전자인증 솔루션 구축 및 활용사례

TrustPro

Robust PKI Solution

1999. 7

삼성 SDS 주식회사

SAMSUNG 삼성SDS

순 서

1. 보안/인증 관련 현황
2. Application 보안기술
3. TrustPro 소개
4. Case Studies
5. Reference Sites
6. Summary

SAMSUNG 삼성SDS

TrustPro

보안/인증 관련 현황

- 1999.7.1 전자서명법 발효
- 1999.7.1 KISA 서비스 개시 (Root CA)
- 국내 공인인증기관 추진현황
  - 금융결제원
  - 한국증권전산주식회사
  - 인간 컨소시움
  - 정부기관
- 비공인인증기관의 설립 및 운영 가능
- 해외현황
  - 전자인증 등을 이용할 경우 서류와 똑같은 법적 효력을 갖도록 각국의 법/제도에 명기하는 한편 인증기술의 표준화 등은 OECD가 강제하지 않고 시장원리에 맡기도록 제안하고 있음.

SAMSUNG 삼성SDS

TrustPro

Application 보안기술

SAMSUNG 삼성SDS

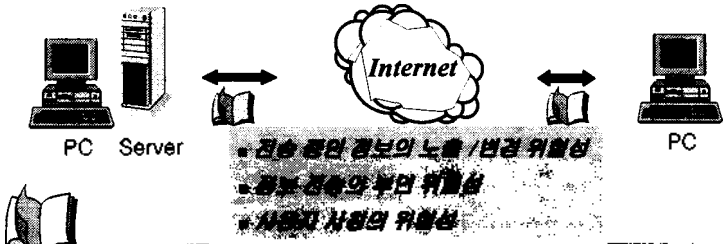
TrustPro

Application 보안

인터넷 금융거래의 대표적인 적용분야인 인터넷 뱅킹, 인터넷 증권거래, 인터넷 보험가입, 인터넷 카드사용, 인터넷 쇼핑몰 등의 보안을 위해서는 다음과 같은 정보보호서비스가 요구됨

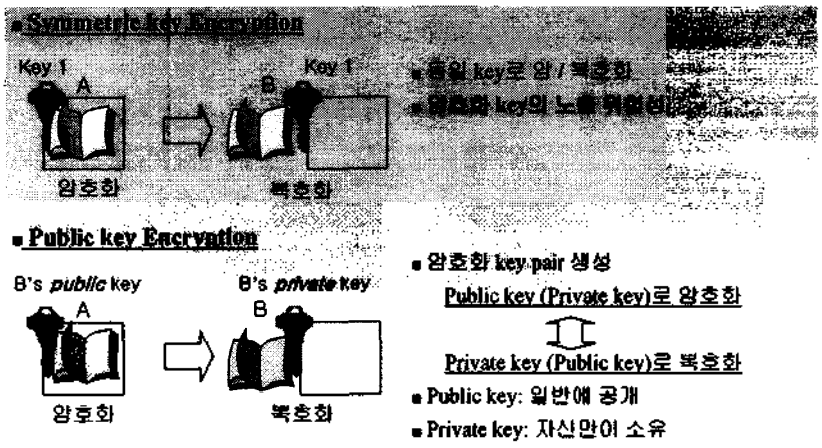
- **가 밀 성** : 전송되는 정보의 비밀 보장
- **무 결 성** : 전송되는 정보가 변경되지 않음을 보장
- **인　　증** : 전송자의 신분을 증명
- **부인방지** : 사후 자신의 행위에 대한 부인 불가

Security Issues on Internet



기업	병원	금융	국방
■ 계약서	■ 환자 검진 기록	■ 고객 계정 정보	■ 사단 배치도
■ 설계 도면	■ 처방전	■ 고객 신상 자료	■ 무기 배치도
■ 인사 기록	■ Digitized X-ray	■ 거래 내역	■ 전략/전술 보고서
■ 급여 명세	■ Digitized CT		■ 상황보고
■ 보고서/제안서			■ 위성 사진

Encryption(암호화)

