Journal of Korea Multimedia Society Vol. 7, No. 2, February 2004(pp. 211-222)

IMT-2000 서비스에 적합한 PKI 기반 시점확인 서비스에 관한 연구

이덕규†, 이임영††

요 약

무선 이동 통신의 발전으로 인해 많은 사용자가 증가하였다. 1세대나 2세대의 경우 이동통신서비스는 기본적으로 음성과 문자를 기반으로 서비스를 하였기 때문에 멀티미디어 서비스와 같은 고속 무선 인터넷 통신 수요자의 요구를 충족시키지 못하였다. 하지만 최근에는 음성위주의 서비스가 아닌 고용량의 데이터와 멀티미디어 서비스, 위치 기반 서비스 등을 제공하고 있다. 서비스와의 발달과는 다르게 보안상에서는 문제점을 가지고 있다. 무선망은 전송로가 노출되어 있어 정당하지 않는 사용자에 의한 불법적인 절취 사용과 도청 등에 많은 문제점이 발생할 수 있다. 이와는 다르게 서비스 측면에서도 문제점이 발생할 수 있다. 이러한 예로 다음을 들 수 있는데, 악의적인 제 3의 사용자가 공유되어 있는 문서 접근에 따른 문제점이 발생할 수 있으며, 양자간의 계약 혹은 과금 정보에 있어 악의적인 행위가 발생될 수 있는데 이에 대한 행위를 막을 방법이 필요하다. 위와 같은 악의적인 행위에 대한 해결책으로써 문서에 대한 내용증명과 시점확인이 필요하게 된다. 이에 본 논문에서는 악의적인 행위나 문제점을 해결하고자 유선에서 사용 중에 있는 시점확인 서비스 혹은 내용 증명 서비스를 향후 발전할 IMT-2000에 적용하여 보았다. 제안한 방식은 IMT-2000의 기반 구조를 그대로 이용하면서 데이터의 보안에 있어 효율적인 방식을 제안하였다.

A Study on Time Conviction Based on PKI for Suitable IMT-2000 Service

Deok-Gyu Lee†, Im-Yeong Lee††

ABSTRACT

By development of wireless mobile communication, many users increased. But, in case of 1st generation or 2nd generation, transfer communication service was not satisfying high speed wireless internet Communication consumer's request such as other multimedia service because serviced based on voice and text basically. Can get through service such as data and transfer multimedia service that is not service of voice putting first in wireless hereafter. Problems by much development of service are happening, because a transmit is exposed, problem point that wireless network is much unlawful stealing use and tapping etc. As is different from this, problem can happen in service side. Can take next time for these example. By user that is not right can happen. Need method to keep away purpose that is enemy of third party in contract between both men as well as problem for document or accounting information which the third user that is enemy of third party is shared. By solution about problems, certification of contents for document and visual point confirmation must it. Applied service or certification of contents service that is rapidly point of time that is using in wire to solve problem that refer in front in this treatise in IMT-2000 to develop hereafter. Way to propose proposed efficient way using individual in IMT-2000 just as it is.

Key words: IMT-2000, Time Conviction, PKI(IMT-2000, 시점확인, 공개키기반구조)

※ 교신저자(Corresponding Author) : 이덕규, 주소 : 충청남도 아산시 신창면 읍내리 646(336-745), 전화 : 041)542-8819, FAX : 041)530-1548, E-mail : hbrhcdbr@sch.ac.kr
접수일 : 2003년 5월 30일, 완료일 : 2003년 7월 28일
† 순천향대학교 대학원 전산학과 박사과정
†† 종신회원, 순천향대학교 정보기술공학부 부교수
(E-mail : imylee@sch.ac.kr)

1. 서 론

이동 통신은 1 세대와 2 세대를 거치면서 비약적인 발전을 거듭하였으며 많은 사용자가 증가하였다. 1 세대와 2 세대 이동통신서비스는 기본적으로 음성과 문자 위주의 서비스를 염두에 두고 개발하였기 때문에 이동 멀티미디어 서비스와 같은 고속 무선

인터넷 통신 수요자의 요구를 충족시키지 못하고 있다. 하지만 최근에는 음성위주의 서비스가 아닌 데이터와 이동 멀티미디어 서비스 등 여러 서비스를 제공하고 있는 실정이다. 이러한 이동통신서비스는 시간과 장소의 제약을 받지 않고 음성 및 데이터 서비스를 제공하는 편리함을 가지고 있는 반면에 사용자가 이동성을 가지고 있고 전파를 통신 매개로 이용하는 특성으로 인하여 보안상의 취약점을 가지고 있다.[7]

제 3 세대 이동 통신 시스템인 IMT-2000의 특징은 현재 유선 망에서 제공하고 있는 서비스의 대부분을 무선망에서도 지원할 수 있게 하면서 무선망에서도 유선 망에서의 품질을 보장한다는 목표를 가지고 있다. 하지만 무선망은 전송로가 노출되어 있어서 정당한지 않은 사용자가 불법적인 절취사용을 할 수 있으며, 악의를 가진 제 3자가 공유된 전송매체를 통해 전파를 도청하기 쉽다는 문제점을 가지고 있다.

위의 경우를 살펴보면 전자의 경우에는 악의적인 공격자가 아닌 사용자에 의해 행해지는 악의적인 행동이며, 후자의 경우에는 실제적인 악의적인 공격자에 의해 발생되는 경우이다. 만약 양자간에 계약에 있어 실제 계약을 맺는 사용자가 악의적인 목적을 가지고 계약을 맺는 경우에 대하여 차단할 수 있는 방법이 필요하다. 이를 해결하는 방법으로는 공증기관을 두어 사용자들 사이에 공증기간을 두어 내용증명과 시점 확인 서비스가 있을 수 있다. 또한 위와 같은 서비스는 사용자간뿐 아니라 사용자와 서비스 제공 업체와도 연결되어 과금 증명에 사용될 수 있어야 할 것이다.

본 논문에서는 유선에서 무선으로 서비스가 증대되면서 유선에서 제공되고 있는 서비스를 IMT-2000에서 적용하여 내용 증명과 시점 확인 서비스를 가능하게 함으로써 사용자의 이동성을 증대시키는 이점을 확보할 수 있다. 하지만 현재 IMT-2000 개발 상황을 고려할 때 시스템이 완벽하게 구축되지 않은 상태에서 전체적인 관점으로 서비스의 체계와 전체적인 서비스를 살펴보는 것은 불가능하다. 현재 제공되고 있는 CDMA 1X EVDO(Evolution-Data Optimized)와 같은 경우 IMT-2000과 2세대의 중간의 형태로 보는 관점과 IMT-2000의 서비스를 제공하는 관점에서 IMT-2000으로 보는 관점으로 나눠져 있다. 이러한 관점들 때문에 아직도 정확한 IMT-2000이라 할 수 없을 것이다. 하지만 IMT-2000은 전체적으로 유선에서 제공하고 있는 서비스를 제공하고자 하는 것이 목적이다. 유선의 서비스를 무선에서 제공하겠다는 IMT-2000의 전체적인 목적을 기반으로 하여 본 논문에서 제안방식을 서술하도록 하겠다.

