전자상거래 인증서 보안 요구사항 연구

송 유진 *김 선호

동국대학교 정보산업학과
*동국대학교 전자상거래 연구소

1999. 11.

목 차

연구의 배경 및 필요성

- 전자상거래에서 인증기술은 인터넷 등 개방형 네트워크 상에서 안전한 상거래를 보장해 주는 필수적인 보안 수단으로 인식되고 있음
- 선진 각국은 안전한 공개키 기반구조 확립을 위해 거래 당사자 및 거래 문서를 인증해 주는 인증시스템 구축이 활발히 진행되고 있음
- 효율적으로 전자상거래 인증을 제공해 줄 수 있는 인증 시스템 기능 분석 및 인증서 활용분야별 보안 요구사항 정립에 대한 연구가 필요함

인증서비스의 기능

? 인증서비스 목표를 달성하기 위해 전자상거래에 적용되는 인증 기능은 일반적으로 다음과 같이 구분

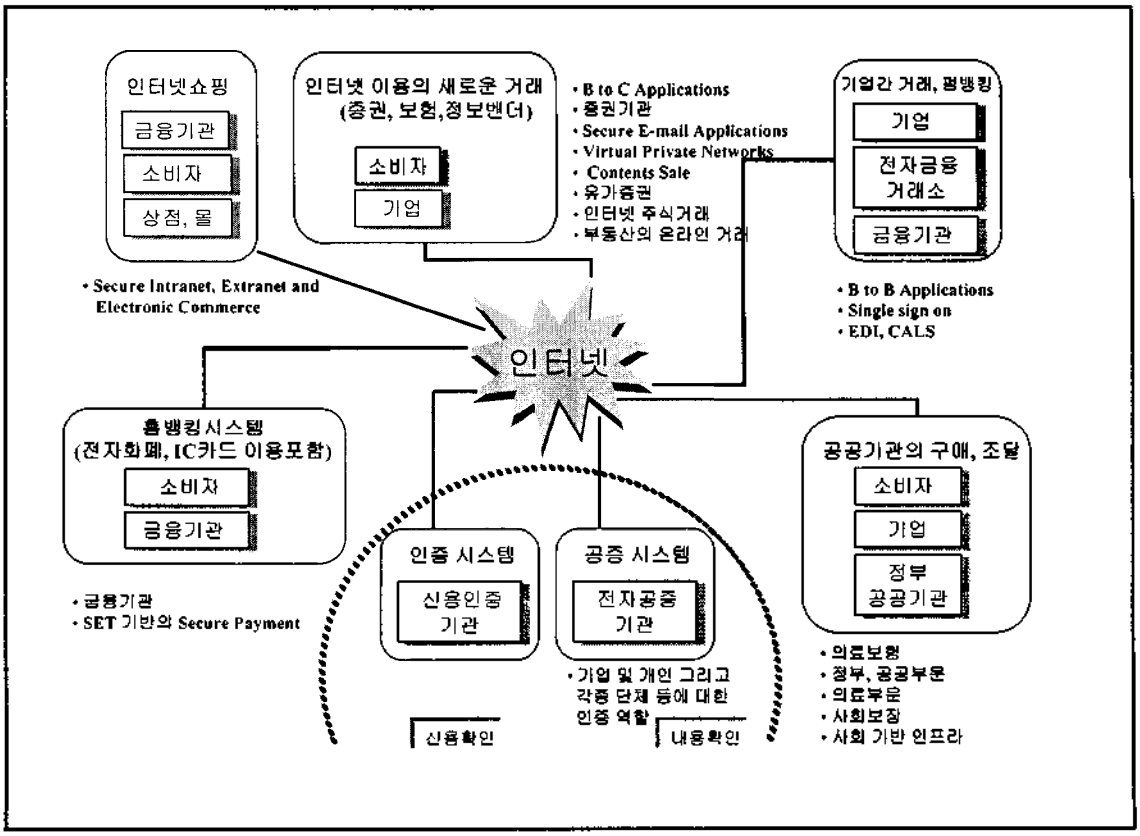
? 본인확인 기능: 상대방의 본인성을 확인
? 내용확인 기능: 거래내용, 일시 등을 확인
? 신용확인 기능: 거래상대의 신용능력을 확인

