□특집□

PCS 이동단말기 인증을 위한 키분배 방법에 관한 연구

박 형 일† 강 지 훈††

◈ 목 차 ◈

요 약

AC(인증센터)의 주요한 기능은 이동국과의 인증을 수행하고 이동국과 인증센터간에 사용하는 인증정보를 갱신하는 일이다. 이러한 일을 수행하는데 있어서 인증키의 교환, 관리, 분배는 가장 기본적인 것이라고 할 수 있을 것이다. KDS는 위와 같이 인증에 관여하는 여러 블럭중에서 특히 키의 생성, 관리, 분배 등을 맡고 있는 블럭이다. 즉, 가입자의 인증 키는 KDS에 의해서 생성되고 관리된다. KDS는 인증센터 내부에 하나의 블럭으로 존재할 수도 있고, 인증센터와 분리될 수 도 있으므로 설계시 이 사항을 고려해야 한다. 본 논문에서는 이동국과 인증센터간의 정확한 인증키의 공유(분배)를 위한 KDS의 역할 및 KDS와 주변 블럭들간의 메시지 흐름를 설명한다.

† 정회원 : 삼성전자(주) 주임연구원
†† 정회원 : 삼성전자(주) 선임연구원

1. 서 론

이동통신 시스템은 이동가입자가 무선채널을 통해 통신함으로써 야기되는 특정 가입자의 불법 사용 문제점을 해결하기 위하여, 가입자에 대한 서비스를 제공해 주기 전에 해당 가입자가 과연 서비스가 허용된 가입자인지를 확인한다. 이와 같이 가입자에 대한 서비스 실시의 허용 여부를 확인하는 기능을 인증기능이라 할 수 있다. 이는 이동통신 시스템에서 이동국과 네트웍간에 서로 비밀키를 공유하여, 동일한 인증알고리즘을 수행한 후 그 결과를 비교하여 이동국의 적합성을 확인하여 해당 이동국이 네트웍으로의 접근을 허용하도록 하는 절차이다.

이동국과 네트웍간에 공유하는 비밀키는 인증키라고도 하며 제3자에게는 절대로 알려져서는 안되는 매우 중요한 인증의 요소로서, 그 생성과 관리에도 각별한 주의가 필요하며 관리 주체도 인증센터 내의 다른 블럭들과 구별된다. 이렇게 인증키를

적절히 생성하고 저장하며 이동국과 시스템간에 정확하게 분배할 수 있도록 해 주는 기능을 담당하는 블럭이 KDS(Key Distribution Server)이다.

본 논문에서는 2장에서 인증센터내의 KDS와 그 주변 블럭에 관한 간략히 기술 하고, 3장에서는 KDS가 생성하고 관리할 인증키의 순환구조를 기술한다. 4장에서는 KDS의 인증키 관리기능을 위한 메시지의 흐름, 5장에서는 인증키의 관리를 위해 필요한 데이터베이스 구조를 기술하고 6장에서 결론을 맺는다.

