전자기록물의 보안과 인증

2009. 9. 11

중부대학교 정보보호학과
이 병 천 교수

차 례

1. 역사 속의 기록물 보안

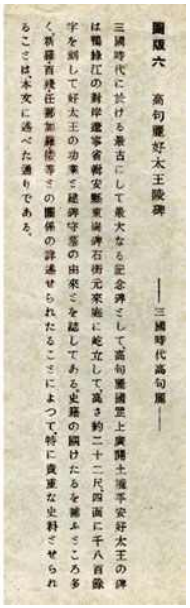
- 기록물 보존을 위한 노력
  - 우리 민족은 역사의 기록에 많은 노력을 기울여 온 민족
  - 역사서, 족보
  - 많은 전란과 외세 침탈로 기록소실
  - 역사왜곡: 일본제국주의, 중국의 동북공정, 조선시대 소중화 사상
- 역사 속의 기록물 보안 사례
  - 성공적 보존 – 조선왕조실록
  - 유실 – 고대 역사서
  - 도난 – 각종 고분의 도굴
  - 변조 – 광개토대왕비와 임나일본부설
- 현재: 정보화 시대의 기록문화를 선도

홍산문화 (요하문명)

위_ 삼좌점 터에서 발굴된 성벽. 움푹 튀어나온 '치'는 고구려 고유의 축성양식을 연상시킨다.
아래_ 삼좌점 발굴현장에서 모습을 드러낸 대형 집터. 대문과 문설주는 물론 곡식창고까지 완벽하게 보존돼 있다. 이곳 60여 채의 군락은 매우 드문 큰 규모로 파악된다. <국학 학술원 제공>

- 기록 이전의 시대
- 고조선, 단군신화와의 연관성
- 고대 역사서들의 유실로 역사단절 초래

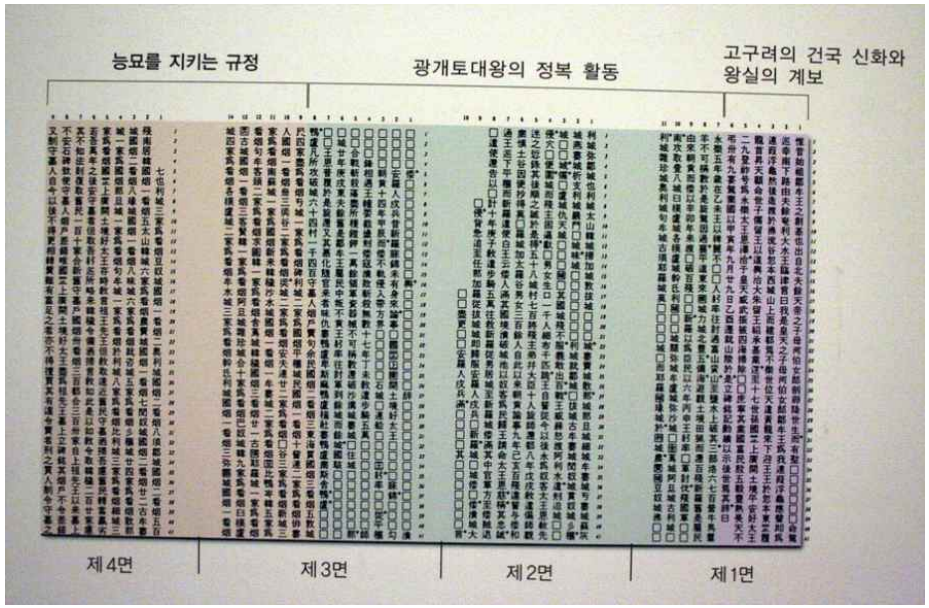
광개토대왕비



圖版六　高句麗好太王陵碑

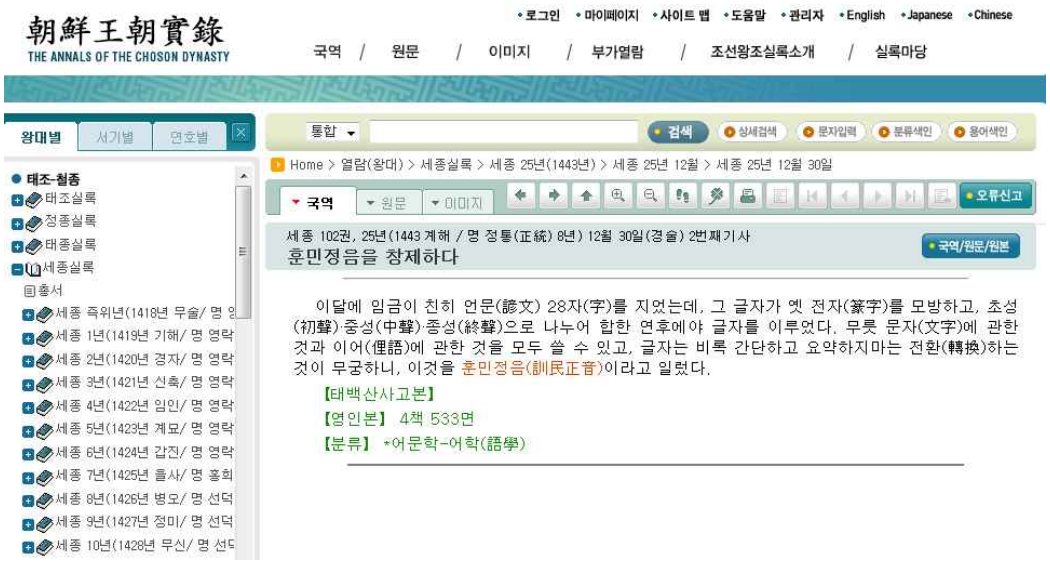
——三國時代高句麗——

三國時代に於ける最古にして最大なる記念碑として高句麗國境内上廣開土境平安好太王の碑は鴨綠江の對岸集安縣東南碑石街元來南に屹立して高さ約二十二尺四面に千八百餘字を刻して好太王の功業と建碑守墓の由來とを記してある史蹟の關けたらを藏ふところ多く殊に百殘任那加羅從等との關係の詳述せられたることによつて特に貴重な史料とせられることは本文に述べた通りである。



- 국가패망으로 인한 역사의 중단, 파괴
- 고구려의 역사서 <유기>와 <신집> 유실
- 일제시대 비문의 위조여부에 대한 논란
- 능묘를 지키는 엄격한 규정

조선왕조실록



- 엄격한 역사기록 체계
- 백업의 중요성
- 임진왜란시의 보존 노력
- 세계기록문화유산으로 등재
- 온라인 정보서비스 제공

국가기록원 나라기록포털

정보화 시대의
전자기록 문화 발전을 선도

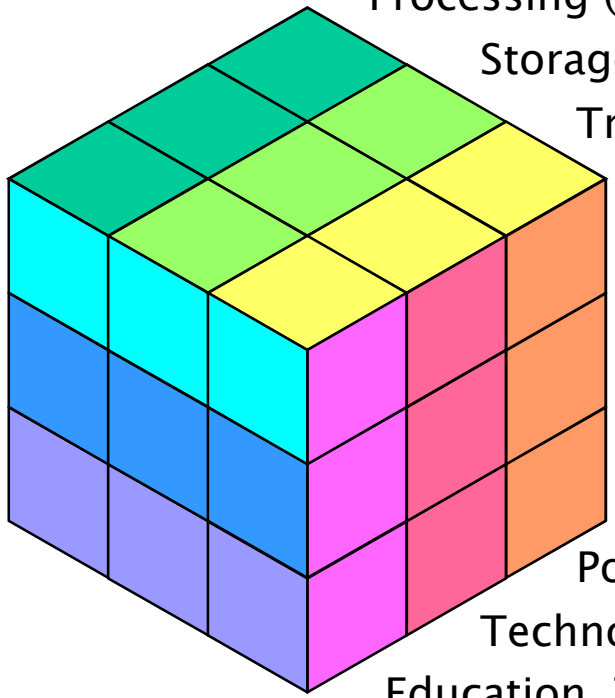
전자문서 시대의 기록 보존

- 전자문서 시대의 기록 보존 노력
  - 물리적 보안
  - 시스템, 네트워크 보안
  - 기록물 생성 관리 체계
  - 보안성 강화된 기록물정보서비스
- 전자기록물 요구사항 – ISO 15489
  - 진본성 (authenticity)
  - 신뢰성 (reliability)
  - 무결성 (integrity)
  - 가용성 (usability)
- 암호기술 활용이 필수

2. 정보보호와 암호기술

- 정보보호
- 주요 암호기술
  - 대칭키 암호
  - 공개키 암호
  - 해쉬함수
  - 전자서명
  - 전자봉투

정보보호



Processing (처리)

정보의 상태

Storage (저장)

Transmission (송신)

Confidentiality
(기밀성)

Integrity
(무결성)

Availability
(가용성)

보안특성

Policy & Procedures (정책)

Technology (기술)

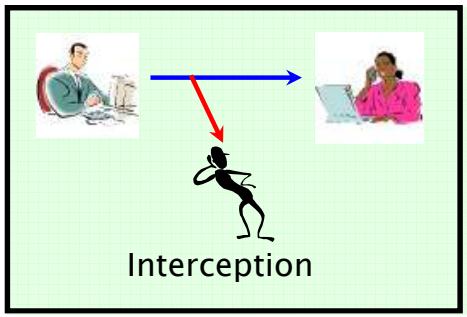
Education, Training &
Awareness (교육)

보안 도구

NSTISSI 4011: National Training Standard for Information Systems Security Professionals, 1994

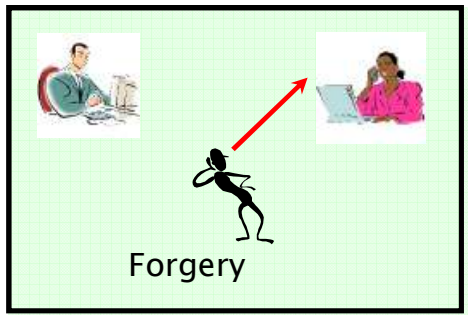
통신상의 보안 요구사항

기밀성



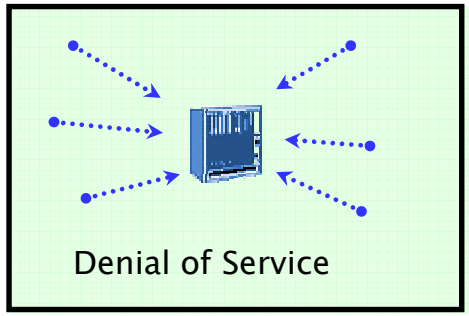
Is Private?

