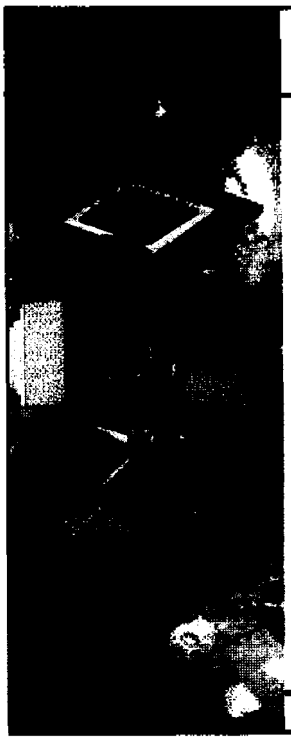


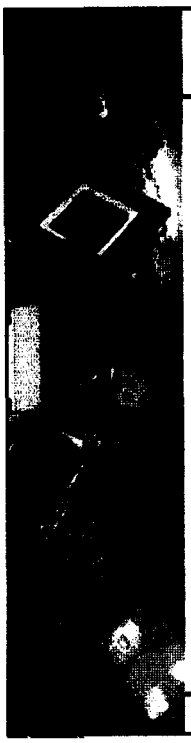
JAVA 보안 컴포넌트 기술

발표자: 박대하

2000.8.29

STI, ㈜ 시큐리티 테크놀로지스
www.stitec.com

S ECURITY Technologies on Internet



목차

STI

S ECURITY Technologies on Internet

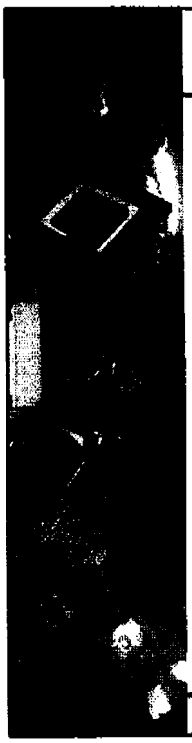
1. E-Commerce 보안

STI
S ECURITY Technologies on Internet

보안 기술

- 인증(authentication)
  정보의 송/수신자 또는 정보시스템 이용자의 신원을 식별, 확인하는 것
- 기밀성(confidentiality)
  전송 또는 보관중인 정보를 비인가자가 부정한 방법으로 입수하더라도 그 내용을 알 수 없도록 보호하는 것
- 무결성(integrity)
  전송 또는 보관중인 정보에 대한 허가되지 않은 변경을 발견할 수 있도록 하는 것
- 부인방지(non-repudiation)
  사용자가 정보통신시스템을 통하여 정보를 송/수신하거나 처리한 사실을 부인할 수 없도록 하는 것
- 접근통제(access control)
  비인가자가 정보통신시스템에 부정한 방법으로 접근하여 사용하는 것을 방지하는 것