본 방식에서 사용되는 시점 확인 서비스는 앞으로 사용자들이 유선에서 벗어나 무선으로 이동하는 시점에서 유선에서 사용하였던 거래나 이체를 무선에서도 이용할 수 있도록 하는데 있다. 서비스들이 무선으로 이동하는 상황에서 무선이 가지고 있는 취약점을 시점확인과 같은 서비스로써 보완할 수 있다. 위와 같은 상황과 같이 이체나 거래시에 무선에서도 안전하고 효율적으로 IMT-2000상에서 사용할 수 있는 시점확인 서비스를 제안하도록 한다.

본 논문의 2장에서는 IMT-2000에 대한 개요 및 보안 요구사항에 관하여 설명하고, 3장에서는 공증서비스 개요에 대하여 살펴본다. 이를 바탕으로 4장에서는 IMT-2000에서 적용될 수 있는 시점 확인 서비스를 제시한다. 그리고 5장에서는 제안방식에 대하여 분석하고 결론을 내리도록 하겠다.

2. IMT-2000 개요 및 보안 요소

2.1 IMT-2000 개요

GSM(Global System for Mobile Communication)이나 IS-95 CDMA(Code Division Multiple Access) 시스템과 같은 2세대 이동 통신 시스템과 비교하여, 진보된 3세대 방식인 IMT-2000 시스템은 고속의 멀티미디어 서비스 제공 및 글로벌 로밍을 특징으로 한다.

이러한 이동 통신 환경의 변화는 정보보호에 대한 대책을 절실히 요구하고 있고, 또한 정보보호 기술도 새로운 환경 변화에 맞추어 발전해야 한다. 이에 부합하여 IMT-2000의 발전을 주도하고 있는 지역 그룹인 3GPP(3rd Generation Partnership Project)와 3GPP2(3rd Generation Partnership Project2)에서는 각각 자신들의 기술에 맞는 표준화 작업을 진행 중이다. 특히, 비동기 방식 표준을 제정하고 있는 3GPP는 ETSI(Europe Telecommunication Standard Institute), ARIB(Association of Radio Industries and Business), TTA(Telecommunication Technology Association), TI(T1 Committee), TTC(Telecommunication Technology Committee)로 구성되어 있고 여러 작업 그룹에서 활발한 활동을 보이고 있다.

보안 아키텍처, 인증 메커니즘, 암호 알고리즘 등과 같은 정보보호와 관련해서는 3GPP의 TSG SA WG3(Technical Specification Group Service and system Aspect Working Group 3)에서 담당하고 있다.

IMT-2000에서 보안을 제공하기 위한 구조를 그림 1에 나타내었다.[1-5] 그림 1에서는 다섯 가지의 보안 관련 부분을 정의하였으며, 각각의 부분은 다음과 같다.

① 네트워크 액세스 보안 : 3G(3rd Generation) 서비스에 대한 안전한 접근 및 radio link 상에서 제3자의 공격을 방지하는 기능을 제공한다.

② 네트워크 도메인 보안 : 네트워크의 유선구간에서 전송되는 정보의 보호 및 signaling 정보에 대한 보호를 제공한다.

③ 사용자 도메인 보안 : MS(Mobile Station)에 안전하게 접근하는 부분을 제공한다.

④ 어플리케이션 도메인 보안 : 사용자와 Serv ice provider domain에서 안전하게 메시지가 전송되도록 하는 기능을 제공한다.

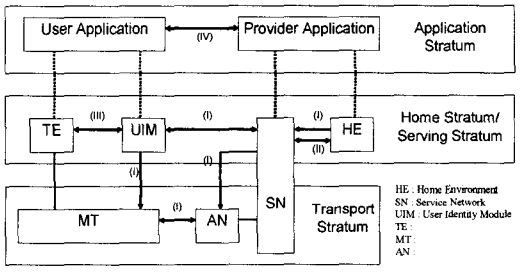


그림 1. IMT-2000 보안 구성도

2.2 3GPP 인증 메커니즘

2.2.1 인증 개요

3GPP에서의 가입자 인증은 USIM(Universal Subscriber Identity Module)과 AuC(Authentication Center)가 같은 비밀키를 소유하고 있음을 증명함으로써 이루어진다. VLR(Visitor Location Register)은 서비스를 제공하기 전에 가입자를 인증하기 위해 HLR(Home Location Register)/AuC에 의해서 생성된 AV(Authentication Vector)를 사용한다. 인증이 성공하면 VLR과 MS는 보안 모드에서 사용하는 CK(Ciphering Key)와 IK(Integrity Key)를 공유한다. 그리고 VLR은 KSI(Key Set Identifier)의 값을 바탕으로 AKA(Authentication and Key Agreement) 절차의 생략 유무를 결정한다.[4-6]

3GPP 인증 메커니즘에서 전송되는 메시지를 간단하게 기술한 것이다. 초기 전송되는 값(Initial L3)에 대하여 AKA 과정을 거쳐 마지막으로 보안 모드 협상 단계(Security Mode Command)를 거치게 된다. 자세한 과정은 아래의 과정과 같다.(그림 2 참조)

① 먼저 MS는 Initial L3 메시지를 MM(Mobility Management) 연결과정에서 VLR로 전송한다.

② 실제로 AKA 과정이 일어나기 전에 MS와 RNC (Radio Network Controller) 사이에는 RRC(Radio Resource Control) 연결 설정이 일어난다. 이때 MS는 사용할 암호 알고리즘과 무결성 알고리즘 등을 RNC에 전송한다.

③ Initial L3 메시지에는 사용자 ID, KSI, LAI(Location Area Identification)를 포함하고 있어서 VLR은 KSI 값을 가지고 AKA의 수행여부를 판단한다. 이것과 관련해서 이전 가입자 방문망(VLRo)과 새로운 가입자 방문망(VLRn) 사이에는 ID(Identification) 확인 절차가 일어날 수도 있다.

④ AKA가 수행된다면 VLR은 HLR/AuC에게 AV 생성을 요구한다.

⑤ 인증이 성공하면 보안 모드(Security Mode) 협상 단계로 들어간다.

