ITU-T SG13 WP2/13

이재섭 • ITU-T SG13 부의장, WP2/13 의장
KT 제네바 사무소 소장

1. ITU-T WP2/13 개요

ITU-T의 SG 13은 Multi Protocol 환경에서의 통신망 구조 및 IP 기반의 통신망에 관한 연구를 담당하고 있는 연구반으로 산하에 4개의 Working Party를 가지고 망 연동, 프로토콜 메커니즘, Performance 및 NGN 등에 관한 표준화 연구를 폭넓게 수행하고 있다. 이 중 WP 2/13은 망 구조와 연동에 관한 표준화를 담당하고 있는 그룹이다. 금번 연구회기(2000~2003) 들어 본 그룹에서 추진되고 있는 주요 표준화 쟁점은 MPLS 기반의 통신망을 공중망에서 수용하기 위한 연동문제와 NGN에 관한 표준화 등이 그 주가 되고 있다.

WP2/13은 이와 같은 망 구조 및 연동에 관한 주제를 기반으로 총 6개의 연구과제(Questions)를 가지고 표준화 활동을 진행하고 있으며 각 연구과제의 구성 및 연구범위는 다음 표와 같다.

금번 회의는 2002년 7월 2일부터 11일까지, 일본 치토세(Chitose)시에서 Special Rapporteur 그룹 회의를 포함한 Working Party 총회로 진행되었다. 금번 회의 주요 주제는 연동 일반구조 모델에 관한 권고(안)의 승인과 ATM-MPLS 연동을 위한 권고 개발 및 VoMPLS를 위한 표준의 개발 그리고 NGN에 관한 기초작업들이 이루어졌으며 QoS Architecture에 관한 권고 초안의 작업이 또한 이루어지기도 했다.

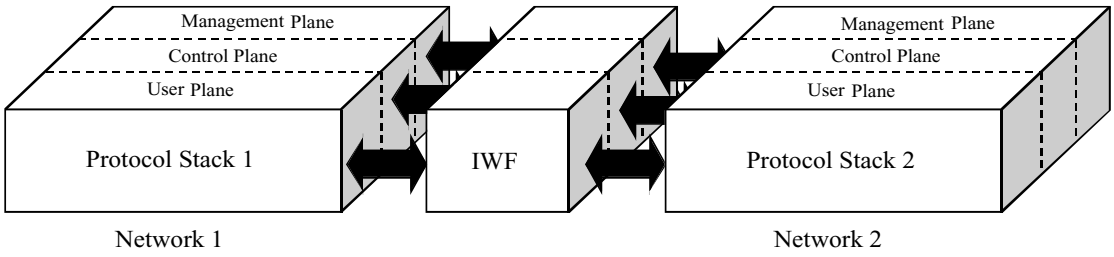
연구과제	연구주제	담당 Rapporteur
Q1/13	Principles, Requirements, Frameworks and Architectures for an Overall Heterogeneous Network Environment	Mr. Keith KNIGHTSON(캐나다, NT)
Q5/13	Network Interworking including IP Multiservice Networks	Mr. Ghassem KOLEYNEI(캐나다, NT)
Q10/13	Core Network Architecture and Interworking Principles	Mr. Naotaka MORITA(일본, NTT)
Q13/13	Interoperability of Satellite and Terrestrial Networks	Mr. Tolgar ORLS(미국, Intelsat)
Q14/13	Access Architecture Principles and Features at the Lower Layers for IP-Based and Other Systems	Mr. L.-O. HASTER(스웨덴, Ericsson)
Q16/13	Telecommunication Architecture for an Evolving Environment	Ms. Hui-Lan, LU(미국, Lucent)

2. 연동구조 모델에 관한 표준의 개발 (Q 1/13)

IP를 기반으로 하는 통신기술이 발전하면서 발생하는 쟁점 중에 하나가 IP 기반의 통신망과 공중망(Public Network)간의 연동(Interworking) 문제이다. 특별히 IP를 기반으로 하는 서비스가 증가하면서 기존 공중망을 통하여 제공되던 서비스와의 통신 요구가 급격히 증대되고 있으며 이는 결국 연동에 관한 문제로 제기되고 있는 것이다. 이러한 IP 기반의 연동문제를 다루는 데 있어서 어려움 중에 하나가 연동구조의 문제라 할 수 있다. IP의 속성상 특정한 하부계층 기능에 영향을 별로 받지 않는 터에다 최근 각광받고 있는 MPLS의 경우 그 속성이 "MPLS over Anything and Anything over MPLS"로 불리워질 만큼 어느 특정계층(Layers)에 대한 제한을 받지 않는 상황에서 공중망과의 연동을 원활히 이루기 위해서는 무엇보다도 연동에 관한 구조적 안내가 필요하다 하겠다.

