전자상거래 보안 및 인증

동서대학교 인터넷공학부
암호 & 네트워크보안연구실
CNSL(Cryptography & Network Security Lab.)
이 훈 재

PC확산속도와 같이 인터넷은 대변혁을 예고하는 파도이다.

인터넷상의 전자상거래는 모든 사업의 기본이 될 것이며,

이런 흐름을 인식하지 못하는 사람은 그 파도에

휩쓸려 생존하기 힘들 것이다.

By Bill Gates

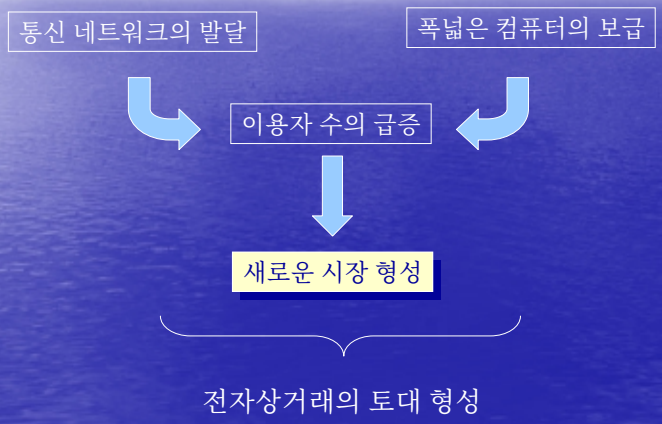
1. 전자상거래 개요

주요 현안들

- **EDI, Internet, Intranet**
- **Cybershopping Mall**
- **Online Advertising: 배너광고, Affliate**
- **Retailing: 구매자 패턴, 구매 방법, A/S 방법, Online Store**
- **Online Publishing: Online Magazine, Intercasting**
- **보안(Security): SET, SSL**
- **전자지불시스템: Digital Cash, NetCheck, Debit Cards**
- **Cyberbank: On-line banking, SFNB**
- **가상교육**
- **제도: 법규, 세금, 관세**

1. 전자상거래 개요

전자상거래 도래



1. 전자상거래 개요

전자상거래의 정의

광의의 정의:
사이버 공간에서 수행되는 모든 상거래 행위와 이를 지원하는 활동

협의의 정의:
인터넷 쇼핑몰에서 이루어 지는 거래 행위

1. 전자상거래 개요

- 네트워크를 통한 상품의 구매와 판매
- 상거래의 새로운 혁명
- 상행위와 마케팅의 핵심 요소인 지역적,공간적 제약의 제거
- 구매자 및 판매자의 거래시간 및 경비의 혁신적 감소

1. 전자상거래 개요

정보보호 서비스

- 전자상거래가 활성화되는 경우 발생할 수 있는 정보화의 역기능을 방지하기 위해서는 다음과 같은 정보보호서비스가 요구됨
  - 기 밀 성 : 전송되는 정보의 비밀 보장
  - 무 결 성 : 전송되는 정보가 변경되지 않음을 보장
  - 인 증 : 전송자의 신분을 증명
  - 부인방지 : 사후 자신의 행위에 대한 부인 불가

암호 시스템	→	**기밀성 보장**
디지털 서명	→	**무결성, 인증, 부인방지 보장**

1. 전자상거래 개요

장점과 단점

장점	단점
시간적 공간적 제약의 해결	제한된 사용자그룹
다양한 상품정보	상품정보탐색의 어려움
비용의 감소	상품규격의 비표준화
고객의 구매형태 분석 용이	안전성
마케팅과 상품광고	
정보산업의 활성화	
낮은 진입장벽	

1. 전자상거래 개요

전자상거래의 장단점

- 전자상거래 장점
  - 시간적, 공간적 제약 극복
  - 전 세계인을 대상으로 한 마케팅(방대한 시장 형성)
  - 상점의 유지와 관리가 용이
  - 사용이 편리함
- 전자상거래 단점
  - 기존의 지불 매체를 적용하기 곤란
  - 새로운 개념의 지불 시스템 요구
  - 보안 문제가 크게 대두

1. 전자상거래 개요

EC의 유형

B to B: 기업 간 전자 상거래

B to C: 기업과 소비자간 전자 상거래

B to G: 기업과 정부 기관간 전자 상거래

2. 기본적인 암호기술

전자상거래에서의 정보보호기반기술

암호시스템	대칭형 / 비대칭형 암호시스템
전자서명시스템	비대칭형 암호시스템,해쉬함수

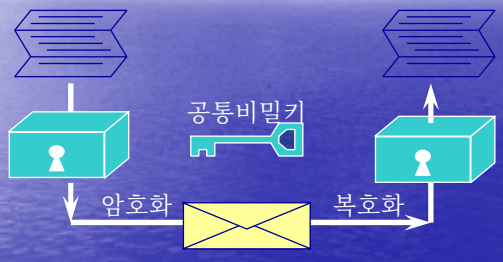
인증서

인증기관

공개키 기반구조

2. 기본적인 암호기술

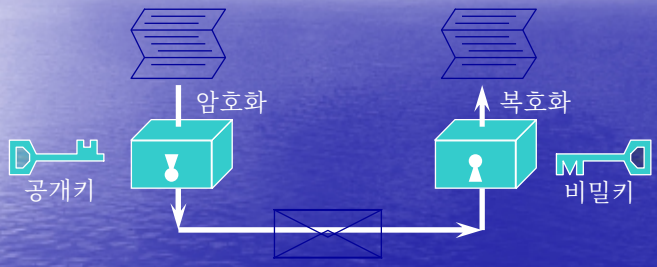
대칭형 암호시스템



- 특징 : 암호화키와 복호화키가 동일
- 장점 : 암호화 및 복호화 속도가 빠름
- 단점 : 키관리의 어려움. 키분배의 문제. 다양한 응용의 어려움
- 사례 : DES, FEAL 등

2. 기본적인 암호기술

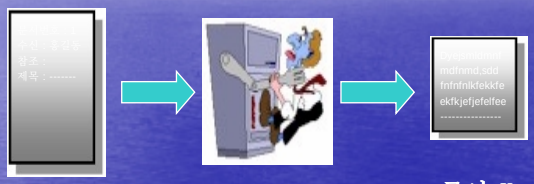
비대칭형 암호시스템



- 특징 : 복호화키(=비밀키)와 암호화키(=공개키)가 다름
- 장점 : 키관리가 용이. 다양한 응용이 가능. 안전성이 뛰어남
- 단점 : 암호화 및 복호화 속도가 느림
- 사례 : RSA 등

2. 기본적인 암호기술

해쉬함수



- 특징 : 일방향 함수 + 메시지 압축(Message Digest)
- 장점 : 디지털서명에서 주로 사용
- 사례 : MD5, SHA 등

3. 전자 지불 시스템

전자지불 시스템 등장

- 인터넷의 활성화 ⇨ 전자상거래를 구체화하는데 큰 기여를 함
  - 시각적, 청각적 데이터에 쉽게 접근할 수 있음
  - 가상의 쇼핑공간이 등장, 실시간으로 물건 거래
- 전자상거래가 주목을 끌게 된 이유
  - 인터넷 이용자수의 급증
  - 전자상거래에 필요한 보안기술의 진전
  - 홈페이지 구축 기술의 진전

⇨ 온라인으로 주문이나 결재가 가능한 안전한 지불 시스템이 필요함

3. 전자 지불 시스템

전자지불 시스템의 분류

- 3가지 부류

3. 전자 지불 시스템

전자화폐 시스템

- 몬덱스 시스템: 전자화폐로 처음 유통.
  - 영국 웨스트민스터 은행과 브리티시 텔레컴
- 전자화폐의 장점
  - 화폐 제작/현금 수송/보관 등 비용 절감
  - 화폐 분실/도난 위험 방지
  - 신속한 금전처리
- 인터넷 가상공간에서 통용되는 새로운 화폐의 발행을 목표로 만들어지고 있는 시스템.
- 소액의 거래, 개인의 물품 구입이나 서비스에 적합함.

