
9. SSL/TLS, 인터넷뱅킹 및 전자결제

담당교수: 차 영욱
ywcha@andong.ac.kr

목 차

□ SSL/TLS 보안 프로토콜

- 핸드셰이크 프로토콜
- 암호사양 변경 프로토콜
- 경고 프로토콜
- 레코드 프로토콜

□ 인터넷뱅킹

- 인터넷뱅킹의 개요 및 접속 절차
- 금융기관별 ActiveX 설치 현황

□ 전자상거래 절차 및 결제

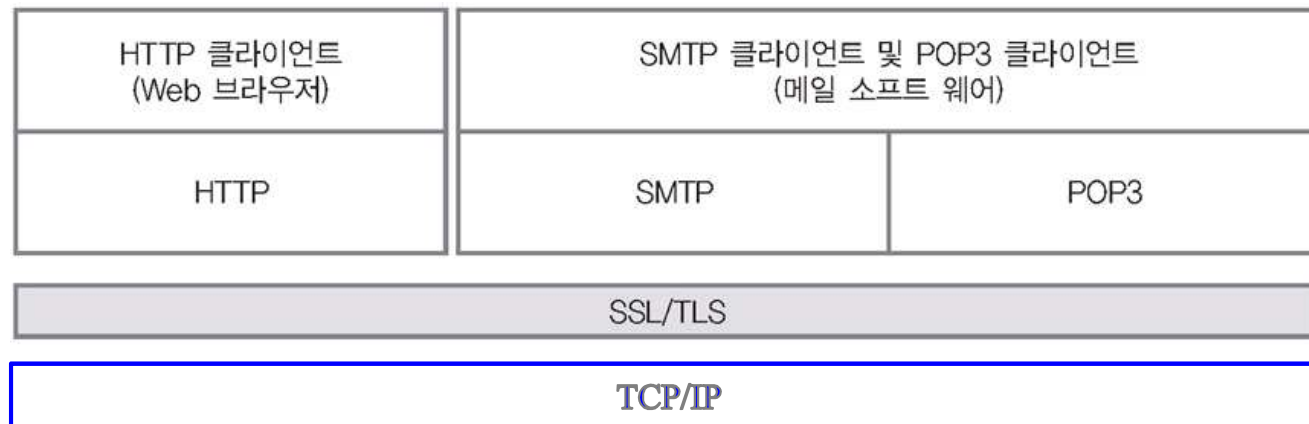
- 비자 안심클릭
- 안전결제(ISP)



SSL/TLS 보안 프로토콜

□ 보안소켓 계층(SSL: Secure Socket Layer)

- 1993년 웹 서버와 브라우저 사이의 안전한 통신을 위하여 Netscape 사에서 개발 → **현재 많은 웹 브라우저에서 사용되어 사실상의 업계 표준**
- HTTP뿐만 아니라 메일 전송을 위한 SMTP나, 메일 수신을 위한 POP3(Post Office Protocol) 같은 프로토콜이 SSL/TLS 상에서 동작할 수 있음



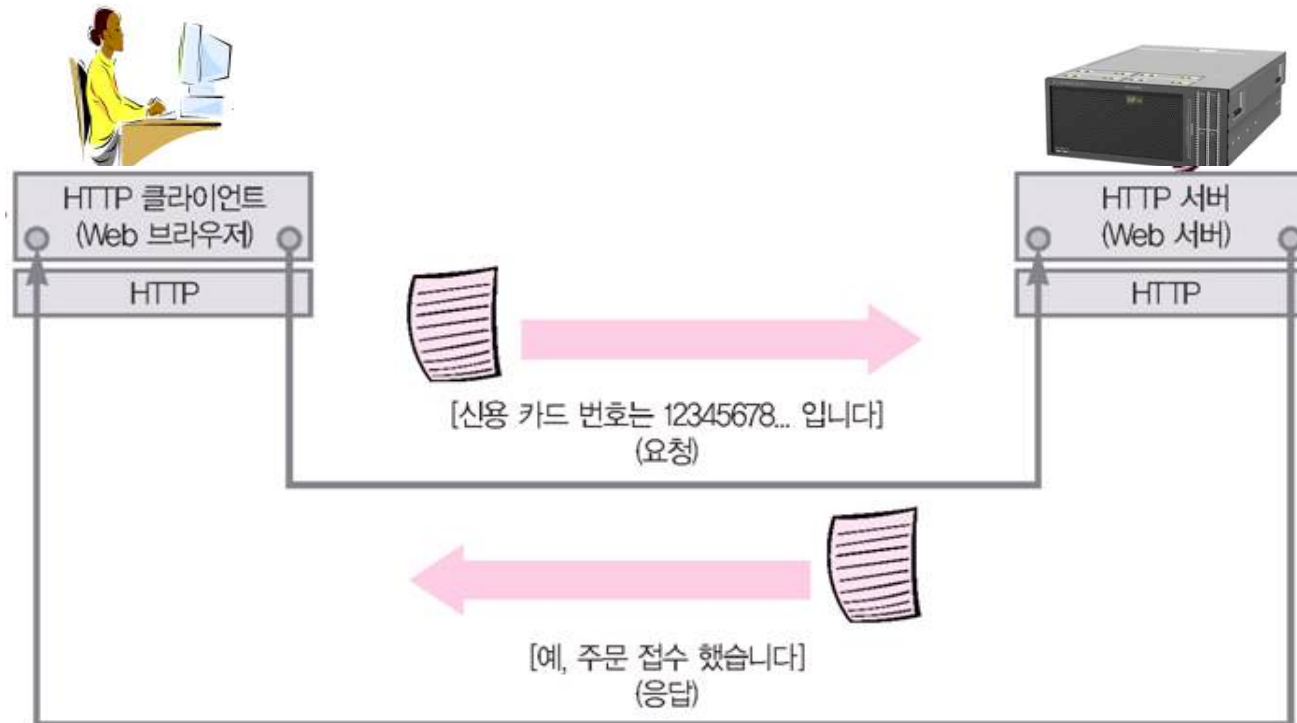
□ 트랜스포트 계층 보안(TLS: Transport Layer Security)

- 1996년 발표된 SSL 버전 3.0을 기반으로 1999년 IETF가 TLS1.0(SSL3.1) 규격인 RFC2246 발표

SSL/TLS를 사용하지 않은 HTTP 통신

□ 인터넷 서점에 영심이가 책을 주문

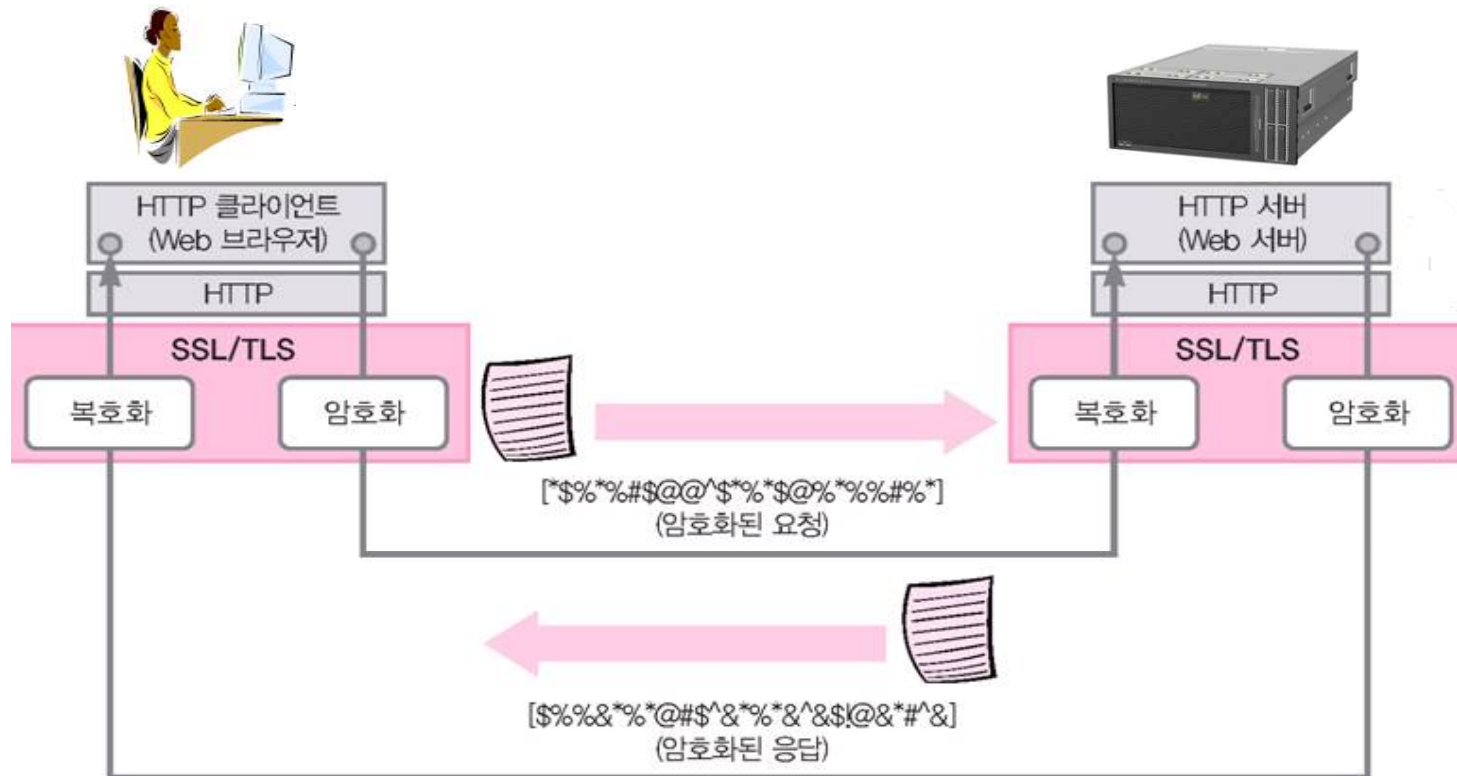
- SSL/TLS를 사용하지 않고 웹 브라우저에서 웹 서버로 신용카드 번호를 보냈을 경우에 **네트워크 상에 신용카드 번호가 노출**



SSL/TLS를 사용하는 HTTP 통신

□ 인터넷 서점에 영심이가 책을 주문

- HTTP를 SSL/TLS 상에 올려서 요청과 응답 메시지를 암호화 → 신용카드 번호의 노출을 방지할 수 있음

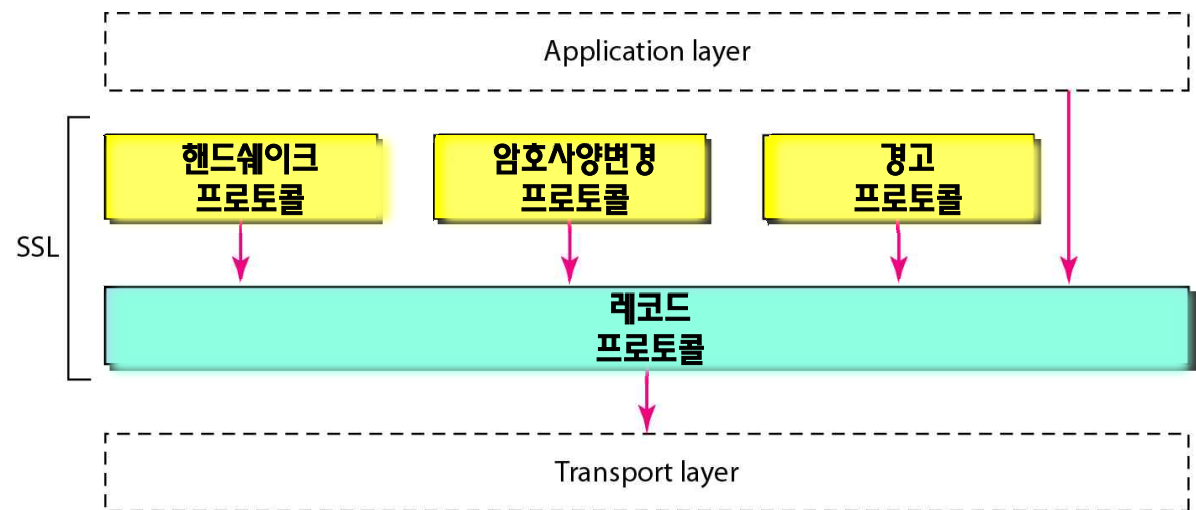


SSL/TLS의 보안 서비스 및 구조

- 인터넷 서점을 통한 책의 주문 시에 SSL/TLS가 제공하는 보안 서비스
 - **기밀성**: 주문자와 인터넷 서점이 교환하는 정보(예, 신용카드 번호와 주소)의 암호화
 - **무결성**: 공격자에 의하여 주문자와 인터넷 서점이 교환하는 정보의 위조나 변조 방지
 - **인증**: 주문자와 인터넷 서점의 상호 확인

