타원곡선 암호 알고리즘

임채훈 • 세종대학교 인터넷학과
이동훈 • 퓨쳐시스템 암호체계센터

요 약

타원곡선 암호는 기존의 RSA나 Diffie-Hellman, DSA 등에 비해 짧은 키 길이를 사용하면서도 훨씬 빠른 구현이 가능하므로 다양한 국제 표준들에서 이를 지원하고자 하는 노력이 급증하고 있다. 본 기고에서는 타원곡선 암호와 관련된 국제 표준들의 표준화 동향과 함께 현재 TTA 정보통신단체표준으로 제정된 국내 타원곡선 전자서명 표준인 EC-KCDSA에 대해서 간략히 소개하기로 한다.

1. 서론

타원곡선 암호시스템(Elliptic curve cryptosystem)은 유한체(Finite field)상의 타원곡선 점들간의 연산에서 정의되는 이산대수 문제(Discrete logarithm problem)의 어려움을 이용하는 것으로 전자서명 알고리즘과 키 교환 알고리즘에 주로 사용된다. 타원곡선 암호시스템의 안전도는 키 길이의 증가에 따라 거의 지수 함수적으로 증가하므로 준 지수함수적인 증가를 갖는 RSA나 ElGamal/Diffie-Hellman 등과 같은 기존의 공개키 암호시스템에 비해 장기적으로 기술의 발전에 따른 키 길이의 증가 비율면에서도 대단한 장점을 가지고 있다(예를들어 RSA 암호시스템이 512비트 정도의 타원곡선 암호시스템과 유사한 안전도를 제공하기 위해서는 대략 15,000비트 정도의 합성수를 사용하여야 한다). 타원곡선 암호는 이러한 장점들로 인해 스마트 카드나 무선통신 단말기 등과 같이 메모리와 처리능력이 제한된 응용분야에서 특히 효율적으로 사용될 수 있다. 이에 따라 각종 국제 표준들에서 타원곡선 암호에 대한 표준화가 활발히 진행되고 있고, 또한 실제로 다양한 보안응용들에서도 타원곡선 암호를 속속 지원하고 있다.

현재 가장 널리 사용되는 타원곡선 암호시스템은 크게 전자서명과 키 교환으로 나눌 수 있다 (암호화를 위해서는 거의 사용되지 않는다). 전자서명은 미국 연방 표준인 DSA(Digital Signature Algorithm)를 타원곡선위로 적용한 ECDSA(Elliptic Curve DSA)가 국제적으로 가장 널리 사용되고 있으며, 국내에서도 기존의 전자서명 표준인 KCDSA(Korean Certificate-based Digital Signature Algorithm)의 타원곡선 변형을 EC-KCDSA(Elliptic Curve

KCDSA)라는 이름으로 작년 말 TTA 표준으로 제정한 바 있다. 키 교환 알고리즘으로는 ANSI X9.63의 ECDH(Elliptic Curve Diffie-Hellman) 알고리즘이 가장 널리 사용된다. 이들 알고리즘은 여러 표준에 포함되어 있는데 표준의 범위에 따라서 약간씩 차이를 보이고 있으므로 상호호환성을 위해 표준의 성격을 정확히 이해하고 구현하는 것이 필요하다.

2. 타원곡선 암호의 국제 표준화 동향

2.1 IEEE P1363/P1363a

IEEE의 P1363(Standard specifications for public key cryptography) WG은 세계적인 암호학계의 전문가들로 구성된 공개키 암호 표준화 그룹으로 합성수의 소인수 분해문제, 유한체의 이산대수 문제와 타원곡선의 이산대수 문제 등을 기반으로 하는 거의 모든 종류의 공개키 암호기술들에 대한 표준화를 추진하고 있다. 이미 기본적인 공개키 암호기술들에 대해서는 1999년 말 P1363으로 표준화가 완성되었고, 현재는 시간적인 제약으로 P1363에 포함되지 못했던 추가적인 암호기술들을 P1363a로 표준화 중에 있다[1, 2].

