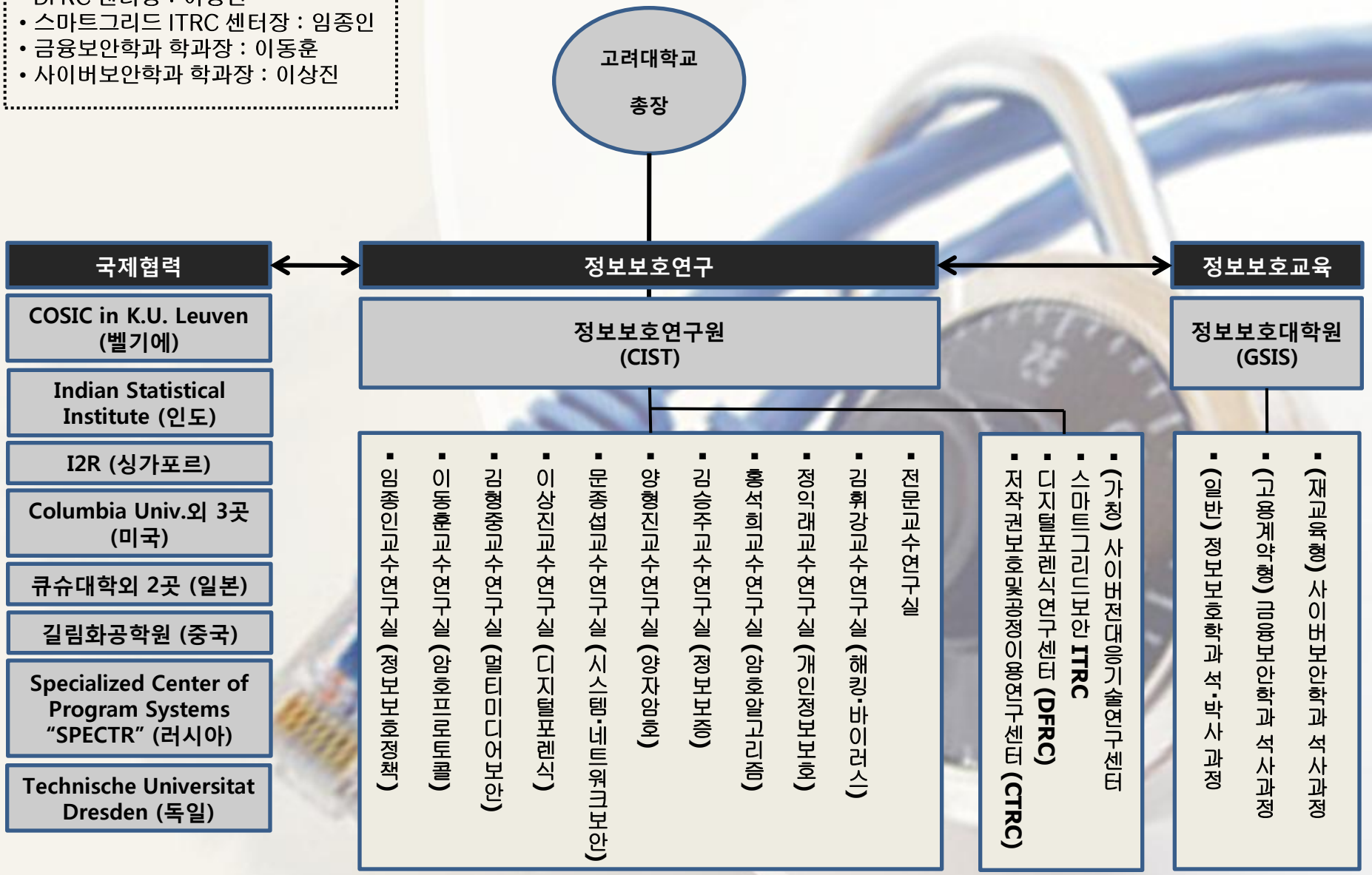
최근 금융보안 문제의 해결방향 및 정책 제언

김 승 주
고려대학교 정보보호대학원
skim71@korea.ac.kr
Twitter : skim71
Facebook : fb.com/skim71

고려대학교 정보보호대학원

- CIST 및 GSIS 원장 : 임종인
- CIST 및 GSIS 부원장 : 이동훈
- CTRC 센터장 : 이동훈
- DFRC 센터장 : 이상진
- 스마트그리드 ITRC 센터장 : 임종인
- 금융보안학과 학과장 : 이동훈
- 사이버보안학과 학과장 : 이상진