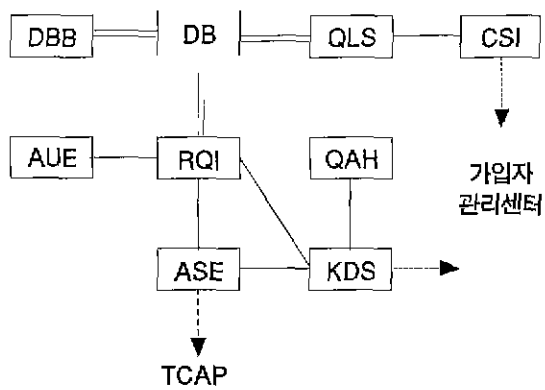
2. AC 소프트웨어 구조

소프트웨어의 구성은 그림1과 같이 하여 PCS HLR 시스템의 구성과 유사하나 AuEx와 KDS는 인증기능을 위하여 새로이 구성된 기능체이다. 데이터베이스를 관리하는 기능체는 HLR과 유사하게 RQI와 QLS로 구성된다. RQI를 통하여 데이터베이스에 접근하는 기능체는 ASE와 AuEx, 그리고 KDS로 이중 특히 ASE와 AuEx는 실시간 처리를 필요로 한다. 물론 KDS도 자체 기능수행의 절차에 따라 실시간 처리를 필요로 할 수 있다. ASE는 사건중심적인 처리를 하는 반면 AuEx는 사건중심 및 시간중심처리를 수행한다. AuEx는 이벤트가 발생하지 않아도 끊임없이 가입자의 인증정보를 검색한다. 그러므로 휴지시간이 적고 일정부하 이상을 항상 유지한다.

한편 OAH, CSI는 QLS를 통하여 데이터베이스에 접근한다. QLS는 SQL(Standard Query Language)과 유사한 명령어를 지원하여 사용자가 쉽게 데이터베이스를 사용할 수 있도록 해준다. QLS는 high-level 언어를 지원하기 때문에 실시간 처리가 어렵다. 그러므로 QLS를 사용하는 응용계층은 비실시간 처리를 수행하는 기능을 가지고 다양한 검색을 필요로 하는 응용계층이다.

DBB는 메모리로 구성되어 있는 데이터베이스를 비휘발성 기억장치인 하드디스크로 백업시키는 기능을 한다. 또 CSI는 가입자관리센터와의 정합을 담당하는데, 사업자와 합의하에 작성된 독점적인 프로토콜과 QLS의 질의어 간을 매핑하는 기능 하며 주로 tcp/ip를 사용한다.

마지막으로 KDS는 인증키를 생성하고 이를 RQI를 통해 데이터베이스에 저장하며, ASE와도 통신을 하여 인증키에 관련된 정보를 주고 받는다.



ASE : Application Service Element
AuEx : Authentication Policy Executive
CSI : Custom Service Interface
DBB : Database Backup
OAH : Operation & Admin. Handler
QLS : Query Language Server
RQI : Realtime Query Interface
KDS : Key Distribution Server
——— : Inernal Message Path
═══ : Database Access Path
····· : External System Access
- - - - - : Intra-system Access

(그림1) AC 소프트웨어 구조

3. 인증키의 순환

이동국를 인증하기 위해서는 단말과 시스템간에 공통으로 사용하는 어떤 값이 존재해야 하는

데 이것이 바로 인증키이다. 그러므로 인증키는 인증을 위한 가장 기본적인 요소라고 할 수 있으며, 이를 제3자에게 노출시키지 않고 단말과 시스템이 교환하고, 키를 분배하며 관리할 필요가 있다. 이러한 인증키 교환, 인증키 관리, 인증키 분배는 Key Management Center의 역할이 인증센터 내에 존재하는 것을 의미하며, 이를 수행하는 블럭이 바로 KDS라 할 수 있다.

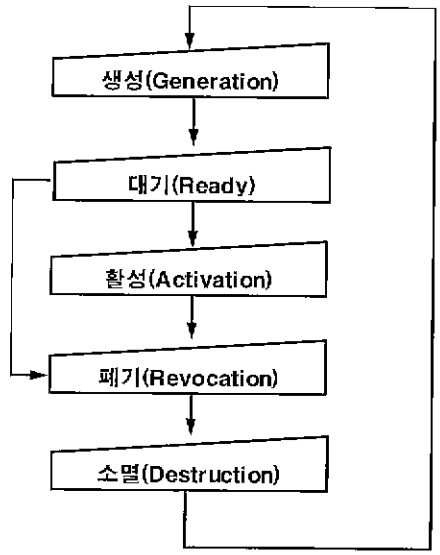
3.1 인증키 Life Cycle

인증키는 단말과 인증센터에서 사용하며 대칭형 세션키를 생성하는 중요한 키이며, 1과 0의 조합으로 구성되는 8바이트, 즉 64비트의 비트열이다. 키는 생성, 대기, 활성, 폐기, 소멸의 5단계에 걸쳐 상태를 천이 한다. 또한 가입자 등록시 할당되어 사용되며, 생성되어 소멸할 때까지 관리된다. 생성되어 있는 키의 수는 life cycle을 순회하는 동안 활성화되어 있는 키의 수보다 많다.