- SSL 프로토콜의 구조

- 핸드셰이크(Handshake) 프로토콜
- 암호사양변경(Change Cipher Spec) 프로토콜
- 경고(Alert) 프로토콜
- 레코드(Record) 프로토콜



핸드셰이크와 암호사양 변경 프로토콜

□ 단계 1~단계 3: 핸드셰이크 프로토콜

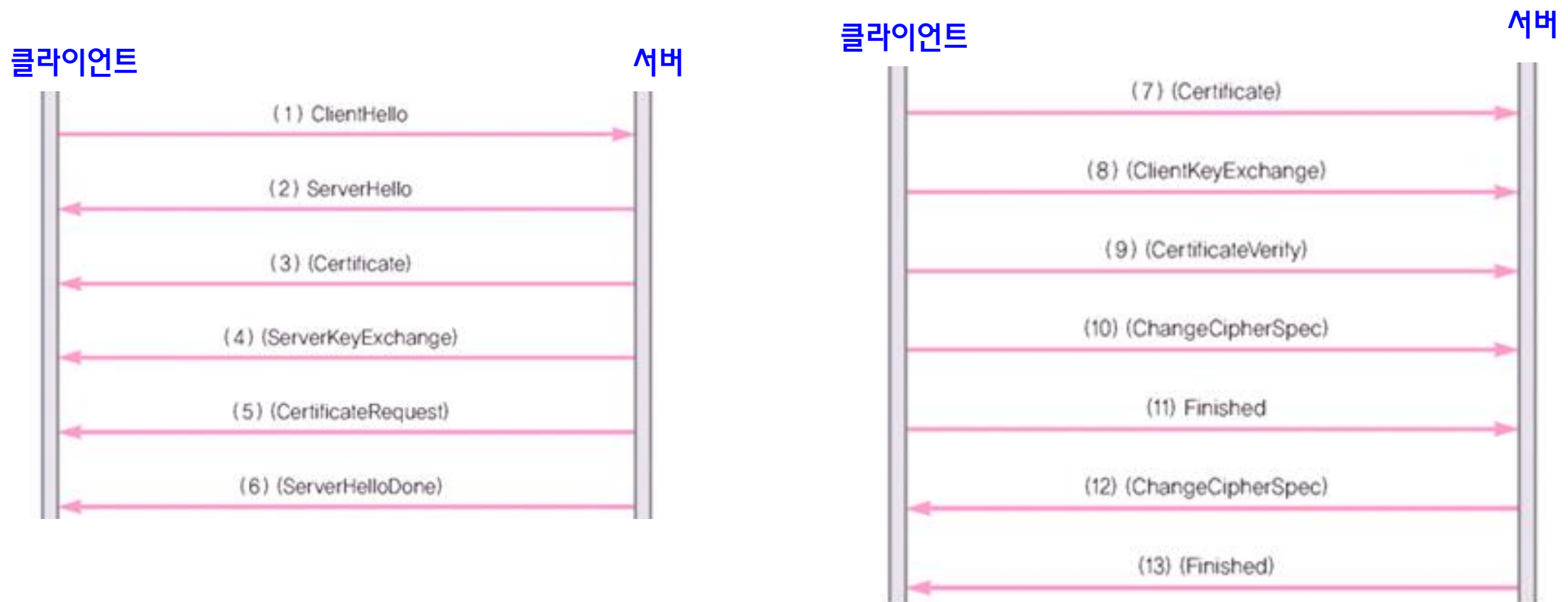
- 클라이언트와 서버가 통신에 사용할 암호 및 인증 알고리즘과 공유 키를 결정하기 위한 암호 스위트(cipher suite) 교환
- 인증서를 이용하여 상호 인증

□ 단계 4: 암호사양변경 프로토콜의 메시지를 교환하므로 이전 단계에서 협의된 암호 스위트의 적용을 개시한다.



핸드셰이크와 암호사양 변경 프로토콜 절차

- ❑ 단계 1(보안능력의 설정): 메시지 1,2
- ❑ 단계 2(서버 인증 및 키 교환): 메시지 3,4,5,6
- ❑ 단계 3(클라이언트 인증 및 키 교환): 메시지 7,8,9
- ❑ 단계 4(암호사양 변경 메시지 교환 및 핸드셰이크 종료): 메시지 10,11,12,13



단계 1: 보안 능력의 설정

□ (1)ClientHello(클라이언트→서버)

□ (2)ServerHello(클라이언트←서버)

- 사용할 수 있는 버전 번호, 현재 시각, 랜덤 값, 세션 ID
- 사용할 수 있는 암호 스위트(cipher suite) 목록

➤ 키 교환 방법:

- ✓ RSA: 사전마스터 비밀 값(premaster secret)이 수신자의 공개키로 암호화되어 전달
- ✓ Fixed Diffie-Hellman: 인증된 공개키 파라미터 값 교환
- ✓ Anonymous Diffie-Hellman: 인증 없이 공개키 파라미터 값 교환

➤ 암호 명세(CipherSpec): 암호 알고리즘(DES, 3DES, AES), 해시 알고리즘(SHA, MD5)

- 사용할 수 있는 압축 방법



단계 2: 서버 인증 및 키 교환

- ❑ (3)Certificate(클라이언트←서버): 클라이언트가 수행하는 서버의 인증을 위하여 서버의 X.509 인증서를 전달
 - 단계 1에서 설정된 키 교환 방법이 **Fixed Diffie-Hellman**인 경우 → 인증기관에 의하여 서명된 **인증서로 공개키 파라미터 값 교환**
- ❑ (4)ServerKeyExchange(클라이언트←서버)
 - 단계 1에서 설정된 암호 스위트의 키 교환 방식에 따라서 다음과 같은 키 값 교환
 - **RSA**: 암호화한 사전마스터 비밀 값
 - **Anonymous Diffie-Hellman**: 공개키 값
- ❑ (5)CertificateRequest(클라이언트←서버): 클라이언트를 인증하기 위하여 클라이언트에게 인증서를 요청
- ❑ (6)ServerHelloDone(클라이언트←서버): ServerHello 메시지부터 시작해서 지금까지 교환된 메시지의 끝을 나타낸다.



단계 3: 클라이언트 인증 및 키 교환

□ (7)Certificate(클라이언트→서버)

- 서버로부터 (5)CertificateRequest 메시지가 왔을 경우에 클라이언트의 인증서를 전달하는 메시지
- 단계 1에서 설정된 키 교환 방법이 Fixed Diffie-Hellman인 경우 → 인증서로 공개키 파라미터 값 교환

□ (8)ClientKeyExchange(클라이언트→서버)

- 단계 1에서 설정된 암호 스위트의 키 교환 방식에 따라서 다음과 같은 키 값 교환
 - RSA: 서버 인증서에 있는 공개키로 암호화한 사전마스터 비밀 값
 - Anonymous Diffie-Hellman: 공개키 값

□ (9)CertificateVerify(클라이언트→서버)

- 마스터 비밀키 값과 핸드셰이크 메시지들의 결합에 대한 해쉬 함수 값(전자 서명)을 서버에게 전달하므로 클라이언트가 전달한 인증서를 보장하게 된다.



단계 4: 암호사양 변경 및 핸드셰이크 종료

❑ (10)ChangeCipherSpec(클라이언트→서버)

- 암호사양변경 프로토콜의 메시지를 교환하므로 이전 단계에서 협의된 암호 스위트의 적용을 개시한다.

❑ (11)Finished(클라이언트→서버)

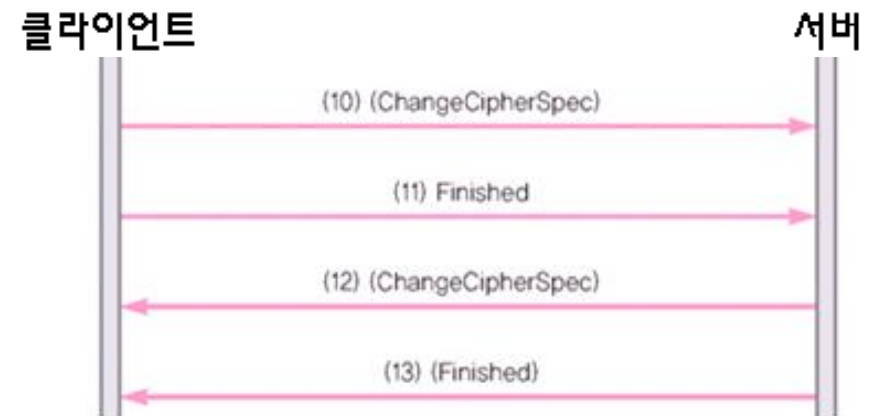
- 핸드셰이크의 종료를 통보하는 메시지

❑ (12)ChangeCipherSpec(클라이언트←서버)

- 암호사양변경 프로토콜의 메시지를 교환하므로 이전 단계에서 협의된 암호 스위트의 적용을 개시한다.

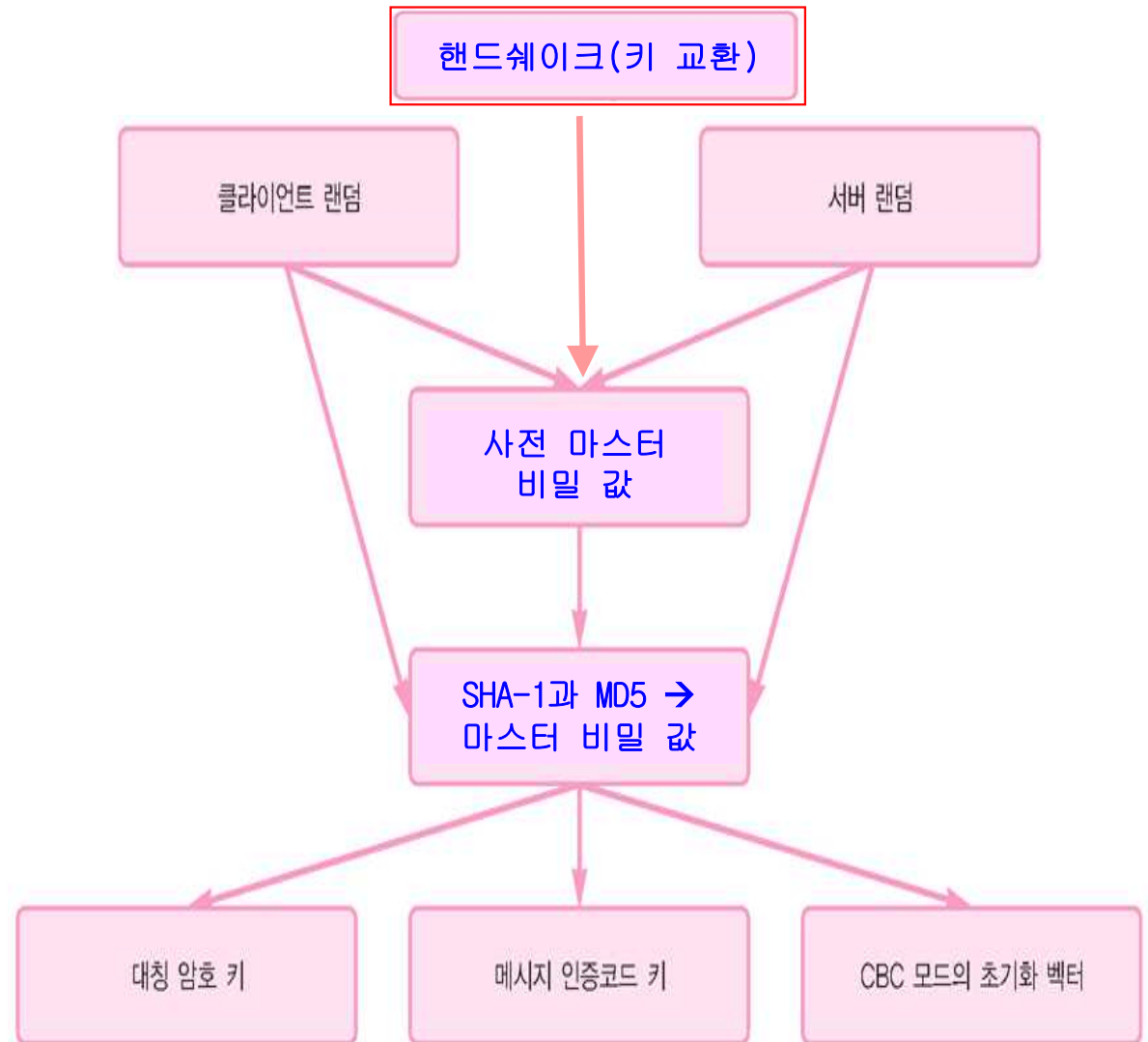
❑ (13) Finished(클라이언트←서버)

- 핸드셰이크의 종료를 통보하는 메시지



마스터 비밀 값

- ❑ RSA 또는 Diffie-Hellman 키 교환
→ 사전마스터 비밀 값(premaster secret) 생성 → SHA-1과 MD5
해시함수를 이용한 **48바이트의 마스
터 비밀 값 (master secret) 생성**
- ❑ 마스터 비밀 값은 SSL/TLS 통신의
대칭암호 키와 CBC(Cipher Block
Chaining) 모드에 이용하는 **초기백
터** 그리고 메시지 인증에 사용되는
비밀키의 생성에 이용된다.



