

## 안전한 전자상거래를 위한 보안플랫폼

The Development of a Secure Platform for E-Commerce

주관연구기관  한국전자통신연구원

정 보 통 신 부

## 요 약 문

### 1. 제목

안전한 전자상거래를 위한 보안 플랫폼

### 2. 연구 개발의 목적 및 중요성

전자상거래의 급격한 확산과 함께 전자상거래에 있어서의 표준문서로 자리 잡고 있는 XML 전자문서의 중요성이 대두됨에 따라 전자상거래에 있어서의 XML 전자문서 보안에 대한 필요성이 날로 증가하고 있다.

이에 대하여 인터넷상의 전자상거래에 있어 보다 안전한 거래를 위해 전자상거래의 문서표준으로 자리잡고 있는 XML 전자문서에 대한 보안 기술을 제공하는 안전한 전자상거래를 위한 보안 플랫폼을 개발한다.

### 3. 연구 개발의 내용 및 범위

본 연구는 ebXML (electronic business XML) 국제 표준 등을 적용한 전자상거래 시 교환되는 XML 전자문서에 대한 다음과 같은 보안 기술들을 포함하는 전자상거래 보안 플랫폼 개발한다.

- XML 전자서명 기능
- XML 암호화 기능
- Java기반의 암호 처리 기능 및 PKI 기반의 정보보호 기술
- 키복구 시스템
- 인증서 내장 자바카드 지원 기능

#### 4. 연구 개발 결과

- 안전한 전자상거래를 위한 보안 플랫폼 구축
  - XML 전자서명 모듈 개발
  - XML 암호 모듈 개발
  - JAVA Crypto API 개발
  - CA Client 서브 시스템 개발
  - 키복구 시스템 개발
  - 인증서 내장 IC 카드 모듈 개발
- 5개 업체 기술이전
- 연구논문 31편 등 다수의 지적재산권

#### 5. 활용에 대한 건의

- 전자상거래 국제표준인 ebXML 등의 전자상거래 플랫폼에서 정보보호 서비스 제공에 활용
- 모든 형태의 전자상거래 및 EDI 서비스에서 전자문서 정보보호에 활용
- 개인과 기업간, 기업과 정부간, 기업과 기업간 전자상거래에서의 전자 문서 정보보호에 활용

#### 6. 기대 효과

- 국내 전자상거래 정보보호 기술 확보로 인한 기술의 독립성 확보
- 국제 표준으로 적용이 확산되고 있는 ebXML에 적용 가능한 정보보호 기술 확보
- 전자상거래의 신뢰도 증가로 인한 전자 상거래의 활성화에 기여

# Summary

## 1. Title

A Report on the Development of a Secure Platform for E-Commerce

## 2. Objective

As electronic commerce services are used widely and XML is being adopted as a commonly agreed standard for electronic documents in the electronic commerce, the needs of XML security in the electronic commerce are increasing.

We develop a secure platform for electronic commerce, which provides security services to XML documents that are being used adopted as standard documents in electronic commerce.

## 3. Research Scope

The final objective of this project is the development of a secure platform for electronic commerce, which provides security services to XML documents for global standards such as ebXML (electronic business XML), supporting functions:

- XML digital signature
- XML encryption

- Java-based crypto library and PKI-based security technology
- Key recovery system
- Java card API that can store and retrieve embedding certificates

#### 4. Results

- Development of a Secure Platform for E-Commerce
  - Development of XML Signature module
  - Development of XML Encryption module
  - Development of JAVA Crypto module
  - Development of CA Client module
  - Development of Key Recovery module
  - Development of IC card API module to store and retrieve certifications
- Technology transfers to 5 companies
- Intellectual property rights including 31 papers, several patents, programs

#### 5. Applications

- Security services for electronic commerce platforms such as ebXML, the global standard for electronic commerce
- Security services for electronic documents of all kind of electronic commerce and EDI services
- Security services for electronic documents used in Customer to business, business to government and business to business electronic commerce