1 사용자 인증 방법

1 인증방법

- 인증 방법은 하나만 적용할 수도 있지만 두 개 이상의 방법을 함께 사용하는 것이 더 안전(이중 보안)

[인증 유형과 종류]

인증 유형	종류
알고 있는 것	패스워드, 주민등록번호, i-PIN
가지고 있는 것	신분증, 여권, 신용카드, 인증서, OTP, Key, 스마트카드
그 자체	홍채, 지문, 각막, 행동, 서명
위치하는 곳	지역, IP 주소

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 알고 있는 것

- 특정인을 인증할 때 사용하는
  가장 일반적이고 오래된 방법
- 해당 정보를 본인 외에는
  아무도 모르고 있어야 하는 것이 중요(패스워드,
  주민등록번호, i-PIN)

2 알고 있는 것

패스워드 기반 인증

[아이디와 패스워드 기반 인증]

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 알고 있는 것

주민등록번호 기반 인증

- 주민등록번호의 앞 여섯 자리는 생년월일,
  뒤 일곱 자리는 성별, 태어난 지역, 출생신고 순서,
  오류 검증 번호로 구성(도용, 위조)

- 성별을 나타내는 숫자는
  태어난 시대에 따라 구분

태어난 시대	성별 코드	
	남	여
1800년대	9	0
1900년대	1	2
2000년대	3	4

[시대별 성별 코드]

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 알고 있는 것

I-PIN(인터넷상 개인 식별번호) 기반 인증

- 주민등록번호를 입력하지 않고도 웹 서비스를 이용할 수 있는 개개인을 식별하는 별도의 식별번호(PIN)

- 개인정보 보호법에 따라 모든 포털 사이트는 회원 가입을 할 때 주민등록번호를 대체하는 수단을 마련해야 함(주민등록번호 필요 없음)

2 알고 있는 것

I-PIN(인터넷상 개인 식별번호) 기반 인증

「개인정보 보호법」 제24조 제2항
(고유식별정보의 처리 제한)

대통령령으로 정하는 기준에 해당하는 개인정보 처리자는 정보 주체가 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공 하여야 한다.

〈공포(2011. 3. 29.) 후 1년이 경과한 날로부터 시행(2012. 2. 29.)〉

3 가지고 있는 것

- 가장 대표적인 예는 열쇠
- 열쇠 외에도 신분증, 여권, 인증서(PKI), 스마트카드(IC) 등이 있음

[<매트릭스2-리로디드>에 등장하는 키메이커]

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 가지고 있는 것

스마트 카드

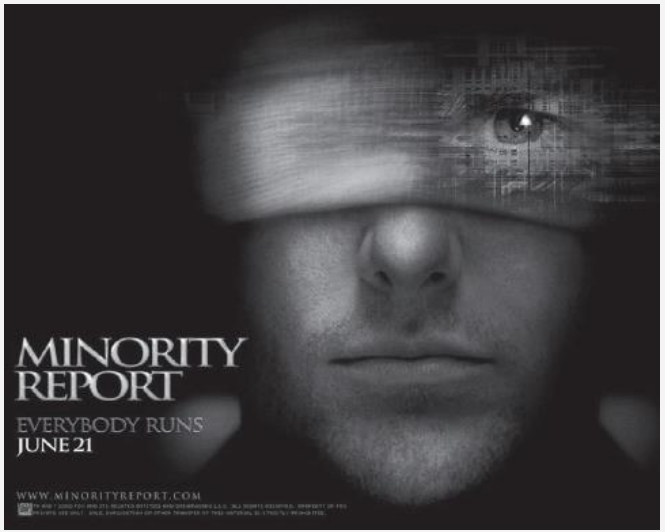
- 스마트카드의 IC 카드 칩에 개인을 식별할 수 있는 코드 또는 현금카드와 같은 정보가 입력되어 있음 (마그네틱 카드)

4 그 자체(생체 인증)

- 대체하거나 모방하기 어렵기 때문에
  더욱더 중요한 인증 수단으로 자리잡을 예정(인식률)
- 현재 생체 인증에는 지문, 홍채, 망막, 얼굴, 목소리,
  DNA 등이 사용되고 있음
- 행위 기반의 인증 수단으로는 서명, 키 누름 등이
  있음(발걸음)

4 그 자체(생체 인증)

[**홍채** 인식이 주요 인증수단인
미래 사회를 그린 영화 〈마이너리티 리포트〉]



※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 위치하는 곳

- IP 주소에 기반을 둔 시스템 접근 통제(NAC, LBS)
- IP 주소나 지역 정보를 토대로 정상 사용자인지 피싱 공격을 하려는 악의적인 사용자인지 확인할 수 있음

6 사용자 인증 - 상세 설명

- Something You Know
  - 사용자가 기억하는 지식을 이용
  - 사례 : 패스워드,
    PIN(Personal Identification Number)등

- Something You Are
  - 생체 조직(Biometrics)을 통한 인증(인식률)
  - 사례 : 지문, 손 모양, 망막, 홍채, 서명,
    키보드, 목소리, 얼굴

6 사용자 인증 - 상세 설명

Something You Have

- 사용자가 소유한 인증 수단을 이용해 인증을 수행(분실)
- 사례 : 스마트 키, 스마트 카드, 신분증, 인터넷 뱅킹 카드와 OTP(One Time Password), 공인 인증서 등
- Something You Have는 다른 사람이 쉽게 도용할 수 있기 때문에 단독으로 쓰이지 않고, 일반적으로 Something You Know 나 Something You Are와 함께 쓰임(멀티팩터)

6 사용자 인증 - 상세 설명

- 하나의 인증수단 만으로는 취약성이 있는 경우
  두 가지 이상의 서로 다른 인증 수단을 함께 사용하는
  (멀티팩터) 방법

- 신분증
  - 학생증, 주민등록증, 운전면허증 등
  - 본인임을 확인하기 위해 얼굴을 대조하므로,
    신분증은 Something You Have 와
    Something You Are 둘 다를 인증 수단으로 이용

6 사용자 인증 - 상세 설명

- 인터넷 뱅킹
  - 인터넷 뱅킹 시 인증서(PKI)와 함께 보안카드나 OTP를 병행 사용

6 사용자 인증 - 상세 설명

▶ 거래이용수단과 보안등급

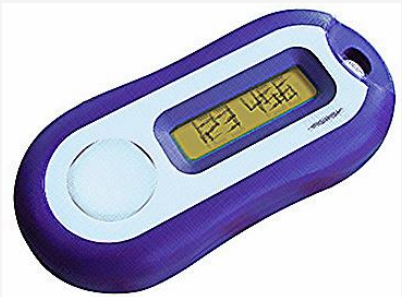
거래이용수단	보안등급
OTP발생기 + 공인인증서	1 등급
HSM 방식 공인인증서 + 보안카드	
보안카드 + 공인인증서 + 2 channel 인증	
보안카드 + 공인인증서 + 휴대폰 SMS(거래내역통보)	2 등급
보안카드 + 공인인증서	3 등급

6 사용자 인증 - 상세 설명

- 공인인증서(PKI)
  - 신뢰된 공인인증기관이 발행하는 인증문서
  - 일종의 전자금융거래용 인감증명서
  - 사용자의 신원확인, 거래 내역에 대한 위변조 방지, 거래 사실의 부인 방지에 사용
  - 2010년말 현재 2,371만건의 인증서 발급
  - 경제활동 인구의 90% 이상이 사용(조만간 폐지)

6 사용자 인증 - 상세 설명

- OTP(One time password) 발생기
  - 고정된 비밀번호 대신 사용되는
    매번 새롭게 바뀌는 일회용 비밀번호
  - 반복?



