# 스마트 카드를 이용한 네트워크 가입자 신분 확인

이 장 원[†] · 홍 기 융[††] · 조 현 숙[†††]


## 요 약

본 논문은 스마트카드를 이용하여 네트워크 가입자들에 대해서 안전한 신분 확인을 하는 방법에 대해서 기술하였다. 네트워크 센터(Network Center)는 키 정보를 생성하며 네트워크 가입자들에게 생성된 키를 안전하게 분배하고 네트워크 가입자등에 대한 검증 기능을 수행함으로서 카드 분실로 인한 불법 도용을 방지할 수 있으며, 네트워크 가입자는 자신의 패스워드를 자유로이 변경할 수 있다. 이와 같은 방법을 이용하여 보다 안전성 있고 효율적으로 상호 신분 확인 및 인증을 할 수 있다.


# An Authentication Scheme for Network Users Using Smart Card

Jang-Won Lee[†] · Ki-Yoong Hong[††] · Hyun-Sook Cho[†††]


## ABSTRACT

In this paper, an authentication scheme for network users using smart card is proposed. The network center generates key information and distributes the generated key to the network users safely. It also carries out the verification of the network users to prevent in-proper use caused by stolen of cards. In addition to that the network users can change their password in anytime they want. Therefore, we provide more secure and efficient mutual authentication methods.


## 1. 서 론

정보화 시대로 접어든 현재 네트워크 가입자들이 증가함에 따라 불법으로 네트워크를 통한 시스템의 엑세스가 늘어나고 있다. 이를 방지하기 위한 연구 노력이 계속되고 있으며 좀 더 안전하고 효과적인 가입자의 신분 확인 방법이 필요 시 된다.

본 논문은 네트워크 서비스를 이용하는 많은 가입자들에 대한 안전한 신분 확인을 위한 것으로, 네트워크 가입자들은 스마트 카드를 발급 받아 네트워크의 서비스를 이용 할 수 있다. 네트워크 센터는 네트워크 가입자들에게 스마트 카드를 발급할 때 네트워크 가입자의 식별자(ID : Identifier) 정보를 근간으로 신분 확인/인증 과정에서 사용될 키 정보를 생성하여 네트워크 가입자에게 안전하게 전달한다. 그리고 키가 저장된 스마트 카드를 소유한 가입자가 네트워크 서비스를 이용하고자 할 때 자신의 스마트 카드를 동작시켜 네트워크 센터와의 검증 과정을 거쳐 신분 확인/인증을 받으며, 네트워크 가입자는 스마트 카드를 동작시킬 때 자신의 패스워드를 입력하여 검증된 후 사용할 수 있도록 함으로써 스마트 카드 분실로 인하여 불법적으로 도용될 수 있는 가능성을 배제 할 수 있다. 네트워크 가입자는 기존의 패스워드를 알고 있을 경우에만 자신의 패스워드를 자유로 변경할 수 있

† 정 회 원 : 한국전자통신연구소 연구원
†† 종신회원 : 한국전산원 선임연구원
††† 종신회원 : 한국전자통신연구소 선임연구원
논문접수 : 1995년 12월 6일, 심사완료 : 1996년 5월 15일

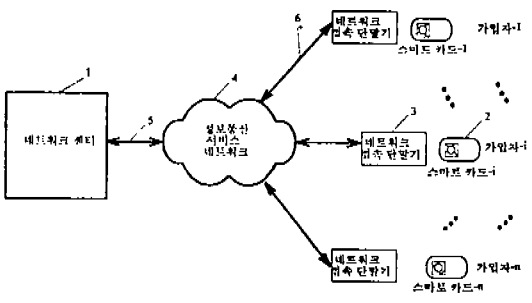
도록 하고, 또한 보다 높은 안전성을 위하여 상호 신분 확인/인증을 가능케 하는 방법에 대한 것이다.

본 논문에서 제시하고자 하는 방법은 네트워크 센터가 스마트 카드를 가지고 있는 네트워크 가입자를 안전하게 상호 신분 확인/인증이 가능하며, 네트워크 가입자는 자신의 패스워드를 안전한 방법으로 자유로 변경할 수 있으며, 네트워크상의 통신 링크에서 가입자의 패스워드가 누출될 위험이 없으며, 스마트 카드가 분실되었을 경우에도 불법 도용을 방지할 수 있다.

## 2. 목적 및 시스템 구성

### 2.1 목 적

네트워크 센터는 키와 패스워드를 생성하여 스마트 카드의 발급과 함께 네트워크 가입자에게 안전하게 제공 한다. 네트워크 가입자가 네트워크 서비스를 이용하고자 할 때 자신의 스마트 카드를 스마트 카드 판독기에 넣고 자신의 패스워드를 입력하여 자신의 인증 데이 타를 생성하여 네트워크 센터에게 전송 한다. 그리고, 네트워크 센터는 네트워크 가입자로부터 전송된 인증 데이타를 수신하여 센터와 가입자간의 상호 신분 확인/인증 과정을 통하여 정당한 가입자 및 센터인지 상호 확인한 후, 허가된 네트워크 가입자만이 안전하게 자신의 패스워드를 자유로 변경할 수 있도록 하는 기능을 제공 한다. 또한, 스마트 카드가 분실되었을 경우에도 불법 도용을 방지하는 기능을 제공할 수 있도록 하는 스마트 카드를 이용한 네트워크 가입자 신분 확인/인증 방법을 제공하는데 그 목적이 있다.




