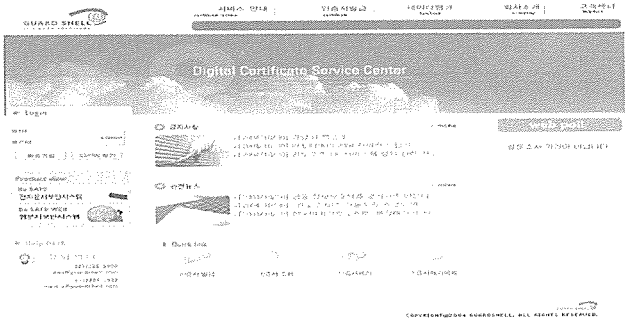
(주)가드쉘 "BeSAFE_PKI"

강력한 보안에 인증까지 -
전자정보자산보호 및 유출방지솔루션



(주)가드쉘 (대표 조성호)의 BeSAFE _PKI 는 가드쉘의 문서보안 및 유출방지 솔루션인 BeSAFE 와 PKI 인증시스템을 통합 구현한 전자정보자산보호 및 유출방지 솔루션이다.

BeSAFE_PKI 는 기업의 중요 보안문서에 대해 검증된 암호화 알고리즘을 이용하여 보안 상태를 유지하고, 사용자별 권한(열람, 저장, 인쇄, 수정)을 설정하여, 사용자의 권한에 따른 문서 사용이 가능하며, 사용자의 문서 사용을 통제/모니터링 할 수 있어, 전자문서의 철저한 보안 (무결성, 기밀성, 가용성)을 가능하게 한다.

BeSAFE_PKI 는 Device Driver를 제어하는 유일한 정보자산 보호 솔루션으로 OS 커널 레벨의 API Hooking 기술,File System 감시기술, Anti- Cracking & Hacking 기술 ,검증된 암호화 알고리즘을 적용하였다. 더불어 PKI 의 CA(Certificate Authority) 시스템은 인증서 및 CRL(Certificate Revocation List)을 배포 관리함으로써 사용자 온라인 인증서비스를 제공한다.

BeSAFE_PKI 로의 통합된 솔루션으로 더욱 강력해진 보안 시스템으로 기업 및 기관에서 디지털 콘텐츠의 남용 및 불법 유출을 미연에 방지할 뿐 아니라, 전자 정보의 훼손 및 변경을 방지하여 저작권보호, 핵심기술 유출방지, 안전한 거래를 가능하게 한다.

BeSAFE_PKI 의 다양한 암호화 알고리즘과 축약 알고리즘으로 공인된 대칭/비대칭 암호화 기법 모두를 활용하여 암호화 할 수 있다. BeSAFE_PKI 사용자의 요구에 따라 사용자 시스템에 국한된 보안 적용과 사용자 이동에 따른 보안정책 모두를 적용할 수 있어 기업 및 기관의 전자정보 자산보호 및 유출방지에 관한 보안 방법에 유연성이 생기게 되었다.

BeSAFE_PKI 는 저작권을 침해 받지 않고 특정한 사용자에게만 문서를 유통 활용하고자 하는 기업 및 기관, 특정한 협력업체 및 산하조직(대리점, 협력업체, 지사) 의 문서의 사용 및 유통을 안전하게 하고 싶은 기업 및 기관에서 도입 활용하면 좋은 효과를 거둘 수 있다.

동 상

BeSAFE_PKI

1. 작품명 : BeSAFE_PKI

(PKI 인증기반의 전자 정보자산 보호 및 유출방지 솔루션)

2. 제작자 : (주)가드쉘

대표자 : 조성호
개발참여자 : 신인철, 유병렬, 김기용
주소 : (143-747) 서울특별시 광진구 군자동 세종대학교
충무관 벤처센터 308c호
전화 : 02) 2205-2900
팩스 : 02) 3408-3881
email : sic@guardshell.com

3. S/W 요약설명

BeSAFE_PKI는 (주)가드쉘의 문서보안 및 유출방지 솔루션인 BeSAFE와 PKI 인증시스템을 통합 구현한 전자 정보자산 보호 및 유출방지 솔루션입니다.

