(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G06F 17/00

(11) 공개번호 특2000-0047643
(43) 공개일자 2000년07월25일

(21) 출원번호 10-1999-0050525
(22) 출원일자 1999년11월15일
(30) 우선권주장 2,256,936 1998년12월23일 캐나다(CA)
(71) 출원인 인터내셔널 비지네스 머신즈 코포레이션 포만 제프리 엘
미국 10504 뉴욕주 아몬크
(72) 발명자 배쳐해미드
미국22066버지니아주그레이트폴즈로쿠스트힐드라이브9510
캐롤로버트브루스
미국10549뉴욕주마운트키스코바이램레이크로드246
밀레스레브
캐나다엘4제이6피4온타리오주쏘온힐밀크로프트웨이98
챠오셩웨이
캐나다엠2엔3케이5온타리오주토론토홀리우드애비뉴168
(74) 대리인 김창세, 김원준, 장성구

심사청구 : 있음

(54) 데이터 보관 시스템에 저장된 전자 데이터 파일을탐색하는 안전 시스템, 전자 데이터 보관소의 안전 전자데이터 탐색 시스템을 유지하는 방법 및 컴퓨터 판독 가능메모리

요약

전자 서류가 다른 엔티티(entity)들에 의한 검토에 이용가능하게 되는 때, 그 서류를 제 3 자에 의해 관리되는 보관소 또는 데이터베이스에 저장하는 것이 편리한 경우가 있다. 데이터 보관소내에 저장된 서류에 대한 액세스 권한을 서류 발원자(document originator)에 의해 부여받은 엔티티들은 보관소 관리자가 액세스 특권에 관한 정확한 정보를 제공할 것인가에 대한 염려를 하지 않고서도 제 3 자 보관소에 파일링된 서류를 안전하게 탐색할 수 있는 시스템이 제공된다. 보관소에 저장된 데이터에 대한 액세스 특권을 가진 서류 발원자, 보관소 관리자 및 모든 엔티티들은 제각기의 작업 공간의 안전한 확장(secure extension)인 볼트 환경(valut environment)을 갖는다. 서류 발원자의 볼트는 보관소에 기탁된 각 서류에 대한 액세스 제어 리스트(ACL)를 보유한다. 보관소에 저장된 어떤 서류에 대한 액세스 특권을 갖는 각 엔티티의 볼트는 보관소에 저장된 서류에 대한 엔티티의 액세스 특권에 관한 능력 리스트(capability list)를 보유한다. 엔티티 자체는 자신의 데스크탑 상에서 능력 리스트의 최신 버전의 증명을 유지한다. 서류의 ACL이 서류 발원자의 볼트에서 갱신될 때, 서류 발원자의 볼트는 어떤 엔티티가 변경에 의해 영향을 받았는지를 판단하고, 그 변경을 상기한 영향을 받은 엔티티들의 볼트로 통신한다. 각각의 볼트는 자신의 능력 리스트를 갱신하고, 첫 번째의 유용한 기회가 있을 때, 엔티티의 데스크탑 상에서 능력 리스트의 최신 버전의 증명을 갱신한다.

대표도

도2

명세서

도면의 간단한 설명

도 1은 제 3 자 관리자를 이용하는 서류 보관소 시스템의 개략도,

도 2는 본 발명의 바람직한 실시예에서 이용되는 볼트 서류 보관소 시스템을 도시하는 도 1과 유사한 개략도,

도 3은 본 발명에 따른 서류 생성 과정을 설명하는 흐름도,

도 4a 및 도 4b는 본 발명에 따른 서류 검색 과정을 설명하는 흐름도,

도 5a 및 도 5b는 본 발명의 바람직한 실시예에 따라 서류 탐색 및 검색에 대한 액세스 제어의 불변성을

제공하는 과정을 예시하는 흐름도,

도 6은 본 발명에 따른 저장된 서류에 대한 소유권자 특권을 할당하는 과정을 설명하는 흐름도.

도면의 주요 부분에 대한 부호의 설명

100, 200 : 서류 발원자 104, 204 : 서류 보관소 서비스

106, 206 : 사업 파트너 210 : 애플리케이션 서버

212 : 데이터베이스 보관소 214 : 볼트 제어기

216 : 서류 발원자 볼트 218 : 사업 파트너 볼트

220 : 애플리케이션 서버 볼트

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 전자 데이터 저장(electronic data storage) 분야에 관한 것이다. 특히, 본 발명은 데이터 탐색 및 검색에 대한 액세스 제어를 실행하는 비밀 데이터 보관소 및 교환 시스템(secure data repository exchange system)으로서 제 3 자 데이터 관리자(third party data custodian)에 의해 관리되는 안전한 데이터 보관소 및 교환 시스템에 관한 것이다.

최근 네트워크 통신과 공용 키 인프라스트럭처(public key infrastructure : 'PKI') 기술의 동반적 진보에 따라 일반 기업체 및 공공 기관에서 기록 보관(record-keeping) 및 모든 형식의 업무를 위하여 전자 서류를 이용하기 시작했다. 전송의 완전성 및 보안성(transmission integrity and security)이 향상됨에 따라, 인터넷 및 다른 개방형 네트워크를 통해 전자적으로 전송되는 서류가 손대지 않은 온전한 상태로 도달될 수 있을 것이라는 확신을 가질 수 있게 되었다. 수 기가비트의 데이터를 저장할 수 있는 모뎀 컴퓨터 메모리와 결합된 데이터베이스 관리 시스템을 사용함으로써, 일반 기업체 및 공공 기관은 물적 비용을 요하는 지면 기록물(paper records)을 유지시킬 필요가 없게 된다.

전형적으로, 한 엔티티(entity)로부터 발원되는 데이터를 기탁, 검토 등과 같은 이유에서 다른 엔티티에게로 전송해야 할 수도 있다. 데이터 요소들은 체계적이지 못한 서류 파일 또는 체계적인 기록물 예를 들어 은행 계정 및 기타 다른 재무 정보의 형태를 취할 수도 있다. 체계적이지 못한 데이터를 사용하면, 서류를 검토 목적으로 데이터 발원 시스템으로부터 동일 시스템내의 다른 컴퓨터로 또는 다른 시스템내의 컴퓨터로 보내야만 할 수도 있는데, 이러한 일은 공공 기관 환경(예를 들면, 대학 논문 심사 위원회에 제출하기 전에 지도 교수에 의해서 검토될 졸업 논문)에서와 같이 사업 환경(예를 들면, 합작 투자 제안 또는 단지 입찰 신청 제안)에서도 마찬가지로 발생할 수도 있을 것이다. 서류는 전자적으로 생성되어야 하는데, 그 이유는 (특히 내용이 많은 경우에는) 매번 서류 전체를 다시 타이프하지 않고서도 수정과 추가가 용이하기 때문이다.