마스터 비밀 값과 키 블록 생성

```
master_secret = MD5(pre_master_secret || SHA( 'A' || pre_master_secret ||
ClientHello.random || ServerHello.random)) ||
MD5(pre_master_secret || SHA( 'BB' || pre_master_secret ||
ClientHello.random || ServerHello.random)) ||
MD5(pre_master_secret || SHA( 'CCC' || pre_master_secret ||
ClientHello.random || ServerHello.random))
```

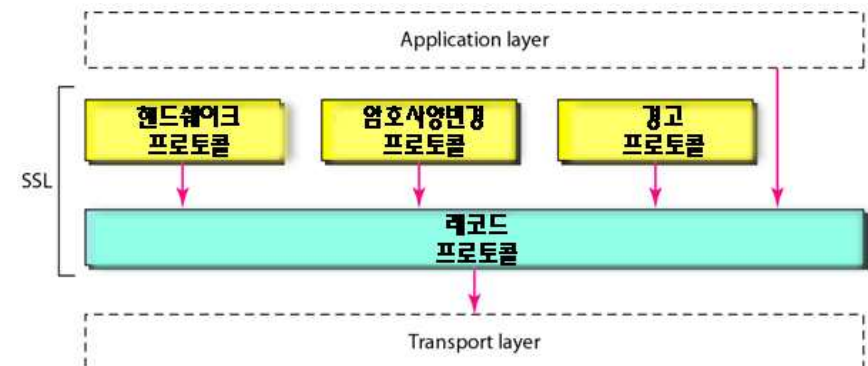
- SSL/TLS 통신의 **대칭암호 키**와 CBC 모드의 **초기벡터** 그리고 메시지 인증의 **비밀키**에서 요구되는 충분한 길이의 키 블록이 생성될 때까지 master secret을 해싱하게 된다.

```
Key_block = MD5(master_secret || SHA( 'A' || master_secret ||
ServerHello.random || ClientHello.random)) ||
MD5(master_secret || SHA( 'BB' || master_secret ||
ServerHello.random || ClientHello.random)) ||
MD5(master_secret || SHA( 'CCC' || master_secret ||
ServerHello.random || ClientHello.random)) || . . .
```

경고 프로토콜

□ SSL/TLS 통신 중에 발생한 에러를 전달하는 프로토콜

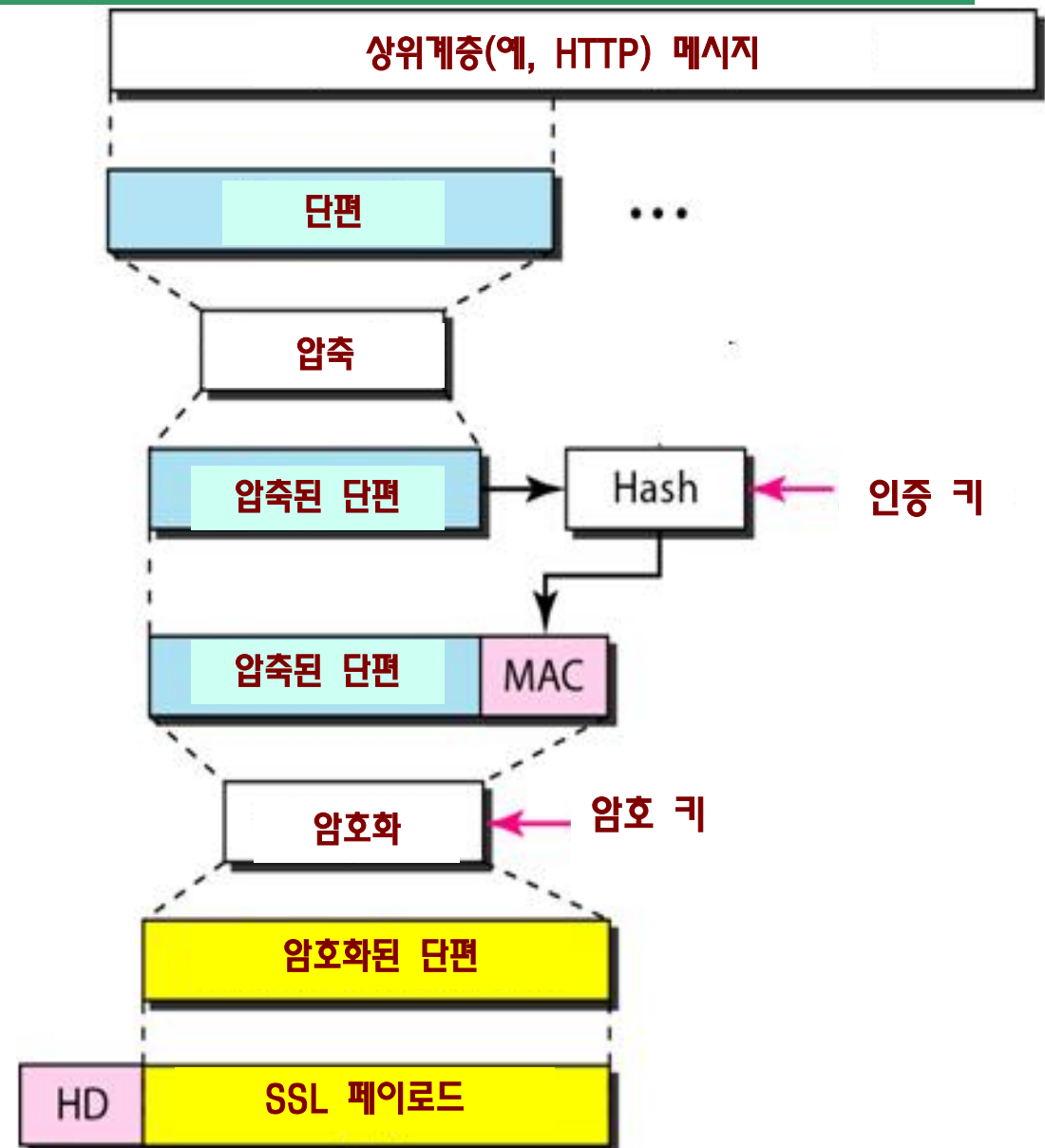
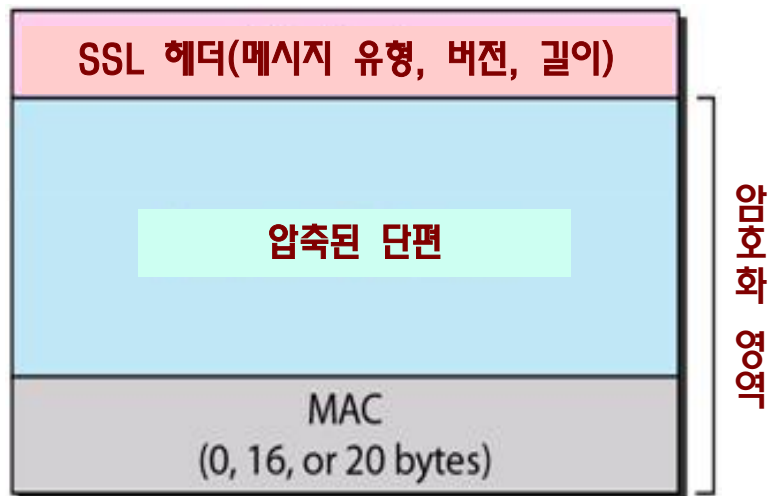
- 기대하지 않은 메시지의 수신(unexpected_message)
- 잘못된 메시지 인증코드(bad_record_mac)
- 압축해제 실패(decompression_failure)
- 핸드셰이크 실패(handshake_failure)
- 잘못된 파라미터의 사용(illegal_parameter)
- 인증서 없음(no_certificate)
- 잘못된 인증서(bad_certificate)
- 지원되지 않는 유형의 인증서(unsupported_certificate)
- 폐지된 인증서(certificate_revoked)
- 인증서의 유효기간 경과(certificate_expired)
- 알수 없는 유형의 인증서(certificate_unknown)



레코드 프로토콜

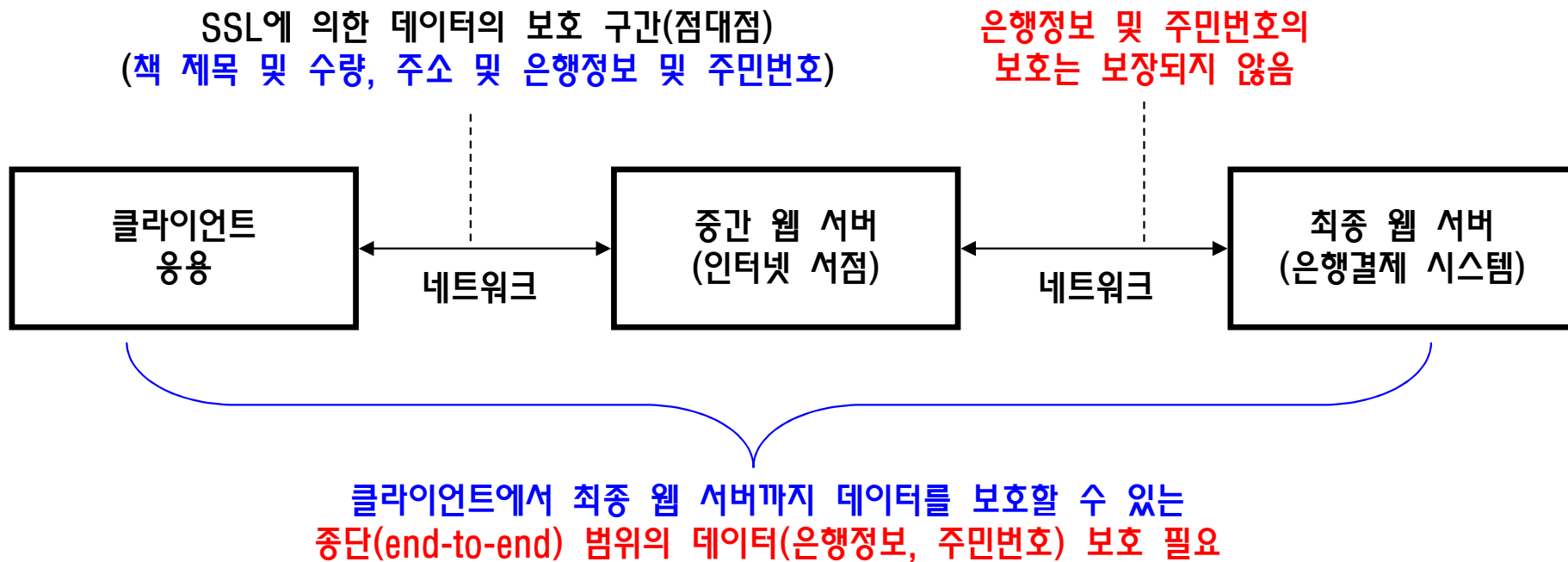
- ❑ 서버와 클라이언트가 핸드셰이크 프로토콜을 사용해서 결정한 알고리즘과 키 값을 이용하여 **대칭 암호화/복호화**와 **메시지 인증코드(MAC)**를 생성한다.