정보보증연구실 @ CIST

Information Assurance & Security Lab

www.kimlab.net

김승주 부교수 (skim71@korea.ac.kr)

미래융합기술관 606호

연구분야

- Security Engineering (= Security + S/W Engineering)
- Cryptographic and Security Design, Implementing and Testing (CMVP, CC, ISMS etc.)
- Usable Security (making computer security not just secure, but also practically usable)

주요 경력 :

1999.2) 성균관대학교 공학박사
1998.12~2004.2) KISA 암호기술팀장 및 CC평가1팀장
2004.3~2011.2) 성균관대학교 정보통신공학부 부교수
前) 정보통신부 위촉 IT 국제표준화 전문가
前) 행정자치부 위촉 전자정부서비스보안위원회 위원
前) 교육인적자원부 유해정보차단 자문위원
現) 한국정보보호학회 이사
現) 대검찰청 디지털수사 자문위원
現) 방통위 정보통신망침해사고 민관합동조사단 위원
現) 한국은행 금융정보화추진분과위원회 자문위원

- Convertible group signatures (AsiaCrypt'96)
- Proxy signatures, revisited (ICICS'97): 400회이상 인용
- '05 : 정보통신부 RFID/USN연구논문공모전 우수상
- '06 : 국가정보원 암호학술논문공모전 우수상
- '07 : 국가정보원장 국가사이버안전업무 유공자 표창
- '07 : Marquis Who's Who in the World ('07~'08) 등재

주요 연구성과

'숫자 6개' 암호는 2초~'영어+숫자' 는 10초면 해킹

뻥뻥 뚫리는 토종 메신저

성균관대 연구팀 분석

"MSN보다 보안 떨어져"

Messenger

메신저 패스워드 파악에 걸리는 시간

중앙일보 경제1면
(2006.11.9.)

인터넷서 나도는 해킹프로그램만 있으면

증권 '사이버 거래망' 뚫는다

성균관대 연구소 직접 실험

28개 증권사 중 11곳

ID·비밀번호 등 유출

중앙일보 3면
(2007.7.5.)

"보안USB에 심각한 결함"

비밀번호 쉽게 노출…패치 꼭 해야

전자신문 10면
(2007.6.19.)

금융보안의 현황

미국 인터넷뱅킹 현황

〈표3〉 미국 주요은행 개인용 인터넷뱅킹 자금이체 서비스 현황

은행명	자행		타행	
	본인계좌	타인계좌	본인계좌	타인계좌
Bank of America	○	○	○	○
JPMorgan Chase Bank	○	○	○	○
Wells Fargo Bank	○	○	일부지역	
Citibank	○	○	○	○
PNC Bank	○	○	○	
U.S. Bank	○	○		
Suntrust Bank	○			
Citizens Bank	○	○	○	
Capital One	○		○	
Regions Bank	○			

(출처 : 미국·일본 인터넷뱅킹 현황 및 시사점, 금융결제원)

미국 인터넷뱅킹 현황

〈표4〉 미국 주요은행 개인용 인터넷뱅킹 자금이체 수수료 현황*

(단위 : 달러)

은행명	자행이체	타행이체		
		ACH Standard	ACH NextDay	Wire
Bank of America	무료	3.00	10.00	25.00 내외
JPMorgan Chase Bank	무료	3.00	—	20.00
Wells Fargo Bank	무료	무료	—	—
Citibank	무료	무료	무료	18.75
PNC Bank	무료	무료	—	
U.S. Bank	무료	—	—	—
Suntrust Bank	무료	—	—	—
Citizens Bank	무료	3.00	—	—
Capital One	무료	무료	—	—
Regions Bank	무료	—	—	—