3. 전자 지불 시스템

인터넷 신용카드 지불 시스템

- SET(Secure Electronic Transaction) :
  - 비자/마스터 카드 등 신용카드 회사
  - 신용카드기반 지불 절차 제시
- 효과적인 거래 유형은 거래액이 트랜잭션 비용보다 크면서 사용한도액을 넘지 않을 것
  - 인터넷 상에서 유통되는 적은 액수의 상품들이 많이 있으므로 트랜잭션 비용의 절감이 필수적이다
- 사용자 정보(이름,주소,신용카드 번호)에 대한 보안 대책 필요

3. 전자 지불 시스템
전자수표 시스템

- 전자수표: 현실 세계에서 사용되고 있는 종이로 된 수표를 그대로 인터넷 상에 구현한 것
- 요구사항: 발행자와 인수자의 신원 인증 필요
  - 여러 가지 보안 기법들이 사용되고 있고, 이로 인해 트랜잭션 비용이 많이 든다.
- 적용분야: 상당히 큰 액수의 거래, 기업간의 상거래 지불 수단으로 적합
- 특　　징: 실제 수표보다 처리 비용이 저렴

3. 전자 지불 시스템
각국의 시스템 개발 현황 (1)

- 미국
  - 네트워크 기술이 발달 - - - 온라인 상의 전자화폐 중심
  - 최근 들어 off-line 형태의 전자화폐 개발
  - Visa + Master Card + Verifone사: “New York City Pilot”
    - 개인 휴대 현금 인출기(PATM) 이용
    - 스마트 카드 사용
  - DEC사: Millicent
    - 소액 거래를 대상
  - CyerCash사: CyberCash 화폐 지불 서비스
    - CyberCash Wallet을 이용, 소액 거래

3. 전자 지불 시스템
각국의 시스템 개발 현황 (2)

- 영국
  - Mondex사: Mondex
    - off-line, on-line 모두 사용
    - 사용자간의 이체가 가능
    - 특별한 h/w 장치가 필요
- 네덜란드
  - DigiCash: Ecash
    - 고객과 상점측의 비밀을 완벽히 보호
- 독일
  - 금융기관들이 전자화폐용 IC카드 보급

3. 전자 지불 시스템
각국의 시스템 개발 현황 (3)

- 프랑스
  - 1991년부터 "텔레팩트" 서비스 제공
    - 은행 카드, 전자 송금, 전자 지불 수표 등의 서비스 제공
    - 정보 단말기('미니텔'), 스마트 카드 이용
- 벨기에: Proton
- 덴마크: Danmont
- 핀란드: AVANT

4. 전자 화폐
전자화폐(Electronic Cash)

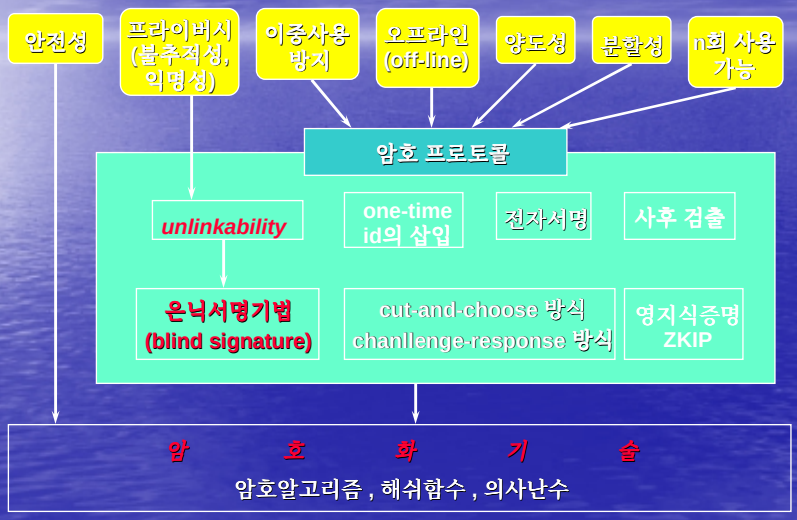
- 전자화폐는 그 자체로써 화폐 가치
  - 공중전화 카드, 버스카드는 넓은 의미의 전자화폐
- 독립적인 신용구조를 가지고 있어서 물품 구입 시 은행이나 카드 발행사로부터의 거래 승인이 필요 없다.
- 인터넷 등의 네트워크 상에서 지불을 필요로 하는 사이버 비즈니스의 지불 수단으로써 필요하다.
- 전자 화폐의 이중사용 문제, 실세계 화폐와의 관계, 세금 등의 사회 경제적인 문제 등 과제

4. 전자 화폐
전자화폐의 요구조건

- **독립성**(Independence): 전자화폐의 보안은 물리적인 위치에 관계 없을 것
- **보안성**(Security): 전자화폐는 복제 또는 재사용 불가할 것
- **추적불가능**(Untraceability): 사용된 지폐 흐름에 대한 추적이 불가능할 것
- **오프라인 지불**(Off -line payment): 사용의 편의성을 위해서 오프라인으로 지불 가능할 것
- **양도성**(Transferability): 타인에게 양도 가능할 것
- **분할성**(Divisibility):액수가 큰 전자화폐는 액수가 작은 화폐로 분할 가능할 것

4. 전자 화폐

전자화폐와 암호기술의 관계



4. 전자 화폐

전자화폐의 분류

- IC카드형 전자화폐
  - 카드 자체가 연산능력을 가지고 있으며 더욱이 비밀 보호 능력도 자기 카드보다 우수하다
  - 비밀키와 암호 알고리즘이 카드 내부에 입력되어 있다
  - 가치의 양도성을 기준으로 폐쇄형과 개방형으로 구분된다
- 네트워크형 전자화폐
  - 인터넷상의 가상은행이나 거래 은행과 접속된 PC에 전자화폐를 저장했다가 필요할 때 공중 통신망을 통해 대금 결제를 하는 방식이다

4. 전자 화폐

전자화폐에서 기술적인 문제들 (1)

- 정보의 보호(Security)
  - 인터넷은 안전하지 못한 네트워크로 네트워크상에서 주고 받는 데이터를 다른 사람이 볼 수 있다.
  - 전자화폐의 보안성은 수학적인 계산에 의해 보증을 받는다.
- 전자서명(Digital signature)
  - 컴퓨터의 디지털 정보는 복제가 가능하기 때문에 이를 방지하기 위해 암호화 기법과 더불어 전자서명 등의 기술이 필요하다.
  - 메시지 인증 기능과 사용자 인증기능을 한다.

