

M-Commerce 시스템 구축

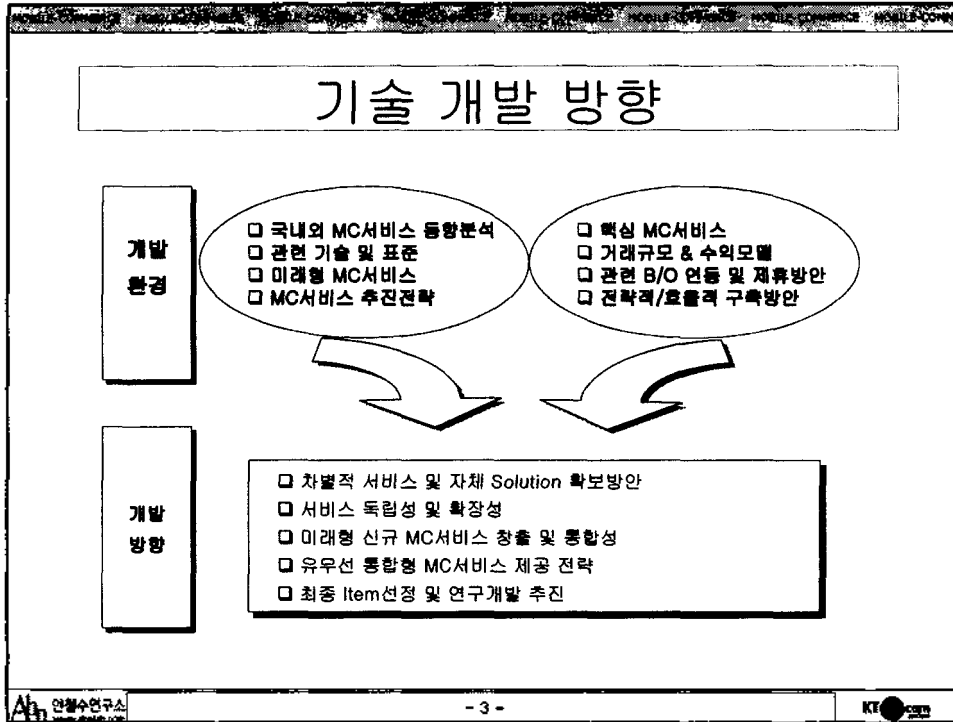
2001. 2.

한상학(안철수연구소)
송영준(한국통신이씨엔)

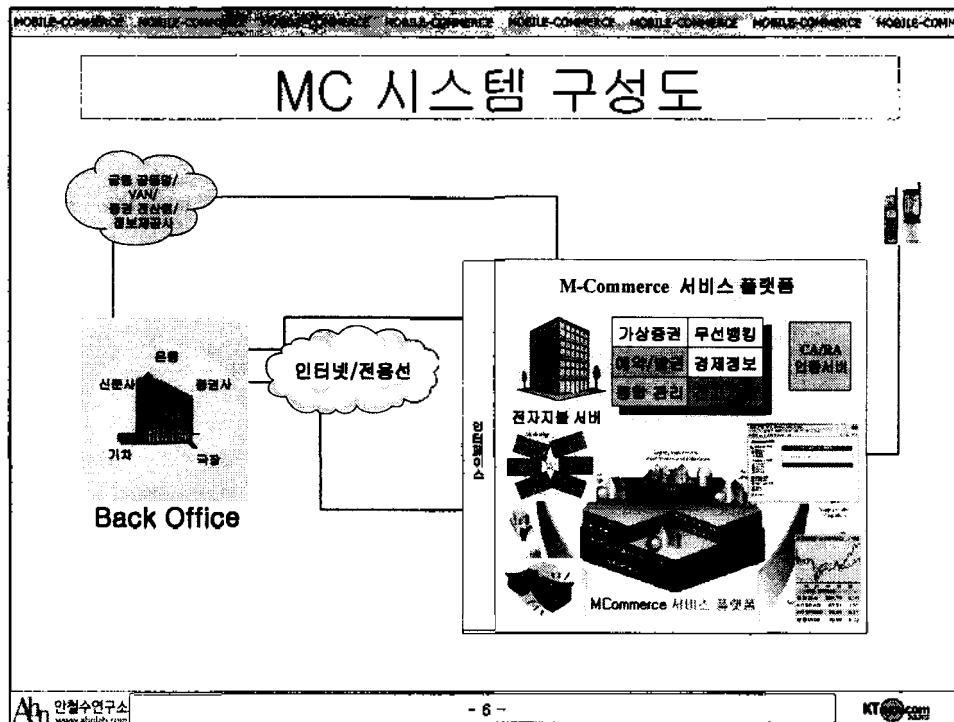
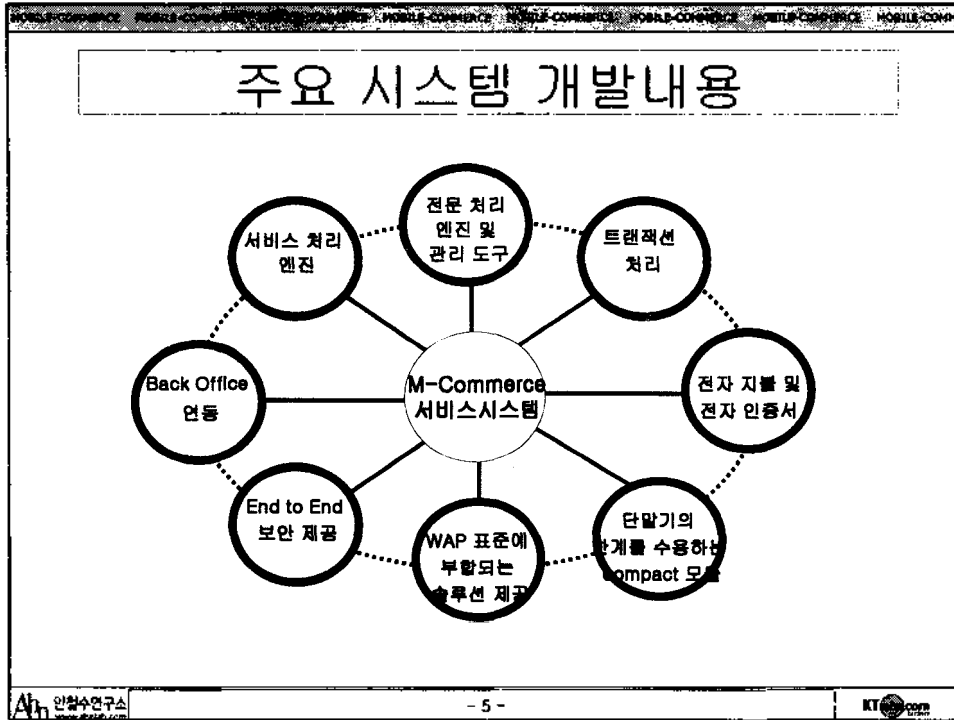
목 차