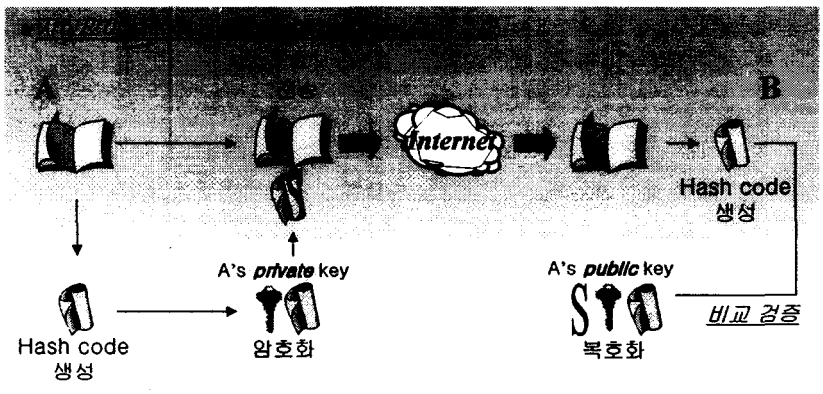


- 동일 key로 암 / 복호화
- 암호화 key pair 생성
  - Public key (Private key)로 암호화
  - Private key (Public key)로 복호화
- Public key: 일반에 공개
- Private key: 자신만이 소유

SAMSUNG 삼성SDS

TrustPro

Digital Signature(전자서명)

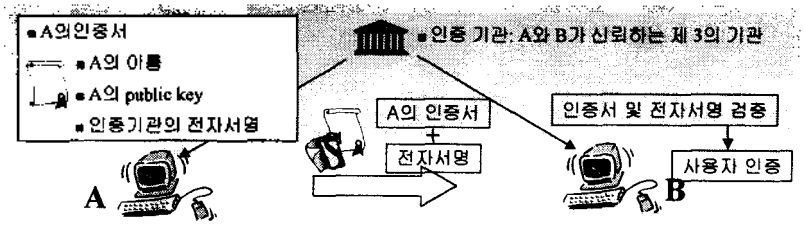


SAMSUNG 삼성SDS

TrustPro

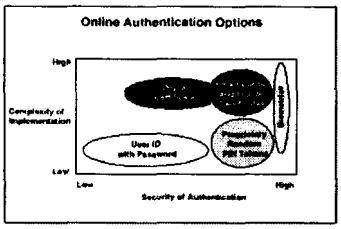
Digital Certificate(인증서)

■ 사용자 사항 발지



■ 사용자 인증 방법 비교 (Source Giga Group)

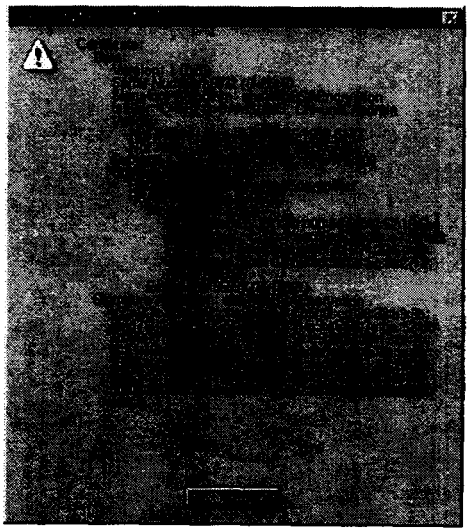
- User ID / Password
- Random PIN Tokens
- Digital Certificate
- Digital Certificate with Smart Card
- Biometric



인증서의 구성 및 내용

영 역	설 명
version	인코딩된 인증서의 버전을 기술
serial number	CA가 각 인증서에 지정한 정수
issuer signature algorithm	인증서를 서명하는 데 이용되는 알고리즘에 대한 알고리즘 식별자
issuer distinguished name	인증서를 서명하는 기관의 유일 식별자 (X.500 고유 이름)
validity period	인증서가 유효한 기간(UTCTime을 이용)
subject distinguished name	인증서 주체의 유일 식별자(X.500 고유 이름)
subject public key information	공개키와 그 키가 사용될 알고리즘을 식별
issuer unique identifier(선택)	발행자 이름의 재사용 가능성을 제어
subject unique identifier(선택)	주체 이름의 재사용 가능성을 제어
extensions(선택)	확장영역 이름과 critical 여부의 값으로 구성 만약 확장영역이 critical이라면 클라이언트는 그 확장영역을 처리할 수 있어야 한다.
issuer's signature on all the above fields	인증서에 대한 서명값

인증서의 구성 및 내용

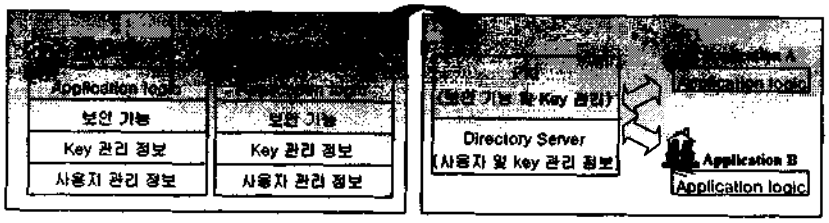


SAMSUNG 삼성SDS

TrustPro

Why a PKI?

