Trustpro

정보통신부장관상

제작자

☐ 회사명 : 삼성SDS
☐ 주소 : 강남구 역삼동 707-9 일옥빌딩
☐ 전화번호 : 3429-5378

1. TrustPro 개요

1.1 제품 개요

TrustPro 제품군은 SSL, LDAP, SET등 다양한 프로토콜을 동시에 지원하는 PKI(Public Key Infrastructure) 솔루션으로 전자 상거래와 같은 상업용 서비스를 위한 어플리케이션은 물론 기업내에서 운영되는 다양한 application들에게 보안 기능 제공할 수 있는 기반 구조 구축을 지원하는 솔루션입니다.

TrustPro는 다양한 플랫폼을 위한 certificate발급과 이 certificate에 기반한 사용자의 인증(Authentication)기능을 기본적으로 제공하며, 사용자간 또는 서버와 사용자간의 메시지에 대한 프라이버시 보장 및 메시지에 대한 무결성 및 부인 봉쇄 구현을 위한 암호화와 전자서명 기능을 제공합니다.

1.2 제품 구성

TrustPro 제품군은 인증 서버와 각종 application에 적용 가능한 toolkit으로 구성됩니다. Toolkit은 크게 client/server application용과 WEB application용으로 구분되며 client/server용 toolkit은 서버용과 윈도우용이 있습니다.

■ TrustPro CA for Enterprise(CAE)

모든 application 및 system을 지원하는 인증기관 S/W package.

■ TrustPro Toolkit for Windows & UNIX

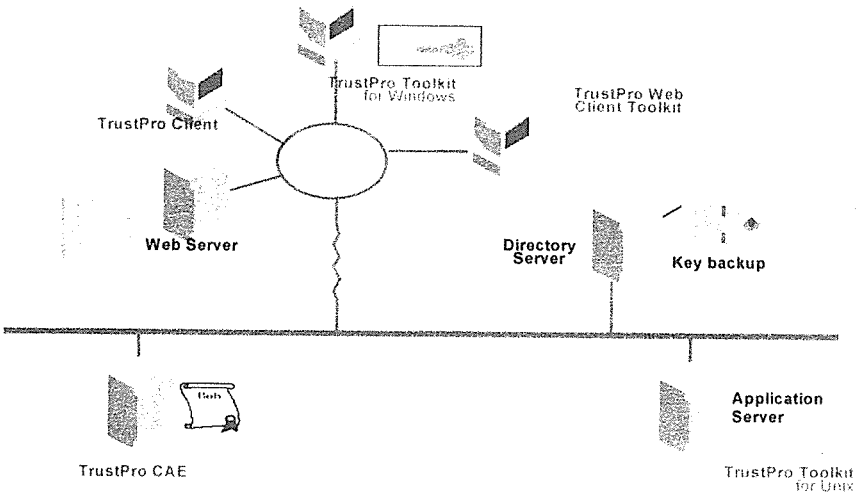
특정 application이나 system을 위해 certificate 관련 기능 및 암호화, 전자서명 기능을 구현하기위한 toolkit.

■ TrustPro Web Client Toolkit

Web application상에서 certificate 관련 기능 및 암호화, 전자서명 기능을 구현하기 위해 web browser에서 사용될 수 있는 toolkit.

■ TrustPro Client

Windows 환경하에서 certificate 요청 및 암호화, 전자서명 기능을 지원하는 end user용 package



2. 제품의 기능과 특징

2.1 TrustPro CAE

기능

■ 국제 표준 수용

- X.509v3, SSL(Secure Socket Layer), SPKM(Simple Public Key Mechanism), LDAP(Lightweight Directory Access Protocol)등의 각종

국제 표준 수용

■ 사용자 정보 관리

- 사용자 등급별 정책 적용 및 정보 검색 기능 제공

■ Certificate 관리 및 Key 관리

- 사용자의 암호화 키 쌍 생성
- 사용자 암호화 및 전자서명 키에 대한 certificate 발급, 폐기
- 인증서 발급/폐기시 사용자별/등급별 auto및 batch 발급 처리
- Key 및 certificate의 자동 생성 및 배포
- CRL(Certificate Revocation List) 자동 생성 및 배포
- PKCS #7 Message 지원
- 키관리 시스템을 이용한 사용자 암호화키 관리