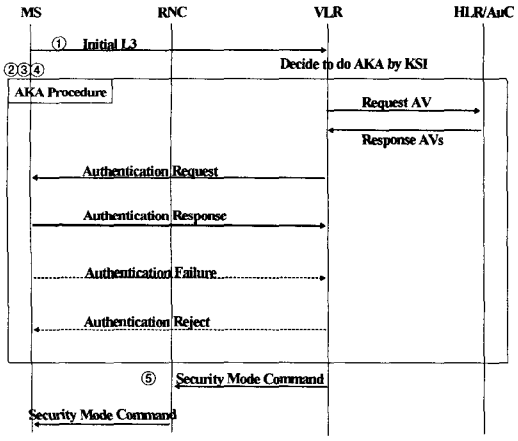


그림 2. 3GPP 인증 메커니즘

2.2.2 인증과 보안 관련 절차

본 절에서는 각각의 인터페이스에서의 인증 절차

에 관해서 좀더 구체적으로 살펴본다. 우선 VLR과 HLR/AuC 구간에서의 AKA에 대하여 살펴본 후, MS(Mobile Station)와 VLR 구간에서의 AKA, 이전 방문지로부터의 IMSI(International Mobile Subscriber Identity)와 인증 데이터 분배 마지막으로 보안모드 Setup 절차에 대하여 알아보도록 하겠다.

2.2.2.1 VLR과 HLR/AuC 구간에서의 AKA

만약 VLR(Visitor Location Register)이 사용자를 인증 하는데 필요한 AV(Authentication Vector)가 없다면 VLR은 HLR/AuC에 새로운 AV를 요구하게 된다. 여기서 필요한 AV는 MS의 인증과정에 필요한 사항으로 보안모드에 들어가기 전에 인증과 키 동의 과정을 거치기 때문이다. 따라서 VLR에 AV가 없다면 AV에 대한 요구로써 HLR/AuC에 요구 메시지를 전송하며 이에 응답으로 AV를 전송 받게된다. 전송되는 메시지는 node identity, node type과 IMSI를 포함하는 메시지를 보내고, HLR/AuC은 이에 응답해서 인증벡터를 생성한 다음 VLR에 전송한다.

2.2.2.2 MS와 VLR 구간에서의 AKA

이 구간에서의 AKA의 목적은 MS와 VLR이 인증을 하고, 새로운 CK(Cipher Key), IK(Integrity Key)를 설정하는데 있다. 먼저, VLR이 RAND(Random Number), AUTN(Authentication Token), KSI를 포함하는 Authentication Request 메시지를 MS에 보내면 MS는 AUTN을 구성하는 요소 중 하나인 MAC(Message Authentication Code)과 자신이 계산할 수 있는 XMAC(Expected Message Authentication Code)을 비교한다. 만약 두 개의 결과가 다르다면 MAC 실패에 대한 이유와 함께 Authentication Failure 메시지를 VLR에 전송하고, 같다면 MS는 USIM에 생성한 SQN_{MS}(Sequence Number)와 AUTN의 또 다른 한 요소인 SQN과 비교한다. SQN이 올바른 범위 내에 있는지를 판단하여, 단말기의 네트워크에 대한 인증 성공 응답 메시지인 Authentication Response 메시지를 전송하거나, SQN 범위의 실패에 따른 Authentication Failure 메시지를 VLR에 전송한다. 만약 SQN이 올바른 범위 내에 있지 않으면, MS는 AUTS(Authentication Synchronization Failure Parameter)를 계산하고, 그것을 Authentication Failure와 함께 보낸다. 한편, MS가 네트워크를 인증 하면 응답으로 RES(Response)를 계산하는데 이는 Authentication Response 메시지와 함께 VLR로 전송이 되어서 VLR이 가지고 있는 XRES(Expected Response)와 같은지를 비교할 수 있게 한다. 이 비교로 네트워크는 단말기에 대한 인증을 성공해서 인증 절차를 완료하거나, 인증 실패에 따른 Authentication Reject 메시지를 MS에 전송한다.

2.2.2.3 이전 방문망으로부터의 IMSI와 인증 데이터의 분배와 Identification 절차

이 절차는 동일한 SN(Serving Network) 내에서 이전 방문망인 VLRo에서 새로운 방문망인 VLRn으로 인증 데이터를 제공할 때 발생한다. VLRn은 TMUI(Temporary Mobile User Identity)와 LAI를 포함하는 Initial L3 메시지를 MS로부터 받자마자 VLRo로 TMSI를 확인하기 위한 메시지를 전송한다. VLRo는 TMSI와 관련된 정보를 자신의 데이터베이스에서 찾아서 남아있는 CK, IK 등을 VLRn에게 전송하거나, 혹은 TMSI 확인 실패 메시지를 전송한다. 바로 위에서 언급한 TMSI를 사용한 Identification 확인 절차가 실패할 경우, VLRn은 IMSI를 이용하여 MS와 Identification 확인을 하게된다.

2.2.2.4 보안 모드 setup 절차

AKA가 성공적으로 완료되거나, KSI 확인으로 인한 AKA가 생략되면 보안 모드 협상 절차를 하게된다. 이 과정에서 사용할 암호 알고리즘을 선택하는 등 MS와 RNC 사이의 많은 협상 과정을 하게 되지만, 본 논문의 주제와는 약간 거리가 있으므로 상세히 다루지는 않는다. 하지만 signalling 메시지에 대한 무결성 체크를 하는 것은 필수적이다.

3. 시점확인 서비스 개요 및 기존 방식

3.1 시점확인 서비스 개요 및 요구사항

실세계의 상거래뿐만 아니라 네트워크상의 상거래에서 정상적인 거래가 행해지고 있는 동안은 특별히 문제가 없지만 거래상의 문제가 발생한 경우를 대비하여 취할 수 있는 조치가 확립되어야 한다.[17]

예를 들면, 거래 상대방의 확인(거래자격 확인), 거래내용의 문서화(계약서, 수발주 문서, 각서 등)을 취할 수 있는 방법이 강구되어야 한다.

이러한 공증서비스(notary service)에 시점확인

서비스가 포함되면 시점확인 서비스는 공증 서비스가 갖는 요구사항을 모두 만족하여야 한다. 공증 서비스의 경우 공증인의 참관 아래 이뤄지며, 시점확인 서비스는 시점을 확인 할 수 있는 기능을 포함하며, 공증인의 참관보다는 시점 확인에 초점을 둔다.

실세계에서는 상대편 확인을 위하여 인감 증명서, 상업 등기부등본 등으로 그 정당성을 확인할 수 있고, 이들 서류에 관해서는 공문서로서의 법적 뒷받침이 있다. 또한 이미 거래가 있는 경우는 대면, 전화 등을 통해 상대방의 확인이 가능하다.

이와 같이 네트워크상에서의 전자 상거래인 경우 제 3자로부터의 위협 해결이 전제인 동시에 거래 당사자간의 신뢰성을 확보하는 것이 필수 요소이다.

