情 報 保 護 學 會 誌
第 11 券 第 4 號, 2001. 8

키 복구 제품에 대한 고찰

국 상 진*, 최 강 은*, 주 미 리**, 원 동 호*

요 약

최근의 암호 사용의 증가와 더불어 무분별한 암호의 사용도 증가하고 있다. 이에 대한 해결책으로 암호 키 관리에 대한 연구의 중요성이 대두되고 있으며, 또한 활발한 연구의 진행도 이루어지고 있다. 최근에는 Microsoft, Netscape communication과 VeriSign 등의 업체들이 키 복구 제품을 개발하여 상용화하고 있으며, 그 기능도 다양해지고 있다. 본 고에서는 기업에서 개발되고 있는 상용화된 키 복구 제품들을 분석해 보고, 각 제품의 동작 방식에 대해서도 설명 해 보았다.

Ⅰ. 서 론

컴퓨터와 통신의 발달은 인류의 생활을 보다 편리하게 바꾸어 주고 있다. 통신의 발달은 한 곳에 설치되어 있는 컴퓨터를 여러 곳에서 사용 할 수 있게 만들어 주었으며, 이에 따라 여러 가지 응용 시스템들이 같이 발전하게 되었다.

빠르게 발전하는 컴퓨터와 그 시스템들은 여러 가지 문제점이 발생하게 되었는데, 그 중에 가장 대표적으로 정보의 유출, 파괴, 위·변조, 해킹 등의 역기능이 대두되기 시작하였고 점차 확산 되어가고 있다. 이러한 역기능에 대비하여 암호의 사용이 점차 증가하고 있는데, 암호의 사용은 이러한 여러 역기능들에 대하여 좋은 해법으로 생각되어지고 있다. 저장된 데이터의 암호화, 혹은 통신로 상의 데이터에 대한 암호화 등은 정보의 유출, 파괴, 위·변조, 해킹 등의 역기능에는 효과적인 해결책이 되고는 있으나 잘 못 사용하면 다음과 같은 역기능들이 발생한다. 이는 크게 국가, 기업, 개인의 측면에서 생각해 볼 수 있으며 각각의 경우는 다음과 같다.

국가 기관에서 법원의 영장을 받아서 합법적으로 정보에 접근하는 경우에, 범법자들이 정보에 접근하지 못하도록 암호화하였을 때 정보에 접근 할 수 없다.

피고용인이 기업의 중요한 정보를 금품의 요구를 목적으로 암호화하였을 때 정보에 접근 할 수 없다.

개인 사용자가 암호화 한 파일이나 데이터에 대하여 사용한 키를 잃어버리거나 손상되었다면 역시 정보에 접근 할 수 없다.

여러 가지 이유로 암호화한 데이터를 복호하고 싶을 때, 키 복구는 그 데이터를 복호할 수 있는 방법을 제공하여 준다. 이렇듯 암호의 역기능에 대하여 그 해결책이 되고 있는 키 복구는 여러 국가와 기업에서 그 연구가 활발히 이루어지고 있고, 그 결과의 산물들도 많이 나타나고 있다.

최근에는 VeriSign, Microsoft, Netscape communications 등의 기업에서 키 복구 가능한 제품들을 발표하고 있는 등 점차 키 복구 기능 탑재 제품들이 늘어가는 추세이다.

키 복구 제품은 동작 방식에 따라 크게 위탁 방식과 캡슐화 방식으로 나뉘어 지며, 각각의 방식은 복구되는 키 정보의 위치에 따라서 결정된다.

본문에서는 키 복구 가능한 제품에 대하여 그 방법에 따라서 위탁 방식을 사용한 제품과 캡슐화 방식을 사용한 제품으로 나누어 각각의 제품에 대하여 분석 해 보았다.

Ⅱ. 위탁 방식을 사용한 제품

위탁 방식은 복구될 사용자의 비밀키, 비밀키의 부분, 또는 관련 정보를 하나 이상의 신뢰 기관에

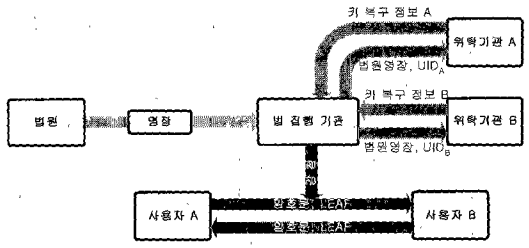
* 성균관대학교 정보통신보호 연구실
** 국가 보안기술 연구소
*** 본 연구는 정보통신학술진흥사업 지정과제(00-08) 지원으로 수행되었습니다.

위탁하는 방식으로 급한 상황에서 위탁 기관에 맡겨 놓은 키로서 정보에 접근 할 수 있도록 하는 방식이다. 이와 같은 방식은 사용자가 비밀키를 위탁 기관에 직접 맡김으로서 개인의 프라이버시가 위탁 기관에 의존한다는 문제점도 있으며, 이에 대한 해결책으로 복수의 위탁기관을 사용하는 방법도 있다.

1. Escrowed Encryption Standard

키 복구 제도는 1993년 4월에 미국 행정부가 정부 및 민간 부문의 정보 보호를 위한 새로운 대칭키 암호 시스템 개발을 명시하는 클리퍼(Clipper) 정책을 발표하면서 실제적인 추진이 이루어졌으며, 이 정책은 1994년에 EES라는 표준으로 승인되었다.

EES(Escrowed Encryption Standard) 시스템은 크게 tamper-resistant 특성을 지니는 클리퍼 또는 캡스톤(Capstone) 칩이 내장된 암호 단말 장치, 암호문을 감청 하여 키 복구의 요청 및 암호문의 복호를 수행하는 법 집행 기관의 LED(Law Enforcement Decryptor), 그리고 LED의 요청을 받아 키를 복구할 수 있는 정보를 제공해 주는 위탁 기관의 세 부분으로 구성된다. 다음은 EES의 동작 과정을 개괄적으로 보여주고 있으며, 그 내용은 다음과 같다.



〔그림 1〕 Key Escrow Standard 개념도

두 사용자 A, B 사이의 암호 통신 과정과 법 집행 기관에 의한 암호문의 복호 과정은 다음과 같다.

1.1 암호통신과정

사용자 A는 사용자 B와 SKIPJACK이라는 대칭키 암호 알고리즘을 사용하여 다음과 같이 암호 통신을 수행한다.

① 사용자 A와 사용자 B는 임의의 키 교환 프로토콜을 사용하여 암호 통신에 사용할 세션키 KS를 설정한다.

② 사용자 A의 클리퍼 칩은 세션키 KS와 칩이 생성한 IV(Initial Vector), 그 외의 파라미터를 통한 Checksum을 가지고 LEAF(Low Enforcement Access Field)를 생성한다.

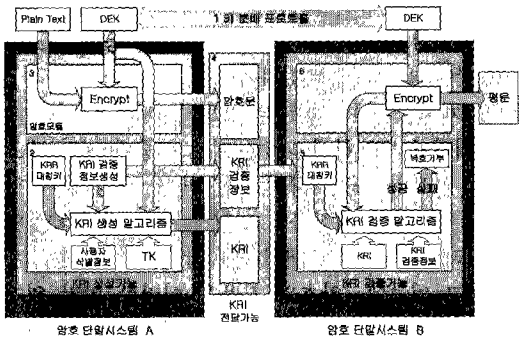
③ 사용자 A는 세션키 KS를 사용하여 암호문을 생성한다.

④ ②에서 생성한 LEAF와 IV를 암호문과 함께 사용자 B에게 전송한다.

⑤ 사용자 B의 클리퍼 칩은 수신한 LEAF내의 체크섬을 통하여 LEAF의 무결성을 검사한다.

⑥ ⑤의 검사가 통과되면 ①에서 설정된 세션키 KS로 암호문을 복호한다.