(그림 1) 하드웨어 시스템 구성
(Fig. 1) Configuration of hardware system

### 2.2 시스템 구성

(그림 1)에서와 같이 정보 통신 네트워크 서비스를 이용하기 위한 모든 가입자에 대한 비밀 정보와 각 가입자에 대한 신분 확인/인증을 수행하는 네트워크 센터(1), 각 가입자에게 발급된 스마트 카드(2), 각 가입자의 스마트 카드와 네트워크 센터 및 정보 통신 네트워크를 접속하기 위한 네트워크 접속 단말기(3), 가입자들에게 서비스를 제공하는 정보 통신 네트워크(4), 네트워크 센터와 정보 통신 네트워크를 접속시키는 인터페이스(5), 그리고 정보 통신 네트워크와 각 네트워크 단말기를 접속시키는 인터페이스(6)로 구성된다.

### 2.3 동작 시나리오

(그림 1)과 같이 시스템의 동작 시나리오를 살펴보면 다음과 같다.

1) 정보 통신 서비스 네트워크를 이용하고자 하는 각 가입자-i에 대하여 네트워크 센터는 키 정보가 저장된 스마트 카드-i 를 해당 가입자-i에게 안전하게 발급한다.
2) 가입자-i가 정보 통신 서비스 네트워크를 이용하고자 할 때에는 자신의 스마트 카드-i 를 네트워크 접속 단말기에 연결하여 자신의 패스워드를 입력시켜 동작시킨다.
3) 입력된 가입자-i의 패스워드는 스마트 카드-i에서 검증된 후 가입자가 스마트 카드-i의 정당한 소유자인지 검증한다. 만약, 스마트 카드-i의 정당한 소유자가 아니면 동작이 종료된다.
4) 상기 3)의 결과가 정당한 소유자로 검증된 경우에, 스마트 카드-i는 가입자 인증 메세지를 생성하여 네트워크 접속 단말기와 정보 통신 서비스 네트워크를 통하여 네트워크 센터에게 전송한다.
5) 네트워크 센터는 수신한 가입자 인증 메세지를 이용하여 가입자-i가 정당한 네트워크 가입자인지 검증한다. 검증이 성공하면 네트워크 센터는 다음의 과정을 계속한다. 만약, 검증이 실패인 경우에는 동작이 종료된다.
6) 상기 5)의 과정이 성공할 경우, 네트워크 센터는 센터의 인증 메세지를 생성하여 정보 통신 서비스 네

트워크 와 네트워크 접속 단말기를 통하여 스마트 카드-i에 전송한다.

7) 스마트 카드-i는 수신한 센터 인증 메세지를 수신하여 네트워크 센터가 정당한 네트워크인지 검증한다. 검증이 성공하면 가입자-i와 네트워크 센터간의 상호 신분 확인/인증이 완료된 것으로 가입자-i는 서비스를 사용할 수 있다. 만약, 검증이 실패인 경우에는 동작이 종료된다.

8) 이상의 과정과는 별도로, 가입자-i가 자신의 패스워드를 변경하고자 할 때에는 자신의 스마트 카드-i를 네트워크 접속 단말기에 연결하여 이전에 사용했던 패스워드를 입력하여 정당한 소유자인지 먼저 검증을 받는다.

9) 입력된 가입자-i의 패스워드는 스마트 카드-i에서 검증된 후 가입자가 스마트 카드-i의 정당한 소유자인지 검증한다. 만약, 스마트 카드-i의 정당한 소유자가 아니면 동작이 종료된다.

10) 상기 7)의 결과가 정당한 소유자로 검증된 경우에, 가입자-i는 새로운 패스워드를 스마트 카드-i에 입력하고 스마트 카드-i는 패스워드 변경 요구 메세지를 생성하여 네트워크 접속 단말기와 정보 통신 서비스 네트워크를 통하여 네트워크 센터에게 전송한다.

11) 네트워크 센터는 수신한 패스워드 변경 요구 메세지를 이용하여 가입자-i가 정당한 네트워크 가입자인지 검증한다. 만약, 검증이 실패인 경우에는 네트워크 가입자는 네트워크 센터에 저장된 가입자의 패스워드를 변경할 수 없게 된다. 검증이 성공인 경우에는 해당된 가입자-i의 패스워드가 변경되어 안전하게 저장된다.

12) 가입자-i의 변경된 패스워드는 단방향 암호 처리되어 스마트 카드-i내에 안전하게 저장된다.