이제 전자 공증이란 네트워크상의 상거래 등에서 누가, 무엇을, 언제 전자적인 교환을 행했는지를 증명함으로써 전자적인 교환의 안전, 신뢰성을 확보하는 개념으로 정의된다. 즉, 전자 공증은 거래 당사자간의 신뢰성을 유지하고, 안정적인 거래 실현의 중심적 역할을 담당하여 거래 문서에 대한 증거력을 높이고 분쟁의 방지나 해결에 유효한 수단을 제공한다. 전자 공증의 기능은 송수신자 특정, 도달확인, 개조 검출, 시각 부여 전자 보존, 접근 기록, 프로세스 기록 등이 있다.

이에 대한 전자 공증의 요구사항은 다음과 같이 들 수 있으며, 시점 확인에서의 요구사항과 동일하다.

(1) 인증(Authentication) : 누가, 언제 누구에 대하여 어떠한 내용의 정보를 제공했는지 제 3자가 증명하도록 하기 위해 인증을 해야한다.

(2) 무결성(Integrity) : 당사자간의 전달되는 내용이 알려지지 않아야 하며 전달 도중에 변경되지 않아야 한다.

(3) 배달증명(Certification of Delivery) : 송신자의 디지털 정보가 틀림없이 수신자에게 배달된 것을 확인할 수 있어야 한다.

(4) 판독성(Legibility) : 데이터의 내용을 필요에 따라 판독가능하게 하는 것을 의미한다.

(5) 보존성(Preservability) : 보존기간 내에서 복원 가능한 상태로 데이터를 저장되어야 한다.

(6) 시간성(Time-Symmetric) : 정보에 일자/시간 데이터를 부가하거나, 부가된 일자/시간 데이터가 정확한지를 조사할 수 있어야 한다.

(7) 책임성(Authenticity) : 책임성의 가장 중요한 요소는 안전성의 추구이며, 운영에 관한 책임을 명백히 보이고 드러내는 것이 요구된다.

3.2 기존 방식

다음은 유선 상에서 사용되는 공증과 시점확인 서비스이다. 기존 유선에서의 공증 및 시점확인 서비스를 살펴본 후 이를 토대로 IMT-2000에서 안전하고 효율적인 시점 확인 서비스에 대해 살펴보도록 한다.

3.2.1 Notary 2.0

Entegrity사에서 제공되는 공증서비스는 PKI (Public -Key Infrastructure) 구조에 기반을 둔 완전한 디지털 인증서 관리 시스템이다. 이구조는 Top CA(Cetrificate Authority)로부터 사용자까지 스마트를 이용한 인증 계층구조를 지원한다. 이 Entegriry사의 Notary 2.0 서비스는 다음과 같은 특징을 갖는다.

- 새로운 공증 관리스 시스템을 제공한다. 관리자 인터페이스의 사용이 용이하고 안전하며, 사용자 추가 삭제, 변경 및 인증서의 폐지, CRM에 보관할 수 있다.

- 새로운 공증 고객 패키지를 제공한다. 이러한 패키지는 설치와 사용이 용이하며, 사용자의 키쌍 생성을 돕는다.

Entegrity사에서 제공되는 공증서비스는 기본적으로 PKI 구조를 따른다. Top-CA를 근원 CA로 두고, 하부의 각 CA는 계층구조로 구성되며, 상위계층의 CA는 하위계층의 CA에 대한 공증용 인증서를 발급한다. 각 CA는 상호 인증 기능이 제공되며, 타 기관 시스템과의 상호 인증 기능도 제공한다. 이 시스템의 공증기관은 CA의 기능과 RA의 기능을 모두 수행하는데, CA의 기능으로써 하위 기관에 대한 인증서 발급, 인증서 폐기, CRL의 주기적 발행, 발급된 인증서와 CRL에 대한 DB관리, 인증서와 CRL의 분배 등을 수행하고, RA의 기능으로써 사용자 등록, 사용자에 대한 키 쌍 발급, 키와 디지털 인증서의 보관, 사용자 공개키에 대한 인증 요구 등을 수행한다. (그림 3 참조)

3.2.2 Digital Notary Record Authentication

Surety사는 기존의 공증 서비스 제공업체와 연계

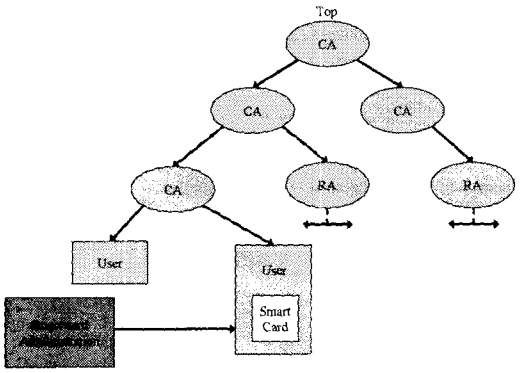


그림 3. Entegrity사의 전자공증 시스템 모델

하여 디지털 공증 기록 인증 서비스(Digital Notary Record Authentication)를 제공한다. 이 서비스는 매초 단위로 발생되는 여러 사용자들의 공증 기록 데이터를 효과적으로 보관하기 위한 방법으로서, 해쉬 알고리즘을 사용하여 각 문서에 대한 디지털 지문(Digital Fingerprints)을 작성·보관한다. 매초 단위의 기록보관 방법은 다음 그림 4와 같다.[18]

① Level 2에서는 매초 단위로 발생되는 각 사용자들의 문서를 각각 해쉬 알고리즘을 이용하여 128bit의 해쉬값을 생성한다.

② Level 1에서는 Level 2에서 생성된 각 문서의 해쉬값을 연결하여 576bit로 만든 다음, 이를 다시 해쉬 알고리즘을 통하여 288bit의 결합 해쉬값을 형성한다.

③ Level 0에서는 Level 1에서 생성된 해쉬값들을 연결하여 576bit로 만든 다음, 이를 다시 해쉬 알고리즘을 통하여 288bit의 결합 해쉬값 RHV(Root Hash Value)를 생성한다.

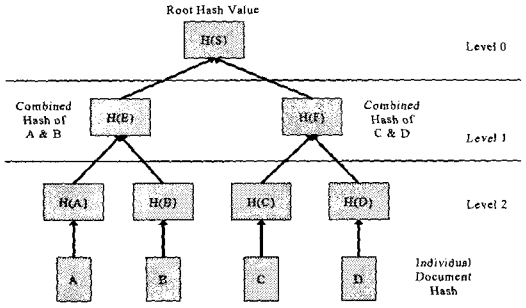


그림 4. Surety사의 매초 당 RHV 생성 방법

이러한 방법으로 매초 당 1개의 RHV를 생성한 다음, 이 RHV들을 다시 연결한 다음, 해쉬 알고리즘을 통해 288bit의 SHV(Supher Hash Value)를 생성한다.

4. IMT-2000 상에서의 시점확인 서비스

본 장에서는 앞에서 살펴본 것과 같이 IMT-2000 상에서의 취약점을 안전하고 효율적인 방법으로 보안하며, IMT-2000의 요구사항인 기존 유선의 서비스가 무선상에서 동일한 품질로 제공될 수 있도록 IMT-2000환경에서 적용 가능한 PKI기반에서의 시점확인 서비스 구조를 제안한다.