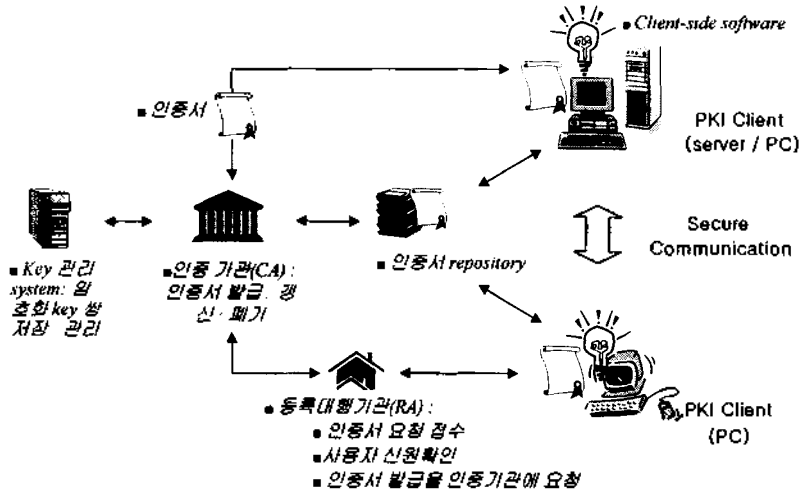
- 통합적인 key 관리를 통한 비용 절감
- 다양한 application에 공통으로 적용 가능한 보안 기능 제공
- ***모든 응용 system 및 transaction의 기반이 되는 기본 구조***



