通信情報保護學會誌
第 11 券 第 2 號, 2001. 4

키 복구 실증 프로젝트에 대한 고찰

이 향 진*, 임 양 규*, 주 미 리**, 원 동 호*

요 약

암호가 급속히 민간에 보급됨에 따라 암호 기술의 여러 장점과 더불어 많은 역기능들이 대두되고 있다. 이에 대한 대책 중의 하나로 키 복구 기술이 제시되었고, 미국을 비롯한 여러 나라에서 이에 대한 연구가 활발히 진행되고 있다. 또한 다양한 상업적 응용 분야에 적합한 키 복구 제품들이 출시되고 있으며, 미국 등에서는 키 복구의 상업적 응용 가능성을 검증하기 위한 키 복구 실증 프로젝트를 진행하고 있다. 본 고에서는 키 복구 기능을 탑재한 제품과 키 복구 기능을 이용할 수 있는 서비스의 범위 등에 대한 고찰을 통해 키 복구의 상업적 이용 가능성을 실증하고자 했던 미국 및 유럽 연합의 키 복구 실증 프로젝트에 대해 살펴본다.

Ⅰ. 서 론

현대 사회가 고도의 정보화 사회로 발전해감에 따라 점차 그 중요성이 부각되고 있는 정보보호의 필요성은 과거 군사적 또는 국가적 차원에서 주로 이용된 암호 사용의 범위를 민간 부문으로 급속히 확대시켰다.

암호의 사용은 정보의 누출 및 오용을 방지하고, 상대방의 신원을 확인할 수 있게 해 줌으로써 온라인 상에서 전자 상거래나 전자 계약 등을 가능하게 하는 등 많은 장점을 가지고 있다. 그러나 이에 반해 범죄자들에 의한 암호의 악용과 키의 분실 및 손상 등에 따른 암호문의 복호 불가 등 그 역기능에 대한 대책으로 현재 키 복구에 대한 연구가 세계적으로 활발히 진행 중이며, 그 결과에 관심이 집중되고 있다.

일반적으로 키 복구란 암호문의 소유자만이 복호할 수 있는 암호화된 데이터에 대해, 특정한 경우에 한해서 허가된 사용자에게 이를 복호할 수 있는 능력을 제공하는 기술 및 체계를 말한다. 그러나 키 복구 방식과 관련하여 개인의 사생활 보호와 정부의 법 집행 능력 보장이라는 두 가지 상반된 목적에 대하여 끊임없는 논쟁이 진행되고 있다.

현재 각 국에서는 정부의 암호화 데이터에 대한 접근권 보장과 개인의 프라이버시 보호 및 전자 상거래 진흥이라는 상반된 요구의 균형점을 찾기 위한 연구가 활발히 진행되고 있으며, 키 복구 방식은 나라마다 정책이나 특성에 따라 조금씩 다른 방식을 사용하고 있다. 또한 이와 함께, 키 복구를 상업적으로 이용하는 경우, 상업적 응용 분야에서의 키 복구 수행 가능성과 실용성 및 실제 서비스 가능한 응용분야의 범위 등에 대한 연구도 활발히 진행되고 있다.

90년대 초에 키 복구가 제안된 미국의 경우, 비교적 정부의 규제가 강한 키 위탁 방식을 주장하여 민간 단체와 업계의 강력한 반대를 불러 일으켰고, 이로 인해 정부의 규제는 다소 완화되었지만 키 복구를 시행한다는 기본 입장에는 변화가 없다. 또한 민간 차원에서의 키 복구가 상업적으로 이용 가능한지를 시험하기 위한 실증 프로젝트 역시 오랜 기간 지속적으로 진행해 오고 있다.

본 고에서는 키 복구 관련 연구 중에서 키 복구의 상업적 응용 가능성을 확인하고자 했던 미국 및 유럽 연합의 키 복구 실증 프로젝트에서 연구된 내용과 각 프로젝트들의 진행 과정 및 프로젝트에 대한 평가 등을 소개하고, 이를 통해 키 복구의 상업적

* 성균관대학교 정보통신보호연구실 (jiinii@dosan.skku.ac.kr)
** 국가보안기술연구소
※ 이 원고는 2000년 정보통신학술진흥사업 지정연구(00-08)에 의하여 연구됨.

응용 가능성을 확인해 본다. 본 고의 2장에서는 미국의 키 복구 실증 프로젝트의 연구 내용과 특징들, 상업적 응용 가능성 등에 대해 알아보고, 3장에서는 유럽 연합에서 진행했던 실증 프로젝트에 관해 소개하며, 마지막으로 4장에서 결론을 맺는다.

II. 미국의 키 복구 실증 프로젝트

다른 국가들에 비해 암호가 발달한 미국은 일찍부터 키 복구에 대해 많은 관심을 가져왔고, 1993년 미 행정부가 발표한 '클리퍼 정책'으로부터 키 복구 정책을 시작했다. 그러나 키 위탁을 전제로 하는 클리퍼의 내용과 기술적 문제 등에 대한 시민단체들의 강한 발발로 정부의 키 복구 정책은 많은 변화를 겪으며, 점차 완화되어 왔다. 특히, 암호 제품의 수출에 있어서도 키 위탁를 강요했던 이전의 수출정책에서 최근 키 위탁의 규정을 제거하는 등의 변화를 보이고 있다[1].

미국은 이 같은 변화를 보이는 키 복구 정책과 함께 키 복구의 상업적 응용 가능성을 검증하기 위한 실증 프로젝트로 KRDP(Key Recovery Demonstration Project)를 오랜기간 진행해오고 있다.

1997년 NIST에서 키 복구 제품과 서비스를 위한 제안서 제출을 공고함으로써 시작된 이 프로젝트는 암호 시스템에 여러 조건들을 만족하는 키 복구 기능을 탑재할 수 있다는 사실을 검증하기 위한 실증 프로젝트의 성격을 가지며, 정부의 지대한 관심과 지원 하에 산업계가 주체가 되어 관련 연구가 활발히 진행되고 있다[2][3].

1. 프로젝트의 목표

IWG(Integragency Working Group)는 GITS(Government Information Technology Services)와 함께 다음과 같은 목표를 달성하기 위한 task group을 설립하고, 10개의 연방 기관를 파일럿으로 선정하여 키 복구 실증 프로젝트를 진행했다[4].

