2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

# 이동 사용자를 위한 인증 및 키 교환 프로토콜

이병래*, 강상승**, 김태윤*
*고려대학교 컴퓨터학과
**한국전자통신연구원
e-mail : brlee@netlab.korea.ac.kr

# An Authentication and Key Exchange Protocol for Mobile User

Byung-Rae Lee*, Sang-Seung Kang**, Tai-Yun Kim*
*Dept. of Computer Science & Engineering, Korea University.
**Electronics and Telecommunications Research Institute

요 약

본 논문에서는 이동 통신 환경에서 사용자가 다양한 서비스 제공자와의 효율적인 인증과 키 교환 프로토콜을 수행할 수 있는 새로운 프로토콜을 제시한다. 사용자의 이동성을 지원하기 위하여 이동 사용자가 방문하고 있는 도메인에서 사용할 수 있는 임시적인 인증서 발급 과정을 제안하였다. 제안된 임시 이동 사용자 인증서는 사용자가 방문하고 있는 도메인에 위치한 TTP 의 비밀키로 전자서명이 이루어져서 사용자에게 발급이 이루어진다. 이동 사용자는 자신에게 발급된 임시 이동 사용자 인증서를 이용하여 이동 통신에서의 AIP(Authentication and Initialization of Payment) 프로토콜을 효율적으로 수행할 수 있다.

## 1. 서론

UMTS(Universal Mobile Telecommunications System)[1]와 같은 제 3 세대 이동 통신 환경에서는 다양하고 수많은 VASP(Value Added Service Provider)들이 증가할 것이다. 다양한 VASP 와의 안전한 이동 통신 시스템을 위하여 사용자는 이동성을 지원하는 효율적인 인증 및 키 교환 기법을 필요로 한다.

ASPeCT[2]에서의 AIP(Authentication and Initialization of Payment) 프로토콜[3,4]은 이동 통신 환경에서의 전자상거래를 가능하게 해주는 인증과 지불 초기 프로토콜이다. AIP 프로토콜에서는 온라인 TTP 의 참여 여부에 따라서 두 가지 종류의 프로토콜로 구분되어 질 수 있다. 온라인 TTP 가 참여하는 경우는 도메인 간의 인증(cross-domain authentication)에 기반 하는 경우이다.

본 논문에서 우리는 이동 사용자는 자신이 속해 있는 도메인의 TTP 의 전자 서명을 검증 할 수 있는 공개키를 가지고 있을 확률이 높다는 것을 가정한다. 반대로 다양한 서비스 제공자가 존재하게 될 3 세대 이동 통신 환경에서 이동 사용자가 다른 도메인에 위치한 VASP 의 인증서를 검증할 수 있는 공개키를 가지고 있을 가능성을 적다.

본 논문에서는 UMTS 에서의 효율적인 이동 정보 서비스를 위한 임시 이동 사용자 인증서를 제안한다. 제안한 임시 이동 사용자 인증서는 등록 프로토콜 수행시 사용자가 방문하고 있는 도메인에 존재하는 TTP 의 비밀키로 전자 서명이 되어 사용자에게 발행이 된다. 제안된 임시 이동 사용자 인증서를 이용하여 사용자가 현재 방문하고 있는 도메인에서 AIP 프로토콜에서 발생하는 인증서 검증시 필요한 공개키 분배 문제를 해결할 수 있으며 개선된 효율성을 제공할 수 있다. 임시 이동 사용자 인증서를 사용한 프로토콜은 사용자와 VASP 가 서로간의 공개키를 가진 상태에서 수행되는 프로토콜과 같은 효율성을 가진다. 또한 기존의 AIP 프로토콜과 달리 익명 서비스 사용이 가능해졌다.