P1363의 표준 성격은 여타의 기존 표준들과는 달리 각 알고리즘의 구현기술들에 대한 포괄적인 참조 표준을 목적으로 하여 사용 가능한(널리 사용되고 있거나 안전성에 문제가 없는) 거의 대부분의 공개키 암호방식들을 포함하고 있다. 즉, 특정 응용이나 국가/단체에서 상세 구현 표준이 필요한 경우 그러한 표준을 만들기 위한 참조 표준으로서의 역할을 할 수 있도록 개발된 백과사전적인 표준이다. 따라서 각 알고리즘들은 알려진 거의 모든 구현방식들을 포함하여 선택사양으로 기술하고 있으며, 특정 안전도를 만족시키기 위한 최소 키 길이나 혹은 특정 구현방식을 강제사양으로 지정하지는 않고 있다. 또한 포함된 각종 암호방식의 구현에 필요한 모든 수학적인 알고리즘들도 부록으로 제공하고 있다.

2.2 ANSI X9.62/X9.63과 NIST FIPS 186-2

각종 국제표준이나 응용분야에서 가장 널리 참조하고 있는 구현 표준으로는 ANSI(American National Standards Institute) X9에서 표준화하고 있는 X9.62와 X9.63, NIST의 FIPS 186-2가 있다[3-5]. X9.62는 DSA에 대한 타원곡선 변형으로 ECDSA로 불리며 1999년에 이미 표준화가 완성되었고, 현재는 표준 개정작업이 진행중인 것으로 알려져 있다. 미국 연방 표준인 FIPS 186은 원래 DSA 서명만을 규정하고 있었지만 이후 개정을 통하여 현재의 FIPS 186-2에서는 X9.31의 RSA와 X9.62의 ECDSA를 포함시키고 있다. 이들은 구현시 발생할 수 있는 문제점들을 모두 고려하여 가장 구체적으로 규정된 상세 구현 표준들이다. X9.63은 타원곡선 버전의 다양한 Diffie-Hellman (ECDH) 알고리즘들에 대한 표준으로 아직 표준화가 완성되지는 않았으나 이미 많은 인터넷 응용들에서는 그 초안을 바탕으로 일부 알고리즘들을 표준화하고 있다.

2.3 SECG의 SEC1/SEC2

SEC(Standards for Efficient Cryptography) Group은 CertiCom을 주축으로 다양한 업계의 단체들로 구성된 타원곡선 암호에 대한 표준화 그룹으로 보안 솔루션의 개발과 적용시에 벤더나 사용자가 직면하는 상호운용상의 문제점들을 해결하기 위해 설립되었다. 따라서 SEC Group은 자체적으로 새로운 표준을 만들기보다는 X9.62나 X9.63, P1363 등 기존 표준들의 실제 구현시 상호호환성을 증진시킬 수

있도록 이들을 프로파일링하는 것을 주 목적으로 한다(예를들어 구현시 상호호환성을 높일 수 있도록 이들 표준에서 허용하는 일부 선택사항들에 대한 제약을 주는 형태로).

SEC Group의 표준으로는 알고리즘을 기술한 SEC1과 권장 타원곡선을 기술한 SEC2가 있다[6,7]. SEC1은 X9.62의 ECDSA와 X9.63의 ECDH 알고리즘들에 대한 프로파일을 기술하고 있고, SEC2는 안전성과 효율성을 고려하여 잘 정의된 선정기준에 따라 생성된 다양한 타원곡선 도메인 변수들을 제시하고 있다. SEC1의 표준은 그다지 업계에 영향력을 미치지는 못하고 있고, 실제로 많은 응용이나 타 표준에서 인용하고 있는 부분은 SEC2의 권장 타원곡선들이다.

2.4 ISO/IEC 15946

타원곡선 암호에 대한 포괄적인 국제표준으로 ISO/IEC JTC1/SC27에서 표준화 중인 ISO/IEC 15946(Information technology – Security techniques – Cryptographic techniques based on elliptic curves)이 있다[8]. 그러나 ISO 표준은 알고리즘의 추상적인 기능위주의 기술만을 담고 있으며, 실제 구현을 위해서는 다른 상세한 구현 표준을 참조하도록 하고 있다. 즉, ISO 표준의 성격은 일부 국가나 업계에서 이미 구현 가능한 형태의 표준 스펙이 존재하여 널리 사용되는 표준들을 국제 표준화 기구에 등록시켜 국제적인 응용에서의 호환성을 주고자 하는 목적이 강하다고 생각할 수 있겠다.