- 연방 정부가 지원하는 응용분야 안에서 키 복구의 실용성을 시험한다.
- 어떤 범위의 상업적인 제작품(Commercial Off-The-Shelf)이나 상업적으로 현재 사용가능한 서비스가 키 복구를 위해 존재하는지를 결정한다. 최소의 난이도로 수정되어질 수 있는 제품이 고려되어질 것이다.
- 어떻게 이러한 제품들과 서비스가 존재하는 응용분야에 결합되어질 수 있는지 결정한다.
- 다양한 키 복구 기술을 식별하고, 실현하고, 테스트하고 평가한다.
- 다른 키 복구 기술을 사용하는 응용분야들 사이의 상호운용성(Interoperability)에 대한 장애를 확인하고 그러한 장벽들을 제거하거나 줄이는 권고안을 만든다.

2. 키 복구 모델의 기준

각각의 파일럿 프로젝트에서 동작하는 키 복구 시스템은 다음과 같은 기준으로 설계되었다.

- 키 복구의 다른 여러 가지 방법에 대한 테스트가 수행될 것이다.
- 암호키는, 인가된 요구에 대한 확인서를 전제로 키 복구 기관에 의해 복구되어진다.
- 디지털 서명을 위해 사용된 키는 복구되지 않을 것이다. 규격화된 기술이 이 프로젝트에 대한 사용을 위해 조사될 것이다.
- 표준 협력이나 알고리즘 사용에 대한 어떤 제약도 없다.
- KRDP는 기본적인 CA(Certification Authority)와 몇 개의 하위 CA들로 구성된 PKI를 포함한다.
- CA는 특별한 사용자 집단의 공개키를 검증하고, 다른 CA영역 내의 공개키가 검증되어지도록 다른 CA에게 인증 경로를 제공한다.
- 기본 CA는 NIST에 위치하고 NIST에 의해 운영될 것이며, 나머지 CA는 프로젝트에 참가하는 에이전시의 사이트나 제 삼자의 사이트에 위치하게 될 것이다.
- BAA(Board Agency Announcement)하에서 얻게될 KRDP의 다른 내용들은 기구 등록 기관(Organization Registration Authorities)과 키 복구 기관(Key Recovery Agents)을 포함한다.
- 키 복구 기관은 인가된 요구의 확인서 하에 키, 키 구성 요소, 혹은 평문 메시지의 복구를 위해 사용되어 진다.
- 기반구조는 구현에 대한 제한요소를 부과하지

않는다.

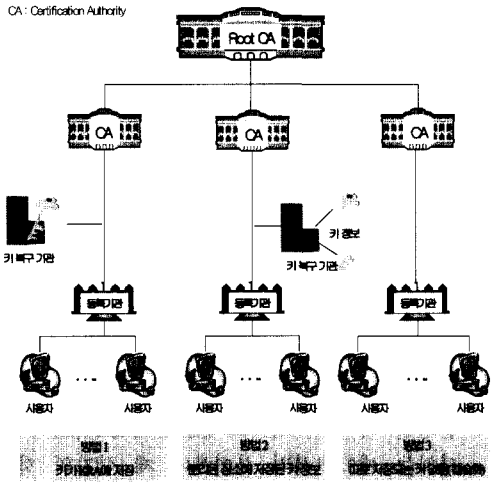
- CA와 키 복구 기관에 의해 제공된 서비스의 예제는 단일 제품 내에 포함되어질 수 있다.
- 공개키 기반 구조(Public Key Infrastructure :PKI)에서 키 복구를 수행하는 세 가지 가능한 방법을 설명한 예제 기반구조는 그림 1과 같다[5].

3. 프로젝트 내용 및 특징

1997년 NIST에서 공고한 키 복구 제품과 서비스를 위한 제안서에서 요구하는 제품의 구성 요소 및 서비스에 대한 내용은 다음과 같다

3.1 제품 및 서비스 관련 요구 내용

키 복구 제품 개발자는 키 복구 실증 프로젝트에 사용될 수 있는 규격화된 제품과 서비스들에 관하여 다음의 사항들을 명시하도록 했다



〔그림 1〕 PKI 환경에서 가능한 키 복구 모델

- 제품 또는 서비스(예: CA, 등록 기관, 키 복구 기관, 사용자)의 기능.
- 제품 또는 서비스 제공 여부.
- 제품 또는 서비스에 의하여 제공되는 모든 특징들의 목록.
- 제안된 키 복구에 사용되는 방법에 관한 설명.
- 제안된 제품 또는 서비스가 현재 이용 가능한지 여부, 만약 현재 이용 가능하지 않다면 예상되는 가용 날짜.
- 제안된 제품 또는 서비스를 조작, 운용, 그리고 이것과 통신하기 위한 요구사항들.
- 제품 또는 서비스가 어떻게 다른 제품 개발자 또는 다른 프로젝트 요소들 (예, CA, 등록 기관)에 의하여 제공된 제품 또는 서비스에 집적될 수 있는지를 상술하는 정보.
- 특별한 암호학적 알고리즘, 암호학적 제품, 통신 인터페이스 등에 대한 의존성과 같은 제품 통합 상의 제약들.

3.2 KRDP 요소들에 관한 요구 내용

KRDP의 요소들로 인증센터, 키 복구 기관, 기구 등록 기관, 사용자 소프트웨어, 파일럿을 규정하고, 각 요소들에 요구되는 다음의 사항들을 명시하도록 했다.

3.2.1 인증 센터

- 인증 센터 시스템은 공개키들을 인증하고 공개·비밀 키 쌍들을 선택적으로 생성하고 인증하는 역할을 수행한다.
- 만약 인증 센터 시스템이 서비스로서 제공된다면, 제공된 서비스들과 각 서비스의 비용을 일일이 열거한다. 즉, 변경하는 비용과 제공된 서비스를 얻는 방법을 일으키는 요소들을 설명해야 한다.
- 인증하는 장소만을 제공하는 제품 개발자는 이 서비스에 접근하는 비용과 방법을 일일이 열거해야 한다.