인증성



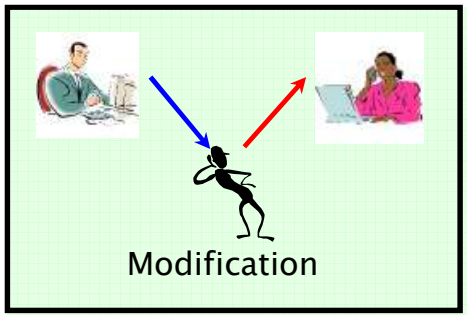
Who am I dealing with?

가용성



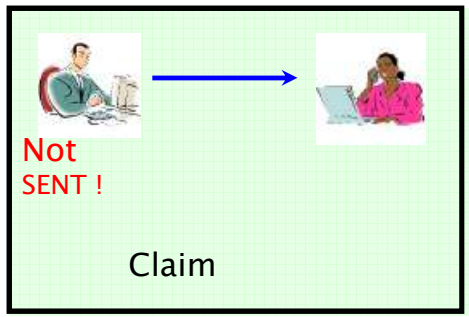
Wish to access!!

무결성



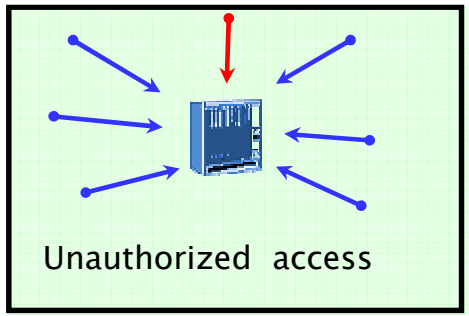
Has been altered?

부인방지



Who sent/received it?

접근제어

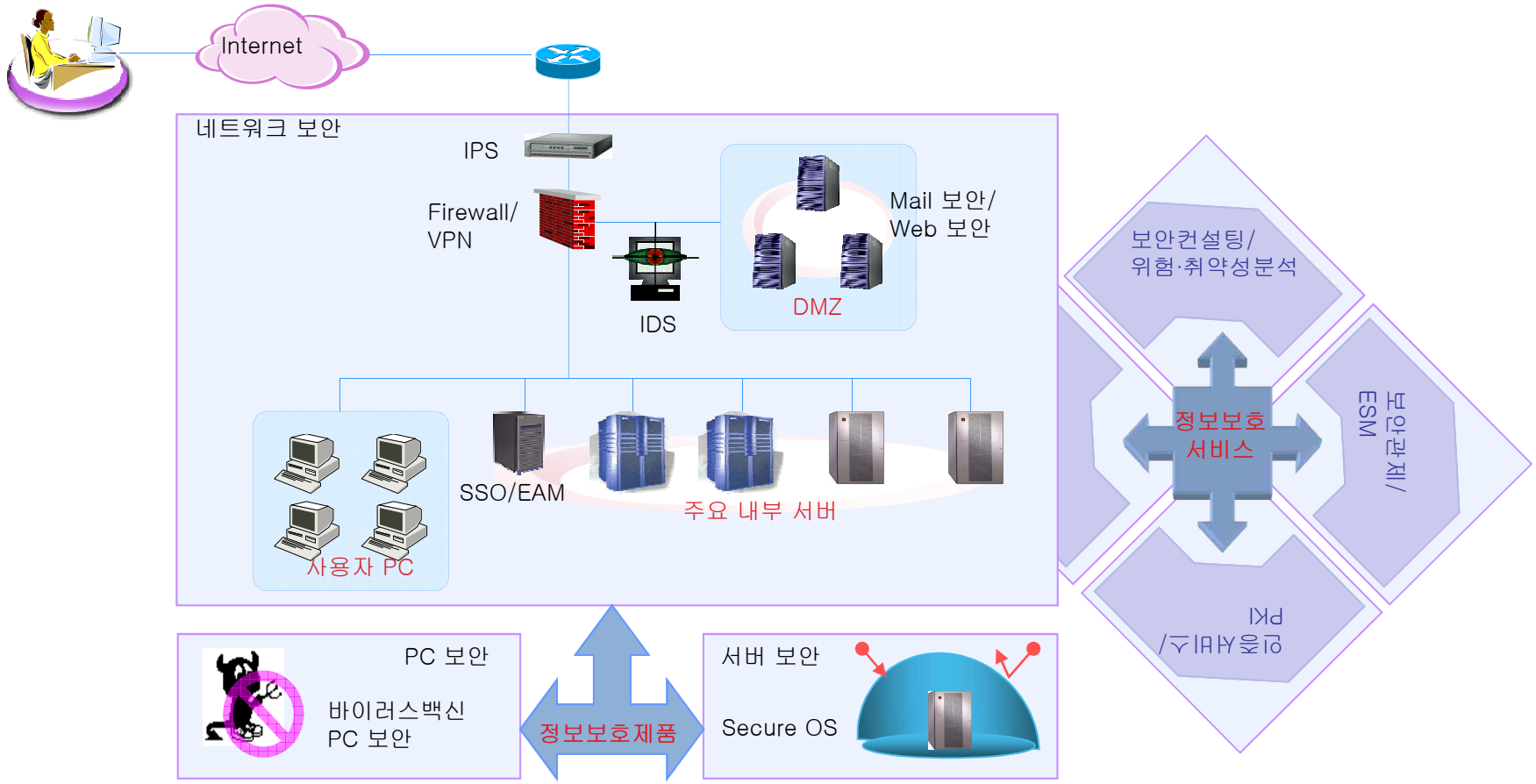


Have you privilege?

정보의 위협요소와 대응방법

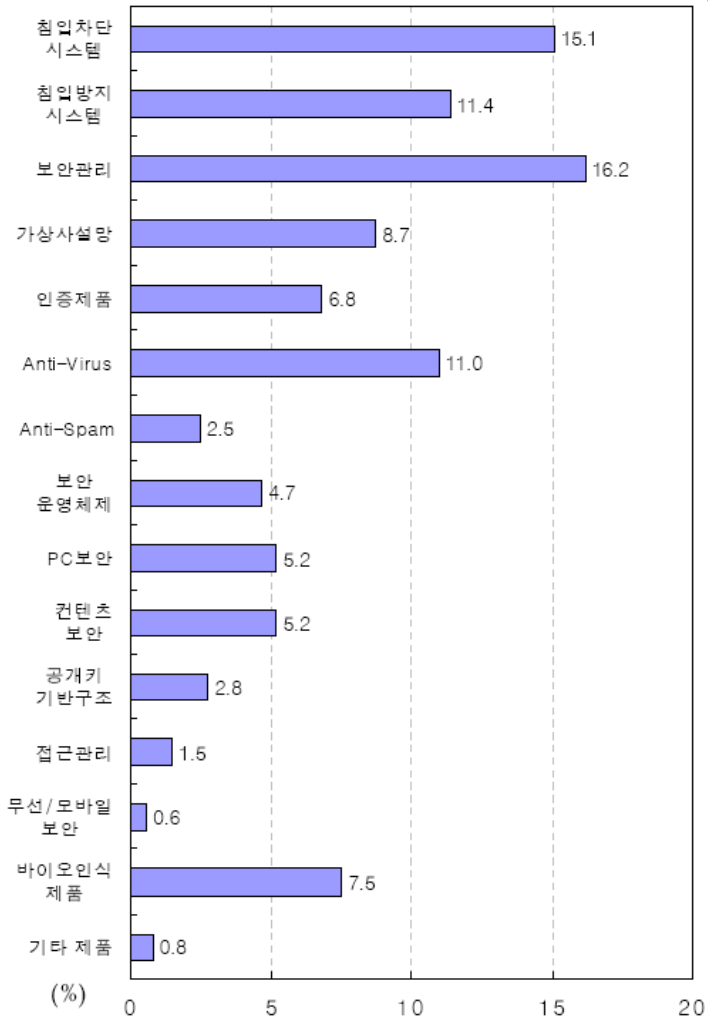
위협 요소	정보보호 서비스	해결 방법
비인가 사용자	Authenticity (인증)	전자서명
데이터 누출	Confidentiality (기밀성)	암호화
데이터 변조	Integrity (무결성)	전자서명
거래 부인	Non-repudiation (부인방지)	전자서명

