무선 PKI 기술 규격

2002. 11. 28

박 정 환
pjh@kisa.or.kr

한국정보보호진흥원/전자서명인증관리센터

목 차

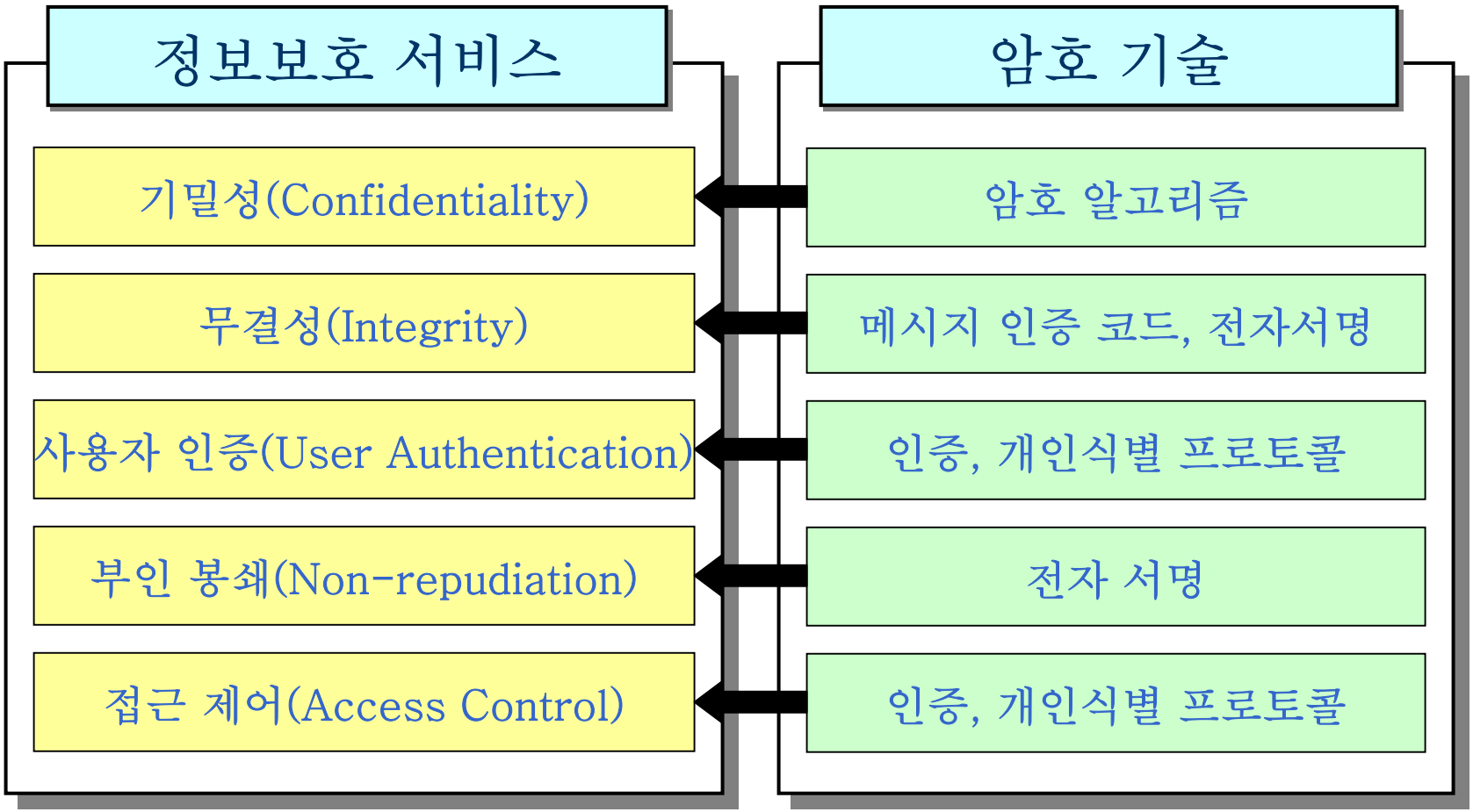
PKI 기술 개요

정보보호 서비스

정보보호 서비스(security service)

기밀성	허가되지 않은 사용자로부터 전송하거나 저장된 데이터에 대한 비밀 보장
인증	정보 시스템에서 정보의 생성, 전송, 처리 등의 행위에 관여한 사용자 A가 바로 그 사용자 A임을 보증하는 기능
무결성	전송하거나 저장된 데이터를 비 인가된 변조로부터 보호
부인 봉쇄	메시지의 송신자나 수신자가 메시지를 송신한 사실이나 수신한 사실을 부인하지 못하도록 하는 기능
접근 제어	비 인가된 동작들의 위협에 대해 자원을 보호하는 기능

정보보호 서비스와 암호기술

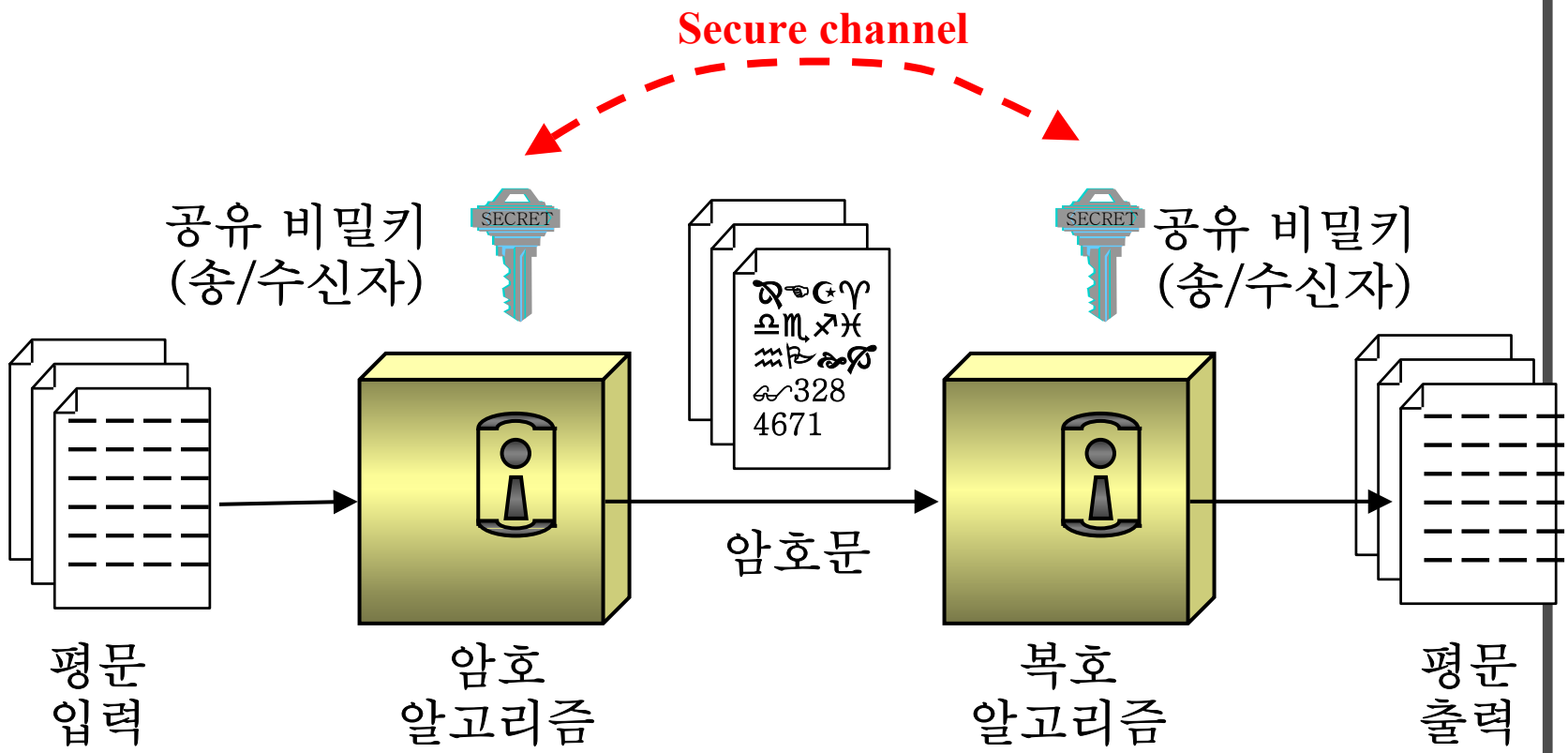


암호 알고리즘

- 관용 암호방식
  - 암호화/복호화에 동일한 키를 사용(대칭키 암호 방식)
  - 예) DES, SEED, AES 등

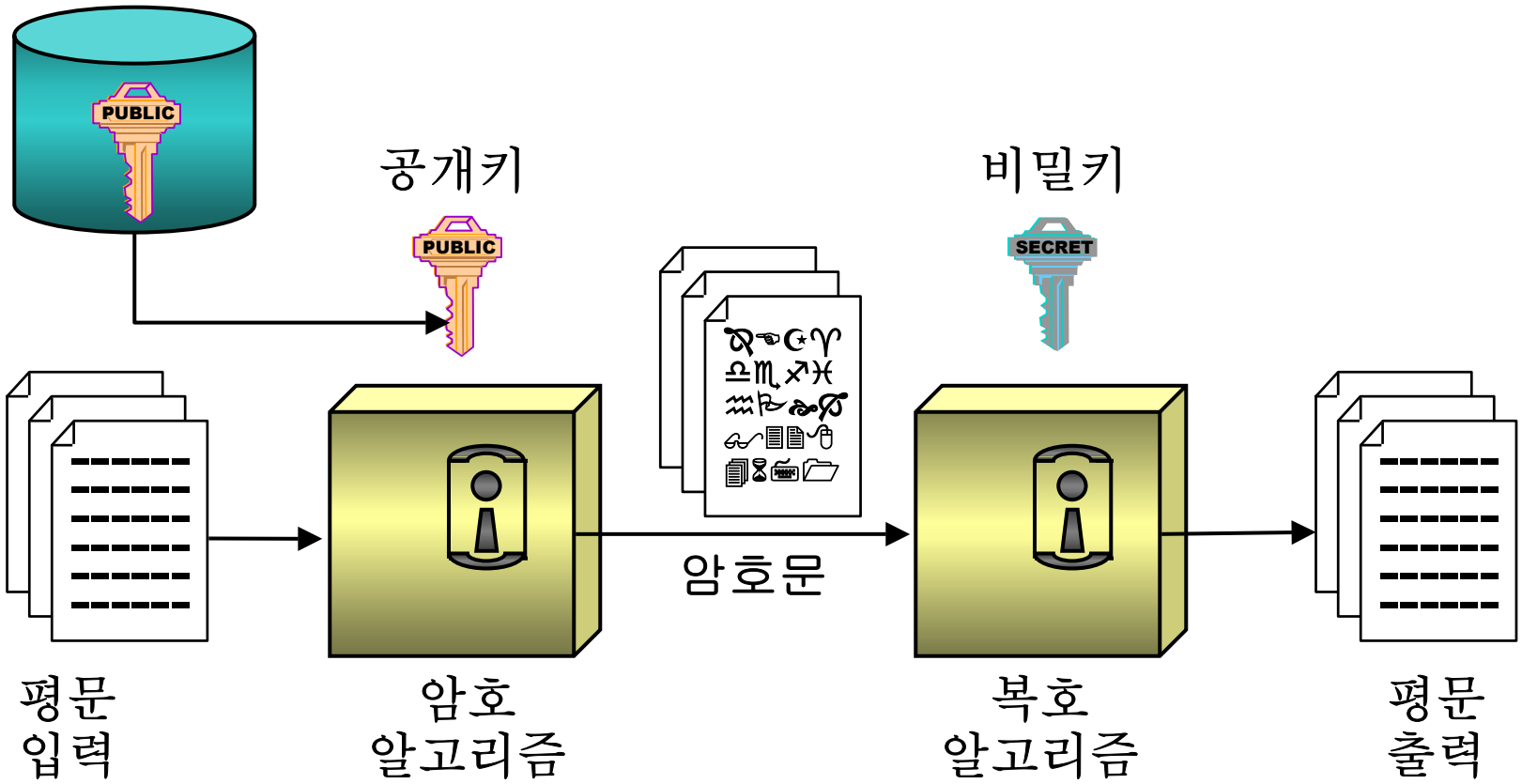
- 공개키 암호방식
  - 암호화/복호화에 서로 다른 두개의 키 사용
  - 비 대칭 암호 방식, Two Key 암호 방식
  - 예) RSA, Rabin, ElGamal, Knapsack 등

관용 암호방식



❖대표적인 암호 시스템 : DES, SEED, AES

공개키 암호방식



❖대표적인 암호 시스템 :RSA, ElGamal, Rabin

대칭키 암호 VS 공개키 암호

항목 \ 암호알고리즘	관용 암호방식	공개키 암호방식
키의 상호관계	암호화키 = 복호화키	암호화키 ≠ 복호화키
암호화키	비밀	공개
복호화키	비밀	비밀
암호알고리즘	비밀/공개	공개
대표적인 예	DES	RSA
비밀키 전송	필요	불필요
키 개수	n(n-1)/2	2n
안전한 인증	곤란	용이
암호화 속도	고속	저속
경제성	高	低
전자서명	복잡	간단