STI
S ECURITY Technologies on Internet



EC 암호화 응용

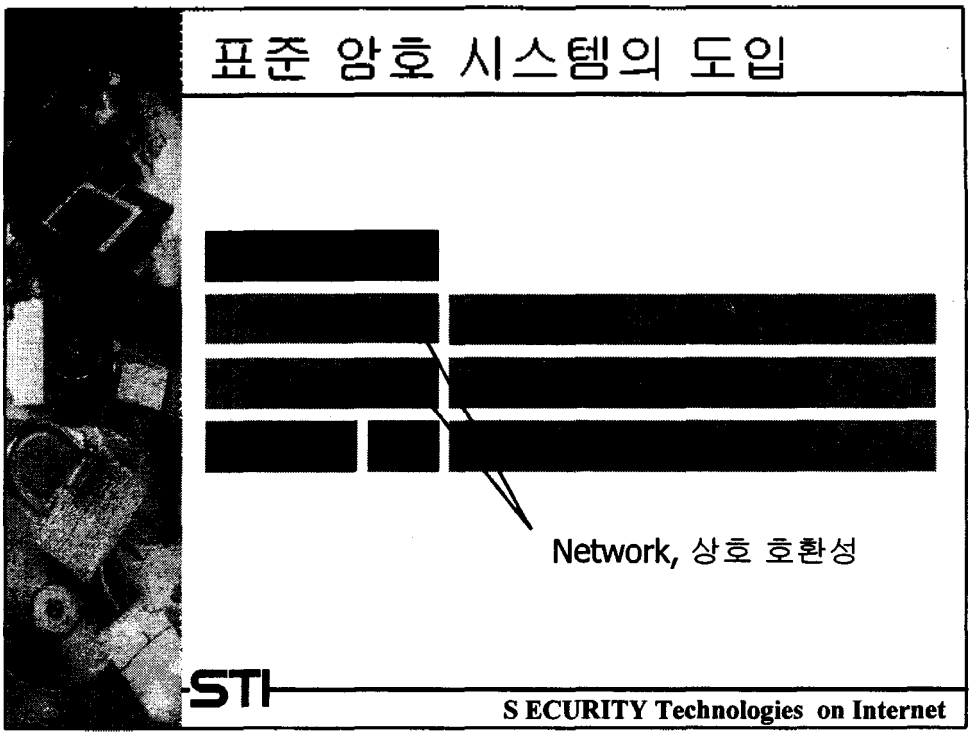
- 보안 로그인
- 보안 (웹) 메일
- 전자 자갑, 전자 수표
- 전자 결제
- 전자 지불 시스템
- 인터넷 뱅킹
- 사이버 트레이딩
- 온라인 쇼핑몰 보안
- ETC.