BeSAFE_PKI 는 기업의 중요 보안문서에 대해
암호화 알고리즘을 이용하여 보안상태를 유지하고,
사용자별 권한(열람, 저장, 인쇄, 수정)을 설정하여,
사용자의 권한에 따른 문서 사용이 가능하며,
사용자의 문서 사용을 통제/모니터링 할 수 있어,
전자문서의 철저한 보안(무결성, 기밀성, 가용성)을 가능하게 합니다.

BeSAFE_PKI 는 Device Driver를 제어하는 유일한 정보자산 보호 솔루션으로 OS 커널 레벨의 API Hooking 기술,File System 감시기술,Anti-Cracking & Hacking 기술 ,검증된 암호화 알고리즘을 적용하였습니다. 더불어 PKI 의 CA(Certificate Authority) 시스템은 인증서 및 CRL(Certificate Revocation List)을 배포 관리함으로써 사용자 온라인 인증 서비스를 제공합니다.

BeSAFE_PKI 는 PKI 인증 기반으로 전자문서 등록/관리 시스템 및 기타 관련 시스템에 등록되어 있는 문서들을 기업이 인증하는 "DRM을 포함한 문서인증" 에 따라 용자들에게 문서 및 자료를 제공합니다.

BeSAFE_PKI 의 다양한 암호화 알고리즘과 축약 알고리즘으로 공인된 대칭/비대칭 암호화 기법 모두를 활용하여 암호화 할 수 있다. BeSAFE_PKI 사용자의 요구에 따라 사용자 시스템에 국한된 보안 적용과 사용자 이동에 따른 보안정책 모두를 적용할 수 있어 기업 및 기관의 전자정보 자산보호 및 유출방지에 관한 보안 방법에 유연성이 생기게 되었습니다.

BeSAFE_PKI 를 통해 기업 및 기관에서는 디지털 콘텐츠의 남용 및 불법 유출을 미연에 방지할 뿐 아니라, 전자 정보의 훼손 및 변경을 방지하여 저작권보호, 핵심기술 유출방지, 안전한 거래가 가능합니다.

3.1 개발 배경

정보시스템의 도입 및 확산으로 대부분의 문서가 PC에 의해 작성되면서, 기업의 정보 자산은 CAD나 오피스 워드 문서와 같이 디지털화 된 전자문서 형태로 변하였습니다.

이에 따라 각 기업이 보유하고 있는 정보 자산의 약 85%는 전자 문서의 형태로 만들어 집니다. (미국 가트너 그룹 조사)

중소기업도 정보화 1단계인 '단순기능 정보화 단계'를 지나 제2~3 단계인 '업무효율화 및 조직 정보화 단계'에 접어 들어 문서의 디지털화가 본격적으로 진행 되고 있습니다.

정보자산의 고 디지털화는 기업으로 하여금, 업무 능률과 생산성 향상을 위해 **"정보 자산의 축적과 관리 체계 그리고 공유 체계의 변화를 요구"**하고 있습니다. 디지털화가 고도화, 광범위화 할수록 **"외부 해커나 바이러스에 대한 정보 보호와 함께 내부자에 의한 기업 정보 무단 유출"**도 막아야 합니다.

그렇지 않으면 중요정보가 무단으로 유출되기 때문입니다.

"지식노동자의 생산성 향상과 함께 경제스파이로부터의 해방, 기업 생존의 필수 요소"입니다.

기업은 막대한 자본, 인력, 시간을 투입하여 경쟁력을 갖는 제품 생산과 서비스 제공을 위해 각종 지적 자산인 기업정보와 Know-How를 축적해 가고 있습니다. 차별화된 Know-How, 기술 및 경영 정보의 축적이 야말로 기업을 성장 발전시키는 유일한 길입니다.

이렇게 중요한 기업의 Know-How가 경쟁자의 수중에 일단 노출되면 경쟁 제품의 등장으로 인한 시장 점유율 감소와 매출 감소 등 심각한 경영상의 타격을 입게 됩니다. 그러므로, 기업 정보자산을 보호하는 것은 기업의 가치 내지는 경쟁력을 유지하기 위한 최소한의 수단입니다.

오늘날 기업의 정보자산은 디지털화로 인해 무단 복제가 용이하고 네트워크를 통한 순간 이동이 가능해져서 이러한 특성에 맞는 보호 대책을 필요로 합니다.