정보보호 산업

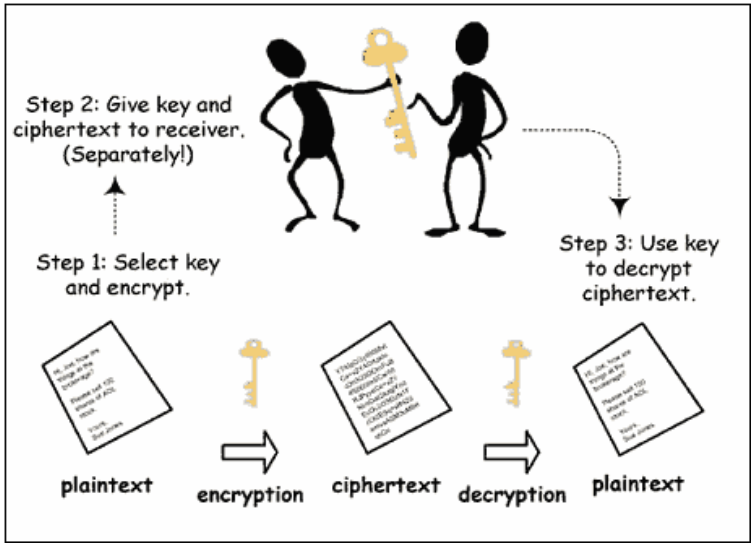

Internet
네트워크 보안
IPS
Firewall/
VPN
IDS
Mail 보안/
Web 보안
DMZ
SSO/EAM
주요 내부 서버
사용자 PC
보안컨설팅/
위험·취약성분석
정보보호
서비스
보안관제/
ESM
인증서비스/
PKI
PC 보안
바이러스백신
PC 보안
정보보호제품
서버 보안
Secure OS

정보보호 산업

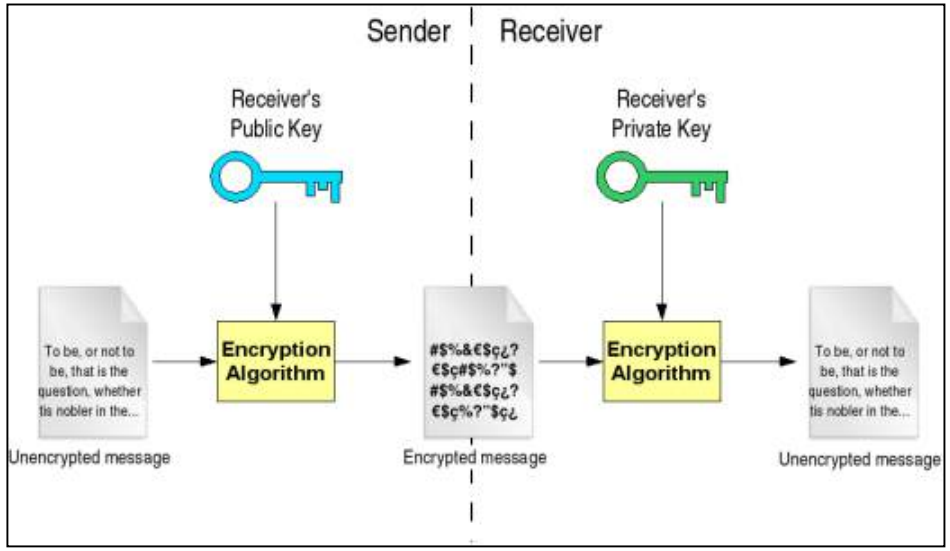
대분류	소분류	기호	세부 항목 예시
정보보호 H/W	침입차단	A	1. 침입차단시스템 2. 웹방화벽 3. 통합보안제품**
	침입방지	B	1. 방화벽 기반 2. 침입탐지시스템 기반 3. 네트워크장비 기반 4. 통합보안 제품**
	가상사설망	C	1. VPN 단일제품 2. 통합보안제품**
	망 전환 장치	D	1. 망 전환 장치
	H/W 인증	E	1. 보안 스마트카드 2. H/W 토큰
	생체인식	F	1. PC/네트워크보안 2. 출입통제/근태관리 3. 법 집행용 4. 금융/결재 시스템 5. 신원인증 6. 기타
정보보호 S/W	보안 관리 S/W	G	1. 통합보안관리 툴 2. 로그 관리/분석 툴 3. 취약점 분석 툴
	침입탐지 S/W	H	1. HIDS 2. HIPS 3. NIDS
	방화벽 S/W	I	1. 개인용 2. 기업용
	Anti Virus	J	1. Virus 백신 2. Anti 스파이웨어
	Anti Spam	K	1. 스팸차단 S/W
	시스템 보안	L	1. Secure OS 2. 서버 보안
	PC 보안	M	1. PC 보안
	어플리케이션 보안	N	1. 내부정보유출방지 2. DB보안 3. DRM(문서/이메일)
	3A	O	1. PKI 2. EAM 3. SSO 4. IM/IAM
	무선/모바일 보안	P	1. WPKI 2. WLAN 보안 3. 모바일 백신
정보보호 서비스	인증 서비스	Q	1. 공인/사설 인증 서비스
	보안 관제	R	1. 보안관제 서비스
	보안 컨설팅	S	1. 안전진단 2. 인증 3. 기반보호
	유지 보수	T	1. 판매 후 유료서비스
	기술 공급	U	1. 기술/ DB 제공
	기타서비스	V	1. 교육 훈련 서비스 2. 보안 제품 렌탈/임대



대칭키 암호와 공개키 암호



대칭키 암호



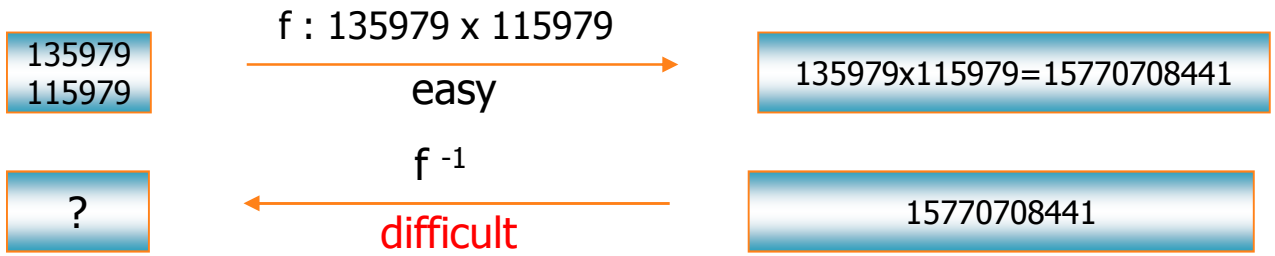
공개키 암호

두 암호방식의 비교

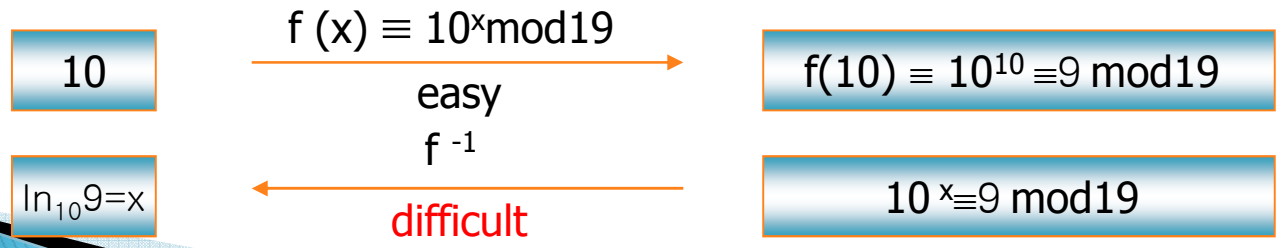
	대칭키 암호 방식	공개키 암호방식
암호키 관계	암호화키 = 복호화키	암호화키 ≠ 복호화키
암호화 키	비밀	공개
복호화 키	비밀	비밀
암호 알고리즘	비밀/공개	공개
비밀키 수	${}_nC_2$	$2n$
안전한 인증	곤란	용이
암호화 속도	고속	저속

어려운 수학적 문제

- 소인수분해 문제(factorization problem)
  - 큰 두 소수의 곱을 구하기는 쉽지만, 큰 두 소수의 곱인 합성수의 소인수 분해는 어렵다