6 사용자 인증 - 상세 설명

- 보안카드
  - 35개 이내의 난수가 적혀진 카드
  - 전자금융 거래시 사용자가 카드에 인쇄된 번호를 직접 입력하고, 응답번호와 일치여부를 판단하여 전자금융거래를 수행

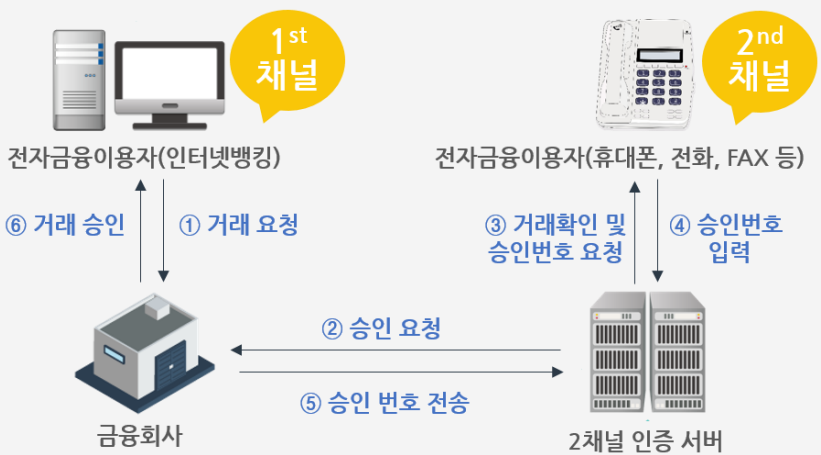
6 사용자 인증 - 상세 설명

- HSM(Hardware Security Module)
  - 일반 USB 메모리 스틱처럼, PC의 USB슬롯에 연결하여 사용
  - 연산 장치와 메모리 등이 포함된 스마트카드 칩을 탑재해 전자 서명과 암호화 등 모든 프로세스가 매체 내부에서 이루어지기 때문에, PC에 설치된 해킹 프로그램이나 악성코드를 통해서 HSM 내부에 저장된 비밀 정보에 접근할 수 없음 (공개된 정보가 없음)
  - 예 : 물리적(하드웨어) 공인인증서

6 사용자 인증 - 상세 설명

2채널 인증

- 전자금융거래 채널 이외에 거래승인을 위한 채널을 분리하여 이용하는 기술(문자 메시지 혹은 전화)



6 사용자 인증 - 상세 설명

휴대폰 SMS(Short Message Service, 거래내역통보)

- 인터넷 뱅킹, 텔레뱅킹 등의 전자금융 서비스를 이용한 자금이체내역을 휴대폰으로 통지하는 서비스
- 사용자의 주요 거래 또는 중요 통지 사항을, 사후에 실시간으로 알려주는 방식

[휴대폰 SMS 인증]

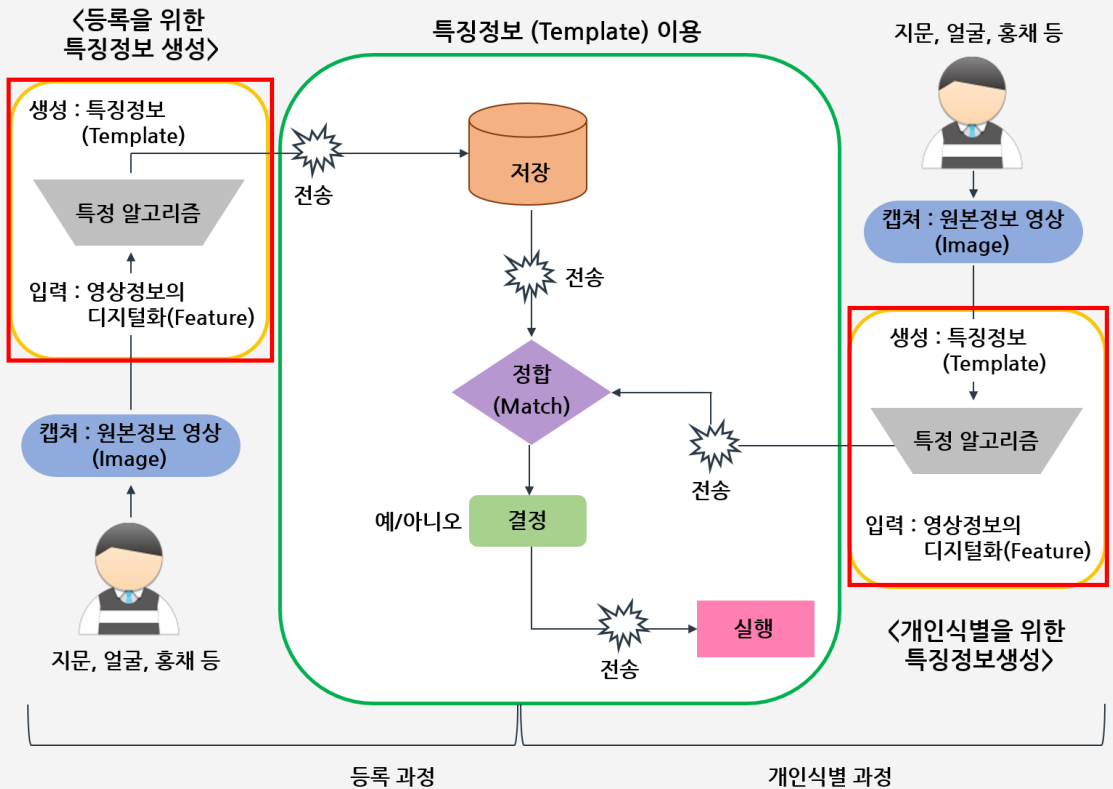
6 사용자 인증 - 상세 설명

- 바이오 인증
  - 지문 인식 기술은 인터넷 뱅킹 접속 시 또는 자금 이체 시 지문 정보를 이용하여 인증을 수행하며, 복제 및 해킹 위험이 적음(인식률)
  - 바이오 인증은 바이오 인식기기의 보급 및 사용자의 인식 등의 문제로 거의 사용되고 있지 않음(현재 : 활성화)
  - 우리은행에서 바이오 인증을 유일하게 적용하고 있음
  - 예 : 홍채 인식 기술