■ 다양한 Client 지원

- TrustPro PKI Client, Netscape Enterprise Server/Navigator, Microsoft IIS/Explorer, SET Client

■ CA(Certificate Authority) 서버 관리

- Certificate 발급 정책관리 : 사용자 등급별 정책관리 및 적용, Certificate 및 Key Lifetime, X.509v3 extensions 적용 정책 관리, CRL 배포 및 갱신 주기관리
- 복수관리자 등록 및 관리 : 운영, 정책, certificate발급 관리자 정보관리 및 작업권한 부여
- 서버 기동 및 종료 : Certificate 서버, Directory 서버, 키 관리서버 기동 및 정지
- Audit 및 status 감시 기능
- Web을 이용한 관리자 환경 지원
- Remote 시스템 접속 관리 : X.500 DS, 키 관리 서버 접속 정보 관리

특징

■ LDAP를 사용한 X.500 DS 접속 지원

■ Certificate Format : X.509v3, ISO standard extensions

■ Standard Compliance : X.509v3, PKCS

■ 지원 알고리즘

- Symmetric : DES, Triple-DES, RC2, RC4, SEAL(국내 개발 알고리즘)
- Asymmetric : RSA, KCDSA (한국 표준 전자서명 알고리즘)
- Hashing : SHA, SHA-1, MD2, MD5

* 사용자가 고유 알고리즘 제공시 대치 가능

■ 지원 Client

- TrustPro PKI Client, Netscape Enterprise Server 3.0, Netscape Navigator 3.0+, Communicator 4.0+, Microsoft IE 3.0+, Microsoft IIS 4.0

■ 지원 Platform

- UNIX

2.2. TrustPro Toolkit for Windows & UNIX

기능

■ 키 관리 및 certificate 관리

- 전자서명 개인키 생성 및 암호화(PBE)
- Certificate 발급 요청
- 암호화 개인키 및 certificate 다운로드/설치
- Certificate 폐기요청
- CRL 다운로드
- Certificate 유효성 검사

■ 파일 암호화 및 복호화

- Symmetric & Asymmetric 암호화, 복호화
- 전자서명 생성 및 verify
- PKCS #7 Message 지원

■ LDAP를 사용한 X.500 DS 접속 지원

특징

■ 지원 알고리즘

- Encryption : DES, Triple-DES, RC2, RC4, SEAL(국내 개발 알고리즘)
  Digital Signature : RSA, KCDSA(한국 표준 전자서명 알고리즘)

Hashing : SHA, SHA-1, MD2, MD5

■ Certificate Format - X.509v3, ISO standard extensions

■ Standard Compliance - X.509v3, PKCS

■ 지원 Platform - Windows 95 & 98, Windows NT, UNIX

2.3. TrustPro Web Client Toolkit

기능

■ 키 관리 및 certificate 관리

- 전자서명 개인키 생성 및 암호화(PBE)
- Certificate 발급 요청
- 암호화 개인키 및 certificate 다운로드/설치
- Certificate 폐기요청
- CRL 다운로드
- Certificate 유효성 검사

■ 파일 암호화 및 복호화

- Symmetric & Asymmetric 암호화, 복호화
- 전자서명 생성 및 verify
- PKCS #7 Message 지원

■ Plug-in 방식의 web browser interface 지원

- Netscape navigator : Plug-in
- Microsoft explorer : Active-X control
- 다양한 web 개발 툴과의 완벽한 호환성

■ LDAP를 사용한 X.500 DS 접속 지원

특징

■ 지원 알고리즘

- Encryption : DES, Triple-DES, RC2, RC4, SEAL(국내 개발 알고리즘)
  Digital Signature : RSA, KCDSA(한국 표준 전자서명 알고리즘)
  Hashing : SHA, SHA-1, MD2, MD5

