TTA FOCUS

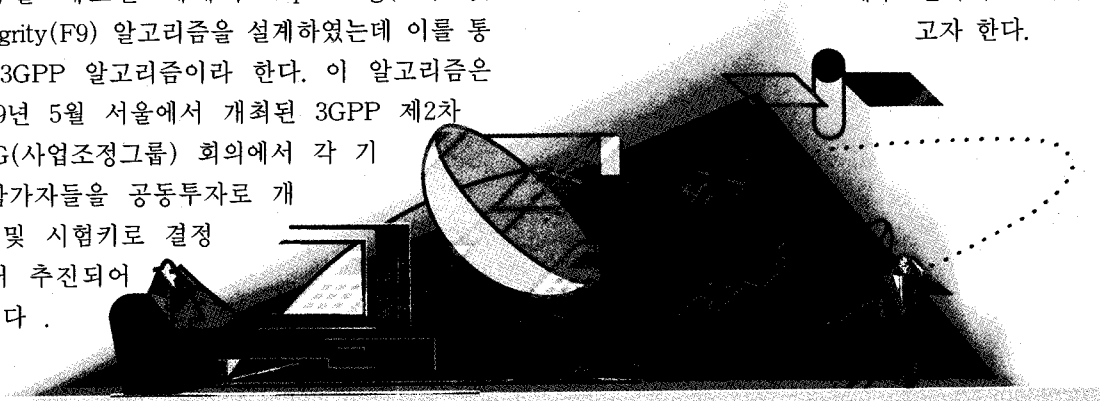
3GPP 알고리즘 배포 · 관리 방안

장명국 / TTA 표준본부장

1. 개요

세계적으로 21세기 멀티미디어 정보화사회로의 진전과 더불어 다양한 정보통신 기반구축 및 서비스 등장으로 인하여 차세대이동통신, 전자상거래, 인터넷 등에서 민감한 정보를 보호할 수 있는 안정성, 신뢰성이 검증된 암호알고리즘 개발 및 표준화가 요구되는 실정이다. 특히 최근 각광받고 있는 차세대이동통신인 IMT-2000 3GPP 진영에서는 진화된 GSM 핵심망과 무선접속기술(W-CDMA)을 기반으로 하여 범세계적으로 적용할 수 있는 기술규격들의 작성을 거의 완료하였는데, 이 중 한 기술그룹인 TSG-SA에서는 3세대 이동가입자들의 인증부문에 적용할 새로운 체계의 Ciphering(F8) 및 Integrity(F9) 알고리즘을 설계하였는데 이를 통칭 3GPP 알고리즘이라 한다. 이 알고리즘은 1999년 5월 서울에서 개최된 3GPP 제2차 PCG(사업조정그룹) 회의에서 각 기관참가자들을 공동투자로 개발 및 시험키로 결정되어 추진되어 왔다.

이 프로젝트는 유럽 표준화기구인 ETSI의 이동통신표준연구센터(MCC)관리하에 TSG-SA산하 SAGE(Security Algorithm Group of Experts) 특별위원회에서 주도적으로 개발되었고, 이 과정에 일본 미쓰비시 암호기술인 「MISTY」가 기본으로 사용되었으며 일본에서는 이에 대한 지적재산권을 무료로 공개하였다. 금년 1월 프랑스 니스에서 개최된 제3차 PCG회의에서는 TSG-SA 의장이 암호알고리즘 개발이 성공적으로 완료되어 공개검증을 각 기관참가자에게 요구하였으나 공개여부를 추후에 결정키로 하고 동 회의에서는 각 기관참가자들이 공동면허부여 공개기준을 마련하여 자국내 업체들에게 면허부여키로 하였다. 이에 따라 한국의 표준화기관인 TTA에서는 3GPP 알고리즘의 공동소유 및 관리기관의 일원으로서 ARIB(일본), ETSI(유럽), T1(미국)과 함께 공동협약체결을 서면으로 진행하고 있어 조만간 이에 대한 국내외 배포 및 관리가 시행되리라 본다. 따라서 여기에서는 3GPP 알고리즘을 국내외에 배포 및 관리하는 방안에 대해 매우 간략히 소개하고자 한다.