"중요 정보 유출 방지, 늦으면 시장에서 퇴출될 수도 있습니다."

최근까지 컴퓨터 보안 사고는 지속적인 증가 추세를 보이고 있으며, 사고의 유형도 다양해지고 있습니다.

이 중 기업에 가장 많은 금전적 피해를 가져오는 보안 사고는 기업 정보자산 유출입니다. 그러나, 중소기업이 주로 도입한 정보보호시스템은 외부로부터의 침입을 차단하거나, 침입을 감시하는 데 그치고 있습니다.

피땀 흘려 만든 기술과 정보, 몰래 새는 것을 막아 기술의 우위성을 지켜나가야 합니다

◎ 중요정보자산보호 및 유출 방지에 대한 요구 증대

■ 시급한 내부 보안관리
- 외부침입에 대한 보안 관리에 비해 내부자 유출에 관한 보안 관리 대비는 거의 전무한 상태
- 정보와 기술력이 생존의 가장 중요한 요소로 인식되면서 내부핵심 기술 및 정보자산에 대한 보안관리 요구 확대

■ 보안과 업무 효율성
- 보안 적용과 업무 효율성은 반비례 관계에 있으나, 업무 효율 저해를 최소화 하면서 강력한 보안을 희망함
- 한층 강화된 보안에 PKI 도입을 통해 이동성을 보장하여 업무 효율을 높임.

■ 보안적용의 다양성과 확장성
- 기존의 정보화 시스템의 형태에 따라 보안정책의 형태가 다양함.

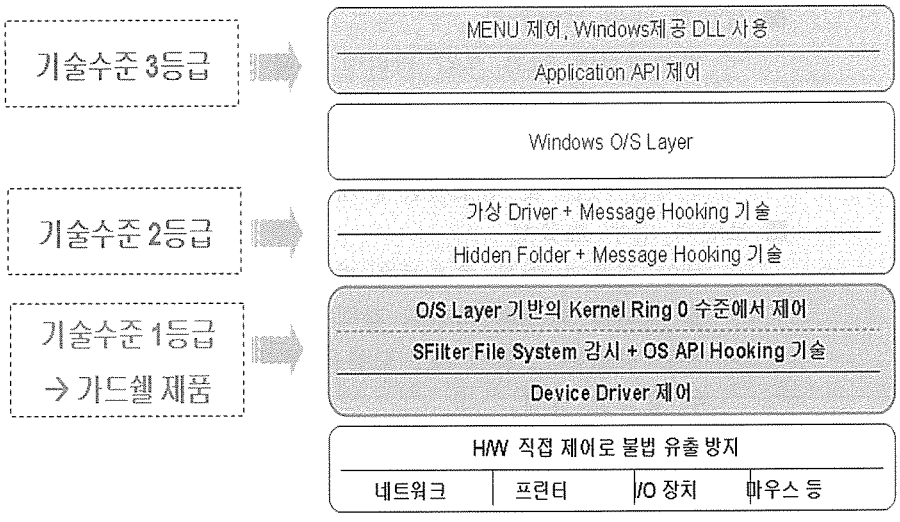
– 합법적인 유출에 대한 데이터 위/변조 도 보호 대상
– 보호자산의 영역이 점차로 넓어짐
– 다양한 요구와 확장성에 따른 대비책 필요

3.2 시스템 개요

기업 및 기관 내에 자료실, 파일서버, 지식관리 시스템, 전자문서 관리 시스템, 전사적 자원관리 시스템, 고객관리 시스템 등에 존재하는 전자문서가 업무 효율성과 원활한 의사소통을 위해 공유되어 있습니다.
BeSAFE_PKI는 이런 기업 및 기관이 보유한 중요한 정보 자산이 공적인 업무를 벗어나, 개인적으로 활용되고 유통되며, 경쟁사나 해외에 유출되는 것을 막기 위해 개발되었습니다.
BeSAFE_PKI 는 기존의 기업 및 기관이 가지는 중요 전자정보 자산에 대한 관리가 개인에 의해 행해지던 관행을, 그 중요정보 자산의 소유 주체인 기업 및 기관에서 유통 및 활용을 관리하고 통제할 수 있도록 만들어 줍니다.
BeSAFE_PKI 는 전자정보의 활용 유통에 권한을 부여하는 것과 더불어 전자서명과 같은 확실한 사용자 인증을 포함함으로써, 중요 전자정보의 유통 경로를 추적할 수 있어 어떤 불법적인 유출 시도에 대해 심리적,제도적 차원에서도 막강한 해결책이 될것입니다.

