 않는 것이 일반적이므로 UICC를 분실하면 사용자는 상기와 같은 개인 정보를 사용할 수 없게 된다. 이와 같은 경우 본 발명에 따라 UICC의 개인 정보를 초기화시키면 UICC를 습득한 자에 대해서는 사용자의 개인 정보가 노출되지 않는다는 장점이 있으나, UICC에 저장된 개인 정보가 모두 삭제되어 사용자가 UICC를 다시 찾거나 또는 다른 매체를 이용하여 UICC에 저장된 개인 정보를 복원할 방법이 없게 된다. 따라서 UICC에 저장된 개인 정보를 초기화시키기 전에 이를 백업 서버(500)에 백업시키고, 후에 사용자 인증 등의 인증 방법을 거쳐 사용자가 원하는 경우 백업시킨 개인 정보를 사용자가 사용할 수 있게 하는 것이 보다 바람직하다.

<45> 도 5는 본 발명의 실시예에 따른 UICC의 개인 정보 보호 방법을 도시한다.

<46> 먼저 초기화 관리 서버(100)가 UICC(Universal IC Card)의 개인정보 초기화 요청에 따라 초기화 단말기 착신 메시지를 생성하는 제 1 단계(S10)를 수행한다. 초기화 단말기 착신 메시지는 UICC(400)에 저장된 개인 정보를 초

기화하는 초기화 명령어가 포함되고 UICC(400)에 할당된 전화번호를 수신번호로 하는 메시지이다. 초기화 단말기 착신 메시지는 도 3에 도시된 바와 같이, Command Packet Identifier(CPI) 필드, Command Packet Length(CPL) 필드, Command Header Identifier(CHI) 필드, Command Header Length(CHL) 필드, Security Parameter Indicator(SPI) 필드, Ciphering Key Identifier(KIC) 필드, Key Identifier(KID) 필드, Toolkit Application Reference(TAR) 필드, Counter(CNTR) 필드, Padding counter(PCNTR) 필드 및 Secured Data 필드와 Redundancy Check(RC) 필드, Cryptographic Checksum(CC) 필드 또는 Digital Signature(DS) 필드 중 어느 하나로 구성되는 단문 메시지이다. 특히, Toolkit Application Reference(TAR) 필드에서는 실행할 초기화 카드 애플리케이션 툴킷(410)을 지정한다. 또한 Secure Data 필드는 초기화 카드 애플리케이션 툴킷(410)을 실행시키는 실행 명령어를 포함한다.

<47> 다음으로, 초기화 관리 서버(100)가 초기화 단말기 착신 메시지를 단문 메시지 센터(SMSC : Short Message Service Center)(200)로 송신하는 제 2 단계(S20)를 수행한다.

<48> 다음으로, 단문 메시지 센터(200)가 초기화 단말기 착신 메시지를 수신하여 휴대 단말기(300)로 송신하는 제 3 단계(S30)를 수행한다.

<49> 단문 메시지 센터(200)는 초기화 단말기 착신 메시지를 UICC(400)에 할당된 전화번호로 전송한다.

<50> 다음으로, 휴대 단말기(300)가 단문 메시지 센터(200)로부터 수신한 초기화 단말기 착신 메시지를 UICC(400)로 전송하는 제 4 단계(S40)를 수행한다.

<51> 다음으로, UICC(400)가 초기화 단말기 착신 메시지를 수신하고 UICC(400)에 저장된 초기화 카드 애플리케이션 툴킷(Card Application Toolkit : CAT)(410)을 실행시켜 UICC(400)에 저장된 상기 개인 정보를 초기화시키는 제 5 단계(S50)를 수행한다.

<52> 보다 바람직하게, 제 5 단계(S50)는 UICC(400)가 초기화 카드 애플리케이션 툴킷(410)을 실행시키기 전에 UICC(400)에 저장된 개인 정보를 백업 서버(500)로 전송하는 제 1 부단계 및 백업 서버(500)가 개인 정보를 백업시켜 저장하는 제 2 부단계를 더 수행할 수 있다.

<53> 제 5 단계(S50) 이후에 백업 서버(500)는 사용자의 요청이 있는 경우 백업 서버(500)에 저장된 개인 정보를 UICC(400) 또는 개인 정보가 저장되었던 UICC가 아닌 타 UICC에 전송하는 제 3 부단계를 더 수행할 수 있다.

<54> 이러한 실시예에 따르면, UICC를 초기화하기 전에 초기화할 개인 정보를 통신망을 통해 수신하여 저장하고 사용자의 요청이 있는 경우 저장한 개인 정보를 전송함으로써 UICC에 저장된 개인 정보를 사용자가 원하는 경우 다시 얻을 수 있는 효과를 제공한다.

<55> 마지막으로, 제 5 단계(S50) 이후에 UICC(400)가 개인정보 초기화 요청에 따른 실행 결과를 초기화 관리 서버(100)로 전송하는 제 6 단계(S60)를 더 수행할 수 있다.