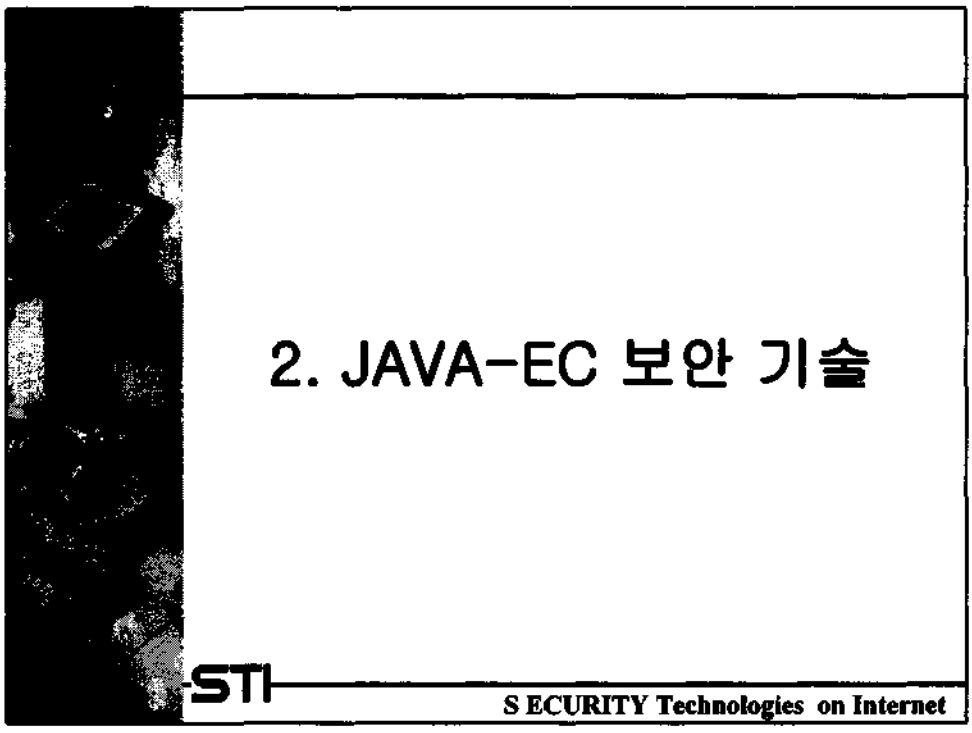
STI S ECURITY Technologies on Internet

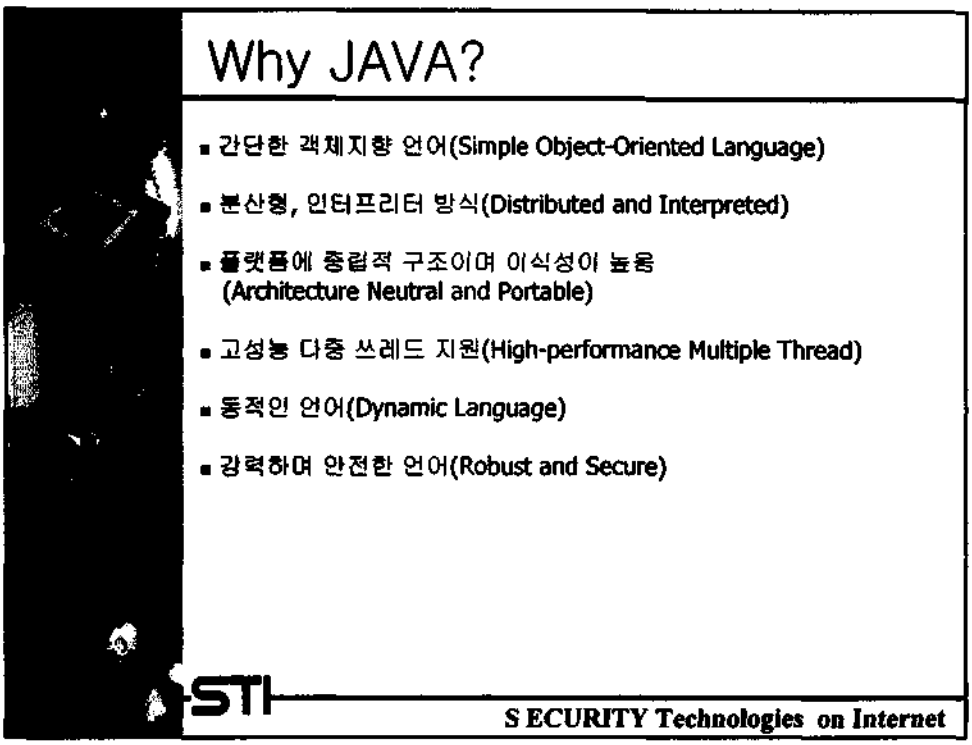
EC 응용 보안 요구사항

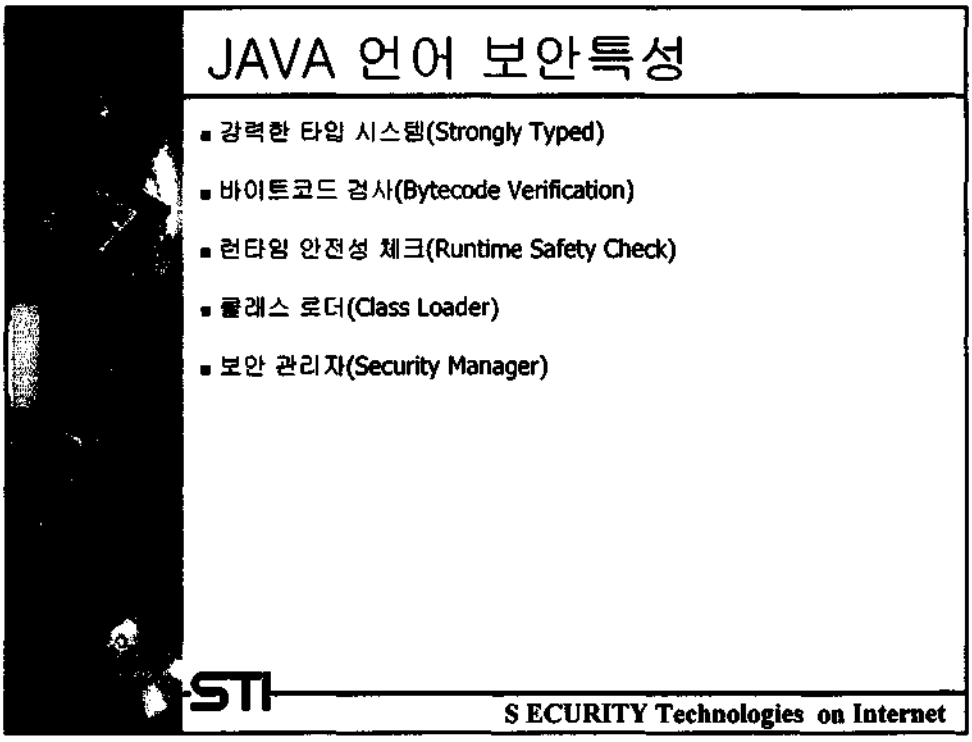
- 사용자 인증
  - Smart Card
  - ID/Password
  - Digital ID(Certificate)
  - One-time Password
- 서버 인증
  - Digital Certificate
- 통신 채널 암호화
  - Web/HTTP
  - MIME
  - SMTP
  - TCP/IP
- 데이터 보호
  - File system
  - RDB
  - XML