3.3 시스템 특징

◎ 기반 기술의 특징



구분	대표 사용 기술	장 점	단 점
기술 수준 3등급	▷ Application API 제어 (Windows O/S 거의 제어 못함)	▷ 대부분의 기술이 Share Ware 로 공개돼 있어 비교적 쉽게 DRM 상품화 가능	▷ 보안 취약이 취약하고 각각의 어플리케이션 마다 또한 버전마다 보안 적용 ▷ 기존 보안 목적물 시스템과의 연동이 곤란 ▷ CAD시스템 등의 Command Line 제어 못함
기술 수준 2등급	▷ 가상 Driver 사용 ▷ Message Hooking 기술 (Windows O/S 일부 제어)	▷ 3등급 기술보다 진일보한 기술 사용 ▷ 복호화 시 흔적 안 남김 (단, 고의 정전이나 고기술 Debugger 사용자는 흔적 발견 가능성 높음)	▷ O/S가 제공하는 가상 Driver를 사용하여 보안의 취약점 발생 ▷ Message를 먼저 Hooking 당하면 보안이 뚫림 ▷ Registry를 방어하지 못함 ▷ Message를 계속 Tracking하기 때문에 Message가 Over-Flow되면 시스템에 치명적 오류 발생
기술 수준 1등급	▷ O/S 커널 레벨의 API Hooking 기술 ▷ Device Driver 제어 ▷ File System 감시 ▷ Anti-Debugging	▷ O/S Layer 기반의 Kernel Ring 0 수준에서 보안기능 수행 ▷ 고의 정전 시에도 복호화 흔적 안 남김 ▷ 기존 시스템과의 연동이 손쉬움 ▷ H/W Device Driver를 Control, 최강의 보안시스템 구축 가능	▷ 기술 구현이 몹시 어려운 최고 난이도 기술 → ㈜가드텔 "Be SAFE 문서 보안" 시스템 구현에서 Infra로 채택된 기술

◎ PKI 개요 및 도입배경

◈ PKI(Public Key Infrastructure) : 공개키 기반 구조의 정의

- 사용자의 공개 키를 인증해 주는 인증기관들의 네트워크
- 모르는 사람과의 비밀 통신을 가능하게 하는 암호학적 키와 인증서의 배달 시스템
- 공개키의 인증서를 이용해 공개 키들을 자동적으로 관리해 주는 기반 구조
- 공개 키 인증서를 발행하고 그에 대한 접근을 제공하는 인증서 관리 기반 구조

◈ **PKI 기반의 인증기술의 특징**

- 인증(authentication) : 수신자가 받은 메시지가 정당한 송신자로부터 전송된 것인지를 확인할 수 있게 하거나, 송/수신자 간에 각자의 실제 신원을 확인하는 것이 가능하도록 하는 서비스(**통신 주체의 신원확인**)
- 무결성(integrity) : 수신한 메시지가 불법적으로 재생된 것인지, 전송과정에서 변조되었거나 재구성되었는지에 대한 확인을 보장하는 서비스(**통신 내용의 완전성 보호**)
- 기밀성(confidentiality): 정당한 권한이 부여된 사용자나 의도

된 수신자를 제외한 어떠한 사용자도 데이터의 일부라도 읽지 못하도록 하는 서비스 **(통신내용의 기밀성 보호)**

- 부인방지(non-repudiation) : 수신자가 받은 메시지에 대하여 송신자가 취소할 수 없도록 하는 서비스**(통신상의 행위에 대한 부인방지)**

◈ **도입배경**

- 인증서 기반 공개 키 암호 시스템의 구현 및 운영을 지원
- 안정된 커뮤니케이션 환경 조성
- 신뢰할 수 있는 데이터 보호 및 사용자 인증방법 채택
- 사용자의 이동성 보장 또는 H/W Binding 등 보안 정책 유연성 확보