- 기술 개발 방향
- 개발 개요
- 주요 시스템 개발 내용
- MC 시스템 구성도
- 관련 소요기술
- MC 서비스시스템 개발 내용
 - 무선 보안/인증 서비스
 - 가상증권 서비스
 - 무선뱅킹 서비스
 - 전자지불 서비스
 - 예약/예약서비스
 - 경제정보서비스
 - 시스템 통합 운용관리
- 개발 고려사항
- Q & A





- ## 개발 개요
- IMT-2000 기반의 이동 멀티미디어 서비스의 일환
 - M-Commerce 서비스 제공을 위한 요소 기반 서비스의 개발
 - 무선 보안/인증 서비스
 - 전자 지불 서비스
 - 무선 뱅킹 서비스
 - 가상 증권 서비스
 - 예약/발권 서비스
 - 경제 정보 제공 서비스
 - 통합형 MC관리 서비스
 - 2002년 IMT-2000 상용서비스에 대비한 개발
 - 위 개별 서비스 근간의 M-Commerce서비스 시스템의 기반 구조 개발 및 구축
- 인텔수연구소
- 4 -
KT



MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMM

MC서비스시스템 주요 기능

- M-Commerce 서비스 엔진
- 전문 및 트랜잭션 처리 엔진
- 메시지 표준화
- 전문 편집기
- 로그 처리
- Back Office 연동
- DB Table 설계
- Web Servlet



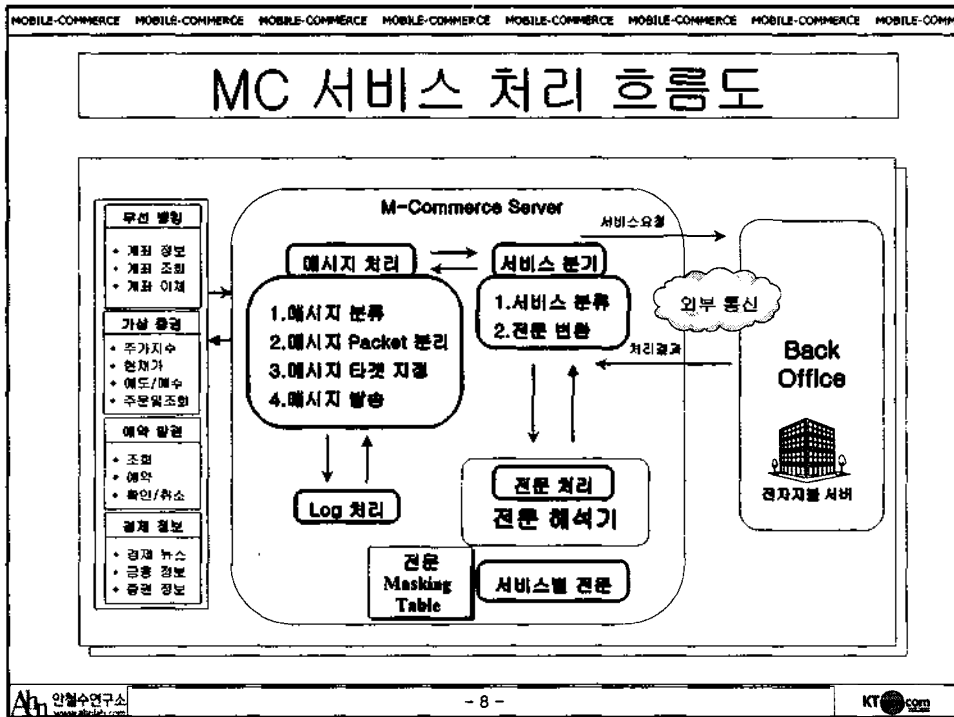
[자동이체]

계좌: 발기력이 달았네
가격: 6,000원
매수: 3매
은행명: 국민은행
계좌번호: 003-56-3456-788
예약하시겠습니까?