3.2.2 키 복구 기관

- 만약 키 복구가 서비스로서 제공된다면, 키 복구 서비스를 가지고 저장하는 비용과 키 복구 연산들의 비용들을 일일이 열거해야 한다.
- 등록된 사용자들의 수와 키 복구가 수행된 수에 의존하는 비용들이 어떻게 변경되는지, 그리고 가능하다면, 제공된 키 기록의 서비스들과 이런 서비스들의 비용을 일일이 열거해야 한다.
- 암호학적 제품들이 키 복구 서비스와의 결합에서 사용되어야 하는 비용들을 목록에 기입하고 일일이 열거해야 한다.

- 만약 키 복구 제품이 사용자에 의하여 동작하기 위하여 획득될 수 있다면, 가격에 영향을 미치는 모든 요소들의 목록을 작성해야 한다.
- 암호학적 제품들이 키 복구 서비스와의 결합에서 사용되어야 하는 비용들을 목록에 기입하고 일일이 열거해야 한다.

3.2.3 기구 등록 기관

- 기구 등록 기관의 획득과 동작과 관련된 모든 비용들을 일일이 열거해야 한다.
- 적용할 수 있는 곳에서, 인증 센터와 키 복구 대리인과 상호작용의 방법을 설명해야 한다.

3.2.4 사용자 소프트웨어

- 암호화·복호화, 키 생성, 키 복구, 인증 경로 획득 그리고 검증을 수행하는 그리고 다른 시스템 요소들(예, 인증 센터, 키 복구 대리인)과 상호 작용하는 모든 사용자 소프트웨어의 기능과 비용을 일일이 나열해야 한다.
- 응답자(responder)들은 기능적 가능성, 수행에 관한 어떤 부가적인 정보 그리고 제공들을 평가하는 키 복구 실증 프로젝트에 참가하는 연방정부의 기관들을 돕는 제품 또는 서비스의 비용 또한 제공해야 한다.
- 암호학적 함수들이 수행되는 것으로, 응답자들은 FIPS 140-1에서 요구하는 응답자의 제공된 제품 또는 서비스의 등급을 명시해야 한다.
- 응답자들은 가능한 NIST 초안 "Minimum Interoperability Specification for PKI Components"에서 요구하는 응답자의 제공된 제품 또는 서비스의 등급을 일일이 열거해야 한다.

3.2.5 파일럿(Pilot)

KRDP를 수행하기 위하여, 다음의 능력을 기준으로 각 분야별로 10개의 기관이 파일럿으로 선정되었다. 선정된 10개의 연방 기관 파일럿들은 다음의 항목들을 바탕으로 각 요소들을 테스트 할 것이다.

- 크기 및 용도상(다른 애플리케이션으로)의 확장성 제공능력.
- 의미 있고 쉽게 이해 가능한 응용 능력(필수조건은 아님)
- 사용자 집단의 다양성에 대한 기술 복잡성 허용 능력
- 9~15개월 안에 구현하고 평가할 수 있는 능력
- 설계와 구현에서 산업계의 광범위한 참가를 보증하는 능력
- 활용 가능한 정도의 상업제품 사용 능력

4. 파일럿 프로젝트

다음은 각 파일럿 프로젝트의 참여 기관과 수행 내용 및 특징들이다[6].

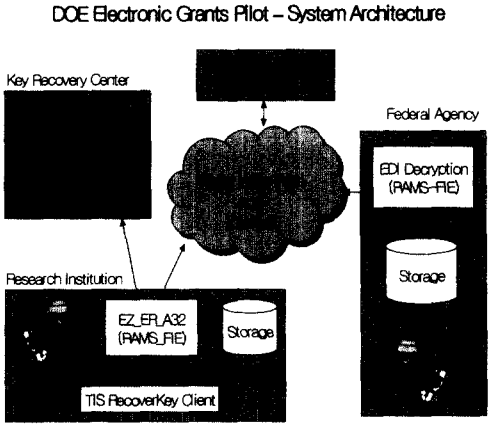
4.1 EDI/Internet Security Project

4.1.1 참여 기관

DOE(Department of Energy)의 Office of Energey Research을 중심으로 ERA (Electronic Research Administration)를 포함하는 8개의 연구기관과 6개의 연방 정부 기관으로 구성되었다.

4.1.2 내용 및 특징

전자 문서의 전송 시 필요한 보안 요구사항으로 EDI 통신 내용에 대한 기밀성과 무결성 및 EDI 처리과정에 대한 인증, 부인불가 기능 등이 있고, 전송된 데이터에 대한 적절한 관리와 안전한 저장이 필요하다. 또한 암호화에 사용된 키를 잃었을 경우 데이터를 복구할 수 있는 키 복구 기능이 필요한데, 이 프로젝트는 이러한 필요를 만족시키기 위해 EDI 시스템에서의 키 복구 기능을 실증해 보이고 있다. 이를 위해 이 프로젝트에서는 안전한 E-Mail을 위



(그림 2) Electronic Grants Pilot.

한 인터넷 표준에 바탕이 되는 EDI 보안을 위한 기술을 테스트하고 있으며, 프로젝트의 초기 구현 목표로 Electronic Grant Application Requirement에 초점을 두고 있다.

그림 2는 이 프로젝트에서 진행하고 있는 키 복구 기능을 가지는 EDI 시스템의 구조이다.

4.2 U.S. Electronic Grants Project

4.2.1 참여기관

DOT(Department of Transportation)의 산하기관을 중심으로 Department of Education, Department of Energy, Environmental Protection Agency, Department of Interior, General Services Administration, Office of Naval Research, Small Business Administration의 기관으로 구성되었다.

4.2.2 내용 및 특징

기존의 데이터 교부 및 인허가 과정은 정부와 사용자 사이에 문서 교환이 많고, 복잡하여 그 과정이 매우 느리기 때문에 이를 인터넷 상에서 가능하도록 하는 Electronic Grants System을 구축하는 것이 이 프로젝트의 목적이다. Internet상에서의 Grant Transaction을 수행하기 위해, 데이터의 공유 및 통합을 용이하게 하고 데이터와 시스템의 보안을 제공하는 공개적이고 유동적인 Electronic Grants System을 구축해야 한다. 이를 위해 안전한 Electronic Grants System이 정부 전역의 데이터 공유해야 하는데, 이 프로젝트에서는 이러한 시스템이 표준 EDI 구조를 유지하면서 낮은 비용과 웹 기술만으로 설계 가능함을 증명하고 있다.