3. 타원곡선 전자서명 ECDSA와 EC-KCDSA

3.1 ECDSA

Elliptic Curve DSA(ECDSA)는 미국 연방 표준 서명 알고리즘(FIPS 186)인 DSA를 타원곡선위의 알고리즘으로 변환한 것이다. 따라서 본질적인 알고리즘은 유한체 위에서의 DSA와 동일하다. ECDSA는 ANSI에서 X9.62로 표준화되었고 FIPS 186-2나 SEC 1에서도 X9.62를 따르고 있다. 현재 X9.62는 개정작업이 진행되고 있으며 기존의 무원칙하게 선정된 도메인 변수도 SEC2의 것을 따를 것으로 알려져 있다.

미 연방정부 표준인 FIPS 186-2에서는 X9.62 표준을 그대로 따르되, 다만 연방정부용으로 사용하기 위한 권장곡선을 추가로 제공하고 있다(SEC2의 권장 타원곡선은 FIPS 186-2의 것을 모두 포함하고 있음). FIPS 186-2의 권장 타원곡선은 블록 암호의 키 길이 80(Skipjack), 112(2DES), 128(AES-128), 192(AES-192), 256(AES-256)비트에 상응하는 안전도를 주도록 선택되었으며, 이에 따른 유한체 GF(p)와 GF(2^m)상의 권장곡선을 각각 제공하고 있다.

ECDSA는 n을 타원곡선의 위수라고 할 때 메시지 m에 대한 서명과 검증이 다음과 같이 이루어진다. 서명자의 공개키 Q는 비밀키 d로부터 Q = dG로 계산된다.

서명	검증
$k \leftarrow \{1, \ldots, n-1\}$	$e \leftarrow SHA1(m)$
$(x_1, y_1) \leftarrow kG$	$a \leftarrow s^{-1}e \bmod n$
$r \leftarrow x_1 \bmod n$	$b \leftarrow s^{-1}r \bmod n$
$e \leftarrow SHA1(m)$	$(x_2, y_2) \leftarrow aG + bQ$
$s \leftarrow k^{-1}(e + dr) \bmod n$	$t \leftarrow x_2 \bmod n$
서명 : (r, s)	r = t인지 검증

3.2 EC-KCDSA

EC-KCDSA[9]는 국내 전자서명 표준인 KCDSA를 타원곡선위의 알고리즘으로 변형한 것

으로, 표준화 작업은 1999년부터 한국정보보호학회 산하 정보보호표준연구회 주관으로 시작되었다. 그러나 업계나 학계의 참여가 지지부진하여 ECDSA 같은 구현 가능한 표준보다는 ISO /IEC 형태의 기능 표준으로 작업이 진행되다가 2001년 6월말에 산학연의 본격적인 TFT(Task Force Team)가 결성되어 약 4개월 여의 집중적인 작업결과 2001년 말에 실제 구현이 가능한 수준의 TTA 표준으로 제정되었다.

EC-KCDSA는 X9.62를 기본 모델로 FIPS 186-2, SEC1/SEC2, P1363 등 기존의 국제 표준들로부터 최대한 장점을 취하면서도 이들과 거의 동일한 구조로 구현 가능하게 하여 구현 부담을 최소화하도록 설계되었다. 실제 구현에 필요한 모든 수학적 알고리즘과 X.509 PKI 기반에서의 ASN.1 표기를 포함하고 있으며, 안전성과 효율성을 최대한 고려하여 선정된 다양한 권장 타원곡선들도 포함하고 있다. EC-KCDSA는 전체적으로 5장의 본문, 3장의 부속서, 8장의 부록으로 구성되어 있으며, 본문과 부속서는 EC-KCDSA를 구현하는데 반드시 준수해야 하는 부분이며, 부록은 구현에 도움이 될 수 있는 각종 알고리즘 및 안전성 분석, 참조구현 값 등으로 이루어져있다.

EC-KCDSA는 n을 타원곡선의 위수라고 할 때 다음과 같이 메시지 m에 대한 서명과 검증이 이루어진다. 서명자의 공개키 Q는 비밀키 d로부터 $Q = d^{-1}G$로 계산된다 (여기서 상수 c_Q는 서명자의 공개키 Q의 x, y 좌표를 연접하여 해쉬함수의 블록길이만큼 취한 값이다).

EC-KCDSA는 ECDSA에 비해 메시지를 해쉬할 때 서명자의 고유의 상수 cQ를 추가함으로써 잠재적인 위협이나 서명의 오용을 막을 수 있도록 하였고, 또한 이상적인 해쉬함수를 가정하면 안전성 증명이 가능하다는 장점도 있다. 그리고 유한체의 범위를 GF(p)와 GF(2^m)뿐만 아니라 GF(p^m)으로 확장하여 더욱 다양한 타원곡선을 사용할 수 있도록 하였고, 보다 효율적인 연산이 가능한 Koblitz 곡선을 포함시키고 있다. 실제로 EC-KCDSA 표준의 부록에는 각 유한체별로 각각의 안전도에 따라서 안전하고 효율적인 권장 타원곡선 39개를 제시하고 있다.