무결성/출처인증/부인봉쇄 : 전자서명

❖ 전자서명의 요구 조건
- 위조 불가(unforgeable)
- 서명자 인증(user authentication)
- 재사용 불가(not reusable)
- 변경 불가(unalterable)
- 부인 불가(non-repudiation)

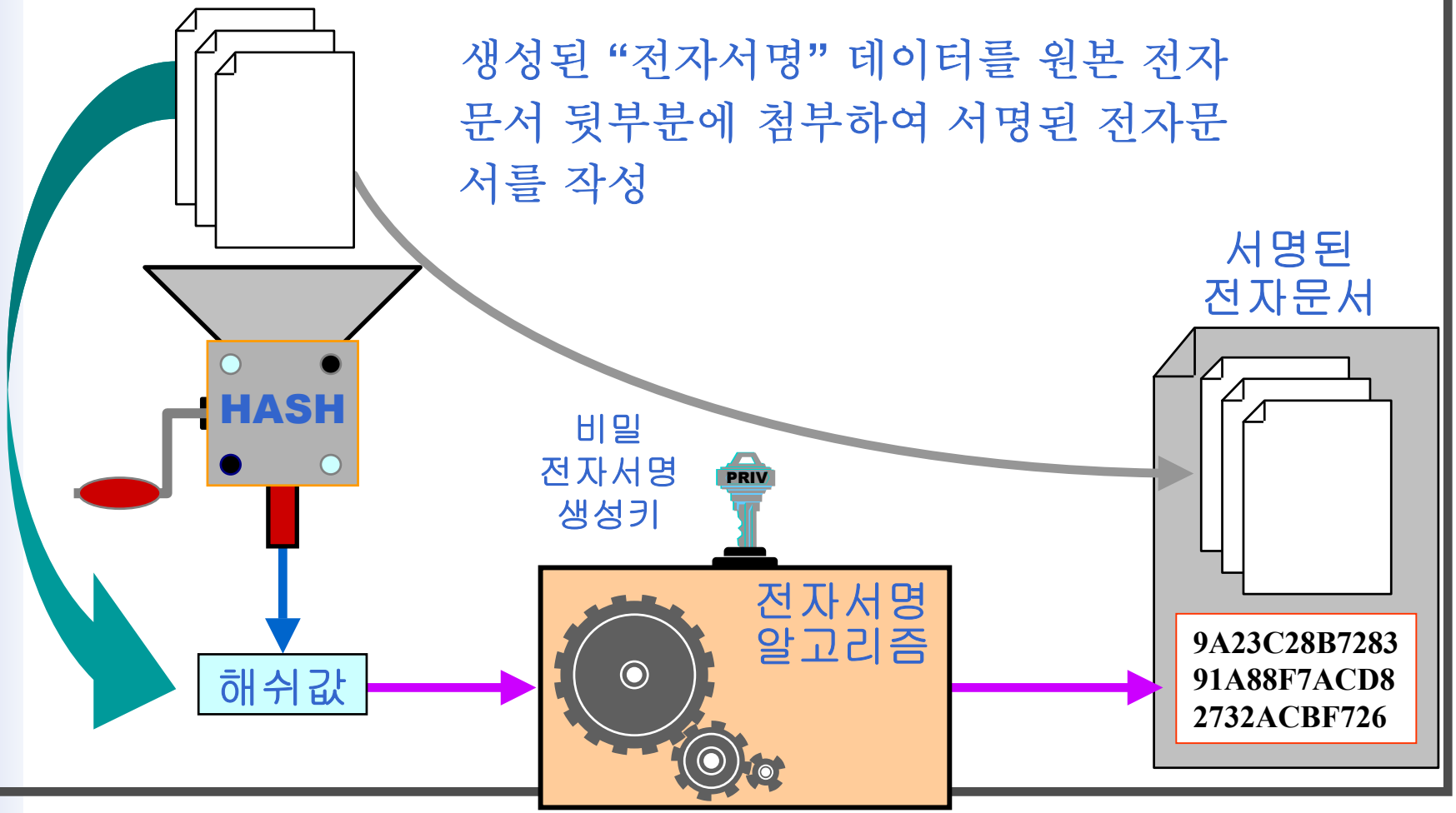
❖ 요구 조건을 충족하는 전자서명 : 디지털 서명

※수기서명 그래픽 정보를 전자서명으로 사용하는 방식은 안전성, 신뢰성 확보 곤란

무결성/출처인증/부인봉쇄 : 전자서명

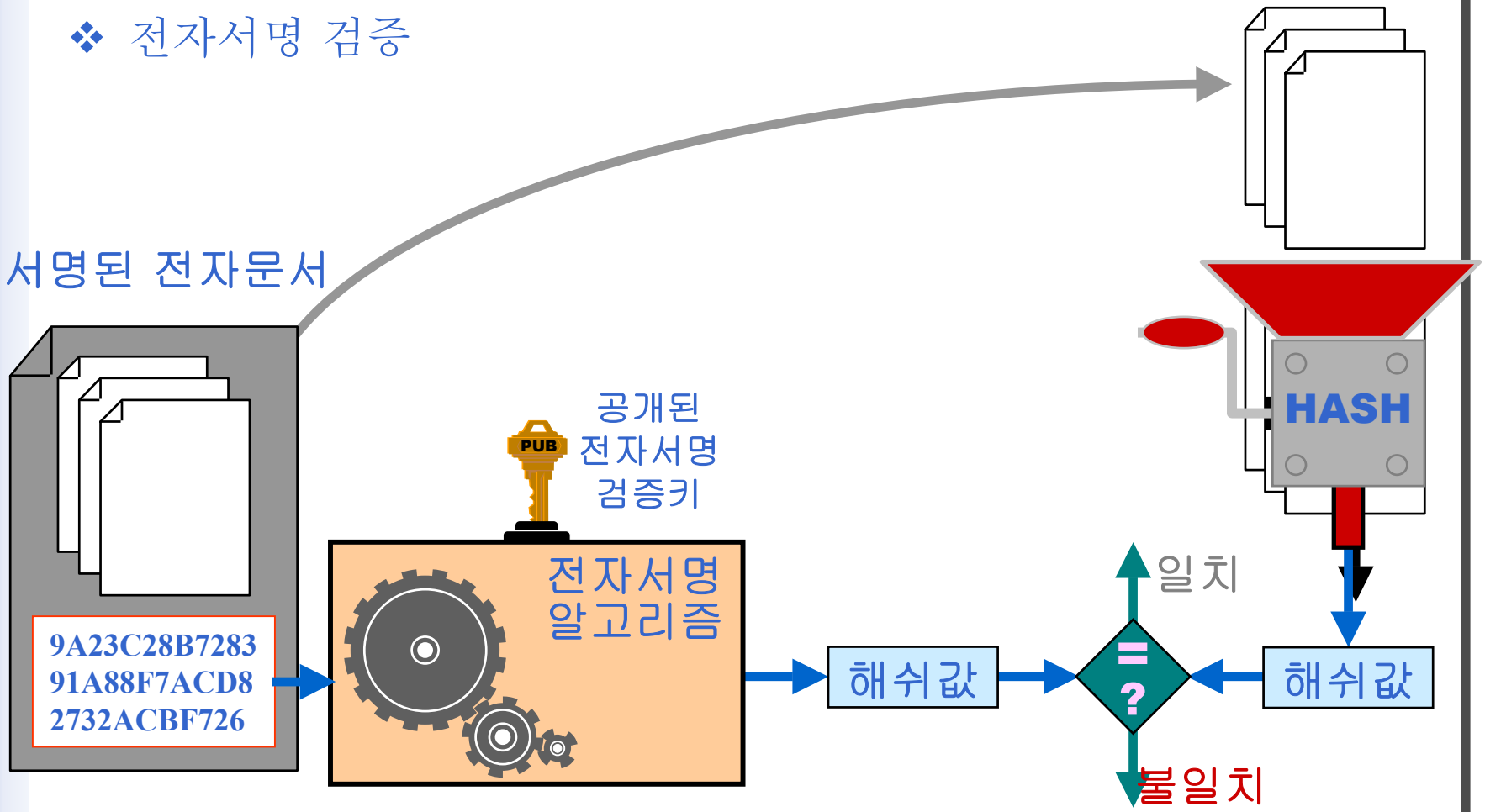
❖ 전자서명 생성

생성된 "전자서명" 데이터를 원본 전자문서 뒷부분에 첨부하여 서명된 전자문서를 작성



무결성/출처인증/부인봉쇄 : 전자서명

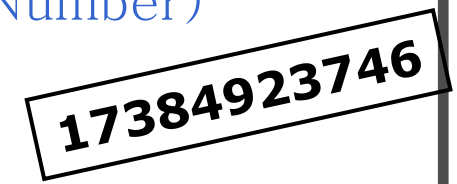
❖ 전자서명 검증



※ 만일 두 해쉬값이 다르다면 전자서명이나 전자 문서가 위.변조 되었음

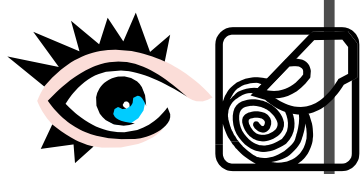
사용자 인증

❖ 그 사람만이 알고 있는 것(지식)을 확인
- Password, Pass Phrase, PIN(Personal Id. Number)
- 단점 : 망각, 남이 추측 가능, 남에게 알려줌
- 장점 : 원거리 신원확인 가능



❖ 그 사람만이 가지고 있는 것(소유물)을 확인
- 열쇠, 신분증, 도장, Token, Smartcard, …
- 단점 : 분실, 도난, 복제, 남에게 빌려줌
- 장점 : 기억할 수 없이 긴 암호키를 저장하 가능

❖ 그 사람만의 신체적/행위적 특징 확인
- 신체적 : 지문, 얼굴모양, 손모양, 망막, DNA, …
- 행위적 : 목소리, 수 서명, Typing Dynamics, …
- 단점 : 피할 수 없는 오류율, 비싼 가격



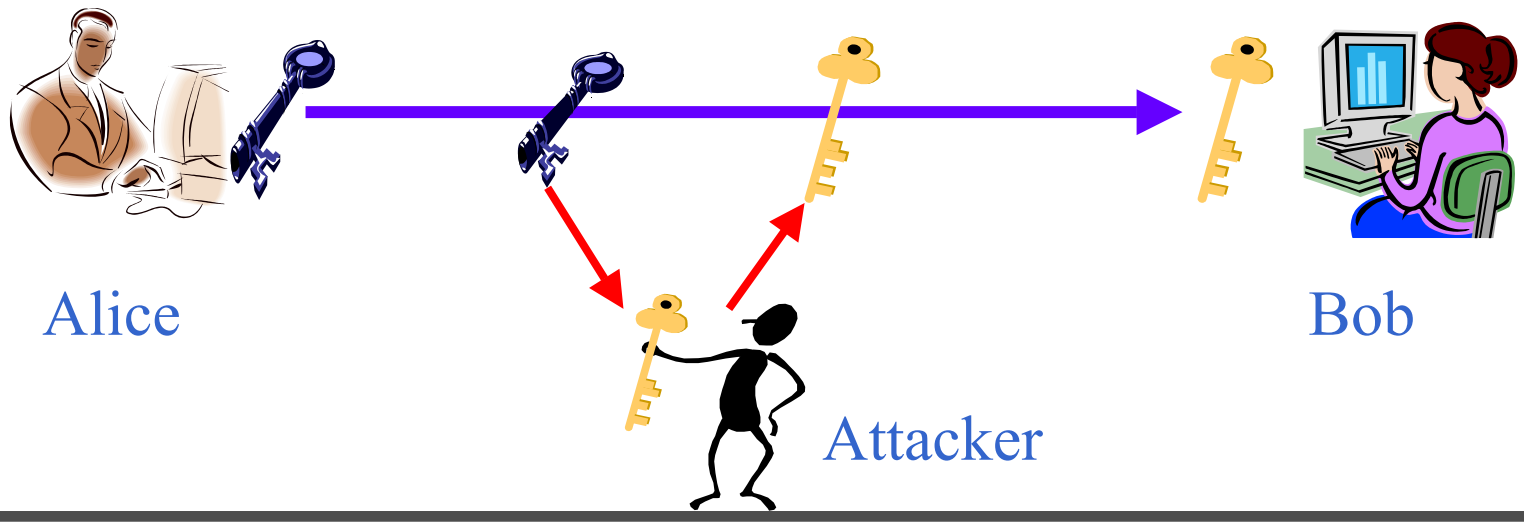
접근 제어

- 비 인가된 동작들의 위협에 대해 자원을 보호하는 기능
- 어떤 주체(who)가 언제(when), 어떤 위치에서(where), 어떤 객체(what)에 대하여, 어떠한 행위(how)를 하도록 허용(또는 거부)할 것인지 접근 제어의 원칙을 정의
- 접근 제어 정책(OSI 보안구조의 분류)
  - 신분 기반(identity-based) 정책
  - 규칙 기반(rule-based) 정책
  - 직무 기반(role-based) 정책