이 프로젝트의 키 복구 시스템은 실시간에 가까운 수행시간을 보장하고, 자바와 Information Broker를 이용한 손쉬운 사용자 인터페이스를 제공하고 있다. 또한 시스템의 보안을 위해 디지털 서명 및 암호화를 제공하고 있으며, 스마트 카드의 내용에 대한 키 복구 능력을 제공함으로써 키 복구의 사용을 실증하고 있다.

4.3 Public Key Infrastructure Project

4.3.1 참여 기관

LLNL(Lawrence Livermore National Laboratory)을 중심으로 구성되었다.

4.3.2 내용 및 특징

이 프로젝트는 LLNL의 기술적, 상업적 기능을 지원하기 위한 공개키 기반구조를 구축하는데 그 목적을 두고 있다. LLNL의 공개키 기반구조에서 제공하는 기능들의 일부분은 많은 다른 DOE의 연구소들과 국가 기관들 및 서비스 제공자들 간의 네트워크를 통한 상호 작용을 포함한다. 이를 위해 LLNL의 공개키 기반구조는 송, 수신되는 정보에 대해 강한 인증과 부인 불가, 메시지 무결성 및 기밀성을 제공 한다. 또한 데이터의 기밀성을 위한 공개키 암호화 기술을 고려할 때 비밀키 복원을 위한 키 복구 능력은 이 공개키 기반 구조에서 중요한 부분으로 고려되었다.

4.4 Federal Bridge CA Project

4.4.1 참여 기관

NIST(National Institute of Standard and Technology)를 중심으로 구성되었고, NIST는 KRDP에 참여하는 다른 정부기관에 대해 기술적 지원을 제공할 책임과 각각 파일럿 시스템에 적합한 테스트를 통해 각 시스템을 평가하고 이를 보고하는 책임을 가진다.

4.4.2 내용 및 특징

NIST는 KRDP에 참여하는 모든 파일럿들의 키 복구 시스템에 대한 적절한 테스트 방법을 개발하여, 각각의 시스템의 키 복구 기능에 대한 테스트를 수행하고, 그 결과에 대해 평가한다[7]. 또한 KRDP를 위해 각 파일럿들이 구축하는 공개키 기반구조에서 각각의 CA들간에 다른 파일럿 프로젝트와의 호환성 및 상호 작용을 테스트하기 위해, NIST는 root CA의 역할을 수행하는 Federal Bridge CA Project를 진행했다[8].

NIST에서는 "NIST Pilot Root Certification Authority Policy for the Key Recovery Demonstration Project"와 "Root Certification Practice Statement for the Key Recovery Demonstration Project"를 통해 KRDP에 참여하고 있는 파일럿들에 대해 root CA의 인증서에 있는 공개키의 정당성 및 무결성에 대한 신뢰 정도를 결정하는 기준을 제시하고 있다[9][10].

4.5 FedWorld Secure Web and Cer tificate Authority Project

4.5.1 참여 기관

NTIS(National Technical Informations Service)를 중심으로 프로젝트가 진행되었다.

4.5.2 내용 및 특징

이 프로젝트는 디지털 서명, 파일 및 메시지 암호화와 키 복구 관리 기능을 통해 암호화된 정보에 인가된 키 복구가 제공되는 trusted-agent 서비스의 기본형을 제공하고 있다.

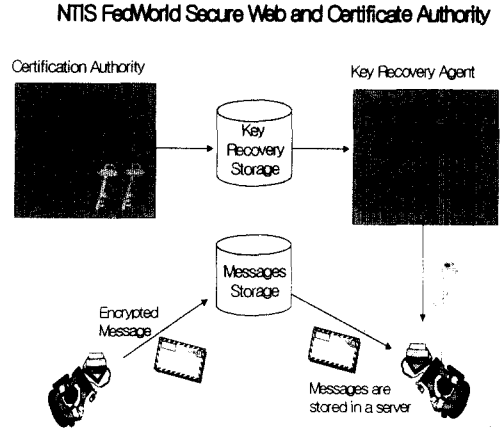
NITS는 DOT의 메시지 복구 기법과 NIH의 키 복구 기법 중 키 위탁을 기본으로 하는 NIH의 기법을 채택하고 있으며, 이 프로젝트에서 NTIS는 키 복구 기관로서 위탁된 키를 보유하고 있고, 인가된 사용자들은 암호문과 비밀키 사본에 대해 합법적인 요청을 할 수 있다. 이에 대해 NTIS는 사용자들의 요청의 정당성을 확인하고, 인가된 사용자들에 한해 위탁된 키나 복구된 평문을 제공한다.

그림 3은 시스템의 키 복구 과정을 나타낸다.

4.6 Proof-Of-Concept Demonstration Project

4.6.1 참여 기관

SSA(Social Security Adminstration)와 Pitney Bowes Inc.를 중심으로 프로젝트가 진행되었다.



〔그림 3〕 Fedworld Secure Web and Certificate Authority

4.6.2 내용 및 특징

Proof-of-concept 실증 프로젝트는 소규모 그룹들을 대상으로 키 복구 실증 프로젝트의 개념을 실제로 수행했다.

프로젝트의 참가자들은 공개키, 비밀키 기술을 이용하여 인터넷 상으로 데이터를 안전하게 SSA에게 제출하는데, 이 프로젝트에서 SSA는 전송된 데이터에 대하여 복구 기능을 포함함으로써 키 복구 실증 프로젝트의 개념을 실제로 수행할 수 있도록 프로젝트를 진행했다.

4.7 NATAP(North American Trade Automation Proto type)

4.7.1 참여 기관

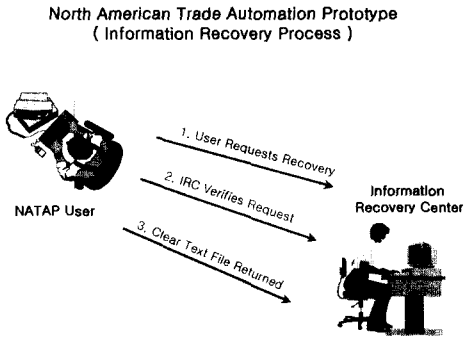
Trilateral Information Exchange과 Automation Working Group 중심으로 Customs, Immigration, Transportation, Census, state and local authorities, International trade community들이 참여했다.