4. 전자 화폐

전자화폐에서 기술적인 문제들 (2)

- 은닉서명(Blind signature)
  - David Chaum이 고안한 서명기법
  - 전자화폐를 인출할 때 일련번호를 사용하기 때문에 현금 사용 상황을 추적할 수 있다
  - 은행에서 인출할 화폐의 시리얼 번호를 제공할 때 불특정한 숫자로 이 번호를 곱해서 은행에게 보내 주고 은행은 이 번호를 전자 현금화해서 사용자에게 넘겨주면 사용자는 이 번호를 곱한 숫자로 다시 나누어 원래의 번호로 환원해서 사용하는 방식
- 전자화폐의 이중사용(Double spending)
  - 전자화폐를 복사해 두 번 이상 사용 방지

4. 전자 화폐

불추적성 실현 (blind signature)

4. 전자 화폐

전자화폐 시스템 거래 주체

- 고객: 전자화폐의 인출, 보관 및 지불
- 판매자: 지불청구, 보관 및 입금
- 발행기관: 전자화폐 발행 및 인출, 예탁관리, 위조 및 이중 사용 방지
- 브로커: 고객과 판매자 사이의 중개자

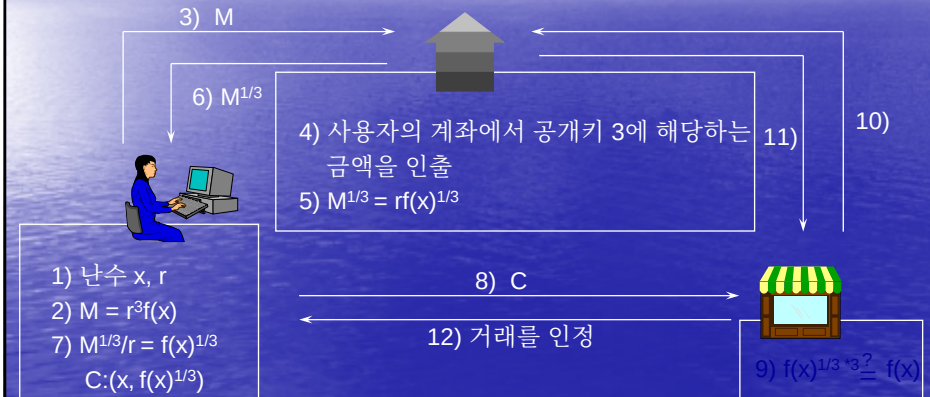
4. 전자 화폐

제안된 전자화폐시스템

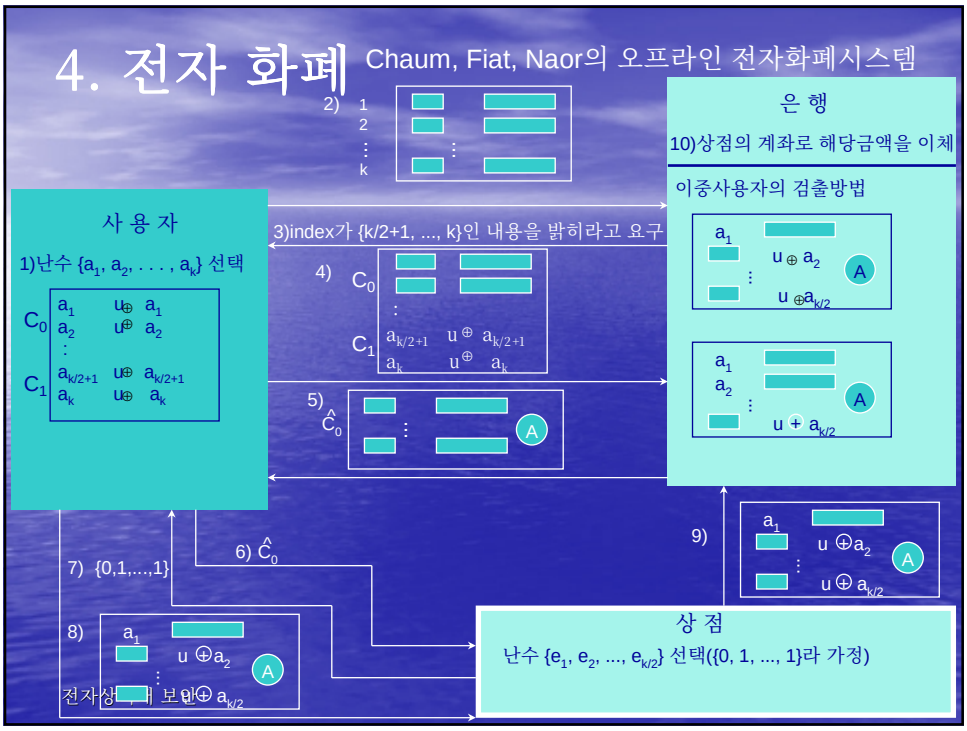
- Chaum
  - RSA를 이용한 온라인 전자화폐시스템
  - RSA를 이용한 오프라인 전자화폐시스템
- Brands
  - Restrictive blind signature를 이용한 전자화폐시스템
- Stadler 등
  - Fair 전자화폐시스템