인증키는 보안에 있어서 매우 중요한 것이므로 임의적으로 생성되거나 소멸될 수 없도록 해야 한다. 인증키의 life cylcle은 그림2와 같은 순환 구조를 하고 있다.

(1) 생성 및 대기

생성은 키를 특정 알고리즘 혹은 다른 어떤 방법을 통해 64 비트를 만드는 과정이다. 생성된 키는 인증센터에서 방금 생성했기 때문에 키에 대한 정보가 없을 뿐만 아니라 이동국도 이에 대한 아무런 정보를 가지고 있지 않고, 단말과 인증센터이 인증키를 성공적으로 나누어 가지기 전이므로 대기상태로서 존재해야 한다. 대기상태의 키는 일련의 인증과정을 거쳐 이동국과 인증센터간에 정상적으로 분배되었는지 검증을 해야 하고 검증에 통과해야 활성화상태가 된다. 대기상태의 키를 검증하는 방법은 분배받은 장치에서 이 키를 사용하여 암호화된 메시지를 작성하고 생성한 장치에서 복호화 하여 규정된 메시지가 정상적으로 전달됨을 확인하면 된다. 만일 이동국과 인증키를 공유하는 과정에서 문제가 발생하거나 공유가 취소되면 대기중인 키는 바로 폐기된다.



(그림2) 키의 Life Cyle

(2) 활성

활성화된 키는 실제로 하나의 이동국과 매핑을 이루며 사용되는 키이고, 인증정책에 의하여 폐기되는 순간까지 이동국과 인증센터간의 인증에 유효하다.

(3) 폐기

활성화되어 있는 키는 이동국의 영구적인 사용금지 혹은 폐기, 가입자의 등록해지 등과 같은 상황에서 더이상 사용되지 못하도록 폐기되어야 한다. 폐기된 키는 일정기간 이 상태를 유지하다가 소멸된다. 폐기된 키를 일정기간 동안 보존하는 이유는 폐기된 키가 곧바로 사용되는 현상을 막기 위해서 이다. 폐기된 키가 곧바로 사용될 경우 불법적인 사용의 소지가 있으며, 또한 이 키가 노출되었다면 악용당할 가능성이 있다.

(4) 소멸

폐기된 키가 재생성되기 위해서는 소멸되어야 하고 소멸된 키는 다시 생성을 통해 인증키로서의 새로운 life cycle을 가지게 된다. 소멸은 폐기된 키가 재활용되기 위한 필수적인 과정으로 폐기기간(재생성불가능기간)동안 재생이 금지된 키는 소멸됨으로써 더 이상 존재하지 않게 된다. 이는 곧 생성이 가능하다는 의미가 된다. 소멸된 키는 그에 대한 정보가 함께 소멸하는 것으로 이력에 사용기록을 남길 수 있다.

4. 인증키 관리 기능

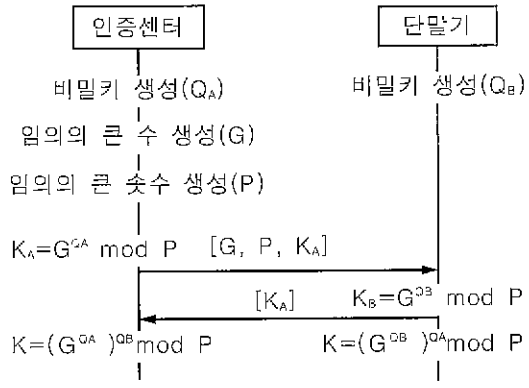
인증센터에서는 인증에 관한 정보를 보안을 유지하며 안전하게 관리하는 기능을 제공할 수 있어야 하며, 특히 인증키의 생성 및 관리는 KDS에서 별도로 수행한다. KDS는 인증센터 내부에 위치 할 수도 있고, 분리되어 하나의 독립적인 시스템으로 운용될 수도 있으므로 별도의 데이터베이스를 구축해야 한다.