권고(안) Y.1251 "General architectural model for interworking"은 이러한 요구사항을 담은 신규 권고(안)으로 현재와 같은 Multi-Protocol 환경에서 연동을 위한 하부기반으로서 수평적, 수직적 관점의 연동구조를 규명하고 있다. 즉 연동에 필요한 Protocol adjacency를 수직적인 관점과 수평적인 관점에서 규명함으로써 다양한 환경에서의 연동처리를 위한 기본 틀을 제시하고 있는 권고이다. 또한 본 권고(안)에서는 현재 여러 목적으로 혼용되어 사용되고 있는 "Service Interworking"과 "Network Interworking"에 대해 다음과 같이 정의하고 있어 향후 다양하게 요구되어질 연동상황에 대비하도록 하고 있다.

- Service Interworking : In service interworking, the Interworking Function (IWF) terminates the protocol used in network 1 and translates(i.e. mapping) the Protocol Control Information(PCI) to the PCI of the protocol used in network 2 for User, Control and Management Plane functions to the extent possible. In general, since not all functions may be supported in one or other of the networks, the translation of PCI may be partial or non-existent. However, this should not result in any loss of user data since the payload is not affected by PCI conversion at the service interworking IWF.
- Network Interworking : In network interworking, the PCI of the protocol used in network 1 and network 2 and the payload information are transferred transparently by an IWF. Typically the IWF encapsulates (known as tunneling in some specifications) the information which is transmitted by means of an adaptation function and transfers

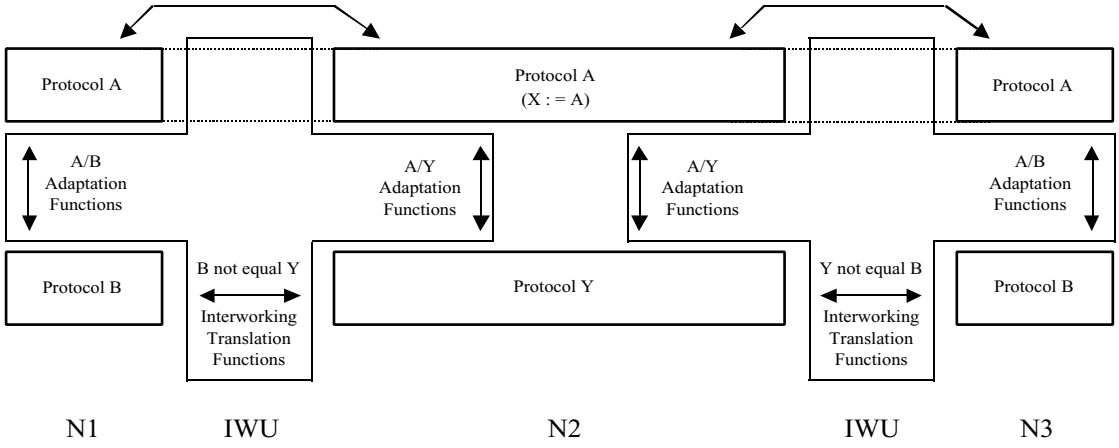


(그림 1) Interworking Function

it transparently to the other network.

이 권고(안)은 작년 11월 회의에서 제안되어 지난 1월 회의 및 금번 회의를 통해 정식 권고(안)으로 확정하기 위한 AAP 승인절차에 회부되었다. 본 권고(안)에서 규정하고 있는 프로토콜 계층의 관계성을 간략히 도시하면 다음과 같다.

통일하기 위하여 약 18개월에 걸친 노력을 하였으나 하나의 안 개발은 차치하고 기본적인 인식조차 접근하지 못함으로써 관련 표준화 협의에 상당한 지장을 초래하였었다. 결국 금번 회의를 통해서도 단일 방안을 도출하는 데는 실패하였으나 이들 두 가지 모드(Mode) 모두를 표준으로 채택하기로 함으