* 송금 기준

(출처 : 미국·일본 인터넷뱅킹 현황 및 시사점, 금융결제원)

보안에 대한 접근방법의 차이

- 우리나라
  - 특정 보안리스크에 대한 보안대책을 직접 규율
- 미국, 일본
  - 은행이 인터넷뱅킹과 관련된 리스크를 직접 평가하고 적절한 보안대책을 채택

보안에 대한 접근방법의 차이

- 우리나라
  - 장점 : 어떤 은행을 이용하는가에 상관없이 최소한의 보안수준을 확보할 수 있음
  - 단점 : 은행의 능동적 보안대책 시도 부족 및 보안기술간 경쟁 저하
- 미국, 일본
  - 장점 : 은행이 보안문제에 대해 좀 더 적극적으로 개입하도록 유도할 수 있음
  - 단점 : 인터넷뱅킹 발전이 우리나라에 비해 상대적으로 더딤

해결방향 및 정책 제언

정책 제언

- 포렌식준비제도의 도입
- 보안성평가제도(CC)의 일원화
- OTP+서명(인증서) 기술 개발
- 독자 암호기술의 사용 타당성 검토

포렌식준비제도의 도입

개인정보 유출로 인한 손해배상 소송 결과

기업	사건 내용	법원 판결
엔씨소프트	게임 '리니지2' 이용자 수십만명의 개인정보 유출	32명에게 10만원씩 배상
옥션	1800만여명의 정보 유출. 14만명 소송	배상책임 인정 안함, 항소심 진행 중
다음	메일 서비스 장애로 e메일 내용 유출. 70명 소송	배상책임 인정 안함
GS칼텍스	직원이 1150만여명의 정보 유출. 2만8000명 소송	배상책임 인정 안함
SK브로드밴드	초고속 인터넷 고객 600만명 정보 유출. 2만여명 소송	소송 진행 중

(출처 : 경향신문)

포렌식준비제도의 도입

- 허니넷(Honeynet) 프로젝트의 연구결과에 따르면, 해킹에 30분정도 소요될 때 이에 대한 증거를 수집하고 원인을 밝히는데 수사관 1명당 34시간 정도가 소요됨

- 증거수집(Forensic)과 복구(Recovery)는 서로 반비례하기 때문에, 농협사태의 경우와 같이 신속한 복구가 필요한 경우에는 증거수집 및 분석에 더욱 많은 시간이 필요

포렌식준비제도의 도입

- 보안은 업체가 자발적으로 최선을 다하도록 유도하고, 책임규명설비 구축을 의무화해 문제 발생시 피해보상을 확실히 하는 것이 중요!
  - 영국의 경우 포렌식준비(Forensic Readiness) 제도를 공공기관에 의무화

보안성평가제도(CC)의 일원화

- '96년 '정보화촉진기본법' 제정을 계기로 우리 정부는 '98년 2월부터 업체에서 개발한 IT제품에 내장된 보안기능의 안전성과 신뢰성을 국가차원에서 검사하고 보증해 주기 시작

- '02년에 이르러 정부는 세계적인 수준의 안전성을 갖는 보안제품이 국내시장에 보급될 수 있도록 전격적으로 CC(Common Criteria)라는 국제표준을 도입

보안성평가제도(CC)의 일원화

- 하지만 제품 평가에 과거보다 엄격한 잣대를 적용하다보니 이는 곧 평가기간의 장기화와 평가적체를 야기하게 되었고, 이에 우리 정부는 여론의 악화를 우려하여 '07년 3월부터 평가·인증 제도를 국내용과 국제용(해외수출용)으로 이원화