본 논문의 구성은 다음과 같다. 2 장에서는 기존의 등록 프로토콜과 AIP 프로토콜에 대해서 살펴본다. 3 장에서는 임시 이동 사용자 인증서를 제시한다. 4 장에서는 임시 인증서를 사용자에게 발급하기 위한 새로운 등록 프로토콜을 제안하고 5 장에서는 임시 이동 사용자 인증서 기반의 AIP 프로토콜을 제안한다. 6 장

에서는 제안된 프로토콜에 대한 분석을 한다. 7 장에서는 결론을 제시한다.

## 2. 관련 연구

본 장에서는 Siemens 등록 프로토콜 C[2]과 AIP 프로토콜을 고찰한다.

기본적인 프로토콜의 표기 형식은 다음과 같다. $id_X$ 는 $X$ 의 신원을 의미하며, $CertX$ 는 $X$ 의 인증서를 뜻한다. $X$ 의 메시지 $M$ 에 대한 전자서명 알고리즘은 각각 $Sig_X(M)$ 으로 표기된다. 세션키 $K$ 로 암호화된 메시지 $M$ 은 $\{M\}_K$ 로 나타내어진다. $h1$, $h2$, $h3$ 는 [3,4]에 정의된 해쉬함수 이다.

### 2.1 Siemens C 등록 프로토콜

본 등록 프로토콜의 참여자는 사용자 $U$, 네트워크 오퍼레이터 $N$, 인증 기관 $CS$ 이다. 사용자는 외부 도메인에 접근했을 때 네트워크 오퍼레이터 $N$ 과 통신을 시작한다.

$$U \qquad\qquad N$$
$$\xrightarrow{\quad g^{RND_U} \,\|\, idCS \,\|\, \{IMUI\}_L \quad}$$

<그림 1> 등록 프로토콜 – 1

프로토콜이 시작되면 $U$ 는 난수 $RND_U$ 를 생성하여 공개키 $g^{RND_U}$ 를 생성하고 $g^w$ 와 같이 세션키 $L = g^{w(RND_U)}$ 을 계산한다. $U$ 는 자신의 인증 서버의 신원 $idCS$ 그리고 자신의 신원 $IMUI$ 를 $L$ 를 이용해서 암호화하여 $N$ 에게 전송한다.

$$N \qquad\qquad CS$$
$$TS1 \,\|\, g^s \,\|\, g^{RND_U} \,\|\, \{IMUI\}_L \,\|\, Sig_N\left(h3\left(TS1 \,\|\, g^s \,\|\, g^{RND_U} \,\|\, \{IMUI\}_L\right)\right) \xrightarrow{\quad\quad}$$
$$CertN \,\|\, TS \,\|\, idN \,\|\, CertU \,\|\, Sig_{CS}(TS \,\|\, idN \,\|\, CertU) \xleftarrow{\quad\quad}$$

<그림 2> 등록 프로토콜 – 2

<그림 2>에서 $N$ 은 $U$ 로 부터 전송 받은 메시지를 자신이 생성한 타임스탬프 $TS1$ 와 자신의 공개키 $g^s$ 를 자신의 비밀키로 서명을 하여 $CS$ 에게로 보낸다.

$CS$ 는 $U$ 의 공개키 $g^{RND_U}$ 와 같이 세션키 $L = g^{(RND_U)w}$ 을 계산하고 $\{IMUI\}_L$ 를 복호화해서 $U$ 의 신원을 파악한다. $CS$ 는 $N$ 이 생성한 서명을 검증하고 $N$ 의 공개키 $g^s$ 에 대한 인증서 $CertN$ 을 만든 후, 타임스탬프 $TS$, $N$ 의 신원인 $idN$, $CertU$ 를 서명을 하여 $N$ 에게 전송한다.

<그림 3>을 보면 $N$ 은 $TS \,\|\, idN \,\|\, CertU$ 에 대한 서명과 $CertN$ 을 검증하고 간략화된 인증서 $CertN*$ 를 생성하고 세션키 $K_s = h1\left(g^{(RND_U)s} \,\|\, RND_N\right)$ 을 계산해낸다. 계산된 $Auth_N$ 은 $N$ 으로부터 전송 받은 것과 비교되어진다.