At 인철수연구소
KT.com



MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE

관련 소요기술 (1/2)

- 자바 Servlet / JSP(Java Server Page)
- WML 1.1 (Wireless Markup Language)
- 통신 프로토콜
 - TCP / IP , X.25
- 전문 Agent
 - 시스템 확장성, 유연성
- 전문 편집 기술
 - 메시지 프로토콜 표준화
- WebLogic
 - Web Application Server
- 데이터 베이스 처리
 - JDBC(Java DataBase Connectivity)
- Thread 처리
 - Process & Back Office 사이의 메시지 처리
- Payment Gateway
 - 전자 지불 연동
- WAP Browser
 - PDA Client

An 인텔수연구소 www.ahn.com
KT com
- 9 -

MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE

관련 소요기술 (2/2)

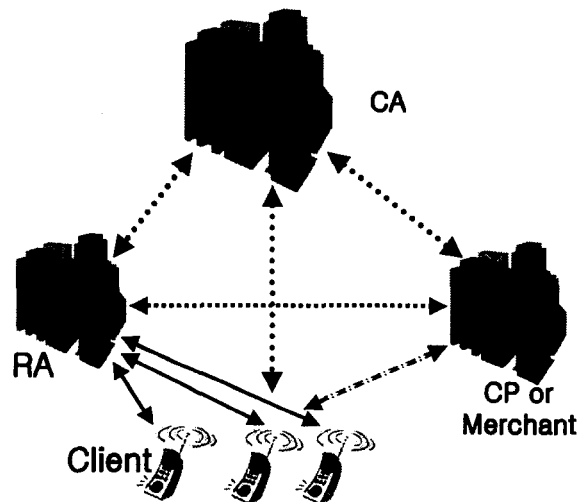
- 무선보안 Client & Server Module (Class3)
 - 인증서 Library
 - WTLS 서명/검증 Library
- WTLS CA
 - 무선보안 Client & Server 에 WTLS용 Cert 발급 기능
 - X.509 발급 CA 연동 Module
- 유무선 X.509 CA
 - 공인인증기관과 동일한 SPEC의 CA

An 인텔수연구소 www.ahn.com
KT com
- 10 -

MC 서비스시스템 개발 내용

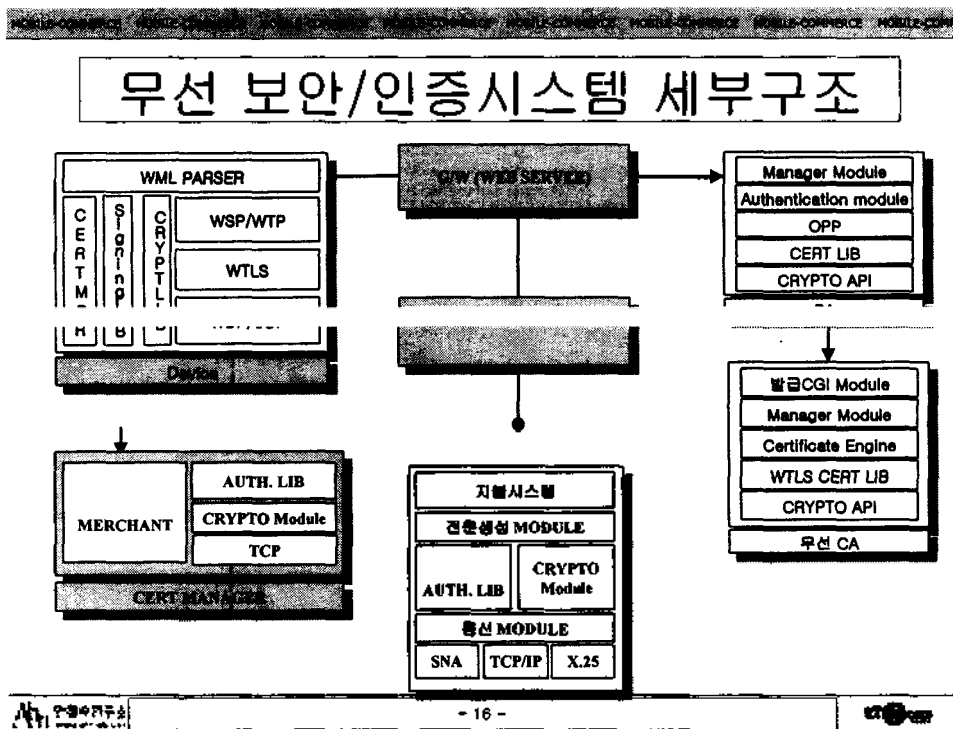
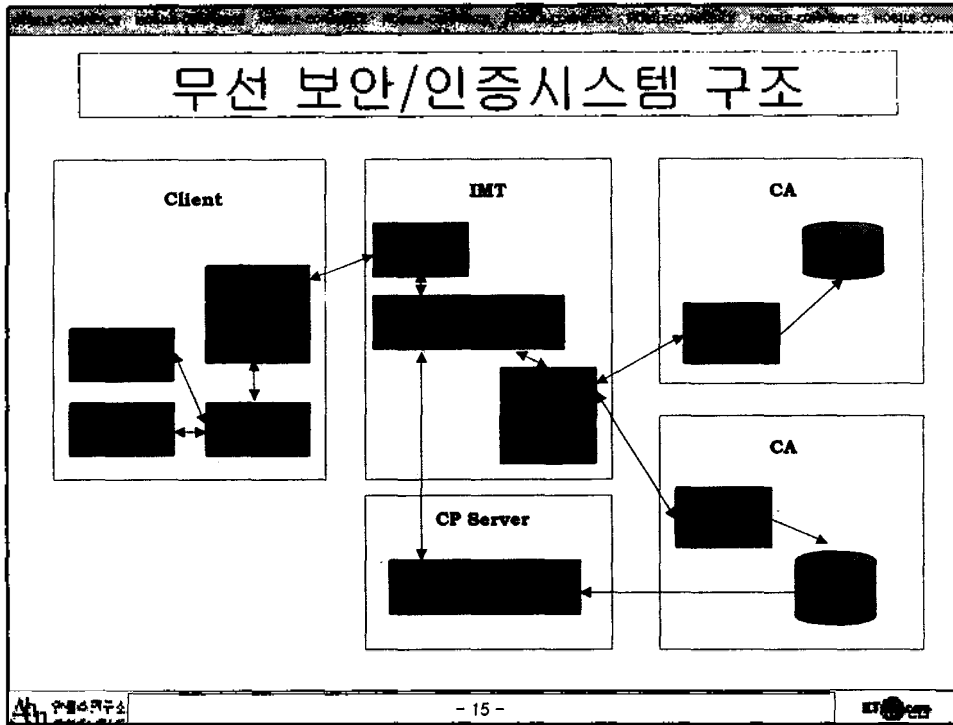
- 무선 보안/인증 서비스
- 가상증권 서비스
- 무선뱅킹 서비스
- 전자지불 서비스
- 예약/예매서비스
- 경제정보서비스
- 통합 운용관리