- ❑ SSL 메시지




SSL 보안의 한계

- ❑ SSL은 **점대점(point-to-point) 범위**로 데이터를 보호할 수 있지만 중간 웹 서버를 통해서 다시 전달(forwarding) 되는 데이터의 보호는 보장되지 않음 → 응용 계층에서의 암호화를 통한 **중단 범위의 암호화**가 요구됨
- ❑ 전체 메시지를 암호화/복호화하는 오버헤드 문제 → XML(eXtensible Markup Language)의 보안을 이용하여 필요한 정보만을 암호화



응용 계층에서의 XML 암호화

- ❑ 책을 주문하기 위한 XML 메시지 
- ❑ XML 암호를 사용해서 신용카드 번호에 해당하는
엘레먼트만을 암호화 한 XML 메시지



```
<?xml version='1.0'?>
<PurchaseOrder>
  <Cart>
    <Item>
      <Title>Developing Enterprise Web Services:
        An Architect' s Guide</Title>
      <Quantity>210</Quantity>
    </Item>
  </Cart>
  <Payment>
    <PaymentType>VISA</PaymentType>
    <Number>123456789000</Number>
    <Expiration>01-23-2024</Expiration>
  </Payment>
</PurchaseOrder>
```

```
<?xml version='1.0'?>
<PurchaseOrder>
  <Cart>
    <Item>
      <Title>Developing Enterprise Web Services</Title>
      <Quantity>21</Quantity>
    </Item>
  </Cart>
  <Payment>
    <PaymentType>VISA</PaymentType>
    <Number>
      <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
        Type='http://www.w3.org/2001/04/xmlenc#Content'>
        <CipherData>
          <CipherValue>A23B45C56</CipherValue>
        </CipherData>
      </EncryptedData>
    </Number>
    <Expiration>01-23-2024</Expiration>
  </Payment>
</PurchaseOrder>
```

신용카드 번호
암호문

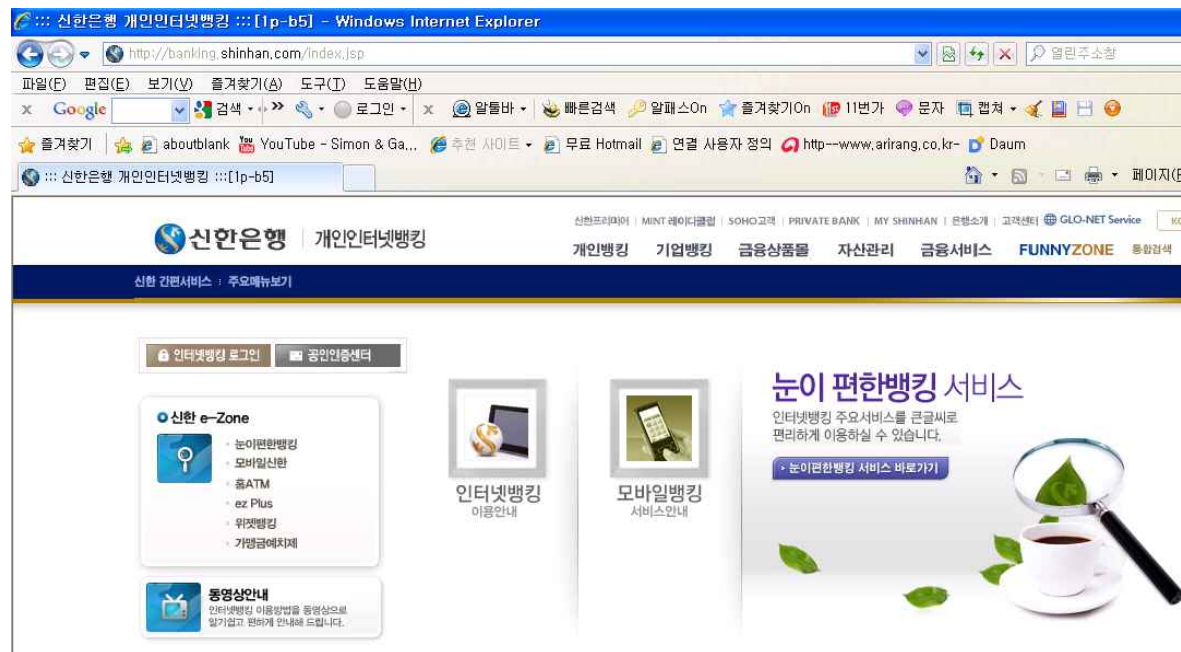
인터넷뱅킹의 개요

□ 세계 최초의 인터넷뱅킹

- 1995년 10월: 시큐리티퍼스트 네트워크은행(SFNB)

□ 한국 최초의 인터넷뱅킹

- 1997년: 미래산업(주) – 인터넷뱅킹 시스템 개발
- 2000년부터 대부분의 은행들이 인터넷뱅킹 시스템 구축



인터넷뱅킹 가입 및 인증서 발급

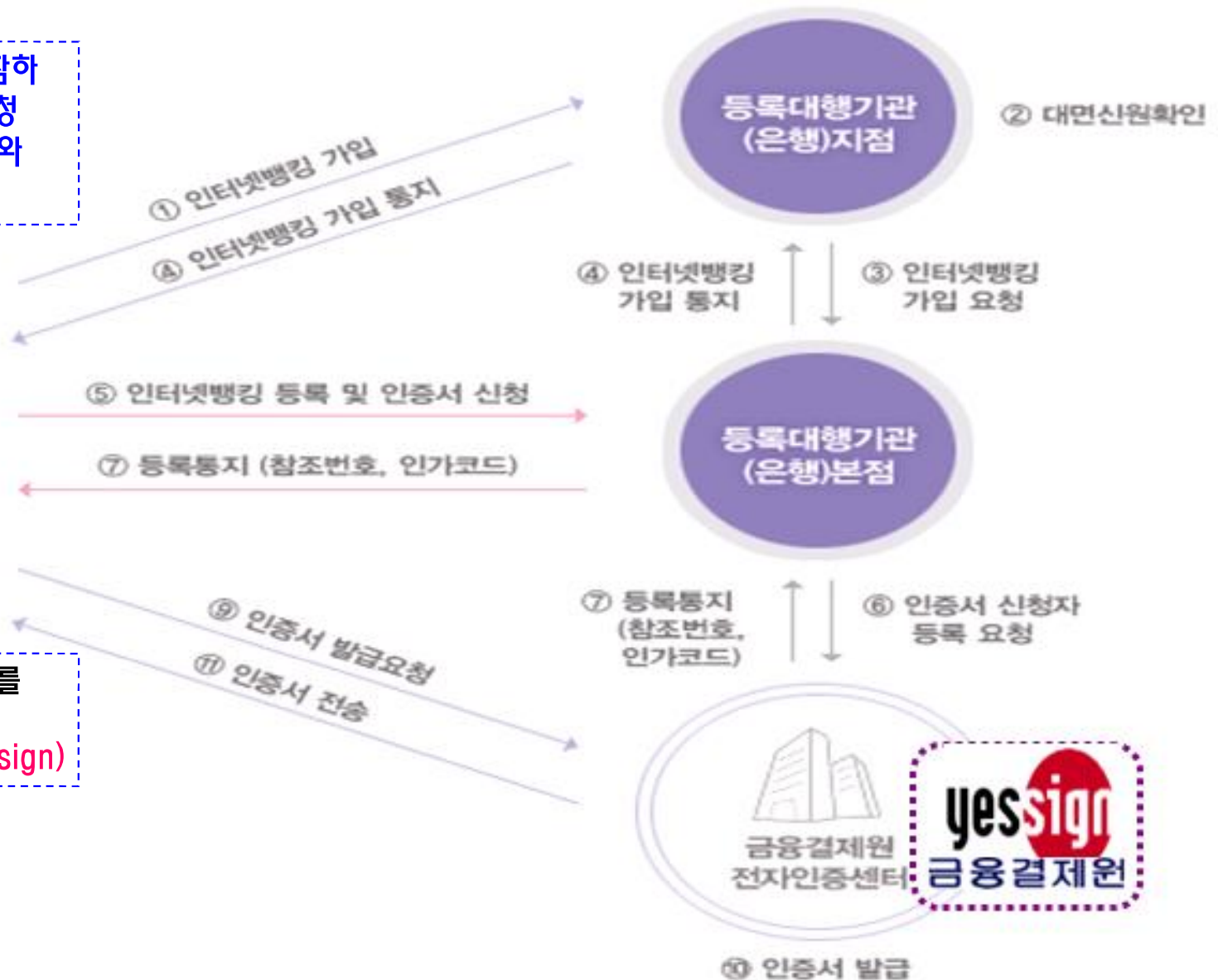
- 신분증, 도장, 통장을 지참하여 은행에 인터넷뱅킹 신청
- 은행은 고객에게 고객 ID와 패스워드 카드 발급



가입자

⑧ 키 쌍 및 인증서 발급요청 메시지 생성

인증기관은 인증서와 개인키를
고객의 컴퓨터에 설치
(C:\Program Files\NPKI\yessign)



공인 인증서(yessign) 발급(1)

① 신한은행(<http://banking.shinhan.com>) 접속 → 공인인증 선택

② 보안 모듈 설치



공인 인증서(yessign) 발급[2]

③ 공인인증센터로 이동

신한은행 | 개인인터넷뱅킹

신한프리미어 | MINT 레아디클럽 | SOHO고객 | PRIVATE BANK | MY SH

개인뱅킹 기업뱅킹 금융상품물 자산관리

신한 간편서비스 : 주요메뉴보기

인터넷뱅킹 로그인 **공인인증센터**

인터넷뱅킹 이용안내

영업점에서 인터넷뱅킹을 가입하신 고객중

- 인증서 발급이 처음인 경우
- 타행/타기관 인증서를 사용하는 경우
- 유의사항 확인하기 (꼭 읽어보세요)
- 유의사항 동영상 보기

인터넷뱅킹에 대한 전반적인 이용안내를 원하시는 경우

- 인터넷뱅킹 이용안내 바로가기

신한 e-Zone

- 눈이편한뱅킹
- 모바일신한
- 홈ATM
- ez Plus
- 위젯뱅킹
- 가맹금예치제

동영상안내

인터넷뱅킹 이용방법을 동영상으로 알기 쉽고 편하게 안내해 드립니다.



④ 공인인증서 발급/재발급 클릭

신한은행 | 개인인터넷뱅킹

신한프리미어 | MINT 레아디클럽 | SOHO고객 | PRIVATE BANK | MY SHINHA

개인뱅킹 기업뱅킹 금융상품물 자산관리

해당차단기작동중 100%

Today is 2010. 09. 30

개인 인터넷뱅킹 로그인

공인인증센터

- 은행/신용카드/보험용
- 전자거래범용(결제원)
- 전자거래범용(코스콤)
- 휴대폰인증서 서비스
- 타공인인증서 등록/해제
- 공인인증서 관리안내
- 신한S뱅크 공인인증서 가져오기

신한은행고객센터
무엇이든 물어보세요.
1577-8000

신계좌/구계좌 조회하기

공인인증서란

정부에서 인정한 공인인증기관이 발행하는 법적 효력을 가지고 있는 인증서입니다. 따라서 인터넷뱅킹 이용뿐만 아니라 각종 계약, 신청 등에 이용될 수 있습니다.

신한은행은 금융결제원과 코스콤(구증권전산원)의 인증등록기관으로서 공인인증서 등록/발급 관련지침을 준수하여 고객들에게 서비스를 제공하고 있습니다.

공인인증서 바로가기 선택해 주세요

공인인증서 발급/재발급 바로가기

처음 인터넷 뱅킹을 신청하신 고객
암호분실/인증서식재/PC를 포맷한 고객
인증서 유효기간 만료고객

공인인증서 갱신 바로가기

유효기간 만료 1개월 고객
갱신 안내를 받은 고객

전자세금공인인증서 바로가기

전자세금계산서를 발급받을 수 있는
전자세금 전용 공인인증서
바로가기

공인 인증서(yessign) 발급(3)

⑤ 약관 동의 체크 → **확인** 클릭

⑥ 공인 인증서 발급을 위해 주민등록번호, 출금계좌번호, 계좌비밀번호 입력 → **확인** 클릭

공인인증서 발급/재발급

01 약관동의 → 02 사용자 본인확인 → 03 보안카드/이체비밀번호입력 → 04 인증서암호및 저장위치선정 → 05 인증서 발급완료

은행/신용카드/보험용 공인인증서는 무료입니다.
한개의 인증서로 인터넷뱅킹 포함 모든 전자거래를 이용하실 수 있습니다.