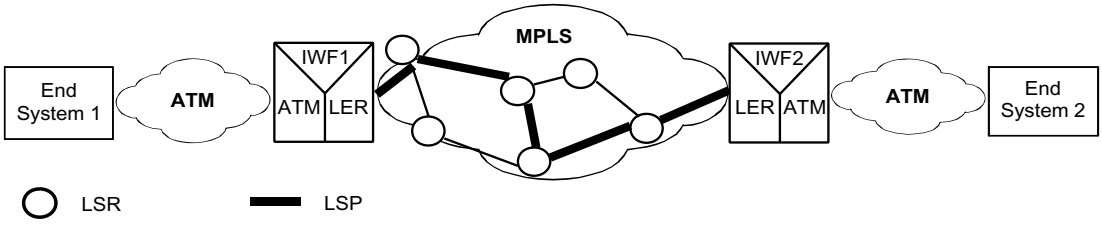


(그림 2) 연동 구조 응용 예

3. ATM-MPLS 연동에 관한 표준의 개발

금번 회의 주요 결과 중 하나는 ATM-MPLS 연동을 위한 기본 합의라 할 수 있다. 그 동안 ATM-MPLS 표준의 신속한 개발의 걸림돌이 되어 왔던 서로 다른 모드(Cell Mode와 Frame Mode)에 대한 상호 이해가 넓어져 기본적인 합의에 이르게 된 것이다. 그동안 이 두 가지 서로 다른 모드를 하나로 로써 현재의 답보적인 상태에서 벗어나 MPLS를 보다 다양하게 공중망에 사용하기 위한 작업으로 나설 수 있게 되었다. 서로 다른 두 가지 모드에 대한 궁극적 판단은 시장의 선택에 맡겨야 하는 아쉬움은 있으나 다양한 환경변화를 고려할 시 나름대로는 최선이었다는 판단이다.