EES의 암호통신과정을 나타내면 그림 2와 같다.



〔그림 2〕 EES 암호통신 과정

1.2 키 복구 과정

위의 암호문을 감청한 법 집행 기관은 다음과 같이 사용자 A의 세션키를 복구한다. 그림 3은 EES의 키 복구를 나타낸 것이다.

① 법 집행 기관은 키 복구 요청자에게 키 복구 요청을 한다. 요청을 받은 키 복구 요청자는 법원에게 영장을 요구한다.

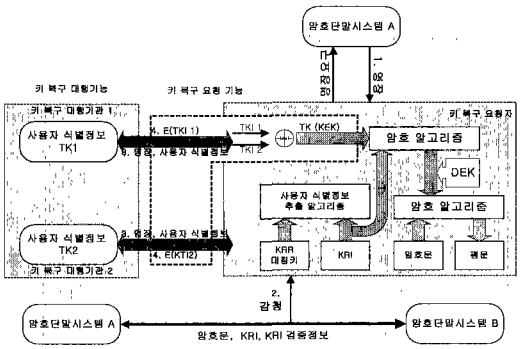
② 키 복구 요청자는 두 사람의 암호 통신을 감청한 후, 감청한 LEAF로부터 UID_A와 $E_{KU_A}(KS)$를 구한다.

③ 키 복구 요청자는 법원 영장과 UID_A를 각

키 위탁 기관에게 전송한다.

④ 각 위탁 기관은 UID_A에 해당하는 사용자 A의 키 복구 정보를 법 집행 기관으로 전송한다.

⑤ 법 집행 기관은 각 위탁 기관으로부터 수신한 사용자 A의 키 복구 정보로부터 구해진 KU_A를 사용하여 세션키 KS를 구해낸다.



〔그림 3〕 EES 키 복구 과정

2. Netscape Certificate Management System

CMS(Certificate Management System)는 Netscape Communications에서 개발된 시스템으로서 인증서를 생성하고, 알맞게 사용하고, 관리하는 도구이다. 이 시스템은 가장 많이 사용되는 플랫폼인 windows NT 및 Solaris에서 사용 가능하도록 제작되었으며, 여러 가지 독립된 서버들로 이루어져 있다. CMS의 여러 가지 기능 중에 키 복구에 관한 기능이 있으며, 이는 Long-term 키를 저장해 두었다가 사용하는 위탁 방식이다.

2.1 키 위탁과 복구를 위한 PKI 셋업

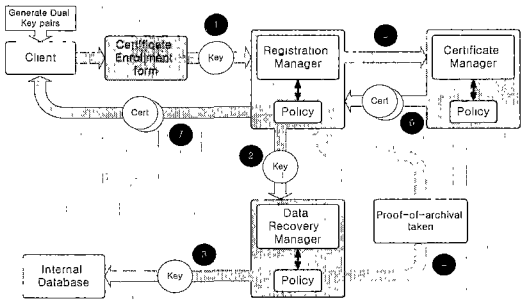
① 사용자들은 두 개의 키 쌍을 생성해야한다. (암호용과 서명용) 단지 암호용 비밀키만이 위탁되어야 하며, 서명용 비밀키는 결코 위탁되어져는 안된다.

② 단지 하나의 키 쌍 만을 생성한 사용자는 서명과 암호화에 같은 키를 사용하기 때문에 자신의 비밀키를 위탁하거나 복구할 수 없다. 따라서, 사용자들은 암호용과 서명용을 위한 각각의 키 쌍을 생성해야 한다. 두 개의 키 쌍 생성과는 부가적으로, 사용자는 인증서 요구 시에 암호용 비밀키 위탁 옵션을 제공되어야 하며, 이 옵션이 선택되면 키 위탁 과정은 실행된다.

2.2 CMS의 키 위탁과정

① 사용자는 Dual Key-pair를 생성하고 등록 매니저에(RM) 의해 공급되는 증명서 등록 양식에 모든 정보에 기입하고 제출한다. 등록 매니저(RM)는 사용자의 인증서 요구에서 키 위탁 옵션을 검사하고, 의뢰인에게 사용자의 암호화 비밀키를 요청한다. 의뢰인은 데이터 복구 매니저(DRM)의 transport certificate의 공개 암호키로 사용자의 암호화 비밀키를 암호화한다. transport certificate의 사본은 등록 양식에 포함되어 있다.

② 의뢰인으로부터 암호화된 암호화키를 받는 것과 함께, 등록 매니저(RM)는 저장하기 위해 데이터 복구 매니저(DRM)에게 키를 보낸다. 그 다음 데이터 복구 매니저(DRM)에서 등록 매니저(RM)는 키의 도착과 저장 암호화키와의 일치 확인을 기다린다.



〔그림 4〕 CMS 키 위탁 과정

③ 등록 매니저로부터 암호화되었던 키를 수신한 DRM는 자신의 비밀키를 사용하여 암호화된 사용자의 비밀키를 복호화 한 후에, 암호화키가 사용자의 공공 암호화키에 대응한다라고 확인하고, 자료 회복 매니저는 그것을 그 내부의 데이터 베이스에 보관하기 전에, 그 저장용 암호화키를 가지고 다시 그것을 암호화한다.

④ 사용자의 개인의 암호화키가 성공적으로 저장되었더라면, DRM는 비밀키를 사용하여 키가 성공적으로 저장되었다 라고 확인하는 문서에 서명하고,

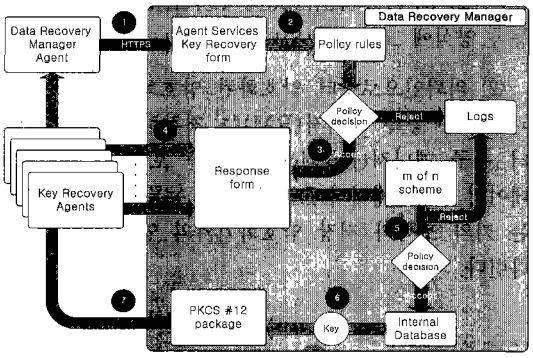
등록 매니저(RM)에게 보낸다.

⑤ 등록 매니저(RM)가 서명을 확인 받고, 인증서 매니저(Certificate Manager: CM)에게 인증서 요청을 보낸다.

⑥ 인증서 매니저는 2개의 증명서들(서명용 공개키, 암호용 공개키)을 생성하고, 등록 매니저에게 전송한다.

⑦ 등록 매니저는 증명서들을 의뢰인(사용자)에 전송한다.

2.3 CMS의 키 복구 과정



〔그림 5〕 CMS 키 복구 과정

① DRM agent는 적당한 의뢰인 인증서의 사용과, 사용자와 관련된 식별 정보를 이용해 키 복구 폼에 접근하고 request를 제출한다. 요청은 HTTPS를 이용하여 DRM에게 제출된다.

② DRM는 요청이 적당한지 판단한다.

③ 만일 요청이 모든 정책에 합당하다면, DRM는 에이전트가 사용하는 웹 브라우저에 확인 HTML 페이지를 보낸다. 만일 요청이 DRM의 정책에 위반하면, 서버는 적당한 에러 메시지를 기록한다.

④ 키 복구 agent(KRA)는 확인 페이지의 정보를 검사하고, MIME-64 형식의 인증서, PKCS#12 패키지를 위한 패스워드와, 그들의 개개의 식별자와 암호를 입력한다. DRMA는 페이지를 DRM에게 제출한다.

⑤ DRM는 KRA의 정보와 "n of m scheme"을 검사한다. 만족되는 RA의 수와 암호들이 증명되었다면 Agent의 패스워드를 이용하여 PIN 값을 생성한다.

⑥ DRM는 사용자의 비밀키를 저장소로부터 받아오고, 이를 storage key pair 사용하여 해독한다.

⑦ DRM은 사용자 인증서와 암호용 비밀키를 PKCS#12 패키지로 만들어내고 이를 PKCS#12 패스워드로 암호화한다.