$N$ 은 $K_s$, $data1$, $data2$ 를 알고 있으므로 $h3(K_s \,\|\, data1 \,\|\, data2)$ 를 계산해낸다. 또한 $Sig_U(h3(K_s \,\|\, data1 \,\|\, data2))$ 로부터 $h3(K_s \,\|\, data1 \,\|\, data2)$ 를 복구해내어 자신이 계산한것과 비교한다.

$$U \qquad\qquad N$$
$$RND_N \,\|\, Auth_N \,\|\, CertN* \,\|\, \{data1 \| data3\}_{K_s} \xleftarrow{\quad\quad}$$
$$\{Sig_U(h3(K_s \| data1 \| data2))\}_{K_s} \,\|\, \{data2\}_{K_s} \xrightarrow{\quad\quad}$$

<그림 3> 등록 프로토콜 – 4

### 2.2 AIP 프로토콜

본 프로토콜의 참여자는 사용자 $U$, 서비스 제공자 $V$, 그리고 신뢰기관 $T$ 가 있다. 신뢰기관은 사용자와 서비스 제공자간에 공개키 분배 문제를 해결하기 위하여 인증서 체인을 이용하여 각자의 공개키를 $U$ 와 $V$ 각각에게 전송해준다.

키 설정 방식은 다음과 같다. $U$ 는 $T$ 와 같이 ElGamal 키 설정 방식[5]으로 세션키를 성립하고, $V$ 와는 Diffie-Hellman 방식[6]에 의하여 세션키를 설정한다.

$$U \qquad\qquad V$$
$$\xrightarrow{\quad g^u \,\|\, idT \,\|\, \{idU\}_L \quad}$$

<그림 4> AIP 프로토콜 – 1

프로토콜(<그림 4>)이 시작되면 $U$ 는 난수 $u$ 를 생성하여 키 설정용 공개키 $g^u$ 를 생성하고 $T$ 의 공개키 $g^w$ 와 같이 세션키 $L = g^{wu}$ 을 계산한다. 이와 같이 자신의 $T$ 의 신원 $idT$, 그리고 자신의 신원 $idU$ 를 세션키 $L$ 을 이용해서 암호화해서 $V$ 에게 보낸다.

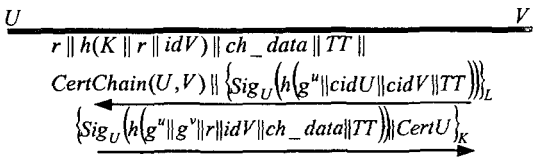
$$V \qquad\qquad T$$
$$g^u \,\|\, \{idU\}_L \,\|\, CertV \xrightarrow{\quad\quad}$$
$$TT \,\|\, CertChain(U,V) \,\|\, CertChain(V,U)$$
$$\|\, CertChain(V,T) \,\|\, Sig_T\left(g^u \,\|\, cidU \,\|\, cidV \,\|\, TT\right) \xleftarrow{\quad\quad}$$

<그림 5> AIP 프로토콜 – 2

<그림 5>에서 $V$ 는 $U$ 로 부터 전송 받은 $g^u$, $\{idU\}_L$ 를 자신의 인증서 $CertV$ 와 같이 $T$ 에게로 보낸다.

$T$ 는 $U$ 의 공개키 $g^u$ 와 같이 세션키 $L = g^{uw}$ 을 계산한다. $T$ 는 $V$ 로부터 전송 받은 $idU$ 를 이용하여 $U$ 의 인증서를 찾아내고 인증서 체인 $CertChain(V,U)$ 을 생성한다. 마찬가지로 $T$ 는 $CertV$ 에 기반해서 $CertChain(U,V)$ 을 만들어내고 $g^u$ 를 이용하여 $CertChain(V,T)$ 를 계산한다. $T$ 는 타임스탬프 $TT$ 를

생성하고 $U$ 의 공개키 $g^u$ 와 인증서 식별 번호 $cidU, cidV$ 에 전자서명을 수행하여 $V$ 에게 전송한다.