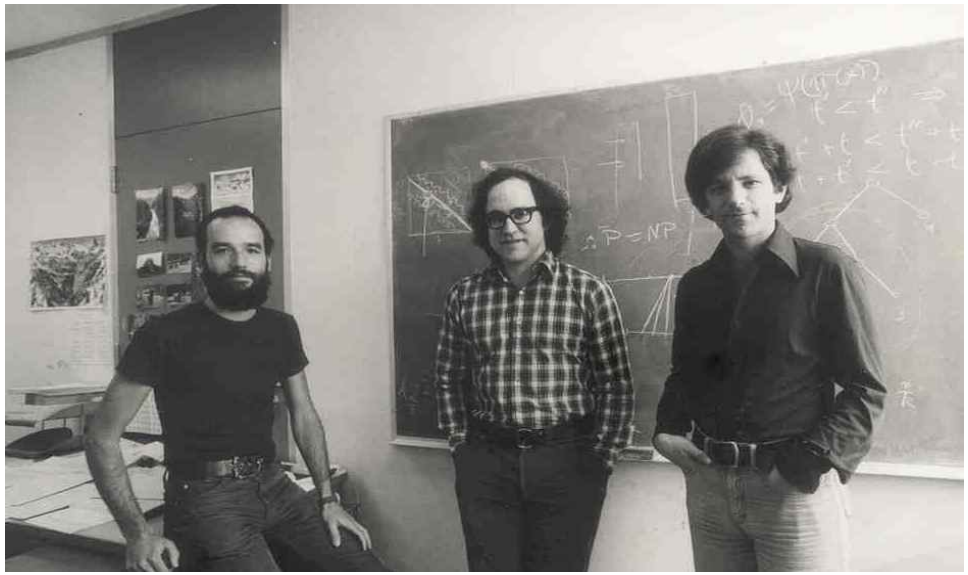


- 이산대수 문제(discrete logarithm problem)
  - 큰 수 n을 법으로 하는 지수승 $y \equiv k^x \bmod n$은 계산하기 쉽지만, 주어진 y와 k에 대하여 식 $y \equiv k^x \bmod n$을 만족하는 x를 구하기는 어렵다



RSA 공개키 암호

- 1977년 MIT의 Ron Rivest, Adi Shamir, Leonard Adleman에 의해 처음으로 제안된 공개키 암호 알고리즘
- 아직도 안전하다고 인정되고 널리 사용됨
- 키 길이 : 1024비트, 2048비트



Shamir Rivest Adleman

공개키 암호의 해독

RSA-200 해독
2005. 5. 9.
F. Bahr, M. Boehm, J. Franke, and T. Kleinjung

Date: Mon, 9 May 2005 18:05:10 +0200 (CEST)
From: Thorsten Kleinjung
Subject: rsa200

We have factored RSA200 by GNFS. The factors are

RSA-200
= 27997833911221327870829467638722601621070446786955428537560009929326128400107609345671052955360856061822351910951365788637105954482006576775098580557613579098734950144178863178946295187237869221823983

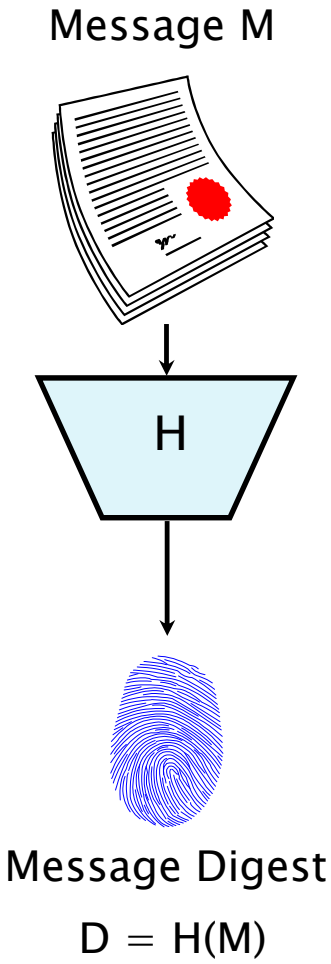
= 35324619344027701212726049781984643686711974001976250236493034687761212536794232000585479565280883496
× 79258699544783330333470858414800596877379758573642199607343303414557678728181521353814093047401854677

병렬컴퓨터 이용
2.2GHz Opteron 컴퓨터의 75년 계산량 사용

http://www.loria.fr/~zimmerma/records/rsa200

해쉬함수

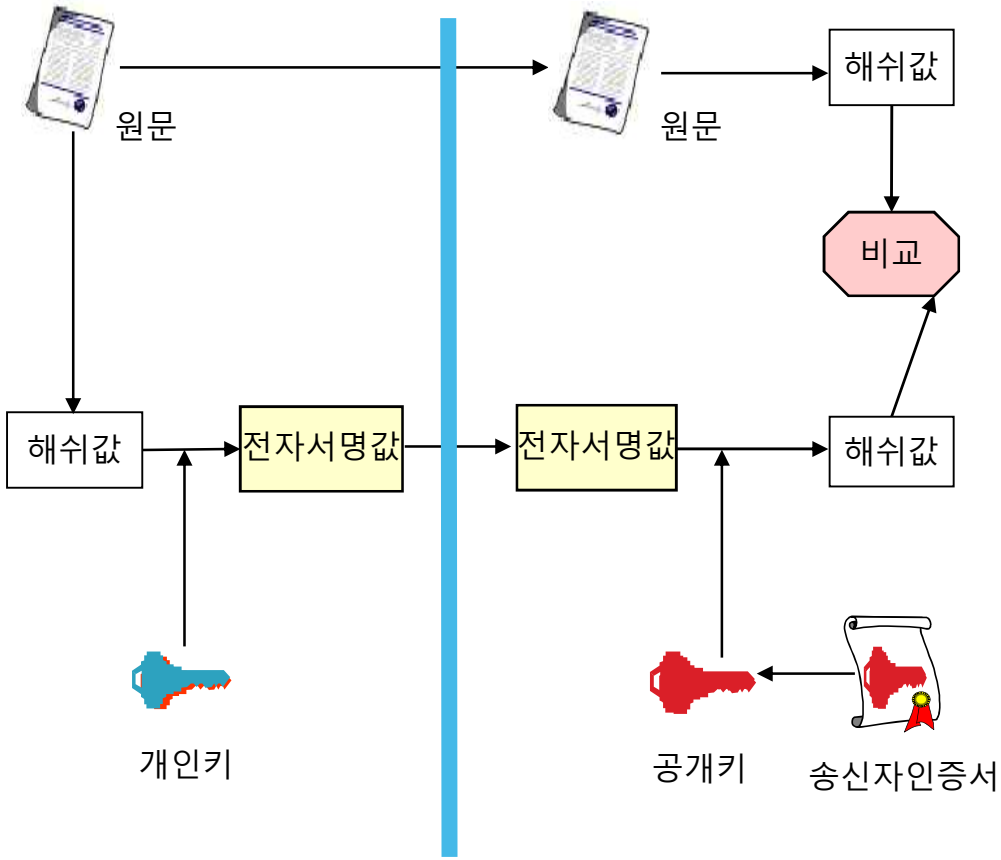
- 해쉬함수란?
  - 임의의 길이의 입력메시지에 대해 고정된 길이의 해쉬값(특징값, 지문)을 출력하는 함수
  - 키를 사용하지 않는 공개된 함수
  - 일방향함수: 출력 해쉬값으로부터 입력메시지를 찾아내기 어렵다.
  - 충돌회피성: 같은 해쉬값을 가지는 메시지 쌍을 찾는 것이 어려워야 함
  - MD5, SHA1, SHA2, HAS160 등
- 해쉬함수의 응용
  - 전자서명
  - 메시지인증코드 (공유키 사용)



전자서명

- 전자서명
  - 전자문서에 대한 서명
  - 공개키 암호 및 해쉬함수 이용
  - 전자서명법에 의해 유효성을 법적으로 인정
- 전자서명의 보안요구사항
  - 위조불가 (unforgeable)
  - 서명자 인증 (user authentication)
  - 부인불가 (non-repudiation)
  - 변경불가 (unalterable)
  - 재사용 불가 (not reusable)