4.7.2 내용 및 특징

Trilateral Information Exchange과 Automation Working Group는 여러 참여 기관들과 함께 북미 자유무역 동의서 512조항의 전자 거래 수행하는데 있어서 새로운 방법을 개발하였다. 전자 거래에 있어서 발생하는 문제점으로 크게 거래되는 데이터와 거래 방법에 대한 표준화와 거래 정보의 소유권에 대한 보안을 들 수 있다. 이를 해결하기 위해 NATAP는 다음과 같은 특징을 포함하며, 결정적인 거래 정보에 대해 실시간으로 복구가 가능하도록 설계했다.

- ○ 거래 데이터 및 거래 방법에 대한 표준화
  - 표준화된 데이터 및 메시지 형태 : UN/ EDIFACT
  - 표준화된 통신 방법 : Internet
  - 표준화된 거래 내용 핸들링 방법 : Trade Software Package(TSP)

- ○ 거래 정보의 소유권에 대한 보호
  - 표준으로 정해진 암호화 기법 사용
  - 디지털 서명 이용
  - 결정적인 거래 정보에 대한 실시간 복구 기능



〔그림 4〕 Information Recovery Process

그림 4는 NATAP의 키 복구 진행 과정을 나타내고 있다.

4.8 International Patent Document Exchange Project

4.8.1 참여 기관

PTO(Patent and Trademark Office)을 중심으로 프로젝트를 진행했다.

4.8.2 내용 및 특징

이 프로젝트는 Trilateral Offices(U.S. Patent and Trademark Office, European Patent Office, Japanese Paten Office)와 세계 지적 재산권 기구(WIPO)간에 안전한 전자적 형태의 특허권 교환이 기존 교환 방식에 비해 수행 비용 및 부담을 줄일 수 있음을 보여주고 있다. 특히, 전자적 형태의 특허권 교환이 안전하게 이루어지도록 암호화 및 디지털 서명 등을 제공하고, 암호화된 특허권에 대한 복구 기능도 포함함으로써 키 복구 기능을 테스트하고 있다.

4.9 Electronic Lending Prototype

4.9.1 참여 기관

SBA(Small Business Adminstration)를 중심으로 진행되고 있으며, SSA에 속한 그룹들을 대상으로 키 복구 기능을 테스트하고 있다.

4.9.2 내용 및 특징

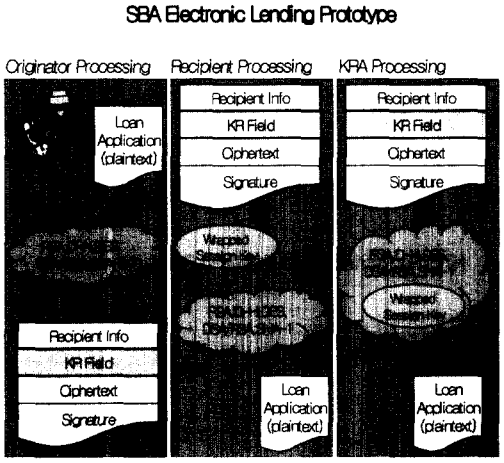
SBA의 Electronic Lending 프로그램은 대출 보증 과정(business loan guarantee proce sses)을 전자적으로 설계한 것으로 FA$TRAK system을 중심으로 이루어지고 있다.

FA$TRAK의 상업적 요구사항은 다음과 같다.

- ○ 대출 과정이 용이
- ○ 문서 이용 과정 축소
- ○ 처리 시간 단축
- ○ 전송 및 저장 데이터에 대한 기밀성 보장
- ○ 데이터에 대한 복구 가능 보장

위 요구사항을 만족시키기 위해 FA$TRAK는 공개된 인터넷 상으로 전송되는 대출 신청 정보에 대해 암호화를 수행하고, 디지털 서명을 이용한 강한 인증을 제공한다. 또한 보관된 대출 신청 정보에 대한 보호와 암호화된 데이터에 대한 키 복구 기능을 제공하고 있다.

상업적 요구사항을 만족하는 FA$TRAK의 대출 신청자 및 접수자, 키 복구 기관의 복구 과정은 그림 5와 같다.



〔그림 5〕 Electronic Lending Prototype

4.10 Electronic Messaging Services Network Infrastructure

4.10.1 참여 기관

Department of the Treasury 와 GSA Center for Electronic Messaging Technologies를 중심으로 프로젝트가 진행되고 있다.

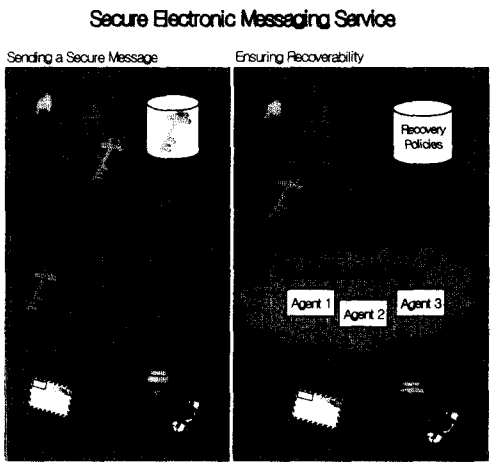
4.10.2 내용 및 특징

이 프로젝트의 목적은 안전한 Electronic Messaging Services Network Infrastructure 개발하고, 정부 기관들 간의 안전한 messaging 서비스를 제공하는데 있다. 이를 위해 프로젝트는 연방정부가 제공하는 출처 인증, 접근 제어, 데이터의 기밀성 및 무결성, 부인 불가, 암호문에 대한 복구 기능 등을 이용하기 위한 private Administrative Management Domain으로 프로젝트를 진행했다.

이 프로젝트의 상업적 응용을 위한 요구사항은 다음과 같다.

- 계약 체결 과정에 필요한 자원과 시간 최소화
- 전송 중 중요한 정보에 대한 보안
- 디지털 서명을 통한 전자적 인증 제공
- 암호화된 정보에 대해 복구 기능 제공
- 현존하는 messaging 기반 구조 이용 가능
  : Infonet
- 표준화된 인증 기술 이용 가능
  : Xcert's Sentry
- 다른 정책들을 수용할 수 있는 유동적인 복구 모델 필요

그림 6은 이와 같은 요구사항들에 대한 Secure Electronic Messaging 기반 구조와 이 기반 구조에 포함된 데이터의 복구 기능을 나타내고 있다.