<그림 6> AIP 프로토콜 – 4

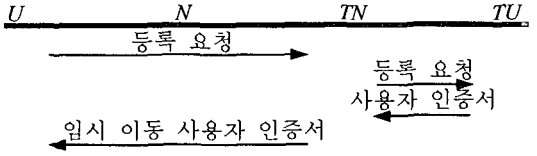
<그림 6>을 보면 $V$ 는 $CertChain(V,T)$ 를 검증하여 $T$ 의 서명을 검증할 수 있는 공개키를 얻고 $CertChain(V,U)$ 을 이용하여 $U$ 의 전자서명을 검증할 수 있는 공개키를 얻는다. $V$ 는 $U$ 의 공개키 $g^u$ 를 이용하여 세션키 $K = h(g^{uv} \| r)$ 를 계산해 낸다.

$U$ 는 $V$ 로부터 받은 $CertChain(U,V)$ 를 이용하여 $V$ 의 전자서명을 검증할 수 있도록 공개키를 복구해 낸다. 그리고 $V$ 의 $g^s$ 를 이용하여 세션키 $K = h(g^{vu} \| r)$ 를 계산해낸다.

### 3. 임시 이동 사용자 인증서

이동 사용자는 외부 도메인에서의 VASP 의 인증서를 검증할 공개키를 가지고 있는 확률이 적다는 경우에서 임시 이동 사용자 인증서는 시작된다. 임시 이동 사용자 인증서는 방문하고 있는 도메인의 TTP 에 의해서 전자 서명이 이루어져서 사용자에게 발급된다.

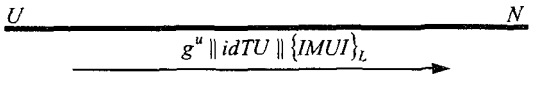
임시 이동 사용자 인증서의 발급 모델은 아래와 같다. 방문 도메인의 TTP 는 사용자의 TTP 와 통신을 필요로 한다.




<그림 7> 제안한 등록 프로토콜 모델

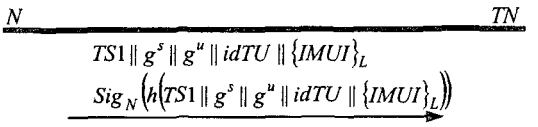
### 4. 제안한 등록 프로토콜

제안한 등록 프로토콜은 사용자 $U$, 네트워크 오퍼레이터 $N$, 네트워크 오퍼레이터의 신뢰기관 $TN$ 그리고 사용자의 신뢰기관 $TU$ 가 참여한다.



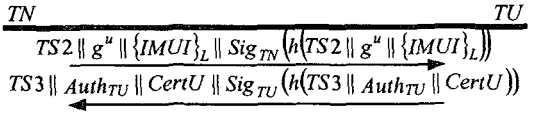

<그림 8> 제안한 등록 프로토콜 – 1

프로토콜(<그림 8>)이 시작되면 $U$ 는 난수 $u$ 를 생성하여 공개키 $g^u$ 를 생성하고 $TU$ 의 공개키 $g^w$ 와 같이 세션키 $L = g^{uw}$ 을 계산한다. 이와 같이 자신의 $TU$ 의 신원 $idTU$, 그리고 자신의 신원 $idU$ 를 세션키 $L$ 을 이용해서 암호화해서 $N$ 에게 보낸다 $IMUI$ 를 암호화해서 보내는 이유는 사용자의 익명성을 보장하기 위해서이다.