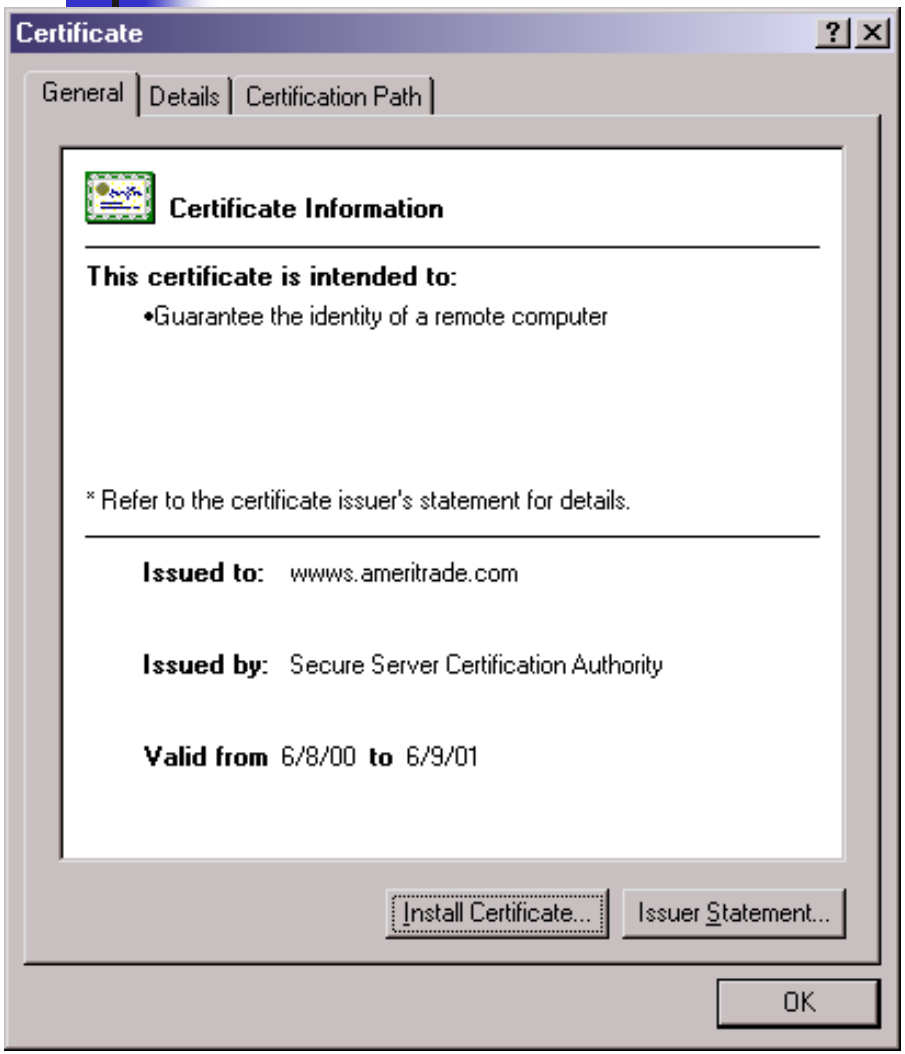
- 국내에서 타고 다니는 내수용 자동차의 안전수준과 수출용 자동차의 안전수준이 다르다면, 그것도 수출용 자동차의 안전수준이 더 높다면 과연 누가 납득할 수 있을까?

