소액지불시스템인 Millicent에 관한 연구

박정선, 김동우 (명지대학교 산업공학과)

요약문

전자상거래는 거래의 많은 부분을 차지할 수 있는 잡지, 신문, 음악, 소프트웨어 등의 거래에 필요한 소액 지불수단이 필요하다. 이러한 요구조건을 만족시기 위해서는 과도한 암호화 부담을 줄이고 처리비용을 낮추는 것이 필요한데 가장 잘 된 프로토콜로는 Millicent가 꼽인다. 본 연구에서는 Millicent의 구현 방안에 대하여 고려해 본다.

발표 순서

1. 개요
2. 전자 상거래 지불방식
3. 암호화 방식
4. Millicent
5. Millicent 구현
6. Millicent 보안
7. Millicent 활용방안
8. 결론 및 추후 연구과제

명지대학교 MYONGJI UNIVERSITY

1. 개 요

	현재		2002년
전자상거래 규모	8백억 달러	⇨	4천억 달러 예견
전세계 인터넷 사용자수	1억명	⇨	3억 2천만명 예상
온라인 구매자 수	1천 8백만명	⇨	1억 2천 8백만명 예상

⇩

전자지불 시스템 요구

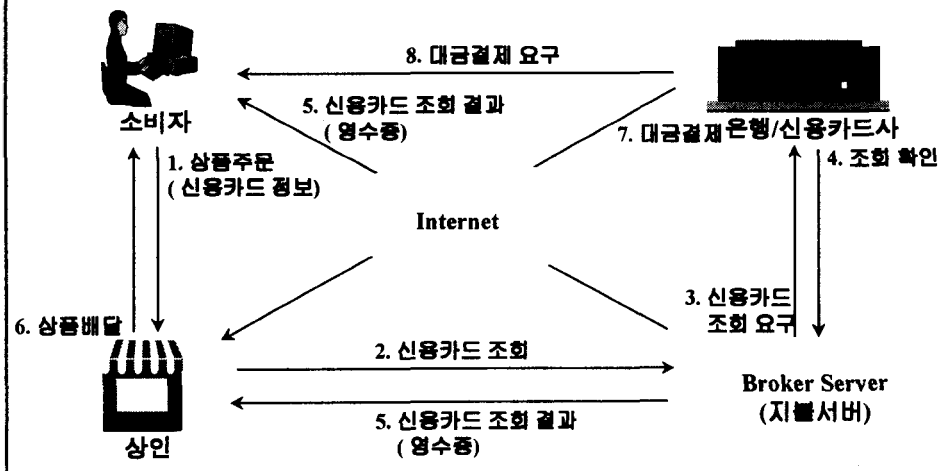
명지대학교 MYONGJI UNIVERSITY

2. 전자 상거래 지불방식

가입자 기반 방식	• 사용자와 상인간의 가장 간단한 모델 • 사용자는 상인계좌에 등록 • 계좌관리에 많은 오버헤드 발생
트랜잭션 처리 방식	• 가입자 방식과 유사 • 계좌관리의 오버헤드를 줄이기 위해 • 어느 정도의 금액에 이르면 결제