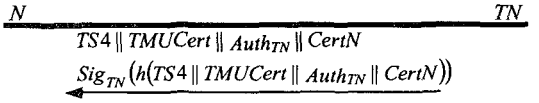

<그림 9> 제안한 등록 프로토콜 – 2

<그림 9>에서 $N$ 은 $TN$ 로 부터 전송 받은 $g^u$, $\{IMUI\}_L$ 를 자신의 키 설정용 공개키 $g^s$ 와 같이 서명을 하여 $TN$ 에게로 보낸다.



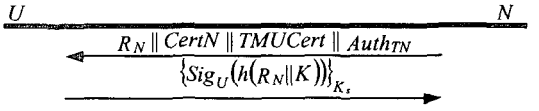

<그림 10> 제안한 등록 프로토콜 – 3

<그림 10>에서 $TU$ 는 $U$ 의 공개키 $g^u$ 와 같이 세션키 $L = g^{uw}$ 을 계산한다. $TU$ 는 $TMUCert$ 를 생성하고 $U$ 가 $TN$ 의 공개키를 검증하는데 필요한 $Auth_{TU}$ 를 생성한다. $TU$ 는 $U$ 의 인증서와 $Auth_{TU}$, 타임스탬프 $TS3$ 에 전자 서명을 하여 $TN$ 에게 전송한다.




<그림 11> 제안한 등록 프로토콜 – 4

$TN$ 은 $TU$ 로부터 전송 받은 $CertU$ 와 $Auth_{TU}$ 를 검증하고 $U$ 가 현재 방문하고 있는 도메인에서 사용할 수 있는 $TMUCert$ 를 생성한다. $TMUCert$ 는 $TN$ 의 비밀키로 서명이 이루어져 있으며 사용자의 공개키에 대한 인증서이다. $TN$ 은 $U$ 가 $N$ 의 공개키 $g^s$ 를 얻을 수 있도록 $CertN$ 를 생하고 자신의 공개키를 얻을 수 있도록 $Auth_{TU}$ 를 계산하여 타임스탬프 $TS4$, $TMUCert$, $CertN$ 과 함께 서명을 하여 $N$ 에게 전송한다.



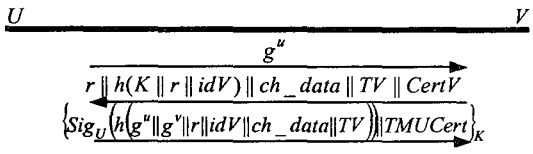

<그림 12> 제안한 등록 프로토콜 – 5

<그림 12>에서 $N$ 은 $TMUCert$ 를 이용하여 $U$ 의 공개키를 검증할 수 있다. $N$ 은 자신이 받은 메시지와 난수 $R_N$ 을 생성하여 $U$ 에게 전송하고 $g^u$ 를 이용하여 세션키 $K_s = (g^{us} \| R_N)$ 를 계산해 낸다.

$U$ 는 $N$ 로부터 받은 $CertN$ 를 이용하여 $N$ 의 전자서명을 검증할 수 있도록 공개키를 얻고 $N$ 의 공개키 $g^s$ 를 이용하여 $N$ 과의 세션키 $K_s = (g^{su} \| R_N)$ 를 계산해낸다.

## 5. 제안한 AIP 프로토콜

$U$ 는 사용자, $V$ 는 서비스 제공자를 나타낸다. $U$ 는 등록 프로토콜의 수행 결과로 $TMUCert$ 와 $CertV$ 를 검증할 수 있는 공개키를 가지고 있다.




<그림 13> 제안한 AIP 프로토콜

프로토콜(<그림 13>)이 시작되면 $U$ 는 세션키 설정을 위한 공개키 $g^u$ 를 $V$ 에게 보낸다.

$V$ 는 난수 $r$ 을 생성하고 $g^u$ 와 자신의 공개키 $g^v$ 를 이용하여 세션키 $K = h(g^{uv} \| r)$ 를 계산해 낸다. $V$ 는 $K, r, idV$ 를 해쉬화 하고 지불 데이터 $ch\_data$, 타임스탬프 $TV$, 인증서 $CertV$ 를 $U$ 에게 전송한다.