[그림 6] Secure Electronic Messaging Service

5. 최근 파일럿 프로젝트

현재 미국의 키 복구 실증 프로젝트의 1차 파일럿 프로젝트는 종료되었고, 2차 파일럿 프로젝트가 진행되고 있으나, NIST에서 진행하고 있는 "KRDP and S/MIME"을 제외한 다른 파일럿 프로젝트에 대한 내용은 공개되지 않고 있다.

현재 NIST는 각 파일럿들의 키 복구 실증 프로젝트 수행을 위한 root CA로서의 역할을 수행하기 위해 진행했던 "Federal Bridge CA project"를 끝냈고, 키 복구 테스트에 적합한 응용으로 안전한 이메일 시스템인 S/MIME에 키 복구 기능을 포함하는 "KRDP and S/MIME project"를 2차로 수행하고 있다[11].

이 프로젝트는 2001년까지 S/MIME의 상호 운용성과 키 복구 능력에 대한 테스트를 통해, 상용화 가능한 S/MIME을 개발을 목표로 진행되고 있다.

또한 NIST는 지속적인 키 복구 실증 프로젝트의 진행을 위해 Bridge CA 개념과 S/MIME을 이용하는 대규모 공개키 기반구조 구축을 진행해나가고 있다.

Ⅲ. 유럽 연합의 키 복구 실증 프로젝트

유럽에서는 ETS(European Trusted Service)와 ICE라는 2개의 프로젝트를 중심으로 공개키 기반구조 및 서비스, 기타 보안관련 핵심 기술연구가 수행되어 왔다. 그러나, 아직까지 키 복구를 본격적으로 다루는 프로젝트는 진행되고 있지 않고 있다. 따라서, 본고에서는 ETS I을 중심으로 ETS I에서 부분적으로 다루었던 키 복구 관련 프로젝트에 대해서 그 내용을 살펴보도록 하겠다[12].

1. DG XIII(Directorate-General)프로젝트

1.1 배 경

유럽위원회의 DG XIII은 1992년 정보 시스템 보안분야 관련 위원회의 명령으로 신뢰할 수 있는 서비스(Trusted Service)문제를 연구하기 시작하였다. 또한, 이와 병행하여 1993년 수행된 보안조사(Security Investigation) 프로그램에서 인증

기관과 같은 신뢰할 수 있는 제3의 기관에 대한 역할을 규명하는 작업을 하였다. DG XIII은 이러한 일련의 사전작업을 통하여 정보기반구조의 보안 수립을 위한 신뢰개념을 적용하는 것이 필수적인 요소임을 인식하고 유럽 신뢰 서비스 구축작업을 전개하게 되었다.

DG XIII은 1996년 유럽 신뢰 서비스(ETS)를 위한 준비작업을 마치고 1997년부터 파일럿 프로젝트(ETS I)를 시행·완료하였으며 1998년에는 그 후속 연구로 새로운 연구들(ETS II)을 수행·완료하였다.

1.2 내용 및 특징

1996년에 시작하여 6개월 동안 범 유럽적인 TTP(Trusted Third Party) 기반구조 확립을 위한 기초 연구로 운영적, 기술적, 법적, 규제적 면을 고찰하며, 다음과 같은 일련의 보고서를 발간하였다.

- INFOSEC 프로그램(보안조사 프로그램)의 TTP 준비 연구 종합 결과
- TTP와 전자서명 관련 법·규제적 문제
- 전 세계적 TTP 기반구조에서 이름과 키 사용을 위한 지침
- ETS에 대한 표준화 문제
- 생체인식 기술 검토와 평가

본 프로젝트의 주요 목적은 유럽신뢰 서비스 추진을 위한 위원회 결성 제안서 준비와 산업계 주도로 범 유럽적인 신뢰 서비스의 기반구조를 확립하기 위한 기반조성에 있다.

2. ETS I

2.1 배 경

ETS I 프로젝트는 1996년까지의 DG XIII의 준비 연구를 바탕으로 연구에 대한 평가와 실제 구현을 위해 1997년 1년 간 수행되었는데, 총 8개의 프로젝트로 구성된 이 프로젝트의 일부에서 키 복구와 관련된 내용을 다루고 있다.

2.2 OPARATE(Operational and Ar chitectural Aspects of TTPs for Europe)

본 프로젝트는 TTP 서비스의 운영적, 구조적 면을 조사하고 이로 인해 제기될 수 될 수 있는 여러 문제들에 대해 연구한다.

2.2.1 연구 분야

- 효과적인 TTP 서비스 제공을 위한 TTP 조직과 운영
- 서로 다른 TTP 시스템간의 상호운용
- 기밀성·키 복구 서비스 제공을 위한 전자서명 TTP 서비스의 확장 문제
- 상호 이질적인 TTP 네트워크간의 상호운용 문제

2.2.2 제공 서비스

- 사용자 등록과 명명
- 키 생성 및 분배
- 상호 인증
- 부인 방지
- 디렉토리 서비스
- 도메인간 키 관리 서비스
- 기밀성, 키 복구 서비스

2.2.3 키 복구 관련 평가

범 유럽적인 경계를 넘어선 문제들(키 복구, 인증서의 상호인정, 사용자 등록)은 깊이 있게 고려되지 못하였다는 평가와 함께 이와 같은 문제들에 대해서, 기술적 해결책(technical solution)만을 제시하는 것만으로는 충분하지 않으며 다른 요소들과 함께 고려되어야 함을 지적했다.

2.3 KRISIS(Key Recovery in Secure Information Systems)

본 프로젝트는 키 복구에 대한 법 집행 기관 및 상업 분야에의 적용을 위한 요구사항들을 정의하고, 영국, 프랑스를 포함한 유럽 5개국에서 키 복구를 모의 실험함으로써 키 복구의 적합성을 검토하며, 추가적인 요구사항을 도출하였다.