인증서 활용분야 분석

? 활용분야를 분석하기 위해 전자상거래 비즈니스 모델을 구성하고 이를 근거로 인증서의 활용업무를 분류 함

? 비즈니스 모델은 각각의 거래주체별로 나타낼 수 있음

? 각각의 거래주체를 인증하기 위한 인증기관이 존재



영역별 분류	거래별 분류	활용분야별 분류	업무별 분류
일반	B to B B to C B to G C to G G to G	공공 부문	납세를 위한 소득신고 제출, 사회보장에 대한 문의와 답변, 사회기반 인프라, 정부간 문서유통, 기업의 재무상태 보고서제출, 우체국의 전자적 소인, 전자적 등기, 사망증명서, 선거인명부등록, 각종 증명서 발행, 정부 조달 문서, 각종 인허가 등
		민간 부문	인터넷 서비스나 자료접근, 인터랙티브 TV, 소프트웨어 안전성 보장, Media Distribution, EDI, CALS, Security Intranet, Extranet & Electronic Commerce, Desktop Security, 전자뱅킹, 전자지불, 전자상점, 디지털 신문구독, Certificate를 이용한 Password의 감소, 디지털 신문구독, 기업의 웹 사이트 접근제어, Online Transaction
		금융 부문	홈뱅킹, 대출·저당 절차, 은행·증권·부동산의 온라인 거래, 부동산 등기부등본 인증, 유가증권, 상품·중개인 면허, 인터넷 주식거래, 온라인 자산매매를 위한 인증서 발행 등
		의료 부문	환자기록에의 접근, 치료계획의 치료인가와 수행된 서비스에 대한 확인, 원격진료·처방 권한, 자격증, 분산된 전문의 협력 작업, 정부와 연계된 의료보험증에 대한 인증 등
		응용 부문	PGP, PEM, S/MIME, VPNs, Internet Telephony, Applet Authentication, 전자지불 프로토콜, 전자수표 등

인증서 등급 분류

- Verisign의 분류를 참고로 하여 전자상거래 분야에 인증서를 응용하기 위한 특성에 따라 인증서 등급분류 기준을 제시

? 세부 분류기준은 주체, 신용도(본인확인), 용도, 확장 영역의 critical 적용, 결제여부, 거래별 요소를 근거로 분류

인증서 등급 분류기준 및 속성

요소 \ 등급	CLASS 1	CLASS 2	CLASS 3
주체	개인	개인	개인, 단체
신용도 (본인확인)	이름+전자우편	class 1 + 신청정보+현주소	class 1 + class 2 + 직접 출두하여 관련 서류 검사
용도	비 상업용	상업용	상업용
확장영역의 critical 적용	No가 대부분	Opt부분 증가	Yes부분 있음
결제여부	결제 없음	소액결제	고액결제
거래별	B to C	B to C	B to C B to B B to G

CLASS 별 인증서 활용분야

등급	활용분야
CLASS 1	인터넷 서비스 · 자료 접근, 인터랙티브 TV, 개인간의 전자메일, 인터넷을 통한 설문조사 등
CLASS 2	전자적 등기 메일, 사회기반 인프라, 전자인 정부 등록, 각종 증명서 발행, 정부조달 문서 · 견적서, 소프트웨어의 안전성보장, Media Distribution, Security Intranet, Extranet, Desktop Security, Certificate를 이용한 Password의 감소, 디지털 신문구독, 전자상점, 환자기록에의 접근, 분산된 전문의 협력 작업, 치료계획의 치료인가와 수행된 서비스에 대한 확인, , 정부와 연계된 의료보험증에 대한 인증, 기업의 재무상태 보고서 제출, 우체국의 전자적 소인, 사망증명서, 납세를 위한 소득신고 제출, PGP, PEM, S/MIME, VPNs, Online Transaction, Internet Telephony, Applet Authentication, 전자지불 프로토콜 등
CLASS 3	각종 인허가, 대금 · 지당 결차, 부동산 등기부등본 인증, 상품 · 중개인 면허, 온라인 자산매매를 위한 증명서 인증, 의료부분의 자격증 인증, 원격치료 · 처방 권한, 전자수표, 정부간 문서유통, Electronic Commerce, 전자뱅킹, 전자지불, EDI, CALS, 인터넷 주식거래, 은행 · 증권 · 부동산의 온라인 거래, 기업의 웹사이트 접근제어, 홈뱅킹, , 유가증권 거래 등