## 3. 네트워크 센터의 기능

### 3.1 구 성

(그림 2)는 (그림 1)과 연관하여 네트워크 센터(1)의 기능 구조도로 2.1은 네트워크의 비밀 키(SK)와 공개 키(PK)의 쌍을 생성하는 센터 키 생성부, 2.2는 생성된 네트워크의 비밀 키(SK)와 공개 키(PK)의 쌍과 가입자-i의 식별자 값인 IDi를 근간으로 가입자-i의 키 (PWi=(Ri, Si, UKi))를 생성하는 가입자 키 생성부, 2.3은 가입자-i의 스마트 카드-i로부터 전송된 인증 메세지(AMi={IDi, Ri, A, B, T})를 수신하여 가입자-i가 정당한 가입자인지 검증함은 물론 센터의 인증 메세지(AMc={IDi, A, B, C, T})를 가입자-i에게 전송함으로써 센터와 가입자간에 상호 검증을 가능케 하는 신분 확인/인증 처리부, 2.4는 가입자-i의 스마트 카드-i로부터 전송된 패스워드 변경 요구 메세지(CRi={IDi, Ri, A, B, T, E[UKi⁀PK]})를 수신하여 가입자-i가 정당한 가입자인지 검증하고 정당한 경우에 가입자-i의 패스워드를 변경하는 가입자 패스워드 변경 처리부, 2.5는 입력된 메세지에 대하여 단방향 암호계산 값을 구하는 단방향 암호처리부, 2.6은 마스터 키(MK)가 임시적으로 저장되어 사용되는 키 버퍼, 2.7은 센터의 비밀 키(PK), 공개 키(PK), 모든 가입자의 변경 가능한 패스워드(UK1, UK2, ..., UKi, ..., UKn)를 각각 암호화한 결과들을 저장하는 메모리, 2.8은 키 버퍼(2.6)의 마스터 키를 이용하여 암호 처리하는 대칭키 방식 암호처리부를 각각 나타낸다.

### 3.2 기능 수행 절차

네트워크 센터의 기능은 (그림 2)와 같이 다음의 절차에 의하여 이루어진다.

1) 네트워크 초기에 네트워크 센터(1)는 센터 키 생성부(2.1)을 동작하여 센터 고유의 비밀 키(SK)와 공개 키(PK) 쌍을 생성한다. 이 생성 과정은 다음과 같다. p는 큰 소수, $\alpha$는 GF(p)의 원시 근(Primitive Root)에 대하여 $PK = \alpha^{SK} \bmod p$.

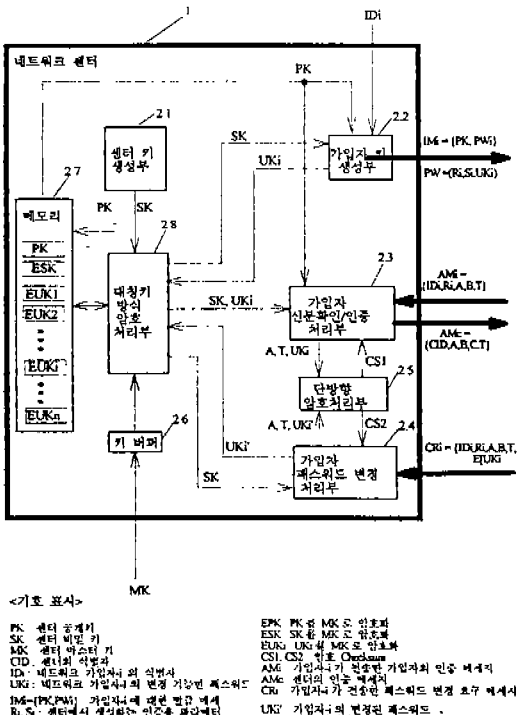
2) 생성된 센터의 비밀 키(SK)는 대칭키 방식 암호처리부에 의하여 암호화되어 암호화된 비밀 키(ESK)의 형태로 메모리(2.7)에 안전하게 저장되며 공개 키(PK)는 그대로 메모리(2.7)에 저장된다.

3) 가입자-i를 네트워크에 등록하기 위하여 가입자 키 생성부(2.2)는 가입자-i의 식별자인 IDi와 센터 키 생성부(2.1)이 생성한 센터의 비밀 키(SK) 및 공개 키(PK)를 이용하여 다음의 조건을 만족하는 가입자-i에 대한 키(PWi)를 생성한다.

(조건) PWi=(Ri, Si, UKi)의 생성은

i) $0 \le Ri, Si < (p-1)$인 (Ri, Si)는 $\alpha^{IDi} = PK^{Ri} * Ri^{Si} \bmod p$를 만족케 하며,

ii) UKi는 랜덤하게 생성하며 각 가입자에 대하여




(그림 2) 네트워크 센터에 대한 하드웨어 구성
(Fig. 2) Hardware configuration of network center

중복되지 않도록 한다.

상기 조건을 만족하는 (Ri, Si)의 생성 방법은 다음과 같다.

i) 가입자-i에 활용될 임의의 정수 Ki를 생성한다. 단, Ki는 $0 \leq Ki < (p-1)$의 조건과 $gcd(Ki, p-1) = 1$을 만족하며 각 가입자에 대하여 중복되지 않는다.

ii) $Ri = \alpha^{Ki} \bmod p$ 를 계산하여 Ri를 생성한다.

iii) $IDi = SK * Ri + Ki * Si \bmod (p-1)$을 만족하는 Si를 생성한다.