서명	검증
$k \leftarrow \{1, \ldots, n-1\}$ $(x_1, y_1) \leftarrow kG$ $r \leftarrow HAS160(x_1)$ $v \leftarrow HAS160(c_Q \mid\mid m)$ $e \leftarrow r \text{ XOR } v \bmod n$ $s \leftarrow d(k - e) \bmod n$ 서명 : (r, s)	$v \leftarrow HAS160(c_Q \mid\mid m)$ $e \leftarrow r \text{ XOR } v \bmod n$ $(x_2, y_2) \leftarrow sQ + eG$ $r = HAS160(x_2)$ 인지 검증

4. 타원곡선 암호의 응용 표준

ECDSA 등의 타원곡선 전자서명에 대한 표준화가 진전됨에 따라 많은 응용 보안 표준들에서도 이들을 지원하려고 하고 있다. 대표적인 IETF의 인터넷 보안 표준에서의 타원곡선 암호 사용현황을 정리해 본다. 이들은 대부분 아직 초안(draft) 상태이나 이미 구현되어 사용되고 있는 경우도 있다.

4.1 IPsec

IPsec(IP Security) 프로토콜은 IP 계층에서의 보안 프로토콜로 가상사설망(VPN)이나 IPv6, Mobile IP, VoIP 등 각종 응용에서 네트워크 인프라의 보호를 위해 가장 널리 사용되고 있는 인터넷 보안 표준이다. IPsec은 크게 IP 패킷의 내용에 대한 암호화/인증 기능을 제공하는 ESP 프로토콜, IP 헤더를 포함한 패킷 전체의 인증기능을 제공하는 AH 프로토콜, 그리고 키 관리를 위한 IKE로 구성되어 있다.

IPsec에서 가장 계산부하가 많이 걸리는 부분이 각종 보안 파라미터들을 협상하고 상호 인증을 수행하는 IKE 프로토콜인데, 이는 특히 무선 환경과 같은 제약적인 환경에서 큰 부담으로 작용하므로 무선 VPN 환경에서는 ECDH이나 ECDSA 등의 타원곡선 암호를 선호한다[10,11]. 이미 많은 업체들에서 무선 VPN 등의 응용을 위해 이 타원곡선 암호를 구현하여 사용하고 있다.

4.2 TLS

TLS는 잘 알려진 SSL 3.0을 IETF에서 표준화시킨 것으로 기본적인 프레임워크는 동일하지만 SSL 3.0에서 지적된 문제점들을 수정하여 보안성을 강화시킨 것이다[12]. TLS는 크게 보안 파라미터를 협의하고 키 교환을 담당하는 Handshake 프로토콜과 실제로 응용 데이타의 인증과 암호화를 수행하는 Record 프로토콜로 구성되어 있다. Handshake 프로토콜은 IPsec의 IKE와 유사한 기능을 하지만 훨씬 간단 명료하게 구성되어 있다.

원래의 TLS에는 타원곡선 암호가 포함되지 않았으나 최근 TLS의 Cipher suite에 타원곡선 암호를 추가시키고자 하는 draft가 제안되어 검토중이다[13]. 기본적으로 ECDH을 이용한 키 교환과 ECDSA를 이용한 인증을 가능하게 하기 위한 데이타 구조나 Cipher suite들을 정의하고 있다. ECDSA는 X9.62를, ECDH는 P1363을 참조하고 있으며, 권장 곡선으로는 X9.62, FIPS 186-2, SEC2 등의 타원곡선을 사용하도록 권고하고 있다.

4.3 WTLS

WTLS 프로토콜은 WAP Forum에서 표준화한 무선 인터넷에서의 전송계층 보안 표준으로 TLS를 무선 환경에 보다 적합하도록 최적화시킨 것이다[14]. 예를들어 각종 알고리즘이나 파라미터들에서 약간의 안전성을 희생하더라도 효율성을 높일 수 있는 선택사항들을 추가하였고, 복잡한 X.509 인증서 대신 대부분의 확장필드들을 제거하고 간단한 엔코딩을 사용하는 WTLS 인증서를 사용할 수 있게 하였으며, 또한 TCP 뿐만 아니라 UDP상에서도 동작하도록 하였다.