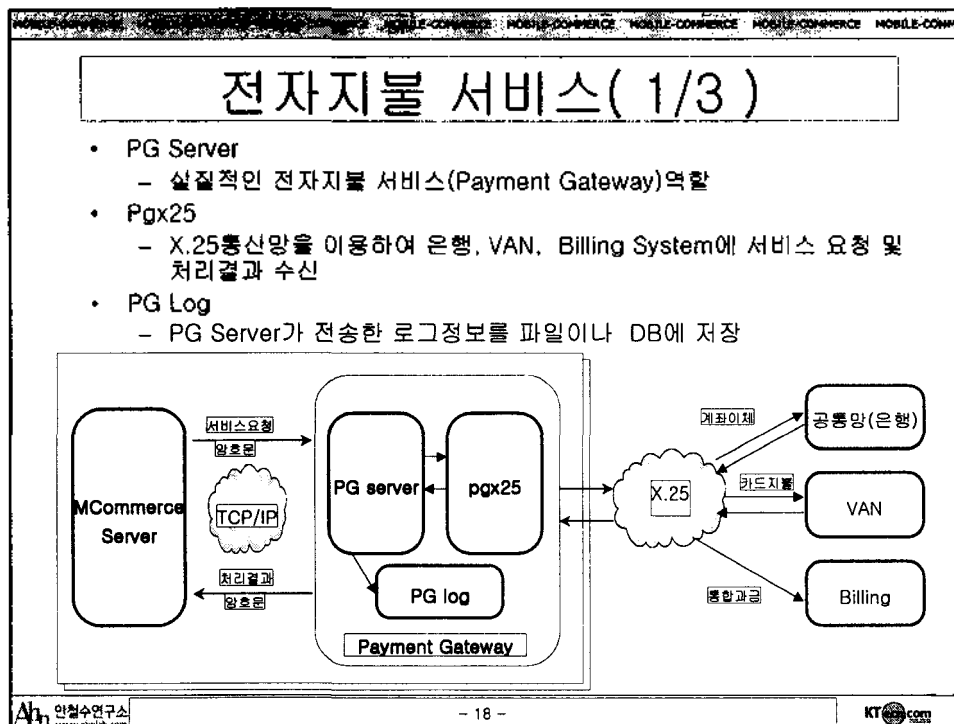
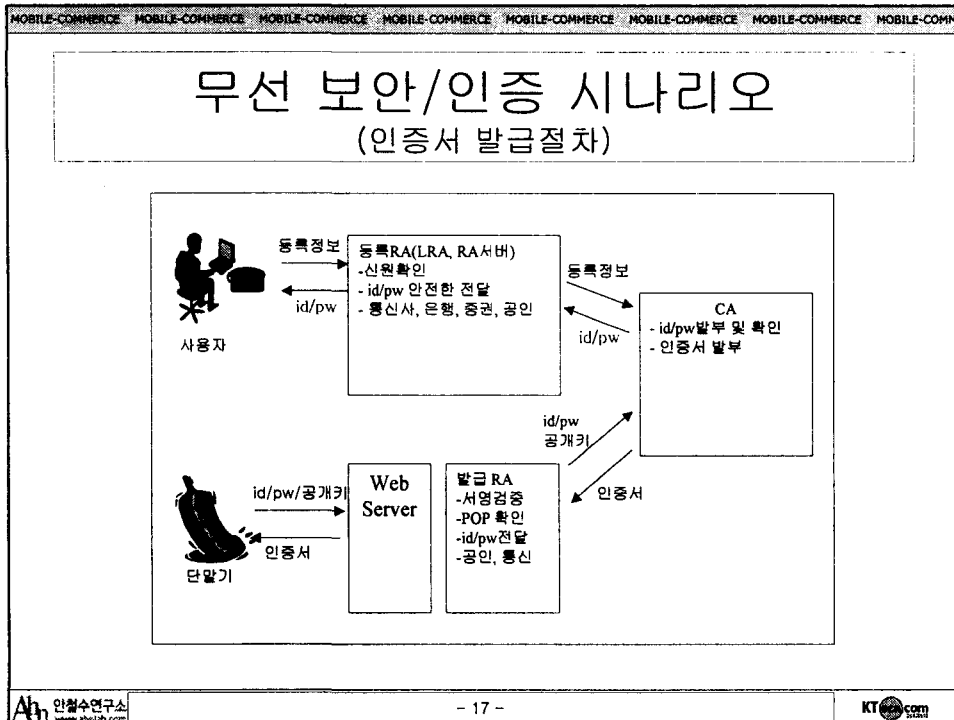
무선 보안/인증 서비스 체계