서류가 전자적 형태를 취하게 하면 또한 그 서류의 검토가 촉진되는데, 이는 그러한 전자 형태의 서류는 용이하게 전송될 수 있기 때문이다. 서류를 입수하고자 하는 검토자는 일단 그들이 서류 보관 장소에 액세스한 상태에서는 시스템을 탐색하는 것에 의해 서류를 입수할 수 있다.

지역적인 서류 저장이 방화벽 이면에서의 제 3 자에 대한 액세스 부여를 의미하는 경우에 서류 발원자는 지역적인 서류 저장을 원하지 않을 것인데, 이는 예를 들어 보안성(security), 데이터 완전성(data integrity) 및 시스템 또는 네트워크 효용성(availability) 등의 여러 가지 이유 때문이다. 이러한 이유들은 미국에서 본 출원과 동일자로 출원되어 본 출원의 출원인에게 양도된 출원으로서 본원 명세서에 참고로 인용되는 'System for electronic Repository of Data Enforcing Access Control on Data Retrieval'(IBM Docket No. CA998-030)라는 명칭의 출원에 상세히 기술되고 있다.

본 출원과 동일자로 출원된 상기한 출원은 보관소에 저장된 데이터에 대한 완전성 및 액세스가 보관소의 제 3 자 관리자의 어떠한 행위에도 무관하게 유지되는 시스템에 관한 것이다.

상기한 출원에 개시된 발명은 많은 수의 서류가 많은 수의 유저들에게 액세스가능한 시스템에서 매우 효과적인데, 이는 그 서류에 대한 액세스 권한을 부여받은 유저의 액세스 관련 정보가 단일의 중앙 위치 즉 보관소 자체내에 저장되기 때문이다. 유저는 서류에 대한 액세스의 보안 지식을 시스템 외부의 수단을 통하여 얻는다.

본 발명은 권한을 부여받은 유저 액세스에 관한 정보를 시스템 자체에 보유하고 있으며 또한 보관소를 관리하는 제 3 자 관리자의 어떠한 행위로부터도 안전하다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명의 목적은 제 3 자에 의해 관리되는 보관소(repository)내에 서류가 물리적으로 저장되어 있지만 유저가 그 보관소내의 어떤 서류에 액세스가능한 지의 판단을 위해 탐색할 수 있게 하는 전자 서류 저장소 및 교환 시스템(electronic document storage and exchange system)을 제공하고자 하는

것이다.

본 발명의 다른 목적은 보관소에 저장된 데이터에 대한 액세스 권한을 부여받은 유저의 액세스 관련 정보에 대한 완전성 및 액세스가 시스템을 통해 유효하나 제 3 자 보관소 관리자의 행위에는 무관한 시스템을 제공하고자 하는 것이다.

발명의 구성 및 작용

따라서, 본 발명의 일 태양에 따르면, 본 발명은 데이터 보관소 시스템(a data repository system)에 저장된 전자 데이터 파일을 탐색하는(searching) 안전 시스템(a secure system)을 제공한다. 이 시스템은 데이터 보관소 시스템내 전자 데이터 파일의 기탁자 컴퓨터(depositor computer)용 제 1 에이전트 프로그램(agent program) 및 전자 데이터 파일에 대한 액세스 특권(access privileges)을 갖는 제 1 유저 컴퓨터(user computer)용 제 2 에이전트 프로그램을 수용하는 통신 환경(a communication environment)을 포함한다. 본 발명의 시스템은 또한 전자 데이터 파일의 액세스 제어를 수록한 전자 데이터 파일용 목록(a manifest)을 포함한다. 이 목록은 제 1 에이전트 프로그램에 대해 액세스 가능하고 제 1 에이전트 프로그램에 의해 유지된다. 제 1 사용자 컴퓨터는 제 2 에이전트 프로그램에 대해 액세스 가능하고 제 2 에이전트 프로그램에 의해 유지되는 전자 데이터 파일에 대한 액세스 특권의 기록(record)을 가진다. 전자 데이터 파일에 대한 제 1 유저 컴퓨터의 액세스 특권에 영향을 미치는 목록이 변경되는 경우, 그들 변경은 제 1 에이전트 프로그램으로부터 제 2 에이전트 프로그램으로 전달됨으로써 제 1 유저 컴퓨터의 액세스 특권 기록은 갱신될 수 있게 된다. 제 1 에이전트 프로그램은 또한 전자 데이터 파일이 제 2 에이전트 프로그램으로 전달되기 전에 전자 데이터 파일에 대한 제 1 유저 컴퓨터의 액세스 특권을 확인할 수 있다.

다른 태양에 따르면, 본 발명은 전자 데이터 보관소에 저장된 각각의 전자 데이터 파일에 대한 액세스 제어를 수록한 목록과 보관소에 저장된 전자 데이터에 대해 액세스하는 각 컴퓨터의 서류 액세스 특권을 수록한 기록을 가진 시스템에 전자 데이터 보관소의 안전한 전자 데이터 탐색을 유지하는 방법을 제공한다. 이 방법은 보관소에 저장된 전자 데이터 파일의 목록을 갱신하는 단계와, 갱신에 의해 전자 데이터 파일에 대한 액세스의 변경이 영향을 받는 모든 컴퓨터를 확인하는 단계와, 액세스의 변경을 상기한 영향을 받은 모든 컴퓨터에 전달하는 단계와, 상기한 영향을 받은 모든 컴퓨터의 액세스 특권 기록을 갱신하는 단계와, 갱신된 액세스 특권 기록을 상기한 영향을 받은 컴퓨터들에 전달하는 단계를 포함한다.

또 다른 태양에 있어서, 본 발명은 데이터 보관소 시스템에 저장된 전자 데이터 파일을 탐색하기 위한 안전 시스템을 제공한다. 이 시스템은 데이터 보관소 시스템에 저장된 각각의 전자 데이터 파일에 대한 액세스 제어를 수록한 목록을 유지하는 수단과, 각각의 목록에 대한 액세스를 기탁 특권을 갖는 컴퓨터로 제한하는 수단과, 데이터 보관소 시스템에 저장되어 있는 적어도 하나의 전자 데이터 파일에 대한 액세스 특권을 가진 각각의 컴퓨터와 연관된 전자 데이터 파일에 대한 액세스 특권을 수록한 기록을 유지하는 수단과, 각각의 기록에 대한 액세스를 액세스 특권을 가진 상기한 연관된 컴퓨터로 제한하는 수단과, 목록내의 액세스 변경에 의해 영향을 받은 각각의 컴퓨터와 연관된 기록을 갱신하는 수단을 포함한다.