3. VeriSign OnSite

VeriSign의 OnSite는 키 복구 기능을 가지고 있는 KMS를 포함하고 있다. OnSite의 KMS는 VeriSign Key Recovery Service와 같이 동작을 한다. 사용자의 암호화키를 KMS만이 접근 할 수 있는 데이터 베이스에 암호화하여 저장해 놓는 키 위탁 방식을 사용한다. VeriSign OnSite의 특징은 다음과 같다.

① Single 키 쌍 사용 방식과 Dual 키 쌍 사용 방식의 2가지 선택 사양을 가진다. Single 키 쌍 사용 방식은 키 쌍을 암호화와 서명에 사용하며, Dual 키 쌍의 사용 방식은 두 개의 키 쌍을 암호화와 서명에 각각 사용한다. 이때 KMS(Key Management Service)에서 생성되어지는 키 쌍은 암호용 키 쌍이 되며, 서명용 키 쌍은 개인이 생성 할 수 있다.

② 3DES를 사용하여 사용자의 비밀키를 암호화 시켜 보관하며, 비밀키의 암호화 이후에 3DES 키를 OnSite 서버만이 복구 가능하도록 파기시킨다.

③ 비밀키의 전송 시에 PKCS#12 파일 포맷을 사용한다.

3.1 키 생성 및 위탁

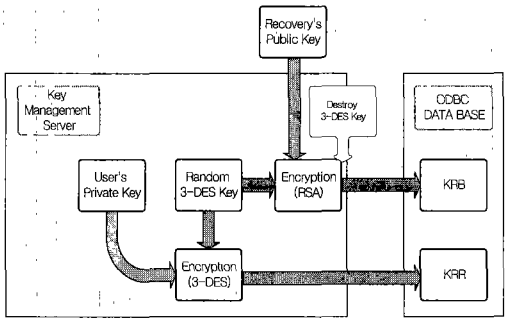
① 가입자의 비밀키는 KMS 서버의 내부에서 생성되어지고, 랜덤하게 생성된 3DES 키로 암호화되어 진다. 단지 KMS 서버로부터 접근 가능한 암호화된 데이터 베이스에 위탁되어진다. 이는 VeriSign에게 보여지지 않는다.

② 비밀키는 대칭키인 3DES 키로 암호화되어 진다.

③ KMS 서버는 대칭키로부터 KRB를 생성한다.

- KRB는 대칭키를 VeriSign의 공개키를 사용하여 암호화시킨 것이다.

④ 암호화된 비밀키(KRR)와 KRB는 KMS 데이터 베이스에 저장된다. 이는 단지 VeriSign Key Recovery Service 만이 KRB로부터 대칭키를 복호 할 수 있다. VeriSign 데이터 센터에서 안전하게 복구 가능하다.



〔그림 6〕 OnSite KMS의 키 생성 및 저장 과정

3.2 키 복구 과정

① 사용자 또는 사용자가 속한 기관의 대리인 혹은, 법 집행기관의 키 복구 요청이 들어오면 관리자는 사용자의 인증으로 Key Recovery Reference Number를 찾는다.

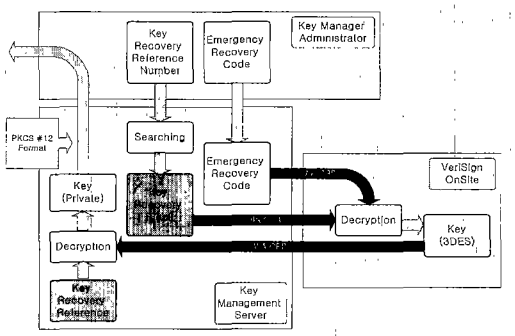
② 관리자는 키의 KRR Number와 ERC를 전송한다.

③ KMS는 KRR Number를 이용하여 KRB를 찾는다. KRB와 ERC를 VeriSign에 CRS를 이용하여 보낸다. - 서명 및 암호화 사용 -

④ VeriSign은 서명과 ERC를 확인한 후, 대칭키를 KRB로부터 복호해 낸다. VeriSign은 복호해 낸 대칭키를 CRS를 이용하여 전송한다. - 암호화 사용 -

⑤ KMS는 대칭키를 사용하여 사용자의 비밀키를 복호해 내고, VeriSign으로부터 인증서를 요구한다. VeriSign은 실시간으로 인증서에 응답한다.

⑥ KMS는 PKCS#12 파일과 새로운 패스워드를 생성해 내고, 사용자에게 안전한 방법으로 분배한다.



〔그림 7〕 OnSite 키 복구 과정

4. SecureKEES

SecureKEES(Secure Key Escrow Encryption System)은 CertCo에서 개발되었으며, 암호화에 사용하는 키의 백업을 위하여 사용한다. 이는 키의 캡슐화 방식을 사용하는 구조를 가지고 있으며 이는 메시지 헤더를 통해서 이루어지고 있다. 주로 스마트 카드와 같은 매체를 사용하며 파일의 암호화 및 커뮤니케이션상의 암호화에도 사용 가능하다.

SecureKEES 주요 특징은 다음과 같다.

① 암호화 알고리즘에 제약을 받지 않는다. 이는 어떠한 표준화된 암호 알고리즘도 사용할 수 있다.

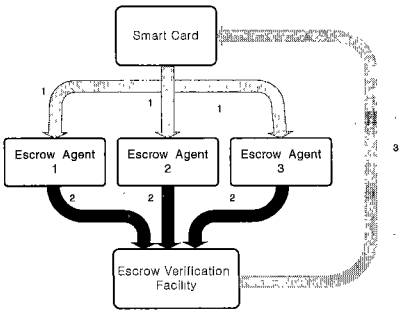
② 키 분배 스킴도 역시 제약을 받지 않는다.

③ 메시지 헤더에 단지 데이터 복구 필드만 추가된 형태로서 추가적인 메시지의 전달이 없다. 이 방법은 데이터 전송 뿐만 아니라 저장된 데이터에도 쉽게 적용이 가능하다.

CertCo의 스킴은 사용자의 공개/비밀 암호키 쌍을 생성한 스마트 카드와 같은 하드웨어 장치를 사용한다. 비밀 암호화키는 Silvio Micali의 특허 메커니즘 방법에 의해 조각들로 나뉘어 진다. 이 메커니즘 속에는 어떻게 비밀 키들이 여러 개의 조각으로 나뉘어지고 각각의 조각들은 위탁 기관으로 분산되어지는지에 관하여 기술되어져 있다. 각각의 위탁 기관들은 어떠한 정보 없이도 적당한 부분의 비밀키를 받았는지 검증 할 수 있다. CertCo의 스킴은 스마트카드 설치, 작동, 법인의 정보에 접근, 법 집행 기관의 정보에 접근의 구성으로 프로토콜이 이루어져 있다.

4.1 스마트카드 설치

CertCo의 제품은 스마트 카드와 같은 하드웨어 장치를 사용하여 동작한다. 이때 먼저 초기화하는 과정이 필요하게 된다. 이 과정은 스마트 카드에 대한 비밀키를 위탁하는 과정이다. 또한 어떠한 스마트 카드도 모든 키 위탁 기관으로부터 비밀키의 인증이 요구되어진다.



〔그림 8〕 CertCo 스마트 카드의 설치

① 사용자는 스마트 카드의 비밀키와 공개키 쌍을 생성하여 스마트 카드에 넣고 비밀키 조각들을 키 위탁 기관에 보낸다. 또한 확인 데이터를 위탁 기관에 같이 보낸다.

② 각각의 위탁 기관들은 스마트 카드로부터 받은 확인 데이터를 디지털 서명을 이용하여 위탁 검증 기관에 보낸다.