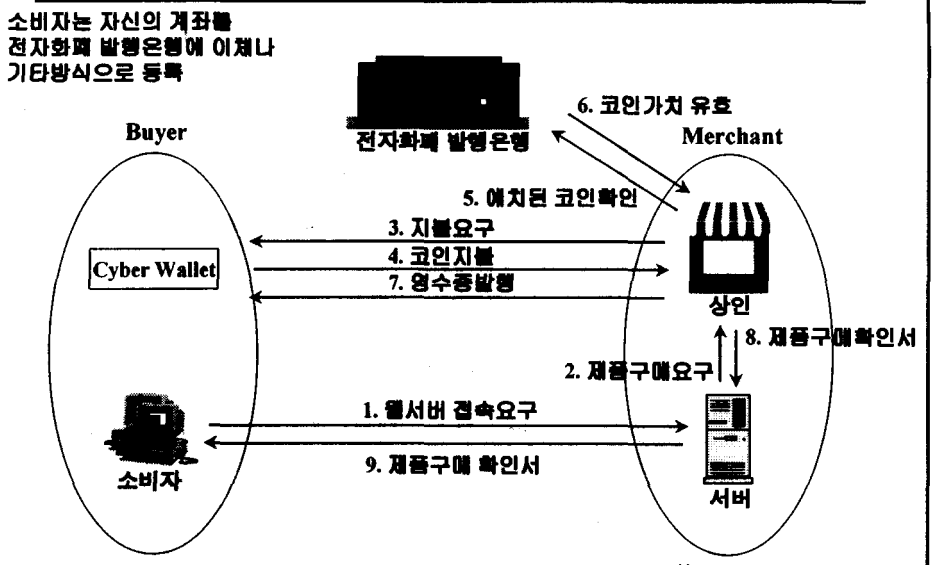
명지대학교 MYONGJI UNIVERSITY

2. 전자 상거래 지불방식(신용카드방식)



명지대학교 MYONGJI UNIVERSITY

2. 전자 상거래 지불방식(전자 화폐 시스템)



명지대학교 MYONGJI UNIVERSITY

2. 전자 상거래 지불방식

신용카드방식	• 신용카드를 이용한 방식은 소비자나 상인 를 다 유리 • 결제비용이 높다 • 자신의 카드정보에 대해 보안사항 요구
전자화폐 시스템	• 인증된 중앙서버에 의해 발행 • 인증은 화폐 발행 기관의 전자서명을 통해 이뤄진다.

명지대학교 MYONGJI UNIVERSITY

3. 암호화 방식

대칭키 암호화 방식

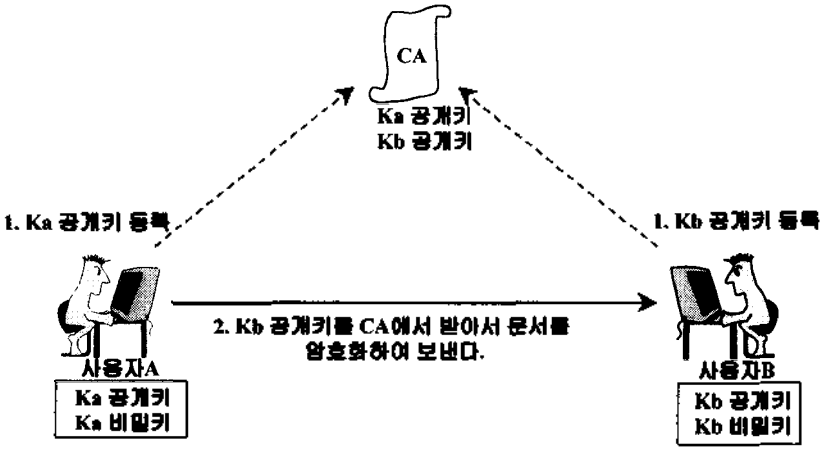
- 암호화 하는 키와 복호화 하는 키가 같다.
- 복수의 사용자가 같은 자료를 공유할 때, 키 분배문제 발생
- DES, SKIPJACK, IDEA 방식 등이 있다.

비대칭키 암호화 방식

- 일명 공개키 암호화방식
- 대칭키 암호화 방식에서 키 분배문제와 인증문제를 해결할 목적으로 개발
- 비밀키는 메시지 송수신에 관련된 모든 사람들이 개인적으로 비밀보관
- 공개키는 공개된 인증기관에 보관하여 자신이 원하는 공개키 획득가능

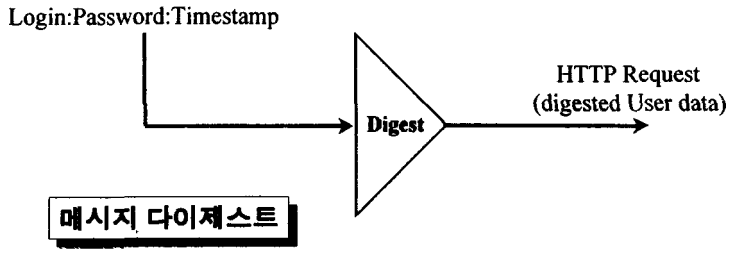
명지대학교 MYONGJI UNIVERSITY

3. 암호화 방식(공개키 방식)