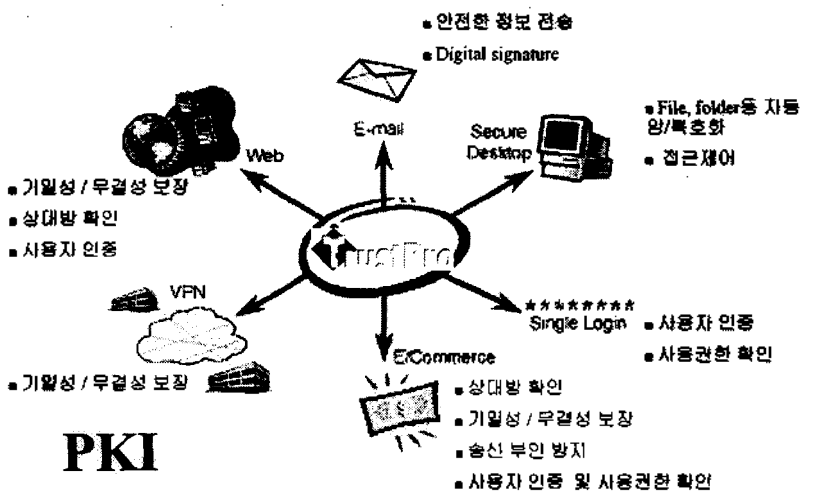
SAMSUNG 삼성SDS

TrustPro

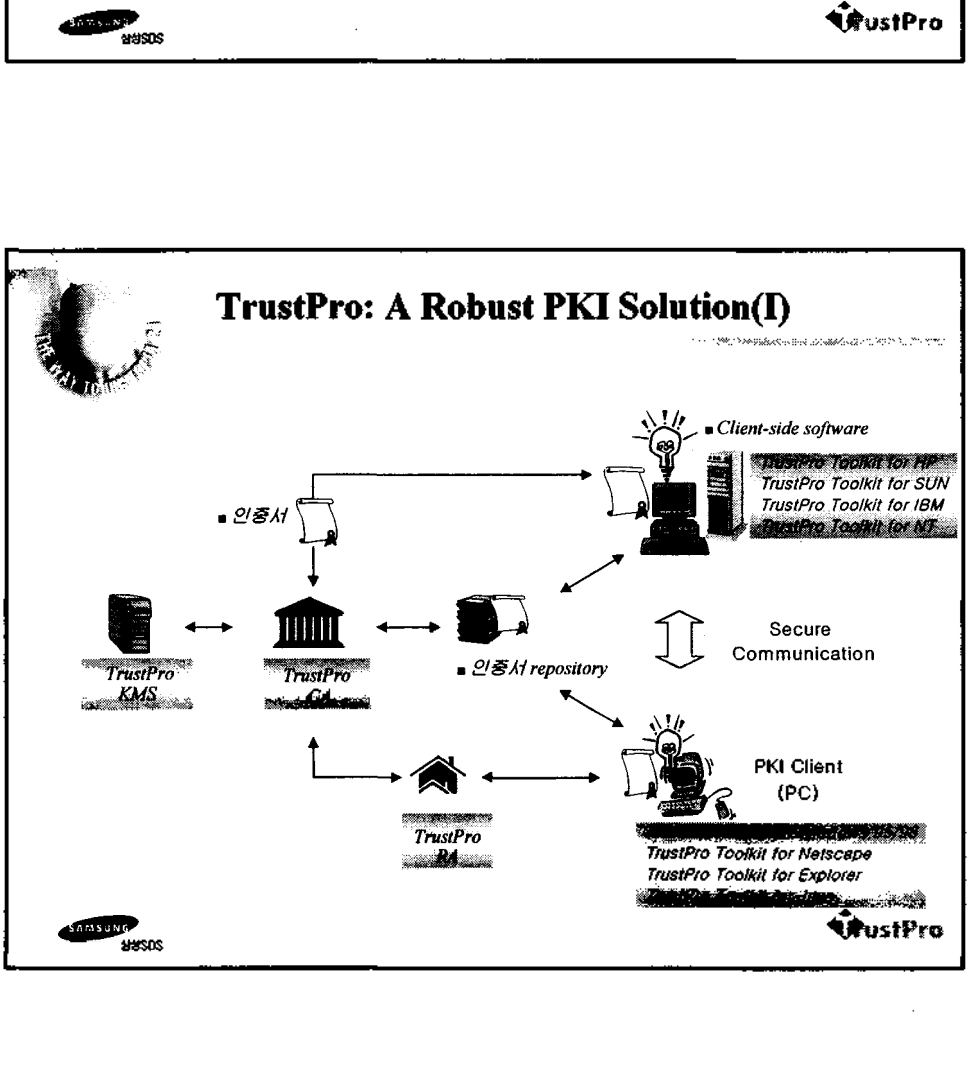
Public Key Infrastructure: An Overview



What Can You Do with a PKI



TrustPro


TrustPro: A Robust PKI Solution(I)
Client-side software
TrustPro Toolkit for SUN
TrustPro Toolkit for IBM
인증서
TrustPro KMS
TrustPro
인증서 repository
Secure Communication
PKI Client (PC)
TrustPro
TrustPro Toolkit for Netscape
TrustPro Toolkit for Explorer

TrustPro: A Robust PKI Solution(II)

제품 구성	출시일
■ CA Server Family	
✓ TrustPro Certificate Authority	1999.7.31
✓ TrustPro Registration Authority	1999.7.31
✓ TrustPro Key Management	1999.7.31
✓ TrustPro OCSP	1999.8.31
✓ TrustPro TimeStamp	1999.8.31
■ Toolkit Family	
✓ TrustPro Toolkit for Unix	1999.7.31
✓ TrustPro Toolkit for Windows	1999.7.31
✓ TrustPro Toolkit for Web	1999.7.31
✓ TrustPro Toolkit for Java	1999.7.31.

SAMSUNG 삼성SDS

TrustPro

TrustPro CA Server Family

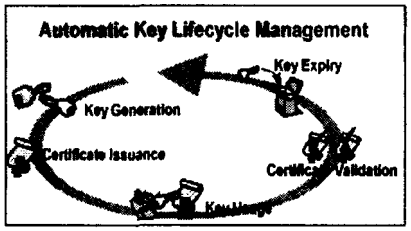
- 국가 공인 인증기관 운영 system 규격안을 지원하는 분산 system 제공
  - TrustPro Registration Authority Server (*등록관리 system*)
    인증서 / CRL등 각종 신청 정보 처리
  - TrustPro Certificate Authority Server (*인증서 생성 system + 키 생성 system*)
    인증서 및 CRL 생성 관리
    독립적인 CA key 및 관리자 key 생성 / 저장 관리
    Smart card interface 지원
  - TrustPro Key Management Server
    암호화 key 쌍 저장 관리
- 인증서 발급 권한 분산 기능 (1명 이상의 관리자 확인을 통한 인증서 발급)
- 기능별 관리자 설정 기능
- 다양한 정보 검색 / 관리 기능
- 강력한 auditing 및 back-up 기능