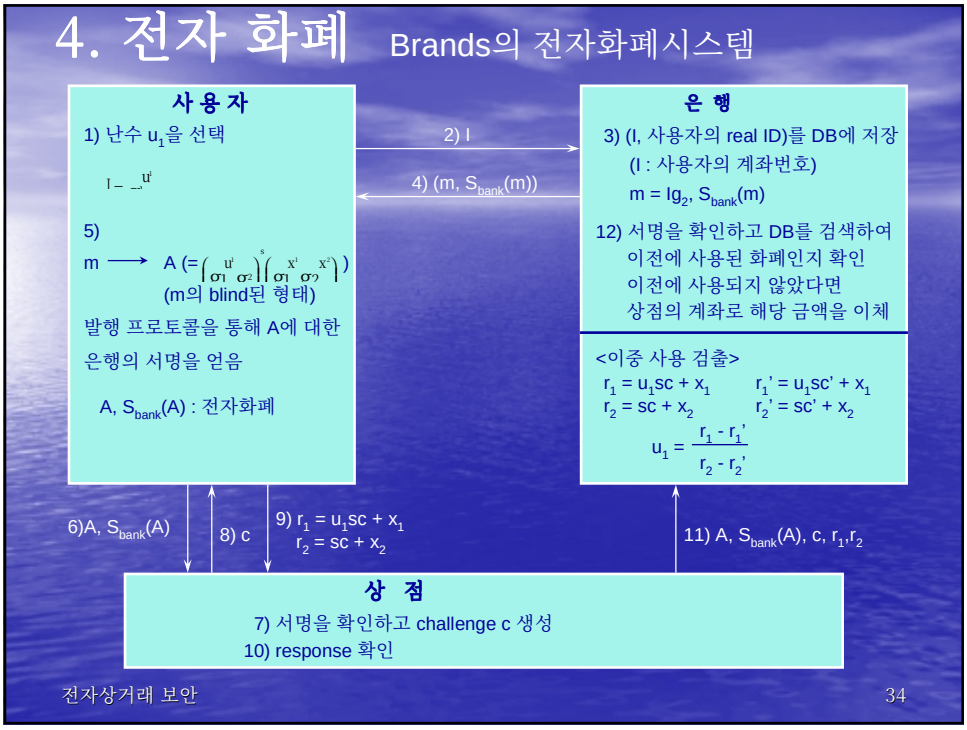
4. 전자 화폐 RSA를 이용한 온라인 전자화폐시스템

- f : 해쉬함수
- n : n=p*q의 합성수 p,q는 은행만이 알고 있음
- 3,1/3 : 일정한 금액에 해당하는 은행의 공개키 및 비밀키



10) C의 재사용 여부를 물어봄
11) C가 재사용되지 않았으면 상점의 계좌로 해당금액을 이체


4. 전자 화폐
Chaum, Fiat, Naor의 오프라인 전자화폐시스템
은 행
10)상점의 계좌로 해당금액을 이체
이중사용자의 검출방법
사 용 자
1)난수 {a1, a2, . . . , ak} 선택
3)index가 {k/2+1, ..., k}인 내용을 밝히라고 요구
4)
5)
6)
7) {0,1,...,1}
8)
9)
상 점
난수 {e1, e2, ..., ek/2} 선택({0, 1, ..., 1}라 가정)


4. 전자 화폐
Brands의 전자화폐시스템
사 용 자
1) 난수 u1을 선택
5)
(m의 blind된 형태)
발행 프로토콜을 통해 A에 대한
은행의 서명을 얻음
A, Sbank(A) : 전자화폐
은 행
2) I
4) (m, Sbank(m))
3) (I, 사용자의 real ID)를 DB에 저장
(I : 사용자의 계좌번호)
12) 서명을 확인하고 DB를 검색하여
이전에 사용된 화폐인지 확인
이전에 사용되지 않았다면
상점의 계좌로 해당 금액을 이체
<이중 사용 검출>
6)A, Sbank(A)
8) c
9) r1 = u1sc + x1
r2 = sc + x2
11) A, Sbank(A), c, r1,r2
상 점
7) 서명을 확인하고 challenge c 생성
10) response 확인
전자상거래 보안
34

4. 전자 화폐 현재 사용되는 전자지불시스템 현황

유형		제품	안전성	불추적성	이중사용 방지	오프라인	양도성	분할성	n회사용 가능
네트워크형	전자화폐	Ecash	o	o	o	온라인	x	x	x
	신용카드 기반	FV	o	x	-	온라인	x	x	x
		Cyber Cash	o	x	-	온라인	x	x	x
	전자수표 기반	NetCheque	o	x	o	온라인	x	x	x
		Echeck	o	x	o	온라인	x	x	x
전자지갑형	영국	**Mondex**	**o**	**o**	**o**	**오프라인**	**o**	**x**	**x**
	벨지움	Proton	o	o	o	오프라인	x	x	x
	포르투칼	MEP	o	o	o	오프라인	x	x	x
	덴마크	Danmont	o	o	o	오프라인	x	x	x
	핀란드	AVANT	o	o	o	오프라인	x	x	x
	독일	Chipknip	o	o	o	오프라인	x	x	x
	한국형	전자지갑	o	x	o	오프라인	x	x	x

4. 전자 화폐

현재 인터넷에서 사용되는 지불방식들

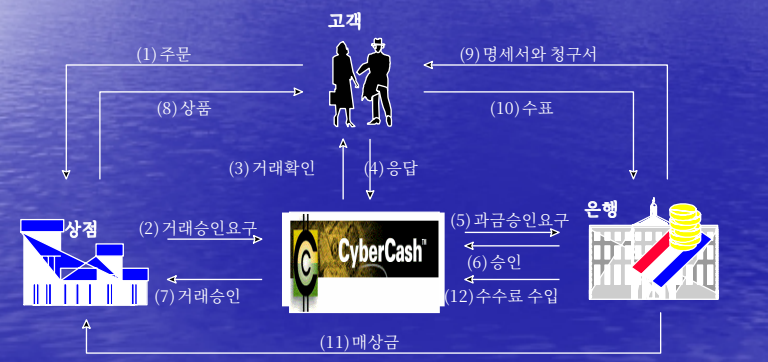
- 신용카드 기반
  - First Virtual(http://www.fv.com)
  - Cyber Cash(http://www.cybercsh.com)
- 전자 화폐
  - e-Cash(http://www.digicash.com)
- 스마트 카드 기반
  - 몬덱스 카드(http://www.mondex.com)

4. 전자 화폐
First Virtual

- 개인의 신상정보를 전화등을 이용해 등록해 두고 ID 번호를 이용자에게 발행하는 방식, 전자 우편을 이용

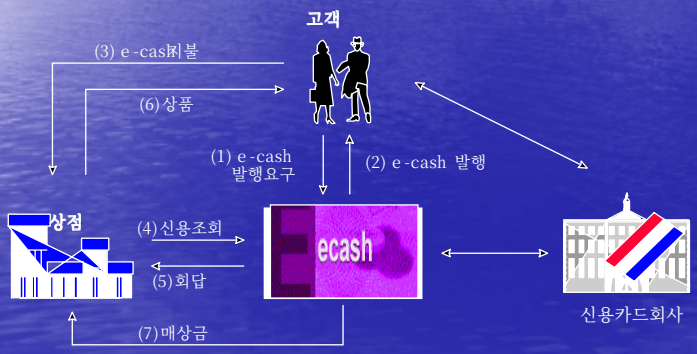
4. 전자 화폐
Cyber Cash

- 전용 소프트웨어를 사용
- 사용자의 신용카드 정보는 암호화되어 전송됨



4. 전자 화폐
e -Cash

- DigiCash사에서 개발
- 전자화폐 개념에 기반



4. 전자 화폐
Mondex

- 영국의 몬덱스사에서 개발
- 스마트 카드를 이용하여 오프라인 방식

4. 전자 화폐
Ecash - Introduction

- 최초로 인터넷 상에서 전자 현금 서비스 개시
- Ecash 중앙 은행인 FDB(First Digital Bank)에서 전자화폐 발행
- 지불된 전자화폐 입금 가능
- 미국 마크 트웨인 은행, 핀란드 메리타 은행 /EUnet에서 실세계 화폐와 환전 가능
- 독일 도이치 은행이 시범 전자화폐 발행 은행 서비스 계획

4. 전자 화폐
Ecash - Money Flow

- 인출(withdraw)
  - 사용자의 인출요구에 의해서만 ecash 계좌에 접근 가능
  - 동전의 도난을 막기 위해 password -encrypted 방식으로 사용자의 하드디스크에 저장
- 지불(payment)
  - 동전들은 상점이나 어떤 사람에 의한 도난을 막기 위해 은행의 공개키로 암호화
- 입금(deposit)
  - 지불 프로토콜에서 상점이 수행하는 부분
- 복구(recovery)
  - 사용자와 발행기관 사이의 복구 프로토콜로서 이전의 체크포인트 이후에 인출되었던 모든 동전을 복원 가능

4. 전자 화폐
Ecash - Cryptographic Primitive

- David Chaum이 제안한 은닉서명(blind signature) 기법 사용
- Ecash 시스템에서는 RSA와 3-DES를 조합 사용
- Ecash 시스템에서는 SHA-1 해쉬함수사용