WTLS는 무선환경을 위한 보안 프로토콜인 만큼 설계시부터 이러한 제약된 환경에서 보다 효율적인 타원곡선 암호를 염두에 두고 설계되었다. 사용자 인증을 위한 ECDSA 서명과 키분배를 위한 ECDH을 포함하고 있으며, 또한 IPsec에서와 마찬가지로 호환성을 위한 독자적인 권장 곡선들도 규정하고 있다.

4.4 S/MIME

IETF의 S/MIME 작업반에서 표준화하고 있는 CMS(Cryptographic Message Syntax)는 PKCS#7을 확장시킨 것으로 서명, 인증, 암호화 등을 위한 각종 Content에 대한 구문을 정의하고 있다[15]. 각 Content를 생성하는 방법과 수신자측에서 이를 해석하고 검증하는데 필요한 모든 정보(알고리즘이나 키에 대한 정보 등)를 ASN.1 구문으로 명확히 규정하여 이를 이용하는 각종 응용(S/MIME, PKIX 등)에서 호환성을 보장하고자 하는 것이다.

원래의 CMS 표준(RFC 2630)에서는 암호학적인 메시지의 Syntax와 지원 암호 알고리즘에 대한 내용이 하나의 문서로 결합되어 있었으나, 이의 개정판 draft에서는 향후의 확장성을 위해 구문과 알고리즘을 분리시켜 각각 독립된 문서로 기술하고 있다. 한편 CMS에서도 SignedData, EnvelopedData, AuthenticatedData 등의 Content type에서 타원곡선 암호를 사용하기 위한 수정사항을 기술한 draft가 제안되어 있다[16]. 여기에는 ECDSA에 의한 서

명을 이용한 메시지 인증을 포함하고 있고, 관련 표준으로는 X9.62, P1363, SEC1 등을 참조하고 있다.

4.5 PKIX

IETF의 PKIX 작업반에서는 각종 인터넷 응용에서 공개키 암호의 사용을 위한 인터넷 공개키 기반 구조에 대한 표준화 작업이 진행되고 있다. 일련의 일단계 표준 문서들이 RFC로 등록되었는데, 그 중 하나인 RFC 2459에서는 인터넷 PKI를 위한 X.509 인증서와 CRL(인증서 폐기 목록)에 대한 프로파일을 기술하고 있다[17].

S/MIME의 CMS에서와 마찬가지로 원래 RFC 2459에 통합되어 있던 인증서/CRL의 프로파일 부분과 이 때 사용되는 암호 알고리즘이나 파라미터/키 등의 ASN.1 구문 부분이 현재는 각각 분리되어 독립적인 draft로 개정작업이 진행되고 있다. 후자의 문서에는 인증서나 CRL의 발행시 사용할 수 있는 서명 알고리즘으로 RSA, DSA와 더불어 ECDSA를 포함하고 있고, 인증서 내의 사용자 공개키 알고리즘으로는 RSA, DSA, Diffie-Hellman, KEA 등과 함께 ECDSA와 ECDH을 포함하고 있다[18].

참고 문헌

1. P1363 : Standard specifications for public key cryptography, D13, IEEE, Nov. 1999.
2. P1363a : Standard Specifications For Public Key Cryptography: Additional Techniques, D8, IEEE, April 27, 2001.
3. X9.62 : Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA), ANSI, X9.62-1998, approved Jan. 1999.
4. X9.63 :, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography, ANSI, Working Draft, November 2000.
5. FIPS PUB 186-2 : Digital signature standard(DSS), NIST, Jan. 2000.
6. SEC1 : Elliptic Curve Cryptography v1.0, SECG, September 20, 2000.
7. SEC2: Recommended Elliptic Curve Cryptography Domain Parameters v1.0, SECG, September 20, 2000.
8. ISO/IEC 15946 : Information technology - Security techniques - Cryptographic techniques based on elliptic curves, Part 1: General, Part 2: Digital Signatures, Part 3: Key Establishment, Part 4: Digital Signature giving message recovery.
9. EC-KCDSA : 부가형 전자 서명 방식 표준 - 제3부 : 타원곡선을 이용한 인증서 기반 전자서명 알고리즘, TTA 정보통신단체표준, December 2001.
10. RFC2409 : The Internet Key Exchange (IKE), November 1998.
11. Internet Draft : Additional ECC Groups For IKE, Simon Blake-Wilson, Y. Poeluev and M. Salter, IPsec WG, March 2001.
12. WTLS: Wireless Transport Layer Security, WAP Forum, Proposed Version 06-Apr-2001.
13. RFC2246 : The TLS Protocol v1.0, January 1999.
14. Internet Draft : ECC Cipher Suites for TLS,