명지대학교 MYONGJI UNIVERSITY

3. 암호화 방식



메시지 다이제스트

- 일방향 특성을 갖는 메시지 다이제스트 방식을 적용하여, 사용자 정보를 암호화하여 전송하는 방식 (사용자ID 및 패스워드 정보)
- MD5와 같은 일방향 함수를 사용하여 다이제스트 하여 전송하면 서버에 이미 저장되어 있는 정보와 비교하여 사용자를 인증
- 재연(Replay)공격을 막기 위해 Timestamp 정보를 함께 보낸다.

명지대학교 MYONGJI UNIVERSITY

4. Millicent

1992년 10달러 미만의 현금 거래액은 1조 8천억 달러

▶ 신용카드 거래액 420억 달러의 4배

Millicent는 크게 5000원 정도에서 작게는 10원 미만의 소액정보 상품 구매

벤더와 구매자가 아주 작은 수준까지 세분화 가능

▶ 불필요한 정보의 구매 방지

구성요소

- 스크립
  선 지불된 만큼의 가치를 대신
  특정 서비스 벤더에게만 사용 가능한 일종의 전자수표
  브로커가 발행 - 1회 사용가능
- 브로커
  복수의 서비스 벤더를 대신하여 스크립을 만드는 대리인

명지대학교 MYONGJI UNIVERSITY

4. Millicent

- 벤더
  정보나 서비스를 파는 상점

  특성
- 처리비용
  과도한 암호화 트랙잭션 부담을 줄임
  하나의 소형 웹서버 만으로 하루 250만건의 소액거래 처리
- 계정관리비
  모든 금액처리 및 계정관리를 브로커가 대신
- 신용부담
  선불 계정 방식
- 통신비용
  계정확인이 즉각적으로 이루어진다.

명지대학교 MYONGJI UNIVERSITY

4. Millicent

Vendor	Value	ID#	Cust ID#	Expires	Props

스크립의 구조

- Vendor : 스크립을 발행한 Vendor ID
- Value : 스크립의 화폐가치
- ID# : 스크립의 유일한 식별번호
- Cust ID# : 스크립을 사용하는 사용자 ID
- Expires : 스크립의 유효기간
- Props : 기타 데이터