Yessign 이용약관 전자금융거래 기본약관 신한온라인서비스 이용약관

제1장 총 칙

제1조 (목적)
이 약관은 전자서명법(이하 "법"이라 한다)에 의거 공인인증기관으로 지정받은 사단법인 금융결제원(이하 "결제원"이라 한다)이 제공하는 공인인증서비스(이하 "yessign서비스"라 한다)를 이용함에 있어 결제원과 가입자·이용자의 권리, 의무 및 책임사항을 정함을 목적으로 한다.

제2조 (정의)
① "가입자"라 함은 결제원으로부터 인증서를 발급받은 자를 말한다.
② "이용자"라 함은 가입자 인증서의 유효성을 확인하는 자를 말한다.

위 "Yessign 이용약관/전자금융거래 기본약관/신한온라인서비스 이용약관"에 동의 하십니까?

☒ 예, 동의합니다.

확인

공인인증서 발급/재발급

01 약관동의 → 02 사용자 본인확인 → 03 보안카드/이체비밀번호입력 → 04 인증서암호및 저장위치선정 → 05 인증서 발급완료

신한은행 인터넷뱅킹 고객만 공인인증서 발급/재발급이 가능합니다.

주민등록번호	00000000000000000000 [예] 123456-1234567
출금계좌번호	110 [예] 123123123456 (신한은행 계좌 '-'없이 입력)
계좌비밀번호	0000

기존 발급 받으신 인증서의 유효기간이 남아 있으면 재발급으로, 기타의 경우 발급으로 자동 유도 됩니다.
타행에서 이미 공인인증서를 발급 받으신 고객은 바로 로그인 하시면 등록 절차로 자동 유도 됩니다.

확인 **취소**

공인 인증서(yessign) 발급(4)

- ⑦ 보안카드 및 이체 비밀번호 입력(신규 발급 시 수수료 필요 - 재발급 시 불필요)
→ **확인** 클릭

공인인증서 발급/재발급 (코스콤 전자거래비용)

01 약관동의 → 02 사용자 본인확인 → 03 보안카드/이체비밀번호입력 → 04 인증서암호 및 저장위치선택 → 05 인증서 발급완료

* 아래 내용을 확인 및 입력 후 '확인' 버튼을 클릭 하십시오.
* 본인 확인을 위해 아래 정보를 정확히 입력하여 주십시오.

성명	이
공인인증서 발급수수료	4,400 원
이체비밀번호	●●●●●● (6~6자리이며, 5회이상 오류입력시 서비스가 제한됩니다.) ●●●●●● (일련번호 8자리 중 2, 4, 6 번째 숫자를 입력하여 주십시오.)
보안카드일련번호	 <p>▶ 보안카드 일련번호 입력 예시 예시: 일련번호 8자리 중 1, 3, 4 번째 숫자 1 ● 5 7 ● ● ● ● ● ●</p> <p>▶ 보안카드번호 입력 예시 예시1: 21번째 암호 중 앞 두자리 8 9 ● ● ● ● ● ● ● ● 예시2: 17번째 암호 중 뒤 두자리 ● ● ● ● 3 4</p> <p>• 본화면은 고객님의 이해를 돕기 위한 입력예시 참조 화면입니다. • 고객님의께서 보유하신 보안카드의 해당번호를 입력해 주시기 바랍니다.</p>
보안카드번호	22 번째 암호 중 앞 두자리 ●●●●●● 30 번째 암호 중 뒤 두자리 ●●●●●●를 입력하여 주십시오. (5회 이상 오류입력시 서비스가 제한됩니다.)
e-mail주소	naver.com [국] abs@shinhan.com
전화번호	010 [국] 02-1234-5678

[확인] [취소]

공인 인증서(yessign) 발급(5)

⑧ 공인 인증서 발급/재발급
→ 발급 클릭

⑨ 저장 매체 선택 → 확인 클릭
인증서 암호 입력 → 확인 클릭

공인인증서 발급/재발급 (코스콤 전자거래비용)



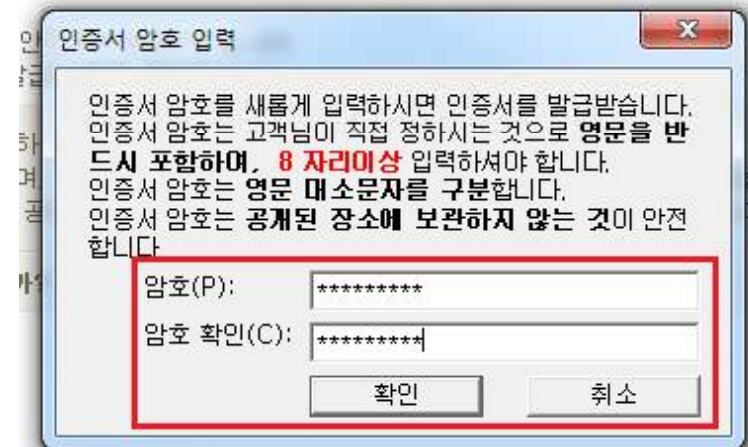
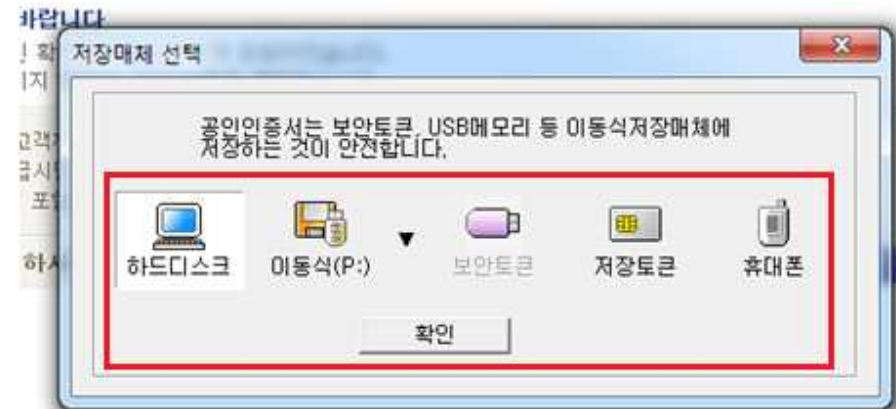
■ 아래 내용을 확인하시기 바랍니다

- 공인인증서 발급을 위한 본인 확인절차를 안전하게 종료하였습니다.
- 발급을 실행하시려면 본 페이지 하단의 '발급' 버튼을 클릭하십시오.

- 공인인증서 발급완료시 고객께서 제출하신 계좌에서 수수료 4,400원(부가세 포함)이 인출됩니다.
- 수수료는 최초로 신규발급시만 부과되며, 신규발급일로부터 1년 이내에 재발급하실 경우에는 부과되지 않습니다.
- 발급일로부터 7일(발급일 포함) 이내에 공인인증서 폐기신청을 하시면 발급시 수수료 인출 계좌로 환급됩니다.

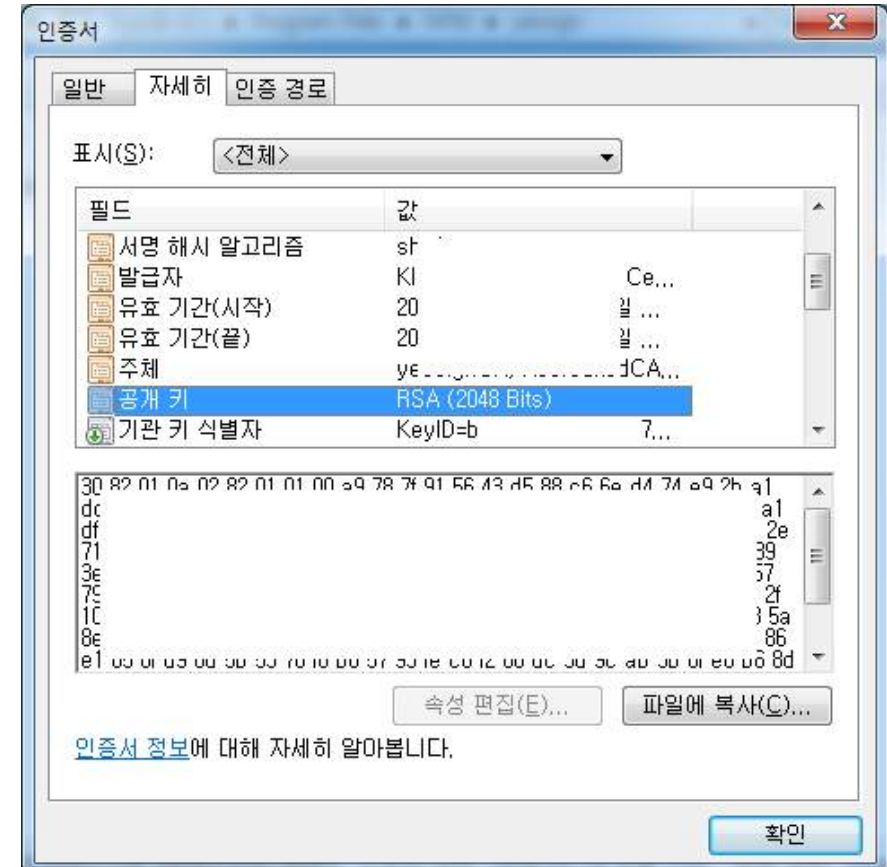
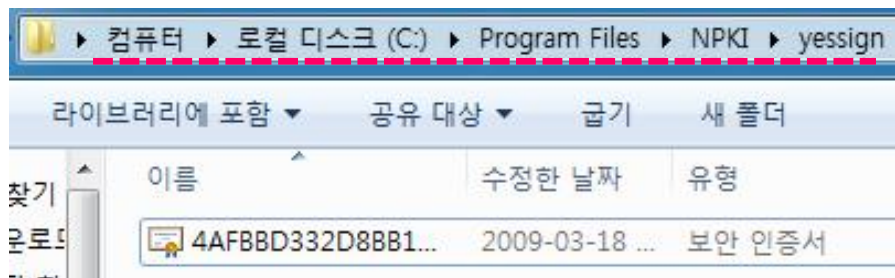
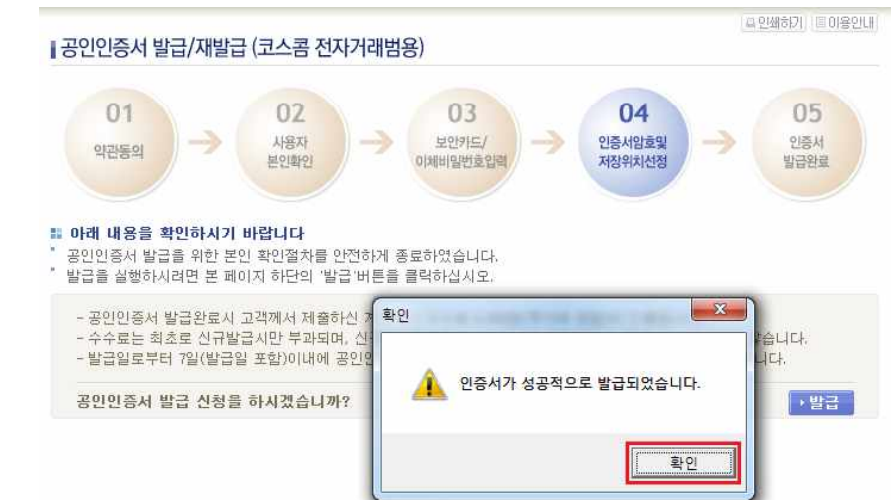
공인인증서 발급 신청을 하시겠습니까?