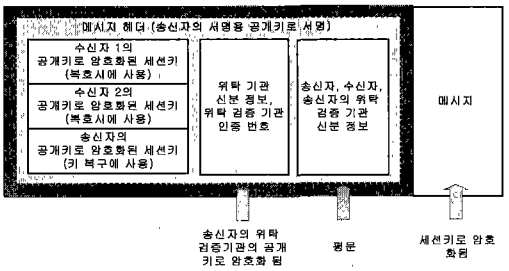
③ 위탁 검증 기관은 스마트 카드에 위탁 인증을 보낸다.

4.2 스마트 카드 작동

① 초기화가 성공적으로 끝난 후에는 스마트 카드는 데이터를 암호화할 수 있다. 실제로 통신에 사용하는 암호화는 사용자가 만들어낸 세션키를 이용하게 되고, 스마트 카드에 넘겨진다.

② 스마트 카드는 이 세션키를 메시지의 암호화와 메시지 헤더를 생성하는데 사용한다. 메시지 헤더에는 송신자의 공개 암호화키로 암호화된 세션키가 들어 있다. 이는 송신자가 세션키를 수신자에게 보내는 방법으로 사용된다. 또한 키 복구를 위하여 송신자 자신의 공개키로 세션키를 암호화하여 보관한다. 메시지 헤더는 또한 송신자, 수신자, 송신자의 비밀 암호화키를 위탁한 위탁 기관의 정보와 타임 스탬프 등을 포함하며 이는 송신자의 위탁 암호화키로 암호화되어 있다.

③ 송신자와 수신자의 위탁 검증 기관의 신원은 암호화되지 않은 평문으로 메시지 헤더에 첨가되고 스마트 카드의 비밀키를 사용하여 서명되어진다. 스마트 카드는 세션키로 메시지를 암호화한다.



〔그림 9〕 CertCo 메시지 헤더의 내용

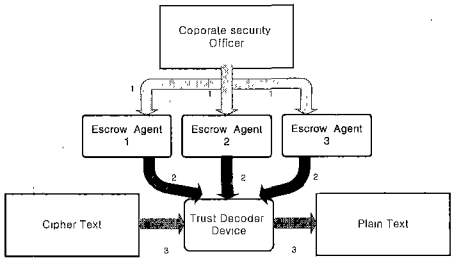
4.3 법인의 정보에 접근

① 피고용자에 의하여 암호화 된 파일이나 데이터에 접근을 원할 때, 법인의 보안 관리자는 위탁 기관에게 자기 자신을 인증하고, 키 조각들을 "trusted decoder device"에게 보내도록 위탁기관에 요청한다.

② 위탁 기관은 키 조각들을 trusted decoder device에게 보낸다.

③ Trusted decoder device는 위탁기관으로부터 받은 키 조각으로부터 헤더에 있는 세션키를 복호화 한다.

④ 복호된 세션키를 가지고 메시지를 복호화 해낸다. trusted decoder device는 결코 비밀 암호화키 또는 그 일부분을 법인의 보안 관리자에게 드러내지 않는다.



〔그림 10〕 CertCo 법인의 정보접근

4.4 법 집행 기관의 정보에 접근

① 법 집행 기관은 법원의 명령을 획득한다.

② 법 집행 기관은 통신을 가로채고, 송신자의 위탁 검증 기관에 가로챈 메시지 헤더와 법 집행 근거를 전달하고, 키 위탁 기관들의 이름을 요청한다.

③ 위탁 검증 기관은 요청을 인증하고 메시지 헤더를 복호화하여 법 집행기관에 위탁기관의 이름을 보내준다.

④ 법 집행기관은 모든 키 위탁 기관에게 키 조각에 대한 요청과, trusted decoder device에 전달 요청을 보낸다.

⑤ 위탁 기관들은 키 조각들을 trusted decoder device의 공개키로 암호화하여 전달하고, trusted decoder device는 비밀 암호화키를 재 조합한다.

⑥ 법 집행 기관은 trusted decoder device로부터 복호된 메시지를 전달받는다. 마지막으로 법 집행기관은 가로챈 메시지를 decoder device에 넣는다.

Ⅲ. 캡슐화 방식을 사용한 제품

캡슐화 방식은 키 위탁 방식과는 달리 각 세션마다 키를 복구 해 낼 수 있는 정보를 포함하는 필드를 생성해서 해당 암호 메시지에 부가시키는 방식으로 키 위탁기 이루어지지 않는다.

1. Microsoft Windows 2000 EFS

Microsoft에서 개발된 Windows 2000은 EFS (Encryption File System)을 통해 파일을 암호화/복호화를 하며, 또한 키 복구 기능을 제공한다. EFS의 암호화와 복호화는 Windows NT의 전통적인 파일 시스템인 NTFS 파일 시스템을 대상으로 행하여지며, 파일의 암호화 기법은 대칭키를 이용하는 방법으로 동작한다.

Windows 2000은 암호화된 NTFS에의 접근으로 반드시 비밀키를 요구하게 된다. EFS는 NTFS 파일 시스템의 파일이나 폴더를 암호화 할 때 사용한 대칭키를 복구 에이전트의 공개키로 암호화를 시켜 놓은 후 그 키를 이용하여 키 복구를 하며, 이때 키는 캡슐화 하는 방법을 사용한다.

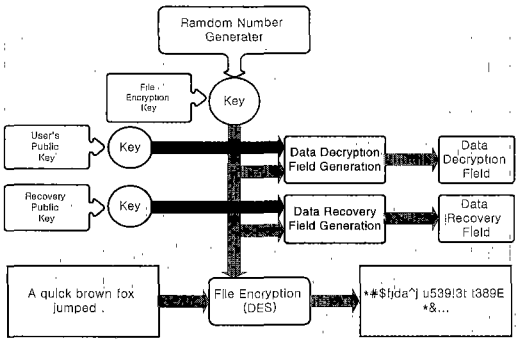
1.1 암호화 과정

① 사용자의 일반 텍스트 파일은 임의로 생성된 FEK를 사용하여 암호화된다.

② 암호화키는 파일과 함께 저장된다.

③ DDF는 사용자 공개키를 가지고 암호화된다.

④ DRF는 복구 에이전트의 공개키를 사용하여 암호화된다.



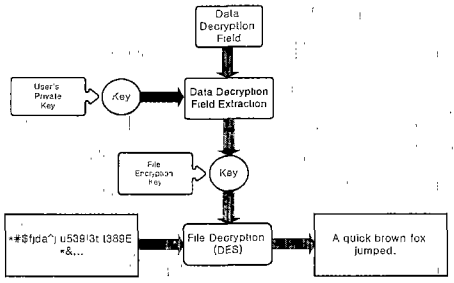
〔그림 11〕 Windows 2000 EFS의 암호화 과정

1.2 복호화 과정

① 사용자의 개인키를 가지고 암호화된 FEK를 복호 하는데 사용한다.

② FEK는 블록 기준으로 파일 데이터 읽기의 암호를 해독하는 데 사용된다.

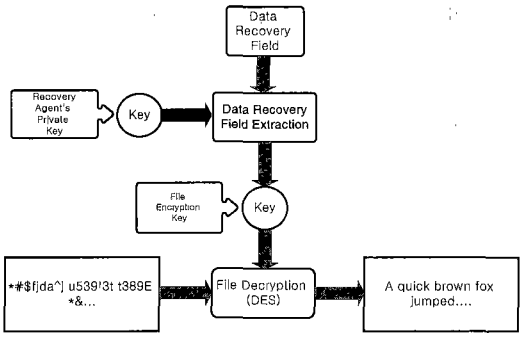
③ 큰 파일을 무작위로 액세스하면 이 파일의 디스크로부터 읽은 특정 블록의 암호만 해독한다. 전체 파일의 암호를 복호할 필요는 없다.



〔그림 12〕 Windows 2000 EFS의 복호화 과정

1.3 복구 과정

① 복구 에이전트의 개인 키를 사용하여 DRF의 FEK 암호를 복호 한다는 점을 제외하고는 복호 과정과 같다.