이상과 같이 생성된 PWi=(Ri, Si, UKi)는 가입자-i를 위한 키로 활용되며, 이중에서 Ri와 Si는 네트워크 센터에서 생성되는 가입자-I에 대한 인증용 파라메터들로서 가입자-i가 임의로 변경할 수 없으나, 초기에 제공된 가입자-i의 패스워드 UKi는 추후 가입자-i가 원할때 자유롭게 새로운 패스워드 UKi′으로 변경할 수 있다.

4) 가입자 키 생성부(2.2)는 상기 제3항에서 생성한 가입자-i의 패스워드(UKi)는 대칭키 암호처리부(2.8)를 통하여 암호화한 형태(EUKi)로 메모리(2.7)에 안전하게 센터(1)내에 저장한다.

5) 이상의 과정을 수행한 후, 센터 키 생성부(2.1)에서 생성한 센터 공개 키(PK)와 가입자 키 생성부(2.2)에서 생성한 가입자-i의 키(PWi=(Ri, Si, UKi))는 가입자-i에 대한 발급 메세지(IMi={PK, PWi})로 형성되어 안전한 방법으로 스마트 카드내에 저장된 후 가입자-i에게 발급된다.

6) 스마트 카드-i를 발급 받은 가입자-i가 네트워크를 사용하고자 할 때 가입자-i는 자신이 소유하고 있는 스마트 카드를 동작시켜서 인증 메세지(AMi={IDi, Ri, A, B, T})를 네트워크 센터에게 전송하고, 네트워크 센터(1)의 가입자 신분확인/인증 처리부(2.3)는 이 인증 메세지를 수신하여 다음의 과정을 거쳐 가입자-i를 검증한다.

i) 가입자 신분확인/인증 처리부(2.3)는 메모리(2.7)에 저장된 암호화된 센터 비밀 키(ESK)와 가입자-i에 대한 암호화된 패스워드(EUKi)를 대칭키 방식 암호 처리부(2.8)를 통하여 복호화함으로써 센터 비밀 키(SK)와 패스워드(UKi)를 각각 얻어낸다.

ii) 수신된 인증 메세지 AMi의 정보 중에서 A, T와 메모리(2.7)에서 얻어낸 UKi를 단방향 암호처리부(2.5)에 입력하여 암호 Checksum 값인 CS1 결과를 기다린다.

iii) 단방향 암호처리부(2.5)는 가입자 신분확인/인증 처리부(2.3)가 보낸 A, T, UKi를 이용하여 암호 Checksum 값인 CS1을 계산하고, 이 값을 가입자 신분확인/인증 처리부(2.3)에게 보낸다.

iv) 가입자 신분확인/인증 처리부(2.3)는 CS1을 수신한 후 다음의 계산 과정을 통하여 A′을 구한다.
$A' = Ri^{B} ((PK^{-Ri} * \alpha^{IDi})^{-1})^{CS1} \bmod p$

v) 가입자 신분확인/인증 처리부(2.3)는 상기 과정에서 계산한 A′과 A를 비교하여 서로 일치한 경우에만 가입자-i가 정당한 네트워크 가입자인 것으로 판단하여 서비스를 이용할 수 있도록 한다.

vi) 가입자-i가 정당한 가입자로 검증된 경우에, 센

터는 상호 신분확인/인증을 위하여 다음과 같이 센터 인증 메세지(AMc={CID, A, B, C, T})를 생성하여 가입자-i에게 보낸다.

$A = PK^{t} \bmod p$

$B = t + SK * CS1 \bmod p$

$C = PK^{SK} \bmod p$

(단, t는 랜덤 값, T는 시간 정보, CS1은 A와 T를 단방향 암호처리부(2.5)를 통하여 얻어낸 암호 Checksum 값)

7) 이상의 과정과는 별도로, 가입자-i가 자신의 패스워드를 변경하고자 할 때 가입자-i는 자신이 소유하고 있는 스마트 카드-i를 동작시켜서 패스워드 변경 요구 메세지(CRi={IDi, Ri, A, B, T, E[UKi']PK})를 네트워크 센터(1)에게 전송하고 네트워크 센터(1)의 가입자 패스워드 변경 처리부(2.4)는 수신된 패스워드 변경 요구 메세지(CRi)를 이용하여 다음의 과정을 거쳐 가입자-i의 패스워드를 변경시킨다.

i) 가입자 패스워드 변경처리부(2.4)는 대칭키 방식 암호처리부(2.8)을 통하여 메모리에 저장되어 있는 센터 비밀 키(SK)를 얻어 내고, 수신된 패스워드 변경 요구 메세지 CRi의 정보 중에서 E[UKi']PK를 센터 비밀 키(SK)로 복호화하여 UKi'을 얻어낸다.

ii) 수신된 패스워드 변경 요구 메세지 CRi의 정보 중에서 A와 T, 그리고 상기 i)의 과정에서 얻어낸 UKi'를 단방향 암호처리부(2.5)에게 입력하여 암호 Checksum 값인 CS2 결과를 기다린다.

iii) 단방향 암호처리부(2.5)는 패스워드 변경 처리부 처리부(2.4)가 보낸 A, T, UKi'를 이용하여 암호 Checksum 값인 CS2를 계산하고, 이 값을 패스워드 변경 처리부 처리부(2.4)에게 보낸다.

iv) 패스워드 변경 처리부 처리부(2.4)는 CS2를 수신한 후 다음의 계산 과정을 통하여 A'을 구한다.