4. 전자 화폐
Ecash - Coins

- 각 화폐생성에서 발행기관은 임의로 새로운 RSA modulus $N=pq$ 생성
- 화폐생성시 금액은 사전에 액수가 지정된 공개 멱지수(exponent) e_i를 이용해서 암호화
- 액면 금액 D_e의 ecash 동전 C는 RSA 서명으로 구성

$$C = f(x)^{\frac{1}{e}} \bmod N \quad \text{f: redundancy-adding 함수}$$

- 발행기관은 동전의 서명 유효성과 동전이 이전에 사용되었는지를 검사한 후에 동전의 번호만을 저장

4. 전자 화폐
Ecash - Withdraw

- 인출

$M=f(x)r^e \bmod N$

$S = M^d \bmod N$

$M^d \leftarrow f(x)^d r \bmod N$

$Coin = M^d / r = f(x)^d \bmod N$

  - $f(x) = x_t \,||\, \bullet\bullet\bullet \,||\, x_1 \,||\, x_0$, $x_0 = x$, $x_{i+1} = H(x_0 \,||\, \bullet\bullet\bullet \,||\, x_i)$
  - x: coin number
  - r: blinding factor
  - f: redundancy -adding, modulus N과 동일 길이

4. 전자 화폐
Ecash - Payment

- 지불

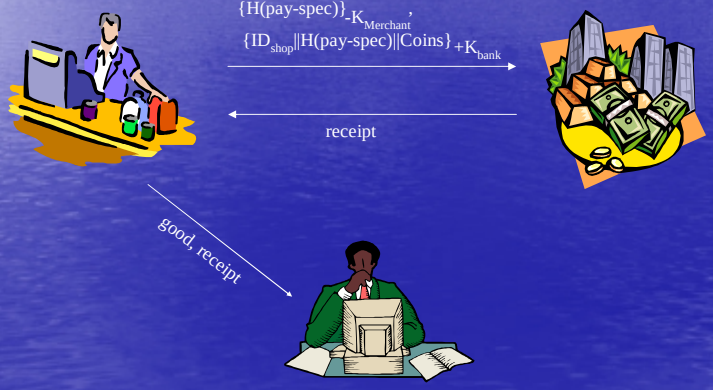
지불협상

$\{ID_{shop} || H(pay\text{-}spec) || Coins\}_{+K_{bank}}$

  - pay -spec: 구입할 물건과 물건의 금액에 대해서 사용자와 판매자가 합의한 결과를 기록한 문자열

4. 전자 화폐
Ecash - Deposit

- 입금



4. 전자 화폐
NetCash - Introduction

- 캘리포니아 대학의 Information Science Institute에서 개발.
- 확인된 전자화폐(발행기관이 일련번호를 알고있음)를 사용하지만 익명성과 수용성(acceptability)을 제공하기 위해서 다른 통화서버와 화폐의 교환 가능
- 확장성을 위하여 다중 통화서버 사용

4. 전자 화폐
NetCash - Certificate

- 통화서버(Currency Server)를 설치, 관리하고 싶은 은행이나 기업, 또는 단체는 중앙 인증국(Central Certification Authority)으로부터 인증을 받아야 한다.
- 통화서버는 공개키쌍을 생성하여 중앙 인증국으로부터 서명 받음으로써 인증된다.
- 인증서에는 인증 이름, 통화서버의 이름, 통화서버의 공개키, 발행날짜, 소멸날짜로 구성되며 중앙 인증국의 개인키로 서명된다 $-K_{Certif}$
- {Certif_id, CS_name, $+K_{CS}$, issue_date, exp_date}

4. 전자 화폐
NetCash - Coins

- 통화서버는 전자화폐를 발행하는데 전자화폐에는 통화서버 이름, 통화서버의 네트워크 주소, 소멸날짜, 일련번호, 화폐금액으로 구성됨 $-K_{CS}$

  {CS_name, CS_addr, exp_date, serial_num, coin_val}
- 통화서버는 발행된 모든 화폐들의 일련번호 리스트 유지
  - 만약 화폐의 일련번호가 데이터베이스에서 발견되면 사용되지 않았던 것이기에 유효하고, 한 번 화폐의 일련번호는 데이터베이스에서 영구히 제거됨.

4. 전자 화폐
NetCash - Payment

지불협상

{Coins, K_{Buy}, K'_{Buy}, S_id} $_{+K_M}$

- 고객은 지불을 위해 전자화폐, 새로 생성된 세션 키와 상품을 암호화하기 위한 비밀키 그리고 구매하는 상품의 이름을 판매자의 공개키로 암호화해서 판매자에게 보낸다.

4. 전자 화폐
NetCash - Deposit

{Coins, K_M, trans} $_{+K_{CS}}$

{new coins} $_{K_M}$

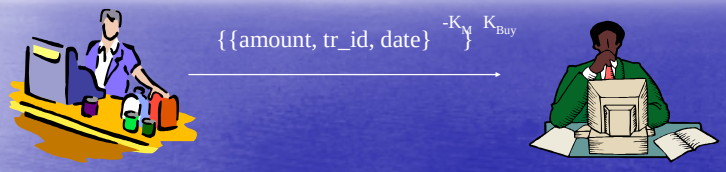
- 판매자는 받은 화폐가 유효한 지를 검사하기 위해 통화서버에게 보낸다.

  {Coins, $K_{Merchant}$, transaction_type} $_{+K_{CS}}$

- 통화서버는 그 화폐들이 유효한지 검사한 후 트랜잭션의 타입에 따라 입금시키거나 새로운 화폐를 판매자의 세션키로 암호화해서 돌려줌

  {New_coins} $_{K_{Merchant}}$

4. 전자 화폐
NetCash - Receipt



- 새로운 화폐를 받거나 아니면 입금이 되면 상점은 구매자가 적절히 지불한 것을 알게 됨
- 영수증을 상점의 비밀키로 서명하고 구매자의 공개키로 암호화 해서 구매자에게 되돌려 줌

{{Amount, transaction_id, date} }
-K_Merchant K_Buyer

4. 전자 화폐
PayMe

- 아일랜드의 Trinity 대학에서 제시
- 온라인 지불 방식
- DigiCash사의 Ecash의 완전한 익명성과 NetCash의 확장성(Scalability) 결합
- 공개키 암호화와 대칭키 암호화 사용
- 발행기관은 유통되고 있는 전자화폐의 일련번호를 관리함
- 제한된 익명성
- 현재 프로토콜만 제시되어 있음

4. 전자 화폐
PayMe - Protocol

4. 전자 화폐
VarietyCash

- 네트워크 기반과 스마트 카드기반 지불 환경에서 둘 다 이용할 수 있고 원자성(atomicity)을 제공하는 시스템이다.
- 신뢰에 의존한 익명성을 제공한다.
  - 화폐 발행기관은 발행된 화폐의 일련번호와 사용자에 대한 정보를 기록하지 않는다.
- 트랜잭션을 처리하는데 따르는 오버헤드를 최소화해서 비용을 줄임.