공개키 암호를 이용하는 전자서명

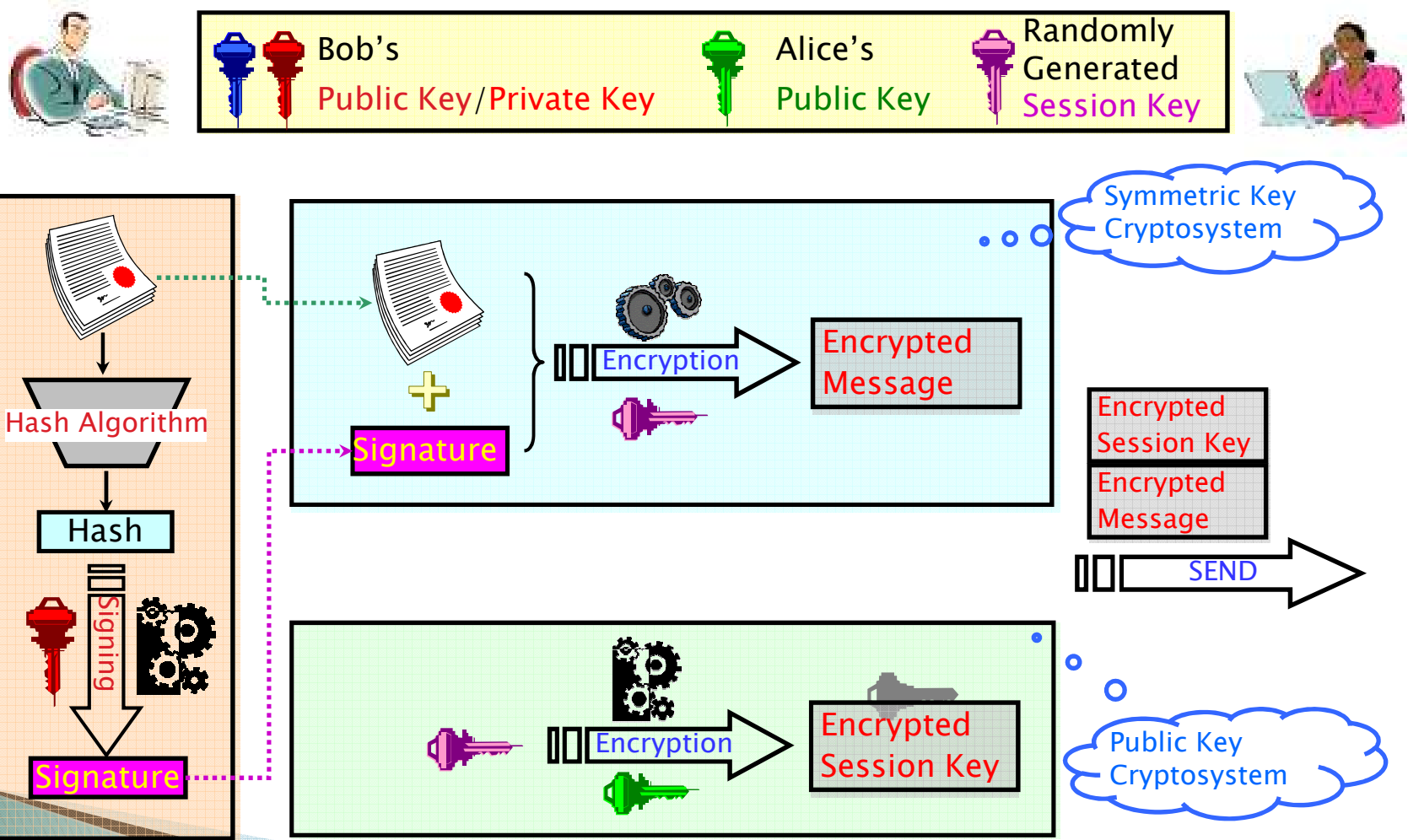


※ 본인 인증
송신자는 자신만이 가지고 있는 개인키와 인증기관에서 인증 받은 공개키, 즉 인증서를 통해 본인임을 입증

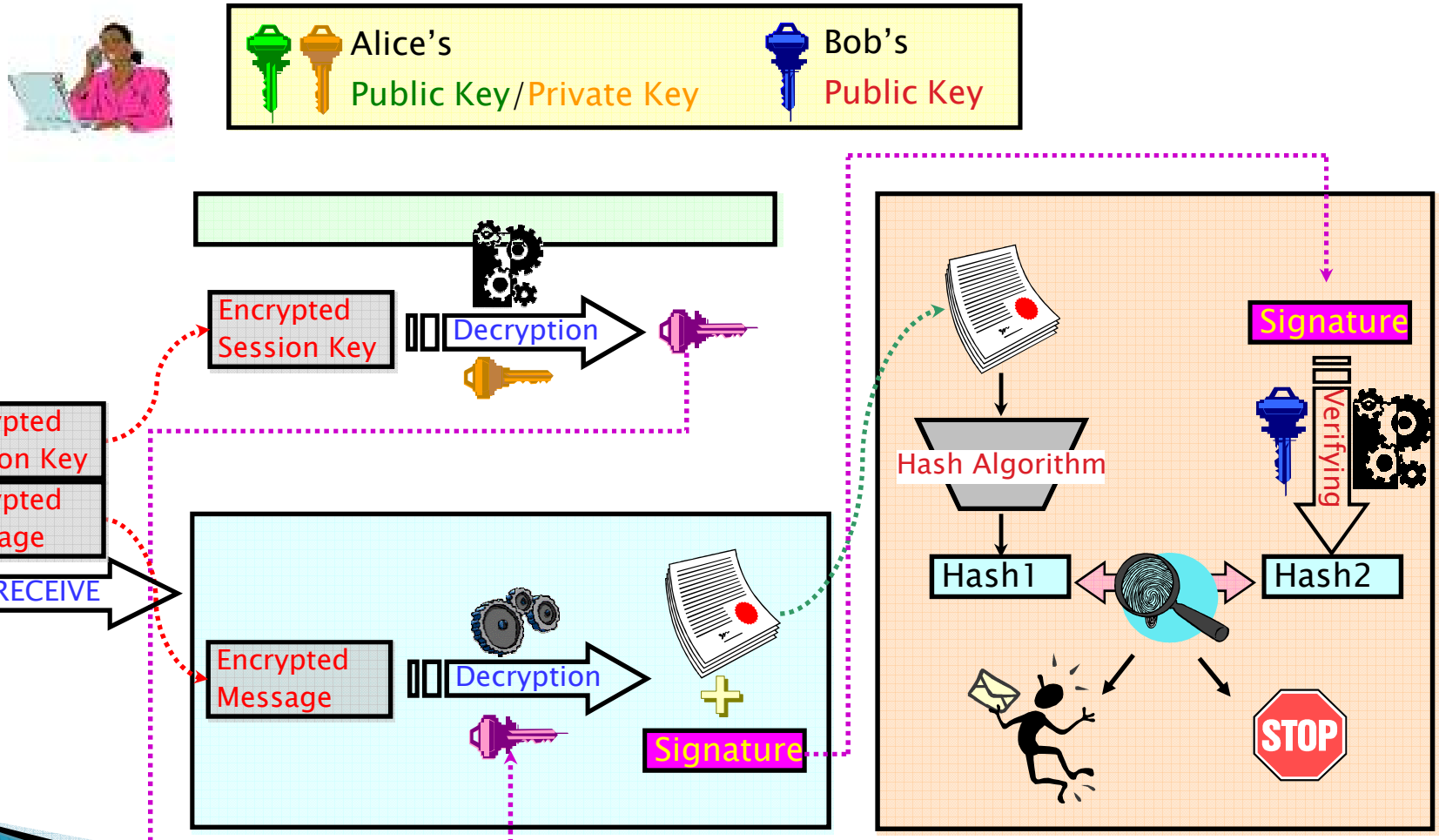
※ 무결성 보장
원문의 해쉬값과 전자서명값을 복호화한 해쉬값을 비교함으로서 위.변조 여부를 판단