SAMSUNG 삼성SDS

TrustPro

TrustPro CA Server

- 인증서 발급 / 갱신 / 정지 / 회복 / 폐기 (*Key lifecycle 관리*)
- 암호화 key 쌍 생성
- 인증서 폐기 목록 (Certificate Revocation List: CRL) 자동 생성
- 인증서 repository (directory server)로 인증서 및 CRL 자동 배포
- Key management server 및 directory server 원격 관리 기능
- 인증서 발급 정책 설정 / 관리 기능
- 인증기관간 상호 인증 설정 기능
- 관리자 전자서명 key 생성 및 저장 관리
- Smart card interface 지원



SAMSUNG 삼성SDS

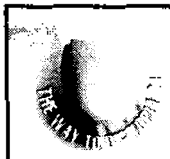
TrustPro

TrustPro RA Server

- **TrustPro Registration Server**
  - 인증서 발급 / 갱신 / 정지 / 회복 / 폐기 요청 정보 관리
  - 인증서 발급 정보 관리
  - CRL / CSL 생성 요청 정보 관리
  - 감사 기록 관리
  - 사용자 정보 관리: 사용자 등록 / 수정 / 검색
- **TrustPro Key Management Server**
  - 암호화 key 쌍 저장
  - Key 검색 / 조회
  - Key history 관리

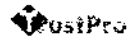
SAMSUNG 삼성SDS

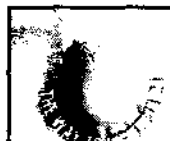
TrustPro



TrustPro Toolkits

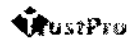
- Key 생성 및 인증서 관리
  - Symmetric key 생성
  - 전자서명 key 쌍 생성
  - 전자서명 private key 암호화 저장
  - 인증서 발급 / 재발급 요청
  - 인증서 download 및 설치
  - 인증서 폐기 요청 및 확인
  - 인증서 사용 관리 기능 (1 PC 다수 사용자 또는 1인 다수 인증서)
  - CRL download 및 인증서 유효성 검사
- 암호화
- 전자서명
- Smart Card interface 지원



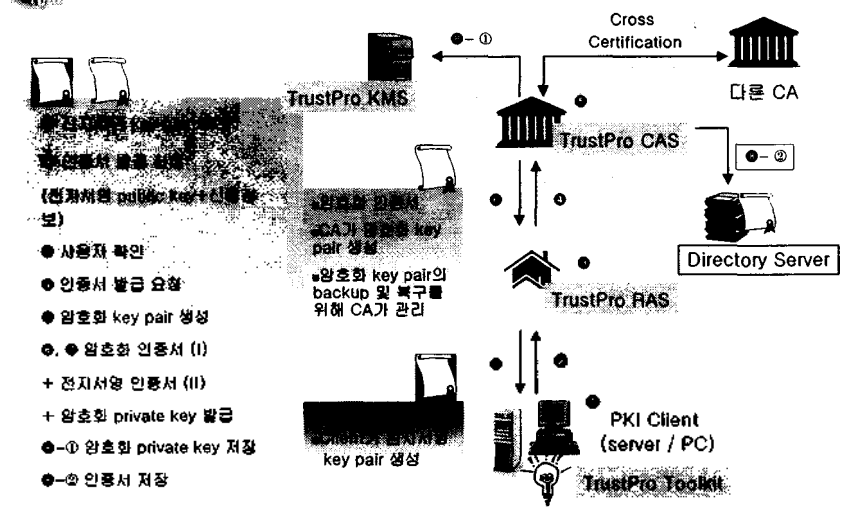


TrustPro Toolkit Family

- TrustPro Toolkit for Unix
  - Hardware Platform: HP, SUN, DEC, etc
- TrustPro Toolkit for Windows
  - Hardware Platform: Windows 95, Windows 98, Windows NT
- TrustPro Toolkit for Web
  - Netscape: Plug-in
  - MS IE: Active-X controls
- TrustPro Toolkit for Java
  - Java programming을 위한 JNI 및 MS Java/Com Integration model에 기반한 Java Classes