◎ **시스템의 주요 특징**

■ **OS 커널 레벨의 API Hooking 기술 적용**

Client에서 이루어지는 문서보안의 핵심 기술로 사용
OS보안커널 상에서의 API Hooking을 통한 Device Driver제어
cf) Application Program 레벨의 Win32 API 제어가 아님
사용자의 각종 불법, 비권한 활용을 원천적으로 차단

■ File System 감시기술 사용

MS에서 인정하고 있는 파일시스템의 최고 감시 기술인 FILTER 기술 적용
암호화 문서의 복호화 폴더 접근 제어
암호화된 문서의 복호화 시 연결프로그램 설정제어

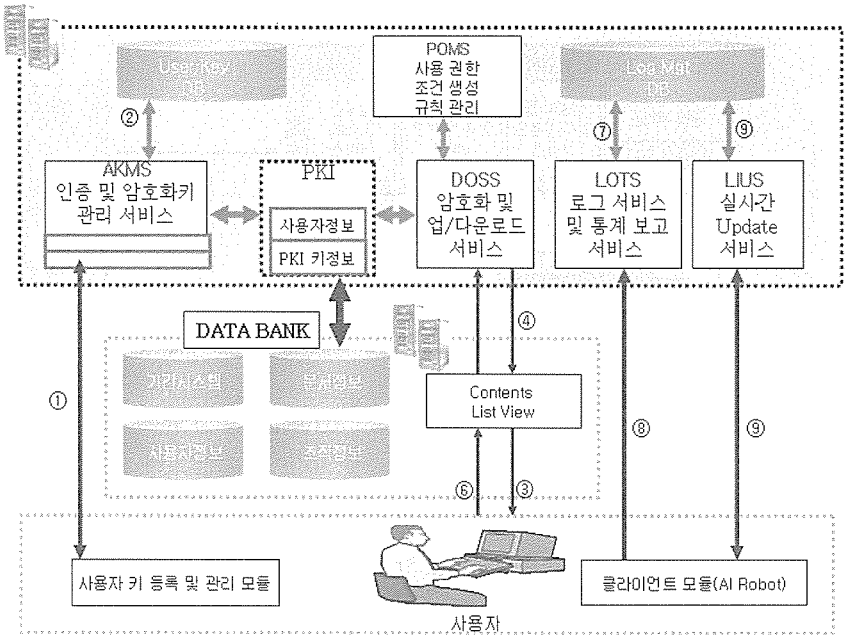
■ Anti-Cracking & Hacking 기술 적용

보안시스템 자체를 분석하지 못하게 사전 예방
(Reverse Engineering 불가)