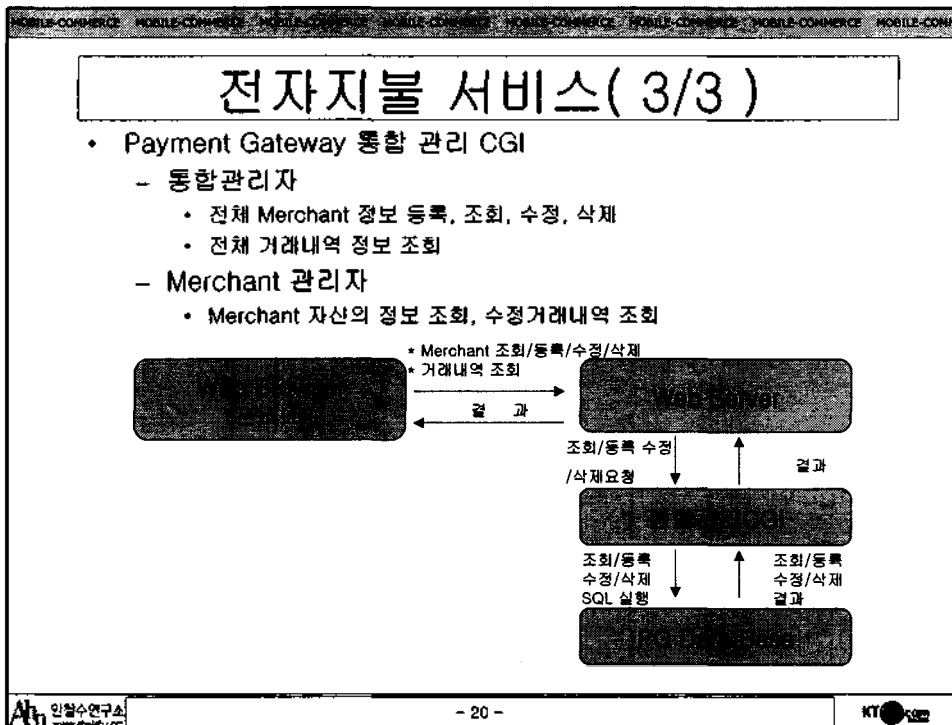
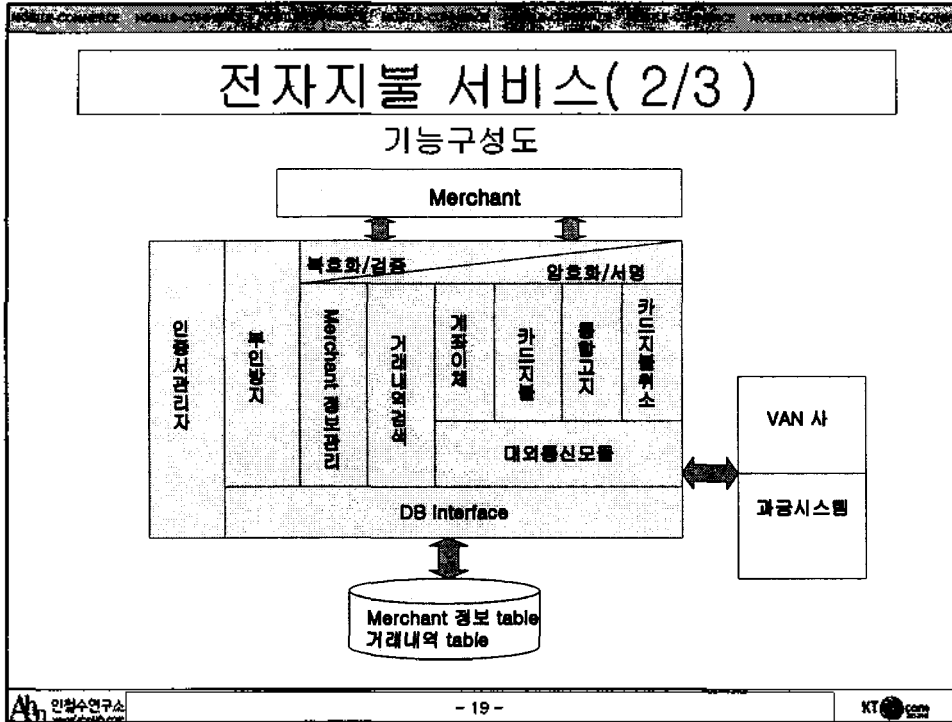