$A' = Ri^{B} ((PK^{-Ri} * \alpha^{IDi})^{-1})^{CS2} \bmod p$

v) 패스워드 변경 처리부 처리부(2.4)는 상기 과정에서 계산한 A'과 A를 비교하여 서로 일치한 경우에만 가입자-i가 정당한 네트워크 가입자인 것으로 판단하여 가입자-i의 새로운 패스워드 UKi'을 대칭키 방식 암호처리부(2.8)를 통하여 메모리(2.7)에 안전하게 변경 및 저장한다.

## 4. 스마트 카드의 기능

### 4.1 구 성

(그림 3)은 스마트 카드(2)에 대한 세부적인 시스템 구성도로, 3.1은 네트워크 센터로 부터 스마트 카드를 발급 받을 때 스마트 카드내에 초기 키 정보를 저장하기 위한 초기 키 주입부, 3.2는 단방향 암호처리부, 3.3은 네트워크 가입자-i에 대한 신분확인/검증에 이용될 정보를 저장하는 메모리, 3.4는 네트워크 가입자-i가 스마트 카드-i의 정당한 소유자 인지 검증하고, 또한 네트워크 센터가 가입자-i에 대한 신분확인 및 인증을 실행할 수 있도록 가입자-i의 인증 메세지(Ami={IDi, Ri, A, B, T})를 생성 및 이를 네트워크 센터(1)에게 전송하고, 센터가 전송한 센터의 인증 메세지(AMc={CID, A, B, C, T})를 수신하여 센터의 신분확인/인증을 상호 검증하는 가입자 검증 및 신분확인/인증 처리부, 3.5는 가입자-I 가 자신의 패스워드를 변경 하고자 할 때 이를 위하여 패스워드 변경 메세지 (CRi={IDi, Ri, A, B, T, E[UKi']PK})를 생성하고 이를 네트워크 센터(1)에게 전송하는 패스워드 변경 처리, 3.6과 3.7은 가입자 검증 및 신분확인/인증 처리부(3.4)가 메모리(3.3)를 액세스하기 위한 액세스 포트를 각각 나타낸다.

### 4.2 기능 수행 절차

스마트 카드(2)의 기능은 (그림 3)에서와 같이 다음의 절차에 의하여 이루어진다.

1) 네트워크 센터(1)가 가입자-i를 위하여 스마트 카드-i를 발급할 때 네트워크 센터가 생성한 가입자-i에 대한 발급 메세지(IMi={PK, PWi})를 안전하게 초기 키 주입부(3.1)을 통하여 가입자-i의 스마트 카드-i(2)내의 메모리(3.3)에 저장한다. 이 단계에서 메모리(3.3)는 가입자-i에 대한 식별자 값(IDi), 센터 공개 키(PK), 가입자-i를 위하여 센터(1)가 생성한 Ri 및 Si 정보, 그리고 가입자 패스워드인 UKi를 단방향 암호처리부를 통하여 계산해 낸 암호화된 패스워드 OEUKi를 포함하게 된다.

2) 상기 제1항의 과정에서 스마트 카드-i(2)를 안전하게 발급 받은 가입자-i는 네트워크를 이용하고자 할 때 가입자 검증 및 신분확인/인증 처리부(3.4)를 통하여 다음과 같은 검증 과정을 거친다.

i)가입자-i는 자신이 알고 있는 패스워드 UKi를 입력한다.

ii)가입자 검증 및 신분확인/인증 처리부(3.4)는 입력된 패스워드 UKi를 근거로 단방향 암호처리부를 통하여 OEUKi를 계산하고, 메모리(3.3)에 저장된 가입자-i에 대한 OEUKi를 액세스 포트(3.6, 3.7)를 통하여 읽어 낸다. 이 두 값이 서로 일치하면 가입자 검증 및 신분확인/인증 처리부(3.4)는 그 검증 결과가 참(T:True)임을 패스워드 변경 처리부(3.5)에게 알리고 다음의 동작을 진행한다. 만약 검증이 실패하면 가입자 검증 및 신분확인/인증 처리부(3.4)는 그 검증 결과가 거짓(F:False)임을 패스워드 변경 처리부(3.5)에게 알리고 동작은 중지된다.

iii)상기 ii)의 검증이 성공적일 경우, 가입자 검증 및 신분확인/인증 처리부(3.4)는 다음과 같은 과정을 실행하여 가입자 인증 메세지(AMi)를 생성한다.

a)랜덤 값 $t(0 \le t \le (p-1))$를 생성하고 다음과 같이 A를 계산한다.

$A = Ri^t \bmod p$

b)시간 정보 T를 얻어낸 후 단방향 암호처리부에게 A, T, UKi를 입력하여 암호 Checksum 값 CS1를 얻어내어 B를 생성한다.

$B = t + Si * CS1 \bmod p - 1$

c)상기 a)와 b)에서 얻은 값을 근간으로 인증 메세지(AMi)를 생성한다.