STI S ECURITY Technologies on Internet

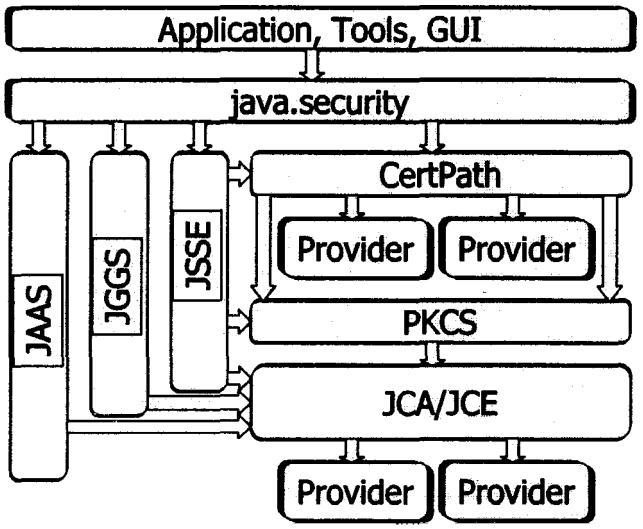

표준 암호 시스템의 도입
Network, 상호 호환성
STI
S ECURITY Technologies on Internet


2. JAVA-EC 보안 기술
STI
S ECURITY Technologies on Internet


Why JAVA?
■ 간단한 객체지향 언어(Simple Object-Oriented Language)
■ 분산형, 인터프리터 방식(Distributed and Interpreted)
■ 플랫폼에 중립적 구조이며 이식성이 높음
(Architecture Neutral and Portable)
■ 고성능 다중 쓰레드 지원(High-performance Multiple Thread)
■ 동적인 언어(Dynamic Language)
■ 강력하며 안전한 언어(Robust and Secure)
STI
S ECURITY Technologies on Internet


JAVA 언어 보안특성
■ 강력한 타입 시스템(Strongly Typed)
■ 바이트코드 검사(Bytecode Verification)
■ 런타임 안전성 체크(Runtime Safety Check)
■ 클래스 로더(Class Loader)
■ 보안 관리자(Security Manager)
STI
S ECURITY Technologies on Internet

JAVA 보안 로드맵 (from SUN Microsys.)



STI
S ECURITY Technologies on Internet

3. JAVA 보안 컴포넌트

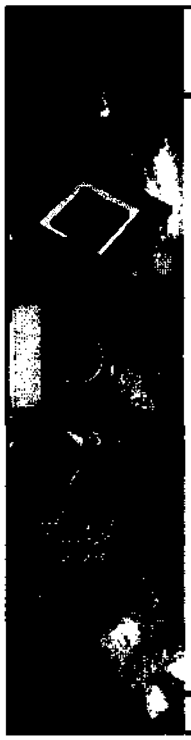
STI
S ECURITY Technologies on Internet

STI 보안 컴포넌트(J-Series)

- J/LOCK™ - Java 암호화 라이브러리
- J/SSLock™ - Java SSL v3 구현 및 API
- J/SecureSession™(J/SS) - 보안 세션 설정용 Java API
- J/CAS™ & J/RAS™ - Java 인증서 발급 및 관리 시스템
- J/PKI™ - Java 기반 PKI 응용 개발 도구
- J/XCT™ - Java 기반 XML 암호화 도구
- K/LOCK™ - KVM 상에서 작동하는 Java 암호화 라이브러리

STI

S ECURITY Technologies on Internet



J/LOCK – 특징

- 100 % pure Java™로 개발된 ㈜STI의 보안 라이브러리
- JCA compliant: JCE 1.2 재구현(100% 호환성)
- Cryptography Provider
- PKCS(RSALab), PKIX(X.509) 표준 지원
- JDK 1.1 및 JDK 1.2 보안 모델을 동시에 지원