상술한 시스템 또는 방법을 구현하는 프로그램 코드로 인코딩된 매체가 또한 본 발명에서 제공된다.

이하, 본 발명의 실시예들은 첨부 도면과 관련하여 상세히 설명될 것이다.

도 1에는 제 3 자 관리자를 이용하는 서류 보관소 시스템의 통상적인 구성이 도시된다. 서류 발원자(document originator)(100)는 제 3 자에 의해 관리되는 데이터베이스와 같은 원격 서류 보관소 서비스(104)와의 접속 수단(102)을 통하여 서류를 기탁한다(deposit). 기탁된 서류의 소유자로서, 서류 발원자(100)는 그 서류에 대한 액세스를 할당할 수 있다. 예를 들면, 서류 발원자는 사업 파트너(160)에게 '판독' 특권('read' privilege)을 갖도록 할당할 수 있는데, 이것은 지정된 사업 파트너가 서류 보관소 서비스(104)와의 접속 수단(108)을 통하여 서류를 검색하는 것은 허용되지만 기탁된 서류에 변경을 가할 수는 없다는 것을 의미한다.

이러한 통상적인 시스템에 있어서는, 서류 발원자에 의해 기탁된 서류가 통상 암호화되지 않기 때문에, 사업 파트너(106)는 그 서류를 요구가 있는 즉시 검토할 수 있을 것이다. 이것은 종래 기술에서 서류를 암호해독하는 것과 연관된 문제가 있기 때문이다. 서류의 암호해독은 서류 발원자(100)의 개인키(private key)에 대한 액세스를 필요로 한다. 개인키에 대한 액세스를 부여하기 위해서, 서류 발원자(100)는 암호해독 자체의 수행을 위해 암호해독이 요청될지도 모르는 기간 내내 이용가능한 온라인 상태를 유지해야만 하거나(시스템 효용성의 문제), 서류 발원자(100)는 그의 개인키가 사업 파트너(106)에게 직접적으로 또는 신뢰성있는 프록시(trusted proxy)(도시 안함)를 통하여 이용가능하게 되도록 체계를 사전에 설정해야만 한다.

IBM 소유의 미국 특허 제 5,491,750 호는 'Method and Apparatus for Three-Party Entity Authentication and Key Distribution Using Message Authentication Codes' 에 관한 것이다. 이 특허에서는 통신 파트너가 신뢰성있는 중재자를 통하여 인증 받은 후에 둘 이상의 통신 파트너에 의해 공유되는 비밀 세션-관리키(secret session-management key)들을 분배할 수 있게 하는 시스템을 기술하고 있다. 그러나, 이러한 구성 등에서 생성된 키들은 수명이 짧은 것으로서 절대적으로 필요한 만큼 거의 사용되지 않으리라고 생각된다. 이러한 구성이 영구적인 서류 보관소를 갖는 서류 검토 시스템의 통신 파트너들간에서 암호해독키를 안전하게 전송하기에 적절한 것인 지는 분명하지 않다.

그래서, 서류를 소정 기간 동안 기탁하고 암호화하지 않는 통상의 시스템(도 1 참조)에 있어서는, 보관소 서비스(104)의 제 3 자 관리자는 서류의 완전성 유지에 믿음이 있어야 한다.

본 발명의 바람직한 실시예에 따른 서류 보관소 시스템은 'Secure Sever and Method of Operation for a Distributed Information System' 이라는 명칭으로 1997년 11월 26일 출원된 미국 특허출원 제 980,022 호의 주제인 'IBM Vault Registry' 제품에 의해 구성된다. 미국 특허출원 제 980,022 호는 본 명세서에 참고로 인용된다. IBM Vault Registry 제품은 클라이언트 환경의 안전한 확장(a secure extension) 소위

볼트(vault)를 구현하는 향상된 웹 서버 환경을 제공한다. 이 시스템은 본 명세서의 본 명세서의 서두 부분에서 기술한 바와 같이 전자적으로 전송되는 서류 및 기타 다른 데이터가 에러가 없는 상태로 온전하게 도달되게 할 최신 전송 기술에 의존한다. 클라이언트의 볼트내에 보유된 자원은 인증된 개인 키(certified public keys)에 의한 엄격한 인증을 통해 클라이언트로부터 액세스될 때만 유용하다. 클라이언트 환경에 의존하여, 액세스는 클라이언트의 웹 브라우저를 통해 이루어질 수 있다.

볼트의 정보 내용은 비밀을 위해 암호화된다. 서버상의 각각의 볼트는 그 볼트의 소유자에 의해 승인된 신뢰성있는 경로 예를 들어 브라우저를 통하지 않고서는 키에 대한 액세스를 금지하는 특유의 암호 키 및 메커니즘을 갖는다. 볼트내에서 동작하는 프로그램들은 운영 체제 서비스에 의해 분리되어,

(a) 그러한 프로그램들이 시스템의 정체(a system identity)(가상적 로그온(a virtual logon))갖고서 소정의 프로세스에서 동작함으로써 그 정체가 볼트내에서 동작하는 프로그램에 의해 변경될 가능성이 없는 상태로 종속 프로세스에서 이용가능하도록 하고;

(b) 그러한 프로그램들이 다른 곳이 아니라 그들이 동작하는 볼트의 데이터 내용에 대해 액세스하도록 하고;

(c) 그러한 프로그램들이 볼트 소유자에 의해서 그 볼트내에서의 동작을 위한 승인을 받도록 하며;

(d) 그러한 프로그램들이 부정한 변경 및 '트로잔 호스(Trojan horse)' 공격으로부터 보호되도록 서명되도록 한다.