인증키의 관리는 인증의 기본사항이라 할 수 있는 인증키를 인증센터와 이동국이 정확하고 안전하게 공유(분배)하는 방법에 따라 조금씩 다를 수 있다.

4.1 OTASP에 의한 인증키 분배

OTASP[1](Over The Air Service Provisi-oning)는 이동국을 구입한 비가입자가 대리점과 같이 제3자의 개입없이 가입절차, 즉 새로운 서비스의 등록 등을 가능하게 하는 절차이다. OTASP를 통한 인증키의 분배는 Air(무선접속)상으로 인증키에 대한 정보를 주고 받아야 하기 때문에 제3자에 의한 데이터 유출의 우려가 있으므로 인증키 자체를 통신을 통하여 공유할 수는 없다. 따라서 인증키를 직접 송수신하지 않고, 인증키를 계산하는데 핵심이되는 파라미터를 특정 함수의 입력으로 하여 계산한 결과를 주고 받아서 이동국과 인증센터 각각이 인증키를 계산하게 된다. 물론 이 때 송수신되는 값은 비록 이 값이 노출되더라도 역으로 파라미터를 추출해 내기 어려운 것이라야 한다. 즉, 위의 과정에서 사용된 함수가 단방향의 성격이 강한 것이라야 한다.

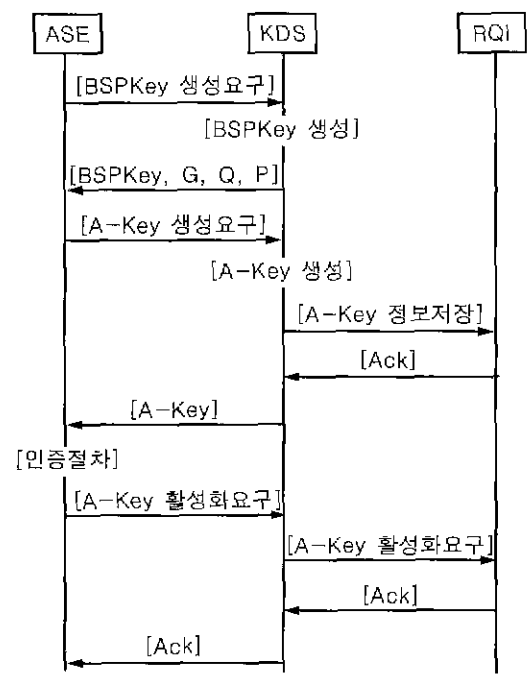
본 KDS에서는 인증키의 분배를 위해 Diffie-Hellman 방식을 사용한다. 이 방법을 사용하면 역으로 파라미터를 추출하는데 discrete logarithm problem을 풀어야 하는 데, 이는 매우 어려운 문제로 알려져 있다. 본 KDS에서 사용하는 인증키 분배절차의 개요는 그림3과 같다. 여기서 QA와 QB는 각각 인증센터와 이동국의 비밀키이고 크기는 160비트이다. G는 인증키를 생성하기 위한 생성자(Generator)로서 160비트의 크기를 갖는다. P는 모듈로 연산을 하기 위한 숫수로 크기는 512비트이며 선택에 의하여 768비트일 수 있고 최상위비트는 1로 정해진다. KA, KB, K는 각각 Base Station Partial Key(BSPKey), Mobile Station Partial Key(MSPKey), 인증키이고 크기는 각각 512비트, 512비트, 64비트이다.