2. 목적

이 제도의 목적은 3GPP 알고리즘을 공동 소유한 3GPP 기관참가자들이 공동보관 및 배포를 하기 위한 관련 협약에 따라 한국의 배포·관리 책임자인 TTA가 국내외의 수요자들에게 3GPP 알고리즘을 공정하고 합리적으로 배포·관리하는 절차 및 체계를 마련하여 시행하는데 있다.

3. 방침

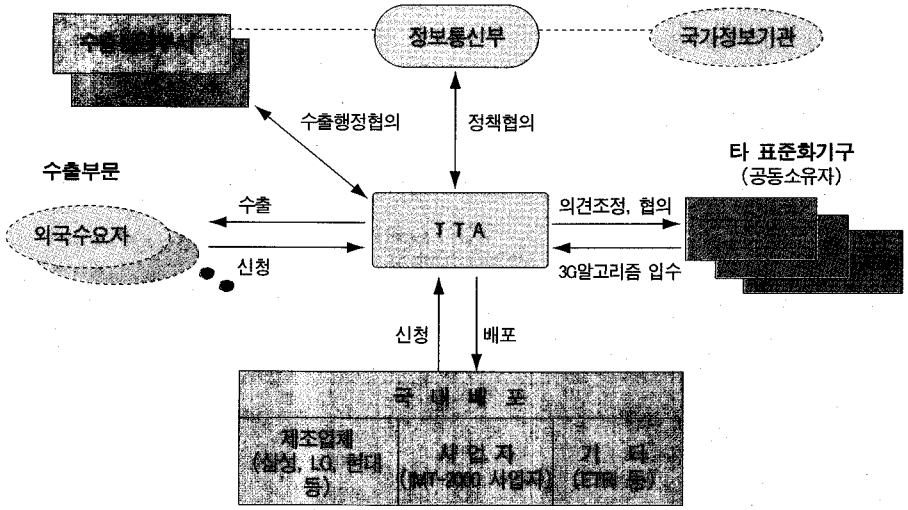
- o 3GPP 암호 및 보전(Integrity) 알고리즘 배포에 관한 관리협약을 기본적으로 준수하며 국내의 환경여건에 따른 세부기준, 절차 등을 보완하여 시행한다.
- o 제도시행에 앞서 수요자인 제조업체, 사업자 등의 의견수렴 및 홍보는 물론 관련 정부유관부처들과의 사전조율이 필요하다.
- o 국내배포인 경우 IMT-2000 사업자 미지정에 따라 제조업체, 연구소 등에 우선배포하고, 사업자는 사업자 지정후 배포하고, 국외수출도 적극 추진한다.
- o 3GPP 알고리즘을 국내에 조기 구현시키기 위해 ETRI와 국내 제조업체들이 공동개발토록 유도한다.

4. 추진 체계

〈그림 1〉 참조

5. 배포(면허부여) 기준

- o 3GPP 알고리즘을 채용하였으며, 3GPP 기술규격 기반의 사업자 면허를 받은 해당국의 전기통신 사업자용으로 3GPP 기술규격 또는 이를 기반으로한 표준에 적합한 장비를 생산하거나 생산할 능력이 있는 기관(장비 제조업체)
- o 최소한 하나의 부품에 3GPP 알고리즘을 구현시켰으며, 3GPP 기술규격기반의 사업자 면허를 받은 해당국의 전기통신 사업자용으로 3GPP 기술규격 또는 이를 기반으로한 표준에 적합한 부품을 생산하거나 생산할 능력



〈그림 1〉 추진 체계

TTA FOCUS

이 있는 기관(부품제조업체)