볼트내에서 동작하는 프로그램들은 정보를 그 동일 볼트내에 기탁할 수 있거나 서로의 공용 키(public key)에 대해 안전하게 액세스하는 다른 볼트들내에 기탁할 수 있다. 통상, 이들 볼트는 동일 볼트 서버상에 위치할 것이나, 개인 키 정보의 제공을 위해 공공 인증 기관(Certificate Authority)에 대해 액세스하는 상이한 볼트 서버들상에 위치할 수도 있다. 볼트 보관소와 관련하여, '기탁'은 다른 것을 의미할 수도 있다. 한 구현예에서, 기탁은 데이터를 타겟 볼트의 암호 키로 암호화하고 그 데이터를 기탁 볼트의 서명키로 서명하는 것을 지칭할 수 있다. 볼트 프로그램은 암호 키 또는 서명키를 직접 액세스할 수는 없고, 이는 API를 통하여 이루어진다. 선택사양적으로, '기탁' 기능은 타겟 볼트에 포함된 큐(queue)내에 정보를 배치할 수 있다. 또 다른 선택사양은 그 정보가 기탁되었고 타겟 볼트내의 프로그램이 그 데이터를 열어 보았다는 것을 보증하는 '회신 접수증(return receipt)'을 제공한다. 이들 모든 '기탁' 기능은

(a) 그들의 원천(origin) 프로세스가 부인될 수 없게 하고;

(b) 그들의 내용이 프로세스간(inter-process) 통신 버퍼를 검사할 수 있는 자에게 보여질 수 없게 하며;

(c) 전달이 보장되도록

하는 방식으로 정보를 볼트들 사이에서 전달하는 수단을 제공한다.

애플리케이션이 타겟 볼트에 대한 데이터의 큐잉(queuing)을 선택하지 않으면, 그 애플리케이션은 정보를 파일 또는 데이터베이스내에 저장하는 것을 선택할 수 있거나 그 데이터를 '불투명한' 항목(opaque item)으로서 처리할 수 있는(예를 들면, 객체 항구성을 위해 데이터를 직렬화할 수 있는) 다른 시스템 서비스들을 사용하는 것을 선택할 수 있다. 이러한 불투명 정보는 백업 및 복구(backup and recovery)의 목적으로 표준 시스템 기술에 의해서 관리될 수 있으나, 그의 내용은 'SecureDepositor' 애플리케이션 프로그래밍 인터페이스를 이용하여 정보를 소유하는 볼트와 연관하여 동작하는 프로그램에 의해서 암호화될 수 밖에 없다.

IBM Vault Registry 제품을 이용하여 본 발명의 바람직한 실시예를 도 2에 개략적으로 예시한 바와 같이 개발했다.

도 1의 시스템에서와 마찬가지로 도 2에 도시된 구성에서는, 서류 발원자(200)가 서류 보관소 서비스(204)와의 접속 수단(202)을 통해 서류를 기탁할 수 있으며, 또한 기탁된 서류의 소유자로서 서류 발원자(200)가 그의 네트워크 접속 수단(208)을 통하여 서류 보관소 서비스(204)내에 저장된 서류에 대한 액세스를 획득한 사업 파트너와 같은 제 3 자에게 서류에 대한 액세스 레벨(level of access)을 할당할 수 있다. 그러나, 상술한 시스템과는 달리, 서류 보관소 시스템의 유저들은 제 3 자가 보관소내에 파일링된 서류의 완전성을 유지할 것인가를 염려해야만 할 필요가 없다.

본 발명의 바람직한 실시예의 서류 보관소 시스템(204)은 애플리케이션 서버(application server : AS)(210)와 볼트 제어기(214)라는 두가지 구성 요소를 포함한다. 애플리케이션 서버(210)는 데이터베이스 보관소(212)를 관장하는 프로그램으로서, 동일 머신(machine)상에 있을 수도 있고 또는 폐쇄 네트워크상에서 원격 배치될 수도 있다. 볼트 제어기(214)는 다수의 구성 요소, 즉 개개의 기준에 따라 서류 발원자(200)들 및 사업 파트너(206)들에게 할당되는 유저 볼트(216, 218), 애플리케이션 서버(210)에 할당되는 AS 볼트(220) 및 볼트 감독자 프로그램(222)을 포함한다.

유저 볼트(216 또는 218)는 적절한 인증 하에서 볼트를 할당받은 유저(서류 발원자(200) 또는 사업 파트너(206))에 의해서만 액세스될 수 있다. 개개의 볼트는 서류 데이터베이스(212)에 직접 액세스하지 못하며, AS 볼트(220) 및 애플리케이션 서버(210)를 통해 액세스된다.

애플리케이션 서버(210)는 신뢰성있는 컴퓨팅 베이스에서 구동하지 않고 플랫폼에서 실행될 수 있다. 애플리케이션 서버는 그에게 할당된 볼트 서버(214)내의 볼트 서버(214)에서 구동되는 교환 성분(reciprocating component)을 갖는다. AS 볼트(220)는 애플리케이션 서버와 통신할 수 있으며, 애플리케이션 서버를 통해 서류 데이터베이스(212)에 액세스된다.

도 3은 본 발명의 바람직한 실시예에 따른 서류 생성 프로세스를 설명하는 흐름도이다. IBM Vault Registry 환경을 이용하는 개인 볼트(personal vault)는 기호법적으로(notationally) 볼트 소유자 환경의 안전한 확장이다. 그래서, 도 3에서 도시한 프로세스 단계들간의 상호작용은 서류 발원자와 애플리케이션 서버의 볼트들 사이에서 이루어지는 것으로 예시된다.

데이터 보관소에서 서류를 생성할 때, 서류는 먼저 그 서류를 생성한 또는 발원한 유저의 데스크탑으로부터 유저(서류 발원자)의 개인 볼트로 보내지고(단계 300), 이곳에서 서류는 유저 볼트의 개인 서명키로 서명된다('signed')(단계 302).

데이터 요소의 전자 서명(electronic signature)은 그 데이터 요소의 완전성에 대한 보증서로서, 이 보증서는 서명에 의해 제공된다. 서명은 데이터 요소의 다이제스트(data element's digest)를 먼저 계산함으로써 산정될 수 있다. 다이제스트는 안전성을 보증하는 특수한 특성을 갖는 비교적 작은 구조(예로, MD2 또는 MD5 다이제스트의 경우 128 비트)이다. 먼저, 다이제스트는 일방향 함수인데, 이것은 다이제스트가 주어지면 그 다이제스트를 생성한 원래 서류를 획득하기가 불가능하고, 또한 다이제스트가 주어지면 동일한 다이제스트를 가지고 있었을 제 2의 이전 이미지(a second pre-image)를 찾기가 불가능(또는 계산적으로 실행 불가능)함을 의미한다. 다이제스트는 또한 내충돌성(collision-resistant)을 갖는데, 이는 두가지의 상이한 이전 이미지들에 의해 동일한 다이제스트가 생성될 가능성이 작음을 의미한다.

다음, 데이터 요소의 다이제스트는 유저 볼트 애플리케이션의 개인 서명키로 암호화된다(단계 304). 본 발명의 바람직한 실시예에서는 대칭적 암호화 기술 및 공용-키 비대칭적 암호화 기술(symmetric and public-key asymmetric cryptography technology) 두가지 모두가 이용된다.