발급



공인 인증서(yessign) 발급[6]

⑩ 발급 완료: C:\Program Files\NPKI\yessign의 하위 폴더에 인증서 저장



인터넷뱅킹 접속(1)

① 개인뱅킹 클릭

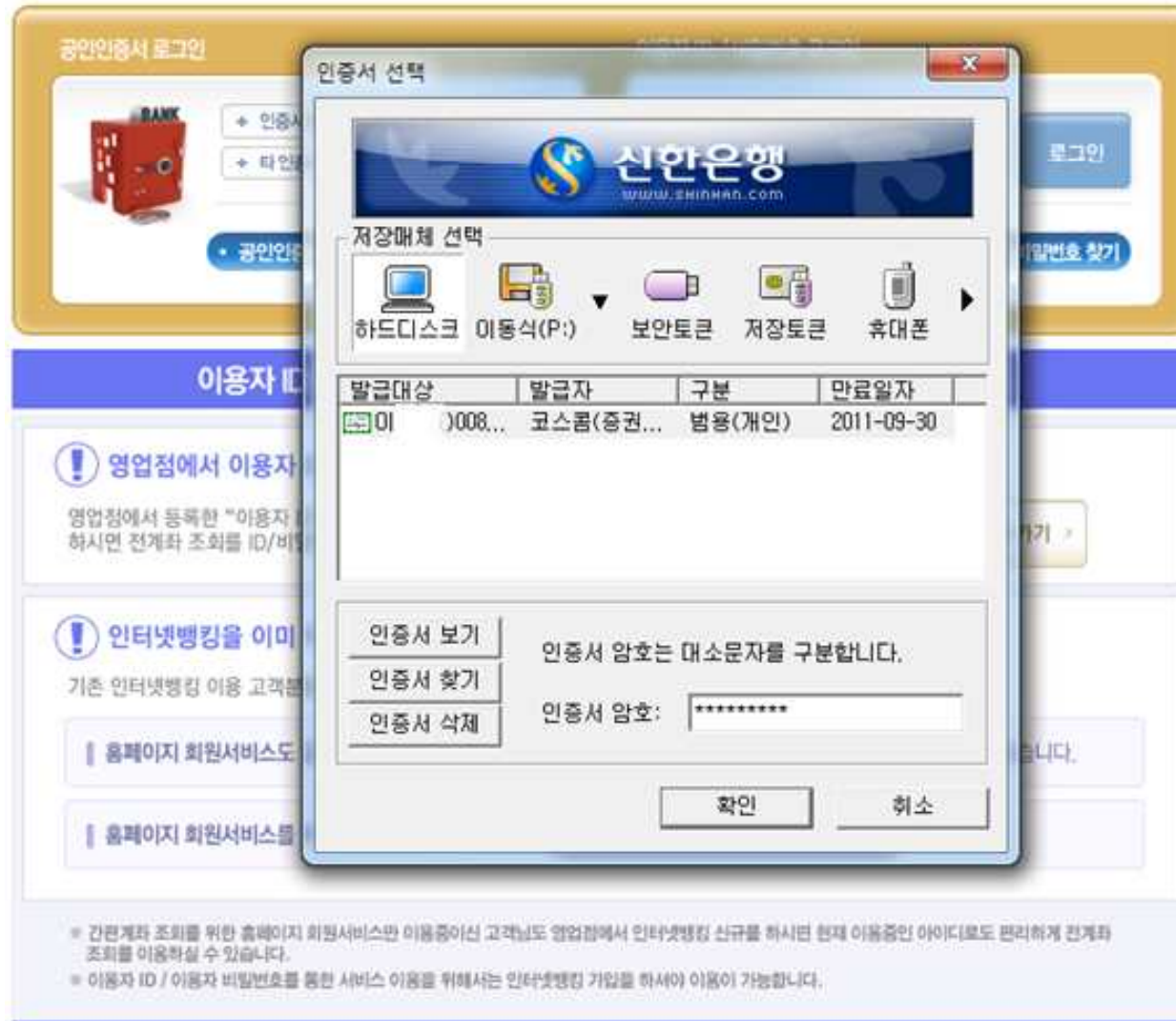


② 인터넷뱅킹 로그인 클릭



인터넷뱅킹 접속[2]

③ 공인 인증서 선택 및 인증서 암호 입력



인터넷뱅킹 접속(3)

④ 인터넷뱅킹 초기화면

신한은행 | 개인인터넷뱅킹

신한프리미어 | MINT 레이디클럽 | SOHO고객 | PRIVATE BANK | MY SHINHAN | 은행소개 | 고객센터 | GLO-NET Service

개인뱅킹 | 기업뱅킹 | 금융상품물 | 자산관리 | 금융서비스 | FUNNYZONE | 통합검색

Money 캘린더 | My 포트폴리오 | 인터넷상품물 | 예금물 | 대출물 | 골드물 | 외환물 | 펀드물 | 보험물

개인인터넷뱅킹 HOME

이 고객님 안녕하세요

신한은행만의 고객맞춤메세지

독지함 열기

로그인

정보변경

조회

이체

신규해지

대출

외환골드

모바일뱅킹

예금/신탁

펀드/수익증권

대출

외화/골드뱅킹

방카슈랑스

증권

글로벌이자넷

예금명

계좌번호

신규일

만기일

잔액

업무

저축예금	110-4	2008.08.21		409,268	조회 이체
예금 총잔액				409,268	

안내

▶ 기존에 신한/조흥은행의 계좌를 가지고 계신 고객님들은 '신계좌전환'버튼을 클릭하여 신한은행 신계좌로 변경하여 주셔야 합니다.
 ※ 계좌번호를 클릭하시면 빠른 서비스를 이용하실 수 있습니다.
 ※ 해지된 계좌의 조회는 [해지현황조회] 서비스를 이용하시기 바랍니다.
 ※ 보안계좌서비스를 이용하시면 인터넷뱅킹/폰뱅킹/VM뱅킹/USIM뱅킹 등 이용시 조회 및 출금거래가 제한됩니다.
 ※ 적금 입금가능시간: 05:00 ~ 23:00 / 신탁 입금가능시간: 08:00 ~ 22:00

인체하기

미용안내

온라인전용 고금리 U드림정기예금

인터넷뱅킹 이용절차(1/2)



인터넷뱅킹 절차[2/2]

- ① 사용자는 은행의 홈 페이지에 접속하여 인터넷뱅킹 로그인을 선택
- ② 은행은 사용자에게 인증서 비밀번호의 입력과 인증서 및 전자서명을 요청
- ③ 사용자는 인증서 비밀번호를 입력함으로써 컴퓨터에 저장되어 있는 **인증서**와 개인키를 이용하여 생성한 **전자 서명**을 은행에 전달
- ④ 은행은 인증서가 유효한 인증서인지 인증기관에 문의
- ⑤ 인증기관은 인증서의 디렉터리 검색을 통해 사용자의 인증서 상태를 확인한 후, 사용자 인증서의 신뢰 여부를 은행에 전달
- ⑥ 신뢰할 수 있는 인증서인 경우에 은행은 사용자의 공개키(인증서에 포함된)로 전자 서명을 복호화하여 사용자가 보낸 것이 확실한지 검증
- ⑦ 위의 단계가 검증되면 은행은 사용자에게 금융 서비스의 접근을 허용
- ⑧ 사용자는 잔액 확인, 송금 등과 같은 인터넷뱅킹을 수행한다. 송금 서비스를 위하여서는 **패스워드 카드의 번호와 이체 비밀번호**를 입력하여 한다.

금융기관별 ActiveX 설치 현황 목록

❑ 국민은행

- nProtect Security Center(nProtect Netizen V4.0): INCA
- XecureWeb Control V7.2(XecureWeb ClientSM 4.1.1.0): SoftForum
- INISAFEWeb v6: Initech
- INIIE8Assist: Initech
- Secure KeyStroke 4.0 : Softcamp

❑ 신한은행

- INISAFEWeb 7.0 Updater: Initech
- Secure KeyStroke 4.0: Softcamp
- Secure KeyStroke Elevation COMDLL: Softcamp
- ProWorksGrid: Iniswave
- Ahnlan Online Security: AhnLab

❑ 우리은행

- XecureWeb Control V7.2(XecureWeb ClientSM 4.1.1.0): SoftForum
- ClientKeeper KeyPro Keyboard Protector: SoftForum
- Ahnlan Online Security: AhnLab
- XecureWeb UCA Update Control: SoftForum
- WRebw: Interzen

❑ 외환은행

- VeraPort: WIZVERA
- VeraPort Main: WIZVERA
- nProtect Security Center (nProtect Netizen V4.0): INCA
- ClientKeeper KeyPro Keyboard Protector: SoftForum
- XecureWeb Control V7.2(XecureWeb ClientSM 4.1.1.0): SoftForum

금융기관별 ActiveX 설치 현황 목록

- ❑ **잉카인터넷 사의 nProtect Netizen:** 악성프로그램(해킹툴, 특정 바이러스 등)을 자동 진단 및 차단하고, PC 보안을 위한 다양한 기능을 제공하여 개인정보 유출을 차단
- ❑ **소프트포럼 사의 XecureWeb Control V7.2:** 암호화/복호화 및 사용자 인증을 바탕으로 웹, DB, 메일 등 다양한 어플리케이션에 데이터 무결성, 기밀성 보장, 사용자 부인 방지 기능을 제공하는 PKI 및 PKI 응용 프로그램
- ❑ **Initech 사의 INISAFEWeb 7.0:** 128비트 암호화 기술을 이용하여 웹 브라우저와 웹 서버 사이에 교환되는 데이터의 암호화, 디지털 인증서를 이용한 전자서명 지원
- ❑ **Softcamp 사의 Secure KeyStroke 4.0:** 키보드를 통해 입력되는 사용자의 중요 정보를 키보드 인터럽트 레벨에서 암호화 하여 악의적인 해킹이나 공격을 방지하는 솔루션
- ❑ **AhnLab의 Ahnlan Online Security:** 온라인을 통해 처리되는 모든 정보의 교류가 안전한 상태에서 이루어지도록 안티-키로거(anti-keylogger), 방화벽, 안티-바이러스/스파이웨어, 시큐어 브라우저의 4가지 보안 서비스로 구성되어 있다
- ❑ **소프트포럼 사의 Keyboard Protector:** 키보드를 통해 입력되는 사용자 중요 정보를 보호하기 위한 키 입력 해킹 방지 컴포넌트
- ❑ **WIZVERA 사의 VeraPort Main:** 인터넷뱅킹 등의 서비스를 위한 보안 프로그램의 설치 과정을 단순화하도록 도와주며, 보안 프로그램으로 인한 장애 상황을 빠르게 대처할 수 있도록 도와주는 프로그램

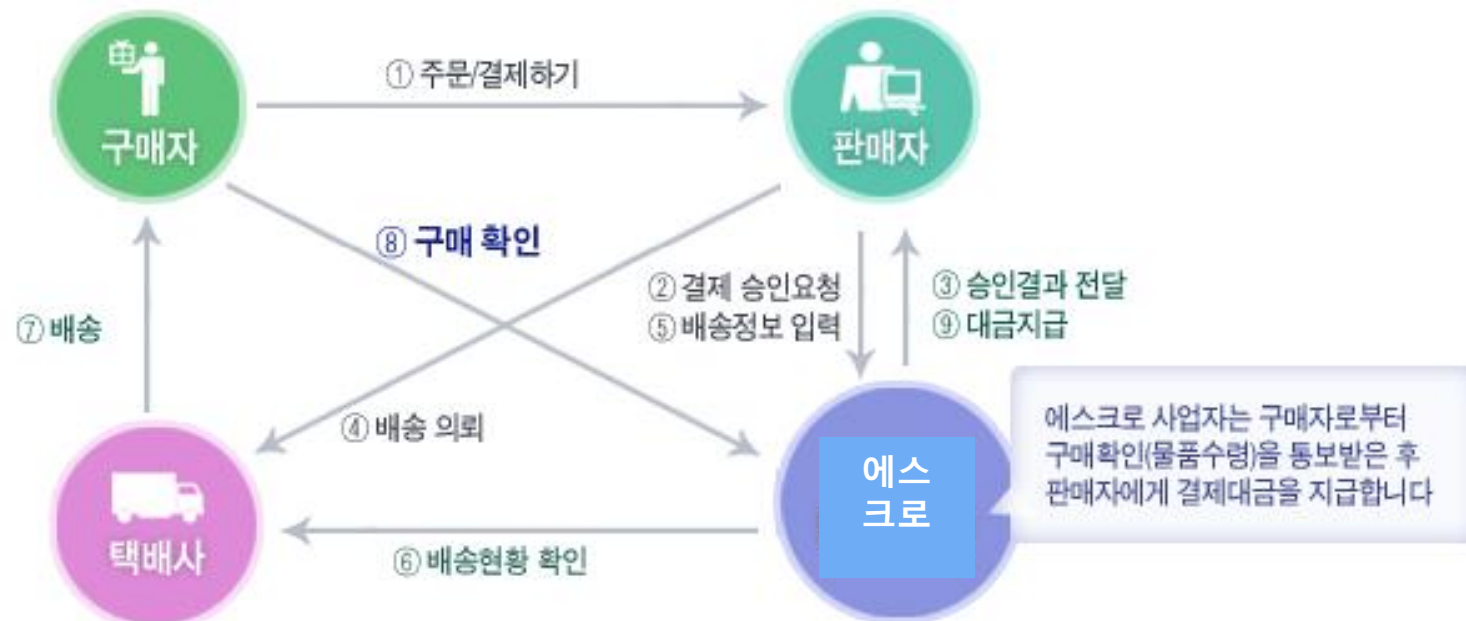
결제대행업체

- ❑ 쇼핑몰은 상품의 등록 및 주문만을 담당하며, 상품 금액의 지불은 **결제대행업체(PG: Payment Gateway)**가 담당
 - **보안 서비스와 다양한 지불/정산 솔루션**(신용카드, 실시간 이체, 핸드폰 결제 등)을 쇼핑몰에 제공
- ❑ PG 업체
 - LG U+: <http://ecredit.dacom.net/>, 이니시스: <http://www.inicis.com/>
 - 티지코프: <http://www.tgcorp.com/>, KCP: <http://www.kcp.co.kr/>