2.3.1 키 복구에 대한 사전 연구결과

- 전자메일, 전자문서 전송 등에 기밀성 서비스가 필수적 요소임
- 기업들은 저장된 데이터에 대한 키 복구 요구
- 통신에 대한 키 복구의 필요성에 대해서는 견해가 서로 다르며 응용에 따라서 다름

- ○ 기업들은 약한 암호사용과 외국에서 개발된 공개되지 않은 암호 알고리즘 사용을 기피함
- ○ 기업들은 국제적으로 사용할 수 있는 단일의 기밀성 서비스 요구

2.3.2 키 복구에 대한 법적 및 상업적 요구사항

- ○ 범 유럽 기밀성 서비스를 위한 상업적 요구사항 도출
- ○ 상업적 관점에서 여러 키 관리·키 복구 방안들을 비교
- ○ 키 복구를 위한 파일럿 기반구조를 유럽 5개국에 구축
- ○ 파일럿으로부터 기술적, 정책적 요구사항 도출
- ○ 5개국으로부터 기밀성 서비스에 대한 법적 요구사항 도출

2.3.3 추가적 요구사항

- ○ 기업들은 자신들이 키 복구를 운영하기 원함
- ○ 엄격한 법 통제에 따라 자신의 국가에서 운영되는 TTP의 가능성
- ○ 정부에 의해 운영되는 TTP는 적합하지 않음
- ○ 외국 국가에 의하여 운영되는 TTP도 적합하지 않음
- ○ 다른 키 복구·비 키 복구 시스템과의 상호운용성 필요
- ○ 자율적인 키 복구가 바람직
- ○ 개인정보보호가 강조되는 특정 응용분야에서의 키 복구 사용 금지

2.3.4 프로젝트의 결과

IBM의 SecureWay(캡슐화 방식), CertCo의 SecureKEES (키 위탁방식), Royal의 Holloway (위탁방식), TIS의 RecoverKey (캡슐화 방식)을 분석 모델로 잡고, 이에 대한 포괄적인 비교와 상세한 설명을 제공하면서, 각각의 장·단점들을 분석하였다. 그러나 각각의 키 복구 방식 중 어떤 방식이 좋은지 나쁜지 혹은, 적당한지 그렇지 않은지에 대한 간단한 기준조차 제시하지 못했고, 정당한 키 복구 능력에 대한 요구사항을 만족하기 위해서는 보다 완벽한 방식을 갖는 접근제어와 키 복구 필드에 추가적인 정보들이 포함되어야 함을 지적하고 있다.

2.3.5 키 복구 관련 평가

KRISIS 프로젝트는 저장된 데이터에 대한 키 복구에 더 많은 비중을 두고 있는 기업 입장에서의 키 복구에만 제한을 두고 있는데, 정부 입장에서는 암호화된 통신 데이터에 대한 키 복구에 더 많은 관심을 가지고 있었으므로 분석한 4개의 키 복구 시스템들은 사용자나 기업에 대한 요구사항과 정부의 요구사항을 동시에 만족시키지 못했다는 평가를 얻었다.

또한 유럽 내에서도 키 복구에 대한 각 정부의 입장이 조금씩 다른데, 이에 대한 요구사항 역시 만족시키지 못했다. 그리고 키 복구 기능이 사용자 시스템에서 우회되거나 사용할 수 없다는 것을 보장해야 하는 필요성에 대해 인식했으면서도, 더 이상 이에 대한 연구는 진행되지 못했다.

2.4 AEQUITAS(Admission as Evide nce In Trials Of Penal Character Of Electronic Documents Digita lly Signed)

본 프로젝트는 법적 소송에서 암호화된 전자 메시지의 적법성에 대한 연구로 이에 대한 여러 사항들에 대해 연구한다.

2.4.1 연구 분야

- ○ 암호화된 메시지를 복호시킬 수 있는 법적 가능성과 기술적 가능성
- ○ TTP가 수행해야 할 법적 규정

2.4.2 키 복구 관련 평가

AEQUITAS 프로젝트는 암호문과 정당한 키 복구로 얻은 사용자의 메시지가 어떻게 검인값을 갖는지 그리고, 형사 처벌의 증거로 인정될 수 있는지에 대한 부분을 다루지 않고 있다. 이러한 경우에 사용자와 암호문과의 연관성을 증명하는 것이 중요한데, 본 프로젝트에서는 이에 대해 다루지 않고 있다. 또한 저장된 암호문을 얻는 것에 대해서는 언급을 하고 있으나, 암호 통신 중에 암호문을 얻는 것에 대해서는 언급하지 않고 있다.

2.5 EAGLE(Pan-European Network Of TTPs Offering Services To Users)

본 프로젝트에서는 TTP의 상업적, 기술적, 규제적 문제에 대해 연구하고, 키 복구를 위한 파일럿 데모를 구현하고 있다.

2.5.1 연구 분야

- TTP의 범 유럽적 네트워크 개발을 촉진하기 위한 TTP 서비스의 상업화 문제 연구
- TTP 서비스 판매를 위한 상업적 모델 개발
- 기술 부문에서 키 위탁과 키 복구를 연구

2.5.2 프로젝트의 결과

- 상업적 연구 : 기업의 입장에서의 키 복구는 암호화된 저장 데이터에 초점을 맞추고 있으며, 저장 데이터에 대한 키 복구는 외부 신뢰 기관과의 연결 없이도 내부 서비스로 구현되어질 수 있다.
- 기술적 연구 : 키 복구 기관의 키 관리 방식과 관련된 사항들을 다루고 있으며 KRISIS에서 조사되었던 3가지 키 복구 방식에 대해 깊이 있게 분석하고 있다.
  - JMW architecture (the Royal Ho lloway scheme)
  - RecoverKey scheme from Trusted In formation Systems
  - SecureWay scheme from IBM
- 규제적 연구 : 본 연구에서는 암호에 대한 법률화가 범 유럽적인 신뢰 서비스 발전의 장벽이 된다고 밝히고 있으며 규제화는 보안 서비스(암호화와 디지털 서명)을 지원하는 TTP를 고려해야 함을 권고하고 있다.

2.5.3 키 복구 관련 평가

상업적 연구는 키 복구가 TTP에 의해 지원되는 다른 서비스에 비해 낮은 우선순위를 갖는다는 것을 명시하고 있으며 유럽 내 TTP 서비스의 상업적 요구사항에 대한 분석을 제공하고 있다. 또한 기술적, 규제적 연구는 주요 키 복구 방식에 대한 새로운 관점을 제공하고 있다. 특히, 규제적 연구에서는 서로 다른 국가별 규제에 대한 요구사항을 인식하는 일반적 기반구조에 대한 권고안을 제시하고 있다.

3. ETS II

3.1 배 경

ETS I의 후속 연구로 1998년 1년 간 진행되었으며 모두 7개의 주요 과제를 수행하였다. 한가지 주목할만한 사실은 ETS에서 부분적으로 다루었던 키 복구 관련 연구가 제외되었다는 것이다.