등급별 인증서 형식화

- X.509 표준과 비교해서 현재 서비스되고 있는 인증서의 경우, 예를 들어 Verisign, Initek, JMI 등의 인증서 확장영역의 critical여부는 다음 표와 같이 설정

인증서 확장영역의 critical 설정

분야	확장자 이름	critical				
		본과제	X.509 V3 표준	Verisign	Initek	JMI
Key and policy information	authorityKeyIdentifier	Yes	No		No	Yes
	subjectKeyIdentifier	Yes	No		No	Yes
	keyUsage	Yes	Opt	Yes	Opt	Yes
	privateKeyUsagePeriod	Opt	Opt		No	
	certificatePolicies	Opt	Opt	Yes	Opt	
	policyMappings	Opt	No		No	
Subject and Issuer attributes	subjectAltName	Opt	Opt		Opt	
	issuerAltName	Opt	Opt		Opt	
	subjectDirectoryAttribute	Opt	Opt		No	
Certification path constraints	basicConstraints	Yes	Yes	Yes	Opt	Yes
	nameConstraints	Opt	Yes		Opt	
	policyConstraints	Opt	Yes		Opt	

등급별 인증서 형식화(계속)

? 본 연구에서는 인증서 등급분류 기준 등을 근거로 다음 표와 같은 확장필드의 적용을 권고 함

? ●는 각각의 등급별로 확장필드를 적용하는 지의 유무(critical이 Yes인지 No인지를 구분)를 나타내는 것 임

? 앞에서 적용한 critical과 인증서의 등급분류 기준에 의해서 등급별 인증서에 적용 가능한 확장필드를 분류한 것 임

분야	확장자 이름 / 세부항목	CLASS 1	CLASS 2	CLASS 3	특 수
Key and policy information	authorityKeyIdentifier	●	●	●	●
	Key Identifier				●
	Authority Cert Issuer		●	●	●
	AuthorityCert Serial Number	●	●	●	●
	subjectKeyIdentifier	●	●	●	●
	keyUsage	●	●	●	●
	Degital Signature		●	●	●
	Non Repudiation	●	●	●	●
	Key Encipherment				●
	Date Encipherment			●	●
	Key Agreement				
	Key Cert Sign	●	●	●	●
	CRL Sign	●	●	●	●
	privateKeyUsagePeriod				●
	certificatePolicies			●	●
	Policy Identifier			●	●
	Policy Qualifiers			●	●
	policyMappings				

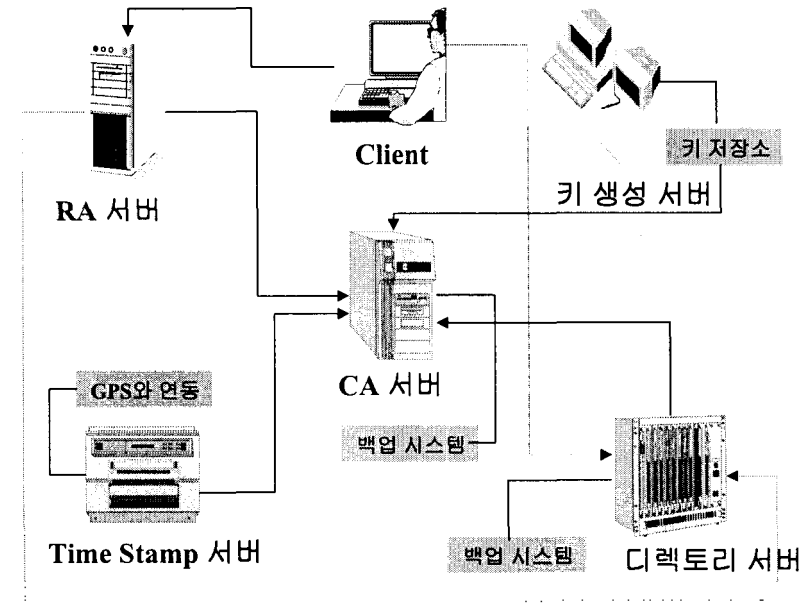
분야	확장자 이름 / 세부항목	CLASS 1	CLASS 2	CLASS 3	특 수
Subject and Issuer attributes	subjectAltName				●
	Other Name			●	●
	Rfc822Name			●	●
	DNS Name			●	●
	X400Address				
	Directory Name				
	Edi party Name				
	Uniform Resource Identifier				
	IP Address			●	●
	Registered ID				
	IssuerAltName	●	●	●	●
	subjectDirectoryAttribute				