4.1 구성요소

다음은 본 방식에서 사용되는 구성요소를 기술하고 있다. 그림 5에서는 전체 구성도를 도식하고 있다. 본 방식에서 사용되는 구성요소는 USIM(Universal Subscribe Identity Module), ME(Mobile Equipment), SN(Service Network), AuC(Authentication Center)로 구성되며 각각의 특징은 다음과 같다.

• AuC/HLR : Authentication Center 혹은 Home Locater Register 로써 사용자에게 공개키 인증서를 송신한다.

• NA : Notary Authority로써 AuC로부터 통신 요청이 완료되면 NA는 AuC로부터 키를 받게되며 이를 바탕으로 세션키를 생성하게 된다.

• SN/VLR : Service Network 혹은 Visitor Locator Register로써 ME_0과 ME_1이 암호화 통신을 할 때 SN에 암호화된 내용이 저장된다.

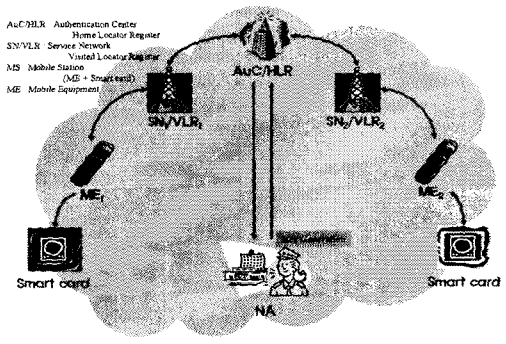


그림 5. 제안 방식 전체 구성도

• ME : Mobile Equipment로 다른 MS에 통신을 요청하며 NA로부터 받은 Key를 USIM에 저장하는 역할을 한다.

• USIM : Universal Subscriber Identity Module으로 Key를 저장한다.

4.2 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수이다.

• C_{Key} : AuC에서 생성하는 Key

• N_{Key} : NA에서 생성하는 Key

• E_{Key} : ME간에서 사용될 세션키

• * : 참여개체(ME: Mobile Equipment, AuC: Authentication Center, NA: Notary Authority)를 가르키는 지시자

• ID_* : Identity

• H() : Hash Function

• PK_*, SK_* : *의 공개키 및 개인키

• Sig_{AuC}, Sig_{ME0}, Sig_{ME1} : AuC의 서명 및 ME_0, ME_1의 서명

• TS_{ME0}, TS_{SN}, TS_{AuC} : ME_0, SN, AuC의 Time-Stamp

• Res : Response 값

4.3 제안 방식

그림 6은 제안방식의 프로토콜을 개괄적으로 나타낸 것이다. 개략적으로 전체 프로토콜은 통신요청, 키 전송 및 키 분배, 메시지 제공의 3단계로 이루어지며, 통신 요청 단계는 ME_0에 의해서 통신이 시작되는 시점이며, 통신 요청에 대한 완료 메시지가 전달되면 AuC가 키를 생성하여 ME_0와 ME_1에게 제공하며 이 키를 바탕으로 하여 메시지를 전송하게 된다. 만약 후에 메시지에 대하여 이상한 행위가 발견되면, 시점확인 서비스 과정을 거치게 된다.

다음은 그림 6을 바탕으로 자세한 프로토콜을 기술한다.

1) 통신 요청 단계

다음은 본 방식에서 처음으로 통신하기 위해 필요한 요청과 응답에 대하여 기술하고 있다. 초기 사용자들이 시점확인 서비스를 받기 위해 상대방에 대한 통신 요청과 통신 수락 단계를 기술한 것으로 일반적인 요청 단계로 표현한다. 초기에 AuC를 통하여 각 사용자는 인증과정을 거친 것이며, 다시 인증 과정을 거칠 필요가 없이 AuC의 인증을 통해 서비스를 실시하게 된다.

① ME_0은 ME_1과의 통신을 SN_0에 요청한다.

② SN_0은 AuC에 ME_1의 위치를 요청한다.

③ AuC는 SN_1에게 SN_0의 정보와 ME_1의 통신을 요청한다.

④ SN_1은 ME_1에게 ME_0의 통신을 요청을 확인한다.

⑤ ME_1은 통신 확인에 대한 응답을 한다.

⑥ SN_1은 응답에 대한 결과를 AuC에 전송한다.

⑦ AuC는 요청에 대한 응답을 SN_0에 전송하면 마지막으로 SN_0은 ME_0에 응답을 전송한다.

2) 키 생성 단계

다음은 본 방식에서 메시지 암호화 및 시점 확인을 위해 필요한 키 생성에 대하여 기술하고 있다. 본 단계에서 필요한 키는 시점확인 서비스를 제공받기 위한 키이며, 제공되어진 키를 이용하여 후에 시점확인, 내용증명 등 다양한 지원을 받게 된다.

① AuC는 통신 요청 단계의 ⑥ 단계가 완료되면

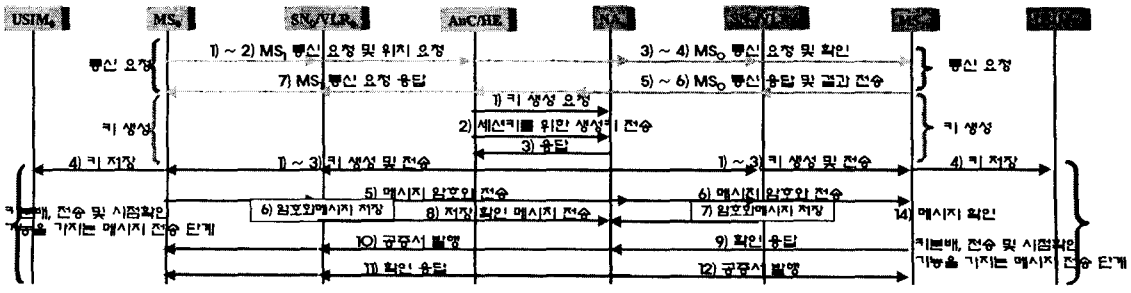


그림 6. 제안 방식 상세 프로토콜

ME_0과 ME_1과의 통신 요청이 올바르게 되었음을 알리고 키 생성 요청을 한다.

② AuC는 C_{Key}(식 (1))을 생성하여 키의 서명값을 암호화 정보(식 2)를 Notary Authority에 전송한다.

$$AuC/He \rightarrow NA:\ C_{Key} = H(ID_{AuC}||ID_{ME_0}||ID_{ME_1}||SK_{AuC}) \quad (1)$$

$$PK_{NA}(C_{Key}||Sig_{AuC}(H(C_{Key}))) \quad (2)$$

③ NA는 AuC의 C_{Key}(식 (1))전송에 대한 응답을 한다.