STI

S ECURITY Technologies on Internet

J/LOCK – 주요기능

- 다수의 국제 관용표준 암호화 알고리즘 구현
- 국산 암호화 알고리즘(SEED, HAS160, KCDSA) 포함
- 암호화 구문 서비스(ASN.1, DER, BASE64)
- 난수 및 키 생성 서비스
- PKCS #1, PKCS #3, PKCS #5
- PKCS #7, PKCS #8, PKCS #10, PKCS #12
- X.509 v3 Certificate, X.509 v2 CRL, X.509 Extensions

STI

S ECURITY Technologies on Internet

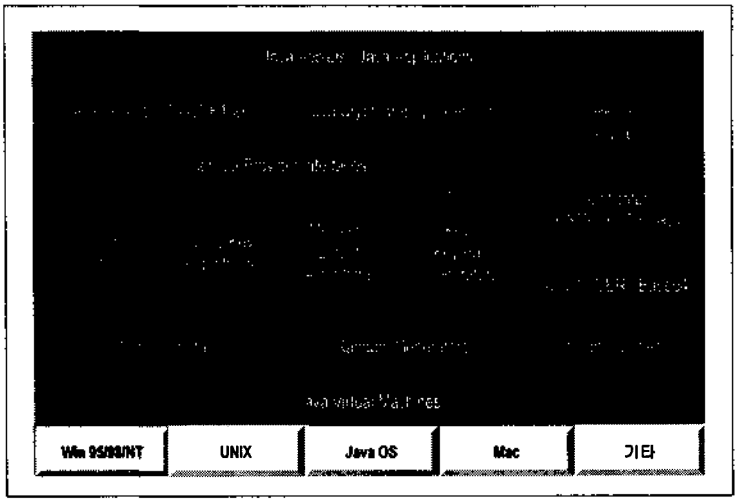
J/LOCK – 암호화 알고리즘

- 해쉬 알고리즘
  - MD2, MD5, SHA-1, RIPEMD128/160, HAS160, HAVAL
- 전자서명 알고리즘
  - RSA(w/MD2, w/MD5, w/SHA1, w/HAS160)
  - DSA(w/SHA1)
  - KCDSA(w/SHA1, w/HAS160)
- 키 협상 알고리즘
  - Diffie-Hellman(PKCS#3)
- 암복호 알고리즘
  - SEED, DES, TripleDES, IDEA, Blowfish, CAST, RC2, RC4, RC5, SAFER, RSA(PKCS#1 Padding) 등
- 메시지 인증 코드
  - HmacMD5, HmacSHA1, HmacHAS160 등

STI

S ECURITY Technologies on Internet

J/LOCK – 아키텍처

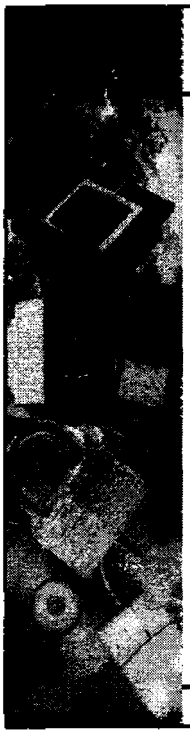


STI
S ECURITY Technologies on Internet

J/SSLock – 특징

- 100 % pure Java™로 개발된 보안 프로토콜
- SSL(Secure Socket Layer) v3.0 호환
- 다양한 암호 알고리즘 조합 지원(국산 표준 알고리즘 포함)
  - SSL_RSA_WITH_SEED_CBC_SHA
  - SSL_RSA_WITH_SEED_CBC_HAS160
  - SSL_DH_DSS_WITH_SEED_CBC_SHA
  - SSL_DH_KCDSA_WITH_SEED_CBC_HAS160
  - SSL_DH_anon_WITH_SEED_CBC_HAS160
  - etc.
- ASN.1, DER 부호화 지원
- 보안 제공자에 독립성 보장(Default - J/LOCK)