AMi={IDi, Ri, A, B, T}

iv)생성한 인증 메세지(AMi)를 네트워크 센터(1)로 전송한다.

v)센터가 상호 신분확인/인증을 위하여 전송한 센터 인증 메세지(AMc={CID, A, B, C, T})를 수신하여 다음의 과정을 거쳐 A′을 계산한 후 A와 A′이 서로 일치하면 센터에 대한 상호 검증이 성공적이다.

$A' = PK^B * (C^{-1})^{CS1} \bmod p$

(단, CS1은 A와 T를 단방향 암호처리부(3.2)를 통하여 얻어낸 암호 Checksum 값)

3)또한, 가입자-i가 자신의 패스워드를 변경하고자 할 때는 패스워드 변경 처리부(3.5)를 통하여 다음과 같은 검증 및 변경 과정을 거친다.

i)상기 제2항에서 기술한 가입자 검증 및 신분확인/인증 처리부의 각 과정을 실행하여 패스워드의 변경을 시도하려는 가입자가 스마트 카드의 정당한 소유자인지 검증한다.

ii)상기 i)의 검증이 성공적일 경우, 패스워드 변경 처리부(3.5)는 다음과 같은 과정을 실행하여 패스워드 변경 요구 메세지(CRi)를 생성한다.

a)랜덤 값 $t(1 < t < (p-1))$를 생성하고 다음과 같이 A를 계산한다.

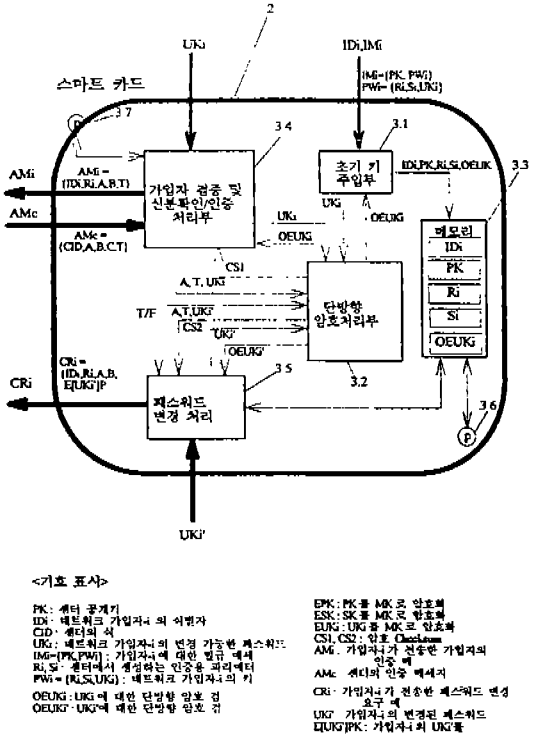
$A = Ri^t \bmod p$

b)시간 정보 T를 얻어낸 후 단방향 암호처리부에게 A, T, UKi′를 입력하여 암호 Checksum 값 CS2를 얻어내어 B를 생성한다.

$B = t + Si * CS2 \bmod p - 1$

c)센터의 공개 키(PK)를 이용하여 UKi′을 암호화한다.

E[UKi′]PK




(그림 3) 스마트 카드에 대한 하드웨어 구성

(Fig. 3) Hardware configuration of smart card

d) 상기 a), b), c)에서 얻은 값을 근간으로 패스워드 변경 요구 메세지(CRi)를 생성한다.

CRi = {IDi, Ri, A, B, T, E[UKi']PK}

iii) 생성한 패스워드 변경 요구 메세지(CRi)를 네트워크 센터로 전송한다.

iv) 패스워드 변경 처리부(3.5)는 새로운 패스워드(UKi')를 단방향 암호처리부(3.2)에게 입력하여 단방향 암호 검증 값(OEUKi')을 얻어내고 이를 메모리(3.3)에 변경 및 저장한다.

## 5. 동작 시나리오

(그림 4)는 네트워크 센터 및 스마트 카드가 동작하는 과정을 기술하기 위한 실행 흐름도로 다음과 같이 설명된다.

단계 1. 실행이 시작되면(4.1) 네트워크 센터는 센터의 공개 키(PK)와 비밀 키(SK)를 생성하고(4.2) 센터의 마스터 키에 의하여 비밀 키(SK)를 암호화하여 저장한 이때 저장된 값은 공개 키(PK)와 암호화된 비밀 키(ESK)이다.

단계 2. 처리되어질 작업의 형태가 선택된다(4.4). 선택이 가입자 등록이면 다음의 단계 3을 실행하며, 네트워크 사용이면 단계 4를 실행하고, 패스워드 변경이면 단계 5를 실행한다.

단계 3. 선택이 가입자 등록이면 가입자 키 생성 및 스마트 카드 발급(4.5)을 실행하고 작업이 종료되어(4.13) 단계 2로 간다.

단계 4. 선택이 네트워크 사용이면

4.1) 가입자 신분확인/인증 처리(4.6)을 실행한다.