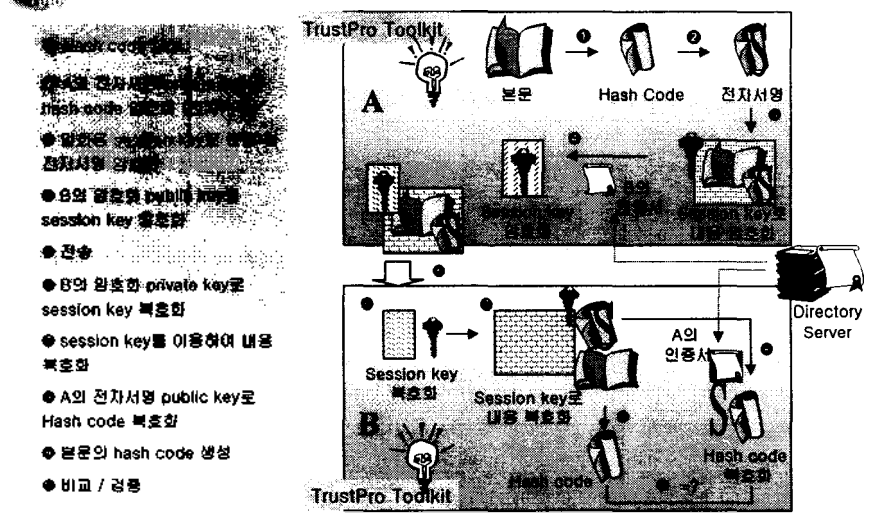
Issuing Certificate with TrustPro



삼성SDS

TrustPro

Encryption & Digital Signature with TrustPro

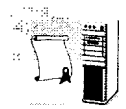


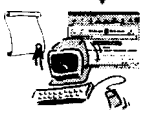
삼성SDS

TrustPro

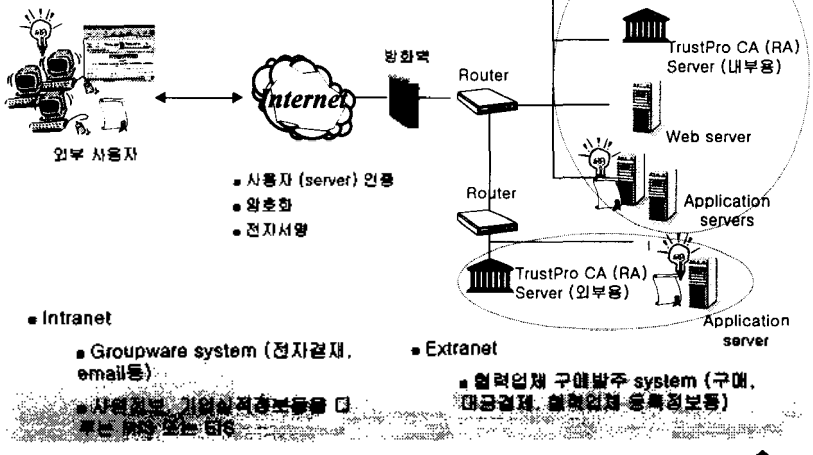
Web-based Security

	SSL	TrustPro
▪ Server	Web server	Web server + TrustPro toolkit
▪ 통신 protocol	HTTPS	HTTP
▪ 보안 기능	① 송수신되는 모든 data의 ② 암호화	① 원하는 data의 ② 암호화 및 전자서명
▪ 암호화 방식		
▪ Data	Symmetric key 방식	Symmetric key 방식
▪ Key 교환시	Public key 방식	Public key 방식
▪ Data 암호화 key 길이	40bit (128 bit)	128 bit
▪ Client	Web browser	Web browser + TrustPro toolkit (Plug-in)