디지털 인증서의 필요성

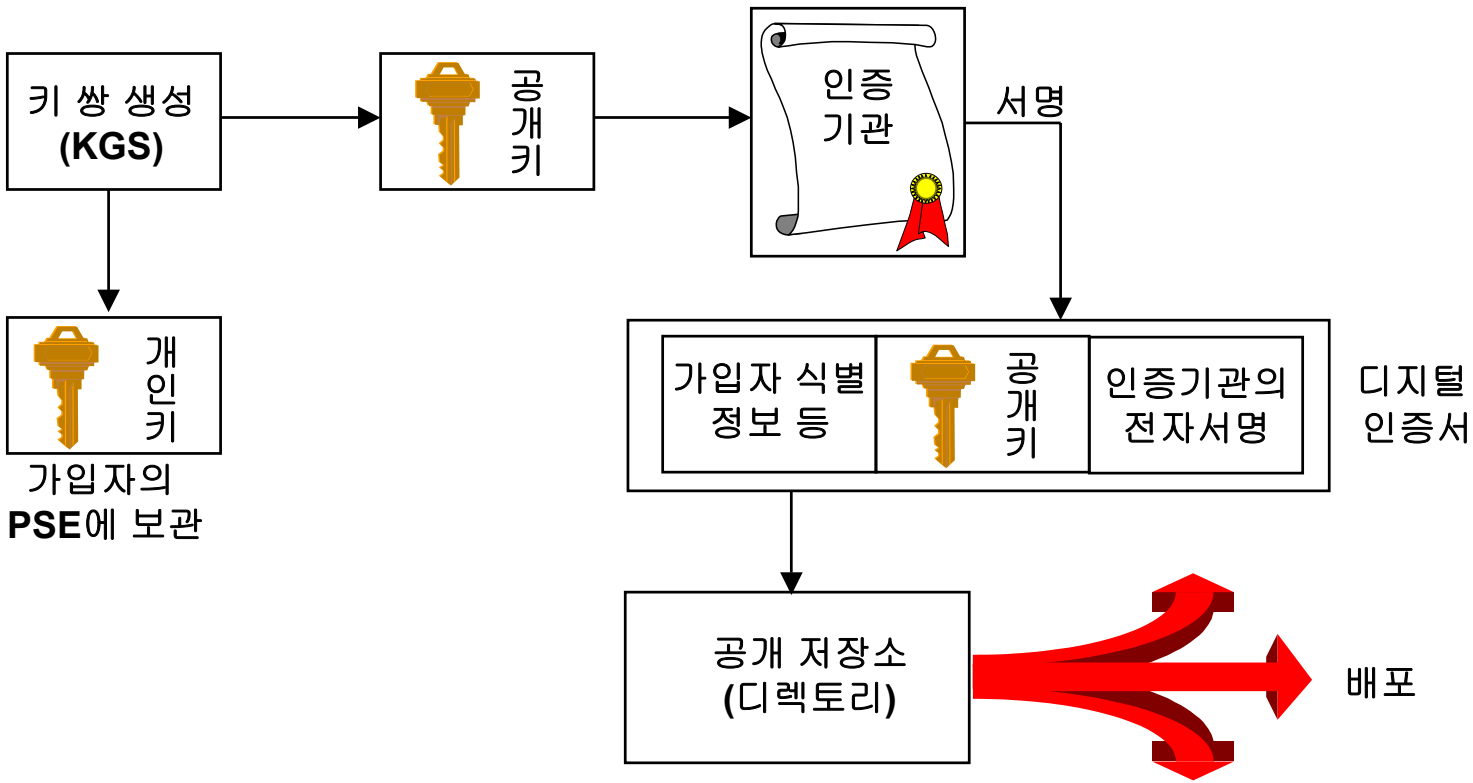
- 송신자는 수신자의 공개키를 어떻게 얻을 수 있는가?
  - 송수신자는 서로의 공개키를 전송
    - E-mail, telephone, fax, mail 등
  - 제3자에 의한 공개키의 교체 가능성??

- 공개키 교체 위협



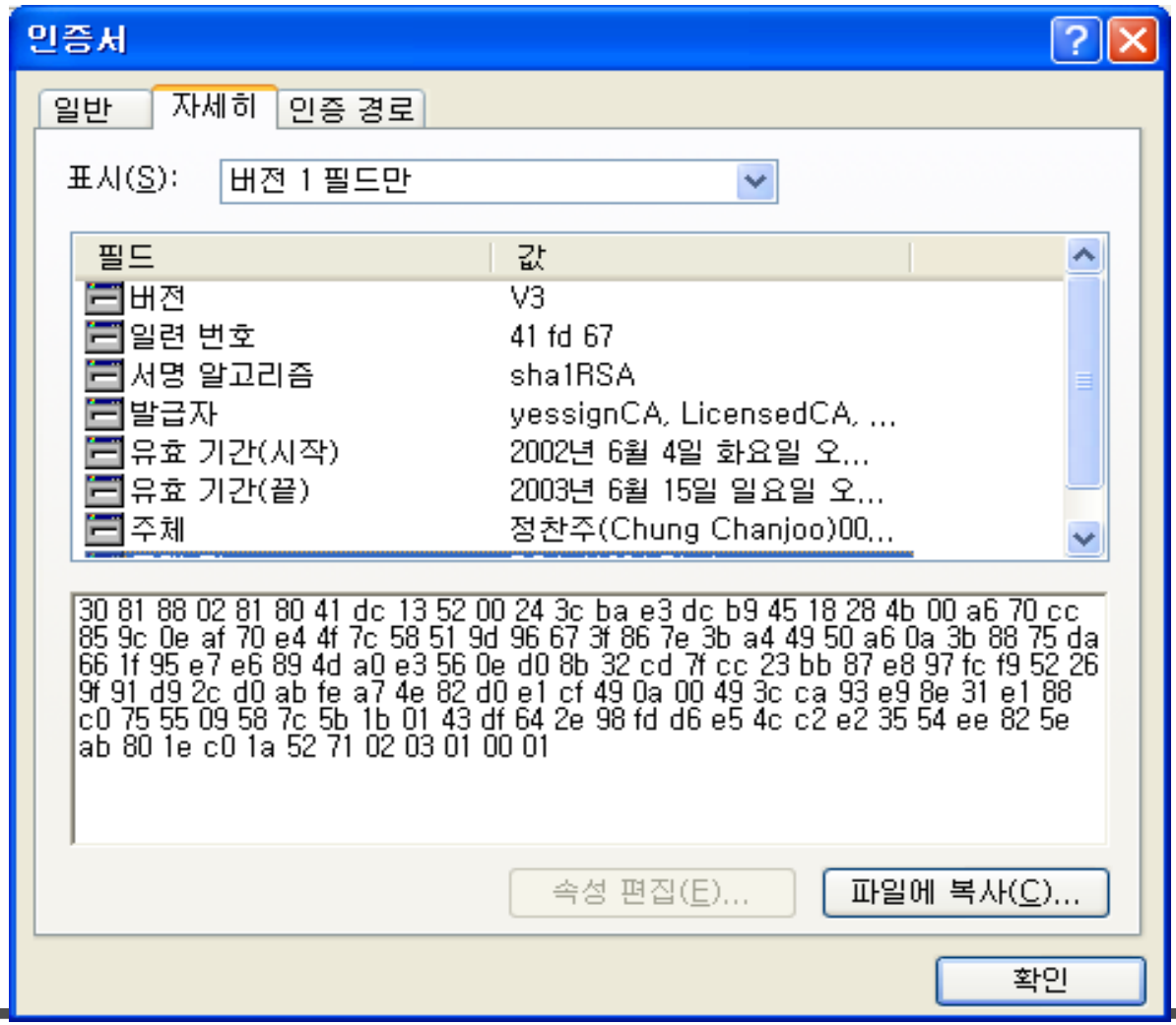
인증서를 통한 공개키 배포

❖ 공개키는 신뢰할 수 있는 인증기관에 의해 서명된 인증서 (Certificate)로 배포

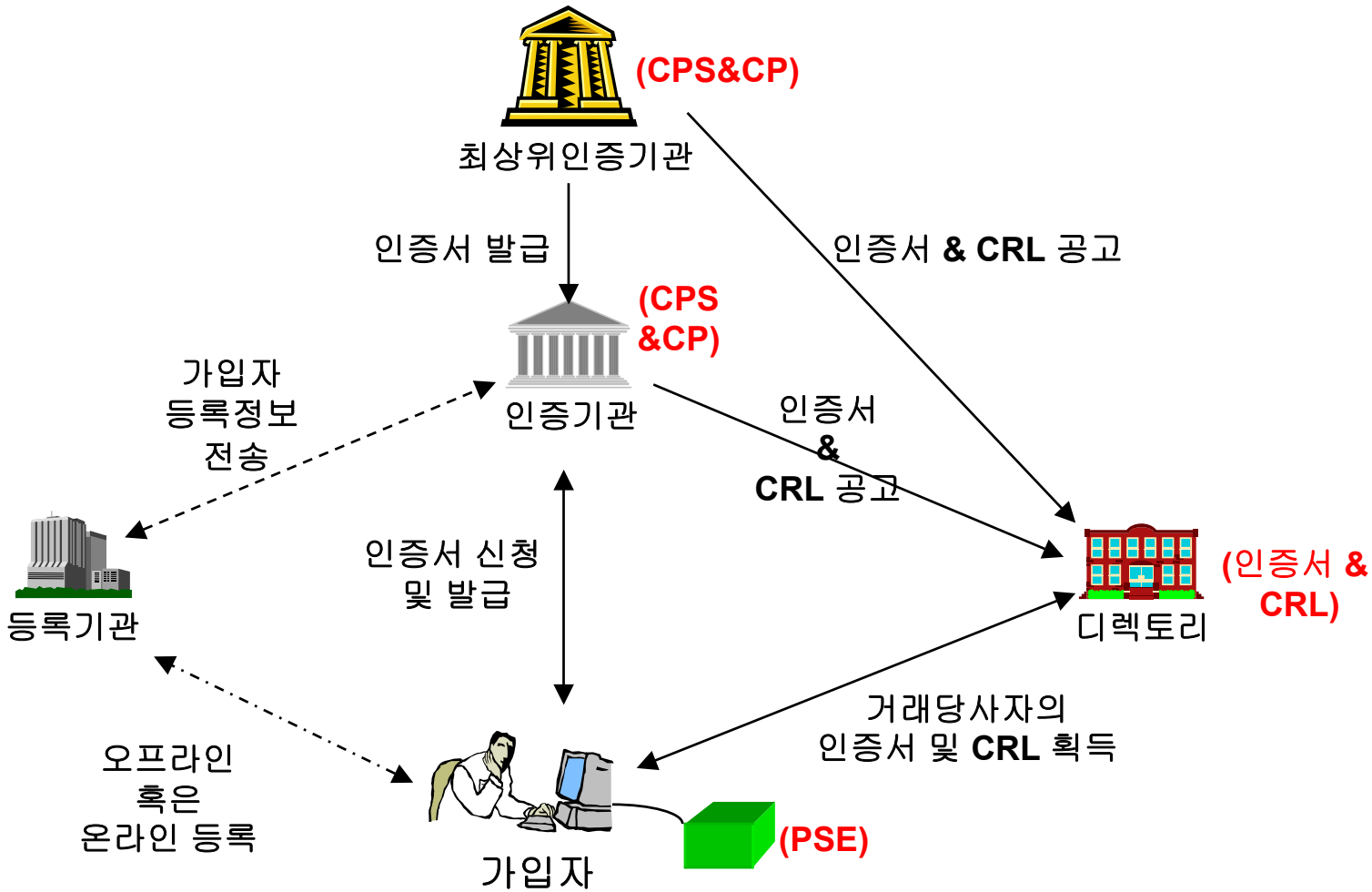


☸ PSE : Personal Security Environment

인증서


인증서
일반
자세히
인증 경로
표시(S):
버전 1 필드만
필드
값
버전
V3
일련 번호
41 fd 67
서명 알고리즘
sha1RSA
발급자
yessignCA, LicensedCA, ...
유효 기간(시작)
2002년 6월 4일 화요일 오...
유효 기간(끝)
2003년 6월 15일 일요일 오...
주체
정찬주(Chung Chanjoo)00...
30 81 88 02 81 80 41 dc 13 52 00 24 3c ba e3 dc b9 45 18 28 4b 00 a6 70 cc
85 9c 0e af 70 e4 4f 7c 58 51 9d 96 67 3f 86 7e 3b a4 49 50 a6 0a 3b 88 75 da
66 1f 95 e7 e6 89 4d a0 e3 56 0e d0 8b 32 cd 7f cc 23 bb 87 e8 97 fc f9 52 26
9f 91 d9 2c d0 ab fe a7 4e 82 d0 e1 cf 49 0a 00 49 3c ca 93 e9 8e 31 e1 88
c0 75 55 09 58 7c 5b 1b 01 43 df 64 2e 98 fd d6 e5 4c c2 e2 35 54 ee 82 5e
ab 80 1e c0 1a 52 71 02 03 01 00 01
속성 편집(E)...
파일에 복사(C)...
확인

PKI의 구성요소


(CPS&CP)
최상위인증기관
인증서 발급
인증서 & CRL 공고
(CPS &CP)
가입자 등록정보 전송
인증기관
인증서 & CRL 공고
인증서 신청 및 발급
등록기관
디렉토리
(인증서 & CRL)
거래당사자의 인증서 및 CRL 획득
오프라인 혹은 온라인 등록
(PSE)
가입자