※ 부인 봉쇄
송신자는 자신만이 가지고 있는 개인키를 이용하여 전자서명을 하였으므로 문서를 전송하지 않았다고 부인 불가

전자봉투: 키전송+암호화+서명



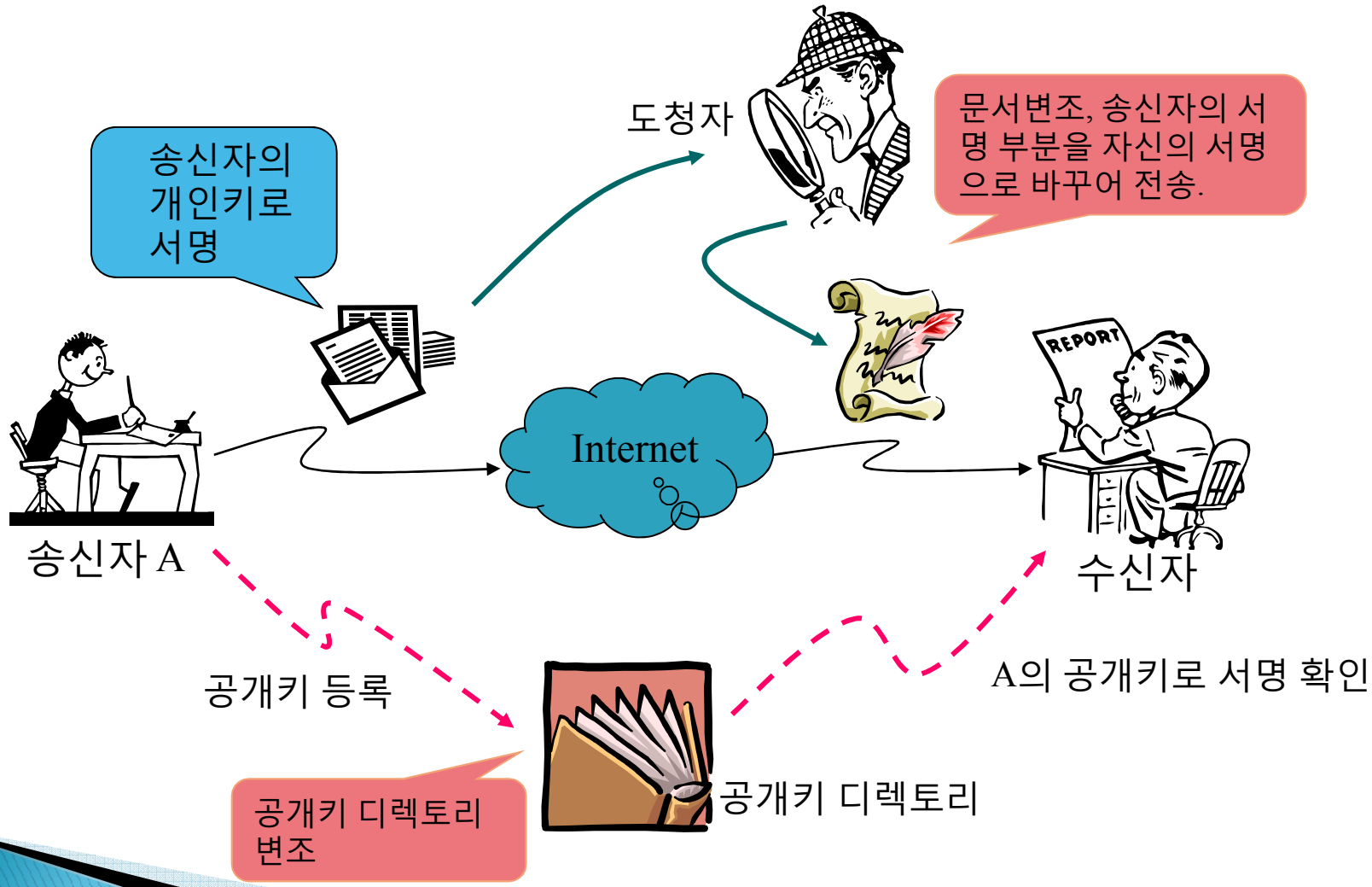
전자봉투: 키복구+복호화+서명검증



3. 전자서명과 공인인증

- 전자서명의 인증 문제
- 공인인증서와 PKI
- 인증서 폐기
- 공인인증체계

전자서명의 인증문제

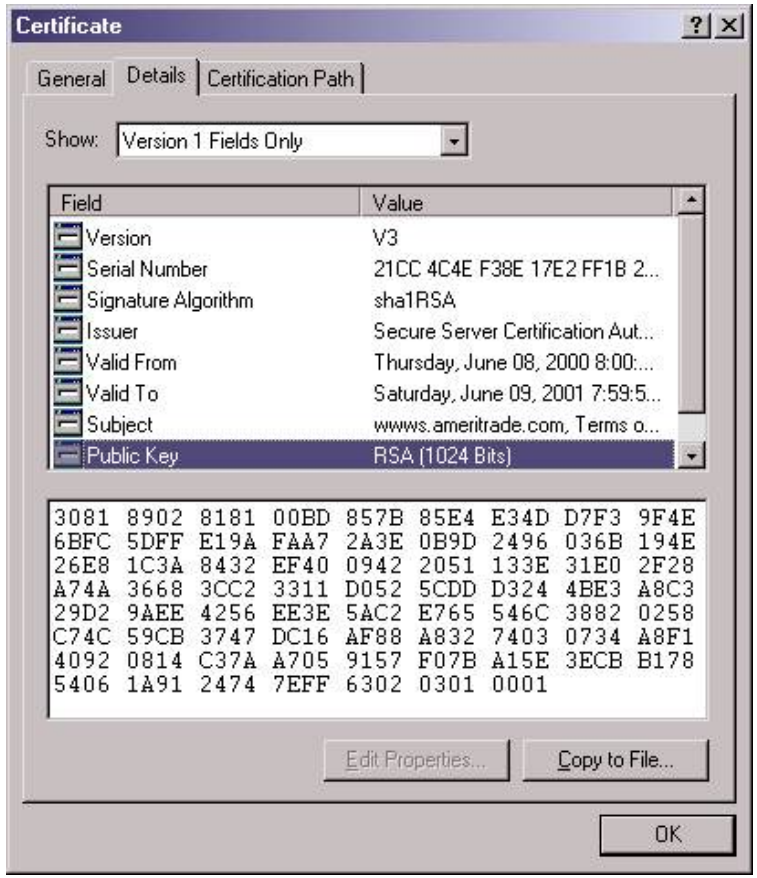

송신자의
개인키로
서명
도청자
문서변조, 송신자의 서명 부분을 자신의 서명으로 바꾸어 전송.
Internet
REPORT
송신자 A
수신자
공개키 등록
A의 공개키로 서명 확인
공개키 디렉토리
공개키 디렉토리
변조

공개키인증서

- 공개키인증서 (Certificate)
  - 사용자의 공개키와 사용자의 ID를 결합하여 인증기관이 서명한 문서, 공개키의 인증성을 제공
  - 사용자 확인, 특정 활동, 권한, 능력을 허가하는데 이용
  - 정보화 사회에서 개인의 신분증 역할
  - CA는 자신의 개인키를 사용하여 전자서명을 생성하여 인증서에 첨부, CA의 공개키를 사용하여 인증서 유효성 확인

공개키인증서

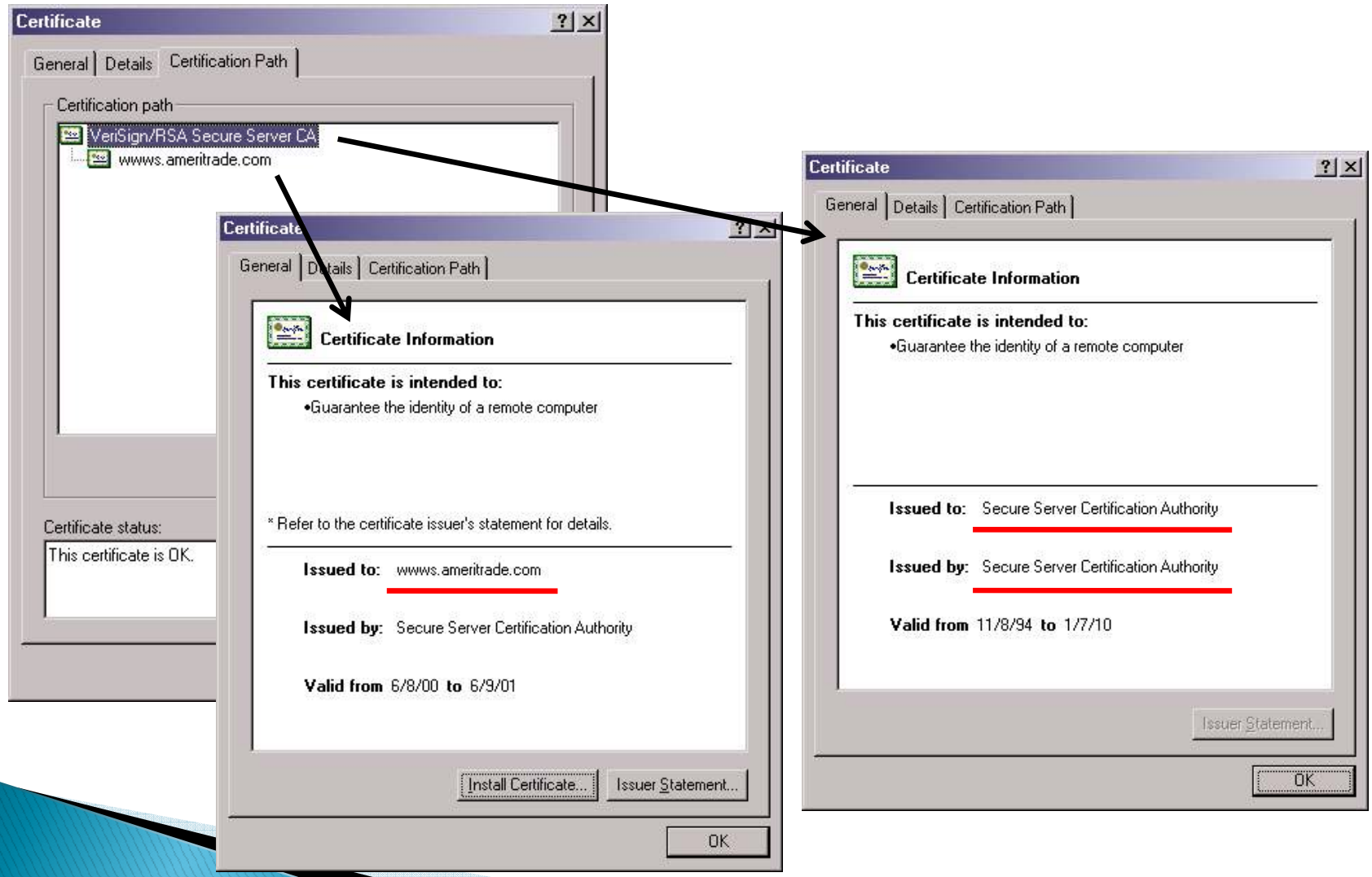

VeriSign - Relying Party Agreement - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites
Address https://www.verisign.com/repository/rpa.html
Go
Home Search Products Support
:Home | Repository | RPA
VeriSign Relying Party Agreement
YOU MUST READ THIS RELYING PARTY AGREEMENT BEFORE VALIDATING A VERISIGN TRUST NETWORKSM DIGITAL CERTIFICATE ("CERTIFICATE") OR USING VERISIGN'S OCSP SERVICES OR OTHERWISE ACCESSING OR USING VERISIGN'S DATABASE OF CERTIFICATE REVOCATIONS AND OTHER INFORMATION ("REPOSITORY") OR ANY CERTIFICATE REVOCATION
Internet


Certificate
General Details Certification Path
Show: Version 1 Fields Only
Field
Value
Version
V3
Serial Number
21CC 4C4E F38E 17E2 FF1B 2...
Signature Algorithm
sha1RSA
Issuer
Secure Server Certification Aut...
Valid From
Thursday, June 08, 2000 8:00:...
Valid To
Saturday, June 09, 2001 7:59:5...
Subject
wwws.ameritrade.com, Terms o...
Public Key
RSA (1024 Bits)
3081 8902 8181 00BD 857B 85E4 E34D D7F3 9F4E
6BFC 5DFF E19A FAA7 2A3E 0B9D 2496 036B 194E
26E8 1C3A 8432 EF40 0942 2051 133E 31E0 2F28
A74A 3668 3CC2 3311 D052 5CDD D324 4BE3 A8C3
29D2 9AEE 4256 EE3E 5AC2 E765 546C 3882 0258
C74C 59CB 3747 DC16 AF88 A832 7403 0734 A8F1
4092 0814 C37A A705 9157 F07B A15E 3ECB B178
5406 1A91 2474 7EFF 6302 0301 0001
Edit Properties...
Copy to File...
OK