<56> 아울러 본 발명의 바람직한 실시예들은 예시의 목적을 위해 개시된 것이며, 당업자라면 본 발명의 사상과 범위 안에서 다양한 수정, 변경, 부가 등이 가능할 것이며, 이러한 수정, 변경 등은 이하의 특허청구의 범위에 속하는 것으로 보아야 할 것이다.

도면의 간단한 설명

<57> 도 1은 본 발명의 실시예에 따른 UICC의 개인 정보 보호 시스템을 도시하는 전체 구성도.

<58> 도 2는 본 발명의 실시예에 따른 휴대 단말기 및 UICC를 도시하는 상세 구성도.

<59> 도 3은 본 발명의 실시예에 따른 초기화 단말기 착신 메시지를 도시하는 구성도.

<60> 도 4는 본 발명의 실시예에 따른 초기화 카드 애플리케이션 툴킷의 실행 전·후를 도시하는 예시도.

<61> 도 5는 본 발명의 실시예에 따른 UICC의 개인 정보 보호 방법을 도시하는 흐름도.

<62> < 도면의 주요부분에 대한 부호의 설명 >

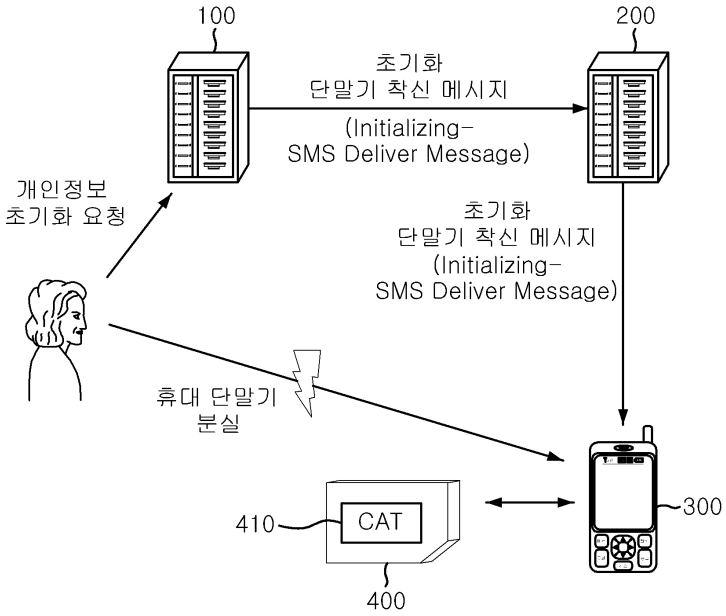
<63> 100 : 초기화 관리 서버 200 : 단문 메시지 센터(SMSC)

<64> 300 : 휴대 단말기 400 : UICC

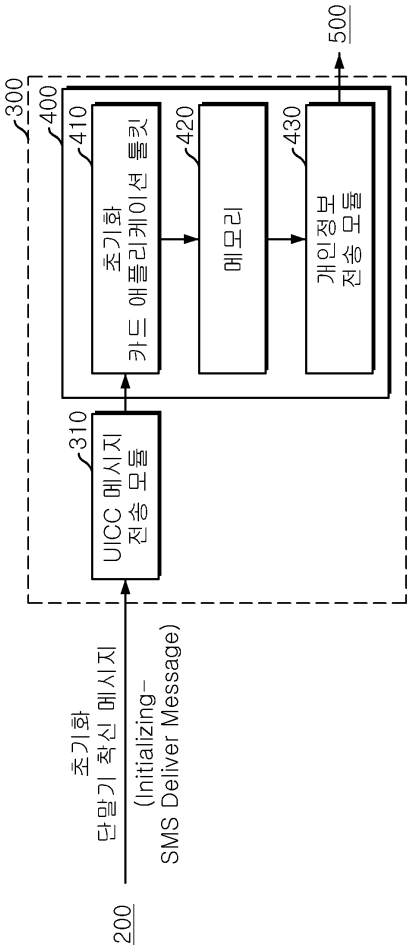
<65> 410 : 초기화 카드 애플리케이션 툴킷 500 : 백업 서버

도면

도면1


100
200
초기화
단말기 착신 메시지
(Initializing-
SMS Deliver Message)
개인정보
초기화 요청
초기화
단말기 착신 메시지
(Initializing-
SMS Deliver Message)
휴대 단말기
분실
410
CAT
400
300