6 사용자 인증 - 상세 설명

바이오 인증

[바이오 인증 절차]



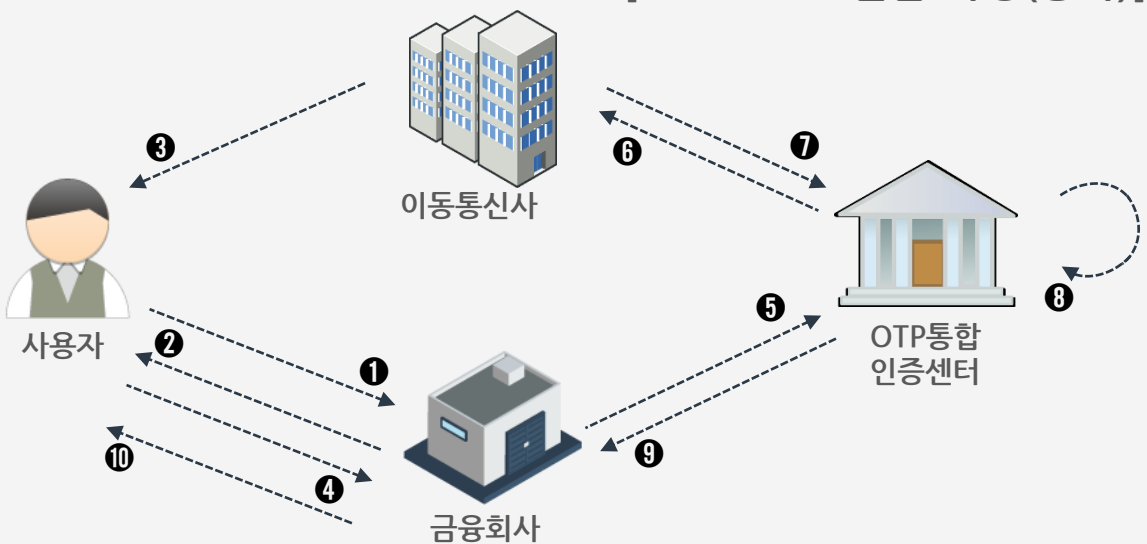
6 사용자 인증 - 상세 설명

- USIM OTP 인증기술(USIM + OTP)
  - 스마트폰에 탑재되는 USIM은 IC칩과 동일한 물리적 보안성을 제공할 수 있고, 다양한 응용 애플릿을 탑재가 가능하여, 다양한 인증기술을 USIM에 구현이 가능
  - OTP 발생기 휴대에 따른 불편함을 해소하여 사용자 편의성을 높임

6 사용자 인증 - 상세 설명

USIM OTP 인증기술

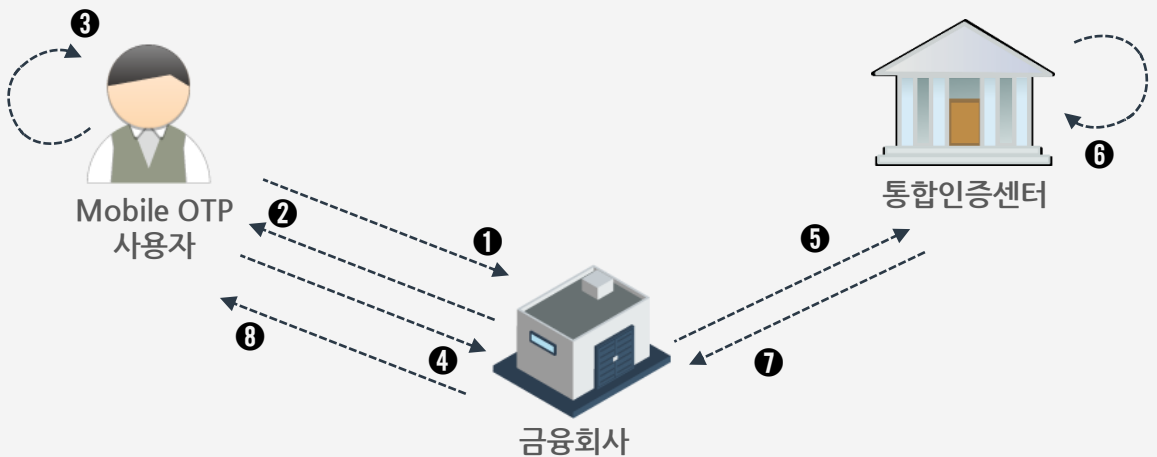
[USIM OTP 발급 과정(등록)]



6 사용자 인증 - 상세 설명

USIM OTP 인증기술

[USIM OTP 인증 과정 (생성)]