〔그림 13〕 Windows 2000 EFS의 키 복구 과정

② 이는 강력한 암호화 기법과 다중 사용자들이 암호화된 파일을 공유하는 능력을 제공하고, 또한 다중 복구 에이전트는 필요한 경우 파일을 복구할 수 있는 능력을 갖게 된다.

③ 이 기법은 완전한 알고리즘으로 다양한 암호화 단계에서 암호 해독 알고리즘을 사용할 수 있다. 새롭고 더 나은 알고리즘이 만들어짐에 따라 이러한 방법은 더욱 효율적으로 사용 가능하다.

2. Entrust/ICE (Integrated Cryptographic Engine)

Entrust/ICE는 여러 가지 PKI 솔루션 및 보안 제품들을 출시하고 있는 보안 전문 업체인 Entrust Technologies가 Microsoft의 EFS의 기능을 보완하기 위해 제작한 제품으로, 키 복구 기능에 있어서 마이크로 소프트의 제품보다 편리하고 강력한 기능을 제공하고 있다.

보안 솔루션으로 사용되고 있는 Entrust Technologies 제품의 용도는 표 1과 같다.

Entrust/ICE는 Entrust/PKI와 연동하여 키 복구 기능을 제공하며, Microsoft EFS가 파일의 암호화만을 제공하는데 비해, Entrust/ICE는 파일 암호화와 디지털 서명을 동시에 제공할 수 있으며, 암호화된 파일을 복호할 때 자동적으로 서명에 대한 검증을 한다.

〔표 1〕 Entrust technology의 여러 가지 보안 제품들

솔루션	용도
Entrust/Entelligence	데스크탑 보안 기술과 단독 로그인 기능
Entrust/SignOn	통합 Windows/Entrust 로그인
Entrust/ICE	파일과 폴더의 암호화
Entrust/TrueDelete	안전한 파일의 삭제
Entrust/Express	E-Mail 보안
Entrust/Unity	통합된 Microsoft와 Netscape의 보안 모델
Entrust/TruePass	웹 보안 및 디지털 서명
Entrust/Direct	high-end 웹 보안 및 스마트 카드 지원
Entrust/ DesktopDesigner	통합된 enterprise software

또한, 개인 사용자만을 지원하는 것과 달리 Entrust/ICE는 working group member의 사용을 지원하도록 제작되어 있다. EFS는 사용자가 복호화 키를 분실한 경우 지정된 복구 기관이 수동적으로 이를 복구시키는데 비해, Entrust/ICE는 사용자의 복호화 키가 Entrust infrastructure에 백업되어 있으므로 복구 기관은 키 복구를 위한 master key나 사용자의 복호화 키를 가지고 있지 않아도 이를 복구해 줄 수 있다.

3. SecureWay

IBM에 의해 개발된 SecureWay는 SKR(Secure Key Recovery)라는 키 복구 기술을 제공한다.

SecureWay는 RSA와 Diffie-Hellman의 키 분배 방식을 이용한 두가지의 키 복구 기술을 제공하며 각 방식들은 암호 통신을 하는 단계와 키를 분실하였을 시 암호 통신 단계의 정보로 키 복구 필드를 뽑아내 키 복구 기관에서 키 복구를 수행하는 단계로 나눌 수 있다. IBM의 키 복구 기술은 캡슐화 방식을 이용하며 통신 데이터에 대한 키 복구를 수행한다.

SecureWay는 키 복구 대행기관을 사용자가 자유롭게 선택할 수 있고, 암호화 알고리즘에 제약을 받지 않고 키 분배를 위해 RSA와 Diffie-Hellman 방식을 사용한다. 또한, 메시지 헤더에 데이터 복구 필드만 추가하며 부가적인 메시지의 전달이 없으며, 전송되는 데이터에 적용할 수 있는 특징을 가지고 있다.

가) RSA 방식 (암호통신, 키 복구)

① 사용자 A와 B는 RSA를 이용하여 비밀 seed를 교환한다.

② 사용자 A와 B는 각 복구 기관들의 ID와 seed를 해쉬한다.

③ 사용자 A는 ②의 해쉬값들을 각각의 키 복구기관의 공개키로 암호화하여 블록1을 만든 후 저장한다.

④ 사용자 A와 B는 RSA를 이용하여 세션키를 설정한다.

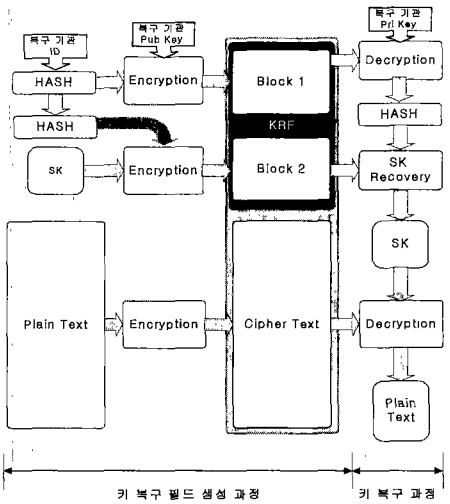
⑤ 사용자 A는 ②의 값을 또 한번 해쉬 함수를 이용하여 K_i를 만들어 낸다.

⑥ 사용자 A는 세션키를 각 K_i로 다중 암호화하고 키 복구 필드를 생성하여 세션키로 암호화한 메시지에 덧붙여 블록2를 사용자 B에게 보낸다. 사용자 B는 seed, 세션키, 각 복구기관의 공개키를 이용하여 블록2를 확인한다.

⑦ 키 복구 요청기관은 블록 1으로 부터 각 복구기관의 공개키로 암호화된 부분을 추출하여 각각의 복구 기관에 전송한다.

⑧ 각각의 복구기관은 자신의 비밀키를 이용하여 키 복구 요청기관으로부터 받은 필드를 복호하고 이 값을 해쉬하여 K_i를 생성한 후 키 복구 요청기관에 보낸다.

⑨ 키 복구 요청기관은 각각의 복구 기관으로부터 $K_1, \cdots, K_n$을 받은 후 블록 2를 복호하여 세션키를 복구한다.



〔그림 14〕 SecureWay 키 복구 필드 생성 및 키 복구과정

나) D-H 방식 (암호통신, 키 복구)

Diffie-Hellman의 키 교환 프로토콜에 의해 사용자들과 키 복구기관 사이의 키는 공유되어 있다고 가정하자.

① 사용자 A는 사용자 A, B와 모든 키 복구기관의 ID 및 타임 스탬프 등이 포함된 헤더 T1를 만든 후 키 복구 기관과 공유된 키와 T1을 해쉬하여 키 J_i를 생성한다.

② 사용자 A는 난수를 선택하고 키 J_i로 암호화하여 키 복구 필드 블록 1을 생성한다.

③ 사용자 A는 세션키를 생성하여 B의 공개키로 암호화하여 보내고 난수를 해쉬함수를 이용하여 K_i를 만들어 낸다.

④ 사용자 A는 세션키를 각 K_i로 다중 암호화한다. 이 결과를 암호화된 메시지에 덧붙여 블록 2를 만들어 사용자 B에게 보낸다.

⑤ 키 복구 요청기관은 블록1으로부터 추출한 키 복구 필드를 키 복구기관에 전송한다.

⑥ 각 키 복구기관은 공유된 키와 공개 헤더 T1을 해쉬하여 키 J_i를 생성하고 키 복구 요청기관으로부터 받은 키 복구필드를 복호하여 난수를 얻는다. 이때 얻은 난수를 해쉬하여 K_i를 만들고, K_i를 키 복구 요청기관에게 전송한다.

⑦ 키 복구 요청기관은 각 키 복구 기관으로부터 $K_1, K_2, \cdots, K_n$을 얻은 후 이 키를 사용하여 블록 2로부터 세션키를 복구할 수 있다.