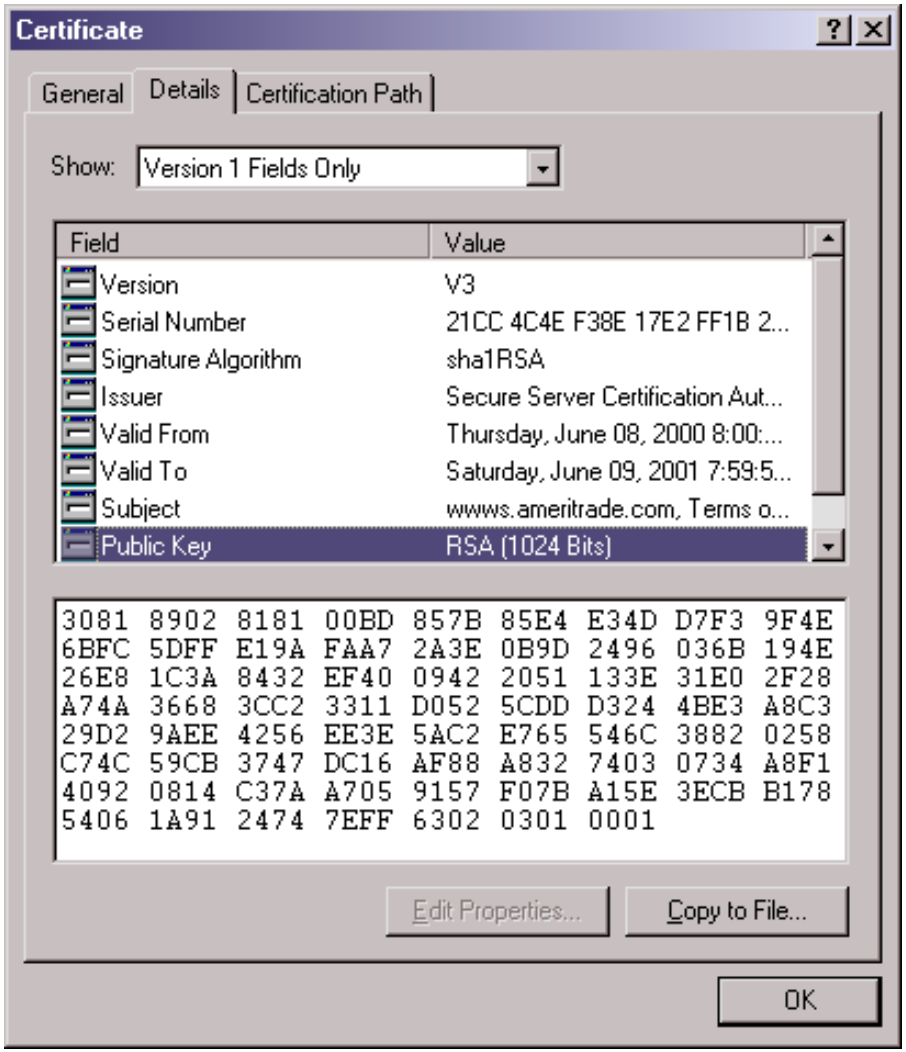
OTP+서명(인증서) 기술 개발

OTP+서명(인증서) 기술 개발

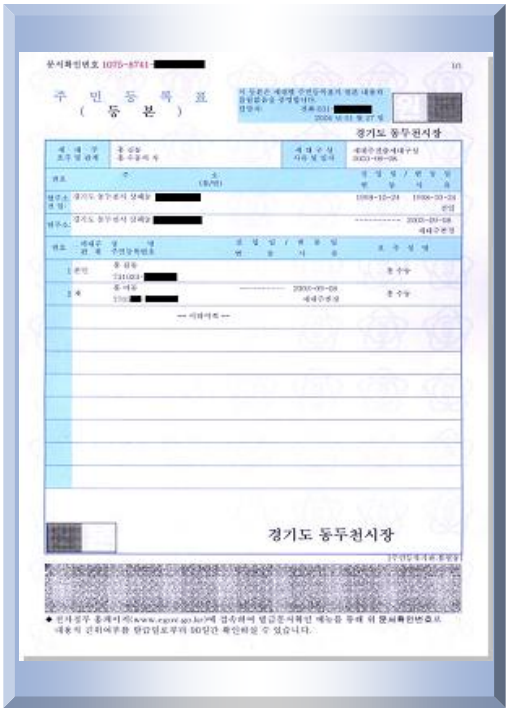
	Digital Signature (X)	Digital Signature (O)
개념		13598293948977765839 19293933923939239239 49294959935939993953 99943049384550490594 49395234898434857558
문제점	재사용 가능	