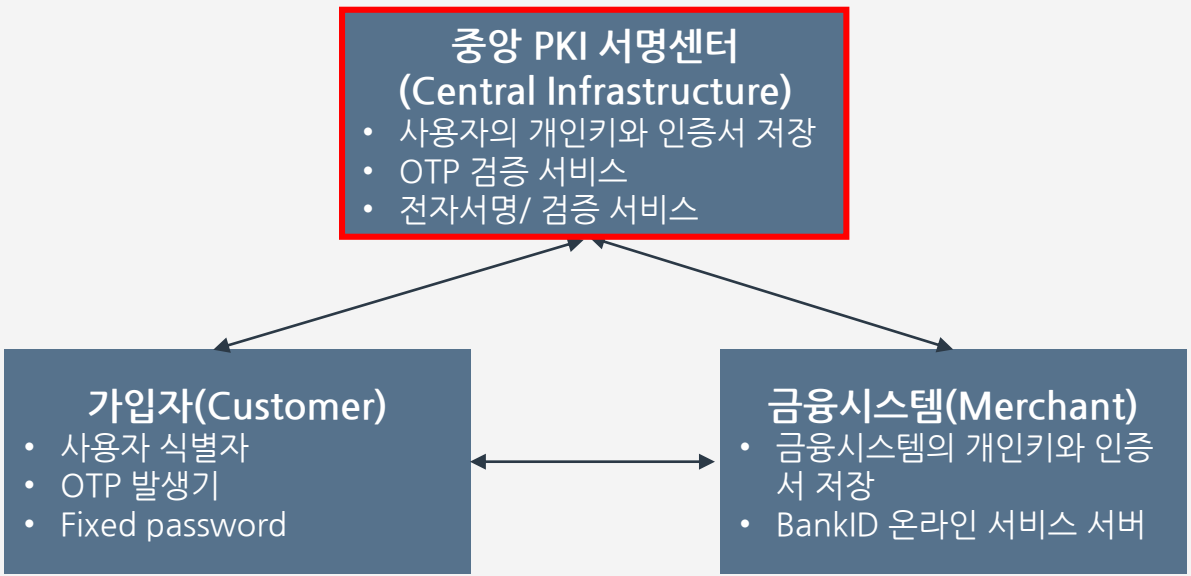


6 사용자 인증 - 상세 설명

- PKI 서명센터(인증서 관리 문제 해결)
  - 현재 PKI 구조에서는 공격자가 사용자의 로컬 PC에 저장되어 있는 개인키, 인증서와 함께 개인키 접근을 위한 비밀번호를 탈취하여 전자 서명을 할 수 있는 취약점이 존재
  - PKI 서명센터 구조에서는 사용자의 개인키 및 인증서 관리시스템인 중앙 PKI 서명센터를 설치하고, 가입된 모든 사용자의 개인키와 인증서를 중앙 PKI 서명센터에 저장함으로써, 사용자 PC보다 상대적으로 안전하게 관리가 가능하여 인증서의 관리적 문제를 해결 가능

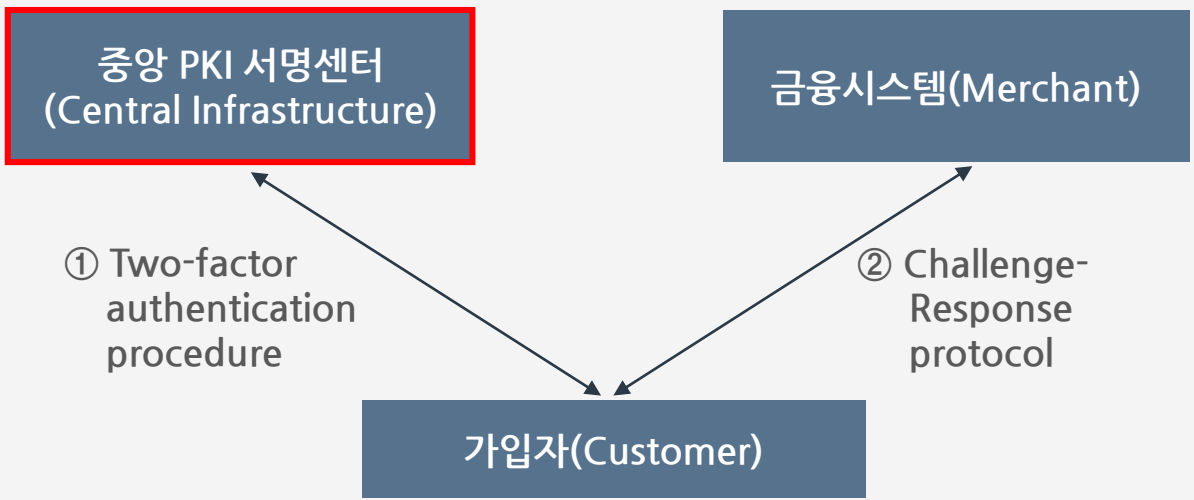
6 사용자 인증 - 상세 설명

PKI 서명센터 구성도



6 사용자 인증 - 상세 설명

인증절차



6 사용자 인증 - 상세 설명

- 스마트채널 인증기술(ETRI)
  - 로그인, 전자서명, 카드결제 같이 보안이 중요한 기능과 인증서, 신용카드, 비밀 번호 등 중요 정보가 있어야 하는 기능은 모두 스마트폰으로 보내서 하는 개념
  - PC에 ActiveX 등 브라우저 부가프로그램 설치 불필요
  - 인증서는 스마트폰에만 저장(도난 문제?)

6 사용자 인증 - 상세 설명

▶ 스마트채널 인증기술(ETRI)

6 사용자 인증 - 상세 설명

스마트채널 인증기술(ETRI)

결제 화면

QR코드

스마트폰으로
결제내역 서명

6 사용자 인증 - 상세 설명

- 패스워드 기반(Weak Authentication)
  - crypt passwd under UNIX
  - one-time password

- 도전-응답(Challenge-response) 기법(Strong Authentication)
  - 질문에 대해 정확한 대답을 할 수 있어야 인증
  - 대칭키암호, 해쉬함수, 비대칭키암호 이용

6 사용자 인증 - 상세 설명

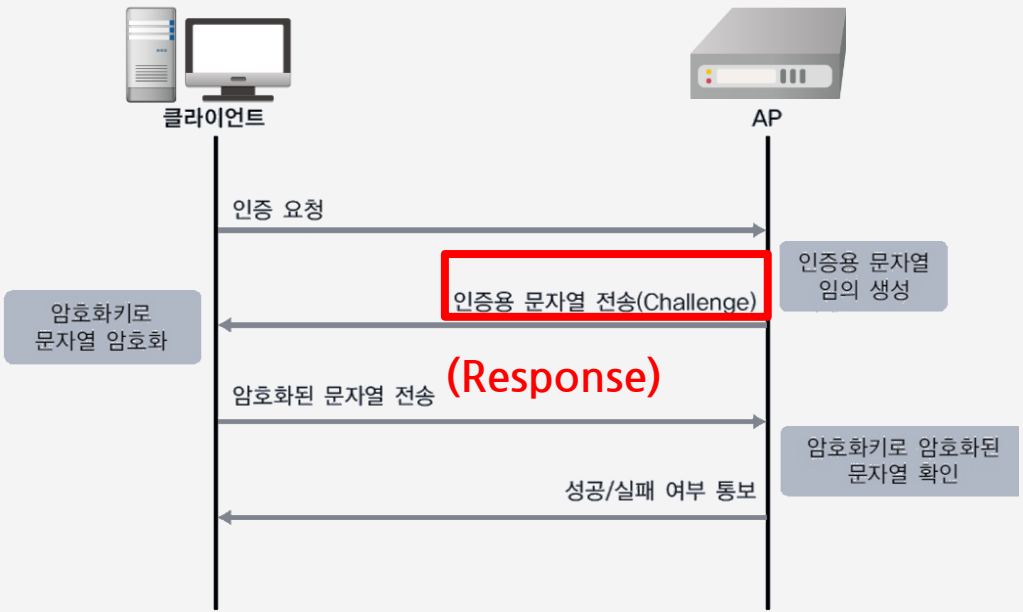
- 암호 프로토콜 이용(기타 방법)
  - Fiat-Shamir identification protocol
  - Schnorr identification protocol

6 사용자 인증 - 상세 설명

- WEP(Wired Equivalent Privacy)
  - 무선랜 통신을 암호화하기 위해 802.11b 프로토콜부터 적용
  - 1987년에 만들어진 RC4 암호화 알고리즘을 기본으로 사용(보안 취약)
  - Challenge & Response