■ Device Driver 제어

USB, CD-ROM, 프린터, Network, Mouse 등의 장치를 직접 제어하므로 완벽한 유출 방지 실현, 최고 난이도의 기술 보유

◎ 시스템 구조

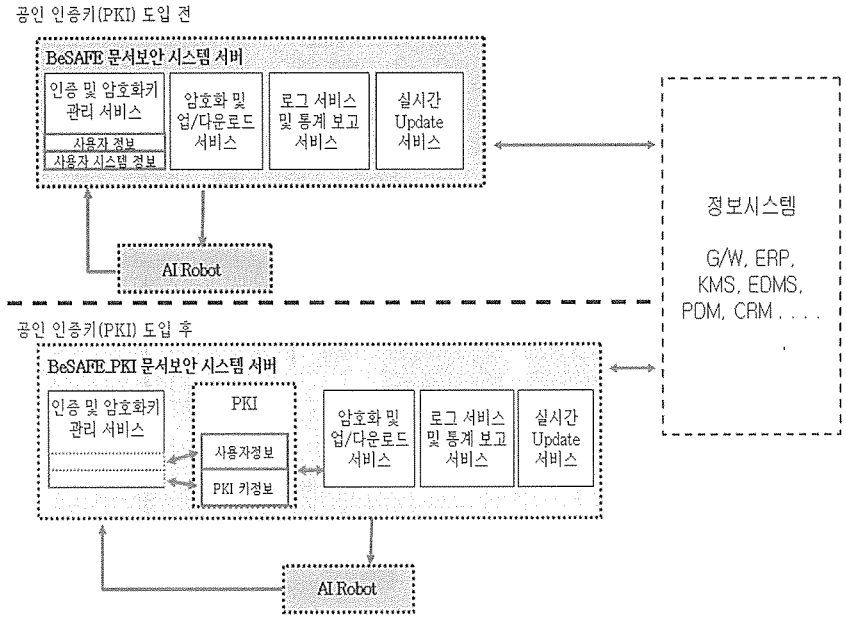


■ BeSAFE_PKI POMS(Policy Management Server)
사용자 및 전자 문서 권한정보 관리시스템

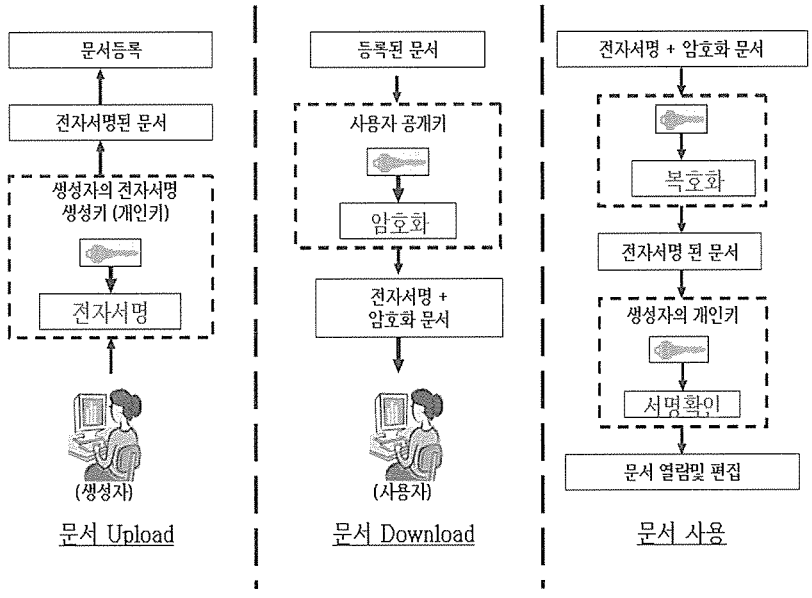
■ BeSAFE_PKI SECS(Service Control Server)
전자 문서 보안 및 관리, 제어, 유통 시스템
AKMS(Authentication & Key Management Service)
사용자 인증 및 키 관리
- PKI (Public Key Infrastructure)
사용자 인증, 사용자정보, 키정보
DOMS(Document Management Service)
문서 관리, 유통 및 암호화
LOTS(Log & Tracking Service)
사용자/문서 사용 Monitoring 및 관리정보 제공
LIUS(Live Update Service)
AI Robot 실시간 갱신