STI
S ECURITY Technologies on Internet

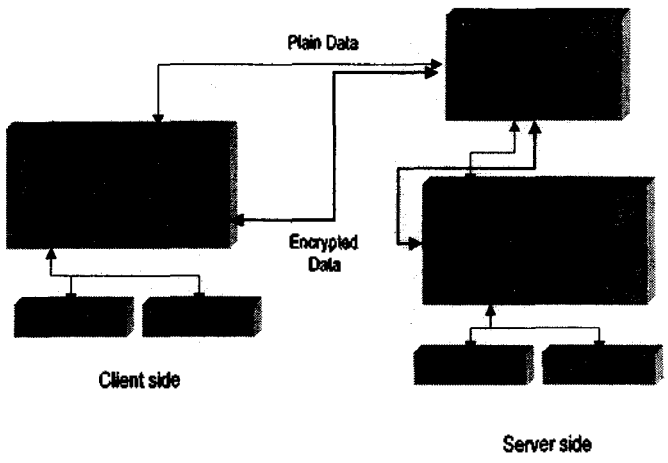


J/SecureSession – 특징

- 다양한 인증 기법을 포함한 보안 채널 설정
  - Digital Certificate
  - SRP(Secure Remote Password)
  - OTP
  - SmartCard
  - CDCard
- 안전한 정보교환 채널 관리
  - TCP/IP Socket
  - HTTP
- SSL보다 빠르고 암호화 알고리즘에 독립적인 전송 프로토콜
- 암호화 라이브러리를 쉽게 이용할 수 있는 API 지원

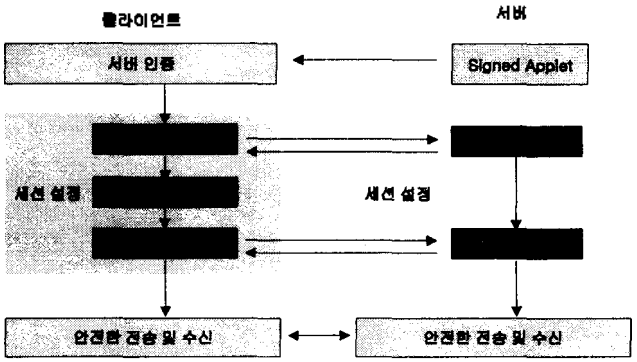
STI
S ECURITY Technologies on Internet

J/SecureSession – Servlet 구조



STI
S ECURITY Technologies on Internet

J/SecureSession – 작동과정



STI
S ECURITY Technologies on Internet

J/PKI – 특징

- 모든 PKI(Public-Key Infrastructure) 기능을 포함하는 라이브러리
  - 키 쌍 생성
  - 인증서 요청 생성
  - 인증서 검색, 수신
  - 키 및 인증서 저장
  - 디렉토리 서버 접근
- 표준 기반의 CA와 호환성 유지
  - X.509(PKIX)
  - PKCS #6, PKCS #7, PKCS #8, PKCS #9, PKCS #10
- 다양한 암호화 알고리즘 지원
- J/CAS, J/RAS, J/SecureSession 연계
- Netscape SSL v3용 RSA 서명 및 확장(extensions)
- 다중 정책 설정 및 인증 경로 검증

STI
S ECURITY Technologies on Internet

J/XCT – 특징

- XML 문서의 보안을 위한 라이브러리 및 도구
  - 서명/검증 : XML Signature
  - 무결성 : DOMHash
  - 암호화 : Element Encryption/Decryption
- ASN.1 DER과 XML간의 상호변환 지원
  - DER(+DTD)/XML 변환
  - XML/DER 변환
- 암호화 표준 DTD 정의 및 자원
  - PKCS #7, PKCS #8, PKCS #10
  - X.509 v3 Certificate, X.509 v2 CRL
  - S/MIME, LDAP
- javax.xml.parsers(JAXP) 기반
  - DOMParser : org.w3c.dom
  - SAXParser : org.xml.sax