4. 전자 화폐
VarietyCash - Withdraw

- 인출
  - C → I: $\{ID_C, K_C\}_{+K_I}$
  - C ← I: $\{ID_I, K_I, R_I\}_{+K_C}$
  - C → I: $\{W\text{-}DESC, \{ID_I, R_I^{CI}, W\text{-}DESC\}_{K_{CI}}\}_{-K_C}$ K_{CI}
  - C ← I: $\{Coins\}^{CI}$, mac $(ID_I, \{Coins\}^{CI})$
  - C → I: mac (ID_C, R_I)
  - R_I: Nonce; $K_{CI}=K_C \oplus K_I$
  - W-DESC: Coin Purchase Description
  - Coin 구조
    - TRIPLE-DES MAC-TAG : CoinID, Amount, Expiration date를 발행 기관의 비밀키를 이용해서 계산한다
    - CoinID: 임의로 선택된 동전의 일련번호
    - Amount: 동전의 금액
    - Expiration date: 동전의 만료기간

4. 전자 화폐
VarietyCash - Payment

- 지불
  - C ← M: $\{ID_M, TID_M\}_{+K_C}$
  - C → M: $\{M, TID_M, Coins\}_{+K_I}$
  - M → I: $\{ID_M, K_M, TID_M, V\text{-}DESC, EncC_1\}_{+K_I}$
  - M ← I: $\{ID_I, K_I\}_{K_{MI}}$, $\{Coins\}^{MI}$, mac $(ID_I, TID_M, EncC_2)$
  - M → I: mac (ID_M, TID_M)
  - TID_M: Time stamp
  - V-DESC: Verification and Execution Request Text
  - $EncC_1$:$\{M, TID_M, Coins\}_{+K_I}$
  - $K_{MI}=K_M \oplus K_I$
  - $EncC_2 = \{Coins\}_{K_{MI}}$

5. 소액 지불
소액지불 (micropayment)

- 소액지불
  - Micropayment 결제 방법이란 고객이 통신망상에서 요금이 $1 미만인 소액의 On-Line서비스를 이용하고 전자화폐와 같은 소액의 지급 결제 수단을 이용하여 대금을 결제하는 방법
    - 전자신문, 잡지, 게임, 음악, 그림 등
  - 스크립(scrip)을 위조하여 얻을 수 있는 이익이 스크립의 비용보다 비싸질 정도의 암호화를 사용
    - Scrip 은 통화, 또는 Access 권한, 또는 Membership 등을 의미
  - 판매자가 직접 scrip을 발행 ⇨ 중앙집중처리 방식에서 오는 거래 지연, 시스템 구축비용 등을 절감
  - 같은 사이트 반복 쇼핑인 경우 판매자로부터 scrip 구매
  - Millicent, Netcent

5. 소액 지불
Millicent

- Digital equipment사에서 개발, 서비스중인 소액지불 시스템
- 고객은 상품 구매대금으로 브로커로부터 구입한 판매자 scrip 제시
- 판매자가 직접 scrip의 유효성과 이중사용 여부를 확인할 수 있는 분산 확인 방식
  - 판매자는 자신이 발행한 scrip의 데이터베이스 유지
- Scrip은 이를 발행한 특정 판매자에게만 유효함
- 처리속도 향상을 위해서 해시 함수 사용
- 통신 비용을 줄이기 위해서 최소한의 암호 사용

5. 소액 지불
Millicent - Scrip

- Scrip 구성
  - Session ID: scrip 일련번호
    - expiration date: scrip의 유효기간
    - session number(N): secret을 상기 시켜주는 일련번호
  - k : 관리와 교환을 위해서 사용되는 세션키.
    - SessionID를 session number에 해당하는 secret으로 서명한 것
    - H(SessionID^X(N))
  - Info: 판매자와 고객에 대한 정보. 암호화하여 전송할 때 키 k를 사용함
  - Coin: 값(사용한도액)과 일련번호(Z)를 가진 문자열
  - j: coin key. Coin이 현재 세션에 속한다는 것을 증명하는 서명
    - H(SessionID^Info^Coin^X(Z))

5. 소액 지불
Millicent - Protocol (1)

판매자 scrip 요청

판매자 scrip

- 고객이 전자화폐, 신용카드 등을 이용하여 Broker Scrip을 구매함
  - Broker는 카드사나 은행과 같은 금융기관, 주요 인터넷서비스 제공기관이 될 수 있음
- 고객이 브로커에게 브로커 Scrip을 제시하여 판매자 Scrip의 구매를 요청함

5. 소액 지불
Millicent - Protocol (2)

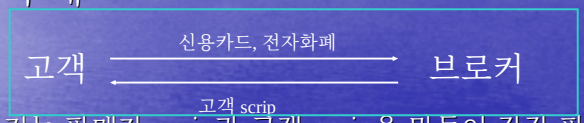
- 고객은 판매자에게 판매자 scrip으로 구매대금을 지불한다
- 구매 대금을 받은 판매자는 scrip 안에 포함되어 있는 정보들을 암호화하여 고객이 보낸 값과 비교하여 같으면 유효한 것으로 간주하고 고객이 선택한 상품과 함께 거스름 scrip을 만들어 고객에게 보낸다.

5. 소액 지불
NetCent

- 소액지불 시스템
- 한 판매자로부터 다른 판매자에게 scrip을 건네줄 수 있음
- 전자화폐의 분산된 검증, 여러 화폐 발행기관 지원
- 서명 알고리즘으로 RSA 공개키 알고리즘 사용
- 온라인 중재자를 통한 분쟁 해결
- 동작 비용을 최소화하도록 설계

5. 소액 지불
NetCent

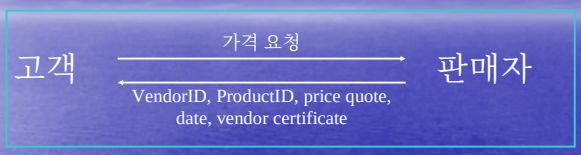
- Scrip 구매



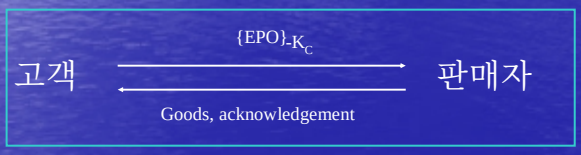
  - 브로커는 판매자 scrip과 고객 scrip을 만들어 각각 판매자와 고객에게 준다
  - 판매자 scrip
    - 고객의 서명을 확인할 수 있는 공개키
    - 유효기간
  - 고객 scrip
    - 전자 지불 주문서(Electronic Payment Order)에 서명하기 위한 개인키
    - 유효기간