공용키 암호화 기술에 따르면, 애플리케이션은 키 쌍(key pair)이라 지칭되는 두 개의 키 즉 공용키와 개인키를 갖는다. 공용키는 애플리케이션에 의해 지역적으로 보유되는 것으로서, 이하에서 보다 상세히 설명된다. 공용키는 통상 X.500 분산 디렉토리(distributed directory)와 같은 디렉토리 서비스를 통하여 모든 유저들에게 이용가능하게 된다. 공용키의 분산은 당해 기술 분야에서 잘 알려져 있으므로 본 명세서에서는 더 이상 상세하게 설명하지 않는다.

공용 키 암호화 기술이 사용될 때, 공용키로 암호화된 데이터 요소는 대응하는 개인키로만 암호해독될 뿐이다. 마찬가지로, 개인키로 암호화된 데이터 요소는 공용키로만 암호해독될 뿐이다.

대칭 키 기술에서, 암호화와 암호해독 양자에 대해 단일 키가 사용된다. 현실적으로, 암호화/암호해독 및 키 생성은 공용 키 비대칭적 기술보다 대칭적 키 기술이 훨씬 빠르다.

데이터는 통상 랜덤하게 생성된 대칭 키에 의해 암호화된다. 그 다음, 대칭 키 자체는 유저의 공용 암호키에 의해 암호화되고, 서류와 함께 저장되어 서류의 일부로 된다.

도 3을 계속하여 참조하면, 암호화된 서류와 전자 서명은 서류 데이터베이스내의 파일링을 위해 애플리케이션 서버의 볼트로 전달된다(단계 306). 암호화된 서류를 수신하면(단계 308), 애플리케이션 서버의 볼트에서 구동하는 애플리케이션은 자신이 소유하고 있는 개인 서명키에 의해 재서명함으로써 그 서명을 공증한다(단계 310).

서명 공증(the notarization of a signature)의 전자적인 면에서의 의미는 '공증인(notary)'으로서 작용하는 제 3 자가 서명의 내용을 인증하는 것이다. (본 명세서에서 '공증인' 및 '공증'을 언급하는 것에 의해, 정부 당국이 수여한 공증 사무소가 지키는 모든 의무를 망라하려고 하는 것은 아니다). 일반적으로, 서명의 전자적 공증은 나중에 서명의 불법적인 변형을 방지하기 위한 별도 예방 조치로서 이루어진다. 본 발명의 사례에 있어서, 유저의 디지털 서명에 대한 공증은 유저가 서류 보관소내에 저장된 원래의 서류를 교체 또는 변형시키는 것을 방지한다. 서류와 관련된 공증된 서명의 검사를 통해 어떠한 불일치를 알 수 있을 것이다.

공증된 전자 서명에는 두가지 정보 즉 소정 데이터 요소의 발원자 서명과 발원자 서명의 공증인 서명이 포함된다. 공증인의 서명은 발원자의 서명과 현재 타임 스탬프(time stamp)를 통해 계산되어야 한다.

그 다음, 애플리케이션 서버의 볼트에서 구동하는 애플리케이션은 수신된 서류에 서명한다(단계 312). 서류 발원자로부터 수신한 데이터가 암호화되기 때문에, 애플리케이션 서버는 실제로 서류의 내용을 알지 못한다. 그러므로, 본 발명에 따르면, 이러한 두 번째 서명은 암호화된 서류와 발원자의 공증된 서명을 통하여 계산된다. 애플리케이션 서버의 서명은 보관소 서비스가 서류를 수신했음을 서류 발원자(기탁자)에게 증명하는 불반려 접수증(non-repudiation receipt)을 구성한다. 보관소에서의 서류의 생성은 이때 보관소 서비스에 의해서 나중에 부인되지 않을 수도 있다.

암호화된 서류, 서류 발원자의 공증된 서명 및 불반려 접수증은 모두 애플리케이션 서버의 보관소 또는 애플리케이션 데이터베이스에 저장된다(단계 314). 불반려 접수증은 서류 발원자의 볼트로 전송된다(단계 316). 서류 발원자의 볼트는 암호화된 서류의 서명을 확인하는 것에 의해 불반려 접수증의 정확성을 검사한다(단계 318). 서류 발원자의 볼트는 또한 공증된 서명에서 타임 스탬프의 통용 기간을 검사한다(단계 320). 타임 스탬프의 허용 오차는 애플리케이션에 따라 다르다. 검사 결과가 부정적인 경우에는, 에러 메시지가 AS 볼트로 리턴되고(단계 322) 시스템내에 로깅된다. 그러나, 불반려 접수증이 정확하고 타임 스탬프가 통용 기간내의 것이면, 유저의 볼트에서 구동하는 애플리케이션은 불반려 접수증을 서류 발원자에게 리턴(return)시켜(단계 324), 서류가 보관소에 저장되었다는 사건 증명이 필요한 경우에 추후 참조될 수 있도록 지역적으로 저장되게 한다.

서류 발원자는 자신이 소유한 고유의 기술을 이용하여 서류에 서명하고/하거나 그 서류를 암호화한 다음에 서류 저장을 위해서 그 서류를 그의 볼트에 제공할 수도 있다. 그러나, 서류 보관소는 저장되는 서류의 내용에는 민감하지 않다. 그러므로, 암호화된 서류는 어떤 다른 서류가 처리되는 것처럼 유저의 볼트에 의해 재서명되고 재암호화될 것이다.

도 4는 본 발명의 바람직한 실시예에 따라 매 서류마다 서류 발원자에 의해 유지되고 있는 액세스 제어 리스트(access control list : ACL)라고 하는 소정 형태의 목록(manifest)하에서 권한을 부여받은 요청자(requester)가 서류를 검색할 수 있게 수행되는 단계들을 설명하는 흐름도이다. 도 3에서와 같이, 본 프로세스 단계들은 세 행위자, 즉 유저, 애플리케이션 및 요청자에 대해 각자의 볼트가 제각기의 작업 공간(work space)의 기호법적인 안전한 확장(notational secure extension)이라는 것에 근거해서 배분된다.

도 4a를 참조하면, 요청자는 자신의 볼트 애플리케이션에 대해 애플리케이션 서버 보관소로부터 서류를

검색하기 위한 요청을 전송하고(단계 400), 요청자의 볼트 애플리케이션은 그 서류에 대한 요청을 애플리케이션 서버 볼트로 전달한다(단계402).

애플리케이션 서버의 볼트 애플리케이션은 액세스 요청을 수신하고(단계 404), 암호화된 서류 및 발원자의 공증된 서명을 애플리케이션 데이터베이스로부터 검색한다(단계 406).