6 사용자 인증 - 상세 설명

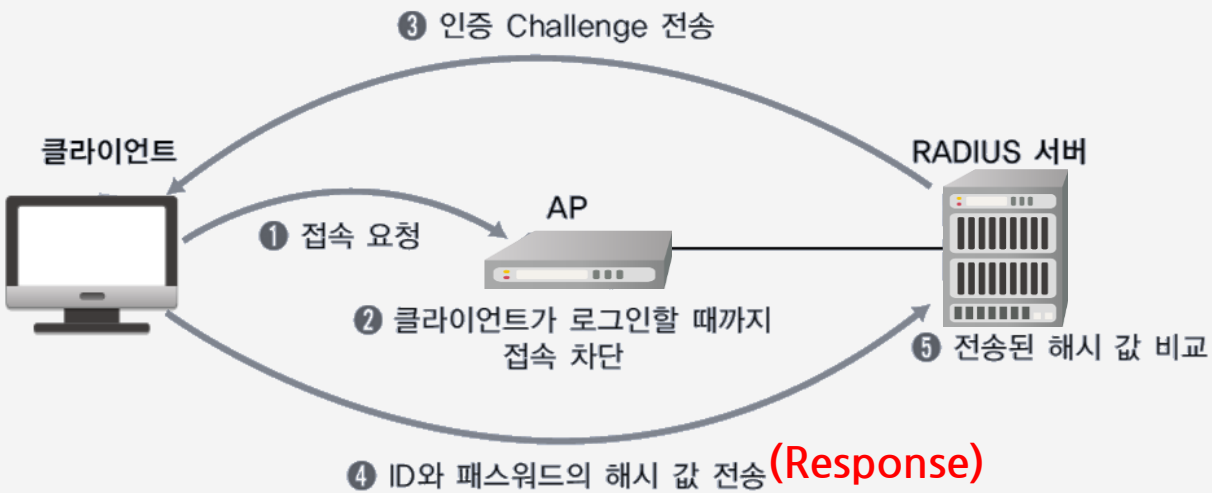
WEP(Wired Equivalent Privacy)



6 사용자 인증 - 상세 설명

WEP(Wired Equivalent Privacy)

[RADIUS와 802.1X를 이용한 무선 랜 인증 1]



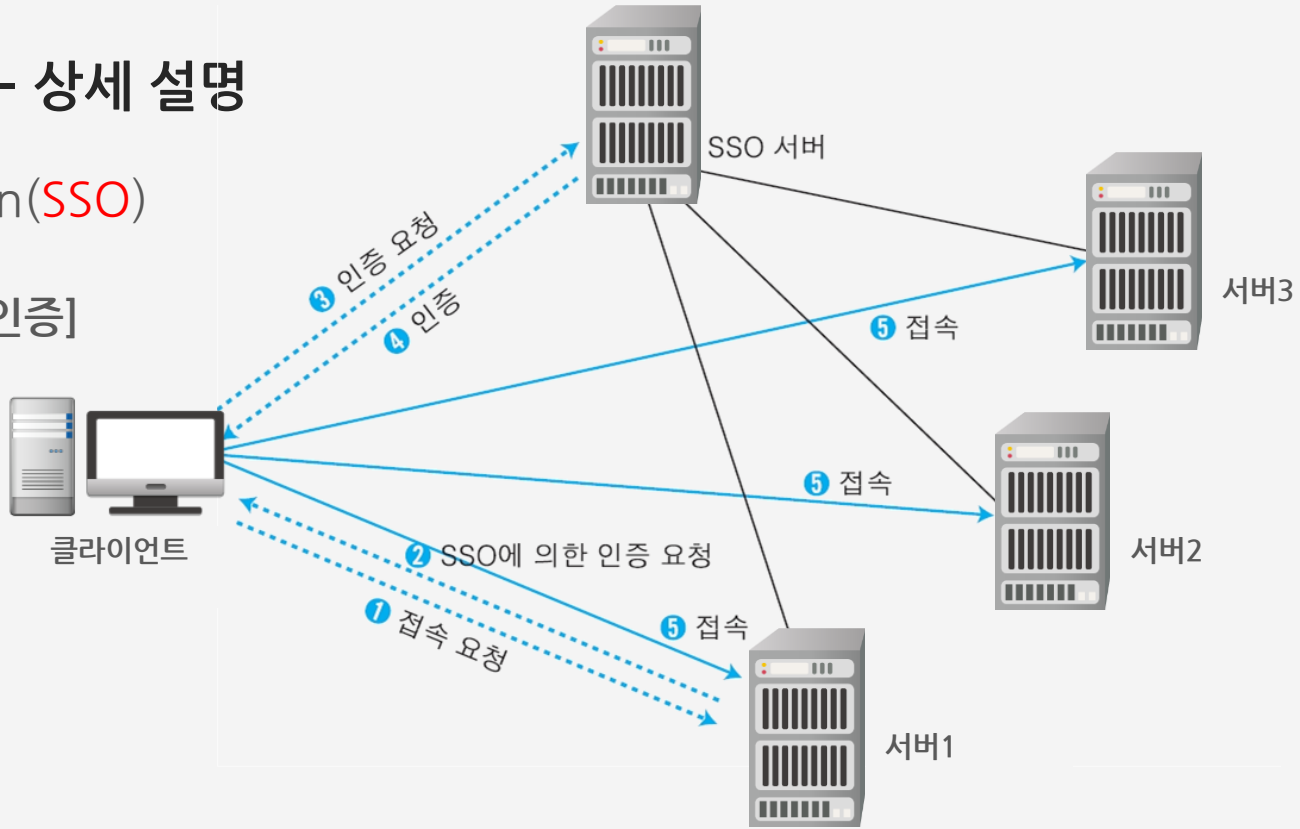
6 사용자 인증 - 상세 설명

- Single Sign On(SSO)
  - 모든 인증을 하나의 시스템에서
  - 시스템이 몇 대가 되어도 하나의 시스템에서 인증에 성공하면, 다른 시스템에 대한 접근 권한도 모두 얻음
  - 이러한 접속 형태의 대표적인 인증 방법으로는 커버로스(Kerberos, AS, TGS)를 이용한 윈도우의 액티브 디렉토리(Active Directory)가 있음

6 사용자 인증 - 상세 설명

- Single Sign On(SSO)

[SSO에 의한 인증]



6 사용자 인증 - 상세 설명

- 서버별 인증
  - 서버별 사용자 등록
  - 사용자가 각기 다른 아이디, 패스워드 관리 필요

- 조직 내 인증
  - 싱글사인온(SSO)
  - 한번의 사용자 등록으로 조직 내 모든 서버에 인증 가능(Trust)

6 사용자 인증 - 상세 설명

- 공인인증
  - 제한 없는 인증 확장을 위해 공인인증이 필요
  - 공인인증서를 이용한 인터넷 뱅킹 접속
  - 공인인증서와 공개키기반구조(PKI)(없어질 예정)