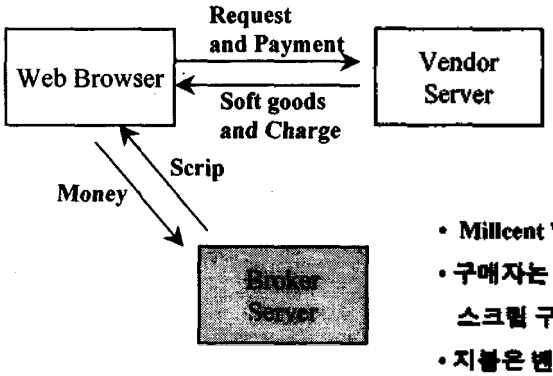
스크립의 특징

- 특정한 벤더와 거래가능
- 단 한번 사용가능
- 위조에 대해 보안성
- 정당한 사용자만이 지불가능
- 스크립을 생산, 확인하는 데 효율적

명지대학교 MYONGJI UNIVERSITY

4. Millicent

구매자 관점

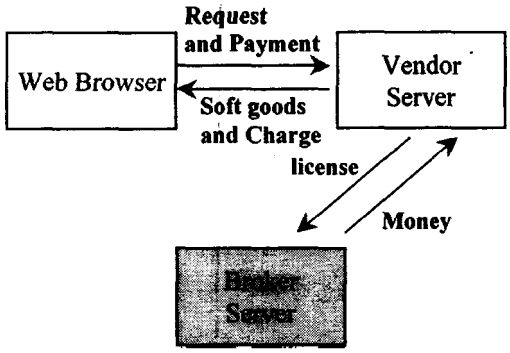


- Millcent Wallet은 스크립 소유
- 구매자는 브로커로부터 실제금액으로 스크립 구입
- 지불은 벤더와 양방향 가능

명지대학교 MYONGJI UNIVERSITY

4. Millicent

벤더 관점

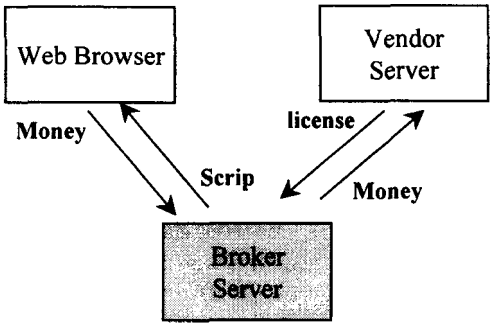


- 벤더의 브로커 선택기준
  (브로커비용과 서비스, 지급빈도)
- 벤더는 스크립을 판매하기 위해 브로커와 License
- 벤더 서버
  - 가격관리
  - 스크립의 타당성 확인
  - 타 웹서버와 연동
- 브로커는 팔린 스크립에 따라 벤더에게 지불

명지대학교 MYONGJI UNIVERSITY

4. Millicent

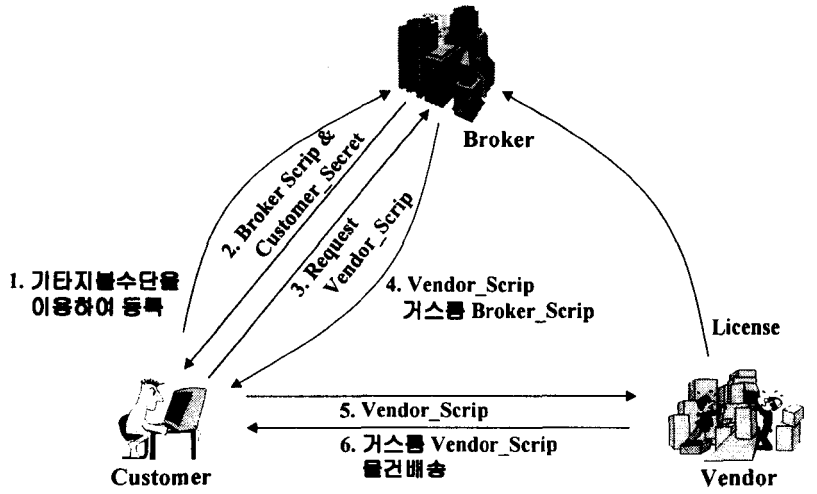
브로커 관점



- 브로커는 중간 매개체
- 구매자는 수 천개의 벤더와 각각 거래할 필요없음
- 벤더는 수 백만명 의 구매자와 각각 거래할 필요없음
- 금융기관과 Internet access provider 가 좋은 브로커

명지대학교 MYONGJI UNIVERSITY

4. Millicent



명지대학교 MYONGJI UNIVERSITY

5. Millicent 구현

개발환경	개발도구
OS	Windows NT 4.0 (Service Pack 3)
DBMS	MSSQL 6.5
개발도구	ACTIVE CONTROL PAD, INTERDEV 1.0
암호화 알고리즘	MD5, DES
LANGUAGE	VISUAL BASIC 5.0, VISUAL C++ 5.0 JAVA SCRIPT
WEB SERVER	IIS 3.0

명지대학교 MYONGJI UNIVERSITY

5. Millicent 구현

가상 시나리오

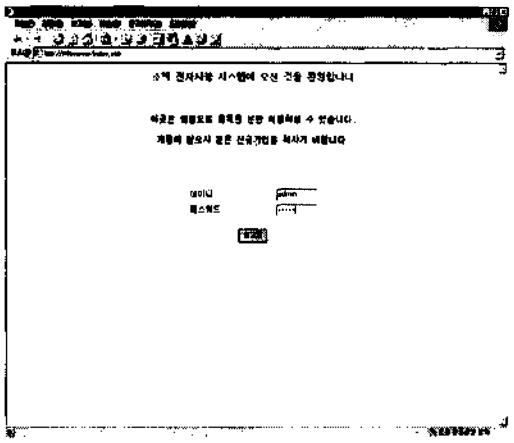
1. Broker Server에서 Web client에게 스크립을 MD5를 사용해서 보낸다.