애플리케이션 서버의 볼트 애플리케이션은 암호화된 서류 및 공증된 서명을 서류 발원자의 볼트로 전송한다. 또한, 애플리케이션 서버의 볼트는 요청자 볼트의 정체(identity)를 발원자의 볼트로 전송한다(단계 408).

발원자의 볼트는 그 요청자가 서류를 검색할 권한을 부여 받았는 지를 검사한다(단계 412). 바람직한 실시예에 있어서, 서류 액세스 제어는 권한을 부여받은 엔티티에게만 서류 액세스를 국한하는데 사용되는 액세스 제어 리스트를 통해 가능하게 된다. 액세스 제어 리스트(ACL)는 서류와 연관되어 있으며, 도 5a 및 6과 관련하여 하기에서 설명되는 바와 같이 서류 발원자의 볼트에 저장되고 유지된다. ACL은 요청자가 서류 검색 요청을 전송하는 시점을 검사하여야 한다. 요청자는 액세스 권한을 부여받은 경우 서류의 복사본만을 받게 될 것이다.

본 발명의 바람직한 실시예에 따르면, 능력 리스트(capability list)는 요청자들이 액세스를 요청하기에 앞서 자신들의 서류에 대한 액세스를 확인할 수 있도록 하는데 사용될 수 있다. 능력 리스트는 특정 사용자가 액세스 특권을 가지고 있는 보관소내의 모든 서류를 식별한다. 요청자의 능력 리스트는 자기 소유의 볼트내에 저장되고 유지된다. 능력 리스트의 사용 및 유지에 대해서는 도 5b와 관련하여 더욱 상세히 후술한다.

요청자가 서류에 대한 액세스 권한을 부여받지 않았다면, 에러 메시지가 서류 발원자에게 리턴되고 시스템내에 로깅된다(단계 414).

도 4b를 계속하여 참조하면, 요청자가 서류를 수신할 권한을 부여받은 경우, 서류 발원자의 볼트 애플리케이션은 그 서류를 암호해독하고(단계 416) 공증된 서명을 확인한다(단계 418). 발원자의 원래 서명은 암호화되지 않은 서류 내용에 대하여 계산되었기 때문에, 그 서류 내용에 대해 액세스하는(즉, 서류 발원자의 개인키를 갖는) 자들만이 서명을 확인할 수 있다. 서류 발원자가 자기 소유의 파일에 가지고 있는 것과 서명이 일치하지 않으면, 기탁된 것과 동일 버전(version)의 서류가 아니라는 것이 분명할 것이고, 발원자는 에러 메시지를 애플리케이션 서버로 리턴할 것이다(단계 420).

서명이 확인되면, 발원자는 암호해독된 서류와 공증된 서명을 요청자의 볼트로 전달한다(단계 422).

암호해독된 서류를 수신하면, 요청자의 볼트 애플리케이션은 발원자의 공증된 서명을 확인하려 한다(단계 424). 요청자가그 서명을 확인할 수 없으면, 에러 메시지가 서류 발원자에게 리턴되고 시스템에 로깅된다(단계 426).

서류 발원자의 공증된 서명이 확인될 수 있으면, 요청자의 볼트는 서류와 함께 수신한 공증된 서명에 서명한다. 이 서명은 공증된 서명 및 현재 시간 스탬프에 대하여 계산되며, 요청자가 보관소로부터 서류를 검색하였음을 증명하는 불반려 접수증을 구성한다(단계 428). 요청자의 볼트는 암호해독된 서류를 불반려 접수증과 함께 요청자의 데스크탑으로 리턴한다(단계 430). 또한 요청자의 볼트는 불반려 접수증을 애플리케이션 서버의 볼트로 전달한다(단계 432). 애플리케이션 서버는 요청자 볼트의 서명을 수신시에 확인한다(단계 434). 서명이 확인될 수 없으면, 에러 메시지가 서류 발원자에게 리턴되며 시스템에 로깅된다(단계 436). 서명이 확인될 수 있으면, 요청자가 서류를 검색하였던 것을 애플리케이션 서버가 입증하여야 하는 경우 애플리케이션 서버 볼트는 접수증을 애플리케이션 데이터베이스에 차후의 사용을 위해서 저장한다(단계 438).

서류 검색을 위한 액세스 제어의 불변성(Immutability of Access Control for Document Retrieval)

상기 기술된 바와 같이, 데이터 보관소에서는 서류 액세스 제어에 필요한 요건이 있다. 이것은, 서류 소유자에 의해 권한을 부여받은 유저들만이 서류를 볼 수 있으며, 서류 액세스 허가는 서류 소유자(즉 서류 발원자)와 그 서류 소유자로부터 소정 서류의 액세스 제어 리스트를 변경하기 위한 권한을 부여받은 다른 유저들에 의해서만 변경될 수 있다는 것을 의미한다. 심지어는 보관소 관리자라도 서류 소유자로부터 권한을 부여받지 않고서는 서류 액세스 허가를 변경할 권한(the power)이 없다는 확신을 갖는 것이 중요하다.

서류 액세스 제어의 불변성에 대해서는 상이한 두가지 형태의 애플리케이션 요건이 있다. 서류 액세스는 다음과 같은 경우, 즉

(1) 유저가 열람 권한이 부여된 모든 서류를 찾고자 탐색(search)을 실행할 때;

(2) 유저가 서류의 실제 검색(retrieval)을 실행할 때

검사되어야 한다.

모든 애플리케이션은 서류 검색에 대해 액세스 제어(상기 액세스 타입 2)를 시행하여야 한다. 이러한 유형의 액세스 경우, 보관소는 서류 액세스 제어가 사업 경쟁자와 같은 권한을 부여받지 않은 유저에 의해 변경될 가능성이 없다는 것을 보장하여야 한다.

그러나, 몇몇 응용예에 있어서는, 유저가 열람 권한이 부여된 모든 서류에 대해 서류 보관소에 문의(query)할 수 있도록 하는 것이 필수적인 것은 아니다. 예를 들면, 이러한 지식은 사업 회의를 통해 또는 전화를 통해 오프-라인으로 통신될 수도 있다. 그 경우, 유저는 어떤 서류를 액세스할 것인 지를 알고 있으므로 요청자 자신의 서류 액세스에 관한 지식은 보관소의 행위로 인하여 영향받지 않을 수 있다.