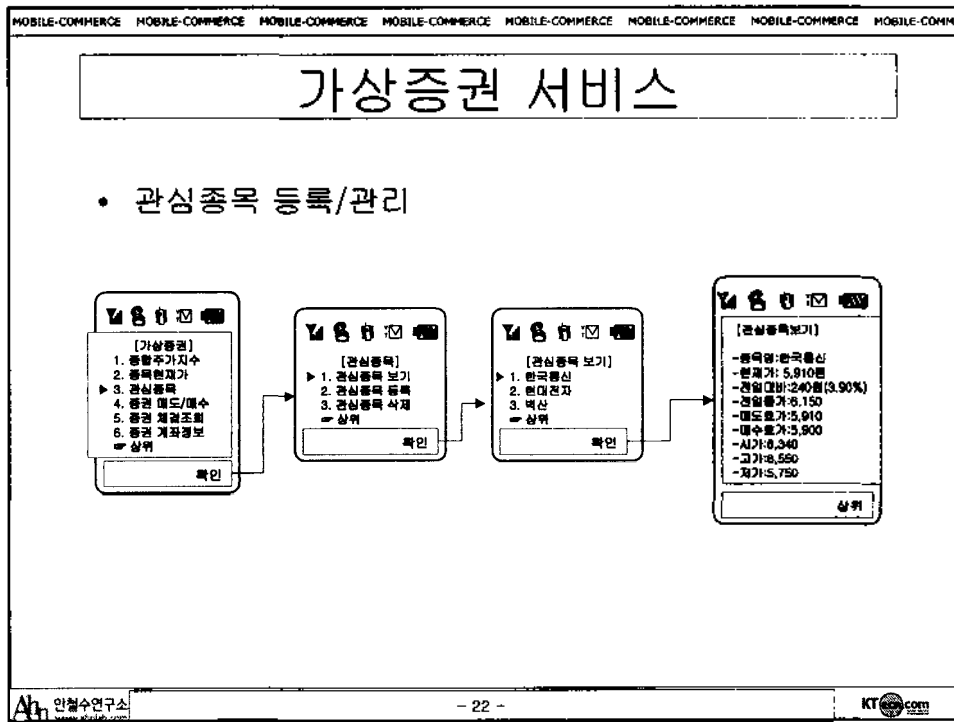
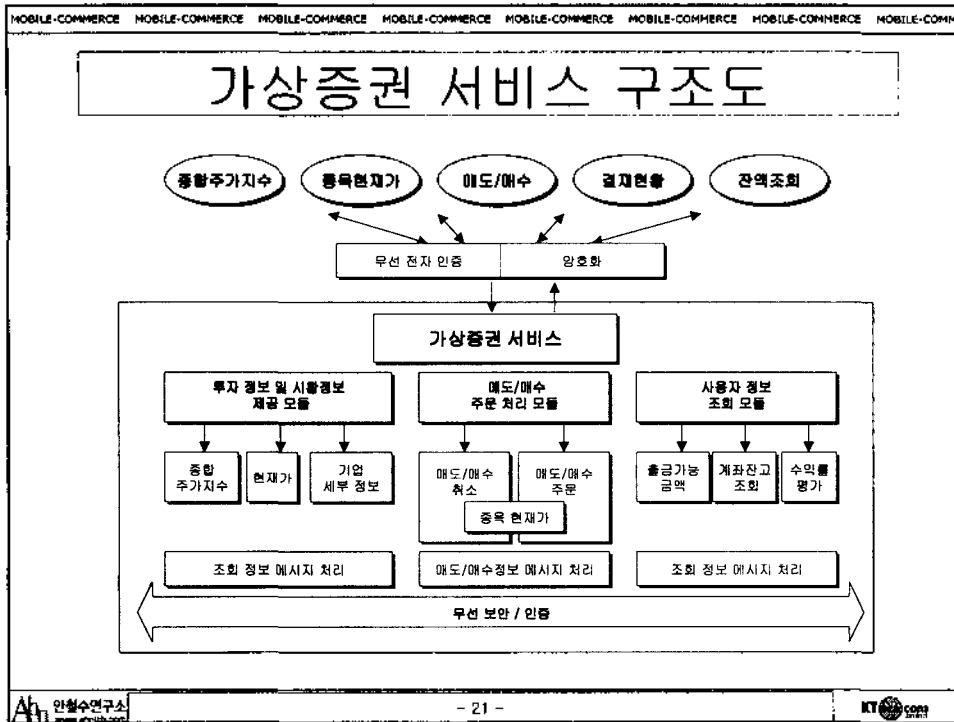
MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMM			
무선 보안/인증 관련 표준			
		구분	비고
키생성	단말기	단말기에서 생성 RSA (1024)	
	서버	단말기에서 생성 RSA (1024)	
전자서명	단말기	RSA (1024bit)	
	서버	RSA (1024bit)	
암호화 알고리즘	단말기	SEED (128bit)	
	서버	SEED (128bit)	
해쉬알고리즘	단말기	SHA1	
	서버	SHA1	
인증서 규격	단말기	WTLS인증서	
	서버	WTLS인증서 WPKI (WAP-217-WPKI,2000.3)	
CRL 규격	단말기	Short-lived Cert(48시간)	
	서버		
An 인텔수연구소		- 13 -	KT