3.2 내용 및 특징

- 공개키 기반구조와 전자서명 구조 개발
- 표준 인터페이스, 프로토콜을 포함하는 PKI 구조 선정
- 보안제품 시스템과 서비스 신뢰를 위한 기술적, 법적 기틀 마련
- 신뢰와 사용자의 확신을 증진하기 위해 서비스 평가에 필요한 방법론 분석, 개발
- 기술적 기반구조의 비용, TTP의 재정적 위험요소 등 서비스에 대한 비용 모델 분석·개발
- 타임 스탬핑 서비스 관련 문제 분석·구현
- 서비스 제공자 입장에서의 TTP 서비스 규정에 대한 분석과 시장 조성을 위한 정부의 역할
- ETS의 도입에 따른 WWW의 영향 분석

Ⅳ. 결 론

현대 사회가 점차 고도의 정보화 사회로 발전해 가면서 다양한 정보의 개방과 공유, 네트워크 상의 전자상거래 등 새로운 서비스를 창출하게 되었고, 이를 안전하게 제공하기 위해서 정보보호 문제가 주요 요소로 부각되었다. 정보 보호란 보다 안전하고 신뢰성 있게 정보를 관리하는 방법으로 암호 기술에 기반을 두고 있다.

암호 기술은 크게 데이터를 보호하기 위한 기밀성 관련 기술과 신분 확인 등을 위한 인증 기술로 나눌 수 있다. 이 중 기밀성이란 암호키와 알고리즘을 이용하여 평문을 알아보기 힘든 암호문 형태로 변환시켜 비밀키를 아는 정당한 사람만이 암호문을 복호할 수 있는 기능을 말한다.

기밀성을 제공하기 위해 사용되는 암호 기술은 정보의 누출을 방지하고 개인의 프라이버시를 보호해 주는 등 많은 장점을 가지고 있어 전자상거래나 전자 계약 등 다양한 응용이 가능하다. 그러나, 범죄 집단 등에 의한 암호의 부당한 사용 은 사회의 안전을 위협할 수 있으며, 키를 분실하거나 키가 손실되었을 경우 정당한 사용자조차 암호문을 복호할 수 없다는 문제점을 가지고 있다.

본고에서는 이러한 암호의 역기능으로 인하여 발생하는 문제들을 해결하기 위해 제시된 키 복구 기술의 상업적 응용 가능성을 확인하기 위한 키 복구 실증 프로젝트의 진행 사항을 조사·분석했다. 특

히, 오랫동안 키 복구 정책을 고수하고 있는 미국의 KRDP를 중심으로, 프로젝트의 내용과 진행사항들을 고찰하였고, 최근까지 키 복구 정책을 진행했던 유럽 연합의 키 복구 실증 프로젝트의 내용 및 평가들에 대해서도 분석하였다.

현재 국내에서는 키 복구에 대한 연구가 미흡한 실정이나 키 복구에 대한 정부 및 학계의 관심이 집중되고 있으므로, 국내에서도 미국 및 유럽 연합에서 수행한 키 복구 실증 프로젝트의 결과에 대한 고찰을 통해 키 복구의 가능성을 검증해 보아야 한다.

참 고 문 헌

[1] "Crypto Law Survery Ver-18.4", http://cwis.kub.nl/~frw/people/koops/lawsurvey .htm

[2] OMB Report, "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure", May 1996

[3] NIST, "Broad Agency Announcement", http://csrc.nist.gov/krdp/baa.html

[4] NIST, http://csrc.nist.gov/krdp/eadpps.html

[5] NIST, http://csrc.nist.gov/krdp/exa.html

[6] GiTS Security, http://gits-sec.treas.gov/krdp.htm

[7] NIST, http://csrc.nist.gov/krdp/eadpic.html

[8] NISt, http://csrc.nist.gov/pki/rootca

[9] NIST, Draft "NIST Pilot Root Certificate Practice Statement for the Key Recovery Demonstration Project", http://csrc.nist.gov/ krdp/CPS-2.doc

[10] NIST, "NIST Pilot Root Certification Authority Policy for the Key Recovery Demonstration Project", http://csrc.nist.gov/krdp/Policy.doc

[11] NIST, http://csrc.nist.gov/pki/smime

[12] "Cryptography in Europe", http://www.mod eemi.cs.tut.fi/~avs/eu-crypto.html

〈著者紹介〉

이 향 진 (Hyang-Jin Lee)
2000년 2월 : 성균관대학교 전기, 전자 컴퓨터 공학부 (공학사)
2000년 3월~현재: 성균관대학교 전기전자 및 컴퓨터 공학부 석사과정
관심분야 : 전자 상거래 보안, 무선 PKI

임 양 규 (YangKyu Lim)
1999년 2월 : 국민대학교 정보관리학과(학사)
2000년 3월~현재: 성균관대학교 전기전자 및 컴퓨터공학과 석사과정
관심분야 : 디지털 워터마킹, 무선 PKI, 전자상거래 보안

주 미 리 (Mi-Ri Joo)
1996년 2월 : 성균관대학교 정보공학과(공학사)
1998년 2월 : 성균관대학교 대학원정보공학과(공학석사)
1999년 2월~현재: 성균관대학교 전기전자 및 컴퓨터 공학부 박사 과정
2001년 3월~현재: 국가 보안기술 연구소 연구원
관심분야 : 암호이론, 정보이론

원 동 호 (Dong-Ho Won)
1976년 : 성균관대학교 전자공학과 졸업
1978년 : 성균관대학교 전자공학과 석사
1988년 : 성균관대학교 전자공학 박사
1978년~1980년 : 한국전자통신연구소 전임 연구원
1985년~1986년 : 일본 동경공대 객원연구원
1992년~1994년 : 성균관대학교 전산소장
1995년~1997년 : 성균관대학교 교학처장
1996년~1998년 : 국가정보화 추진위원회 자문위원
1990년~1999년 : 한국통신정보보호학회 이사
1998년~1999년 : 성균관대학교 정보통신기술연구소장
1999년~2000년 : 성균관대학교 전기전자 및 컴퓨터 공학부장
1982년~현재: 성균관대학교 전기전자 및 컴퓨터 공학부 교수
관심분야 : 암호이론, 전자 상거래