서류 검색시에만 액세스 제어의 불변성을 시행하고 서류 검색시에는 시행하지 않는 시스템은 본 출원과

동일자로 출원된 'System for Electronic Repository of data Enforcing Access Control on Data Retrieval' (IBM Docket No. CA998-030)이라는 출원의 주제이다. 이 시스템에서, 액세스 제어 정보는 애플리케이션 서버의 데이터베이스/보관소에 저장된다.

유저들이 그들의 서류 액세스에 관한 독립적인 정보를 가지고 있지 않은 경우에 사용될 수도 있는 한층 강화된 형태의 액세스 제어 불변성은 서류 탐색과 서류 검색 양자에 관련된다. 이러한 요건 때문에, 액세스 제어 정보는 애플리케이션 데이터베이스에 저장될 수 없고, 그 대신에 서류 소유자의 볼트에 저장된다. 이러한 본 발명의 주제는 도 5 및 도 6의 흐름도를 참조하여 상세하게 설명된다.

본 발명의 바람직한 실시예에서, 각각의 서류에는 액세스 제어 리스트(ACL)가 연관되는데, 이 액세스 제어 리스트는 여러 다른 유저들의 서류 액세스 권한을 식별한다. 또한, 시스템에서 각각의 유저는 능력 리스트(capability list)를 가지고 있는데, 이 능력 리스트는 유저가 소유하고 있지는 않지만 액세스되는 모든 저장된 서류를 식별한다.

불변성 보장을 위하여, 각각의 ACL은 도 5a에 예시된 바와 같은 서류 소유자의 볼트에서 처리되며, 이와 병행하여, 각각의 능력 리스트는 도 5b에 예시된 바와 같은 연관된 유저의 볼트에서 처리된다.

도 5a를 참조하면, ACL이 갱신될 때마다(단계 500), 서류 소유자의 볼트는 유저들이 그 변경에 의해 영향을 받았는 지를 판단하고(단계 502), 액세스의 변경(액세스 추가, 확장 또는 제한)의 유형을 식별하는 메시지는 서류 액세스가 변경된 각각의 유저의 볼트내에 기탁된다(단계 504).

각각의 ACL은 그의 최종 변경의 타임 스탬프 및 버전 번호와 관련된다. 그래서, 서류 소유자의 볼트는 ACL의 버전 번호를 증가시키고(단계 506), 그와 연관된 이전 타임 스탬프를 가장 최근의 타임 스탬프로 대체한다(단계 508). ACL의 불변성을 보장하기 위한 토큰(token)은 ACL과 연관된 현재 버전 번호 및 타임 스탬프로부터 생성되어 서류 발원자의 볼트에 의해 서명된다(단계 510). 또한 ACL은 서류 발원자의 볼트에 의해서도 서명된다(단계 512).

그 다음, ACL 토큰은 서류에 대한 액세스 권한을 부여받은 유저의 볼트로 전달되어, 차후의 ACL 확인을 위해 유저의 데스크탑상에 유저의 액세스 애플리케이션과 함께 저장된다(단계 514). 서명된 토큰은 서류 발원자의 데스크탑으로 전달되어 저장된다(단계 516). 서류 발원자는, 서명된 토큰의 복사본을 보유하고 있기 때문에, 서류 ACL이 갱신되었는지 갱신되지 않았는 지의 여부에 관한 최종 중재자(final arbiter)로 된다.

사업 파트너가 서류 검색을 원할 때, (도 4a의 단계 408에서) 상술한 바와 같이 AS 볼트 애플리케이션은 암호화된 서류를 서류 발원자의 볼트로 전송한다. 요청자의 권한을 확인(도 4a의 단계 412)하기 위하여, 서류 발원자의 볼트는 지역적으로 저장되어 있는 확인된 ACL에서 요청자가 지시된 서류에 대해 액세스하고 있는 지를 검사한다. 이러한 기술에 따르면, 서류 발원자의 볼트에 의해 변경이 검출되지 않는 한, 어느 누구도 애플리케이션 데이터베이스에 저장된 ACL을 변경할 수 없다.

상기 기술한 바와 같이, 보관소내의 서류를 소유하는 각각의 유저는 자신의 데스크탑에 각 ACL의 정확한 버전의 서명된 토큰을 가지고 있다. 유저의 볼트가 가지고 있는 ACL 버전은 유저의 데스크탑에 저장된 서명된 토큰을 유저의 볼트에 저장된 토큰과 비교함으로써 확인된다. 이러한 비교는 여러 다른 시점에서 실행될 수 있으며, 유저의 볼트내에 저장된 ACL을 확인하는 한가지 좋은 기회는 로그온을 행하는 기간 동안이므로, 유저가 로그온을 행할 때마다 유저의 ACL이 확인될 수 있다.

ACL 확인에 실패하면, 유저의 볼트 애플리케이션은 ACL에 의해 보호되는 서류를 검색하고자 하는 모든 요청을 자동적으로 중단할 수 있다. 이러한 서류 액세스 불가능 상태는 유저가 새로운 ACL을 생성하던가 기존의 ACL을 재인증할 때까지 지속된다. 기존 ACL의 재인증 프로세스는 유저의 볼트에 저장된 ACL 토큰을 유저의 데스크탑에 저장된 토큰과 동기화시키는 것을 포함한다.

ACL이 갱신될 때마다, 도 5a에서 설명한 단계들과 병행하여 많은 단계가 수행된다. 이러한 단계들은 도 5b에서 설명된다.

각 유저의 볼트는 유저가 액세스하는 모든 서류의 리스트를 포함하고 있는 능력 리스트의 유지를 담당한다. 능력 리스트 자체의 통용 기간은 버전 번호와 최종 타임 스탬프에 의해 식별된다. 유저의 서류 액세스 능력 변경(서류 ACL의 갱신)을 나타내는 메시지가 유저의 볼트에 도달할 때(단계 520), 유저 볼트내의 능력 리스트가 버전 번호에 의해 자동으로 갱신되고(단계 522) 최종 타임 스탬프에 의해 자동 갱신된다(단계 524). 토큰은 능력 리스트의 정확성을 확인하는데 사용될 수 있는 버전 번호와 타임 스탬프에 대하여 계산된다. 토큰은 유저의 볼트에 의해 서명되며(단계 528), 마찬가지로 능력 리스트도 서명된다(단계 530). 서명된 토큰과 능력 리스트는 둘다 유저의 볼트에 저장되지만(단계 532), 유저의 볼트는 이전(old) 능력 리스트 및 그와 연관된 토큰을 보존하는데 이는 이전 능력 리스트에 대한 토큰이 갱신이 이루어질 때까지는 유저의 데스크탑에 저장된 토큰에 상응하기 때문이다.