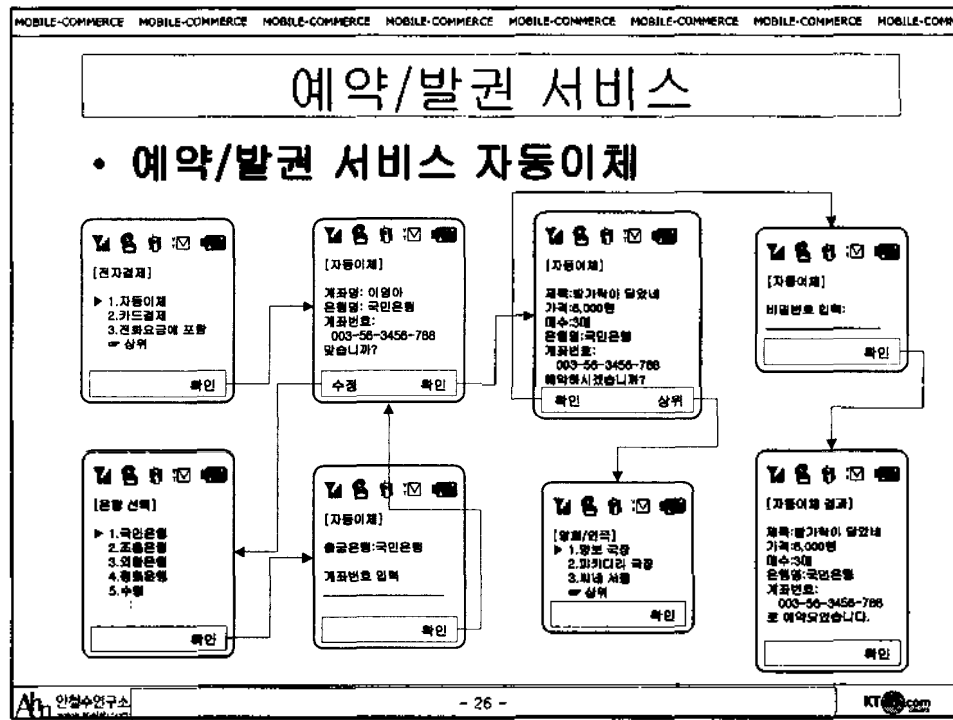
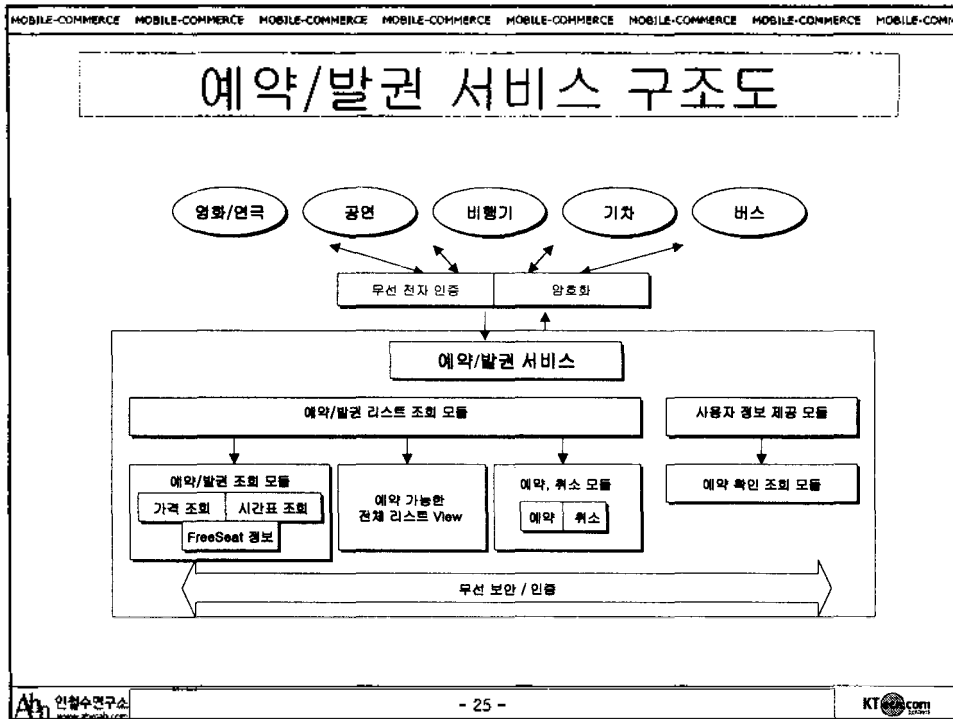
MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMMERCE MOBILE-COMM			
무선 보안/인증 관련 표준			
		구분	비고
코딩 방법	단말기	DER/PEM/WTLS 인증서인코딩규격	
	서버		
DN	단말기	DER/PEM/WTLS 인증서인코딩규격	
	서버		
인증 요청서	단말기	PKCS#10 / CMP	
	서버	PKCS#10	
인증서 전송방식	단말기	인증서의 URL 전송	
	서버	인증서의 URL 전송 / 전체 인증서 전송	
전자서명키 저장방식	단말기	PKCS#5로 암호화 PKCS#8로 저장	
	서버	PKCS#5로 암호화 PKCS#8로 저장	
인증서 및 CRL 획득방식	단말기	HTTP / LDAP	
	서버		
An 인텔수연구소		- 14 -	KT