2 취약점 및 공격 기법

1 패스워드 설정의 취약점

[해커에게 쉽게 노출되는 취약한 패스워드]

순위	패스워드	순위	패스워드	순위	패스워드	순위	패스워드	순위	패스워드
1	pssword	6	monkey	11	baseball	16	ashley	21	654321
2	123456	7	1234567	12	111111	17	bailey	22	supeman
3	12345678	8	letmein	13	iloveyou	18	passwOrd	23	qazwsx
4	qwerty	9	trustno1	14	master	19	shadow	24	michael
5	abc123	10	dragon	15	sunshine	20	123123	25	football

사전 공격(Dictionary Attack)

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 패스워드 크랙으로 패스워드 취약성 확인하기

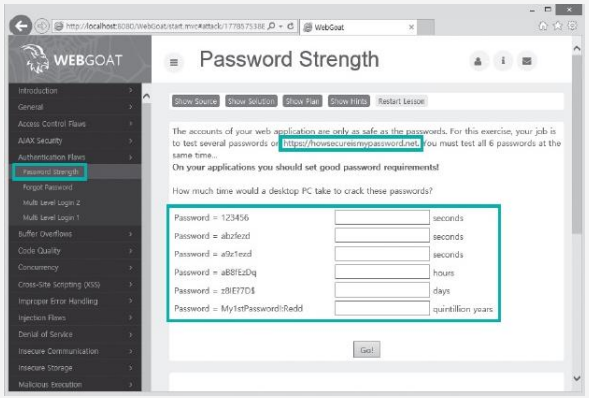
실습환경

- 윈도우 계열의 사용자 운영체제
- 필요 프로그램
  : OWASP WebGoat v7.1

2 패스워드 크랙으로 패스워드 취약성 확인하기

① Password Strength

- WebGoat를 실행 후
  [Authentication Flaws]-[Password Strength] 선택



[WebGoat의 패스워드
강력도 테스트 준비 화면]

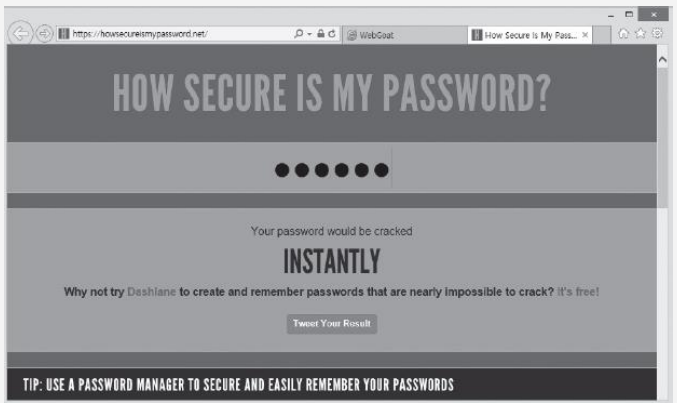
※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 패스워드 크랙으로 패스워드 취약성 확인하기

② 패스워드 취약성 확인

- 빨간색 링크를 클릭하거나 https://howsecureismypassword.net에 직접 접속
- '123456' 입력

['123456' 을 패스워드로 사용할 경우 크랙 가능 시간이 INSTANTLY(즉시) 라는 것을 알려주는 화면]



※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 패스워드 크랙으로 패스워드 취약성 확인하기

② 패스워드 취약성 확인

- ‘abzfezd’ 입력

[‘abzfezd’ 을 패스워드로 사용할 경우 크랙 가능 시간이 200밀리세컨드(2초) 라는 것을 알려주는 화면]

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 패스워드 크랙으로 패스워드 취약성 확인하기

② 패스워드 취약성 확인

- ‘My1stPassword!:Redd’ 입력

[‘My1stPassword!:Redd’
을 패스워드로
사용할 경우 크랙 가능
시간이 36Quintillion
year(3600경일)
라는 것을 알려주는 화면]

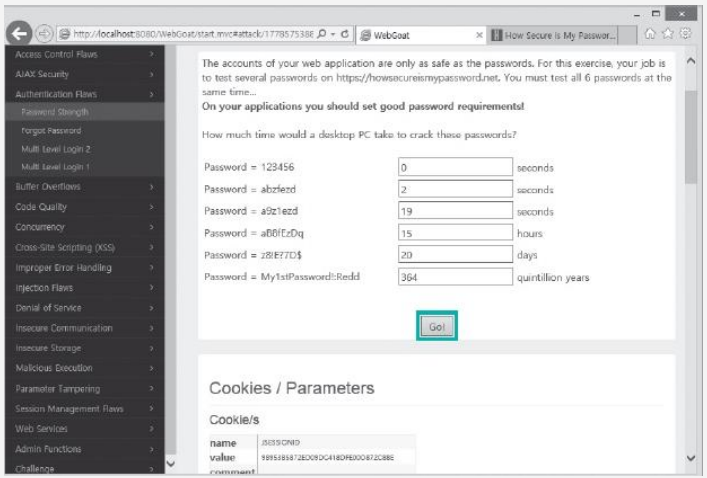
※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 패스워드 크랙으로 패스워드 취약성 확인하기

③ 패스워드를 크랙하는 데 걸리는 시간 입력

[패스워드 조합에 따른 크랙 예상 소요 시간]

패스워드 조합	크랙 예상 소요 시간
숫자만으로 구성된 여섯 자리 패스워드	0초
영문 소문자만으로 구성된 일곱 자리 패스워드	2초
영문 소문자와 숫자가 조합된 일곱 자리 패스워드	19초
영문 소문자와 대문자, 숫자가 조합된 여덟 자리 패스워드	15시간
영문 소문자와 대문자, 숫자, 특수문자가 조합된 여덟 자리 패스워드	20일
영문 소문자와 대문자, 숫자, 특수문자가 조합된 열아홉 자리 패스워드	364경 일



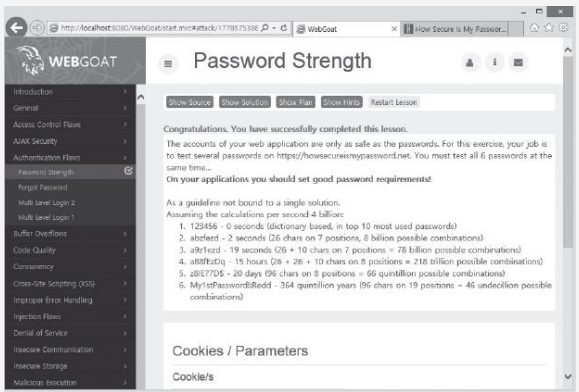
[패스워드 강력도 테스트의 전체 결과를 WebGoat에 입력]