분야	확장자 이름 / 세부항목	CLASS 1	CLASS 2	CLASS 3	특 수
Certification path constraints	basicConstraints	●	●	●	●
	CA	●	●	●	●
	PathLenConstraint				
	nameConstraints				
	policyConstraints				

인증서 등급별 보안 요구사항 분석

? 인증서 및 CRL 생성/관리
? 인증서 등록
? 키 관리
? 디렉토리 정보관리
• Time Stamp 기능

인증 시스템의 구성



인증서 및 CRL 생성/관리 보안 요구사항

인증서 생성 관리

구분	CLASS 1	CLASS 2	CLASS 3
작성	인증서버 관리자와 인증서 발급자의 업무를 명확히 할 것	오프라인으로 생성하는 경우에는 심사 처리를 분리함과 동시에 권한을 갖은 자 이외에는 액세스할 수 없는 시스템으로 만들 것	좌동
송부		인증서 송부에 스마트카드에 저장하여 송부하는 방식과 같은 보안 수단을 마련할 것	원본 내용과 함께 수신자 확인이 가능한 수단을 선택할 것
등록 / 보관		인증서의 등록 . 보관에 있어서 부정 액세스를 방지하기 위해 액세스 관리를 할 것	원본 내용과 함께 재해 또는 소실에 대비해서 백업을 받아둘 것
공개		* 인증서의 공개에 대해 정책적으로 명확히 할 것 * 공개할 경우는 공개대상, 공개방법, 공개기간에 대하여 명확히 할 것	좌동
보존		발행한 인증서의 유효기간이 끝난 후에도 변경, 소거, 누설 등에 대한 보호를 하여 일정기간동안 보존할 것	좌동

인증서 및 CRL 생성/관리 보안 요구사항

CRL 생성 관리

구분	CLASS 1	CLASS 2	CLASS 3
CRL 생성	CRL 생성 및 서명에 대해서는 인증서 발행과 동등한 수준의 보안관리를 할 것	CRL 발행은 효력상실 발생 유무에 관계없이 정기적으로 할 것. 또 발행 사이클을 이용자에게 명확히 할 것	좌동
CRL 보관		CRL에 대한 부정 액세스에 의한 변경, 소거, 누설 등에 대한 보호를 할 것	원본 내용과 더불어, 재해 또는 소실에 대비해 백업을 받아둘 것
CRL 게시		CRL 또는 인증서의 최신 상태는 CRL 등에 의해서 정당한 이용자가 문의할 수 있도록 할 것	좌동
CRL 보존		CRL은 당초의 유효기간 경과 후 에도 일정기간 동안 CRL 및 관련 데이터를 보존할 것	좌동

인증서 등록 보안 요구사항

신규 발행시 심사

구분	CLASS 1	CLASS 2	CLASS 3
본인확인 및 정보의 사실성 확인	신청된 정보가 신뢰할 수 있는 기관, 조직 또는 사람에 의한 증명 또는 확인을 타인정보와 일치하는지의 여부를 조사할 것	* 심사결과 등보를 신청시의 수단과는 별도의 방법으로 하는 등 본인확인의 신뢰성을 더욱 강화 * 온라인 신청이외의 경우에는 심사처리를 복수가 분담 할 것	본인출두에 의한 확인할 것
신청 수리와 의사확인	온라인을 통한 신청확인을 할 것	인증 신청을 수리했음을 신청자에게 회답과 동시에 신청의사를 확인할 것	좌동
유일성 확인	신청자의 이름이 해당 인증기관에서 중복이 없고 유일함을 확인할 것	신청자의 공개키가 해당 인증기관에서 중복되지 않음을 확인할 것	인증서에 포함된 서명키에 대응하는 공개키의 소유여부를 확인할 것
심사 정보의 등록	신청정보 및 심사 정보를 등록할 것	좌동	신청시 효력상실 등의 사고에 대한 대처에 관한 정보를 등록할 것
심사 결과의 통지		통지 또는 문의에 대한 회답 등에 의해 신청자에게 통지할 것	좌동