   • 데이터의 기밀성 유지 ⇨ DES

   • 데이터의 위조,변조 방지 ⇨ MD5

명지대학교 MYONGJI UNIVERSITY

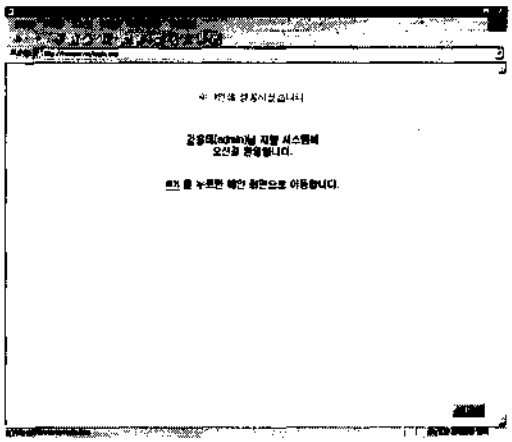
5. Millicent 구현



• 전자지불 시스템
로그인 화면

명지대학교 MYONGJI UNIVERSITY

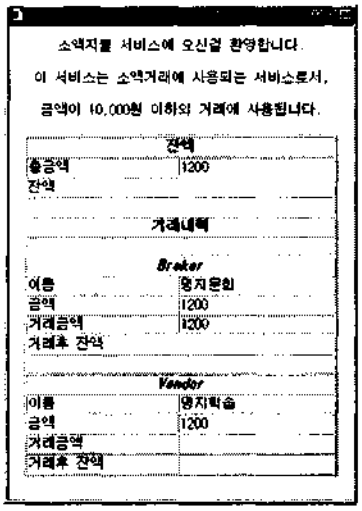
5. Millicent 구현



• 로그온
성공화면

명지대학교 MYONGJI UNIVERSITY

5. Millicent 구현

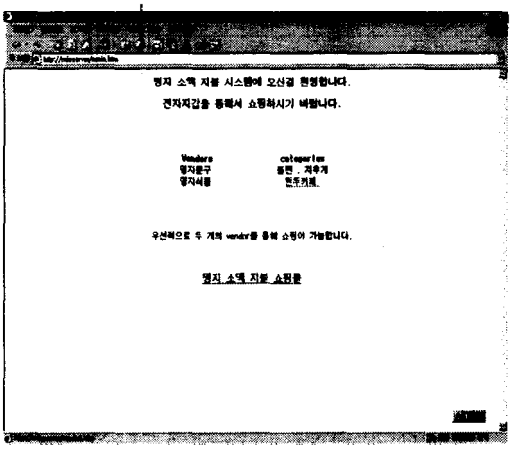


전자지갑 내용

- 잔액
- 거래내역

명지대학교 MYONGJI UNIVERSITY

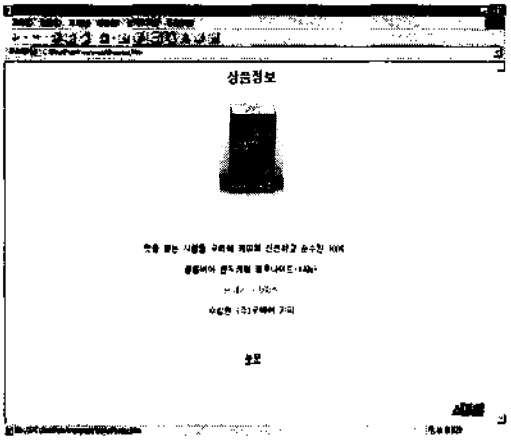
5. Millicent 구현



- 메장 메인 화면

명지대학교 MYONGJI UNIVERSITY

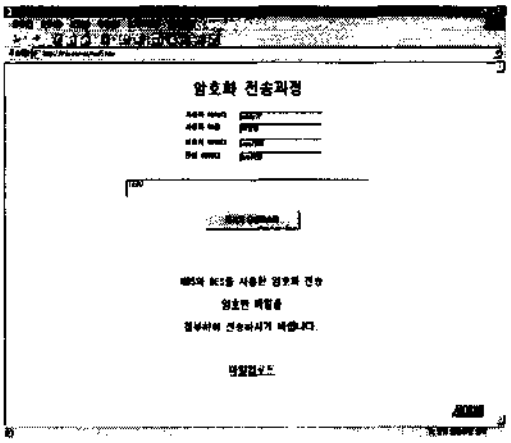
5. Millicent 구현



- 상품주문 화면

명지대학교 MYONGJI UNIVERSITY

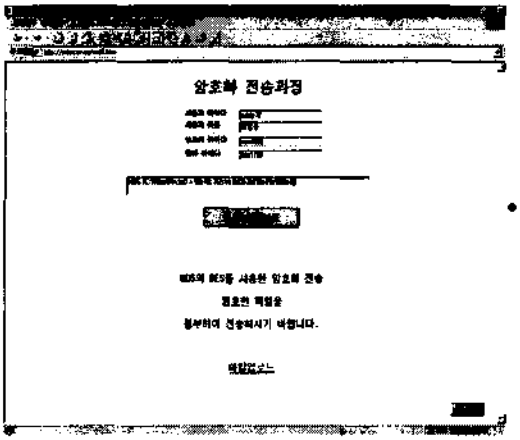
5. Millicent 구현



- MD5로 메시지 다이제스트 하는 과정

명지대학교 MYONGJI UNIVERSITY

5. Millicent 구현



- MD5로 메시지 다이제스트 된 결과

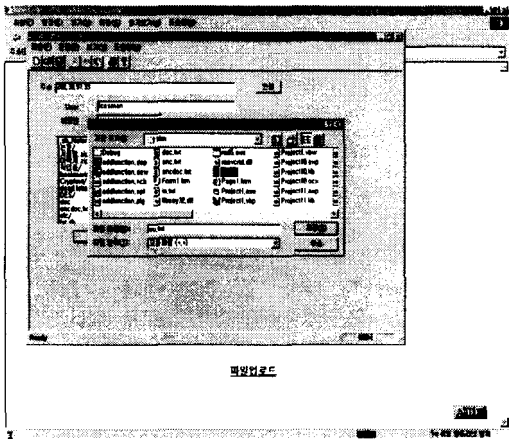
명지대학교 MYONGJI UNIVERSITY

5. Millicent 구현

- 다이제스트 한 파일을 DES로 암호화 시키는 과정

명지대학교 MYONGJI UNIVERSITY