5. 소액 지불
NetCent

지불협상



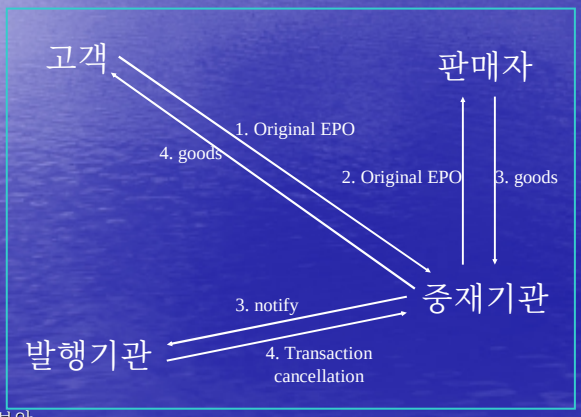
지불



EPO: {고객, 판매자, 구매상품 식별자, scrip 잔액, 트랜잭션 시간}

5. 소액 지불
NetCent

- 상품이 전송되지 않을 경우



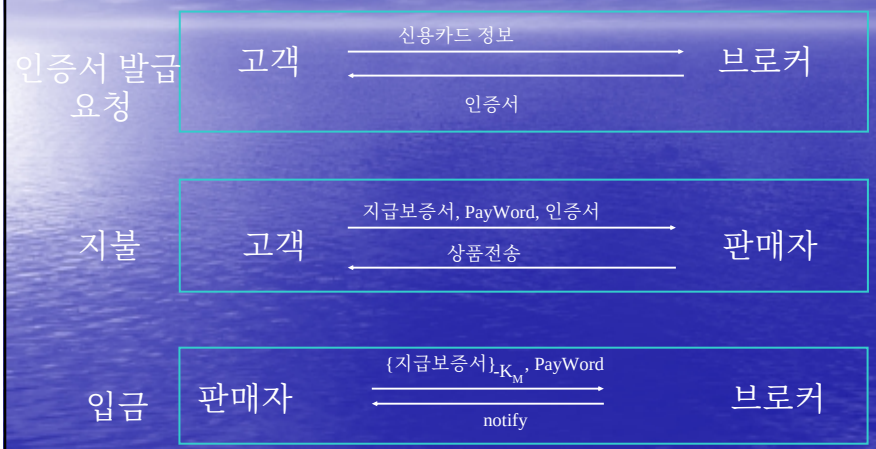
5. 소액 지불
PayWord

- Ron Rivest와 Adi Shamir가 공동으로 제시한 소액지불 시스템
- 고객이 직접 PayWord 발행
- 처리속도 향상을 위해서 해시함수 사용
- 참여자간 통신을 최소화한 시스템
- 해시체인(hash chain) 방식 사용
- 완전한 익명성을 제공하지 않는다

5. 소액 지불
PayWord

- 인증서
  - {브로커명, 고객명, 고객의 상품배달주소, 고객의 공개키, 인증서의 유효기간, 기타정보} $-K_b$
- PayWord 발행
  - 판매자에게 지급할 총금액을 결정(PayWord의 길이)
  - 임의의 숫자 W_N을 선택한 후 역순으로 해시값을 구해서 최종적으로 W_0을 산출한다.
    - $W_i = H(W_{i+1})$, $i = n-1, n-2, \ldots, 0$
  - 지급메시지 $P=(W_i, i)$
- 지급보증서
  - {판매자명, 고객의 인증서, PayWord root(W_0), 지급보증서의 유효기간, 기타정보} $-K_c$

5. 소액 지불
PayWord



6. 전자 수표
NetBill

- Carnegie mellon 대학에서 제시한 전자수표 시스템
- 원자성(atomicity) 보장
  - 상품 배달 후 대금 결제
- 공개키 암호화 방식과 대칭키 암호화 방식 사용
- Kerberos 티켓 사용
- 전자서명 알고리즘(Digital signature algorithm) 사용
- 현재 테스트를 위한 Alpha 버전이 구현되었다
- 97년 5월 미국의 CyberCash사가 NetBill 시스템에 대한 권리 취득

6. 전자 수표
NetBill

- 전자지급 지시서(Electronic Payment Order)
  - Identity: 고객의 신원확인 내용(pseudonymous)
  - productID: 상품 번호
  - Price: 협상된 가격
  - M: 판매자의 신원확인 내용
  - CC(E_K(Goods)): 암호화 된 상품의 checksum
  - CC(PRD): 고객이 요청한 제품 데이터의 checksum
  - CC(Cacct, AcctVN): 고객의 계좌 번호와 계좌 확인 nonce의 checksum
  - EPOID
  - T_{CN}(TrueIdentity): 고객의 실제 신원을 증명하는 kerberos 티켓
  - E_{CN}(Authorization: 인증 토큰
    Cacct : 고객의 NetBill 계좌번호
    AcctVN : 계좌 확인 nonce
    Cmemo : 고객 메모 부분
)

6. 전자 수표

NetBill

7. 기타 지불 시스템

기타

- Modex
  - IC 카드 중심의 전자화폐 시스템으로 가장 대표적인 전자화폐 시스템
  - 오프라인 시스템
  - 거래시 거래승인이 필요없고 개인간의 자금 이체가 자유롭다
  - 5개국 통화로 가치를 저장가능
- CAFE(Conditional Access for Europe)
  - 사용자의 익명성을 보장하는 오프라인 전자화폐이다
  - 유럽 여러나라의 13개 파트너들이 참여하고 있다
  - DigiCash사의 Ecash시스템의 portable을 추가한 형태이다
  - 1997년에 프로젝트가 끝났으며 현재 테스트중이다
  - OPERA 프로젝트를 추진중이다

7. 기타 지불 시스템
기타

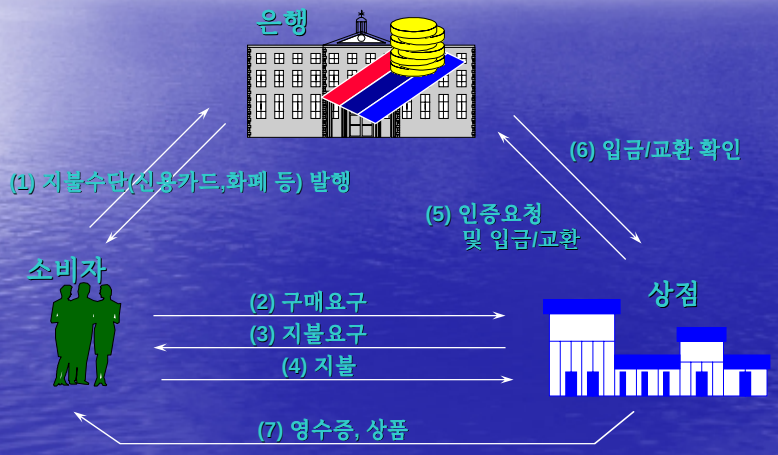
- MiniPay
  - 이스라엘 IBM Haifa Research Lab에서 제시한 소액지불 시스템
  - 현재 시험 서비스중이다
- iKP Micropayment
  - 스위스 IBM Zurich Research Lab에서 제시한 소액지불 시스템
- PAYSYST
  - St. Gallen 대학에서 제시한 시스템으로, 통합된 전자 지불 시스템 개발을 목적으로 제시되었다
- NetCard
  - Cambridge 대학에서 제시한 IC 카드 기반의 소액지불 시스템이다
  - 비익명, 추적가능

7. 기타 지불 시스템
기타

- JEPI(Joint Electronic Payments Initiative)
  - 자동화된 지불 협상을 위한 프로토콜
  - W3C consortium, CommerceNet, CyberCash, Microsoft, NetBill, OSF, and OpenMarket등이 참여하고 있다
- SEMPER(Secure Electronic Marketplace for Europe)
  - 자동화된 지불 협상과 지불 시스템 통합을 위한 프로토콜이다

8. 전자상거래 인증 모델

전자상거래 인증 및 암호화 기술



8. 전자상거래 인증 모델

전자인증제도와 초고속인증망

전자인증제도

사이버 공간상의 전자문서, 전자거래 등 관련 전자업무에서의

- 당사자의 신분확인 기능 (신원 확인)
- 전자업무 내용의 정보보호 및 무결성 기능(비밀성 보장)
- 전자행위에 대한 부인봉쇄 기능(분쟁해결) 등