STI

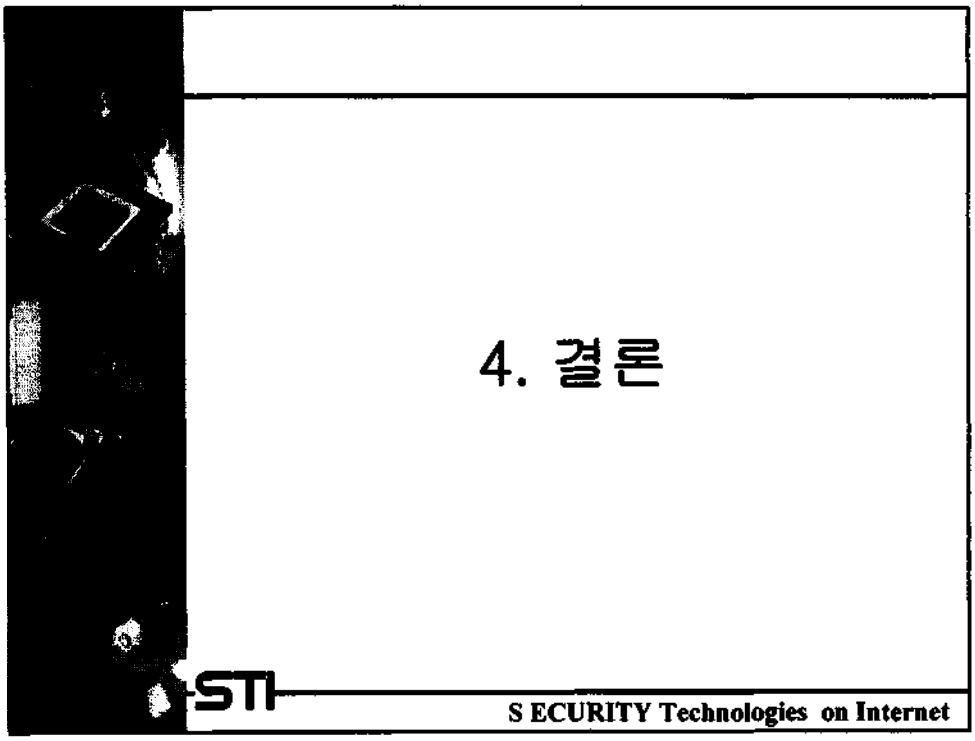
S ECURITY Technologies on Internet

K/LOCK – 특징

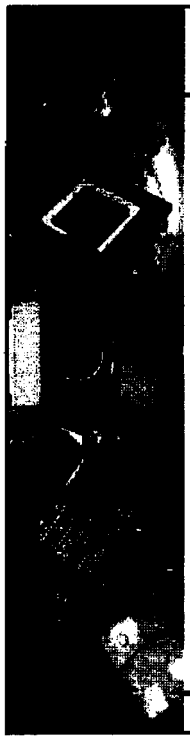
- KVM 상에서 작동하는 Java 암호화 라이브러리
  - CLDC 기반
  - Footprint < 80K
- J/LOCK과 상위 호환성 유지
  - JCA/JCE API의 compact version
  - Cryptography Provider Architecture
- ECC(Elliptic Curve Cryptosystem) 지원
- W/PKI용 Certificate 지원
- C Native 코드와 연동하는 BigInteger 함수 개발

STI

S ECURITY Technologies on Internet


4. 결론
STI
S ECURITY Technologies on Internet


To do list...
■ 다양한 JAVA 기술 접합
• JavaBeans™, EJB(Enterprise JavaBeans)
• RMI(Remote Method Invocation)
• Servlet, JSP™(JavaServer Pages)
• JDBC
• JMS(Java Message Service)
• JavaMail
■ JAVA 표준 보안 프레임워크와의 일관성/호환성 유지
• JAAS(Java™ Authentication and Authorization Service)
• JSSE(Java™ Secure Socket Extension)
• JCA/JCE 1.2.1
• CertPath
• Java Commerce™ & JavaCard
■ 국제/국내 암호화 표준의 지속적인 수용 및 연구 활동 참가
■ 국내 전자상거래용 공용 보안 플랫폼 구축
STI
S ECURITY Technologies on Internet



J-Series

Internet SECURITY !!!

Any Environment, Any Location

STI

S ECURITY Technologies on Internet

감사합니다.

STI, ㈜시큐리티 테크놀로지스

TEL : 929-6890 (代) FAX : 929-6891
www.stitec.com

STI

S ECURITY Technologies on Internet