무선 인터넷 개요

유·무선 인터넷 특성 비교

구 분	유선 인터넷	무선 인터넷
전송속도	56K ~ 1Mbps	14.4 ~ 64Kbps
화면	640 x 480 픽셀이상	4 x 16 chars
인터페이스	키보드, 마우스, 펜 등	소프트버튼, 액정화면
통신 에러율	낮음	높음
휴대성	불편함	편리함
프로토콜	TCP/IP	WAP, TCP/IP
컨텐츠 형태	HTML	CHTML, WML, MHTML
응용 소프트웨어	다양함, 추가변경 용이	한정됨, 추가변경 불편
저장성	데이터 저장 용이	데이터 저장에 제한

무선 인터넷 개요

❖ 무선 네트워크를 통한 무선 인터넷 제공

❑ 무선 통신 환경에 따른
- ➢ 좁은 대역폭
- ➢ 낮은 전송률

❑ 휴대성 강조에 따른
- ➢ 적은 메모리 및 배터리
- ➢ CPU 처리 속도 저하

❑ 인터페이스에 따른
- ➢ 입력의 불편(소프트 버튼)
- ➢ 응용프로그램의 제한

무선 인터넷 접속 프로토콜

❖ WAP(Wireless Application Protocol)

- 인터넷 중심의 데이터 서비스를 무선 환경에서 효율적으로 처리하기 위한 산업체 표준
- 현재 가장 많은 사업자와 단말기 제조업체의 지원
- 국내 현황 : 011, 017, 019에서 채용
- WAP2.0(2001년 8월 발표)

❖ MME(Microsoft Mobile Explorer)

- MS(Microsoft)에서 휴대폰용으로 개발한 무선 인터넷 솔루션으로 Stinger 프로젝트 명으로 유명
- 국내 현황 : 016, 018에서 채용(ME v1.2 채택)

WAP(Wireless Application Protocol)

❖ WAP Forum
- Ericsson, Motorola, Nokia, Phone.com을 주축으로 1997년 설립(단말기 업체 중심)

❖ OMA Forum
- WAP Forum과 Open Mobile Architecture Initiative가 합병되어 2002년 6월에 통신사업자, 단말기사업자 등 200여개의 회사가 주축이 되어 OMA(Open Mobile Alliance) 포럼으로 개칭됨

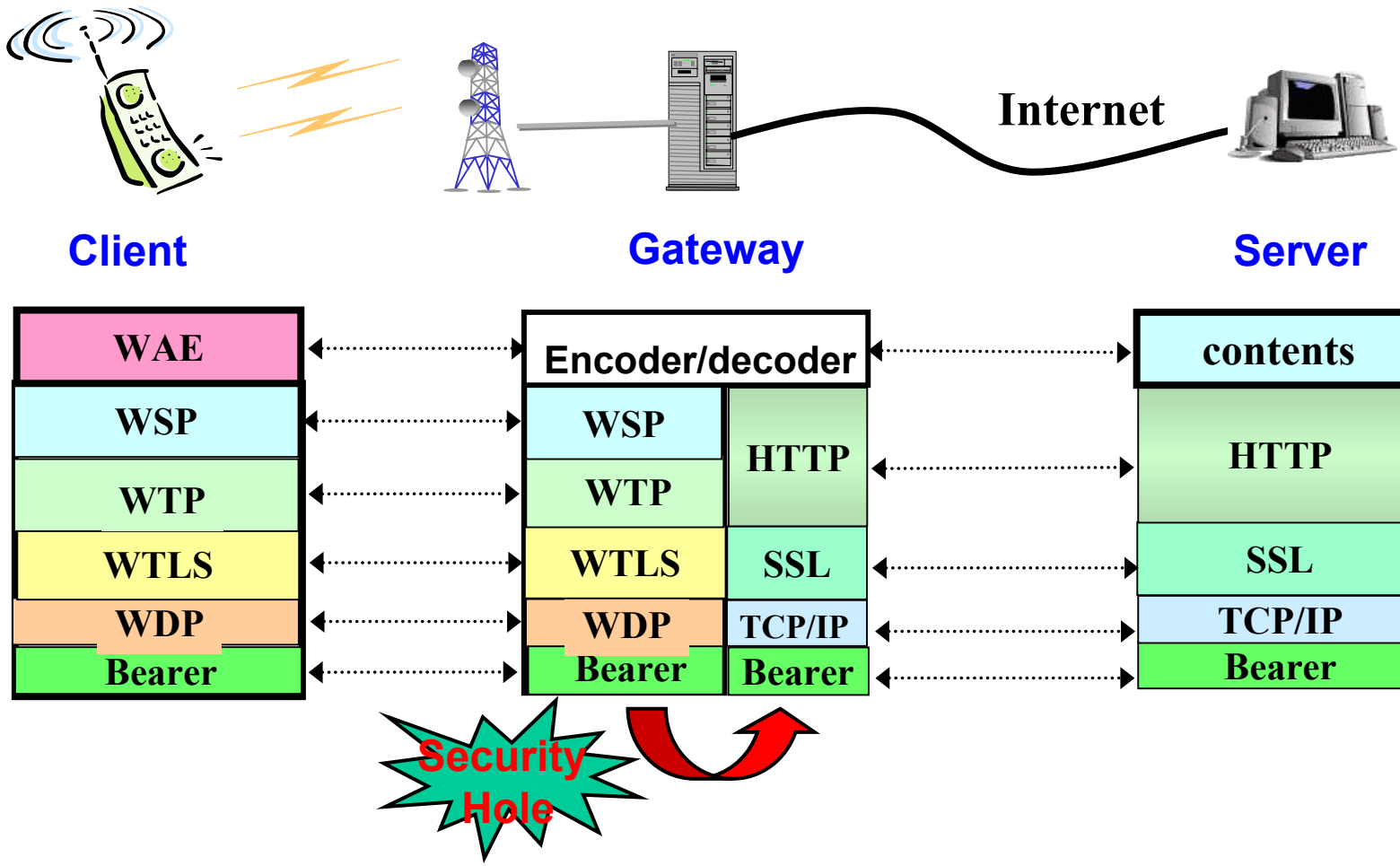
목적

- 무선 환경에 맞는 프로토콜
- 고품질의 인터넷/전화 부가가치 서비스 제공
- 이동통신 인프라의 표준화
- 관련 표준화 단체에 대한 압력
- 서비스 개발 촉진

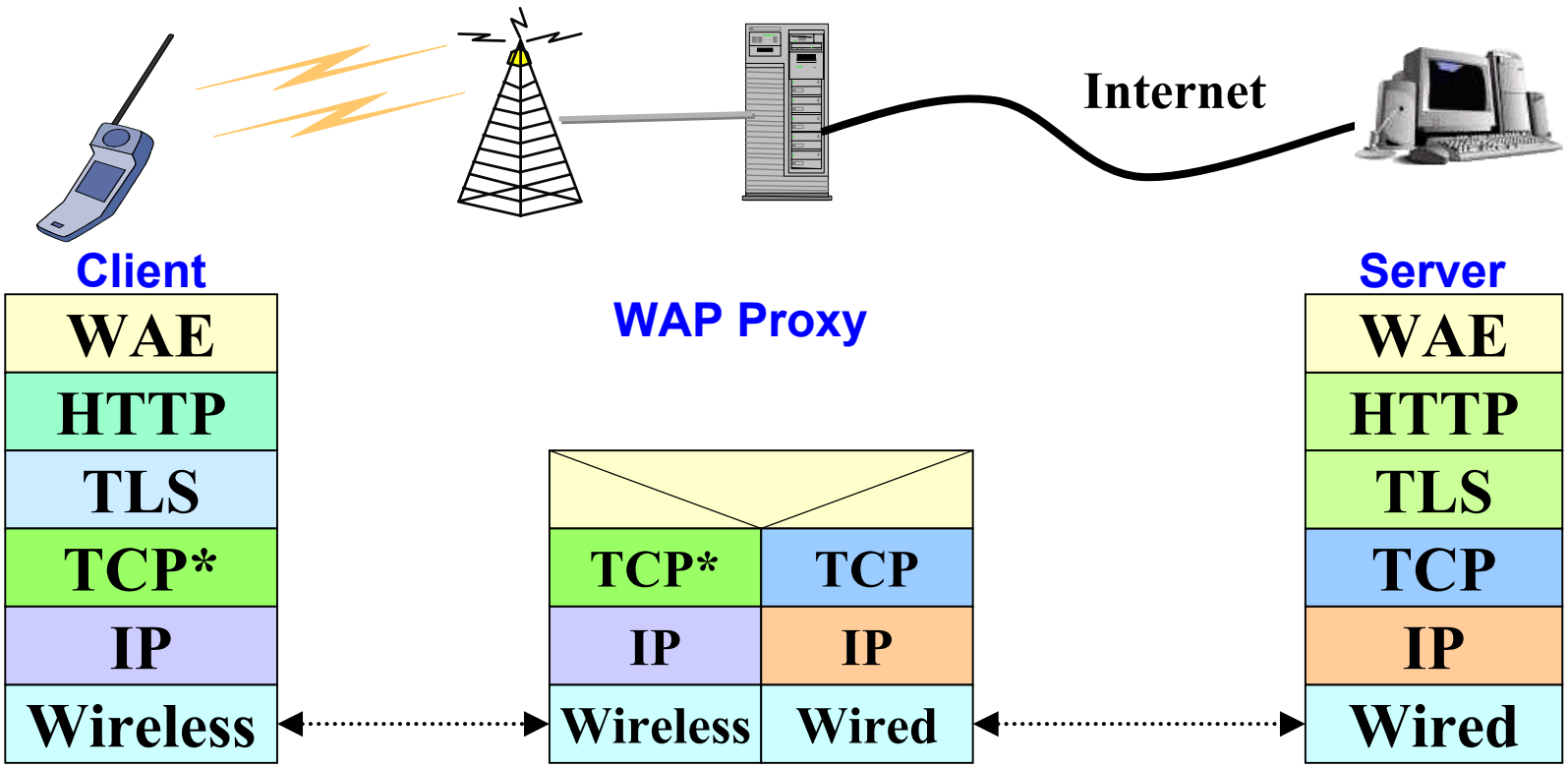
기본 원칙

- 현존 표준과의 호환성(IP, XML 기반)
- 새로운 무선 데이터 서비스 표준 확립
- 다양한 Bearer 지원
- 다양한 Device 지원

WAP 1.x Archtecture

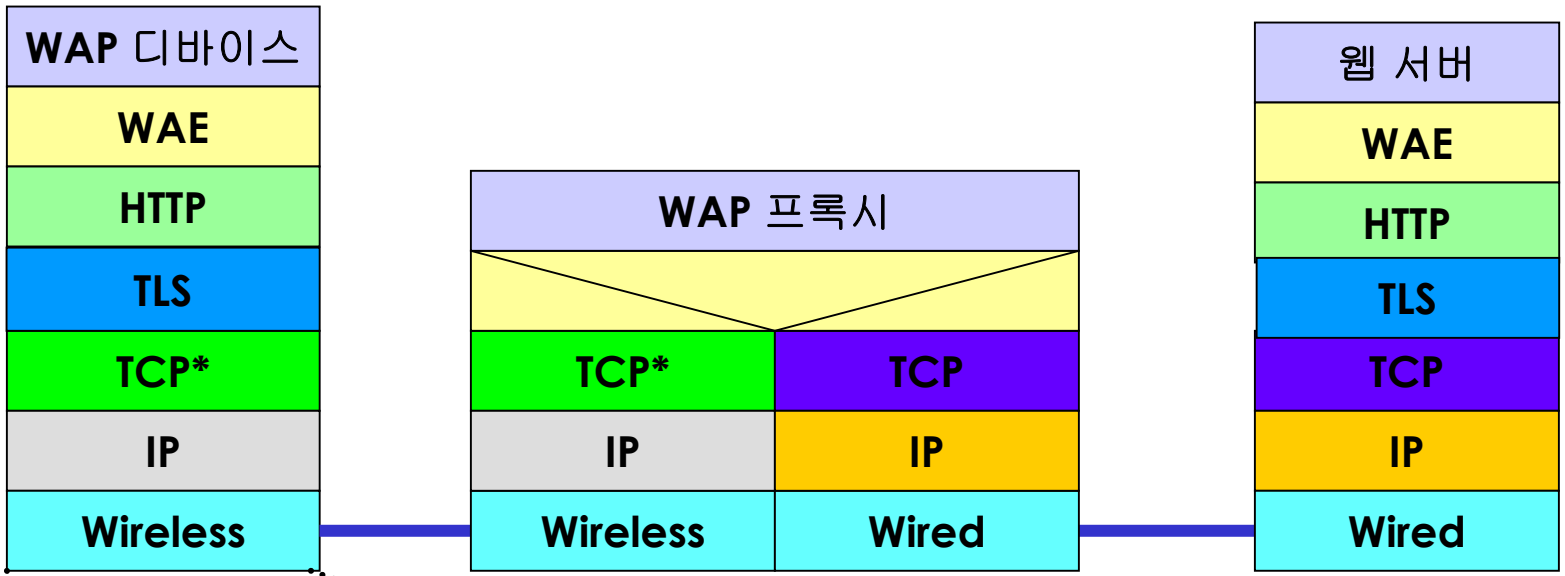


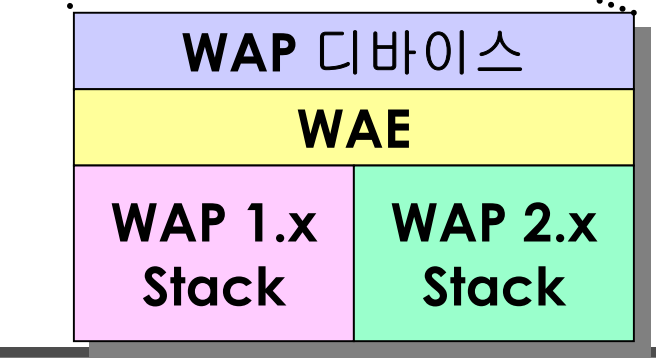
WAP 2.0 HTTP Proxy with Profiled HTTP/TCP