에스크로 서비스

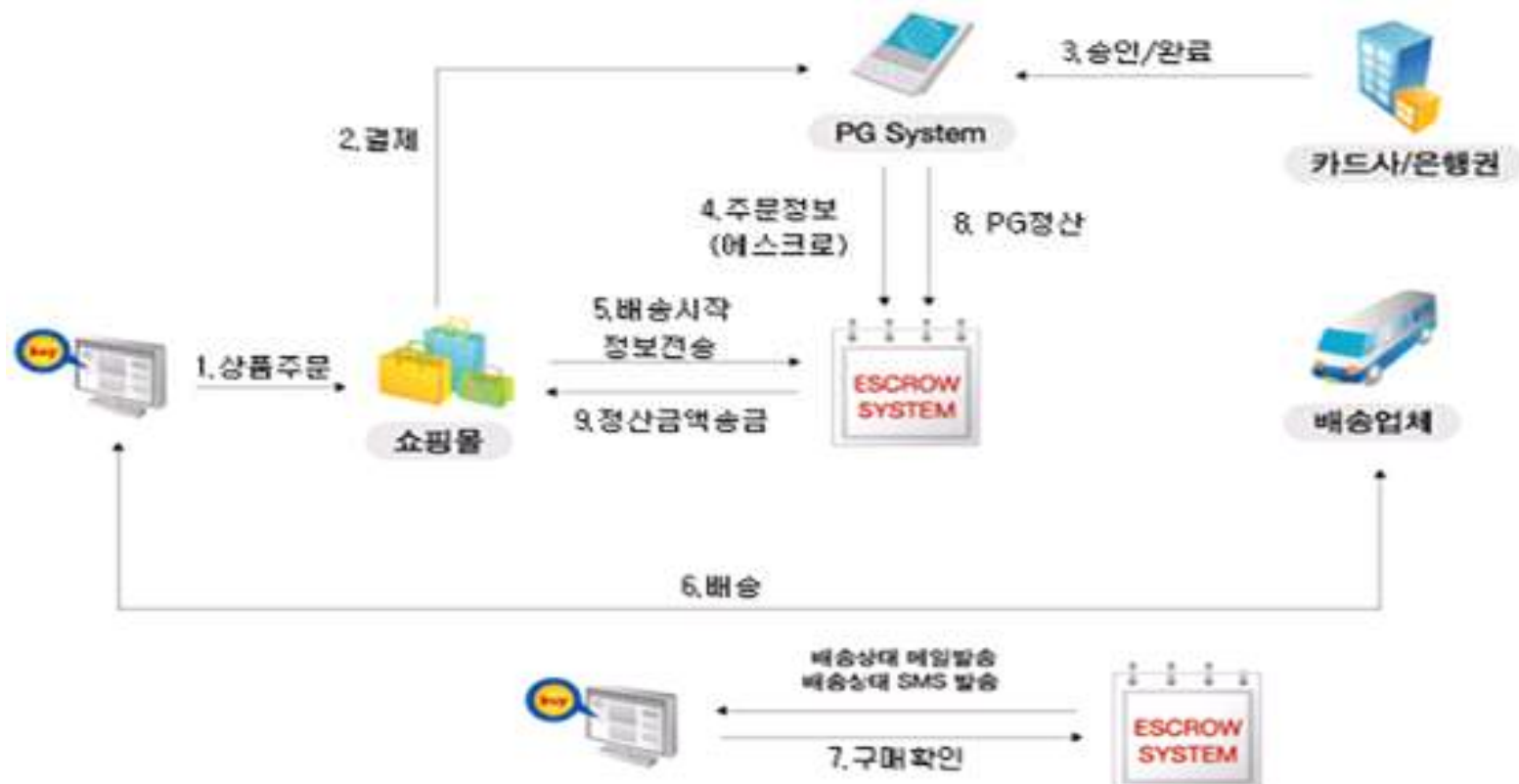
- ❑ 거래합의 후 상품배송 및 결제과정 중의 거래사고를 예방하기 위하여 **에스크로 (escrow)** 사업자(통상적으로 결제대행업체)가 거래대금의 입출금을 공정하게 관리 (2006.4.1 전자상거래 소비자보호법에 따른 의무 시행)
- ❑ 에스크로 의무시행 거래: 10만원 이상의 현금 거래(기존 무통장입금 거래 포함)
- ❑ 에스크로 면제 거래
 - 신용카드로 구매하는 거래 및 10만원 미만의 현금 거래
 - 배송이 필요하지 않은 재화 등을 구매하는 거래(콘텐츠 등)



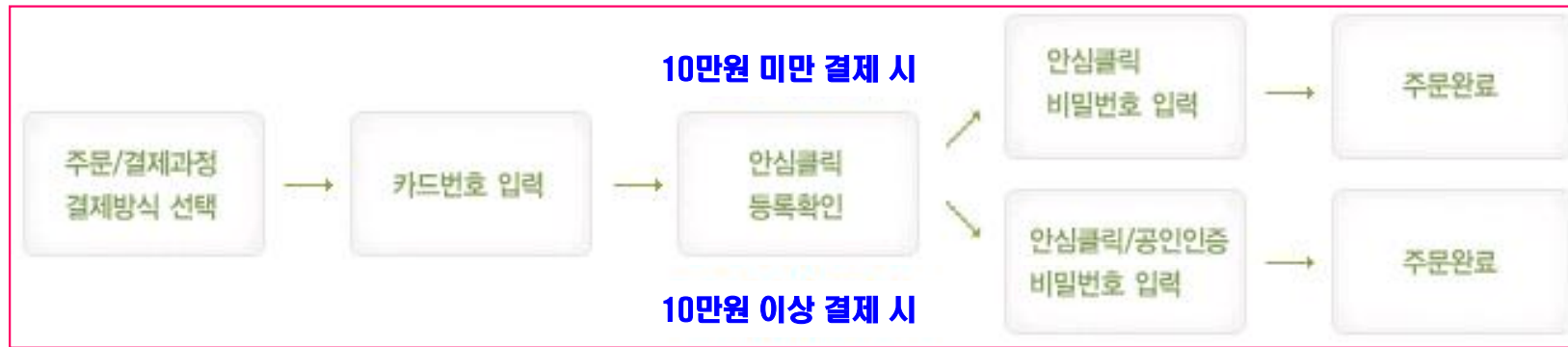
전자상거래 절차 및 결제

□ 신용카드결제

- 비자 안심클릭
- 안전결제(ISP: Internet Security Payment)
- 일반 카드결제: 카드번호, 유효기간, 비밀번호(2자리), 주민등록 번호

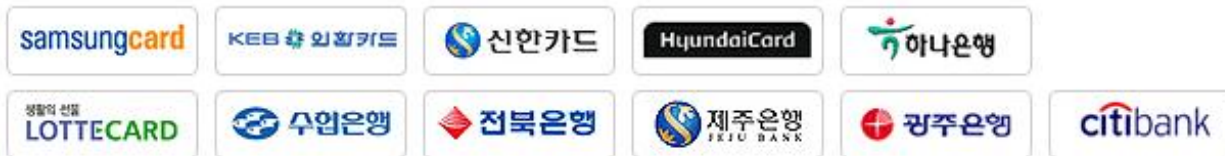


비자 안심클릭



- 카드 번호와 함께 거래금액이 10만원 미만인 경우는 안심클릭 패스워드(카드 인증)로, 10만원 이상인 경우는 안심클릭 패스워드 입력과 함께 공인인증서(본인 인증)를 제출
- 정보 전송 시 VISA 에서 개발한 3-D Secure 프로토콜 및 SSL사용

VISA안심클릭 적용카드사



• 카드번호	XXXX-XXXX-XXXX-1050
• 개인확인메시지	**** card
• 본인인증방법	패스워드방식 <input checked="" type="radio"/> 공인인증서방식 <input type="radio"/>
• 안심클릭 패스워드 :	<input type="text"/>
• CVC :	<input type="text"/>

* 개인확인메시지가 일치하지 않거나 없는 인증화면은 신한카드체크의 안심클릭서비스 인증 화면이 아닙니다.
 * CVC란 카드뒷면 숫자중 끝 3자리를 말합니다.
 * 2005년 11월 1일부터 30만원이상 결제하실 때는 공인인증서를 반드시 사용하셔야 합니다.

[도움말](#)

Copyright © 2004 by Shinhan Card. All rights reserved.

인터넷 안전결제(ISP)

- 안전한 전자상거래를 이용할 수 있도록 **국민카드와 BC카드**가 공동으로 개발한 전용 지불수단
 - 상품을 결제하기 위하여 **인증서가 있는 컴퓨터에서 ISP 비밀번호(6~14자리)**를 입력하여 결제함
 - 입력된 ISP 비밀번호를 통한 전자서명을 통해 모든 거래가 이뤄지므로, **신용카드 정보(카드번호, 유효기간)와 주민등록 번호의 입력이 필요없음**
 - 공개키(PKI)기반의 전자인증방식(공개키1024비트) 및 128비트의 SEED 암호화
 - 10만원 미만의 거래인 경우는 **ISP(카드 인증)로 결제**, 10만원 이상의 거래인 경우는 **ISP로 결제 후 공인인증서(본인 인증)를 통해 한번 더 확인**

안심결제 ISP 적용카드사



인터넷안전결제 (ISP) 서비스

결제내역

주문상품	Magic Synmaster 151SPlus-AZ
금 액	3,000,000 원
할부기간	일시불

결제하기

결제하실 카드선택

000 (비씨바로 MASTER)

ISP비밀번호 입력

(영어와 숫자를 조합한 6~14자리)