■ Certificate Format - X.509v3, ISO standard extensions

■ Standard Compliance - X.509v3, PKCS

■ 지원 Platform - Windows 95 & 98, Windows NT, UNIX

2.4. TrustPro Client

기능

■ 사용자 정보 관리 지원

- 개인 정보 등록 및 변경 요청

■ 키 관리 및 certificate 관리

- 전자서명 개인키 생성 및 암호화(PBE)
- Certificate 발급 요청
- 암호화 개인키 및 certificate 다운로드/설치
- Certificate 폐기요청
- CRL 다운로드
- Certificate 유효성 검사

■ 파일 암호화 및 복호화

- Symmetric & Asymmetric 암호화, 복호화
- 전자서명 생성 및 verify
- PKCS #7 Message 지원

■ LDAP를 사용한 X.500 DS 접속 지원

특징

■ 지원 알고리즘

- Encryption : DES, Triple-DES, RC2, RC4, SEAL(국내 개발 알고리즘)
  Digital Signature : RSA, KCDSA(한국 표준 전자서명 알고리즘)
  Hashing : SHA, SHA-1, MD2, MD5

■ Certificate Format - X.509v3, ISO standard extensions

■ Standard Compliance - X.509v3, PKCS

■ 지원 Platform - Windows 95 & 98

3. TrustPro 제품 특징

■ 표준 지원

TrustPro는 PKI에 관련된 다양한 표준을 지원하여 추후 다른 제품들과의 연동및 타제품 사용자들과 완벽한 호환성을 지원합니다.

- X.509V3, SSL, SPKM, LDAP, PKCS

■ 키 관리 기능

메시지 암호화 및 전자서명 시에 사용되는 각종 키들에 대한 완벽한 관리 기능을 제공합니다.

■ 다양한 알고리즘 지원

국제적으로 사용되는 다양한 공개키/비밀키 암호화 알고리즘, 전자 서명 알고리즘 및 국산 알고리즘을 지원하며 사용자의 고유 알고리즘을 쉽게 적용할 수 있습니다. 또한 각 알고리즘을 위해 다양한 key length를 지원합니다.

■ 인증서 관리 기능

PKI의 주요 요소인 인증서에 대해서 발급, 저장, 조회, 재발급, 폐기 등에 대한 각종 상황을 고려한 다양한 관리 기능을 제공합니다.

■ 확장성

단일 사용자에서 수만의 사용자들까지 확장이 가능합니다.

■ 사용의 편리성

서버 관리 기능을 위해서 WEB기반의 인터페이스를 제공합니다.

■ 다양한 키 저장 매체 지원

이동 사용자나 노트북 사용자들이 TrustPro가 제공하는 보안 기능을 편리하게 사용할 수 있도록 사용자의 키를 플로피 디스켓이나 IC card에 저장할 수 있습니다.

■ C/S 어플리케이션 용 뿐만 아니라, Netscape, Microsoft의 browser들을 지원하는 toolkit을 제공

■ PC에서 사용되는 window용 toolkit이외에 Unix 및 NT 용 Toolkit 제공.

■ Certificate Authority에서 사용되는 Key 관리 서버를 별도로 제공함.

■ TrustPro toolkit을 사용한 경우 이외에 기존 browser(Netscape, Microsoft)들에게도 certificate를 제공함.

4. TrustPro 응용 분야

■ 기업

사용자 인증, 암호화 및 전자서명, Secure WEB application, Secure E-mail등 응용 application에서의 보안기능 구현 및 Firewall, PC 및 Network 보안 솔루션들과의 통합 연계성 확립

■ 은행

Home Banking, 은행간 거래 이체 및 망 보안

■ 보험회사

온라인 가입 및 청구, 요금, 약관, 계정 정보의 접근

■ 증권사

온라인 증권 거래(매수 및 양도) 및 계정 정보 접근, 거래분석등

■ 의료(원격)

환자 기록철의 온라인 접근, 요금 청구, 원격 치료등

■ ISP 서비스

정보자산의 사용관리 및 요금 청구

■ S/W판매

정품 증명(판매자 서명, 무결성 보장) 및 온라인 S/W 판매

■ 오락산업

비디오와 뮤직 앨범등에 전자서명을 하여 도난 및 불법 복제 방지

■ 교육

온라인 코스 운영과 수강생 등록, 요금 청구

■ 회원제 운영

회원들에게 인증서(Certificate)를 발급, 권한 및 특권 부여

5. TrustPro 운영 모델

■ Certificate(이하,인증서) 발급 요청

사용자가 TrustPro Client(또는 Toolkit)를 이용, 자신의 전자서명 키쌍을 생성하고 CA에 인증서 발급을 요청합니다.