TCP* : The wireless Profile of TCP

WAP 2.0 Archtecture



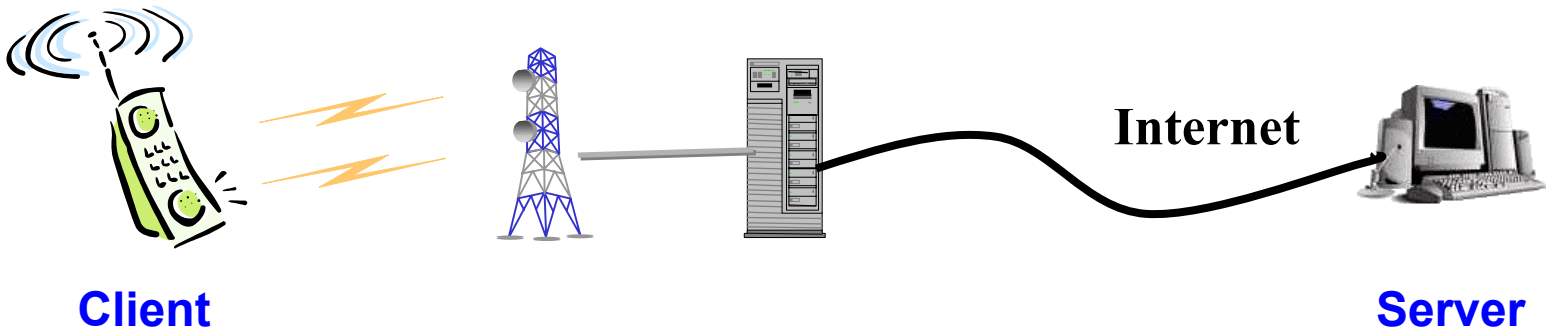


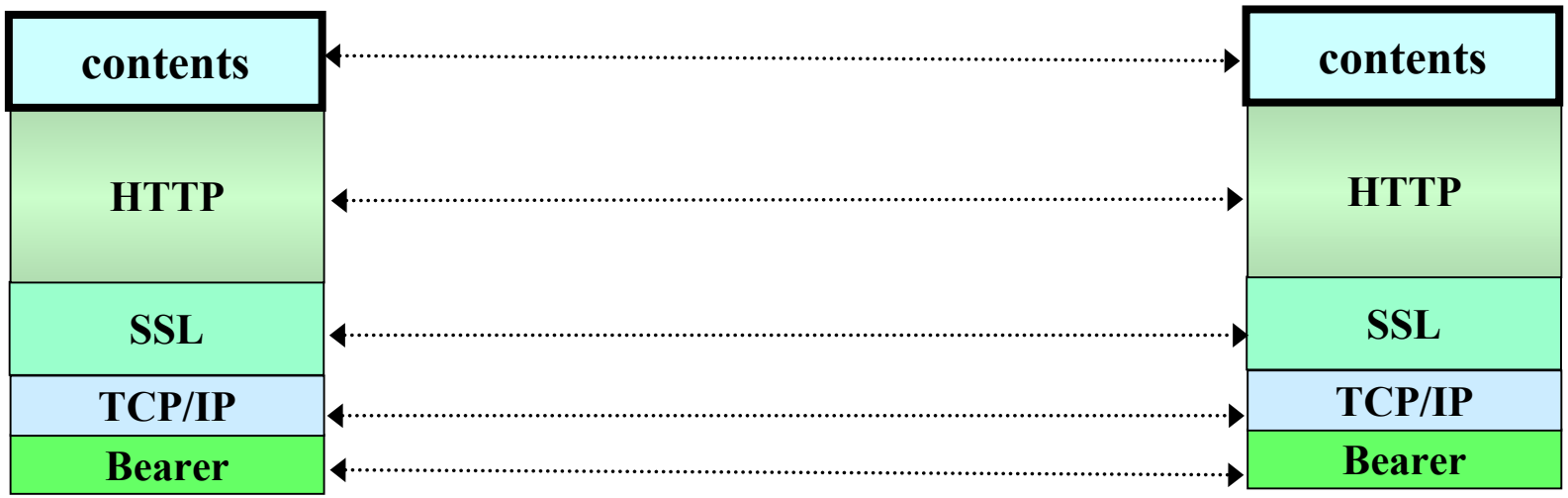
- 기존에 개발되어 있는 표준을 그대로 적용 : XML, HTTP, TCP/IP, SSL 등
- 기존의 응용 프로그램 및 도구들을 사용

ME(Mobile Explorer)

- 마이크로소프트에서 휴대폰용으로 개발한 무선 인터넷 솔루션
- 프로토콜 스택 – mHTML/HTTP/SSL/TCP/IP
- 보안 프로토콜 – SSL이용
- Markup Language – mHTML
  - HTML을 무선의 특성에 맞게 축소 및 변형
  - 약 3KB까지 전송 가능

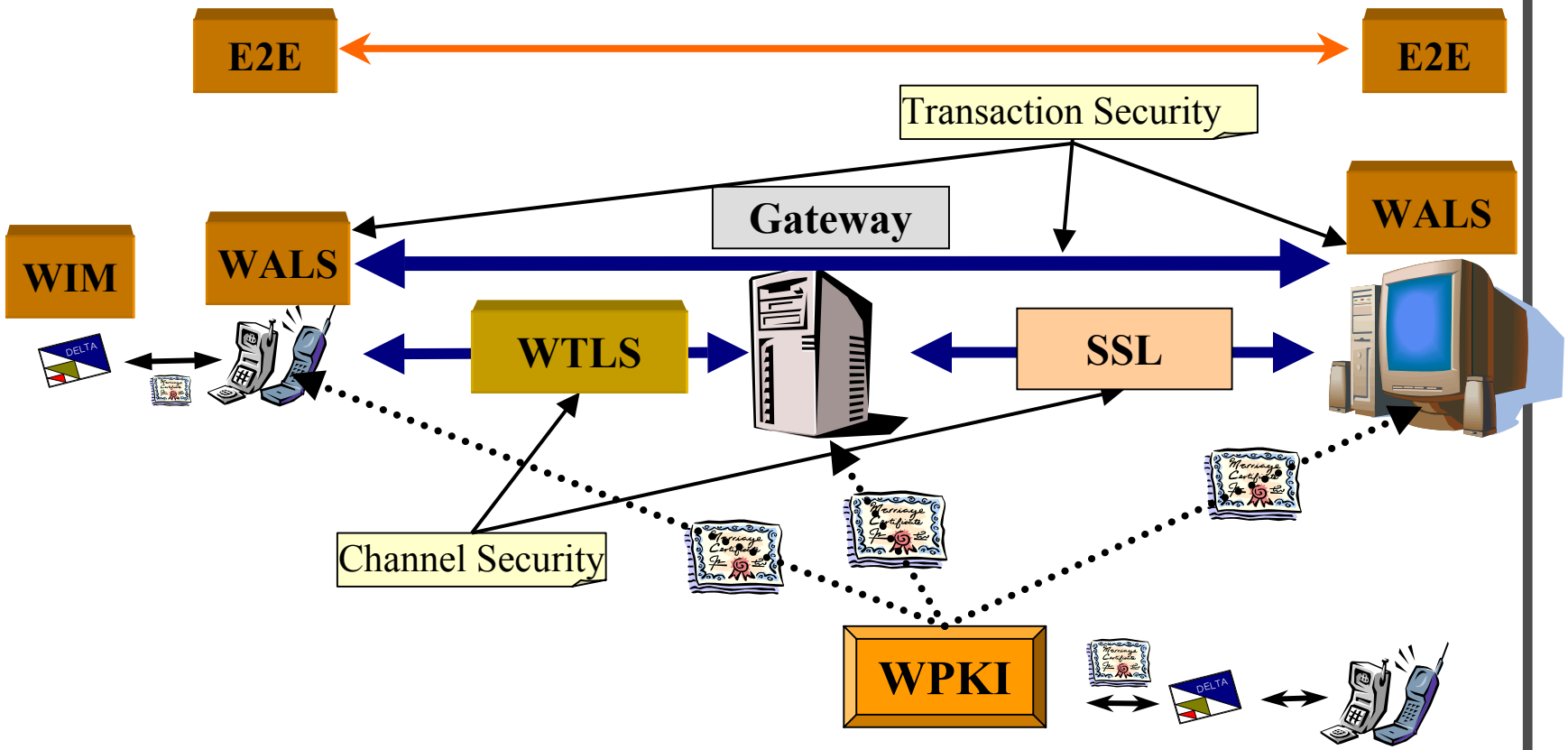
ME Architecture





무선 인터넷 보안 기술 개요

WAP WPKI



Transaction Security : 응용 계층에서 전자서명을 통한 거래의 무결성, 부인 봉쇄 서비스 제공
Channel Security : 전송계층에서 암호화와 MAC을 통한 데이터 기밀성, 무결성 서비스 제공

WML Crypto Script

❖ 현황
- 전자서명 생성 함수만이 정의됨(SignText 함수)
- 암호화 및 해쉬함수 등에 대한 Script Library를 정의하기 위한 논의가 진행중

❖ 문제점
- 각기 다른 인증기관에서 발행한 인증서간 호환성이 보장되지 않음에 따라 이들 인증서를 모두 처리할 수 있는 표준 처리가 어려움
- 인증서 취득/관리의 어려움
- 인증서 검증의 어려움

❖ 구현방안
- Application Layer에서 구현
- 암호화/복호화, 전자서명 검증, 해쉬함수 등 구현하기 위한 독자적인 함수 필요

WTLS 인증서

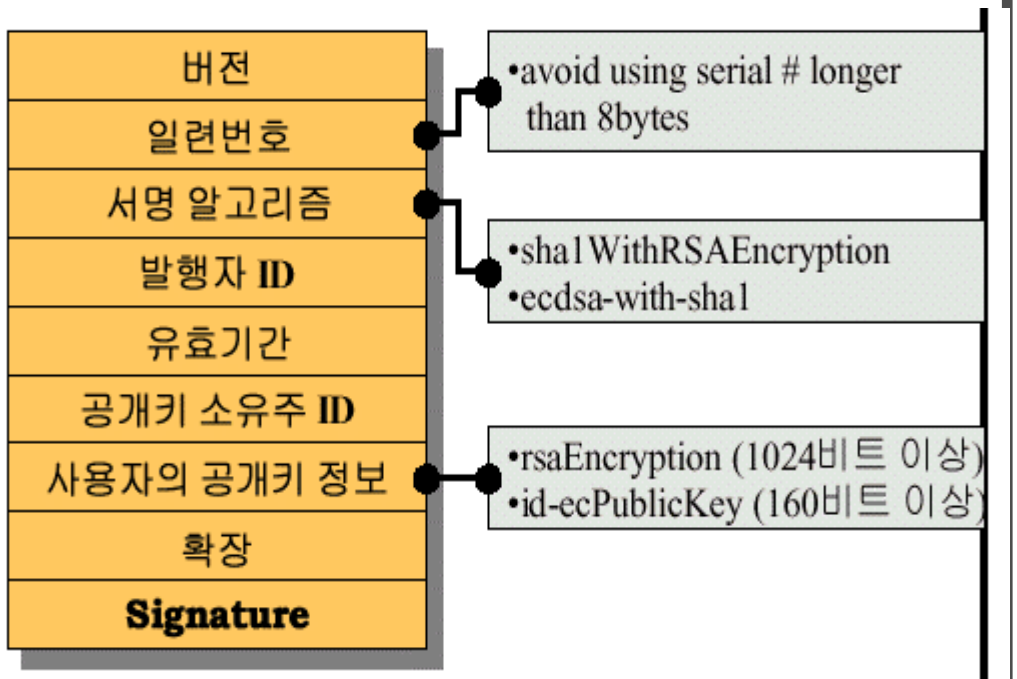
❖ WTLS/WALS 인증서 Format

– User/Server/Role/Authority Certificates

X.509 v3 인증서

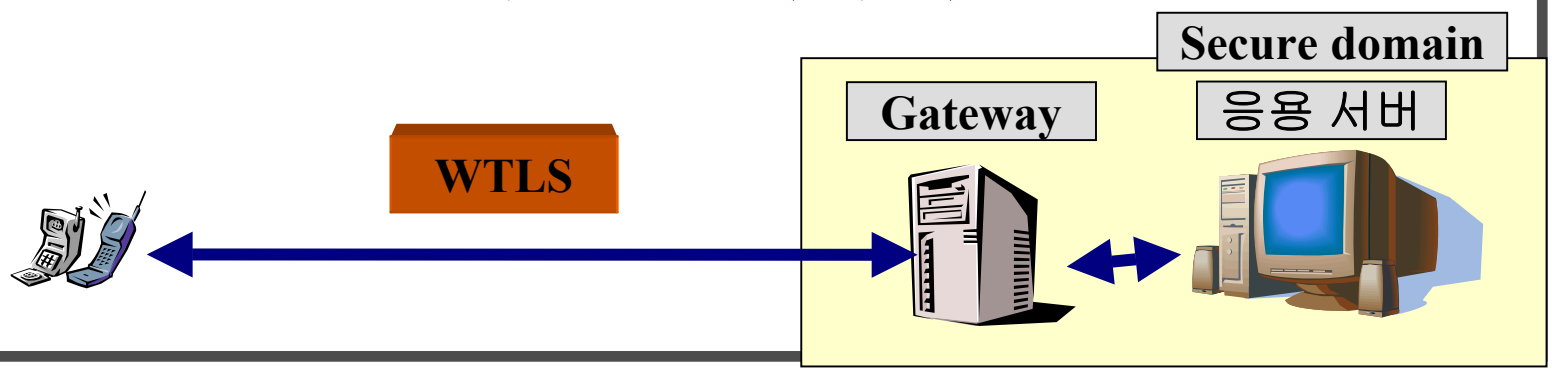
버전
일련 번호
서명 알고리즘
발행자 **ID**
유효기간
공개키 소유주 **ID**
사용자의 공개키 정보
발행자의 부가적인 정보(선택사항)
공개키 소유주의 부가적인 정보 (선택사항)
확장
Signature