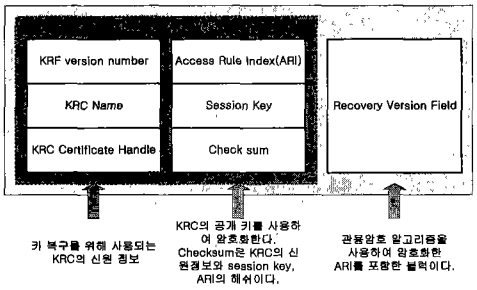
4. RecoverKey

TIS(Trusted Information Systems)에서 개발한 RecoverKey는 키 복구 제품으로 키 복구기관의 역할을 하는 키 복구 센터라 불리는 신뢰기관을 이용한다. 이 제품은 데이터를 암호화하는데 사용되는 키의 정보가 암호화할 때마다 데이터에 첨가되는 캡슐화 방식이다. 저장된 데이터 및 전송되는 파일에 이용할 수 있으며 키 복구 필드를 이용하여 키를 복구할 수 있는 캡슐화 방식이다. 첨가된 키 복구필드의 복호는 키 복구센터만이 가능하다.

RecoverKey의 키 복구필드의 구성은 그림 15와 같고 제품의 동작과정은 사용자 등록 및 데이터

저장 단계, 통신의 세 단계로 나누어진다.

RecoveryKey는 데이타 암호 알고리즘에 대한 제약은 없으나 DES를 사용하고 있으며, 키 복구 센터를 사용자가 선택할 수 있다. 또한 키를 위탁하거나 전송하지 않는다.



〔그림 15〕 RecoverKey 키 복구 필드 생성

4.1 사용자 등록 단계

① 사용자는 Access Rule를 키 복구 센터의 공개키로 암호화하여 키 복구센터에 전송한다.

② 키 복구 센터는 전송받은 자료를 복호하여 데이터베이스에 저장하고 ARI(Access Rule Index)를 사용자의 공개키로 암호화해서 전송한다.

4.2 데이터 저장 단계

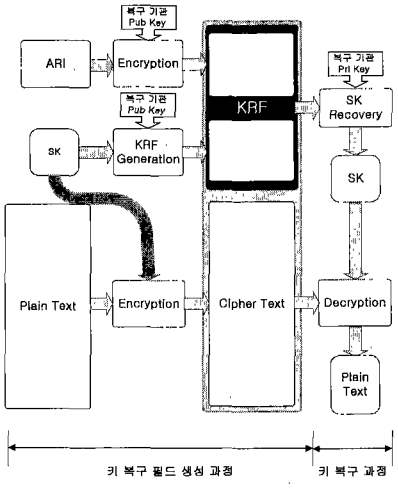
① 사용자는 세션키를 생성하여 세션키로 파일을 암호화한다.

② 세션키는 해당 키 복구 센터의 공개키로 암호화하여 키 복구 필드를 생성한후 암호화된 파일에 키 복구 필드를 첨부하여 저장한다.

4.3 키 복구 단계

① 사용자는 키를 분실하였을 때 인증정보와 함께 복구 필드를 키 복구 센터에 전송한다.

② 키 복구 센터는 인증정보를 확인하여 정당한 사용자에 한하여 자신의 비밀키를 이용해 세션키를 복구하고 사용자의 공개키로 암호화해서 전송한다.



〔그림 16〕 RecoverKey 키 복구 필드 생성, 키 복구 과정

5. Crypto Backup

미국 AT&T에의해 개발된 Crypto Backup은 암호 시스템의 키를 복구하기 위하여 개발한 제품으로 암호 키들을 자동적으로 백업하는 기술을 소개하고 있다. Crypto Backup은 각 암호화된 파일의 헤더에 BRV(Backup Recovery Vector)가 첨부되고 이 BRV로부터 세션키를 복구할 수 있다. 이 제품은 저장된 파일이나 메시지들에 적용할 수 있으며 메시지의 암호화 알고리즘은 관용 암호방식을 이용한다.

또 Crypto Bakcup 시스템은 암호화 알고리즘이나 키 관리 프로토콜과는 독립적으로 구성되며 하드웨어에 최소한으로 의존적이고 사용자의 투명성을 보장해준다.

Crypto Backup은 백업 기관을 여러 개 선택할 수 있으며, 다른 프로젝트 수행이나 응용에 있어서 다른 백업 기관을 선택할 수 있다. 또한 사용자는 패스워드나 암호화 키 등과 같은 모든 종류의 키들을 백업할 수 있는 기능을 가지고 있다.

5.1 키 복구 과정

① Backup 복구 기관은 비밀키와 공개키를 생성한다.

② 공개키에 대한 식별자를 id_y라하고 복구기관

은 ID와 메시지에 서명한다. 공개키와 식별자 id_y, 서명을 backup 기관의 공개 마스터키 벡터라 한다.

③ 사용자는 난수를 생성한다.

④ 사용자는 Bakcup 복구기관의 공개키와 난수를 사용하여 nbit의 암호화키를 계산한다. 또 사용자는 Backup 복구 기관의 ID, 식별자 id_y, 복구기관의 공개키, 사용자가 선택한 난수를 이용하여 키 복구 필드에 해당하는 nbit의 암호화키와 관련된 BRV을 생성하여 저장한다.

⑤ 사용자는 키의 분실 시에 Backup 복구 기관에 BRV를 전송하고 Backup 복구기관은 BRV로부터 n bit의 암호화 키를 복구할 수 있다.

6. CyKey

CyKey는 Cylink사에서 제안한 키 복구 제품으로 캡슐화 방식으로 동작하며, 암호화된 통신 데이터 및 저장 데이터에 대한 키 복구에 사용될 수 있다. 이 제품에 사용되는 암호화 기법으로는 대칭키 암호 알고리즘과 Diffie-Hellman의 키 분배 등이 있고, 미 상무부에서 인정된 제품이다.

CyKey는 키 복구기관을 사용자가 자유롭게 선택할 수 있고, 그 수는 하나 이상이다. 하드웨어 또는 소프트웨어로 구현될 수 있는 특징을 가지고 있다.

키를 분실하거나 키가 손상된 경우, 사용자에 의해 지정된 키 복구 대행 기관만이 키를 복구 할 수 있으며 정부를 포함한 인증되지 않는 제 3의 기관은 키 복구 대행 기관 없이는 키를 복구할 수 없다. 키 복구 기능을 지원하는 CyKey는 사용자, 암호제품의 소유자, 키 복구기관들 사이의 신뢰관계를 전제로 동작하며, 이를 위해 키 복구 동작은 신뢰관계 설정단계와 복구 단계로 진행된다.

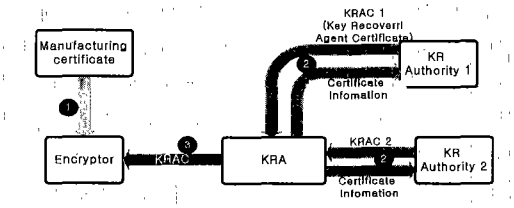
6.1 신뢰관계 설정단계

신뢰관계는 평문을 암호문으로 바꿔주는 장비나 소프트웨어와 같은 암호기, 키 복구기관(Key Recovery Agent), 키 복구기관을 허가해 주는 기관(Key Recovery Authority)들 사이에 설정되어진다.

① 신뢰 관계 설정을 위한 제조 인증서(manufacturing certificate)는 키 복구기관을 인가해 주는 허가 기관을 정의하고 있으며 허가 기관의 공개키를 포함하고 있다.

② 키 복구기관은 허가 기관에 자신의 공개키, ID 등과 같은 인증 정보를 제시한다. 허가기관은 이것에 서명을 하고, 이를 KRAC(Key Recovery Agent Certificate)의 형태로 키 복구기관에 전송한다.

