M-Commerce 보안기술 동향

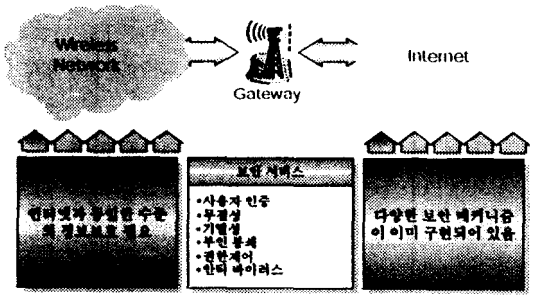
2002. 1.

류 재 철
충남대학교 정보통신공학부
jcryou@home.cnu.ac.kr

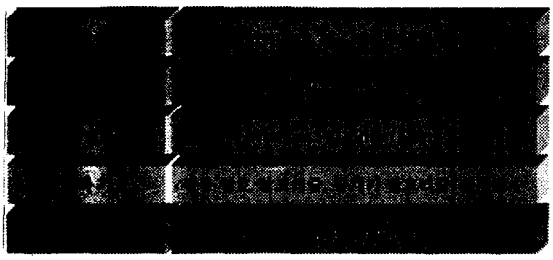
목 차

1. 개 요

무선인터넷 보안



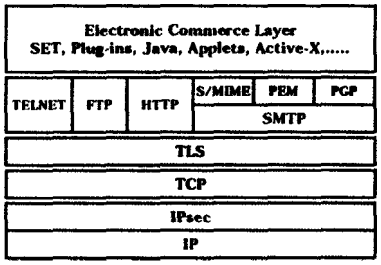
M-Commerce 보안기술



2. 안전한 통신기술

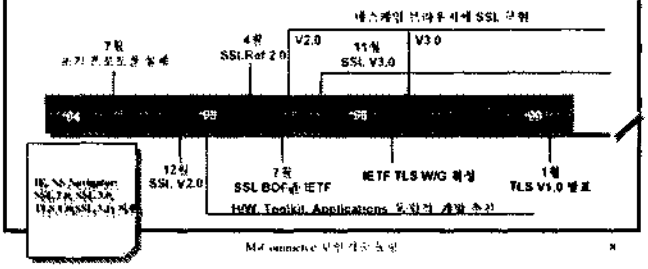
2.1 TLS

❑ Transport Layer Security



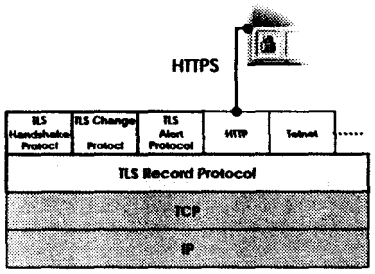
❑ Secure Socket Layer

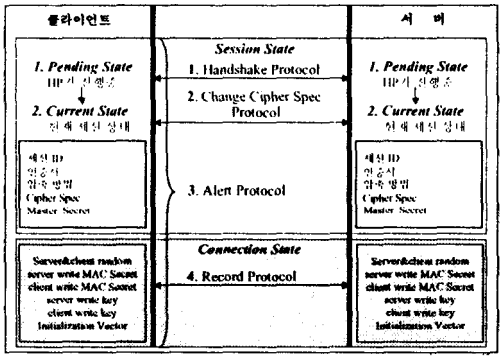
- 1994년 Netscape 사에서 처음으로 제안, 현재 SSL v3.
- TLS : IETF TLS W/G, SSL을 표준화 하기 위해 진행중
  - RFC 2246 : The TLS Protocol Version 1.0