WAP profiled server X.509 Certificate

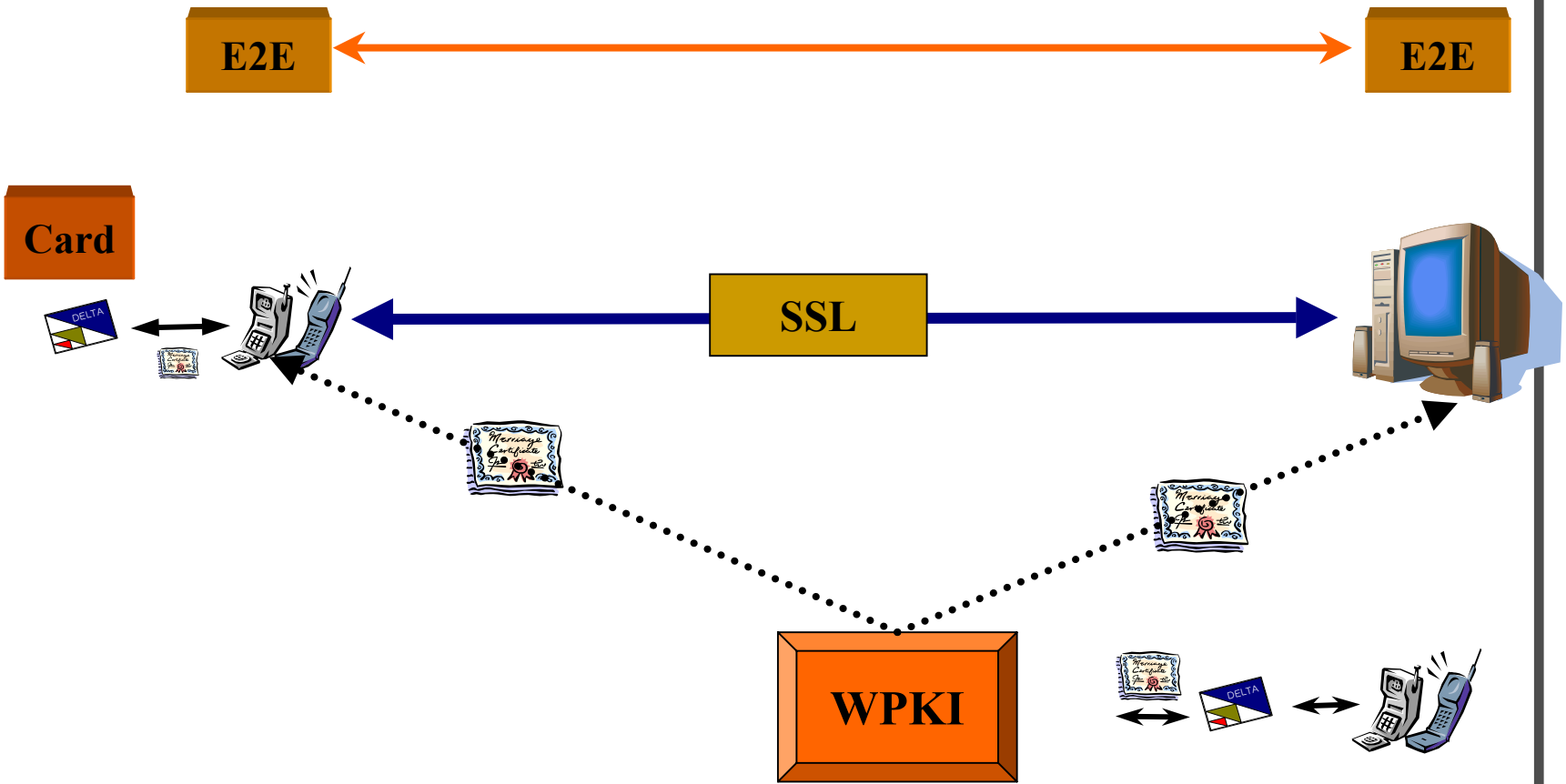


End-to-End 보안

- 대안 1 : Application Layer에서 암호화 수행
  - WML Script를 사용하여 Application Layer에서 암호화 및 복호화를 수행
  - 게이트웨이에서 by pass 형태
- 대안 2 : Secure Domain
  - 응용 서버가 신뢰하는 Gateway를 직접 운영하는 Secure Domain 사용
  - WAP 표준의 WTLS를 이용하여 신뢰할 수 있는 Client authentication 및 기밀성 보장이 가능함



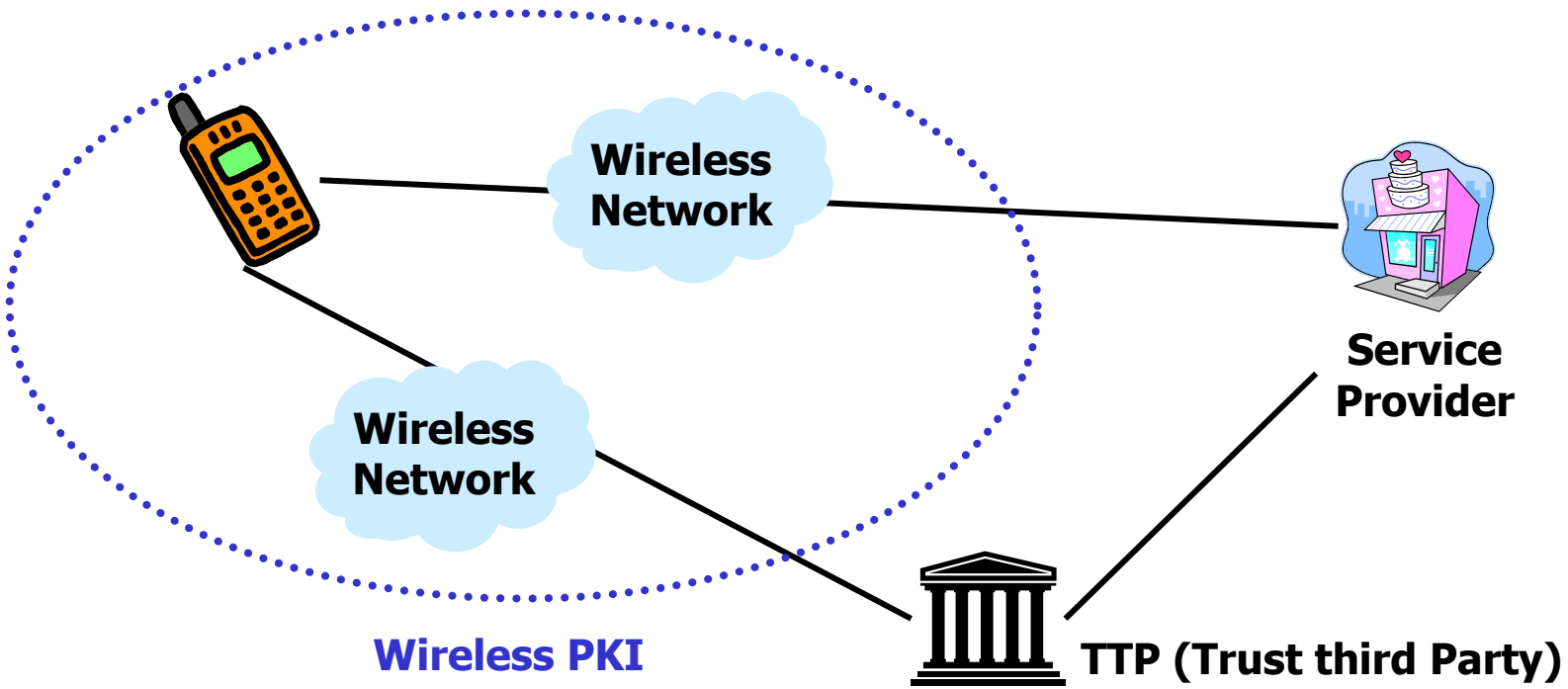
ME Wireless Security



무선 PKI 개요

무선 PKI 개요

- 무선 환경이라고 해서 PKI 구조에 큰 변화가 있는 것은 아니다.
- 모든 환경이 무선 환경은 아님
- Wireless PKI는 인터넷 PKI에 접근하기 위한 하나의 수단임



무선 PKI 적용을 위한 단말기 요구사항

- ❖ 전자서명키 생성기능
- ❖ 메시지 암호화 및 복호화 기능
- ❖ 인증서 요청 및 관리 기능
- ❖ 인증서 수신, 검증, 저장 및 송신 기능
- ❖ 전자서명된 데이터의 수신, 검증 및 저장 및 송신 기능
- ❖ 전자서명 데이터 생성 기능

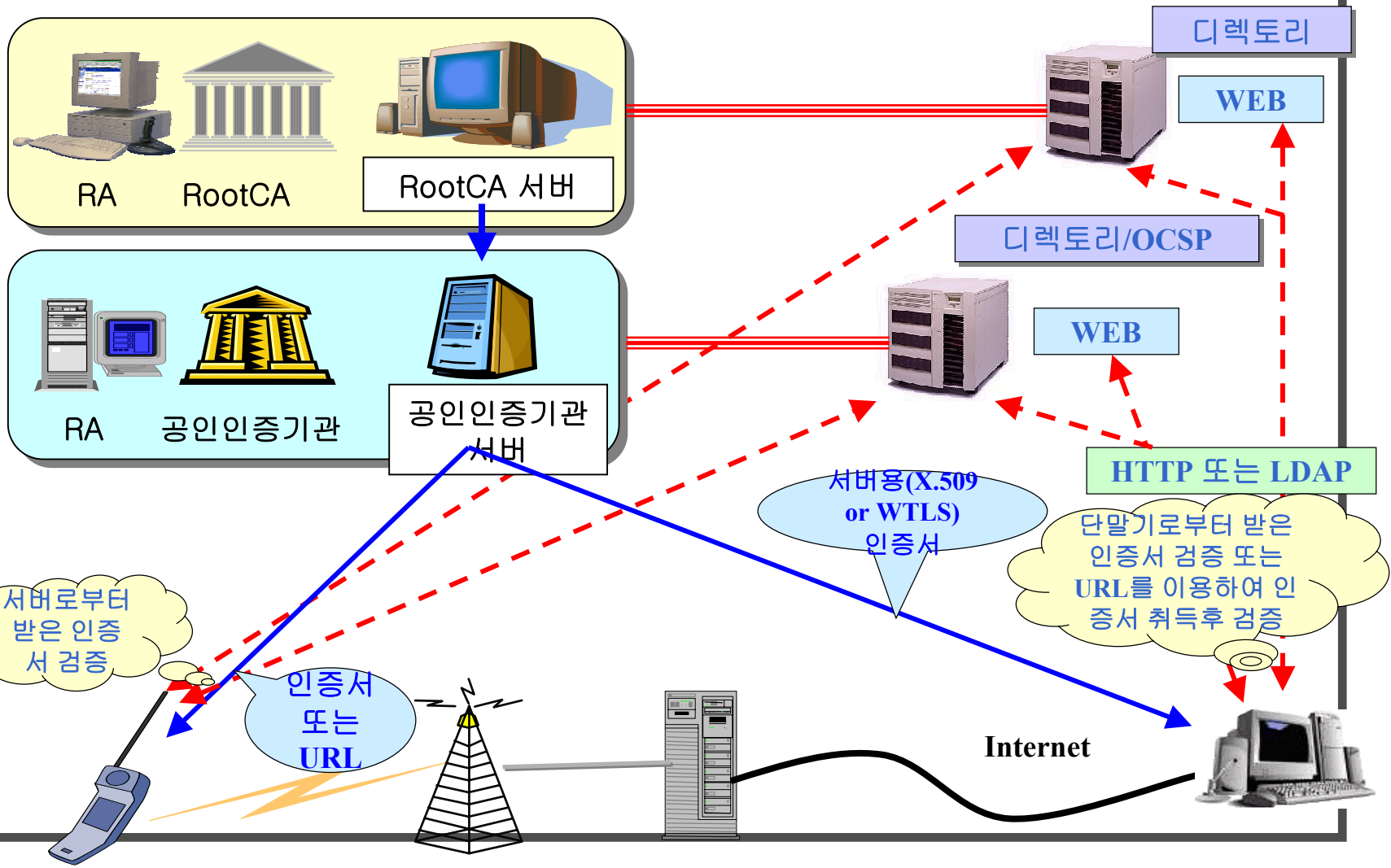
무선 PKI 개발을 위한 고려사항

- 무선 단말기의 CPU가 처리해야 할 데이터를 최소화
  - 처리가능한 서명, 검증, 암호화 알고리즘 채택
- 인증서, CRL 프로파일 규격 및 사용 알고리즘의 최적화
  - 모듈 사이즈 최소화
- 인증서 발급, 저장, 처리, 검증 등에 필요한 프로토콜의 최적화
  - 모듈사이즈 및 처리시간 최소화
- 무선 인터넷 환경에 맞는 인증서 검증 방식을 채택
- 공인인증기관간 상호연동이 가능한 인증서 요청, 관리 프로토콜 적용
- 확장성과 유선 및 국제적 호환성 고려