이로써 통신 요구 단계에 키 분배 단계까지 완료한다.

3) 키 분배, 전송 및 시점확인 기능을 가지는 메시지 전송 단계

다음은 본 방식에서는 키 분배 단계를 거쳐 메시지 전송 단계에 대하여 기술하고 있다 본 단계는 AuC와 NA로부터 생성한 키를 NA가 전송 받은 키를 이용하여 송신하고자 하는 사용자가 자신의 메시지를 암호화하여 시점확인을 위한 타임 스템프를 첨부하여 전송하면 중간에 있는 각각 사용자의 SN이 메시지를 보관한다. 후에 이에 문제가 발생했을 경우 사용자의 요청에 의해 시점확인 혹은 내용증명 서비스를 진행한다.

① NA는 AuC로부터 받은 C_{Key}(식 (1))을 이용하여 N_{Key}(식 (3))과 Key(식 (4))를 생성한다.

$$N_{Key} = H(ID_{NA}||SK_{NA}) \quad (3)$$

$$Key = H(ID_{ME_0}||ID_{ME_1}||C_{Key}||N_{Key}) \quad (4)$$

② NA가 생성한 Key를 각 ME_0와 ME_1에 제공할 식 (5)과 식 (6)을 SN_0과 SN_1에 전송한다.

$$NA \rightarrow SN_0:\ PK_{ME_0}(ID_{ME_0}||Key||Sig_{AuC}(ID_{ME_0}||Key)) \quad (5)$$

$$NA \rightarrow SN_1:\ PK_{ME_1}(ID_{ME_1}||Key||Sig_{AuC}(ID_{ME_1}||Key)) \quad (6)$$

③ 다시 SN_0과 SN_1은 ME_0과 ME_1에 식 (5)와 식 (6)을 전송한다.

④ ME_0와 ME_1은 받은 Key를 USIM에 저장한다.

⑤ ME_0는 메시지 M을 Key로 암호화하여 다음을 전송한다.

$$ME_0 \rightarrow SN_0:\ E_{Key}(ID_{ME_0}||M||TS_{ME_0}Sig_{ME_0}(H(ID_{ME_0}||M||TS_{ME_0}))) \quad (7)$$

⑥ SN_0는 전송 받은 식 (7)을 저장한 후, SN_1에 전송한다. SN_0는 저장할 때 자신의 비밀키로 타임 스탬프를 첨부하여 보관한다.

$$SN_0 \rightarrow SN_1:\ Sig_{SN_0}(E_{Key}(ID_{ME_0}||M||TS_{ME_0}Sig_{ME_0}(H(ID_{ME_0}||M||TS_{ME_0})))||TS_{SN_0}) \quad (8)$$

⑦ SN_1 또한 전송 받은 식 (7)을 저장한 후, ME_1에 전송한다. SN_1 또한 타임 스탬프를 첨부하여 보관한다.

$$SN_1 \rightarrow ME_1:\ Sig_{SN_1}(E_{Key}(ID_{ME_0}||M||TS_{ME_0}Sig_{ME_0}(H(ID_{ME_0}||M||TS_{ME_0})))||TS_{SN_1}) \quad (9)$$

⑧ SN_1은 저장 후 확인 메시지를 NA에 발송한다.

⑨ ME_1은 전송 받은 식 (7)을 확인한 후 SN_1에 확인 응답을 발송한다.

$$E_{Key}(ID_{ME_0}||RES, Sig_{ME_1}(ID_{ME_0}||RES)) \quad (10)$$

⑩ SN_1은 SN_0에 발송하고 다시 SN_0는 ME_0에 응답 메시지를 발송한다.

⑪ ME_0는 응답 확인 메시지를 발송하고 모든 과정을 마친다.

5. 제안 방식 분석

다음은 제안한 방식에 대한 시점 확인 및 증명 단계와 제안 방식의 여러 가지 보안 사항에 대한 분석을 하였다.

5.1 시점확인 및 내용 증명 단계

다음은 본 방식에서 시점에 대한 확인 단계에 대해 기술하고 있다. 본 단계는 사용자가 어떠한 이유에 의해 메시지가 변조되었을 경우 사용자는 NA에 요청하여 시점확인 및 내용 증명에 대한 확인을 받을 수 있다. 이 경우 사용자 모두 혹은 한 사용자에 의해 요청되어 질 수 있다. 최종 변조에 대한 책임은 NA에 부가된다.

① 메시지에 불확실성 확인은 ME의 요청에 의해 이루어진다.

② 사용자로부터 불확실성에 대한 요청이 접수되면 NA는 AuC에게 C_{Key}(식 (1))를 요청한다. AuC로부터 전송되어온 C_{Key}와 N_{Key}(식 (3))를 이용하여 Key(식 (4))를 생성하여 메시지가 저장되어 있는 각 SN에게 Key(식 (4))를 전송한다.

$$AuC \rightarrow NA: C_{Key} = H(ID_{AuC} || ID_{ME_0} || ID_{ME_1} || SK_{AuC}) \quad (1)$$

$$N_{Key} = H(ID_{NA} || SK_{NA}) \quad (3)$$

$$Key = H(ID_{ME_0} || ID_{ME_1} || C_{Key} || N_{Key}) \quad (4)$$

③ 각 SN들은 전달되어진 Key를 이용하여 복호화 한다. 사용자들은 각 SN에 저장되어진 SN의 TS (Time-Stamp)를 이용하여 전송 시간과 내용 증명 확인을 받을 수 있다.

$$SN_0 \rightarrow SN_1: \ Sig_{SN_0}(E_{Key}(ID_{ME_1} || M || TS_{ME_0} Sig_{ME_0}(H(ID_{ME_1} || M || TS_{ME_0}))) || TS_{SN_1}) \quad (8)$$

$$SN_1 \rightarrow ME_1: \ Sig_{SN}(E_{Key}(ID_{ME_0} || M || TS_{ME_0} Sig_{ME_0}(H(ID_{ME_0} || M || TS_{ME_0}))) || TS_{SN}) \quad (9)$$

5.2 제안 방식 고찰

본 방식에서는 전송로 상의 불법적인 도청 및 변조는 각 개체의 공개키 혹은 세션키를 이용하여 문제점을 방지하였다.

또한 이러한 문제점이외에 각 개체들이 악의적인 목적을 가지고 다른 개체에 대해 부정을 저지르지 못하도록 되어있다. 사용자와 서버의 담합의 경우 C_{Key}내에 사용자들의 ID와 AuC의 개인키를 해쉬를 취한 값이 되므로 서버에서 만들어 낼 수 없다. 따라서 서버와 사용자의 불법적인 담합은 막을 수 있다. SN이 불법적인 목적을 가지고 있다할지라도 SN이 NA에게서 사용자에게 전달된 키를 알아낼 수 없으므로 SN은 확인에 대한 요구가 있기 전까지 메시지를 확인할 방법이 없다.