$U$ 는 세션키 $K = h(g^{vu} \| r)$ 를 생성하고 $g^u$, $g^v$, $r$ 과 $V$ 의 신원 $idV$ 와 지불 데이터 $ch\_data$, 타임스탬프 $TV$ 를 해쉬 함수 $h$ 로 처리하고 서명을 구한 후 자신의 인증서 $TMUCert$ 와 같이 $K$ 로 암호화하여 $V$ 에게 전송한다.

## 6. 성능 분석 및 고찰

표 1 은 Siemens 의 프로토콜 C 와 제안한 등록 프로토콜에 대한 성능 평가를 보여준다.

<표 1> 등록 프로토콜

| | Siemens, 프로토콜 C | 제안한 등록 프로토콜 |
|---|---|---|
| 키 설정 알고리즘 | ElGamal, Diffie-Hellman | Diffie-Hellman |
| 참여자의 수 | 3 | 4 |
| 메시지의 수 | 5 | 7 |
| 세션키의 수 | 2 | 2 |
| 사용자의 메시지 생성 | 3 | 3 |
| 사용자의 서명 생성 | 1 | 1 |
| 사용자의 암호화 | 2 | 2 |

제안한 등록 프로토콜은 임시 이동 사용자 인증서를 생성하기 위한 $TN$ 과 $TU$ 와의 추가적인 상호 작용이 필요하지만 사용자 측면에서의 계산량과 메시지 생성은 Siemens 프로토콜 C 와 동일하다.

<표 2> 사용자 측면에서의 계산량

| | TTP 와의 AIP 프로토콜 | 제안한 AIP 프로토콜 |
|---|---|---|
| 익명 인증서 | × | 0 |
| 키 설정 알고리즘 | ElGamal, Diffie-Hellman | Diffie-Hellman |
| 참여자의 수 | 3 | 2 |
| 메시지의 수 | 5 | 3 |
| 인증서 체인의 수 | 3 | 0 |
| 세션키의 수 | 2 | 1 |
| 사용자의 서명 생성 | 1 | 1 |
| 사용자의 인증서 체인 검증 | 1 | 0 |
| 사용자의 암호화 | 2 | 1 |

0 : Yes(possible) × : No(impossible)

온라인 TTP 를 이용하는 AIP 프로토콜과 제안한 임시 이동 사용자 인증서를 이용한 AIP 프로토콜과의 성능 평가는 표 2 에 나와 있다. 제안된 프로토콜은 인증서 체인의 사용을 제거하였으며 암호화와 서명 생성 등에서 개선된 효율성을 보여준다.

## 7. 결론

본 논문에서는 이동 통신 환경에서의 이동 사용자와 VASP 간의 인증과 키 교환을 위하여 등록 프로토콜을 이용한 임시적 인증서 발급 과정을 제안하였다. 이동 사용자는 자신이 방문하고 있는 도메인에서 제안된 임시 이동 사용자 인증서를 이용하여 개선된 효율성을 얻을 수 있다.

## 참고문헌

[1] UMTS Forum, "A regulatory framework for UMTS," Report no. 1, 1997.

[2] ACTS AC095, ASPeCT Deliverable D20 – Project final report and results of trials, 1998.

[3] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," *ESORICS, LNCS*, vol.1488, pp. 469-472 1998.

[4] K.M. Martin, B. Preneel, C. Mitchell, H.J. Hitz, G. Horn, A. Poliakova and P. Howard, "Secure billing for mobile information services in UMTS," *IS&98, LNCS* vol.1430, pp. 535-548, 1998.

[5] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Informatio Theory*, Vol. IT-31, No.4, pp.469-472, 1985.

[6] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 1976.