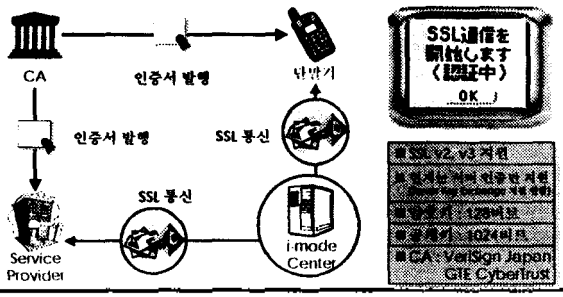
❑ TLS이 제공하는 보안 서비스

- 기밀성, 무결성, 사용자 인증
- 투명통신는 응용 수준에서 제공





I-Mode에서의 SSL



Wireless Extensions to TLS

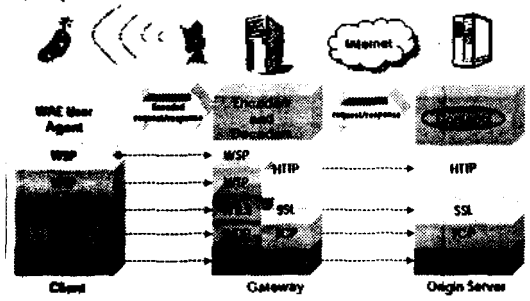
- Maximum Record Size Negotiation
- Client Certificate URLs
- Trusted CA Indication
- Small Session Identifiers
- Truncated MACs
- OCSP

```
struct {
  ProtocolVersion    client_version;
  Random             random;
  SessionID          session_id;
  CipherSuite        cipher_suites;
  CompressionMethod
                     compression_methods.
  Extension
                     client_hello_extension_list;
} ClientHello;

enum {
  reserved(0), max_record_size(1),
  client_certificate_url(2), trusted_key_ids(3),
  truncated_MAC(4), status_request(5), (65535)
} ExtensionType;
```

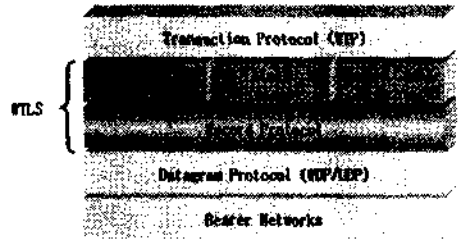
2.2 WTLS

❑ WAP 구조



❑ Wireless Transport Layer Security

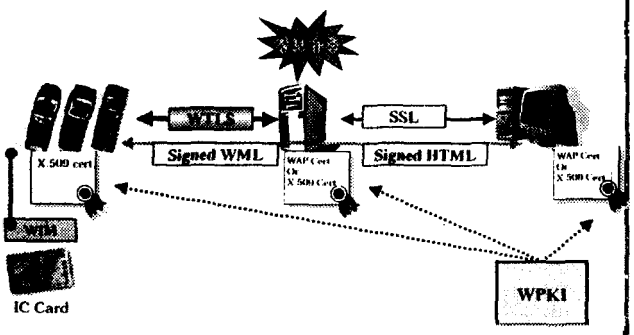
■ SSL 3.0/ TLS 1.0과 유사



WTLS 요구사항

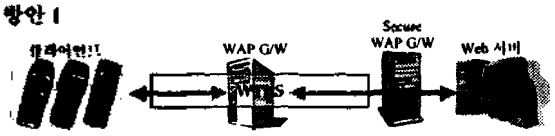
Datagram Transport Protocol	•UDS/WDP 상위에서 동작 •패킷의 중복/순서 등에 대한 처리가 필요
Slow Interactions	•Bearer에 따라 매우 긴 round-trip 시간을 갖는 경우가 있음.
Low Transfer Rate	•Bearer에 따라 전송율이 매우 낮은 경우가 있음.
Limited Processing Power	•단말기내 CPU의 성능 제한을 고려한 암호 알고리즘의 선택 필요
Limited Memory Capacity	•단말기내 메모리의 용량 제한을 고려한 암호 알고리즘의 선택 필요