- o 3GPP 알고리즘을 포함시킨 시스템 시뮬레이터의 경우, 3GPP 기술규격 또는 이를 기반으로한 표준에 따라 시스템 승인 시험용 시스템 시뮬레이터 제조업자나 생산할 능력이 있는 기관(시험장비업체)
- o 국내법에 따라 허가를 받고 3GPP기술규격이나 이를 기반으로한 표준에 준거한 통신망을 사용하는 전기통신사업체(통신사업자)
- o 이상의 기준에 부합되지는 않으나 당사자가 3GPP 알고리즘을 기관에 제공하면 3GPP 회원의 이익에 크게 도움이 된다고 동의하는 경우의 기관
- o 상기 기준외에 국내 심사요건에 적합한 업체인 경우

6. 배포 절차

① 수요자(협약에서 "승인된 수령인")는 어느 한 3GPP 표준화기구(협약에서 "3GPP 알고리즘 보관자")에게 알고리즘 사본 "N"매 요구서(이 경우 N은 10매 이내임)를 제출한다.

② 요구서를 접수한 TTA는 수요자가 면허부여 기준에 적합한가를 심사하여야 한다.

- 3GPP 알고리즘 면허부여 적합 심사위원회 구성운영
- 필요시 요구기관에 대한 실사, 평가

③ 승인기준에 적합한 경우, TTA는 수요자에게 "비밀유지 및 제한사용 보증 약정서" 2매를 송부한다.

④ 3GPP 알고리즘 수요자는 TTA로 1000유로 상당의 관리비와 함께 수요자가 서명한 상기 문서를 제출한다.

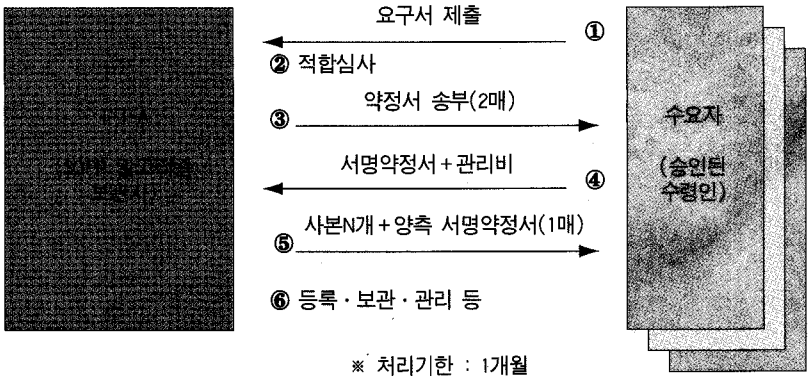
⑤ TTA는 수요자에게 3GPP 알고리즘 사본 N개와 TTA가 서명한 상기 문서 1부를 송부한다.

⑥ TTA는 3GPP 알고리즘 배포에 관련된 등록을 유지하여야 하며, 수요자들에게 송부한 문서와 수요자들이 제출한 "비밀유지 및 제한사용보증 약정서"에 부서(副署 : Countersign) 하여 보관한다.

* 수출에 관한 절차는 기본적으로 상기 절차를 준수하되 수출에 관련된 정부부처나 기관의 절차를 밟아 필요시 정부허가를 취득하기 위한 적절한 조치를 하여야 한다.

7. TTA 관리절차 및 의무

- o 3GPP 알고리즘 요청의 심사 및 승인
- o 수요자와 약정서 체결 및 교환

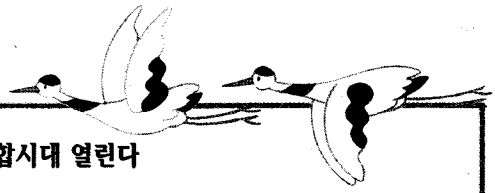


〈그림 2〉 배포 절차

- o 3GPP 알고리즘의 배포
- o 3GPP 알고리즘 등록 유지 및 관리
- o 필요시 국가부처에서 요구되는 행정적인 허가, 정책협의 등과 수출시 수출 관련 행정처리 및 면허 획득
- o 수요자에 대한 제한적인 기술지원(알고리즘이나 시험데이터에서 나오는 질의서 회신)
- o 3GPP PCG와 상호연락 및 통지
- o 다른 3GPP 보관자에게 알고리즘 등록명부를 6개월마다 통보