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 패스워드 크랙으로 패스워드 취약성 확인하기

④ 패스워드 강력도 결과 확인

- ‘값을 모두 입력한 후 〈Go〉 클릭
- 패스워드는 영문 소문자와 대문자, 숫자, 특수문자를 조합해 복잡하게 만들수록 안전(분석)



[패스워드 강력도 테스트의 종합 결과]

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 취약하게 설계된 패스워드 찾기 기능의 위험도 분석

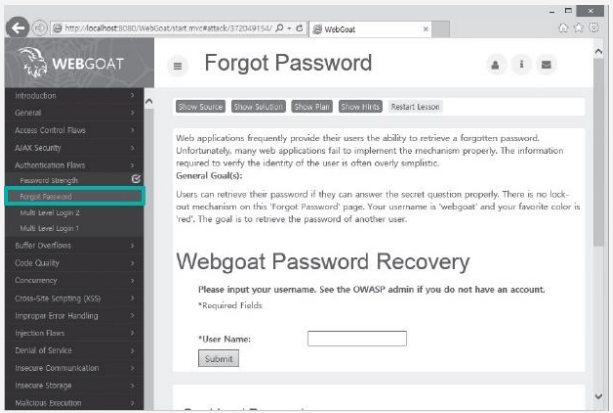
실습환경

- 윈도우 계열의 사용자 운영체제
- 필요 프로그램
  : OWASP WebGoat v7.1

3 취약하게 설계된 패스워드 찾기 기능의 위험도 분석

① Forgot Password

- WebGoat 실행 수 메뉴에서
  [Authentication Flaws]-[Forgot Password] 선택



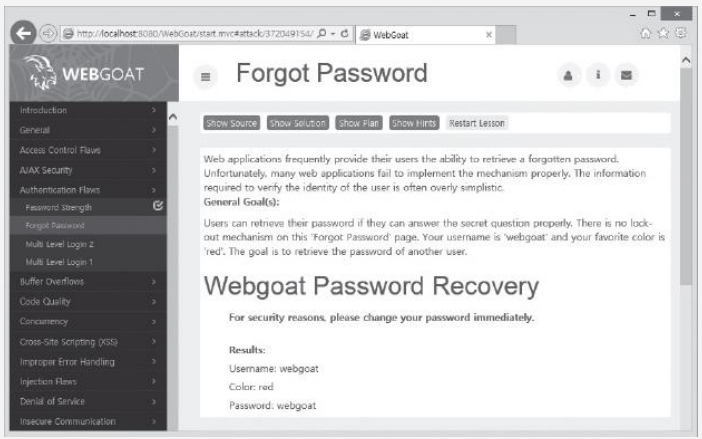
[WebGoat의 패스워드 찾기 예제 화면]

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 취약하게 설계된 패스워드 찾기 기능의 위험도 분석

② 정상적인 사용자 정보로 패스워드 탐색

- User Name에 'WebGoat'를 입력하고 〈Submit〉 클릭
- 다음 화면에서 Answer에 'red'를 입력하고 〈Submit〉 클릭



[정상적인 사용자 정보로 패스워드 탐색]

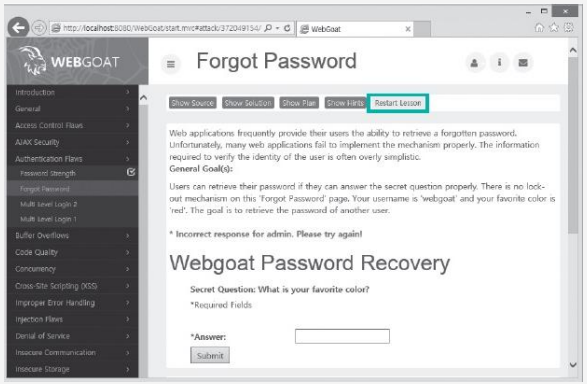
※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 취약하게 설계된 패스워드 찾기 기능의 위험도 분석

③ 다른 사용자의 패스워드 탐색

- 화면 상단의 <Restart Lesson>을 클릭하여 User Name을 입력하는 화면으로 다시 이동
- User Name에 'admin'을, Answer에 'red'를 입력

[틀린 정보로 패스워드 탐색]

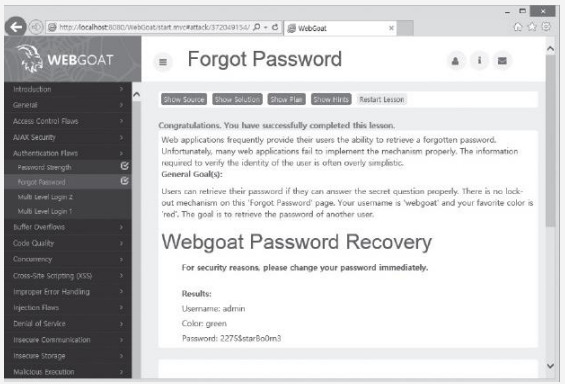


※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 취약하게 설계된 패스워드 찾기 기능의 위험도 분석

③ 다른 사용자의 패스워드 탐색

- 질문의 형태가 단순히 색을 묻는 것이기 때문에 공격자는 yellow, red, blue 등의 색상을 추측하여 응답할 수 있음
- 공격자가 green을 입력하여 결국 패스워드를 얻음 (질문?)



[단순한 질문에 대해 추측한 응답으로 패스워드 탐색에 성공한 화면]

※출처: 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 공개키 기반구조

1 인증서란 무엇인가?

- 공개 키 인증서(public-key certificate; PKC)
  - 이름이나 소속, 메일 주소 등의 개인 정보
  - 당사자의 공개 키가 기재
  - 인증기관(CA; certification authority, certifying authority)의 개인 키로 디지털 서명
  - 결론: 공개키 + 디지털 서명