WAP 보안 메커니즘



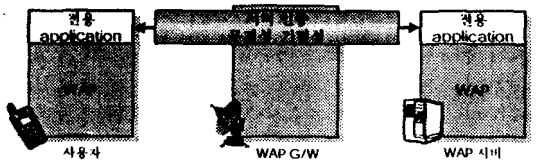
End-to-End Security Solution

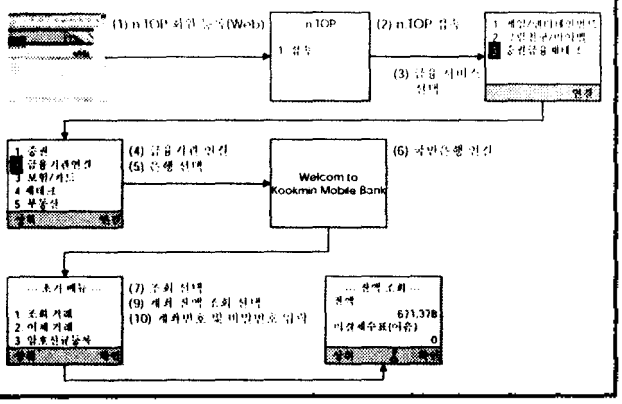
❑ 방안 1



❑ 방안 2

SKT WAP End-to-End Security



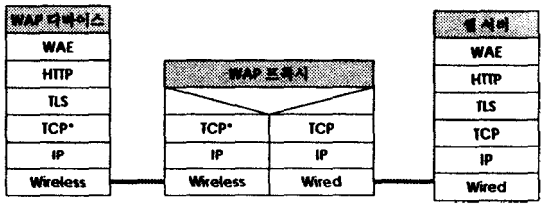


WAP 2.0

		WAP 2.0
컨텐츠 기술언어	• WML	• WML • WML2(XHTML) • CSS mobile profile 기반의 스타일 시트 지원
프로토콜	• WDP/WSP/WTP	• WDP/WSP/WTP • TCP/HTTP
보안 메커니즘	• WTLS	• WTLS • TLS
비 고		• GPRS, HSLSD, W-CDMA, CDMA2000 등에 적합

WAP 2.0 보안 메커니즘

❑ TLS Tunneling



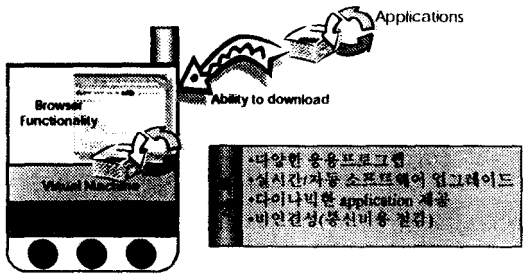
3. MExE 보안

❑ MExE (pronounced "mexy") : 3GPP

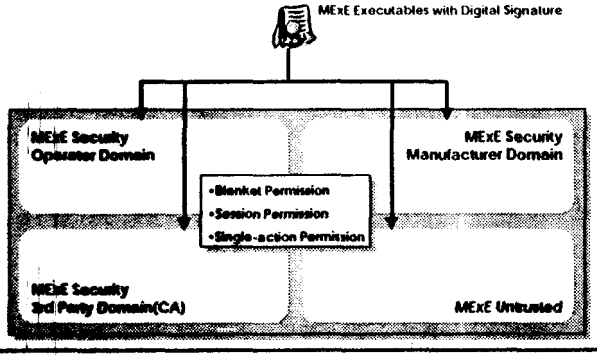
- Mobile Execution Environment
- 이동단말기를 위한 응용 프로그램 실행 환경의 표준화

"The popularity of next-generation mobile devices will be application-driven and not technology-driven!"