ATM-MPLS 연동을 위한 일반 망 구조 모델을 살펴 보면 다음 (그림 3)과 같다. 이 구조 모델은 일반

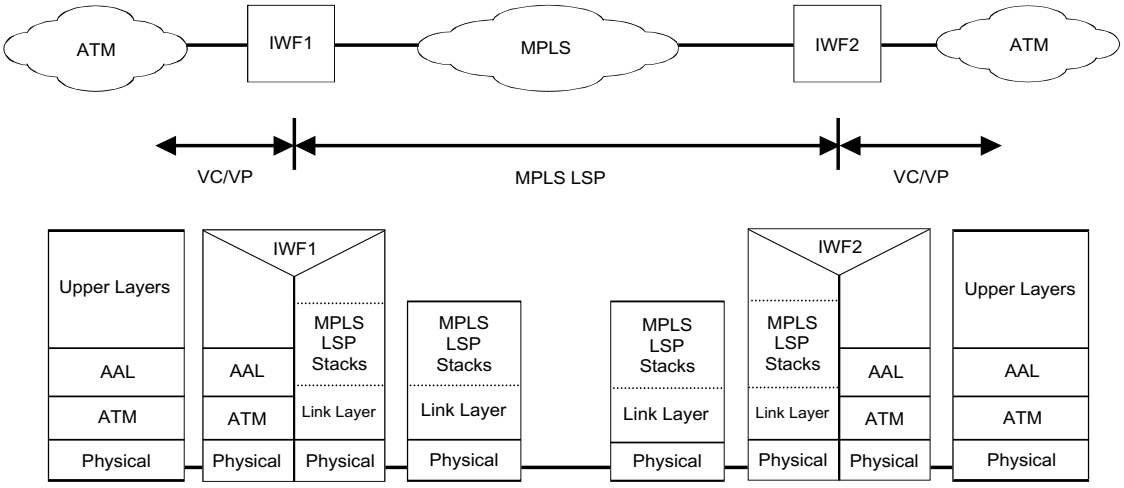


(그림 3) ATM-MPLS Network 연동을 위한 일반 망 구조 모델

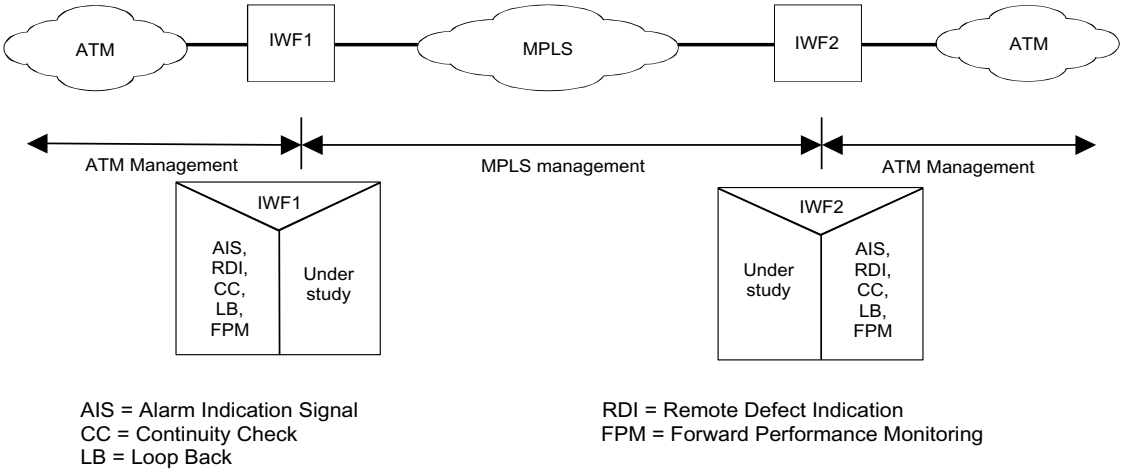
적으로 MPLS가 ATM Access망 간의 전달을 위한 Backbone Transport Network으로서의 역할을 담당한다는 시나리오를 기반으로 하고 있다. ATM→MPLS 방향의 경우 IWF1에서 ATM Cell은 MPLS Frame으로 Encapsulation되게 되며 MPLS→ATM 방향의 경우 IWF2에서 다시 ATM Cell로 재구성 되게 된다. (그림 4)와 (그림 5)는 이러한 환경에서 요구되는 User Plane과 management Plane 연동구조 모델을 나타내고 있다.

3.1 Cell 모드 연동 권고(안) Y.atmplsC

권고(안) Y.atmplsC는 Cell Mode 연동에 관한 권고(안)으로서 ATM Connection과 Interworking LSP 간의 mapping에 있어 "One-to-One" 및 "N-to-One"의 두 가지 응용을 정의하고 있으며 이에 대한 Encapsulation Format을 정의하고 있다. 금번 회의를 통하여 본 권고(안)의 서술 내용이 상당히 안정된 것으로 판단되어 다음 11월 SG 13 회의 시

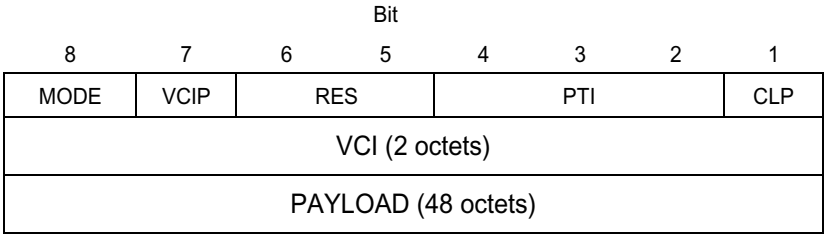


(그림 4) ATM-MPLS User Plane 연동구조 모델

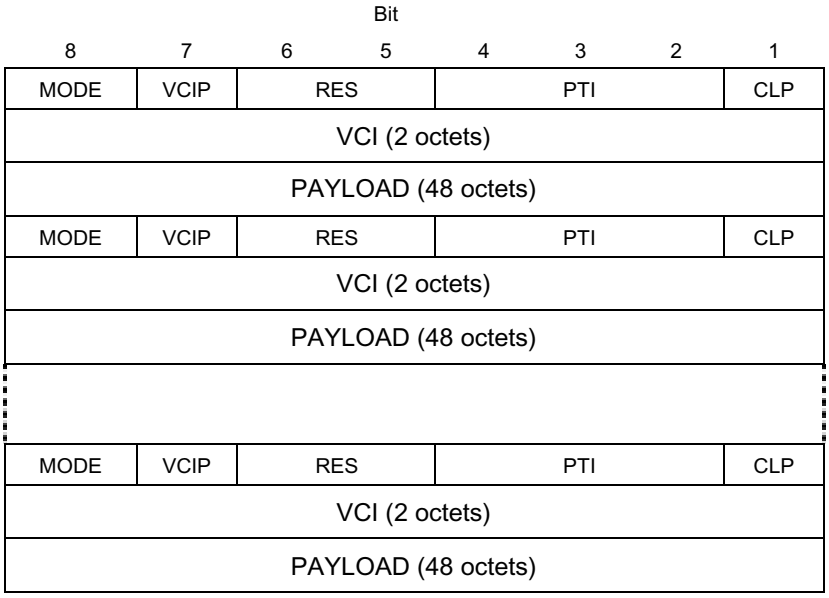


(그림 5) ATM-MPLS Management Plane 연동을 위한 참조 모델

특별한 제안이 없는 경우 권고 승인 절차 AAP에 회
부할 예정이다.