시점확인은 시점에 대한 확인 이외에도 SN에 저장되어있는 암호화된 메시지를 이용하여 사용자들 혹은 법행 기관에서 풀어서 내용 증명 서비스를 시행할 수 있다.

표 1은 제안 방식에 따른 분석을 한 것이다. 분석한 결과는 다음과 같다.

각 부분에 대하여 살펴보면 인증은 초기에 AuC를 통하여 서비스가 진행됨으로 AuC에 대한 인증 과정을 거치게 되고 상대방과 통신 요청을 하게 됨으로 AuC와의 인증과정이 올바르다면 당사자간의 인증은 통과된다. 무결성은 당사자간의 서명을 통하여 무결성이 실현되는데 이때 부족한 통신로 상에서의 위협이나 송·수신자의 위협은 HE와 NA에서 생성한 키를 통하여 이를 해결할 수 있다. 또한 SN 각각에 저장되는 배달 증명을 위한 데이터들은 추후에 당사자간의 이견 발생 시 NA와 AuC의 키를 통하여 복호화할 수 있으므로 SN에 저장된 데이터의 분실에 따른 피해를 막을 수 있다. 배달증명은 각 당사자간에 속한 SN에서 확인할 수 있는데 이것은 문서의 배달이 이뤄지고 난 후 각 SN에 저장이 되며 이 저장된 문서는 추후 문제 발생 시 확인 될 수 있다. 판독성은 데이터의 내용에 따라 판독 가능하게 하는 것으로 이것은 데이터의 내용은 당사자간에 알아야 하지만 문제가 발생하였을 경우 당사자의 의뢰에 따라 AuC와 SN이 생성된 키를 사용하여 데이터를 판독할 수

표 1. 제안방식 분석

	제안 방식	분석
인증	기존의 인증체계에 따라 AuC는 각 당사자를 인증	이는 당사자와의 인증을 통하여 또 다시 사용자간의 인증 과정을 줄일 수 있다.
무결성	$E_{Key}(ID_{ME_0} \| M \| TS_{ME_0} Sig_{ME_0}(H(ID_{ME_0} \| M \| TS_{ME_0})))$	전달하는 메시지에 따른 당사자간의 서명과 AuC와 NA에서 생성한 키를 이용하여 암호화
배달증명	$Sig_{SN_0}(E_{Key}(ID_{ME_0} \| M \| TS_{ME_0} Sig_{ME_0}(H(ID_{ME_0} \| M \| TS_{ME_0}))) \| TS_{SN_0})$	배달증명은 SN에 다음과 같은 메시지를 저장하고 필요시에 확인 과정을 통해 TS를 통해 알 수 있다
판독성	$CKey = H(ID_{AuC} \| ID_{ME_0} \| ID_{ME_1} \| SK_{AuC})$ $NKey = H(ID_{NA} \| SK_{NA})$ $Key = H(ID_{ME_0} \| ID_{ME_1} \| CKey \| NKey)$	AuC와 NA를 통하여 생성되는 키를 이용하여 데이터에 대한 판독 가능
시간성	$E_{Key}(ID_{ME_0} \| M \| TS_{ME_0} Sig_{ME_0}(H(ID_{ME_0} \| M \| TS_{ME_0})))$	각 시간성은 전달되는 시점에서 구성 요소마다 TS를 이용하여 비교함으로써 확인
책임성	$CKey = H(ID_{AuC} \| ID_{ME_0} \| ID_{ME_1} \| SK_{AuC})$	Key의 생성 및 전달이 NA에서 이뤄지고 NA의 요청에 의해 AuC의 키를 생성하게 됨으로 인해 책임에 대한 소재는 NA와 AuC에게 책임이 부여된다.

표 2. 기존방식 비교 분석

	인증	무결성	배달증명	판독성	송/수신 부인방지	제출/전달 부인방지
Notary 2.0[17]	△	○	○	○	RA (Rotary Authority)	RA (Rotary Authority)
DNRA[18]	○	△	○	△	사용자	RA (Rotary Authority)
제안방식	○	○	○	○	SN	SN

있다.

보존성은 데이터의 중요도에 따라 SN에 저장되는 기간을 정할 수 있는데 이것은 메시지가 전송될 때 당사자가 정하거나 Time-Stamp를 통하여 정할 수 있게된다. 시간성은 데이터가 언제 전송되었는지 확인하는 것으로 각각의 구성요소를 거칠 때마다 TS (TimeStamp)를 붙임으로써 후에 시간을 근거로 문서의 변경이나 변조되었음을 확인 할 수 있다.

마지막으로 책임성은 운영에 관한 책임을 AuC와 NA가 가지고 있고, SN 또한 AuC와 인증하고 신뢰체계를 가지고 있으므로 당사자간의 불법 외에 모든 책임은 AuC와 NA에서 가진다.

본 제안 방식은 기존 유선 방식과의 큰 차이점은 다음과 같은 것이 있다. 우선 기존 유선에서 제공되고 있는 방식의 경우는 쌍방의 합의하에 공증인을 중간에 위치시켜 양자간의 계약, 이체 등과 같은 서비스에 대해 후에 사건(부인 등)이 발생하였을 경우 공증인의 시점확인등을 통해 부인 봉쇄 서비스를 받는 것을 의미한다. 하지만 본 제안 방식은 기존의 IMT-2000 기반 구조를 이용하고 있기 때문에 특별히 공증인을 배치하지 않아도 기존 환경에서의 인증센터와 공증 센터로 하여금 시점확인 서비스를 제공할 수 있다. 또한 사용자에의한 송/수신 부인방지 및 제출/전달 부인 방지를 위하여 사용자의 타임 스템프를 이용하는 것이 아니라 IMT-2000 기반 구조에서의 SN이 타임 스템프를 제공함으로써 사용자에게서 발생할 수 있는 사건을 해결할 수 있다.

기존 방식과의 제안 방식과 요구사항을 관점으로써 살펴본 결과이다. 그 중에서 제안 방식과 기존방식의 가장 큰 차이점을 보이기 위해 송/수신 부인방지와 제출/전달 부인방지에 대하여 추가적으로 설명하도록 한다.