■ 암호화 키쌍 생성 및 인증서 발급

CA는 사용자 확인 및 DN의 중복등을 점검하고 암호화 키쌍을 생성하여 키관리 서버(KMS)에 보관합니다. 그리고 암호화 및 전자서명 인증서를 발급하여 Directory Server에 인증서를 배포합니다.

■ 인증서 다운로드 및 설치

사용자는 CA로부터 인증서를 다운로드하여 설치합니다. 이때 사용자 Client로 다운로드되는 정보는 전자서명 인증서, 암호화 인증서, 암호화 개인키등입니다.

■ 암호화 및 전자서명 사인

상대방의 암호화 public key를 Directory Server로부터 획득하고, 이를 이용 암호화한 다음, 자신의 전자서명 private key로 전자서명 사인을 합니다.

■ 복호화 및 전자서명 검증

자신의 암호화 private key로 복호화를 합니다. 상대방의 전자서명 public key를 Directory Server로부터 획득하고, 이를 이용 전자 서명 검증을 합니다.

6. 사용시스템(사용자 요구시스템 : H/W 및 S/W)

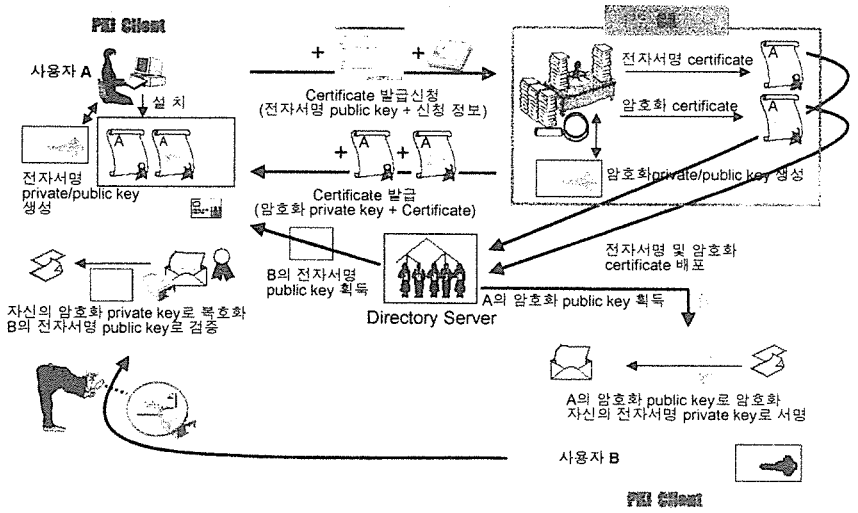
■ Server ;

O/S - HP-UX 9.x, HP-UX 10.x, Solaris 2.4, 2.5

H/W - HP, SUN-Sparc,

기본 memory ; 64MB 이상, HDD ; 120MB

■ PC ;O/S ; Window 95/NT



7. 작용효과

7.1 직접 효과

■ 주요 어플리케이션의 보안성 강화

o 주요 정보들에 대한 암호화 기능

o 사용자에 대한 강력한 인증 기능

o 전자 문서에 대한 검증을 위한 전자서명 기능

■ 강력한 보안 Infrastructure 구성

o 특정 어플리케이션에만 적용하는 것이 아니라 전체 시스템 Infra 차원에서 구현이 되기 때문에 C/S 어플리케이션, WEB 어플리케이션 등에 공통으로 사용되어짐

7.2 간접효과

■ EDI, EC 등 전자상거래 영역에 빠른 선점을 할 수 있음.

■ 최신의 보안 기능을 적용함으로써 know how 축적

■ 특정 어플리케이션 및 시스템 전반에 걸친 보안 level 향상