(그림3) 인증키 분배과정(Diffie-Hellman)

인증키의 공유과정은 먼저 인증센터(KDS)에서

비밀키 QA, 생성자 G, 모듈로값 P를 생성하고 KA를 계산한다. 그 후 계산된 KA, G와 P를 함께 이동국으로 송신하고 QA와 P를 저장한다. 이동국에서도 독자적으로 비밀키 QB를 생성하고 수신한 BSPKey에 QB승을 하여 인증키 K를 계산한다. 한편 수신한 G, QB와 P를 사용하여 MSPKey를 계산하여 다시 인증센터로 송신한다. 인증센터(KDS)에서는 수신한 MSPKey에 QA승을 하여 인증키 K를 계산한다.



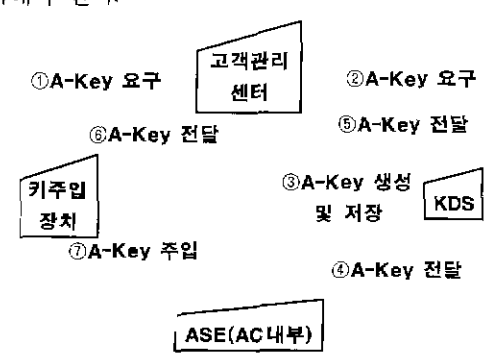
(그림4) 인증키 생성 절차(OTASP)

이렇게 계산된 인증키는 이동국과 인증센터가 독립적으로 계산을 한 것이고 아직 정확하게 똑같이 공유했다는 증거가 없으므로 곧바로 사용되어서는 않되고 인증절차를 거쳐야 한다. 즉 이 키는 생성되어 대기상태로 남게 된다. 이 키가 활성키가 되려면 상기한 검증절차를 통과해야만 한다. 인증키의 분배과정을 2장에서 설명한 소프트웨어 구조와 연관지으면 그림4와 같이 나타낼 수 있다. 여기서는 OTASP에 의한 인증절차를 간단하게 나타내었으나, 생성되어 대기중인 키를 활성화시키기 위한 인증절차는 생략하였다. 또한 복잡함을 덜기 위해 KDS, ASE, RQI의 세 프로세스 간의 상호 전달 메시지 구별자를 그 역할에 따라 간단히 풀이하여 적어 놓았다.

그림에서 KDS가 인증키(대기상태)를 생성하여 데이터베이스에 저장하기 위해 RQI로 송신했을 때 새롭게 생성한 인증키가 Normal Key Table이나 Revocation Key Table에 존재하지 않으면 Ack 메시지를 수신하여 성공적으로 인증키를 생성했음을 ASE로 알린다. 그러나 생성한 인증키가 이미 데이터베이스 테이블(Nomal 또는 Revo-cation Key Table)에 존재하면 이 키는 더이상 사용할 수 없으므로 ASE로 인증키의 생성실패 사실을 알린다.

4.2 키주입 장치에 의한 인증키 분배

여러 가지의 인증키 분배방법중 다른 하나는 전기적 장치를 사용하여 자동으로 이동국에 인증키를 주입하는 방법이다. 이를 위해서는 이동국의 판매 대리점에 추가로 전기적 키주입 장치를 설비해야 한다.

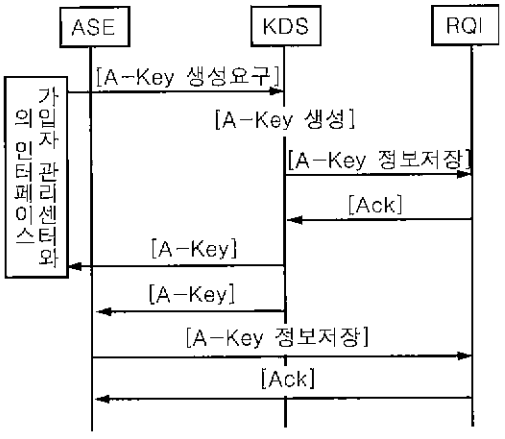


(그림5) 인증키 주입 절차(키주입 장치)