인증서 등록 보안 요구사항

정기 갱신시 심사

구분	CLASS 1	CLASS 2	CLASS 3
인증서 정기 갱신시의 심사	* 신규발행시의 심사와 동일 * 단 본인인증 의사확인은 신규발행시와 다른 수단을 취할 수 있음	좌동	좌동

인증서 등록 및 변경 요구사항

효력상실 심사

구분	CLASS 1	CLASS 2	CLASS 3
신청자 확인	비밀키의 훼손시에는 신속히 본인 확인을 할 것	* 비밀키의 소실, 중요정보 갱신의 경우는 신규발행시와 동일 * 인증서의 잘못이나 부정사용의 감지, 본인에 의한 신청이 곤란한 사유 발생, 또는 인증서의 부정발행등의 경우는 등록기관이나 인증기관 또는 사전에 등록되어있는 기관 등이 본인을 대신해서 신청이 가능 * 온라인 신청이외의 경우는 심사 처리를 복수의 사람이 분담 할 것	좌동
효력 상실 정보의 등록	효력상실 리스트 생성을 위한 신청정보, 심사정보를 등록할 것	좌동	좌동
효력 상실 심사 결과의 통지		통지 또는 문의에 대한 회답 등에 의해 신청자에게 통지할 것	좌동

인증서 등록 및 변경 요구사항

효력 상실 후 재발행 심사

구분	CLASS 1	CLASS 2	CLASS 3
효력상실 후 재발행 심사	* 공개키나 중요정보의 갱신에 의한 효력상실후의 인증서 재발행에 대해서는 신규발행시와 동등한 처리할 할 것 * 본인이외의 효력상실 신청에 근거하여 효력상실후의 인증서 재발행에 대해서는 신규발행과 동등한 처리를 할 것	좌동	좌동

키 관리 보안 요구사항

구분	CLASS 1	CLASS 2	CLASS 3
생성	공개키의 생성은 신뢰할 수 있는 암호키 생성 시스템을 사용한다	공개키의 생성은 신뢰할 수 있는 암호키 생성 시스템을 사용하여 복수인 관리의 아래 행한다	* 암호키 생성 시스템의 기능은 암호키 관리 모듈의 내부에 장착되어 있을 것 * 키 생성이 복수인 관리체제로 이루어지는 경우, 구성원은 다른 조직에 대해 권한을 갖는 사람으로 구성해야 한다
보관	암호키 생성 시스템에 의해 생성된 키는 암호화해서 보관할 것	* 복수의 키구성요소에 지식분산함으로써 단독으로는 키에 관한 비밀정보를 일체 알지 못하도록 보관하거나 또는 암호키 관리 모듈에 보관할 것 * 복수의 키구성 요소에 지식분산할 경우, 각 구성요소는 권한을 갖는 자가 개별적으로 보관할 것 * 암호키 관리 모듈내에서 보관하는 경우는 복수인의 권한을 갖는 자가 갖추어지지 않으면 암호키 관리 모듈을 외부로 가지고 나갈 수 없는 등 복수인 관리하에서 보관할 것	* 키 보관은 암호키 관리 모듈내에 둘 것 * 암호키 관리 모듈 관리는 다른 조직의 임원에 의한 복수인 관리체제로 할 것