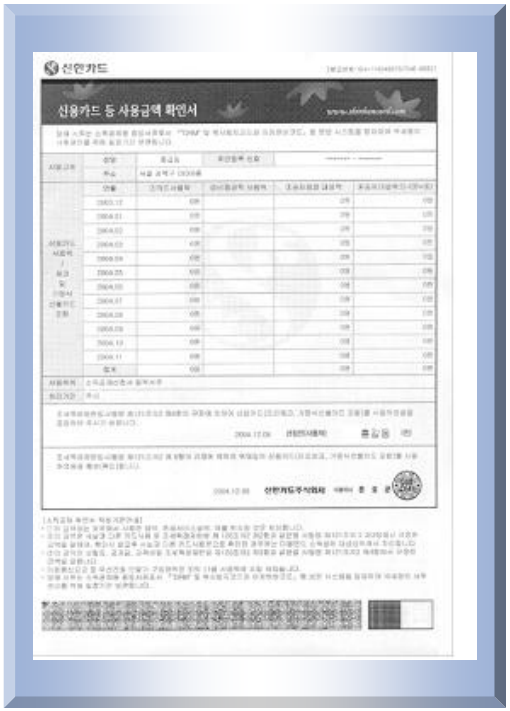
OTP+서명(인증서) 기술 개발

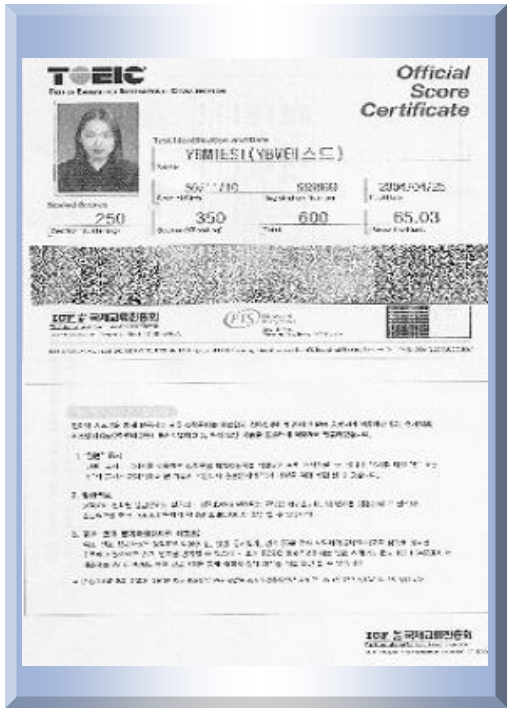




OTP+서명(인증서) 기술 개발





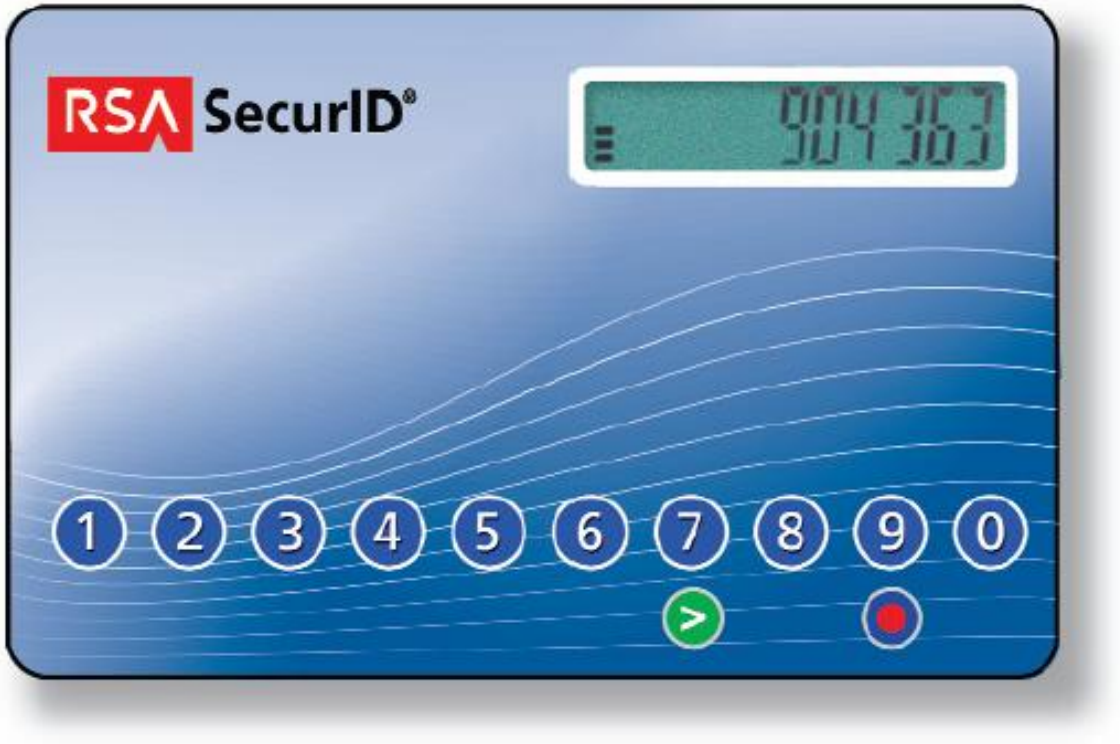


OTP+서명(인증서) 기술 개발

- 본질적으로, OTP의 안전성 < 서명(인증서)의 안전성

- 오프라인 은행업무에서도 매 거래내역마다 거래자 서명 또는 날인을 받고 있으며, 인감의 위조 및 도용이 잦다고 인감을 폐지하지는 않음

OTP+서명(인증서) 기술 개발



RSA SecurID SID900 Transaction Signing Authenticator.
The PIN pad enables implementation of the digital signing function.

OTP+서명(인증서) 기술 개발

뢰성 있는
활용 방안

IT언론의 새로운 대안
디지털데일리

기획 칼럼 포토·동영상 IT문서자료실 딜라이트닷넷 PLAY