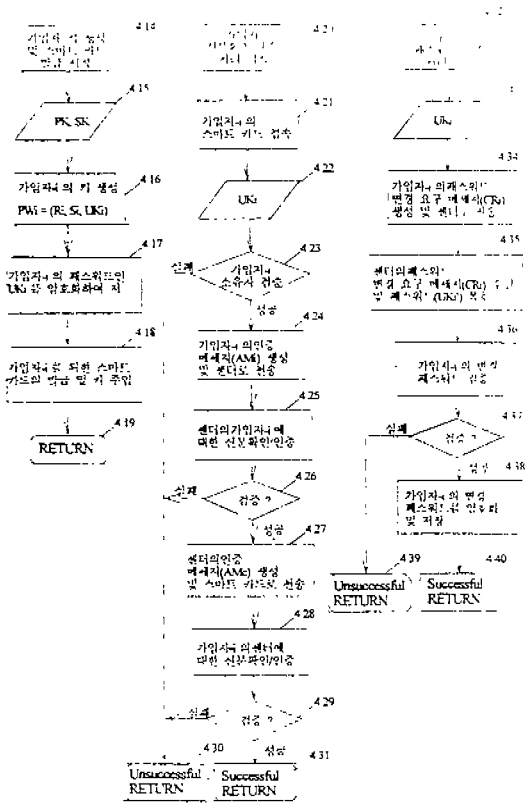
4.2) 가입자 신분확인/인증의 결과를 검증하여(4.7) 성공이면 정보통신 네트워크 서비스를 사용한다(4.8). 검증의 결과가 실패인 경우에는 작업이 종료되어 단계 2로 간다.

4.3) 사용이 끝인지를 비교하여(4.9) 끝이면 작업이 종료되어(4.13) 단계 2로 간다. 그렇지 않으면 네트워크 서비스의 사용(4.8)이 계속된다.

단계 5. 선택이 패스워드 변경이면

5.1) 가입자 신분확인/인증 처리(4.10)을 실행한다.

5.2) 가입자 신분확인/인증의 결과를 검증하여(4.11) 성공이면 가입자 패스워드 변경 처리를 실행한다(4.12). 검증의 결과가 실패인 경우에는 작업이 종료되어(4.13) 단계 2로 간다.




(그림 4) 동작 및 제어 흐름도

(Fig. 4) Flow chart of operation and control

이 종료되어(4.13) 단계 2로 간다.

상기 단계 3의 가입자 키 생성 및 스마트 카드 발급(4.5) 과정의 내부 실행 흐름을 기술하면 다음과 같다.

1) 동작이 시작되면(4.14) 센터의 공개 키(PK)와 비밀 키(SK)를 읽어 낸다(4.15).

2) 가입자-i-를 위한 키(PWi = {Ri, Si, UKi})를 생성한다(4.16). 여기에서 UKi는 스마트 카드의 정당한 소유자가 변경할 수 있는 패스워드이다.

3) 가입자-i의 패스워드(UKi)를 암호화하여 센터의 메모리에 암호화된 패스워드(EUKi) 형태로 저장한다(4.17).

4) 생성한 키를 스마트 카드내에 안전하게 주입하고 가입자에게 스마트 카드를 발급한다(4.18).

5) 작업이 종료된다(4.19).

상기 단계 4의 가입자 가입자 신분확인/인증 처리(4.6)과정의 내부 실행 흐름을 기술하면 다음과 같다.

1) 동작이 시작되면(4.20) 가입자-i의 스마트 카드-i를 네트워크에 접속하여 동작을 시작한다(4.21).
2) 가입자-i의 패스워드(UKi)를 입력한다(4.22).
3) 스마트 카드-i는 가입자-i가 입력한 패스워드(UKi)를 이용하여 가입자-i가 스마트 카드-i의 정당한 소유자인지 검증한다(4.23). 검증이 성공이면 동작이 계속 진행되며, 실패인 경우에는 동작을 중지한다(4.30).
4) 스마트 카드-i는 가입자-i의 인증 메세지(AMi)를 생성하고 이를 센터로 전송한다(4.24).
5) 네트워크 센터는 가입자-i의 인증 메세지(AMi)를 수신하고 이 정보를 근간으로 가입자-i에 대한 신분확인/인증을 실행하여 검증한다(4.25).
6) 가입자-i에 대한 검증 결과를 비교하여(4.26) 성공이면 다음의 과정을 계속 실행하고, 실패인 경우에는 동작을 중지한다(4.30).
7) 네트워크 센터는 센터의 인증 메세지(AMc)를 생성하고 이를 해당 가입자-i의 스마트 카드-i에게 전송한다.
8) 가입자-i의 스마트 카드-i는 센터의 인증 메세지(AMc)를 수신하고 이 정보를 근간으로 센터에 대한 신분확인/인증을 실행하고 검증한다(4.28).
9) 센터에 대한 검증 결과를 비교하여(4.29) 성공이면 성공적으로 작업을 종료하고(4.31), 실패인 경우에는 동작을 중지한다(4.30).

상기 단계 5의 가입자 가입자 패스워드 변경 처리(4.10) 과정의 내부 실행 흐름을 기술하면 다음과 같다.