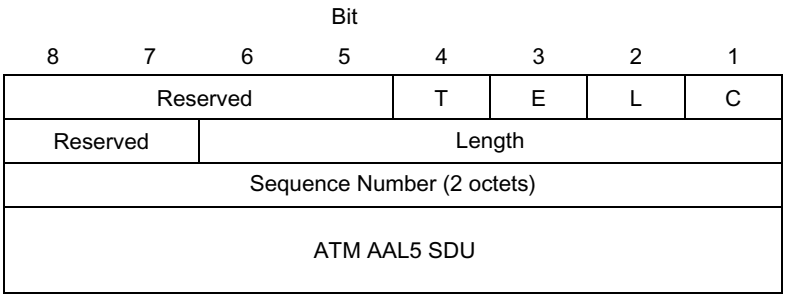


(그림 6) Single Cell Encapsulation Format



(그림 7) Concatenated Cell Transport를 위한 Encapsulation format

3.2 Frame Mode 연동 권고(안) Y,atmplsF



(그림 8) AAL5-SDU transport를 위한 Encapsulation

권고(안) Y.atmplsF는 Frame Mode 연동에 관한 권고(안)으로서 기본적으로 AAL5의 PDU 기반과 SDU 기반의 Frame을 수용하기 위한 두 가지 Sub-Mode를 규정하고 있다. 이 권고(안) 역시 다음 11월 SG13회의에서 특별한 제안이 없는 경우 권고 승인절차 AAP에 회부될 예정이다.

4. Voice over MPLS에 관한 표준의 개발

VoMPLS를 위한 표준화에 있어서는 금번 회의를 통해 서비스 요구사항의 정립이 어느 정도 마무리 단계에 들어가 다음 회의 때 권고 승인절차에 회부하기로 되었다. 또한 이를 위한 프로토콜의 개발에 있어서는 그동안 논쟁의 근간이 되었던 서비스 시나리오에 보다 구체적인 논의가 이루어졌다. 즉, 그동안 MPLS Forum을 기반으로 Voice를 직접 MPLS Frame에 담아 전달하는 Vo direct MPLS의 제안에 대한 검토가 주요 쟁점사항이었으나 이에 대한 시장의 불투명성과 IP 기반을 배제하는 것에 대한 염려 등으로 별 논의의 진전이 없었다. 이러한 염려를 수용하여 금번 회의에서는 Voice over MPLS에 관한 일반적 서비스 요구사항의 정립을 기반으로 관련 프로토콜의 개발을 VoMPLS와 기타 방법(예 : VoIPoMPLS, VoAAL2oMPLS 등)에 관한 부분으로 구분하여 표준화하기로 하였으며 이중 VoMPLS에 대한 부분은 그동안 제시된 기고문들을 근간으로 권고화 작업이 진행되어 Voice over MPLS 서비스 요구사항 권고(안)과 더불어 다음 SG13 회의에서 권고 승인절차에 회부하기로 하였다.

5. NGN에 관한 표준의 개발

현재 Market에서 상당한 수준으로 사용되고 있는 용어인 NGN에 대하여 ITU-T관점에서 표준화를 직접 다루기로 한 것은 지난 2월 SG13 회의의 결정사항이었다. 금번 회의에서는 이러한 결정사항을 기반으로 Q1/13에서 Architecture의 관점에서 NGN 표준화에 관한 보다 구체적인 논의가 이루어지게 되었다. NGN(Next Generation Network)이라는 용어의 속성상 기술적인 비전이나 서비스적인 비전을 담기에 매우 곤란한 어려움이 있으나 다음과 같은 가정을 기반으로 2004년 정도에 구현가능한 모델을 정립하기로 하였으며 금번 회의에서는 이를 위한 Living List Item들이 정리되어 차기 회의 기고문을 위한 참조가 되도록 하였다.

1) 초기 NGN은 Packet Voice 서비스를 위한 Network로 정의되나 향후에는 멀티미디어 서비스를 지향한다.
2) NGN의 주요한 전달망으로써 Ethernet 기반의 전달 능력을 고려하며 이를 공중망에서 수용하기 위한 연구를 포함한다.
3) NGN은 기본적으로 Optic Infrastructure에서 구현되는 통신망으로 정의한다.