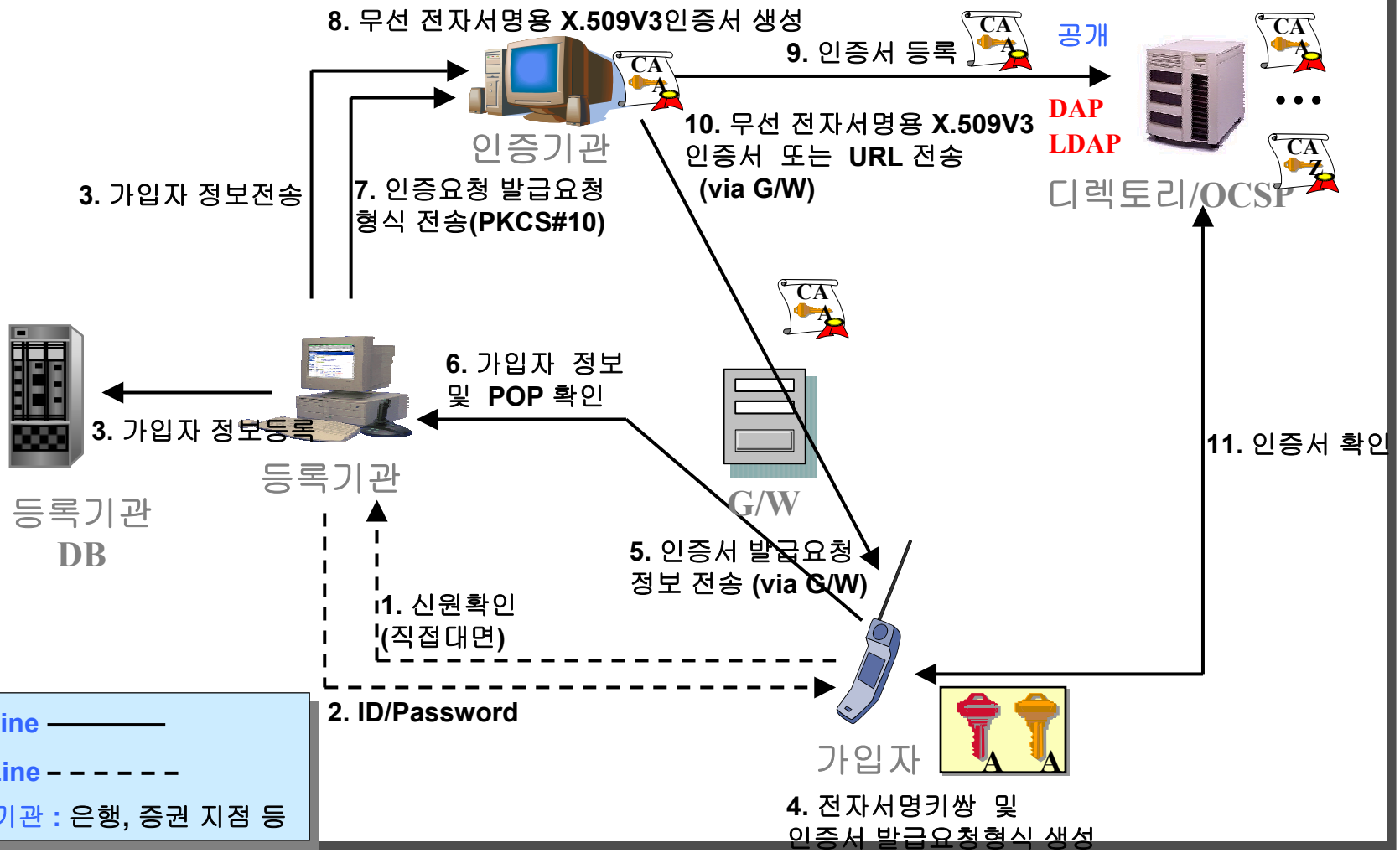
무선 PKI 해결방안

- ❖ 전자서명키 생성 기능
  - RSA와 ECDSA
- ❖ 메시지 암호화 및 복호화 기능
  - 무선 응용계층 보안 프로토콜
- ❖ 인증서 요청 및 관리 기능
  - 무선용 인증서 요청형식 및 관리 프로토콜
- ❖ 인증서 수신, 검증, 저장 및 송신 기능
  - 인증서 URL 사용
  - OCSP를 통한 인증서 검증 및 WTLS 인증서 사용
- ❖ 전자서명된 데이터의 수신, 검증, 저장 및 송신 기능
- ❖ 전자서명 데이터 생성 기능

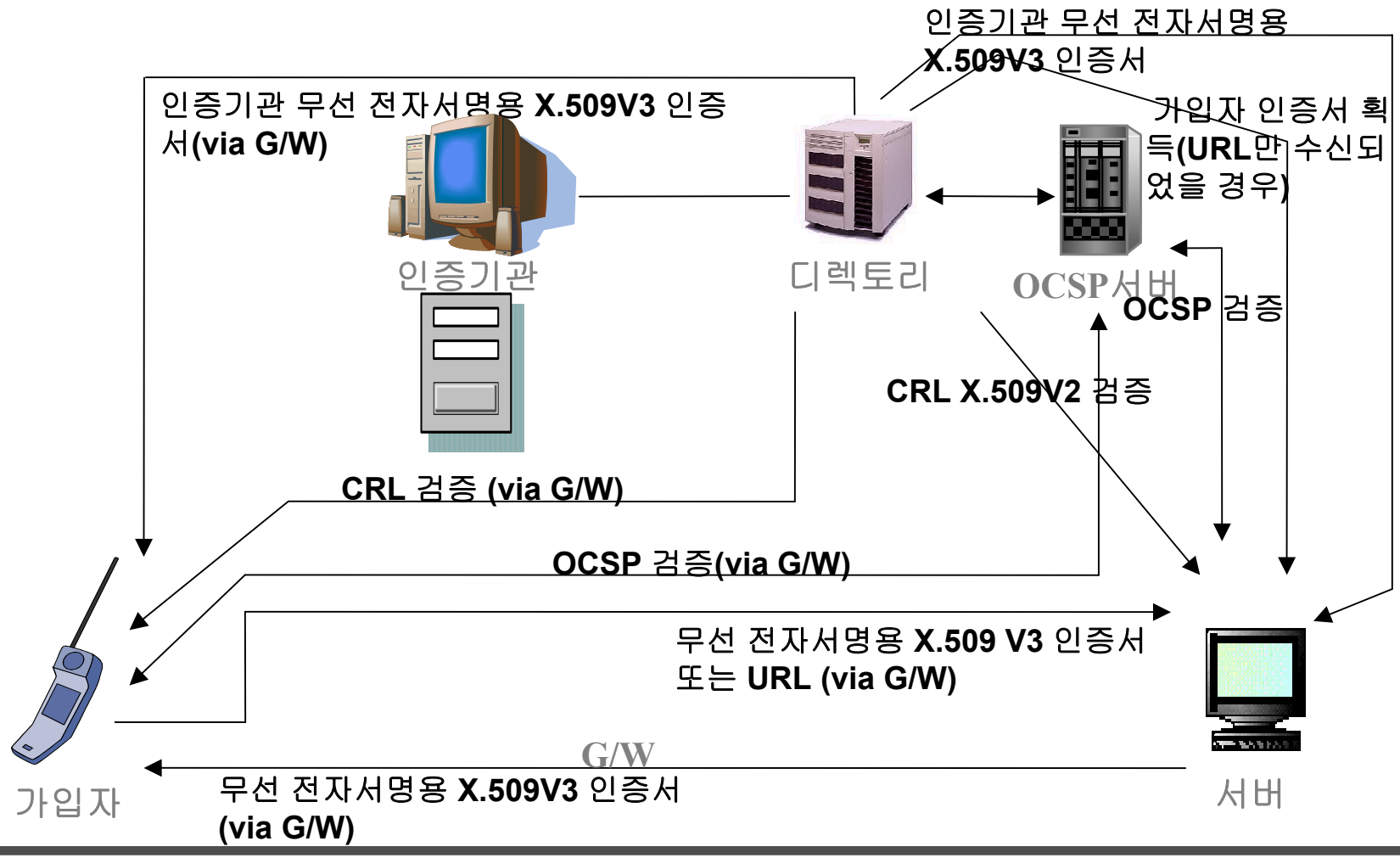
무선 PKI 모델


RA
RootCA
RootCA 서버
디렉토리
WEB
디렉토리/OCSP
RA
공인인증기관
공인인증기관 서버
WEB
HTTP 또는 LDAP
서버용(X.509 or WTLS) 인증서
단말기로부터 받은 인증서 검증 또는 URL를 이용하여 인증서 취득후 검증
서버로부터 받은 인증서 검증
인증서 또는 URL
Internet

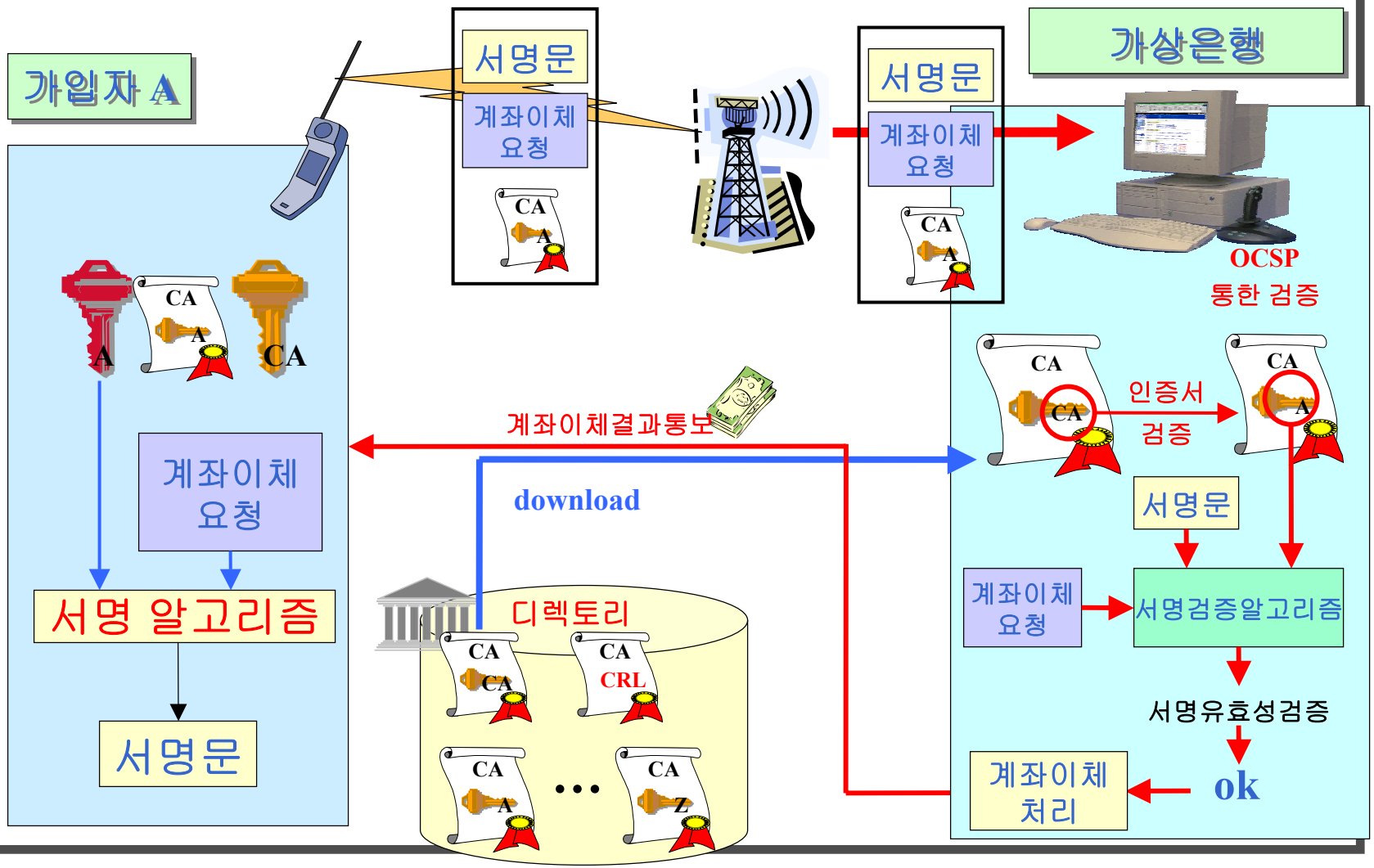
무선 PKI 인증서 발급 모델



무선 PKI 전자서명 검증 모델



무선 PKI 인증서 응용 모델 예



무선 PKI 기술규격

무선 PKI 기술규격 11종

- 무선 전자서명용 인증서 프로파일
- 무선 CRL 프로파일
- 무선 전자서명 DN 규격
- 무선 WTLS 인증서 프로파일
- 무선 WTLS DN 규격
- 무선 전자서명인증관리체계 OID 규격
- 전자서명 알고리즘
- 키분배 알고리즘
- 무선 인증서 요청형식 규격
- 무선 인증서 고나리 프로토콜 규격
- 무선 응용계층 보안 프로토콜 규격