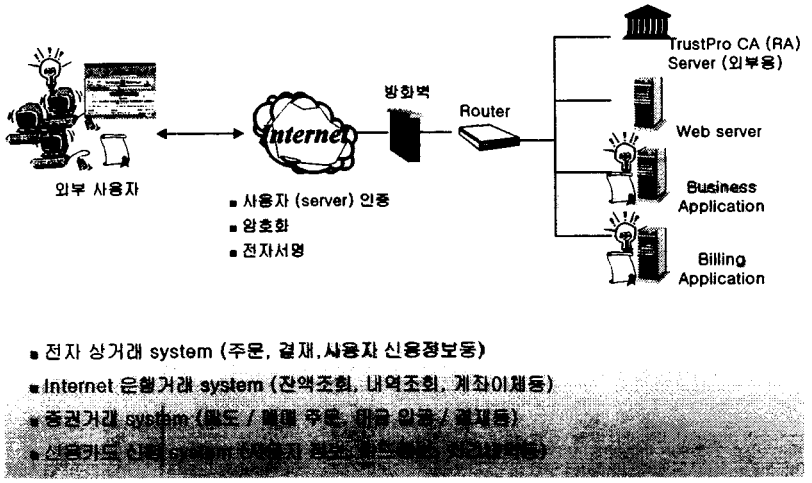
Case Studies (1) - 기업체 적용 사례



▪ Intranet
- Groupware system (전자결재, email등)
- 사원정보, 기업실적등록등을 다루는 MIS 또는 EIS

▪ Extranet
- 협력업체 구매발주 system (구매, 대금결제, 협력업체 등록정보등)

Case Studies (2) - 대고객 서비스 적용사례



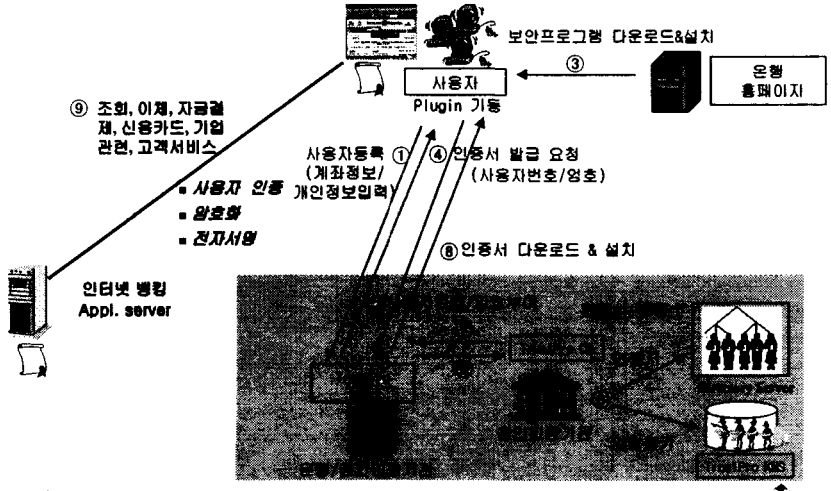
- 전자 상거래 system (주문, 결재, 사용자 신용정보등)
- Internet 은행거래 system (잔액조회, 내역조회, 계좌이체등)
- 증권거래 system (매도 / 매매 주문, 대금 입금 / 출금등)
- 신용카드 신청 system (신청정보 입력, 발급여부, 처리상태등)

삼성SDS

TrustPro

Case Studies (3) - 인터넷뱅킹

인증서 발급 요청 및 설치 등의 관리 프로그램을 RA에서 제공하는 경우

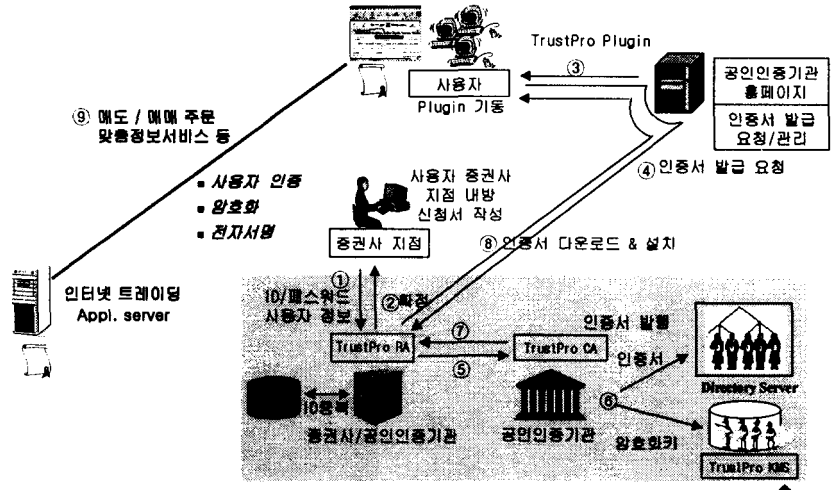


삼성SDS

TrustPro

Case Studies (4) - WEB trading

인증서 발급 요청 및 설치등의 관리 프로그램을 인증기관 홈페이지에서 제공하는 경우



SAMSUNG 삼성SDS

TrustPro

TrustPro Reference Sites

• 조달EDI	조달청 EDI Project
• 삼성전자	삼성전자 구매 EDI PJT(Glonets)
• 삼성증권	Web 기반의 증권거래 system
• 정보통신부	체신금융 관리 system
• 한국디자인진흥원	Internet Shopping Mall
• 삼성SDS	협력업체 구매발주 system
• 삼성SDS	인증기관 구축 (uniSign)