■ BeSAFE_PKI AI Robot
사용자 환경에 설치된 보안 클라이언트 시스템

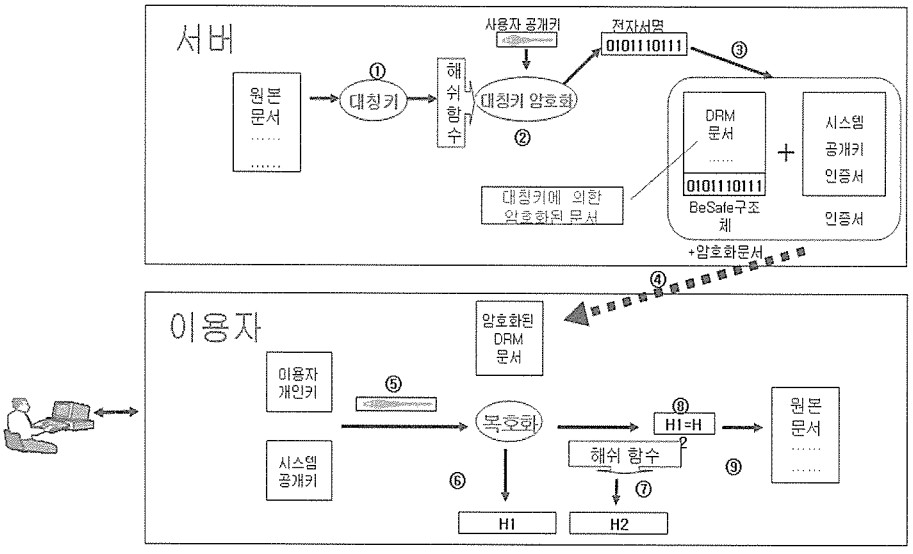
◎ PKI 도입 전 /후 비교



◎ 문서 Up/Down, 문서사용 시 인증과정



◎ 문서 다운로드 과정



◎ 문서 편집 시 보안 제공 기능

- 보안 문서에 대한 다양한 편집 기능을 차단함으로써 보안 문서에 대한 무결성(Integrity) 보장
- Menu Bar, Tool Bar, 키보드 단축키, 마우스 우측버튼등의 사용 차단
- 편집 기능 차단은 아래와 같음
  잘라내기 (Ctrl+ X)
  복사 (Ctrl+ C)
  붙여넣기 (Ctrl+ X)
  지우기 (Del)
  블럭설정 (F3)
  하이퍼링크붙여넣기
  바꾸기 (Ctrl+ H) 등
- 각종 Screen Capture 프로그램에 의한 Capture 차단 및 PDF로의 변환 차단

◎ 문서 저장 시 보안 제공 기능

- 비권한자에 의한 불법적 저장을 차단함으로써 보안 문서에 대한 기밀성(Confidentiality) 보장
- Menu Bar, Tool Bar, 키보드 단축키, 마우스 우측버튼등의 사

용 차단

■ FDD, HDD, CD-RW, USB메모리 등의 각종 저장매체로의 저장 차단

■ 세부 차단 저장 기능은 아래와 같음

저장 (Ctrl+ S)

다른 이름으로 저장

웹페이지로 저장 등

◎ 문서 인쇄 시 보안 제공 기능

■ 비권한자에 의한 불법 인쇄를 사전 차단함으로써 보안문서에 대한 기밀성(Confidentiality) 보장

■ Menu Bar, Tool Bar, 키보드 단축키, 마우스 우측버튼등의 사용 차단

■ 인쇄 회수 지정(Count Bomb)

- 인쇄 일시, 인쇄자 리포트

■ 회수가 초과되면 추가 인쇄 차단

- 추가 인쇄 시 불법 사용 리포트

◎ 문서 전달 시 보안 제공 기능

■ 비권한자에 의한 불법적 전달을 차단함으로써 보안 문서에대한 기밀성(Confidentiality) 보장

■ Menu Bar, Tool Bar, 키보드 단축키, 마우스 우측버튼등의 사용 차단

■ E-Mail 첨부 차단

■ 세부 차단 보내기 기능은 아래와 같음

전자 메일로

이 파일을 첨부한 메일로

회람으로

Exchange 폴더 내에 게시 등

◎ 문서 열람 시 보안 제공 기능

■ 서버에서 클라이언트로 문서가 다운로드될 때 문서 자체를 512bit 공인 알고리즘으로 암호화함

■ 문서를 다운로드할 때 열람요청자의 권한 정보를 암호화된 문서에 이식하므로 사용자는 열람 및 허가된 권한내에서만 문서사용

■ 문서를 다운로드할 때 열람 요청자의 시스템 정보를 조합한 암호화 키를 생성하여 암호화함으로써 복제된 문서는 다른 PC에서

절대 열람할 수 없음

- 암호화된 문서를 열람하기 위해서는 복호화를 해야 하는데, BeSAFE_PKI 는 암호화된 폴더에서 복호화를 수행하기 때문에 안전함
- 문서 열람이 종료되면 사용자 PC에는 열람한 문서의 어떤 흔적도 남지 않아 해킹이 불가능함

◎ 다양한 암호화 기법과 축약 알고리즘

- 암호화 알고리즘

  BeSAFE_PKI에 사용되는 암호화 알고리즘은 기본적으로 Blowfish를 사용하고 있으며, 고객의 요청에 따라 타 알고리즘을 DLL형태로 제공, 손쉽게 사용할 수 있습니다.