기존 방식에서의 인증은 사용자간의 인증이 아니라 공증기관에 대한 인증으로써 양자간의 인증을 거친다. 이러한 경우 사용자와 인증기관이 악의적인 목적을 가지고 담합을 했을 경우 문제가 발생한다. 하지만 본 방식에서는 AuC에게 사용자 인증과정을 거치게 되고 시점확인과 같은 서비스는 TA를 통해서 제공받기 때문에 인증에 따른 문제점은 해결할 수 있을것이다. 무결성에 대한 부분은 대부분의 시스템에서 제공하고 있지만 기존 방식인 DNRA와 같은 시스템에서는 해쉬된 데이터를 트리를 이용하여 계속적으로 사용함으로써 무결성을 해칠 수가 있다. 하지만 본 방식에서는 이러한 무결성에 대한 해결책으로써 HE와 NA를 이용하여 해결하였다. 배달증명은 기존 방식 모두 제공하고 있고 제안방식에서도 제공하고 있다. 하지만 제안방식에서의 배달증명의 특징은 기존 방식에서 배달증명을 위해 공증기관을 통해 사용자가 송신 부인 방지, 수신 부인 방지와 같은 인자를 이용한데 반해 제안방식은 IMT-2000 기반 구조를 이용하고 기반 구조에 존재하는 개체를 이용함으로써 배달증명을 실현할 수 있다. 이같은 경우는 시점확인 시버스를 해주는 공증기관으로의 데이터 쏠림을 해결할 수 있다.

마지막으로 판독성의 경우에는 기존 방식의 경우 데이터의 내용을 공증기관이 알 수 있지만 본 제안 방식에서는 사용자의 동의를 얻어 각각 저장되어있는 SN에 접근하여 정보를 획득할 수 있다. 따라서 공증기관 혹은 AuC 단독으로 사용자간의 정보를 볼 수가 없으며, 사용자가 모두 동의를 하는 경우에만 정보에 대한 판독이 가능하다.

송/수신 부인 방지 및 제출/전달 부인방지는 시점확인에 앞서 사전에 요구되는 사항으로 기존방식에서는 모두 시점확인 서비스등을 제공하는 공증기관에서 담당하고 있지만 제안 방식은 사전에 설명한 배달증명에서처럼 IMT-2000 기반 구조의 개체들을 이용하여 제공하게 되므로 공증기관으로의 정보 쏠림을 사전에 예방할 수 있다.

6. 결 론

지금까지 무선 이동 통신은 1세대와 2세대를 거쳐

오면서 많은 서비스가 제공되고 있다. 향후 서비스를 준비하고 있는 3세대에는 많은 멀티미디어 서비스뿐 아니라 여러 가지 많은 서비스를 준비하고 있다. 그 중에서 사용자와 사용자간의 계약의 문제점, 사용자와 컨텐츠 제공자간의 과금에 대한 시간 및 내용에 대한 증명 등 문제점이 발생할 수 있다. 이러한 문제점을 해결하고자 공증기관을 둔 시점 확인 서비스를 제안하였다. 이러한 공증서비스의 시점확인 서비스는 물론 내용 증명 서비스를 제공 할 수 있어 사용자가 기록에 대한 불확실성을 제기한다면, 공증기관으로부터 키를 제공받아 증거의 유효성을 증명할 수 있다. 이러한 시점확인 서비스는 IMT-2000상에서 이뤄질수 있는 전자 지불 및 전자 거래에서 사용 될 수 있을 뿐만 아니라 추후 제공될 서비스에서 사용자간의 정보에 대하여 공증 서비스를 제공할 수 있을 것이다.

본 논문에서는 향후 발전할 IMT-2000 서비스에서 일부의 서비스를 소개하고 있다. 또한 제안 방식은 사용자와 사용자간 사이에 시점확인을 위한 키를 NA를 통해 생성하며, 생성된 키를 이용하여 사용자들은 암호화하게 되며, 생성된 키를 이용하여 시점확인 기능을 제공하는 일련의 프로토콜을 제시함으로써 사용자가 NA에서 안전하게 암호화 통신을 수행할 수 있는 서비스를 제안하였으며 이 서비스를 통해 다양한 응용 서비스를 연계할 수 있는 가능성을 제시하였다.

향후 실생활과 더욱 관련하여 좀 더 효율적이고 통합적인 공증 서비스를 제공할 수 있는 서비스를 연구해야 할 것이다.

참 고 문 헌

[1] 3GPP TS 33.102 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G Security; security Architecture".

[2] 3GPP TS 22.022 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; Personification of UMTS Mobile Equipment (ME); Mobile functionality specification".

[3] 3GPP TS 33.103 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; integration Guidelines".

[4] 3GPP TS 33.105 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; Cryptographic Algorithm Requirements".

[5] 3GPP TS 33.120 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; Security Principles and Objectives".

[6] 3G TR 33.901 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; Criteria for cryptographic algorithm design process".

[7] 3G TR 33.902 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; Formal Analysis of the 3G Authentication Protocol".

[8] 3G TR 33.908 : "3rd Generation Partnership Project(3GPP); Technical Specification Group Services and System Aspects; 3G security; General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms".

[9] ETSI SAGE : "Security Algorithm Group of Experts(SAGE); General Report Design, Specification adn Evaluation of The MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions".

[10] ESTI SAGE : "Specification of the MILENAGE Algorithm Set: an Example Algorithm Set for the 3GPP Authentication and Key Generation Functions $f1, f1^*, f2, f3, f4, f5$ and $f5^*$". Document 1 : Algorithm Specification.

[11] ESTI SAGE : "Specification of the MILENAGE Algorithm Set: an Example Algorithm Set for the 3GPP Authentication and Key Generation Functions $f1, f1^*, f2, f3, f4, f5$ and $f5^*$". Document 2 : Implementers' Test Data.

[12] ESTI SAGE : "Specification of the MILENAGE

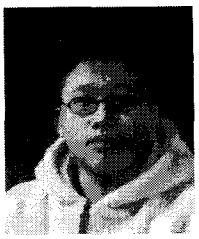
Algorithm Set: an Example Algorithm Set for the 3GPP Authentication and Key Generation Functions $f1, f1^*, f2, f3, f4, f5$ and $f5^*$". Document 3 : Design Conformance Test Data.

[13] ITU : ITU-R SECURITY PRINCIPLES FOR INTERNATIONAL MOBILE : TELECOMMUNICATIONS-2000 (IMT-2000) Recommendation ITU-R M.1078.

[14] ITU : EVALUATION OF SECURITY MECHANISMS FOR IMT-2000 : RECOMMENDATION ITU-R M.1223.

[15] "정보통신 표준화 백서", 정보통신부, 2000.

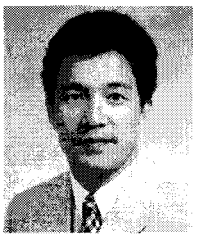
[16] 정원영, 정욱. "IMT-2000 보안 위협 및 대책", 1999.



이 덕 규

2001년 2월 순천향대학교 컴퓨터공학과 졸업
2003년 2월 순천향대학교 전산학과 석사
2001년 3월~현재 순천향대학교 전산학과 박사과정

관심분야 : IMT-2000, PKI, DRM



이 임 영

1981년 8월 홍익대학교 전자공학과 졸업
1986년 3월 오사카대학 통신공학전공 석사
1989년 3월 오사카대학 통신공학전공 박사
1989년 1월~1994년 2월 한국전자통신연구원 선임연구원
1994년 3월~현재 순천향대학교 정보기술공학부 부교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안