방송 | e비즈·솔루션 | 보안 | 금융IT | 콘텐츠 | 기업문화 | 산업 | 국제

Home > 뉴스>보안 > 법제도/정책

자금신청하면 요금할인 20%

서버호스팅, DDOS 업계 최저가 보장
상담전화 02-594-2090
24시간 고객지원센터 1688-2091

OTP로도 전자금융거래 부인방지...공인인증서 대체

금융보안연구원 OTP통합인증센터, 최근 개발 완료... 공인인증서 대체 논의 급물살

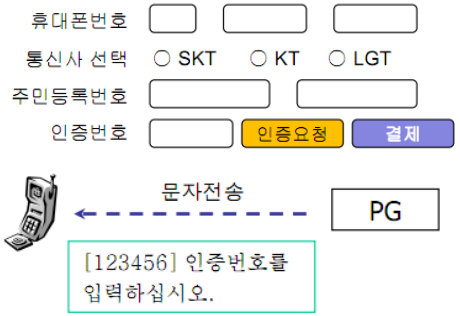
2010년 06월 24일 22:55:59 / 이유지 기자 yjlee@ddaily.co.kr

관련기사
↳하반기부터 전자금융거래 공인인증서 의무화 폐지

- 금융보안연구원, OTP통합인증센터 활용한 거래연동 OTP 부인방지 서비스 개발… '공인인증서와 동등한 수준의 인증방법' 최초 제시

[디지털데일리 이유지기자] 올 하반기부터 전자금융거래에서 공인인증서 말고도 다른 인증방법이 허용되는 가운데, 일회용비밀번호(OTP) 기술로 부인방지 기능을 제공하는 인증기술이 처음 개발돼 주목된다.