전자업무의 중요 인증 문제와 관련하여

신뢰할 만한 제3자(*인증기관*)가 확인 및 증명해주는 제도

전자인증제도의 실체화

- 전자서명법
- 공개키기반구조(***초고속인증망***)

8. 전자상거래 인증 모델

공개키기반구조(PKI : Public Key Infrastructure)

인증기술 : 사용자인증 + 내용인증

전자서명 <--- 공개키암호알고리즘

상대방 공개키 인증 방식이 요구

인증센터(키관리센터)의 필요성

공개키기반구조(PKI)

초고속인증망 구축

8. 전자상거래 인증 모델

초고속인증망(PKI)

정의

키관리시스템의 기반구조로 정보보호서비스를 제공해주는 암호키와 인증서(Certificate)를 안전하게 분배해주는 시스템(Delivery System)

목적

- 전자서명서비스(인증, 무결성, 부인봉쇄)
- UBS 레벨의 암호화 키관리(암호통신용 세션키, 전자메일용 세션키)
- 비밀데이타의 복구기능

특성

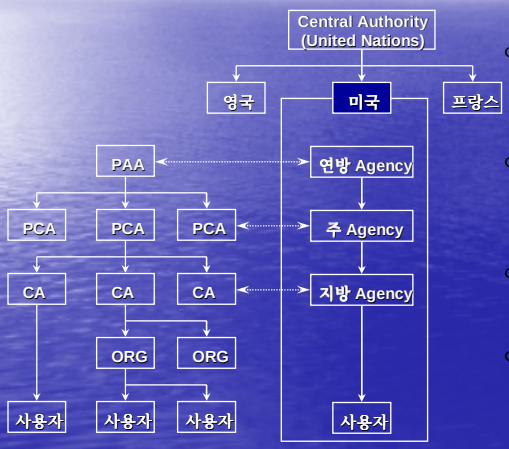
- 정보통신망(초고속정보통신망, 초고속행정정부망)과 연계
- 국제간의 키관리의 상호 인증제도와 연계
- OECD 암호지침과 관련 law enforcement 제도 반영

관련용어

미국(FKMI, FPKI), 캐나다(FPKI), 유럽(ICE-TEL), 호주(PKAF)

8. 전자상거래 인증 모델

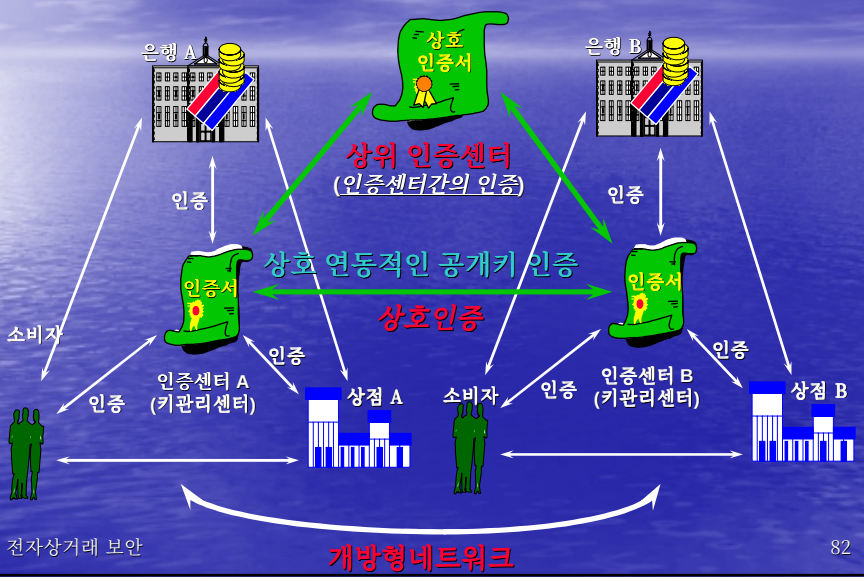
인증기관 계층구조

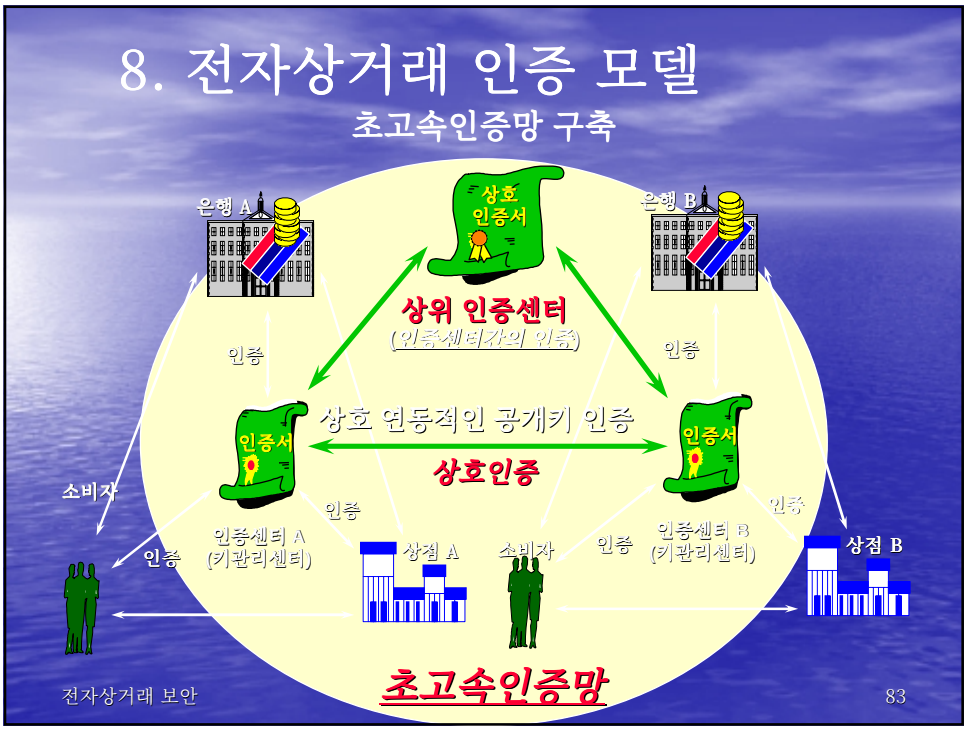


- PAA(Policy Approving Authority)
  - 전체 PKI에 대한 전반적 가이드라인을 수립
  - PCA의 공개키를 확인
- PCA(Policy Certification Authority)
  - 도메인내의 모든 CA와 사용자들의 정책을 수립
  - CA의 공개키를 확인
- CA(Certification Authority)
  - PCA와 PAA의 정책에 따라 사용자의 공개키를 확인
- ORA(Organizational Registration Authority)
  - CA와 사용자 사이의 중재자의 역할

8. 전자상거래 인증 모델

전자상거래 최종 모델




8. 전자상거래 인증 모델
초고속인증망 구축
은행 A
상호 인증서
은행 B
상위 인증센터
(인증센터간의 인증)
인증
인증
상호 연동적인 공개키 인증
인증서
인증서
상호인증
소비자
인증
인증
인증
인증
인증센터 A
(키관리센터)
상점 A
소비자
인증센터 B
(키관리센터)
상점 B
초고속인증망
전자상거래 보안
83