1) 동작이 시작되면(4.32) 가입자-i의 변경하고자하는 새로운 패스워드(UKi')을 입력한다(4.33).
2) 스마트 카드-i는 가입자-i의 패스워드 변경 요구 메세지(CRi)를 생성하고 이를 네트워크 센터로 전송한다(4.34).
3) 네트워크 센터는 가입자-i가 전송한 패스워드 변경 메세지(CRi)를 수신하고 가입자-i가 변경하고자 하는 새로운 패스워드(UKi')을 복호화하여 얻어낸다(4.35).
4) 가입자-i의 변경 패스워드에 대한 검증을 실행한다(4.36).
5) 검증 결과를 비교하여(4.37) 성공이면 가입자-i의 새로운 패스워드를 암호화하여 메모리에 변경 및 저장하고(4.38) 작업을 성공적으로 종료한다. 실패인 경우에는 동작을 종료한다(4.39).

## 6. 결 론

스마트 카드를 이용한 네트워크 가입자 신분확인/인증 방법에 관한 것으로 다음과 같은 효과를 기대할 수 있다. 정보통신 네트워크를 통하여 고부가가치 통신서비스를 가입자에게 제공하고자 할 때 스마트 카드를 이용한 가입자들과 네트워크 센터간의 상호 신분확인/인증 방법에 의하여 보다 안전하고 신뢰성 있는 서비스를 제공할 수 있다.

또한, 정보통신 네트워크상의 모든 가입자들은 자신에게 발급된 스마트 카드를 이용하여 자신이 정당한 가입자임을 쉽고 편리하게 입증할 수 있으며, 또한 네트워크 센터를 상호 신분확인/인증할 수 있으므로 가입자에게 높은 안전성 있는 서비스를 제공하고자 하는 네트워크 서비스에 활용할 수 있다. 스마트 카드를 사용하고자 할 때 가입자는 자신이 알고 있는 패스워드를 입력시켜 자신이 스마트 카드의 정당한 소유자임을 입증한 후 사용할 수 있으므로 본 방법은 스마트 카드를 분실하였거나 또는 불순한 사용자에 의한 스마트 카드의 불법적인 도용으로 인하여 발생할 수 있는 경제적인 손실과 신용에 있어서 고도의 안전성을 제공하고 네트워크상의 통신 링크상에서 가입자의 패스워드가 누출되지 않으며, 해커 등의 공격에 보다 안전한 서비스의 제공이 가능하다.

또한, 가입자가 자신의 패스워드를 안전하게 변경하여 사용할 수 있는 방법을 제공하므로 본 논문에서 제시한 방법은 정보통신 서비스 네트워크의 제공자, 운용자, 그리고 가입자 측면에서 높은 신뢰성, 안전성, 효용성이 있다.

## 참 고 문 헌

[1] Chin-Hen Chang and Wen-Yuan Liao, "A remote password authentication scheme based upon Elgamal's signature scheme," Computers and Security, Vol 13, pp. 137-144, Apr. 1994.

[2] T.Elgamal, "A public key cryptosystem and a sig-

nature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, IT31(4), pp. 469-472, July. 1985.

[3] C.C. Chang and T.C. Wu, "A remote password authentication with smart cards," IEE Proc., Part E, 138(3), pp. 165-168, May. 1991.

[4] C.C. Chang and C.S. Laih, "Correspondence for remote password authentication with smart cards," IEEE Proc., Part E , pp. 372, 1992.

[5] 조현숙, 임춘식, "DigiPass: KoreaSat DBS의 Conditional Access System," 전자공학회지 제22권 제7호, pp. 768-775, 1995년7월.

[6] 조현숙, 임춘식, "Pay-TV 서비스를 위한 스마트카드," 위성통신 우주산업회지, pp. 58-65, 1995년 8월.

[7] 임채훈, 이필중, "개인정보에 기초한 키 분배 방식의 분 석 및 개선 방안," 한국통신정보보호학회 논문지, 제1권, 제1호, pp. 47-65, 1991년 12월.

[8] L.Lamport, "Password authentication with insecure communication," Commun. Assoc. Comput. Math., 24(II), pp. 770-772, Nov. 1981.

[9] E.Okamoto and K.Tanaka, "Identity-based information security management system for personal computer network," IEEE J. Sel. Areas Commun., 7(2), pp. 290-294, May. 1989.

**이 장 원**

1990년 영국 웨일즈대학교 전산과학과 졸업(학사)
1991년 영국 런던대학원(임페리얼 칼리지) 전산과학과(석사)
1992년~현재 한국전자통신연구소 위성통신기술연구단 연구원
관심분야: 시각 및 공간 로직, 위성통신 시스템 정보보호

**홍 기 융**

전남대학교 계산통계학과 졸업(학사)
중앙대학교 전산학과 (석사)
아주대학교 컴퓨터공학과(박사)
1985~1995년 전자통신연구소 선임연구원
1995~현재 한국전산원 선임연구원
관심분야: 컴퓨터 및 네트워크, O.S 및 정보통신 Security 위성망 관리 및 정보보호

**조 현 숙**

1980년 전남대학교 수학과 졸업(학사)
1991년 충북대학교 전산학과(석사)
1982년~현재 한국전자통신연구소 선임연구원
관심분야: 암호학, 통신 정보보호