Simon Blake-Wilson, Tim Dierks and Chris Hawk, TLS WG, March 2001.
15. RFC2630 : Cryptographic Message Syntax, June 1999.
16. Internet Draft : Use of ECC Algorithms in CMS, Simon Blake-Wilson, Daniel R. L. Brown and Raul Lambert, S/MIME WG, May 2001.
17. RFC2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.
18. Internet Draft : Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile, L.Bassham, R.Housley and W.Polk, PKIX WG, October 2001.

차세대 VoIP망 구축 본격화

기간통신 사업자들이 차세대 VoIP(음성데이터통합)망 구축작업에 본격착수했다. 이에 따라 H.323 위주로 전개돼 온 VoIP시장도 차세대 프로토콜과 장비 중심으로 재편되는 등 급물살을 탈 전망이다. 하나로통신(www.hanaro.co.kr 대표 신윤식)은 H.323기반의 VoIP망을 MGCP(Media Gateway Control Protocol)망으로 진화시키기로 하고 이를 위한 핵심장비인 MGCP 게이트웨이 선정에 나섰다고 1월 24일 밝혔다. 이 회사 홍정욱 과장은 "H.323망으로는 다양한 부가서비스 지원과 QoS(서비스 품질) 보장이 어려워 MGCP를 도입하기로 했다"며 "백본망은 MGCP로 가고 단말기는 H.323으로 가져갈 계획"이라고 말했다. 이는 VoIP서비스 확산에 따라 VoIP망 진화가 필수적이지만 MGCP와 함께 차세대 VoIP 프로토콜로 꼽히는 메가코(Megaco)와 SIP(Session Initiation Protocol) 등은 아직 표준 규격이 정해지지 않아 도입에 시기상조라는 판단에 따른 것이다. 또 MGCP 도입은 VoIP망 진화의 과도기적인 단계인데다 기존 H.323망을 대체하는 것이 아니라 연동하는 형태로 SIP나 메가코 등으로 점차 진화해 나갈 것으로 기대된다. 회사는 이미 지난해말 제너시스템즈의 MGCP 소프트스위치를 도입해 시범서비스를 제공하고 있고 MGCP 트렁크게이트웨이도 구축한 상태다. 이에 따라 이번 주까지 10여 개 VoIP 솔루션 업체들을 대상으로 MGCP 게이트웨이 제안서를 제출받고 주요업체들을 선정한다. 또 내주중 RFP(입찰제안서)를 배포하고 2월 8일부터 장비 BMT(성능시험)에 돌입하였다. 이번에 선정할 MGCP 게이트웨이는 중용량급으로 장비규모는 크지 않다. 그러나 앞으로 차세대 VoIP장비 시장을 선점할 수 있는 기회가 된다는 점에서 국내외 VoIP업체들의 경쟁이 벌써부터 치열하다. LG전자, 시스윌, 제너시스템즈, 코스모브리지 등 국내업체와 누에라, 소너스, 시스코시스템즈, 알카텔 등이 BMT에 참가하고 있다. 최종 장비선정은 3월 중순쯤 이뤄질 예정이다. 또 KT(대표 이상철)도 마이크로소프트와 제휴에 따라 SIP기반의 웹투폰 서비스를 추진하면서 SIP망을 구축키로 하고 곧 장비선정에 나선다는 방침이다. 도입장비는 SIP 게이트웨이를 비롯해 기존 H.323망과 연동을 위한 장비 등도 포함될 것으로 알려졌다. 이에 따라 LG전자, 코스모브리지 등 국내외 VoIP 솔루션 업체들이 SIP장비 개발에 나서는 등 SIP시장 준비에 전력하고 있다. 업계 전문가들은 "기간통신 사업자들이 VoIP망 진화에 나섬에 따라 SIP, MGCP 등 프로토콜과 소프트스위치 등 차세대 VoIP장비 시장도 본격 열리게 됐다"며 "VoIP 솔루션 업계 구도도 이에 맞춰 새롭게 재편될 것"이라고 밝혔다.