6. 결론

대부분의 Architecture 문서가 그러하듯이 언뜻 보기에 그저 그렇고 그런 논리들을 잘 정리해 전개해 놓은 것 같은 권고(안) Y.1251의 경우, 현재 모든 면에서 혼동되어 있는 연동의 필요성과 적용 및 그 활용 방안에 대해 잘 규정하고 있어 통신 사업자들이나 산업체에서 관련 시스템을 설계할 때 매우 유익한 지침이 될 것이다. 특히 지금과 같이 IP 기반의 응용이 너무나 다양하게 공중망과 혼동되어 사용되고 있는 상황에서는 매우 유익한 안내서 역할을 할 것이라 생각한다.

현재 대부분의 통신사업자들은 가까운 미래의

Backbone Network로서 MPLS 개념을 갖춘 통신망을 고려하고 있다. 이러한 MPLS의 구현에는 ATM을 기반으로 하는 것과 SDH나 DWDM 등을 기반으로 하는 것 등의 여러 가지가 논의되고 있는 것이 현실이다. 이러한 MPLS의 Backbone Network로서의 활용에 있어 초기에 그 가능성을 갖추고 있는 것이 ATM 기반의 MPLS라 할 수 있다. 이는 기 설치된 ATM 망의 활용도를 높이고 또한 IP 기반의 서비스에서 요구되고 있는 다양한 QoS 요구사항을 좀 더 유연하고 소프트한 방법으로 제공하기 위한 시도의 일환이라 할 수 있다. 이 경우 즉 MPLS가 이러한 환경에서 Backbone Network로 사용될 때 가장 기본으로 필요한 표준이 바로 ATM –MPLS 간 연동에 관한 표준이라 할 수 있다. 이러한 관점에서 비록 이번에 단일(안)을 만드는 데는 이르지 못했으나 전체가 합의하여 두 가지 모드의 권고(안)을 안정된 수준으로 작업하게 된 것은 향후 MPLS의 공중망 응용을 활성화 할 수 있는 좋은 계기가 될 것이라 사료된다.

전자서명 – 유선과 무선PKI의 차이점

유선에서 사용하는 PKI와 무선에서 사용하는 WPKI는 무엇이 다를까. 양자간 가장 큰 차이점은 인증서를 검증하는 데 있다. 일반적으로 PKI 시스템을 사용하는 데 있어 클라이언트가 가지는 가장 큰 컴퓨팅 부하는 상대방의 인증서를 검증하는 것이다. 신뢰할 수 있는 인증기관이 서명한 것인지, 인증기관의 서명이 올바른지, 유효기간은 적절한지 등을 검증해야 한다. 이러한 작업을 하기 위해서는 클라이언트에 인증서폐지목록(CRL)을 비롯한 각종 정보들이 필요한다. 유선환경에서는 디렉터리 서버로부터 이런 정보를 주기적으로 다운로드해 사용하면 되지만 무선 인터넷 환경에서는 제한된 컴퓨팅 파워와 메모리 한계 때문에 사실상 불가능하다. 따라서 무선 환경에서는 SLC(Short Lived Certificate)와 실시간 인증서상태검증(OCSP) 방식을 이용한다. SLC방식은 인증서 유효기간을 기존의 인증서 폐지목록 갱신주기와 비슷하게 해서 클라이언트가 해당 인증서에 대한 인증서 폐지목록 검증작업을 하지 않도록 하는 방식으로 SK텔레콤이나 LG텔레콤의 WAP(Wireless Application Protocol) 환경에 주로 사용된다. OCSP는 별도의 서버를 두는 방식으로 클라이언트가 수신한 인증서를 OCSP 서버에 보내 그 인증서의 유효성을 검증하는 방식이다. 유무선 PKI의 또다른 차이점은 암호화 알고리즘이다. 유선상에서 서명용 알고리즘은 대개 RSA나 국내 표준인 KCDSA가 사용됐지만 무선 환경에서는 단말기의 제한된 성능 때문에 이들 알고리즘을 사용하지 못한다. 대신 엘립틱 커브(Elliptic Curve)를 이용한 ECDSA가 주로 이용된다. RSA는 키의 길이가 1024비트인데 비해 ECDSA는 약 160비트로 짧으면서도 1024비트인 RSA와 같은 수준의 보안강도를 지닌다. 이에 따라 국내뿐만 아니라 세계적으로 무선에서는 엘립틱 커브를 이용한 암호 알고리즘이 강세를 보이고 있다.