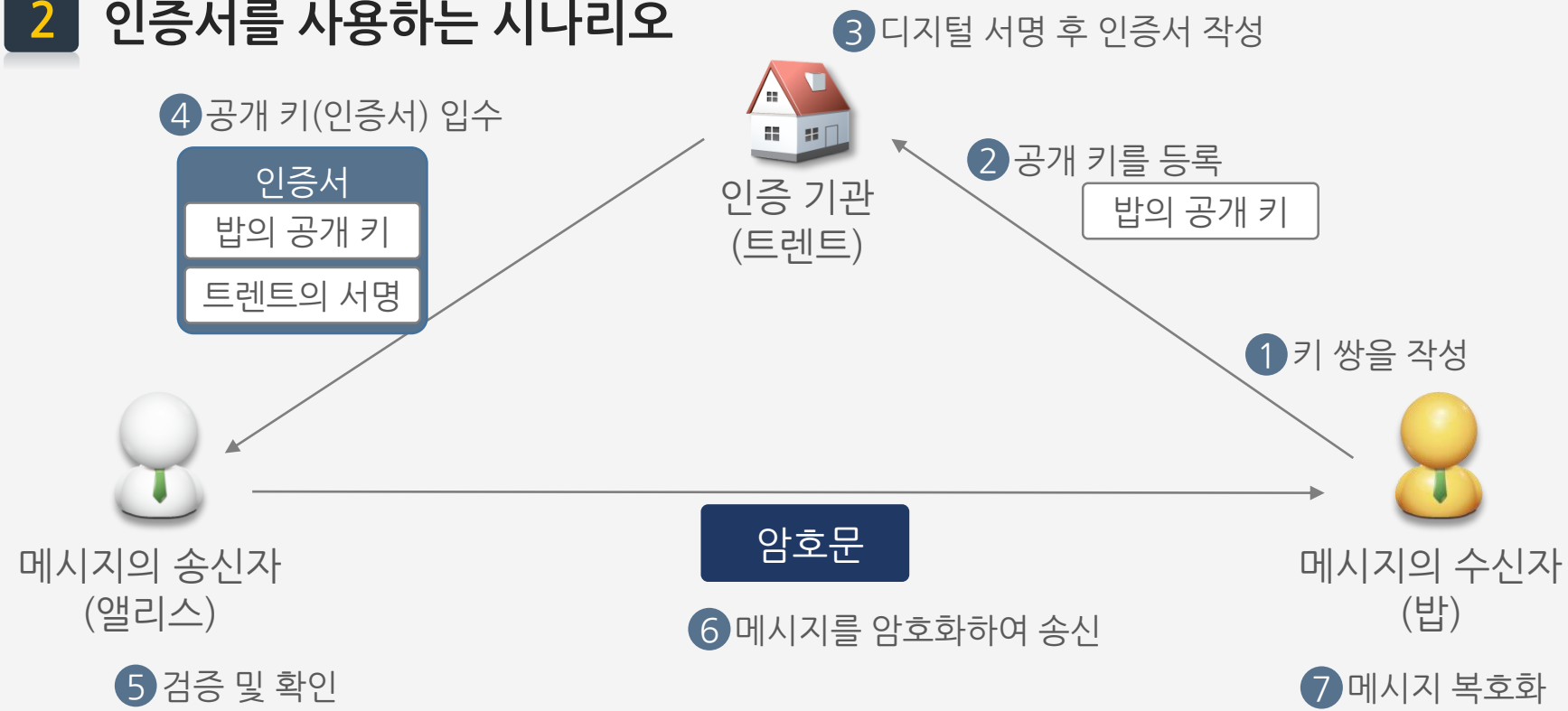
2 인증서를 사용하는 시나리오

- 밥이 키 쌍을 작성
- 밥은 인증기관 트렌트에 자신의 공개 키를 등록
- 인증기관 트렌트는 밥의 공개 키에 자신의 개인 키로 디지털 서명을 해서 인증서를 작성(공개키 인증서)
- 앨리스는 인증기관 트렌트의 디지털 서명이 되어 있는 밥의 공개 키(인증서)를 입수
- 앨리스는 인증기관 트렌트의 공개 키를 사용해서 디지털 서명을 검증하고, 밥의 공개 키가 맞다는 것을 확인

2 인증서를 사용하는 시나리오

- 앨리스는 밥의 공개 키로 메시지를 암호화해서 밥에게 송신
- 밥은 암호문을 자신의 개인 키로 복호화해서 앨리스의 메시지를 읽음

2 인증서를 사용하는 시나리오



3 공인 인증서 종류

- 범용 공인인증서
  - 모든 분야에서 이용
  - 인터넷뱅킹, 온라인증권, 전자상거래, 전자정부 민원서비스, 4대 사회보험, 국세청 홈텍스, 전자세금계산서, 전자입찰/조달, 온라인교육, 예비군 등 다양한 분야에서 활용
  - 소정의 수수료

3 공인 인증서 종류

- 용도제한 공인인증서
  - 은행 및 보험, 신용카드 업무, 정부 민원업무 등 특정분야에서만 이용
  - 해당 기관이 고객에게만 발급
  - 무료
  - 예: 입출금 메시지를 공인인증서를 이용해서 은행에 전송

4 인증서 표준 규격

- X.509
  - 가장 널리 사용
  - ITU(International Telecommunication Union)나 ISO(International Organization for Standardization)에서 규정한 규격
  - 인증서의 생성·교환을 수행할 때 사용
  - 많은 애플리케이션에서 지원

5 공개 키 기반 구조(PKI)

- 공개 키 기반(public-key infrastructure)
  - 공개 키를 효과적으로 운용하기 위해 정한 많은 규격이나 선택사양의 총칭

- PKCS(Public-Key Cryptography Standards): RSA사가 정하고 있는 규격의 집합(공개키 암호 사용 방식에 대한 표준 프로토콜)
- RFC(Requests for Comments) 중에도 PKI에 관련된 문서: 인터넷의 선택사양을 정함
- X.509
- API(Application Programming Interface) 사양서

5 공개 키 기반 구조(PKI)

PKI 구성 요소

이용자	PKI를 이용하는 사람	등록, 이용
인증기관	인증서를 발행하는 사람	vs. 등록기관
저장소	인증서를 보관하고 있는 데이터베이스	디렉토리

5 공개 키 기반 구조(PKI)

- PKI 구성 요소

5 공개 키 기반 구조(PKI)

- 이용자
  - PKI를 사용해서 자신의 공개 키를 등록하고 싶어 하는 사람과
  - 등록되어 있는 공개 키를 사용하고 싶어 하는 사람
  - 예: 은행과 사용자

5 공개 키 기반 구조(PKI)

- 이용자가 하는 일
  - 키 쌍을 작성(인증기관이 작성하는 경우도 있음)
  - 인증기관에 공개 키를 등록
  - 필요할 경우 인증기관에 신청해서 등록한 공개 키를 무효로 함(예: 은행과 사용자)
  - 인증기관으로부터 인증서를 발행 받음 (예: 사용자와 은행)

5 공개 키 기반 구조(PKI)

- 공개키 사용자가 하는 일
  - 수신한 암호문을 복호화
  - 메시지에 디지털 서명을 함(예: 개인키)

  - 메시지를 암호화해서 수신자에게 송신
  - 디지털 서명을 검증(예: 공개키)

5 공개 키 기반 구조(PKI)

- 인증기관(certification authority; CA)
  - 인증서의 관리를 행하는 기관
  - 키 쌍을 작성(이용자가 작성하는 경우도 있음)
  - 공개 키 등록 때 본인을 인증
  - 인증서를 작성해서 발행
  - 인증서를 폐지

5 공개 키 기반 구조(PKI)

- 등록기관(RA; registration authority)
  - 인증기관의 일 중 「공개 키의 등록과 본인에 대한 인증」을 대행하는 기관