공개키기반구조

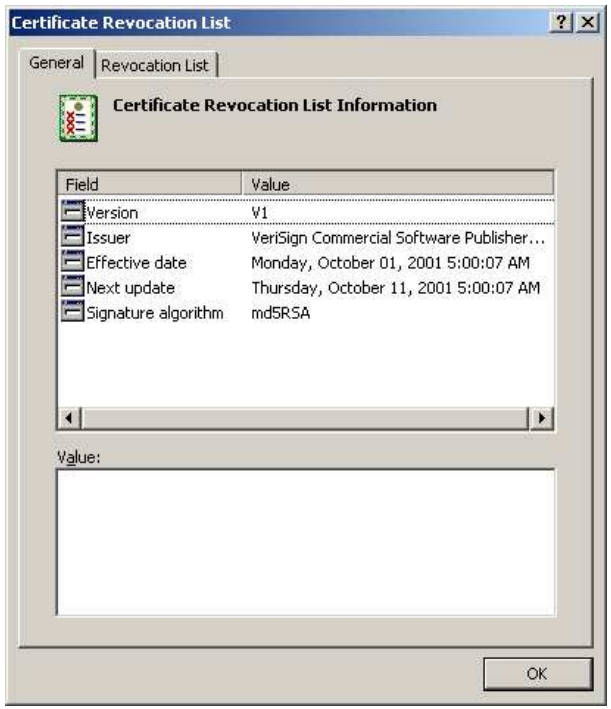
- 공개키 기반구조(PKI, Public Key Infrastructure)
  - 공개키 인증서의 인증성을 제공하는 신뢰구조
  - 다수의 인증기관들을 포함하는 복잡한 구조에서의 상호 인증을 위한 계층적 인증 체계 – 인증서 발행, 배달, 관리, 인증네트워크
- 표준안
  - X.509, The Directory: Authentication Framework, 1993.
  - PKIX: Internet X.509 Public Key Certificate Infrastructure.

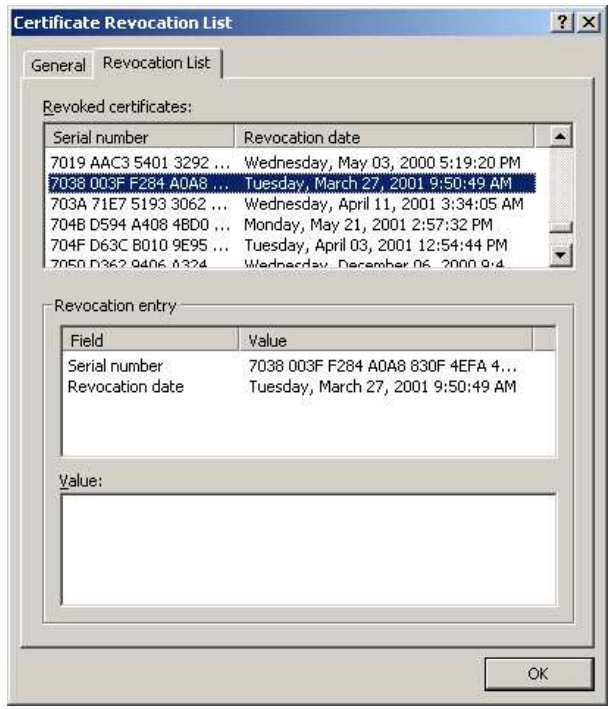
인증경로


Certificate
General
Details
Certification Path
Certification path
VeriSign/RSA Secure Server CA
wwws.ameritrade.com
Certificate status:
This certificate is OK.
Certificate Information
This certificate is intended to:
•Guarantee the identity of a remote computer
* Refer to the certificate issuer's statement for details.
Issued to: wwws.ameritrade.com
Issued by: Secure Server Certification Authority
Valid from 6/8/00 to 6/9/01
Install Certificate...
Issuer Statement...
OK
Certificate Information
This certificate is intended to:
•Guarantee the identity of a remote computer
Issued to: Secure Server Certification Authority
Issued by: Secure Server Certification Authority
Valid from 11/8/94 to 1/7/10
Issuer Statement...
OK

인증서폐기목록(CRL)

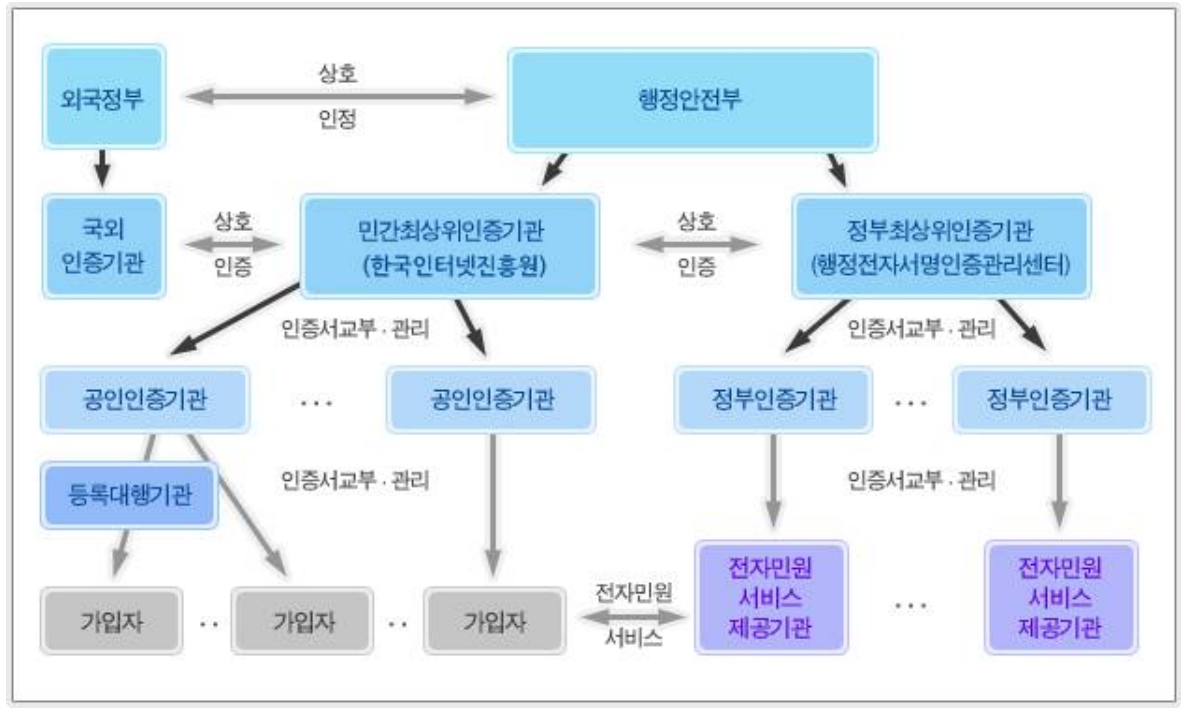
- 인증서 폐기 사유: 인증서 발행 조직에서의 탈퇴, 비밀키의 손상, 비밀키 유출의 의심
- 인증서 폐기 메커니즘: X.509에 정의된 CRL 메커니즘





공인인증체계

- **전자서명법 제4조의 규정에 의하여 지정된 공인인증기관**
  - 한국정보인증(주)
  - (주)코스콤
  - 금융결제원
  - 한국전자인증(주)
  - 한국무역정보통신



4. 전자서명 장기검증

- 전자서명의 유효성 검증 과정
  - 서명검증 (공개키 이용)
  - 공개키 유효성 검증 (인증서 이용)
  - 전자서명의 검증을 위해서는 인증서의 유효성 검증 필요
- 인증서 검증
  - 인증서 내용 확인 : 유효기간, 용도 등
  - CA의 서명 확인
  - 인증서 폐기여부 확인 (CRL 확인)
- 전자서명 장기검증: 오랜 시간이 지난 후의 서명 검증
  - 인증서 및 CRL 유효기간 만료 이후
  - 장기검증을 위한 별도의 조치 필요

전자서명 장기검증 방법

*TSA: 시점확인서비스기관

- RFC3126 방법 (문서의 유효성 연장)
  - 서명된 전자문서에 대해 TSA로부터 타임스탬프를 받아서 저장
  - TSA의 인증서 교체 시점마다 타임스탬프를 다시 받아야 하므로 시간의 흐름에 따라 검증데이터가 증가하고 지속적인 관리 필요
- 전자거래진흥원 방법
  - 인증서 검증을 위한 CRL 정보를 안전하게 장기보관
  - 유효기간이 지난 CRL의 검증을 위한 방안이 필요
- 국가기록원 방법 (CRL의 유효성 연장)
  - 서명검증에 사용되는 CRL에 대해 TSA로부터 타임스탬프를 받아서 CRL이 현시점에서 유효함을 증명받음, TSA 인증서의 유효기간까지 서명의 유효성 연장
  - TSA 인증서가 갱신되면 CRL에 대한 타임스탬프를 다시 받아야 하는 단점.