SAMSUNG 삼성SDS

TrustPro

TrustPro: A *de-facto* Standard

- 수년간의 site 지원 경험을 바탕으로 한 안전하고 효율적인 solution
- 기업 및 공공기관에 다양한 reference sites 구축
- 인증관리센터 구축 solution 및 consulting 제공 (한국정보보호센터 root CA)
- 정보통신부 장관상 수상 (SoftExpo'98)
- Open Standard 지원
  - PKI 표준 (X.509) 인증서 및 CRL 형식
  - Directory server에 PKI 정보를 저장하고 취득을 위한 표준 protocol 지원 (Light Weight Directory Access Protocol (LDAP))
  - Third-party application software와의 (Web browser, server등) 호환성을 위한 표준 지원 (PKCS #1, PKCS #7, PKCS #10)
- 다양한 암호화 방식 지원
  - Symmetric key 방식 : DES, Triple-DES, SEA (삼성, 128 bit), SEED (국내표준)
  - Public key 방식: RSA, KCDSA (국내표준)
  - Hashing: SHA, SHA-1, MD2, MD5, HAS-160 (국내표준)

삼성SDS

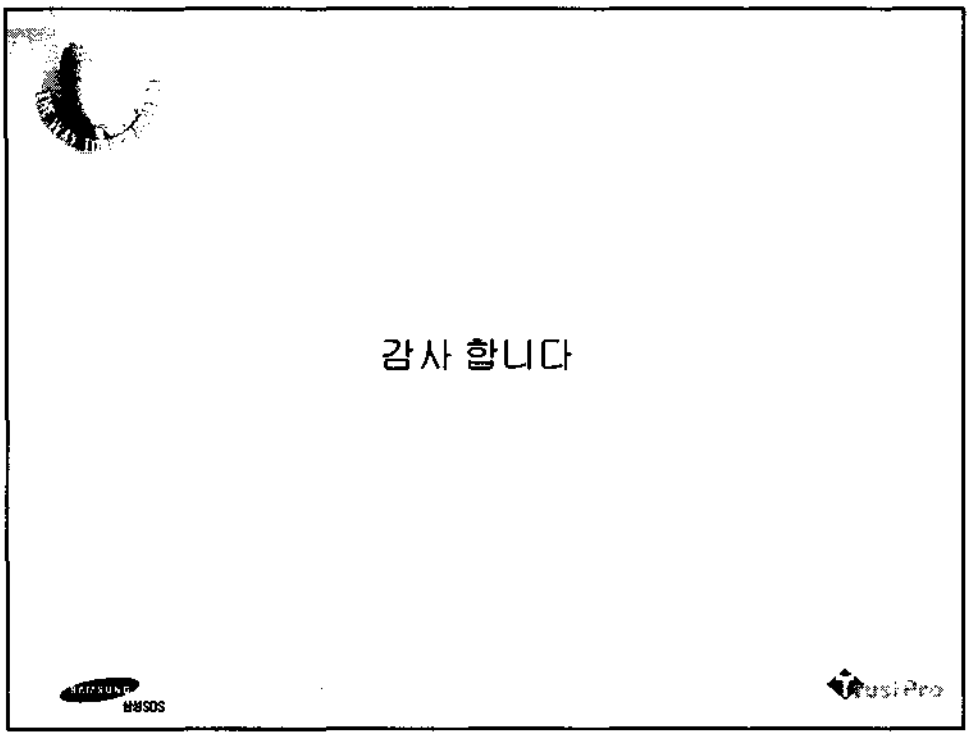
TrustPro

Summary

- TrustPro - A robust PKI solution
- 제품 구성
  - CA service를 위한 Solutions
  - Application Secuity (사용자 인증 / 암호화 / 전자서명)를 위한 toolkits
- 국가 공인인증기관 운영 system 규격안 지원
- 효과적인 PKI 구축을 위한 consulting 제공

삼성SDS

TrustPro


감사 합니다