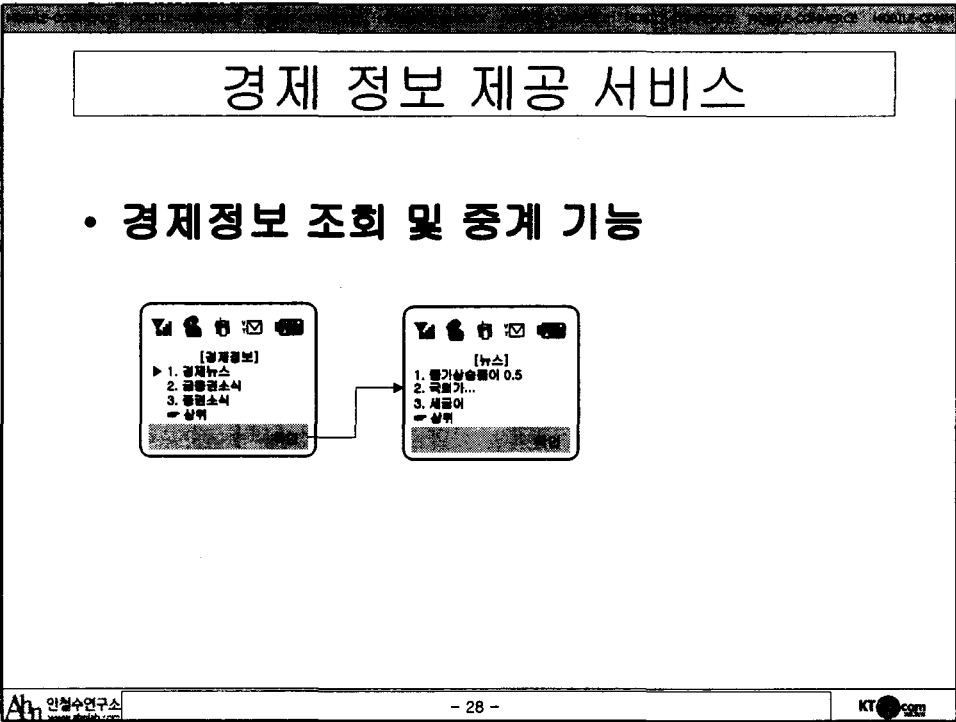
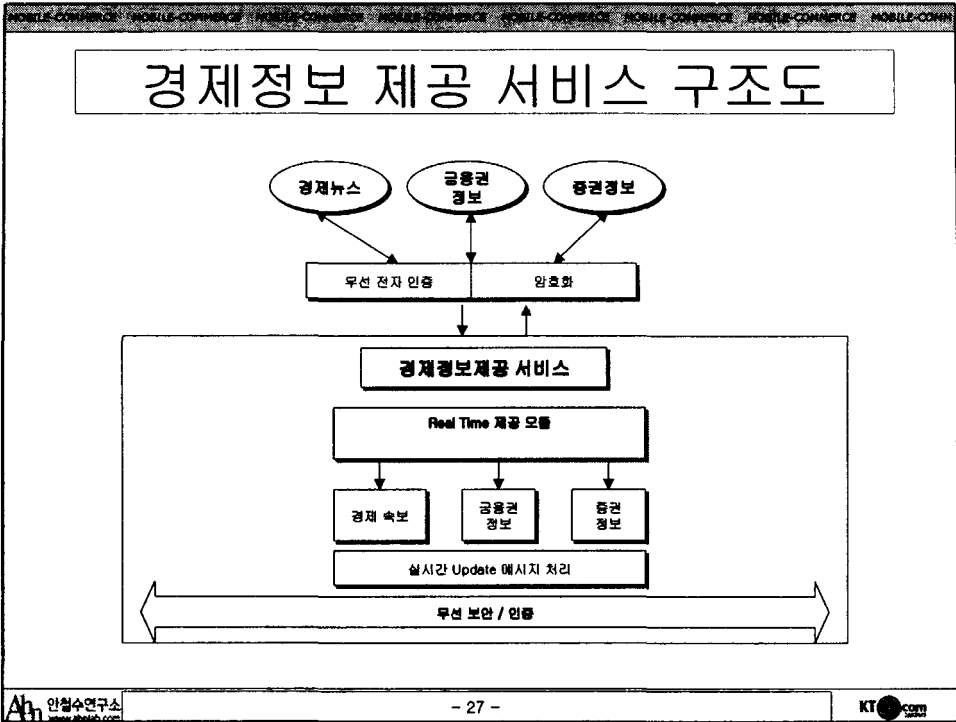






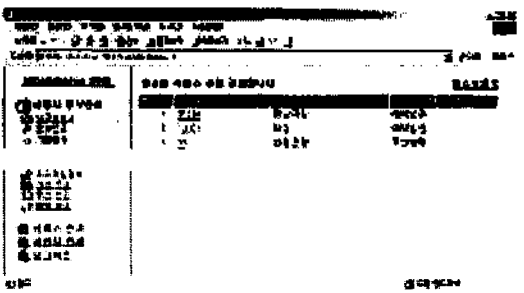






통합 관리 시스템

- Web 에서 사용자 정보 등록 관리
 - 사용자 Profile 관리
 - 저장된 Profile 을 사용하여 서비스 발음
 - 모든 사용자 정보 관리
- Web 에서 Back Office 서비스 등록 관리
 - Back Office 등록 관리
 - 서비스 이용시 적용
- 사용자 시스템 로그 View
 - 사용자별 로그 view



- 29 -

- 무선 인터넷 기반 구축
 - 무선상의 End-to-End 보안
 - 응용레벨 Security
 - 작은 대역폭과 빠른 시간을 위한 WTLS 인증서 사용
 - 공인인증기관의 인증서 에 대한 서명 검증 lib 제공
 - 통합 서비스 플랫폼 구축
- 무선인터넷 표준 프로토콜을 100% 지원
 - WTLS Protocol, WML 적용
- 플랫폼 확장성과 유연성 확보
 - 서비스 처리 엔진과 전문 처리 엔진 분리
 - 전문 처리 Agent 을 이용 - Back Office 연동 유리
 - 전문에 대한 효율적인 관리 가능
- 비즈니스변화에 능동적인 시스템모델
 - SPEED-UP 및 LOW-COST
 - 메모리에 전문 저장, Light 한 전문 구조
- 다양한 통신 Protocol 지원 가능
 - 서비스 기관과의 다양한 통신지원 : TCP/IP, X.25, SNA
- 실시간 상태확인
 - 각 프로세스의 상태 및 회선(X.25 & TCP) 정보관리 : Monitoring

- 30 -