장기검증 개선방안

- 현재 방법의 비효율성
  - TSA 인증서가 갱신될 때마다 CRL에 대한 타임스탬프를 TSA로부터 다시 받아야 한다는 것은 비효율적
  - 개개의 CRL마다 TSA의 타임스탬프를 받는 것은 비효율적
  - 루트CA 보다는 TSA에 대한 신뢰에 의존
- 인증기관의 업무연속성 제공을 통한 개선방안
  - 현 시점에서 인증기관의 과거 인증서가 유효하게 인정될 수만 있다면 CRL의 유효성을 검증할 수 있고 전자서명의 장기검증도 가능함
  - 인증기관의 인증서가 갱신되는 경우 과거 인증서의 효력이 자동 검증될 수 있도록 하는 메커니즘이 필요 (인증기관의 업무연속성)
  - 루트CA의 신뢰에 의존하는 검증방법

인증기관의 업무연속성

- 비유: 지난 정부에서 실행되었던 국가의 주요 업무는 (별도 조치가 없는 한) 현 정부에서도 그 유효성이 인정되어야 함.

루트CA의 업무연속성 제공방안

- 인증서신뢰목록 이용하여 과거 인증서들을 인증
  - 인증기관의 인증서가 갱신되는 경우 자신의 과거 인증서들에 대한 신뢰목록을 발행, 이러한 신뢰목록에 근거하여 과거 인증서들의 유효성을 자동 검증
  - 자신의 과거 인증서들의 유효성을 인정한다는 업무연속성의 명시적 선언 (역사승계선언)
  - 최상위 인증기관에 대해서만 이러한 신뢰목록 서비스를 허용
  - 루트CA의 업무연속성 보장 메커니즘의 존재는 PKI 전체의 효율성 향상에 기여

루트CA 인증서

Root CA Certificate

2000~2010

Data:
Version: 3 (0x2)
Serial Number: 3 (0x3)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=KR, O=KISA, OU=ROOTCA, CN=CertRSA01
Validity
Not Before: Mar 2 15:00:00 2000 GMT
Not After : Mar 3 14:59:59 2010 GMT
Subject: C=KR, O=KISA, OU=ROOTCA, CN=CertRSA01
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:ce:cf:ed:e1:e8:56:1d:c9:4b:32:60:9b:2a:b7:
97:87:61:06:34:68:cb:17:ae:c0:78:c5:c6:11:5b:
4b:7c:97:ab:b9:6c:4e:2f:00:f6:53:2c:e9:e1:9c:
5a:90:6a:3d:7a:38:38:35:5a:ad:1c:0a:59:85:bb:
f5:63:67:09:13:e9:26:4f:d8:3c:5d:ef:53:42:de:
45:62:e4:3e:cd:72:a4:fa:b3:c0:e0:1f:8e:94:e2:
65:2d:55:c1:15:92:2c:6f:f3:43:d4:35:05:05:34:
37:a0:2c:b4:73:5b:f1:27:26:94:9a:f5:ba:12:cc:
fa:78:35:a2:ad:54:d5:66:8f:11:ea:a6:19:4d:d7:
13:35:54:7b:91:97:03:47:63:b0:a9:0f:68:be:d2:
f4:9e:ea:8d:b5:7b:44:b5:b9:2d:38:c9:00:e3:e5:
bf:c6:75:89:03:99:ff:8c:4b:08:0f:c2:05:31:a4:
4d:17:11:ce:c3:75:0f:6b:b0:5f:d0:ac:86:ad:7d:
e9:a0:88:b9:c6:12:d6:c0:3a:2c:d2:6f:6c:27:1d:
aa:ff:45:9b:c6:03:10:02:69:f9:06:ef:9f:22:a0:
38:38:82:c8:24:11:ac:a1:9e:8f:4d:be:78:5f:df:
ba:3f:83:03:7d:51:a3:f8:c7:5d:a8:91:68:1f:1e:
72:dd

Root CA Certificate

2005~2025

Data:
Version: 3 (0x2)
Serial Number: 4 (0x4)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=KR, O=KISA, OU=Korea Certification Authority Central,
CN=KISA RootCA 1
Validity
Not Before: Aug 24 08:05:46 2005 GMT
Not After : Aug 24 08:05:46 2025 GMT
Subject: C=KR, O=KISA, OU=Korea Certification Authority Central,
CN=KISA RootCA 1
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:bc:04:e4:fa:13:39:f0:34:96:20:6b:6c:68:bb:
fa:db:77:ff:27:f7:ac:ec:2f:e7:fd:f0:7f:6d:6f:
8c:2a:cd:25:09:5b:24:f4:a1:68:fc:28:ec:c9:25:
e2:ac:ed:de:c8:33:84:f5:b0:a5:09:3a:a7:b1:47:
48:c5:cc:4f:8c:79:9c:f9:06:57:7d:dd:ee:38:f6:
cf:14:b2:9c:ea:d3:c0:5d:77:62:f0:47:0d:b9:1a:
40:53:5c:64:70:af:08:5a:c0:f7:cf:75:f9:6c:8d:
64:28:1e:20:fe:b7:1b:19:d3:5a:66:83:72:e2:b0:
9b:bd:d3:25:15:0d:32:6f:64:37:94:85:46:c8:72:
be:77:d5:6e:1f:28:2f:c7:69:ed:e7:83:89:33:58:
d3:de:a0:bf:40:e8:43:50:ee:dc:4d:6b:bc:a5:ea:
a6:c8:61:8e:f5:c3:64:af:06:15:dc:29:8b:3f:75:
8c:bc:71:44:db:fc:ad:b5:17:1d:6d:89:83:cf:c6:
33:bd:bf:45:a2:fe:0a:9f:a3:11:5f:0f:b9:1f:9c:
1a:c2:46:cc:9c:28:66:9f:70:26:3c:2e:df:aa:80:
fe:8c:c5:04:09:25:4f:cd:93:47:3c:37:ea:02:67:
92:fe:fc:22:24:5c:ac:d2:2c:e0:5c:01:33:8a:c1:
19:db

인증서신뢰목록

인증서 신뢰목록 사용 사례 (전자서명인증관리센터)

최상위인증기관 인증서 신뢰목록 - KISA RootCA 1

- 인증서 신뢰목록 버전 : X.509 v1
- 발급일자 : 2009년 8월 14일
- 만료일자 : 2009년 8월 28일
- 신뢰목록 내용

1	행정안전부 최상위인증기관 인증서	DN	CN=Root CA,OU=GPKI,O=Government of Korea,C=KR
		Hash	634C 3B02 30CF 1B78 B456 9FEC F2C0 4A86 52EF EF0E
2	한국정보보호진흥원 최상위인증기관 인증서	DN	CN=CertRSA01,OU=ROOTCA,O=KISA,C=KR
		Hash	F5C2 7CF5 FFF3 029A CF1A 1A4B EC7E E196 4C77 D784
3	행정안전부 최상위인증기관 인증서	DN	CN=GPKIRootCA,OU=GPKI,O=Government of Korea,C=KR
		Hash	4A10 0AC6 C005 0435 A75A 4FDD 96D6 11B7 0734 8BA9

- 인증서 신뢰목록 내려받기 [다운로드]

행정전자서명과의 상호연동을 위해 실제 사용

인증기관 업무연속성 보장을 위한 인증서 신뢰목록 (예시)

인증서 신뢰목록 버전 : X.509 v1
발급일자 : 2031년 8월 14일
만료일자 : 2031년 8월 28일
신뢰목록 내용

1	한국정보보호진흥원 최상위인증기관 인증서 1 2001~2010	DN	CN=CertRSA01,OU=ROOTCA,O=KISA,C=KR
		Hash	634C 3B02 30CF 1B78 B456 9FEC F2C0 4A86 52EF EF0E
2	한국정보보호진흥원 최상위인증기관 인증서 2 2011~2020	DN	CN=CertRSA01,OU=ROOTCA,O=KISA,C=KR
		Hash	F5C2 7CF5 FFF3 029A CF1A 1A4B EC7E E196 4C77 D784
3	한국정보보호진흥원 최상위인증기관 인증서 3 2021~2030	DN	CN=CertRSA01,OU=ROOTCA,O=KISA,C=KR
		Hash	4A10 0AC6 C005 0435 A75A 4FDD 96D6 11B7 0734 8BA9

루트CA의 업무연속성 보장을 위해 제안된 예시

루트CA의 업무연속성을 통한 장기검증

- 루트CA의 업무연속성이 보장되는 경우 과거의 인증서들에 대한 유효성 검증이 항상 가능하고 전자서명 장기검증이 효율적으로 가능함.
- 장점
  - 각 문서별, CRL별 타임스탬프에 의존할 필요 없음
  - TSA에 대한 신뢰보다 루트CA에 대한 신뢰에 의존하는 검증방법

5. 맺음말

- 전자기록물의 각종 보안요구사항은 암호기술을 이용하여 구현
- 전자서명 장기검증 효율화 방안
  - 인증기관의 인증서에 대한 업무연속성이 보장된다면 전자서명 장기검증이 효율적으로 가능함
- 루트CA의 업무연속성 제공 방안
  - 루트CA의 인증서가 갱신될때마다 과거 인증서에 대한 신뢰목록을 발행
  - 신뢰목록에 근거하여 과거 인증서들의 유효성을 자동 검증
  - 루트인증기관 차원에서의 장기검증에 대한 대응책
- 정보화 시대의 전자기록문화 발전을 선도하는 대한민국

감사합니다

Q & A