  Blowfish는 DES 등 기존의 암호화 알고리즘의 대안으로 설계된 암호화 알고리즘이며, 32~1024비트까지 가변적인 길이의 키를 사용하는 대칭 블록을 쓰고 있음

  Blowfish는 32비트 명령어 프로세스를 염두에 두고 설계 되었으므로 DES에 비해 속도가 현저히 빠름

- 축약 알고리즘과 전자 서명 알고리즘

  BeSAFE_PKI 는 MD5, SHA1의 축약 알고리즘과 RSA암호를 통한 전자서명 알고리즘을 적용하였으며, 이 또한 고객의 요청에 따라 다양한 타 알고리즘 적용이 가능합니다

- 암호 키 생성

  BeSAFE_PKI 는 서버에서 클라이언트로 문서가 내려갈 때 문서 자체를 암호화하여 내려 보냄

  이 때 각 클라이언트 PC의 유일한 시스템 정보를 조합하여 암호화키를 생성하여 암호화함으로써 문서가 복제되어도 다른 PC에서 문서를 열람할 수 없도록 지원 암호화된 문서를 합법적으로 획득한 이후에도 원문으로의 변경 저장이 불가능

  사용자의 이동성을 위하여 PC의 유일한 정보가 아닌 사용자의 유일한 개인 킷값으로 암호화키를 생성할 수 있습니다.

  이 때는 사용자의 개인키 값을 알지 못하면 문서를 열수조차 없게 되어 문서의 유통과 관계없이 보안이 유지됩니다.

  위의 두 가지 방법을 함께 적용할 수 있습니다.

  강력한 보안과 인증을 함께 구현하고자 하는 경우에 해당됩니다.

3.4 제품 구성 및 기능

◎ BeSAFE_PKI Server

■ **사용자/문서 관리**

보안 정책 설정, 관리
보안정책 예외자의 개인정책 권한 설정
문서별 권한 정책 설정, 관리

■ **사용자/문서 Monitoring**

사용자의 보안문서 사용 내역 기록
문서의 활용 내역 기록
권한 및 비권한 사용 추적(보안담당자, 책임자)
각종 사용 기록 정보 제공

■ **문서 암호화**

문서의 Download시 암호화 처리
암호화 상태로 PC에 보관, 불법 유출 해독 불가

■ **사용자 인증 및 권한 Package 구성**

암호화된 문서에 문서 요청자의 키 및 권한 이식

◎ BeSAFE_PKI Client

■ **문서 등록**

문서의 접근 및 유효권한, 접근 권한 대상자 설정
문서의 보안등급 설정

■ **문서 열람**

비권한자에 의한 열람 차단
접근/유효권한에 의한 열람
사용자 PC의 고유정보 및 ID/PW 인증의 2중 안전

■ **문서 편집**

각종 편집 명령 차단
Screen Capture 차단
PDF로의 변환 차단

■ **문서 인쇄**

권한자에 의한 인쇄 차단
인쇄 횟수 제한

■ **문서 저장**

비권한자에 의한 저장장치로의 저장 차단
비권한자에 의한 각종 저장명령 차단

■ **문서 전달**

비권한자에 의한 각종 전달명령 차단
E-Mail 첨부 차단

4. 개발단계별 기간 및 투입인원수

개발단계	개발시간	인원	공수	비고
BeSAFE	02. 11 ~ 03. 6	6	42	기 문서보안 솔루션
DRM 컨텐츠 유통을 위한 보안 및 인증시스템	04.5 ~ 04. 9	1	4	한국전자통신 연구원(ETRI) 이전 기술
통합 테스트 및 제품 출시	04. 9 ~ 04.10	2	3	BeSAFE_PKI 통합
계	13개월		49	

5. 사용 또는 개발언어, TOOL

C, C++, PHP
.NET

6. 사용시스템

구분	운영S/W 및 장치	최소사항	권장사양
SERVER	O/S	Windows 2000, 2003 Server	
	DBMS	MS-SQL 2000 이상	
	CPU	PⅢ 500MHz	PⅣ 1GHz
	MEMORY	128MB	512MB
	HDD	10GB	30GB
CLIENT	O/S	Windows 98 이상	windows 2000 이상
	CPU	PⅡ 350MHz	PⅢ 700MHz
	MEMORY	64MB	128MB
	HDD	-	-