5. Millicent 구현



- 메시지 다이제스트 한 파일을 브로커 서버로 전송과정

명지대학교 MYONGJI UNIVERSITY

6. Millicent 보안

이중 사용방지	⟷	Scrip의 일련번호
Replay Attack 방지	⟷	Timestamp
Scrip 위조,변조방지	⟷	Certificate
사기 위험방지	⟷	Scrip의 거래가 소액
주문서 변조방지	⟷	전자서명
Scrip의 소유권증명	⟷	소유자의 비밀키사용
메시지의 기밀성	⟷	DES

명지대학교 MYONGJI UNIVERSITY

7. Millicent 활용방안

웹상의 정보 제공자들

전통적인 출판자	Web 기반의 Content 제공자	자가 출판자
• Newspapers	• Applet 개발자	• Personal 에세이
• Magazines	• Search engines	• Subject indexes
• Directories	• Rating services	• 주석을 첨부한 hot lists
• Newsletters	• e-zines	• Personalized newsgroup moderation
• News feeds	• Serialized soaps	• How-To Guides
• Academic journals	• Games	
• Book publishers	• Entertainment	

명지대학교 MYONGJI UNIVERSITY

8. 결론 및 추후 연구과제

- 브로커와 사용자, 벤더간의 거래에서 스크립의 기밀성 문제
  - DES를 이용한 기밀성 문제해결
- 추후, DES 상에서 키 분배 문제 해결을 위해
  - 공개키 방식을 이용한 인증기관의 인증에 따라 상방 간의 안전한 거래방식 요구

명지대학교 MYONGJI UNIVERSITY