8. 결론

우리나라에서 제공되는 제2세대 이동통신서비스에서는 가입자인증 암호알고리즘을 사용안하고 있어서 이러한 암호알고리즘 관리 및 배포제도는 제3세대 이동통신서비스부터 새롭게 도입되는 것이다. 이는 향후 3세대 가입자인증 및 전세계로밍서비스를 위해 필수불가결한 부분이기 때문에 반드시 조기도입해 관련기술의 국내화 및 동 알고리즘을 삽입한 관련 칩의 개발이 국내 제조업체 및 연구기관 등을 통해 조속히 이루어져 국내공급은 물론 외화획득 및 국제 경쟁력 제고에 일익을 담당하여야 할 것 같다. 이 제도는 서론에서도 언급되었듯이 5월말 현재 공동소유 및 관리기관인 4개 표준화기관에 서면으로 협약체결을 추진중에 있어 6월중에는 정식으로 동 제도가 시행될 것으로 예측되며 관련기관 및 업계의 적극적인 협조가 필요한 형편이다. 끝으로 TTA가 우리나라의 통신사업자, 제조업체 등의 요청에 따라 동 알고리즘 개발 및 시험에 공동투자키로 결정하였지만 이에 대한 투자비용은 정부가 정부 연구기관을 통해 정책연구과제에서 전액 지원하였음을 상기할 필요가 있다. TTA



전화선 통한 위성방송 · DSL 서비스 통합시대 열린다

전화선을 통해 인터넷뿐 아니라 위성방송도 시청할 수 있는 길이 열렸다. 인터넷뉴스 「컴퓨터커런츠」에 따르면 미국의 디지털가입자회선(DSL)서비스 개발업체인 엠페이스테크놀로지스(http://www.mphasetech.com)와 위성방송업체 알파스타인터내셔널(http://www.alphab2b.com)은 전화선을 이용한 위성방송, DSL 통합서비스를 세계 처음으로 공동 개발, 5월부터 서비스에 나섰다. 양사는 전화선을 이용한 디지털방송과 고속 인터넷서비스를 위해 엠페이스의「트래버서」기술과 알파스타의 위성방송 수신기술을 결합해 이 같은 성과를 거뒀다. 엠페이스의 「트래버서」기술은 기존의 전화선을 통해 음성통화 외에도 1Mbps의 고속인터넷서비스와 400개 채널의 디지털방송 서비스를 지원할 수 있다. 엠페이스와 알파스타는 이번 서비스 개발로 일반인들이 가정에 설치된 전화선을 통해 유선방송과 위성방송 시청은 물론 DSL서비스를 통해 음악, 게임소프트웨어 등을 고속으로 내려받을 수 있으며 아울러 주문형비디오(VOD) 방식으로 영화도 시청할 수 있다고 밝혔다. 양사는 전화업체들과 계약을 맺고 서비스를 제공하는데 전화업체들은 통신위성으로부터 데이터를 송수신할 수 있는 초소형위성통신지구국(VSAT)을 설치해 가입자들에게 위성방송서비스를 제공한다. 엠페이스와 알파스타는 5월 지역전화회사인 하트텔레폰을 통해 첫 서비스를 제공하는 한편 연말까지 5개 이상의 전화사업체를 확보해 서비스 확대에 나설 계획이다. 아울러 양사는 「엠페이스텔레비전」이라는 합작사를 설립해 이와 관련된 기술과 서비스를 계속 개발해 나갈 예정이다. 알파스타의 매모우드 와바 사장은 이 서비스에 대해 「미 전역에서 기존의 전화선을 통해 유선방송, 위성방송, 라디오방송을 함께 즐길 수 있는 길이 열렸다」고 의미를 부여하며 「곧 전세계를 대상으로 서비스를 실시할 것」이라고 밝혔다. 그는 또 「인터넷과 위성방송을 비롯한 뉴미디어 시장에서 케이블사업체나 위성통신업체에 밀려왔던 기존 전화사업체들도 이 서비스로 인해 경쟁력을 갖출 수 있게 됐다」고 말했다.