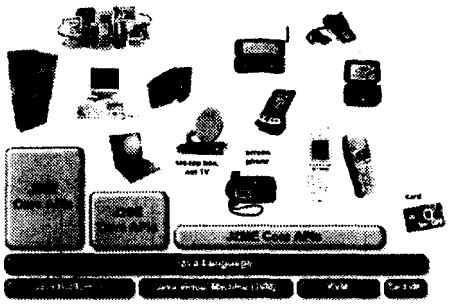
WAP environment	Small devices, limited display, processor and memory
PersonalJava Environment	Contemporary sophisticated devices, enhanced display, processor, memory
Java 2 ME CLDC Environment	Platforms for resource constrained, connected devices



❑ MExE Executable Authentication & User Permissions



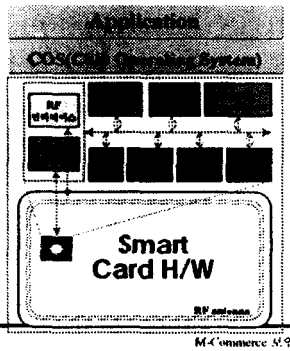
❑ Java Application Environments



4. 이동통신 카드

스마트카드 기술

❑ IC(Integrate Circuit)가 내장된 신용카드 크기의 플라스틱 카드

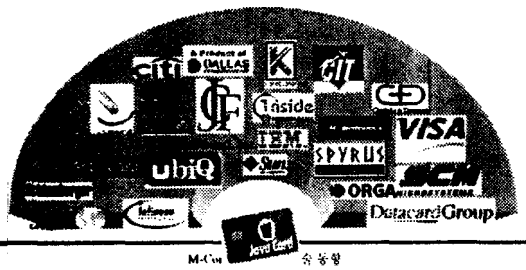


RF+Contact Smart Card

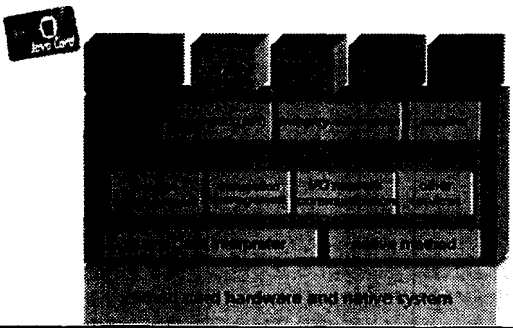
EEPROM : Electrically Erasable & Programmable
MMU : Memory Management Unit
RF : Radio Frequency

❑ Java Card - Sun Microsystems, Inc

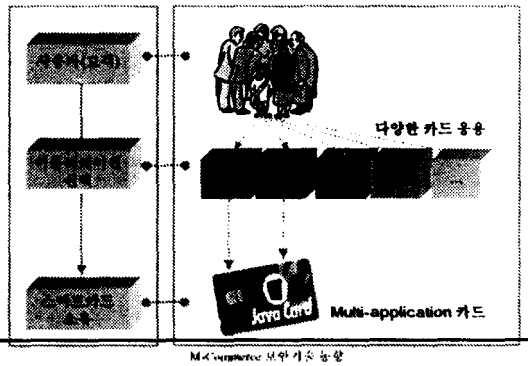
- 자바 프로그램(Applets)을 실행할 수 있는 스마트 카드
- Java Card 2.1 specification 발표 : 1999. 2. 24.
  - 스마트카드에 Java Card VM(virtual machine)과 Java Card 어플리케이션 개발에 필요한 API를 정의