[참고] 기타 소액결제기술

구 분	Ring2Pay	SMS Payment
결제 요청 및 승인 방식	휴대폰번호: 010 - -  ARS 음성멘트 "OO마켓 십오만원 결제를 위해 결제 확인 비밀번호를 입력해 주세요"	
이용한도	통장잔액 최대: 1회/1일 200만원, 월 500만원	휴대폰요금 최대: 월 20만원 (이통사가 수납대행)
가 맹 점	낮은 수수료 / 짧은 정산 주기 실물, 온/오프라인	높은 수수료 / 긴 정산주기 주로 디지털 컨텐츠, 오프라인 불가
고 객	회원가입 후 이용 포인트 적립 등 각종 혜택	누구나 이용가능 하나, 회원혜택 불가
비 고	뛰어난 범용성 / 안전성 / 수익성 새로운 형태의 카드사 운영	일부 결제 환경에만 적합 휴대폰 소액결제 대행업

[참고] 기타 소액결제기술

구 분	I 사 방식 (SMS)	L 사 방식 (SMS)	Ring2Pay 방식
이용 방법	회원가입 → 결제정보 등록 → ID/Password 인증 → 결제 정보 조회 → 결제 인증	회원가입 → 결제정보 등록 → ID/Password 인증 → 결제 정보 조회 → 결제 인증	회원가입 → 결제정보 등록 → 핸드폰 번호 입력 → 결제 인증
결제 인증방식	ID/Password 회원 인증 후 → SMS 결제 인증	ID/Password 회원 인증 후 → SMS 결제 인증	Ring2Pay 방식 (SMS 사용 안함)
회원 관리	가맹점별 별도 회원관리 (통합 회원 관리 X, 비회원 X)	통합 회원 관리 (비회원 X)	통합 회원 관리 (비회원 가능)
지향 모델	한국형 PayPal 간편결제	통합 결제 플랫폼	컨버전스형 휴대폰 결제
서비스 형태	회원 로그인을 통한 PG 주도형 모델	회원 로그인을 통한 PG 주도형 모델 (카드사별 선택창 가능)	카드사 공통형 모델 (카드 선택 후 결제 방식 선택)
제휴 금융사	1곳 진행중	4곳 진행중	1곳 진행중
비 고	국내 특화된 SMS 기반의 간편결제	국내 특화된 SMS 기반의 간편결제	Ring2Pay 기술 기반의 글로벌 간편결제

독자 암호기술의 사용?

- ’48년 12월 육군이 창설되면서 육군본부 직할부대에 전파감시소를 설치하고 미군의 도움을 받아 암호를 제작하여 전군에 배포

- ’61년 암호 제작업무를 중앙정보부로 이관. 이때부터 중앙정보부는 각급 행정부처 및 해외공관에 암호자재를 제작 배포

독자 암호기술의 사용?

- '97년 한국 국가기관용 표준암호 NEAT 제정
  - NEAT : National Encryption AlgoriThm
- '99년 한국 민간용 표준암호 SEED 제정
  - SEED : 정보보호의 씨앗이 되라는 뜻
- '04년 12월 대국민행정업무용 표준 암호 ARIA 제정
  - ARIA : Academy – Research Institute - Agency

독자 암호기술의 사용?

한국	민 간	SEED
	대국민 행정업무	ARIA
	공공 (금융)	NEAT (BUD-F)
미국	Confidential	SKIPJACK
	SBU	3DES, AES

독자 암호기술의 사용?

누가 사용하는가?

한국	민 간	SEED
	대국민 행정업무	ARIA
	공공 (금융)	NEAT (BUD-F)
미국	Confidential	SKIPJACK
	SBU	3DES, AES

무엇을 보호하는가?

독자 암호기술의 사용?

- SEED(한국)와 3DES, AES(미국)은 모두 자국내 표준이자 ISO/IEC 및 IETF 국제표준
  - SEED, 3DES, AES 모두 해독된 사례 없음
- 그러나, SEED의 세계 보급율 < 3DES와 AES의 세계 보급율
- 독자 암호기술의 사용시 장·단점 모두 존재!

Q & A