무선 전자서명용 인증서 프로파일

❖ 공인인증기관 및 가입자 인증서 기본필드

기본 필드	생성	처리
버전	m	m
일련번호	m	m
서명 알고리즘	m	m
발급자	m	m
유효기간	m	m
소유자	m	m
소유자 공개키 정보	m	m
발급자 고유 식별자	x	x
소유자 고유 식별자	x	x
확장필드	m	m

무선 전자서명용 인증서 프로파일

❖ 무선 X.509v3 인증서 확장필드

확장 필드	공인인증기관 인증서			가입자 인증서		
	critical	생성	처리	critical	생성	처리
발급자 공개키 식별자	n	m	o	n	m	o
소유자 공개키 식별자	n	m	o	n	m	o
키 사용 목적	c	m	m	c	m	m
소유자 비밀키 유효기간	n	x	x	n	x	x
인증서 정책	b	m	m	b	m	m
인증서 정책 매핑	n	o	m	n	o	m
소유자 대체 명칭	n	m	m	n	m	m
발급자 대체 명칭	n	o	m	n	o	m
기본 제한	c	m	m	c	x	x
이름 제한	c	o	m	–	–	–
정책 제한	c	o	m	–	–	–
확장 키 사용 목적	b	o	m	b	o	m
CRL 분배점	n	m	o	n	m	o
도메인 정보	n	o	o	n	o	o
발급자 정보 접근	n	m	o	n	m	o
대리인	–	–	–	n	o	o

무선 CRL 프로파일

CRL 확장 필드	critical	생성	처리
발급자 공개키 식별자	n	m	m
발급자 대체 이름	n	o	m
CRL 번호	n	m	m
CRL 발행 분배점	c	o	m
Delta CRL Indicator	n	o	o

Entry 확장 필드	critical	생성	처리
효력정지 및 폐지 사유	n	m	m
효력정지시 수행 명령	n	o	o
효력정지 및 폐지 일자	n	o	o
인증서 발급자	c	o	m

유·무선 전자서명 DN 필드 비교

CommonName
serialNumber
contryName
organizationName
organizationUnitName
businessCategory
emailAddress

유선

CommonName
serialNumber
contryName
organizationName
organizationUnitName
businessCategory
emailAddress
DomainComponent

무선

무선 WTLS 인증서 프로파일 규격

기본 필드	생성	처리
버전	m	m
서명 알고리즘	m	m
발급자	m	m
유효시작시간	m	m
유효종료시간	m	m
소유자	m	m
소유자 공개키 타입	m	m
파라미터 식별자	ECC사용시	ECC사용시
공개키	m	m

WTLS 인증서 DN 규격

- 무선에서 추가된 부분
  - DomainComponent : 도메인 네임 구성요소
- WTLS 인증서
  - Text형태(M), Key_hash_sha1(o), Binary(o), X.509_name(o)

CommonName (M)
contryName (M)
organizationName (M)
organizationUnitName (M)
DomainCompenent (M)

전자서명 알고리즘

- RSA 알고리즘
  - 인증서버, CP, 단말기(생성:M, 검증:M)
  - 키 길이는 1024bit 이상
- ECDSA 알고리즘
  - 인증서버, CP, 단말기(생성:M, 검증:M)
  - 키 길이는 160bit 이상

구분 \ 커브	WTLS 5번	WTLS 7번	WTLS 3번	FIPS 186-2	X9.62
인증 서버	M	M	M	H	H
CP 서버	M	M	M	O	O
단말기	M	O	O	O	O

M : Madatory, O : Optional, H : Highly Recommend

- 해쉬 알고리즘
  - SHA1(FIPS 180-1)

키분배 알고리즘

- RSA 알고리즘
  - 키 길이는 1024bit 이상
- ECDH 알고리즘
  - 키 길이는 160bit 이상

구분 \ 커브	WTLS 5번	WTLS 7번	WTLS 3번	FIPS 186-2	X9.62
인증 서버	M	M	M	H	H
CP 서버	M	M	M	O	O
단말기	M	O	O	O	O

M : Madatory, O : Optional, H : Highly Recommend

- 암호화 알고리즘
  - SEED : 키의 길이는 128bit
  - TripleDES : 키의 길이는 168 bit
- 해쉬 알고리즘
  - SHA1(FIPS 180-1)

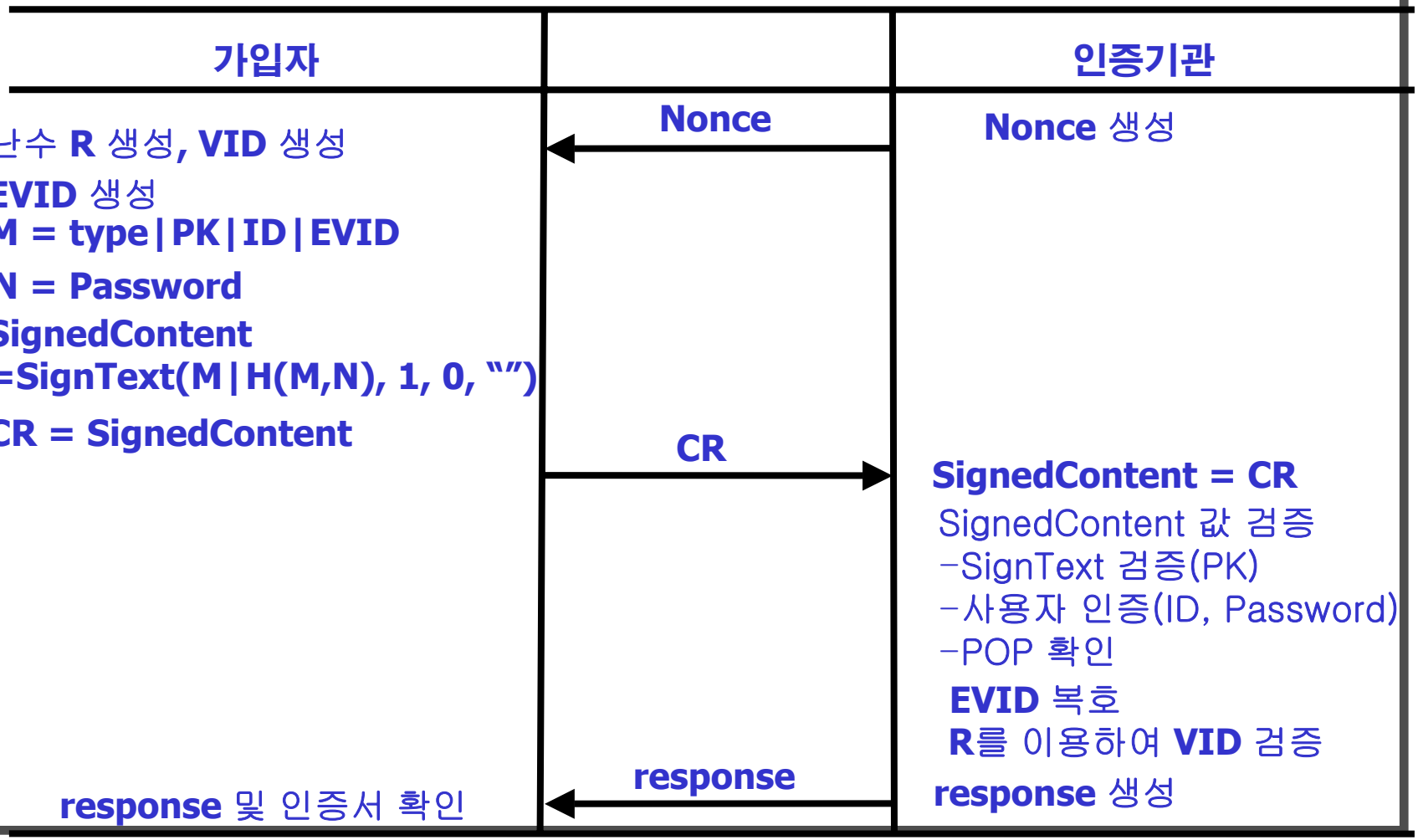
무선 인증서 요청형식 프로토콜 규격

❖ 주요 내용
- 무선단말기 사용자가 인증서 요청형식을 구성하는 방법에 대하여 정의
- 전자서명용과 키분배용 키를 등록기관 또는 공인인증기관에 각각 전달하는 방법과 동시에 전달하는 방법을 정의
- SignText사용(WAP Crypto Library에 정의)

❖ 구성
- 참조번호(ID), 인가코드(PW)
- POP(Proof Of Possession)
- 공개키를 전달하는 방법

❖ 다음의 항목을 만족하고 안전하게 전달되어야 함
- Replay Attack
- 메시지 위변조
- 기밀성

무선 인증서 요청형식 프로토콜 규격



무선 인증서 관리 프로토콜 규격

❖ 주요 내용

- 무선단말기 사용자가 단말기에서 인증서를 관리하는데 필요한 관련 규격을 정의
  - 재발급
  - 갱신
  - 효력정지
  - 인증서 폐지
- 공인인증기관 및 응용프로그램이 관리 프로토콜 형식을 생성하고 처리하는데 필요한 요구사항들을 명시

무선 응용계층 보안 프로토콜 규격

- 주요 내용
  - 인증서 기반의 응용계층 소프트웨어간의 단대단 보안프로토콜에 사용될 Crypto Library 및 단대단 보안 프로토콜을 정의
  - 제품개발시 업체간 상호호환성을 보장하고 암호화된 정보를 생성 처리하는데 필요한 요구사항을 명시
- WAP의 signText()와 encrypt()를 사용
- 프로토콜 Overview
  - End-to-End 보안프로토콜을 사용하기 위해서는 먼저 encrypt()에 필요한 변수(data, 인증서, 암호화 알고리즘 등)을 위한 과정이 필요
  - encrypt()에 필요한 변수 입력과정이 완료되면 encrypt()를 사용하여 End-to-End 보안을 제공할 수 있음

무선 PKI 기술규격 요약

- 무선 전자서명인증서 프로파일
  - Authority Key Identifier와 Subject Key Identifier 필드 : option
- 인증서 검증
  - CRL 검증 및 OCSP 서버를 통한 인증서 상태 확인 기능 제공
- 무선 전자서명 알고리즘으로 ECDSA 정의
  - RSA 알고리즘도 단말기에서 서명, 검증이 가능하도록 정의
- 무선 WTLS 인증서 프로파일
  - 컨텐츠 제공자의 키분배용 인증서로 사용
  - 단말기에서 CRL 검증의 부담을 줄이기 위해 short-lived WTLS 인증서를 사용
- 무선 단말기에서 온라인으로 인증서를 요청할 경우에 사용자 인증과 POP(Proof Of Possession)을 동시에 해결할 수 있는 요청형식을 구성

국내 무선 PKI 구축 현황

- 국내 무선 PKI 기술기준 개발을 위한 실무작업반 구성, 운영(2000.8~11)
- 무선 PKI 기술기준(안) 업체 간담회(2000.11)
- 국내 무선 PKI 기술규격 개발을 위한 실무작업반 구성 (KISA, 공인인증기관, ETRI, 이통사, 무선 PKI 개발업체 등)(2001.1)
- 무선 PKI 기술규격 8종 개발(2001.4)
- 무선 PKI 기술규격 업체간담회(2001.5)
- 무선 PKI 기술규격 3종 추가 개발(2001.8)
- 무선 PKI 기술규격 6종을 ISTF 및 TTA 표준(2002.5)
- 무선 인증서 요청형식 프로토콜 규격을 IETF에 표준으로 제안(2001.12)

Question & Answer