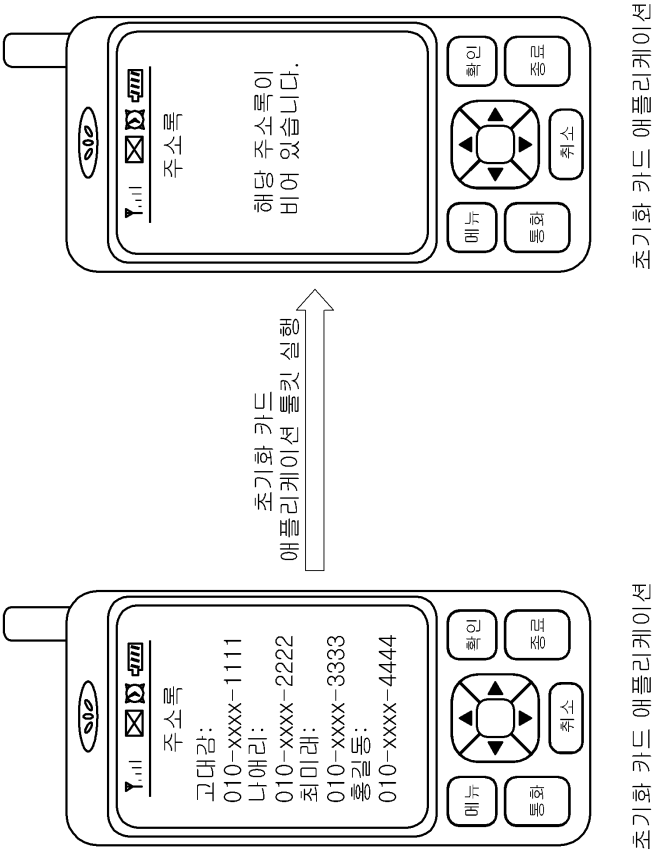
도면2


200
초기화
단말기 착신 메시지
(Initializing-
SMS Deliver Message)
300
310
UICC 메시지
전송 모듈
400
410
초기화
카드 애플리케이션 툴킷
420
메모리
430
개인정보
전송 모듈
500

도면3

Element	Length	Description
Command Packet Identifier (CPI)	1 octet	Identifies that this data block is the secured Command Packet.
Command Packet Length (CPL)	variable	This shall indicate the number of octets from and including the Command Header Identifier to the end of the Secured Data, including any padding octets required for ciphering.
Command Header Identifier (CHI)	1 octet	Identifies the Command Header.
Command Header Length (CHL)	variable	This shall indicate the number of octets from and including the SPI to the end of the RC/CC/DS.
Security Parameter Indicator (SPI)	2 octets	see detailed coding in clause 5.1.1.
Ciphering Key Identifier (KIc)	1 octet	Key and algorithm Identifier for ciphering.
Key Identifier (KID)	1 octet	Key and algorithm Identifier for RC/CC/DS.
Toolkit Application Reference (TAR)	3 octets	Coding is application dependent. (초기화 카드 애플리케이션 툴킷 지정)
Counter (CNTR)	5 octets	Replay detection and Sequence Integrity counter.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for ciphering at the end of the secured data.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	variable	Length depends on the algorithm. A typical value is 8 octets if used, and for a DS could be 48 or more octets; the minimum should be 4 octets.
Secured Data	variable	Contains the Secured Application Message and possibly Padding octets used for ciphering 초기화 카드 애플리케이션 툴킷 실행 명령어

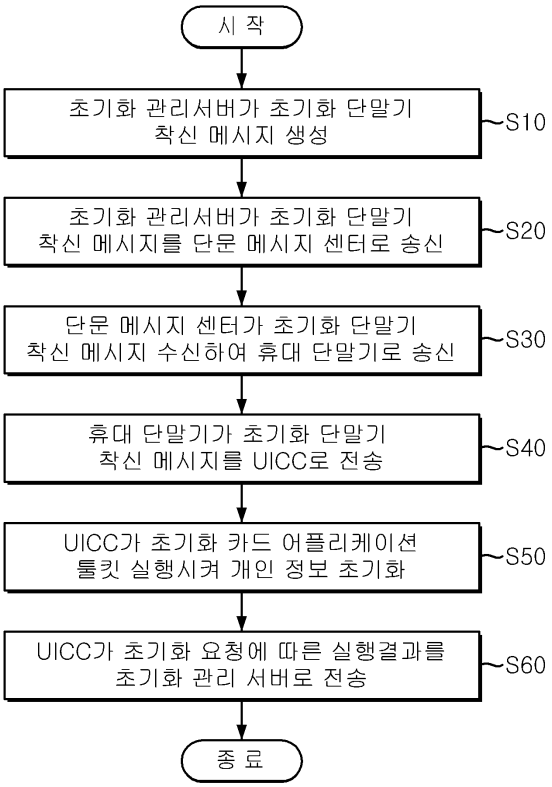
도면4



초기화 카드 애플리케이션 툴킷 실행 전

초기화 카드 애플리케이션 툴킷 실행 후

도면5


시 작
초기화 관리서버가 초기화 단말기 착신 메시지 생성
S10
초기화 관리서버가 초기화 단말기 착신 메시지를 단문 메시지 센터로 송신
S20
단문 메시지 센터가 초기화 단말기 착신 메시지 수신하여 휴대 단말기로 송신
S30
휴대 단말기가 초기화 단말기 착신 메시지를 UICC로 전송
S40
UICC가 초기화 카드 어플리케이션 툴킷 실행시켜 개인 정보 초기화
S50
UICC가 초기화 요청에 따른 실행결과를 초기화 관리 서버로 전송
S60
종 료