③ 사용자는 키 복구기관에 등록하고 해당 키 복구기관의 KRAC를 받는다. 그러나, 사용자의 암호기는 해당 키 복구기관의 KRAC를 받기 전에 지정된 복구기관의 KRAC임을 검증한다.



〔그림 17〕 CyKey 신뢰관계 설정단계

6.2 키 복구 단계

키 복구 단계는 저장된 데이터에 대한 복구 단계와 통신 데이터에 대한 복구 단계를 나누어 진행된다.

암호화된 저장 데이터에 대한 복구는 다음과 같은 순서로 진행된다.

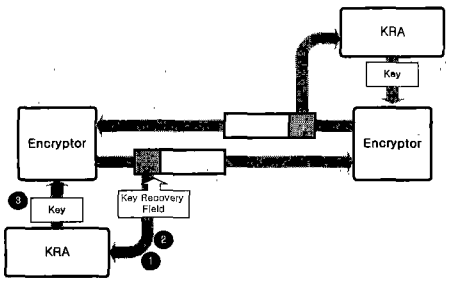
① 사용자는 키 복구기관에 등록한다.

② 사용자는 암호화키를 분실하였을 경우 암호화된 파일로부터 키 복구 필드를 복사하여 키 복구기관에 전송한다.

③ 키 복구기관은 키 복구 요청기관의 정당성을 확인 후 비밀키로 키 복구 필드를 복호하여 세션키를 사용자에게 전송한다.

또한, 암호화된 통신 데이터에 대한 복구는 다음과 같다. 암호화 키의 복구 및 암호화된 통신 데이터의 복호를 위해 키 복구 필드가 포함된 키 교환 프로토콜 메세지와 암호화된 통신 데이터가 필요하다.

① 데이터를 복구하기 위해 키 교환 메시지로부터 키 복구 필드를 추출한다.



〔그림 18〕 CyKey 키 복구 과정

, ② 키 복구 필드를 키 복구기관에 전송된다.

③ 키 복구기관은 사용자의 정당성 확인 후에 암호화키를 사용자에게 전송한다. 암호화된 저장 데이터의 키 복구에서와는 달리 암호화된 통신 데이터에 대한 키 복구에서는 암호화 키가 데이터와 함께 저장되지 않으며, 암호화 키는 다른 키 교환이 있을 때까지 두 사용자의 암호통신을 위해 계속 사용된다.

7. SecretAgent

Information Security Corporation사에 의해 개발된 제품으로 캡슐화 방식으로 동작한다.

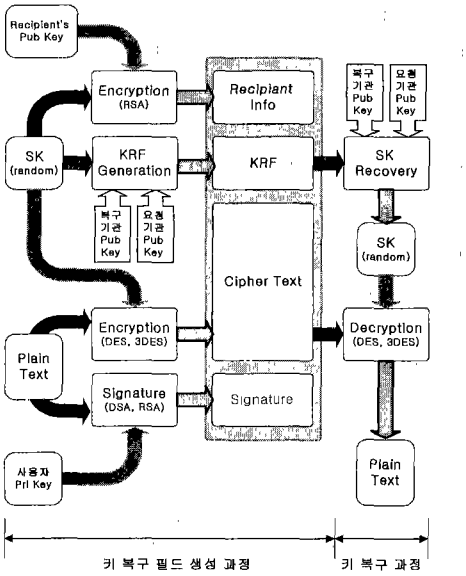
SecretAgent는 사용자가 하나나 그 이상의 수신자를 위해 파일을 암호화하고 서명하는 것을 제공한다. 데이터의 암호화에는 대칭키 암호 알고리즘이 사용되며, 암호화 과정에서 랜덤하게 생성된 암호화 키는 수신자의 공개키로 암호화된다. SecretAgent는 키 교환을 위해 RSA 키 교환, Diffie-Hellman 및 수신자의 공개키를 이용하는 여러 키 교환방법을 제공하고 있으며, 이 방법들은 SecretAgnet가 자동적으로 선택한다. 또한, 서명과 복호를 위한 비밀키의 저장 장치로 스마트 카드나 토큰 등을 제공한다. SecretAgent는 VIM, MAPI, AT&T AccessPlus 등의 메일 시스템과 상호 운용 가능하다.

7.1 암호 통신 단계

① 사용자가 메시지 M를 $B_1, B_2, \cdots, B_n$에게 보내고자 할 때 SecretAgent를 통해 암호화키를 랜덤하게 생성한다.

② 사용자는 $B_1, B_2, \cdots, B_n$의 공개키들로 세션키를 암호화하고, 해당 세션키로 메시지를 암호화하여 이를 각 사용자 $B_1, B_2, \cdots, B_n$에게 전송한다. 전송되는 데이터의 구조는 다음과 같다.

EP1(K), EP2(K), ... , EPn(K), EK(M)



〔그림 19〕 SecretAgent 키 복구 필드 생성, 키 복구과정

③ 사용자 B_i는 수신된 데이터의 헤더에 포함된 암호문으로부터 비밀키를 구하고, 이를 통해 세션키를 얻는다.

④ 세션키를 이용하여 암호화된 메세지를 복호한다.

7.2 키 복구 단계

SecretAgent는 키 복구를 위해 키 복구 요청기관과 키 복구기관의 공개키 및 세션키로 구성된 키 복구 필드를 첨가한다.

① 키 복구 요청기관은 암호문으로부터 키 복구 필드를 추출하고, 서명된 키 복구 요구(KRQ)를 키 복구 기관에 전송한다. 이 요구는 메시지를 포함할 수 있으며 다른 정보들과 함께 키 복구 요청기관의 신분을 증명한다.

② 키 복구기관은 서명된 키 복구 요구를 검증하고, 이를 통해 키 복구 요청기관을 인증한다.

③ 키 복구 요청기관의 요구가 정당하다면 키 복

구기관은 자신의 비밀키를 이용하여 키 복구 필드에서 KRK(Key Revoery Key)를 얻고, 이를 키 복구 요청기관에 전송한다.

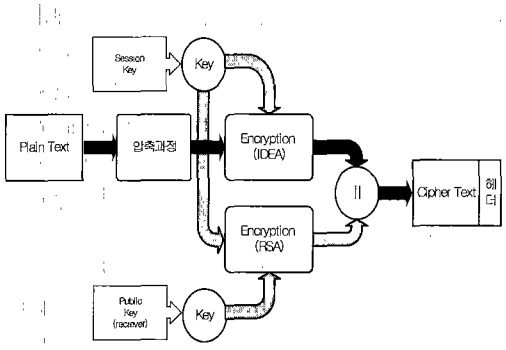
④ 키 복구 요청기관은 전송 받은 KKK를 자신의 비밀키로 복호하여 세션키를 얻는다.

8. PGP

Phil Zimmermann이 많은 노력을 기울여 만든 PGP는 전자 우편 및 파일 저장에 많이 사용하고 있으며, 이는 인증 및 기밀성의 제공을 하고 있다. 또한 PGP 5.x과 6.x versions은 Additional Decryption Key(ADK)를 통하여 키 복구기능을 제공하고 있으며, 이는 주로 기업의 입장에서 활용이 가능하도록 제작되었다. ADK는 기업용의 PGP 버전에서만 지원하고 있으며, 개인용의 PGP에서는 그 기능이 제거되어 있다.

8.1 PGP의 기밀성 제공

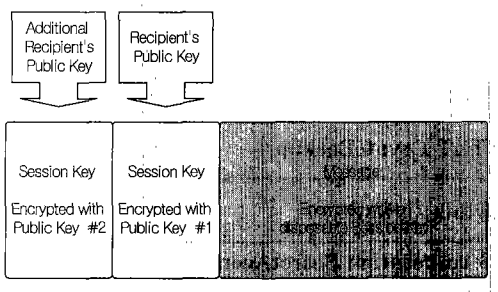
PGP는 속도가 빠른 관용키 방식인 IDEA를 이용한 암호화를 수행하며, 사용한 키는 랜덤하게 생성한다. 또한 세션키는 RSA와 같은 공개키 방식을 사용하여 암호화시킨 후 암호문과 연결시키고, 공개키 암호화에 사용하는 수신자의 공개키는 PGP 공개키 서버에서 가져온다. 수신자는 헤더에서 자신의 공개키로 세션키를 복호화 한 후, 복호된 세션키로 암호문을 복호화 한다.