키 관리 보안 요구사항

구분	CLASS 1	CLASS 3	CLASS 3
이용		* 이용할 때에는 암호키 관리 모듈 내에서 사용할 것 * 암호키 관리 모듈을 이용 또는 정지하는 경우등의 조작은 복수인관리하에서 할 것	* 원칙에 표기된 복수인 관리의 구성원은 다른 조직으로 구성되어 있을 것 * 암호키 관리 모듈을 포함하는 시스템은 스탠드 얼론으로 운용할 것
비업		* 비밀키나 공개키는 백업해 둘 것 * 백업은 보관과 동등한 수준 이상의 보안을 확보할 것	원칙의 내용과 함께 키 이용장소와 떨어진 장소에 백업할 것
보존	* 유효기간이 종료된 후 에도 필요한 것은 보존 기간을 정하여 보존할 것 * 인증기관의 공개키는 유효기간 후에도 가능성을 확보하기 위해 개조되지 않도록 보존할 것	원칙의 내용과 함께 유효기간이 종료된 비밀키나 공통키등, 유효기간 후 에도 필요한 것은 복수인 관리나 지식분산하에서 보존할 것	좌동
폐기	유효기간이 종료된 인증기관의 디지털 서명용 비밀키나 보존 기간이 종료된 키 등은 폐기할 것	원칙 내용과 함께 폐기할 때에는 복수인 관리하에서 비밀정보의 일부라도 노출되지 않도록 할 것	좌동
정기갱신	미리 유효기간을 설정하여 정기적으로 갱신할 것	좌동	좌동

키 관리 보안 요구사항

구분	CLASS 1	CLASS 2	CLASS 3
키의 훼손/재해시의 복구	* 비밀키의 훼손 또는 재해 등의 사태에 대비해 대책을 사전에 마련해 둘 것 * 비밀키가 훼손 또는 그럴 가능성이 있는 경우 인증기관은 신속히 대응하여 인증서의 효력을 상실시킬 것	* 왼쪽 내용과 함께 비밀키가 훼손당한 경우 그 비밀키로 서명한 가입자의 인증서에 대한 효력을 상실시키고 그것을 가입자에게 통보하여 아래와 같은 대응을 할 것 - 신청자로부터의 인증요구를 고려하기 위한 개시 - 이용자가 인증기관의 상황을 확인할 수 있는 창구 설치 *인증기관이 비밀키의 훼손 또는 재해의 사태에서 복구할 때는 아래와 같이 대응할 것 - 안전한 환경인지 확인 - 인증기관의 키와 인증서 갱신 - 가입자의 인증서 재발행 수속	* 왼쪽 내용과 함께 인증기관의 비밀키가 훼손되어있지 않는가를 확인하기 위해서 인증서의 이용상황에 대해 샘플링등의 방법으로 모니터링할 것 * 가입자에 대한 인증서 재발행에 관해서는 자동발행이 아니라 가입자측의 요구에 따를 것

키 관리 보안 요구사항

CA 공개키	* 인증기관은 생성한 키페어의 공개키에 대해 상위 인증기관이 존재할 경우는 그곳에서 인증서를 취득할. 상위 인증기관이 존재하지 않는 경우는 스스로의 비밀키로 서명한 인증서를 작성할 것 * 인증기관의 인증서는 널리 일반에 게시 또는 공개할 것	좌동	좌동

디렉토리 정보관리 보안 요구사항

구분	CLASS 1	CLASS 2	CLASS 3
인증서 및 CRL 저장	* CA에 의해 발행된 인증서와 CRL은 LDAP 프로토콜을 통하여 저장할 것 * 저장되는 객체에 대해 DN이 정해져야 함	좌동	좌동
인증서 및 CRL 검색	검색을 위한 모든 메뉴는 사용하기 쉬운 웹서비스를 통하여 이루어지게 할 것	좌동	좌동
인증서 및 CRL 수정	* 인증된 사용자에게만 권한을 부여함	* 사용자의 요구가 있을 시에만 할 것 * 부정한 변경 등에 대한 보호를 할 것	좌동
인증서 및 CRL 삭제	* 인증된 사용자에게만 권한을 부여함	* 삭제할 경우도 일정기간 동안 보관을 해둘 것 * 부정한 소거 등에 대한 보호를 할 것	좌동
신청자 정보 등록	임의로 변경하지 말 것	좌동	좌동

기대효과 및 향후과제

? 공개키 기반을 응용한 인증서 관리 기술 연구 개발의 선행적 역할이 기대됨

? 인증서의 보안 요구사항 평가가 가능하게 되어 보다 안전한 정보관리가 가능 함

? 보다 안전한 전자상거래의 인증 기능의 기반 기술 확보 가능할 것으로 예상됨

? 인증서의 활용분야 별로 인증서비스에 실제 적용하여 문제점을 도출하고 보완

? 등급별 보안 기능의 문제점을 파악