인증키의 분배과정은 다음과 같다. 먼저 고객이 가입요구를 하면 대리점의 터미널을 통해 고

객관리센터로 새 이동국의 등록사실을 알린다. 고객관리센터에서는 새 가입자의 이동국을 등록하기 위해 HLR로 등록명령을 내린다. 고객관리센터는 HLR에의 등록절차가 종료되면 인증센터로 가입자의 등록을 요구하게 되고, 인증센터 내에서는 이 때부터 인증키의 생성에 관여하게 된다. 새로운 가입자의 등록과 동시에 KDS는 이 가입자에게 할당할 인증키를 생성하여 저장하고, 생성된 키를 대리점의 키주입 장치로 암호화 하여 송신한다. 키주입장치는 수신한 키를 복호화 하여 이동국에 주입한다.

아직은 이 키가 정상적으로 분배되었는지가 확인이 되어 있지 않으므로 이동국이 이 키를 아직 영구기억장치에 저장하면 안되고, 인증센터에서 또한 대기키로 유지하고 있어야 한다. KDS는 생성된 키를 ASE로 전달을 하는데, 그 이유는 나중에 일어날 인증절차를 위해서이다. 키는 인증절차를 통과해야 활성화될 수 있다. 그림5는 키주입 장치에 의한 인증키의 분배를 터미널의 관점에서 나타낸 것이고, 이 과정을 인증센터에 중점을 두어 내부 흐름을 나타낸 것이 (그림 6)이다.



(그림6) 인증키 생성 절차(키주입 장치)

4.3 폐기키의 관리

생성되고 활성키로서 역할을 다한 인증키가 폐기되면 일정기간 동안 폐기상태를 유지하다가 소멸된다. 이 기간을 재생성불가능기간으로 정의한다. KDS는 프로세스의 초기 기동시 RQI를 통해 데이터베이스로부터 재생성 불가능기간을 얻는다. 키가 폐기될 때에는 Normal Key Table에서 해당 키를 삭제하고 Revocation Key Table에 폐기키의 정보를 저장한다. Revocation Key Table에 존재하는 폐기키 중 재생성 불가능기간이 지난 키에 대해서는 이 키를 소멸시켜 재생성이 가능하도록 해야 한다. KDS에서는 이와 같이 폐기키를 소멸시키기 위하여 주기적으로 Revocation Key Table을 검색한다. 이 때, 재생성불가능기간이 지난 키에 대한 정보는 키관리 테이블에서 삭제되지만 필요에 의해 이력으로 남길 수 있다.

5. Database 구조

KDS에서는 가입자의 인증키를 관리하기 위해 인증센터와는 별도의 데이터베이스를 구축한다. 데이터베이스는 크게 대기중인 키와 활성키를 저장하는 Normal Key Table과 더이상 사용되지 않고 소멸되기를 기다리는 폐기상태의 키를 저장하는 Revocation Key Table로 나뉜다. 두 테이블의 구조를 표1과 표2에 각각 나타내었다.

<표1> Normal Key Table

Field	Size(Bytes)
A-Key	8
MIN	5
Creation Date	4
State	1
Creator	1
Serial Number	4

여기서 A-Key는 64비트의 인증키, MIN은 가입자의 번호, Creation Date는 인증키를 생성한 시각, Expiration Date는 인증키가 폐기된 시각, State는 인증키의 상태(대기 또는 활성), Serial Number는 인증키의 생성시 부여되는 일련번호, 그리고 Creator는 인증키를 어떠한 방법으로 생성했는가를 나타내는 값이다.

Serial Number는 생성되는 인증키의 단순한 일련번호로서의 의미외에 복권식 키분배*와 같은 방법에서 인증키를 찾아내는 중요한 단서로 사용된다.