〔그림 20〕 PGP 기밀성 제공을 위한 구조

8.2 ADK의 동작

기업의 입장에서는 다른 회사와의 중요한 정보의 교환이나, 혹은 재무에 관련된 중요한 정보들을 안전하게 전달하기 위하여 암호화를 이용하는 방법을 사용하게 된다. 그러나 기밀성을 제공하는 암호화의 부작용을 없애기 위하여 PGP는 여러 개의 공개키로 세션키를 암호화는 키 복구 방법을 사용한다.



〔그림 21〕 PGP ADK의 메시지 헤더

① 회사 내에 직원들은 중요한 문서를 암호화하여 전송할 때 회사의 공개키를 사용하게 된다. 이때 회사의 직원들의 공개키에는 ADK를 사용 할 수 있음을 나타내는 ADK ID가 포함되어져 있다.

② ADK ID가 포함되어져 있는 수신자를 발견했을 때, 송신자는 ADK를 사용 할 수 있으며 의무사항은 아니다. ADK는 송신자 및 수신자의 동의가 있어야만 동작하도록 되어 있다.

③ 수신자가 ADK를 사용한다면 세션키를 복호화 할 수 있는 사람은 수신자와 ADK의 키 소유자이다.

Ⅳ. 제품분석

다음은 각 제품들에 대한 간략한 비교를 다루었다.

모든 제품들은 각각위탁 방식과 캡슐화 방식을 지원하고 있다. 또한 저장된 데이터 혹은 통신 데이터에 대한 키의 복구를 지원하고 있다.

EES와 같이 표준으로 채택된 것도 있고, PGP와 같이 공개된 프로그램도 키 복구 기능을 지원한다.

Ⅴ. 결 론

정보화 사회는 전자 우편, 전자 상거래, 또는 새

〔표 2〕 각 제품의 간략한 특징

[illegible]	[illegible]	[illegible]
EES	위탁	하드웨어상에서 구현/Skipjack 사용
Netscape CMS	위탁	PKI와의 연동/m of n scheme의 비밀 분산 사용
VeriSign OnSite	위탁	서비스 개념의 키 복구/키의 중앙 통제
CertCo SecureKEES	위탁	Trust decoder device의 사용/다수의 비밀 분산 기관 존재
Windows 2000 EFS	캡슐화	NTFS에 대한 키 복구/DES의 사용
Entrust ICE	캡슐화	Windows 2000의 EFS를 개선
IBM SecureWay	캡슐화	RSA/DH 의 방법 사용/2단계를 거쳐 위탁
TIS RecoveryKey	캡슐화	저장, 통신 데이터 모두 적용
AT&T CryptoBackup	캡슐화	다수의 백업 기관 선택 가능/파일 복구를 위한 키의 백업
Cylink CyKey	캡슐화	저장, 통신 모두 적용/하드웨어, 소프트웨어 구현가능
IS corporation SecretAgent	캡슐화	KRO, KRA의 협동에 의해서만 세션키 복구
PGP	캡슐화	기업용의 PGP에서 사용/전자 우편에서 사용

로운 서비스 등, 여러 가지 불가능한 서비스들을 가능하게 해 주고 있다. 그러나 이러한 편리한 서비스들에 대하여 보안 문제는 더욱 크게 문제시되어 가고 있는 시점에 있다. 이에 대한 해결책으로 생각되고 있는 암호의 사용은 새로운 문제점을 만들고 있고 또한 이 해결책으로 키 복구가 대두되어지고 있다.

본 고에서는 키 복구를 가능하게 하는 여러 키 복구 제품들에 대하여 그 동작 과정을 알아보고, 또 각 제품들의 특징들에 대하여 살펴보았다.

이러한 키 복구제품을 사용하는데 있어서 사용자는 제품에 대하여 좀 더 많은 정보가 필요하며, 사용자들의 올바른 선택을 위해서 키 복구 제품 역시 객관적인 평가가 진해 될 수 있도록 그 평가 기준이 필요하다. 또한 이러한 평가 기준을 만들어 낼 수 있는 평가 기관도 필요하다.

키 복구의 표준화나, 기술적인 측면, 법/제도적인 측면 등의 여러 각도에서 키 복구에 대한 연구가 필요하며, 이는 키 복구를 일반 사용자들이 보다 쉽게, 그리고 많이 사용할 수 있도록 도울 것이다.

앞으로 암호의 사용은 점차 증가하게 될 것이며, 또한 키 복구 제품도 사용이 증가하게 될 것이다. 보다 간단하고, 효율적으로 동작하는 제품의 등장으로 키 복구기능을 편리하게 사용 할 수 있어야 하겠다.

참 고 문 헌

〔1〕 CertCo.,"SecureKEES", KRISIS A Project ; WP2 report

〔2〕 Cylink, "CyKey:Cylink's Key Recovery Solution", 1997

〔3〕 David E Ross "Additional Key Decryption", http://www.vcnet.com/~rossde/pgp-adk.html

〔4〕 David Paul Maher, "Crypto Backup and Key Escrow", 3. 1996. Vol.39. NO.3, Communications of the ACM

〔5〕 Entrust, http://www.entrust.com

〔6〕 IBM Cryptography Center of Competence, "Secure Key Recovery"

〔7〕 Michael J. Markowitz, Roger S. Schlafly" Key Recovery in SecretAgent", 6. 1997

〔8〕 Microsoft, "Encrypting File System for Windows 2000", http://www.microsoft.com/DirectAccess/PartnerGuide/smallbusiness/techread/docs/EFSOverview.doc

〔9〕 Netscape, "Administrator's Guide 4.2"

〔10〕 Stephen T. Walker, Steven B.Lipner, Carl M.Ellison, David M. Balenson "Commercial Key Recovery", 3. 1996. Vol.39. No.3, Communications of the ACM

〔11〕 VeriSign, "Key Management Service Administrator s Guide"

〈著 者 紹 介〉

국 상 진 (Sangjin Kook)
1989년 2월 : 한국항공대학교 정보통신공학과 졸업(학사)
2000년 2월 : 성균관대학교 전기, 전자 컴퓨터 공학부 (공학사)
2000년 3월~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부 석사과정
관심분야 : PKI, 키 복구, 디지털 워터마킹

최 강 은 (Kang-Eun Choi)
2000년 2월 : 단국대학교 수학과 (학사)
2000년 3월 ~ 현재 : 성균관대학교 전기전자 및 컴퓨터공학과 석사과정
관심분야 : 암호이론, 전자 상거래 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)
1978년~1980년 : 한국전자통신연구소 전임 연구원
1985년~1986년 : 일본 동경공대 객원연구원
1992년~1994년 : 성균관대학교 전산소장
1995년~1997년 : 성균관대학교 교학처장
1996년~1998년 : 국가정보화 추진위원회 자문위원
1998년~1999년 : 성균관대학교 정보통신기술연구소 소장
1990년~1999년 : 한국정보보호학회 이사
1998년~1999년 : 성균관대학교 정보통신기술연구소장
1999년~2000년 : 성균관대학교 전기전자 및 컴퓨터 공학부 학부장
1999년~2001년 : 성균관대학교 정보통신대학원 원장
1982년~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부 교수
1999년~현재 : 한국정보보호학회 수석 부회장
2000년~현재 : 정통부 지정 정보보호인증기술연구센터 센터장
관심분야 : 암호이론, 전자 상거래