결제하기 취소 도움말

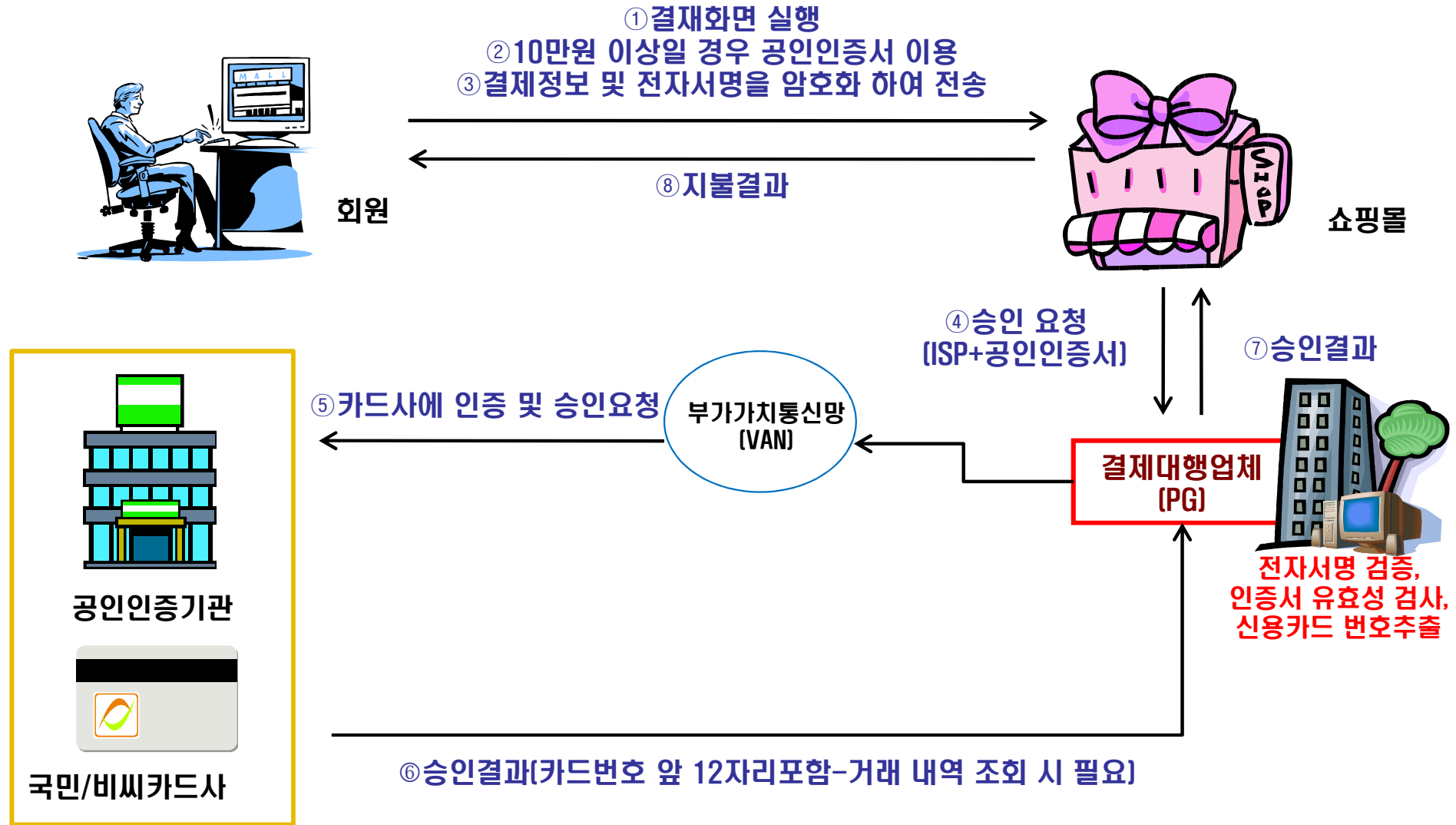
☐ 결제완료후 결제카드 감추기

? 인터넷안전결제 (ISP) 안내 메뉴

ISP 서비스 신청 ISP비밀번호변경 ISP 재발급 신청

인터넷안전결제 (Internet Secure Payment) - ISP 서비스

인터넷 안전결제(ISP) 절차



ISP 발급 절차(1)

① ISP를 사용하는 카드(BC, 국민..)를
이용한 인터넷 **결제하기**

신용카드 결제: 공인인증 안내, 안전결제 안내, 안심몰리 안내

카드 유형: 개인카드, 법인카드

카드 종류: 비씨카드

할부 방식: 일시불, 신용카드 결제 금액 5만원 이상 할부 가능

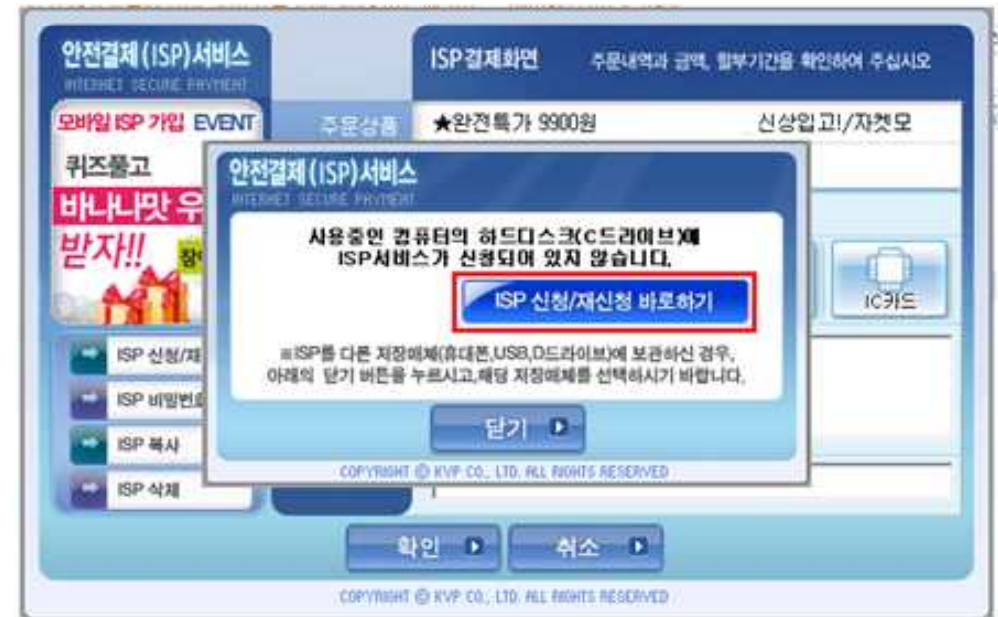
☐ BC TOP 포인트사용 ☐ 포인트 사용 안내

3(일부 상품제외) 11번가는 통신판매 중개자로서 등록 상품에 대한 모든 법적 책임은 판매자에게 있습니다.

HyundaiCard 2~11개월(5만원↑) 이니SK카드 2~11개월(5만원↑)

결제하기 이전페이지로 돌아가기

② ISP 플러그인 실행 → **ISP 신청** 클릭



ISP 발급 절차[2]

③ 카드 번호 및 E-Mail 주소 입력
→ 다음 클릭

④ 신용카드 정보 입력 → 다음 클릭

안전결제 (ISP) 서비스
INTERNET SECURE PAYMENT

ISP신청/재신청

카드번호 E-MAIL 입력

약관동의 정보입력

ISP 비밀번호 입력

신청완료

이제부터 신용카드 전자상거래는 안전하고 편리한 전자인증서 방식의 **안전결제 (ISP) 서비스**로 하십시오.

▶ 카드번호, E-MAIL 주소를 입력하여 주십시오.

- 카드번호 [9 0 - 1 2 - **** - ****]
- E-MAIL [h. i8@naver.com]

다음 ▶ **취소** ▶

COPYRIGHT © KVP CO., LTD. ALL RIGHTS RESERVED

안전결제 (ISP) 서비스
INTERNET SECURE PAYMENT

ISP 온라인 복사

카드번호 E-MAIL 입력

카드정보 입력

ISP 비밀번호 입력

신청완료

기존에 신청하신 ISP 서비스가 네트워크를 통해 복사 됩니다. 해당 카드정보를 입력해 주시기 바랍니다.

▶ 카드정보를 입력해 주십시오.

- 신용카드번호 9 0 - 1 2 - **** - ****
- 카드비밀번호 [****]
- CVC [***] CVC란?
- 유효기간 [12] (월) [2013] (년)

다음 ▶ **취소** ▶

COPYRIGHT © KVP CO., LTD. ALL RIGHTS RESERVED

ISP 발급 절차[3]

⑤ ISP 비밀번호 설정 → 다음 클릭

- 비밀번호 입력만으로 인터넷 결제 가능
- 10만원 이상 결제 시 공인 인증서 필요

안전결제 (ISP) 서비스
INTERNET SECURE PAYMENT

ISP신청/재신청

카드번호
E-MAIL 입력

약관동의
정보입력

ISP 비밀번호
입력

신청완료

▶ ISP 비밀번호를 입력하여 주십시오.

• ISP 비밀번호 [*****]

• ISP 비밀번호 확인 [*****]

(영/숫자를 조합한 6~14자리)

▶ ISP비밀번호는 고객님의께서 직접 만들어서 입력하셔야 하며, 신청완료 즉시 사용하실 수 있습니다.
(ISP비밀번호는 은행이나 카드사에서 별도로 통지하지 않습니다.)

다음 ▶ **취소** ▶

COPYRIGHT © KVP CO., LTD. ALL RIGHTS RESERVED

⑥ 인증서 저장 위치 설정 → 확인 클릭

모바일 안전결제 (ISP) 서비스
MOBILE INTERNET SECURE PAYMENT

Mobile ISP

안전결제 (ISP) 서비스 전자인증서를 PC 하드디스크보다 USB 또는 휴대폰 등 저장매체에 보관하시면 더욱 안전합니다.

모바일 안전결제 (ISP) 서비스 안내
휴대폰을 선택하시면 모바일 안전결제 (ISP) 서비스를 통해 인증서 저장 및 다양한 서비스를 이용하실 수 있습니다.

다음 ▶

COPYRIGHT © KVP CO., LTD. ALL RIGHTS RESERVED

안전결제 (ISP) 서비스
INTERNET SECURE PAYMENT

▶ 저장위치를 선택하여 주십시오.

하드디스크 휴대폰 이동식디스크 IC카드

확인 ▶ **취소** ▶

COPYRIGHT © KVP CO., LTD. ALL RIGHTS RESERVED

ISP 발급 절차[4]

⑦ 발급 완료 → **확인** 클릭

안전결제 (ISP) 서비스
INTERNET SECURE PAYMENT

ISP 신청/재신청

카드번호
E-MAIL 입력

약관동의
정보입력

ISP 비밀번호
입력

신청완료

안전결제(ISP)서비스 신청이 정상적으로
완료되었습니다.

기본정보

• 회원명

박

• 카드종류

농협비씨 농협OK Cashbag 체크
IC 2082



안전결제(ISP)서비스 전자인증서를
휴대폰에 보관하시어 더욱 안전하게 이용하세요.
(금융감독원 권고사항)

확인

COPYRIGHT © KVP CO., LTD. ALL RIGHTS RESERVED

요점 정리(1/2)

□ SSL(Secure Socket Layer)과 TLS(Transport Layer Security)

- 웹 서버와 브라우저 사이의 안전한 통신을 위하여 Netscape 사가 1993년 개발
- SSL 버전 3.0을 기반으로 1999년 IETF가 TLS1.0(SSL3.1) 규격인 RFC2246 발표

□ SSL 프로토콜의 구조

- 핸드셰이크 프로토콜: 클라이언트와 서버가 통신에 사용할 암호 및 인증 알고리즘과 공유 키를 결정하기 위한 암호 스위트를 교환하며, 인증서를 이용하여 상호 인증을 수행
- 암호사양변경 프로토콜: 핸드셰이크 프로토콜에 의하여 협의된 암호 스위트의 적용을 개시
- 경고 프로토콜: SSL 통신 중에 발생한 에러를 전달하는 프로토콜
- 레코드 프로토콜: 클라이언트와 서버가 핸드셰이크 프로토콜을 사용해서 결정한 알고리즘과 키 값을 이용하여 **대칭 암호화와 메시지 인증코드(MAC)**를 생성

□ SSL 보안의 문제점과 해결책

- 점대점 범위의 데이터 보호 제공 → **중단 범위의 보호를 위하여 응용계층의 암호화 요구**
- 전체 메시지를 암호화 → **XML 보안을 이용하여 필요한 정보만을 암호화**

요점 정리(2/2)

□ 인터넷뱅킹 절차

- ① 인터넷뱅킹 로그인 → 사용자는 인증서 비밀번호를 입력 → 개인키를 이용하여 생성한 전자 서명과 컴퓨터에 저장되어 있는 인증서를 은행에 전달
- ② 은행은 수신한 인증서가 유효한지 인증기관에 문의 → 유효한 경우에 사용자의 공개키(인증서에 포함된)로 전자 서명을 복호화하여 검증
- ③ 은행은 검증된 사용자에게 인터넷뱅킹 서비스의 접근을 허용
- ④ 송금 서비스를 위하여서는 패스워드 카드의 번호와 이체 비밀번호를 요구

□ 전자상거래에서 쇼핑몰에게 보안 서비스와 다양한 지불/정산 솔루션을 제공하기 위하여 상품 금액의 지불은 결제대행업체(PG: Payment Gateway)가 담당

□ 거래합의 후 상품배송 및 결제과정 중의 거래사고를 예방하기 위하여 에스크로 사업자(통상적으로 결제대행업체)가 거래대금의 입출금을 공정하게 관리

□ 신용카드결제

- 비자 안심클릭, 안전결제(ISP), 일반 카드결제