<표2> Revocation Key Table

Field Name	Size(Bytes)
A-Key	8
MIN	5
Creation Date	4
Expiration Date	4
Creator	1
Serial Number	4

6. 결 론

인증키를 이동국과 인증센터간에 공유 하기 위한 방편으로 KDS라는 키관리 블럭을 두어 인증키가 생성되어 소멸할 때까지 관리하도록 하였다. 본 KDS에서 구현한 기능중의 하나는 OTASP를 이용한 인증키의 분배 방식으로, 이는 Diffie-Hellman 방식을 도입하여 이동국과 인증센터가 각각 비밀키를 생성하여 MSPKey와 BSPKey를 상대에게 전달함으로써 인증키를 계산하는 절차이다.

또하나의 인증키의 분배방법으로 전기적 키주입 장치를 이용하여 이동국을 이 장치에 연결함으로써 직접 인증키를 주입하는 방법이다. 키주입 장치를 사용할 때는 KDS가 CSI로부터 키의 생성 요구를 수신하면서 새로운 키에 대한 관리가 시작된다. 이 방법은 인증키를 직접 송수신 해야 함으로 송수신시 암호화를 하여 안전하게 인증키가 전달 될 수 있도록 한다.

상기한 방법외에 여러 가지가 있을 수 있으며, 같은 방법이라도 구현여하에 따라 절차가 조금씩은 다를것이다. 어떠한 방법을 택하는냐의 문제는 이동통신 사업자와 시스템 공급자간에 협의를 통해 결정이 되겠지만, 가장 중요한 사실은 얼마나 안전하게 또 신속 정확하게 인증키를 분배할 것인가 하는 문제일 것이다. 앞으로 가입자가 늘어나면서 이동국의 수도 많아지고 서비스도 다양화될 시점에서 인증키의 관리를 운용자 관점에서 보다 쉽게 또 철저하게 할 수 있도록 되어야 할 것이다.

* 복권식 키분배는 이동 단말기를 구입한 고객이 서비스 등록을 할 때 마치 복권과 같은 방법으로 인증키를 분배하는 방법이다. 키는 이미 AC에 생성되어 있고, 단지 MIN, ESN과의 매핑만이 이루어 지지 않은 상태이다. 복권에는 인증키와 일련번호가 적혀 있는데 키는 가려져 있으므로 가입자가 은밀히 이 키를 보고 이동 단말기에 입력해야 한다. 이 때 일련번호를 같이 입력하여 키를 직접적으로 AC에 전달하지 않고 일련번호를 전달하게 되며, AC에서는 일련번호로 실제 키와의 매핑을 하게 된다.

약어 정리

AC : Authentication Center
A-Key : Authentication Key
ASE : Application Service Element
AuEx : Authentication Policy Executive
BSPKey : Base Station Partial Key
CSI : Custom Service Interface
DBB : Database Backup
HLR : Home Locaton Register

KDS : Key Distribution Server
MIN : Mobile Identification Number
MSPKey : Mobile Station Partial Key
OAH : Operation & Admin. Handler
OTASP : Over The Air Service Provisioning
QLS : Query Language Server
RQI : Realtime Query Interface
SQL : Standart Query Language

참고문헌

[1] "CELLULAR RADIO COMMUNICATIONS INTERSYSTEM OPERATIONS-Over The Air Service Provisioning(OTASP) PN-3769", April 15, 1997.

[2] "Cellular Radiotelecommunications Intersystem Operations. IS-41-C. TIA/EIA SP-3385, November, 1995.

박 형 일

1994년 연세대학교 전자공학과
1996년 연세대학교 전자공학과 (석사)
1998년 현재 삼성전자(주) 주임연구원
HLR Application 개발

강 지 훈

1990년 고려대학교 전자공학과
1992년 고려대학교 전자공학과 (석사)
1998년 현재 삼성전자(주) 선임연구원
HLR Application 개발