❑ Java Card Software Architecture

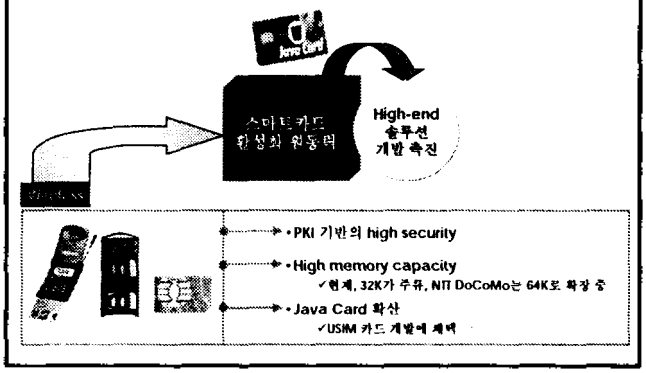


사용자 스스로 스마트카드 응용 선택



M-Commerce 보안기술 응용

이동통신 카드



M-Commerce 보안기술 응용 32

USIM 카드

❑ 다양한 정보 수록
- 가입자 정보(Subscriber data)
  - Phone Book
  - Frequently dialed numbers
  - Short messages…
- Secret Keys
- Applications

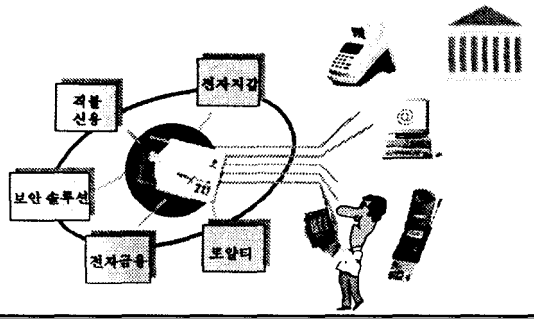
❑ 암호화 알고리즘 지원
- ANSI-41 CAVE(2G CDMA)
- A3/A8 (2G GSM)
- 3G AKA

❑ 자료 갱신
- 가입관련 파라메타의 다운로드
- 사용자 데이타의 다운로드
- 응용 프로그램의 다운로드

❑ 단말기를 통해 개인 정보 및 관련 자료 검색
- USIM카드에 저장된 개인식별 사용자 정보나 억세스 조건에 따라 검색
- 명령어나 동화 조작 가능 (Display, call customer sevice)

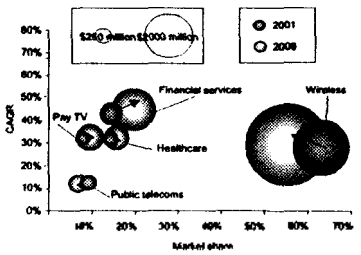
M-Commerce 보안기술 응용 33

Multi-Application



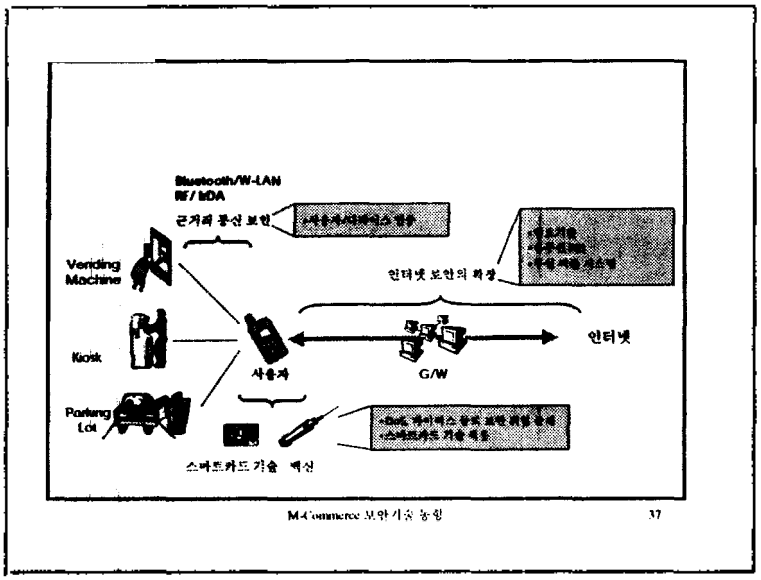
M-Commerce 보안기술 응용 34

시장 전망



M-Commerce 보안기술 응용 35

5. 결 론


Bluetooth/W-LAN
RF / IrDA
Vending Machine
Kiosk
Parking Lot
사용자
G/W
인터넷