현재(current) 능력 리스트를 그에 대응하는 데스크탑에 저장된 유저 토큰과 동기화시키는 한가지 방법은 유저가 로그온할 때(단계 532) 자동으로 동기화시키는 것이다. 유저의 데스크탑에 저장된 토큰의 정확성은 유저의 볼트에 보존된 이전 토큰에 대해 그 다음에는 유저의 데스크탑으로 전송된 갱신된 토큰에 대해 검사될 수 있다(단계 534). 일단 이전 토큰이 유저의 볼트에서 교체되면, 이전 능력 리스트 및 그와 연관된 토큰은 유저의 볼트에서 제거될 수 있다.

유저의 데스크탑에 저장된 능력 리스트를 갱신하는 다른 대안(도시 안됨)은 유저가 그의 마지막 로그온 이후에 능력 리스트에 대한 갱신을 솔선해서 검토하게 하도록 하는 것이다.

ACL과 능력 리스트간의 확실한 일치를 위해, 시스템이 근간으로 하는 환경(예를 들면, IBM Vault Registry 제품)은 하나의 볼트에서 다른 볼트로 기탁되는 메시지의 전달을 보장하여야 한다. 능력 갱신의 전달은 또한 애플리케이션에 의해 예를 들면 갱신을 수신하는 유저로부터 접수증을 요청하는 것에 의해 보장될 수 있다.

이러한 구조의 결과로써, ACL과 능력 리스트는 모두 그들의 소유자에 의해 저장된다. 시스템내의 그 어떤

것도 서류 소유자가 알지 못하는 상태에서 서류의 액세스 제어 리스트를 변경시킬 수는 없다. 또한, 시스템내의 그 어느 것도 권한을 부여받은 유저가 알지 못하는 상태에서 서류 액세스에 관한 유저의 지식(즉 가능)을 변경할 수 없다.

애플리케이션 서버의 볼트에 의해 탐색이 이루어지는 전술한 관련 출원에 개시된 액세스 제어 구조와는 대조적으로, 본 발명의 경우, 유저가 액세스 권한을 부여받은 서류에 대한 탐색은 유저 소유의 볼트 애플리케이션에 의해 이루어진다.

소유권자 특권의 할당(Assignment of Ownership Privileges)

어떤 환경들에서는 서류 소유자가 다른 누구에게 소정 서류의 액세스 리스트를 변경할 수 있도록 하는 것이 필요하다. 예를 들면, 소유자가 유효하지 않은 경우에는, 권한을 부여받은 다른 유저가 소정 서류의 액세스 제어를 갱신할 수 있는 능력을 가질 것이다.

본 발명의 바람직한 실시예에 따르면, ACL 또는 능력 리스트의 갱신은 도 6에서 설명되는 단계들에 따라 시스템내의 다른 유저들에 의해 실행될 수 있다.

예를 들면, ACL 갱신이 시도될 때, 그 갱신을 행하고자 하는 유저는 최근에 서명된 ACL의 토큰을 제시할 수 있어야 한다(단계 600). 서명된 토큰은 유저 소유의 볼트로 전달되고(단계 602), 유저 소유의 볼트는 서명된 토큰을 서류 발원자의 볼트로 전달한다(단계 604). 갱신 유저가 이 서류의 ACL내에 할당된 소유권자 특권을 가지고 있지 않다면, 서류 소유자의 볼트는 그것을 검출하여, 갱신을 거절하고 에러 메시지를 유저의 볼트로 리턴시킬 것이다(단계 606, 608).

서류 발원자의 볼트가 서명 유저의 서류 액세스를 확인할 수 있고 또한 버전 번호 및 ACL 토큰의 타임 스탬프가 현재의 것임을 확인할 수 있으면(단계 606), ACL은 갱신되고(단계 610), 새로운 토큰이 생성되어 서명되며(단계 612), 발원자의 볼트에 저장된다(단계 614). 새로이 서명된 토큰은 갱신자의 볼트로 전송된다(단계 616). 갱신자의 볼트는 새로운 토큰의 저장을 위해 그 새로운 토큰을 갱신자의 데스크탑으로 리턴시킨다(단계 618). 새로이 서명된 토큰은 또한 선택사양적으로 보관소내의 저장을 위하여 애플리케이션 서버의 볼트로 전달될 수도 있다(단계 620).

이러한 절차에서는 어느 주어진 시점에서 단 한 사람만이 ACL 갱신을 실행해야 할 것을 필요로 한다. 예를 들면, 서류 소유자인 존이라는 사람이 휴가를 떠나려 할 때, 그는 그가 없는 동안 동료인 메리에게 서류의 ACL에 대한 자신의 최근 토큰을 부여함으로써 서류의 ACL을 갱신하게 할 수 있다. 그러면, 메리는 그녀의 볼트를 통하여 존의 볼트에 대해 토큰을 제시함으로써 ACL의 갱신을 행한다. 메리는 ACL에 대한 새로이 서명된 토큰을 수령하고, 그녀는 존이 회사에 복귀할 때 존에게 돌려준다. 존은, 새로운 토큰을 인스톨한 후, 그 자신의 ACL을 갱신할 수 있다.

데이터 백업 및 복구(Data Backup and Recovery)

경우에 따라서는, 서류 보관소의 관리자는 서류 데이터베이스를 이전 백업으로부터 복원(restore)시켜야만 할 수도 있다. 이것은, 예를 들면, 디스크 크래시(disk crash)와 같은 파멸적인 데이터베이스 고장의 경우에 필요할 수도 있다.

백업에 포함될 필요가 있는 데이터는 서류 그 자체와, (애플리케이션 데이터베이스에 저장되어 있든 또는 소유자의 볼트에 저장되어 있든) ACL과, (상술한 바와 같이 그들을 구현하는 시스템에 대한) 능력 리스트와, ACL 및 능력 리스트의 확인 토큰(verification token)이다.

데이터 복원에 따라 가장 최근의 백업 후에 이루어진 갱신이 손실될 수 있다. 본 발명의 목적상, 그러한 갱신에는 ACL 갱신과 능력 리스트 갱신이 포함될 수도 있다. 이러한 일이 발생할 때, 유저의 데스크탑에 저장된 확인 토큰이 대응하는 볼트들내의 토큰과 일치하지 않아 유저들의 타당한 액세스가 거부될 수도 있다.

그러므로, 다음의 시스템은 여러 다른 상황에서 데이터 복원의 표준을 제공하도록 구현되었다. 백업은 TIME1에서 취해지고 복원은 그 이후의 TIME2에서 일어난 것으로 가정한다.

서류 데이터베이스, ACL, 능력 리스트 및 볼트내에 저장된 대응하는 토큰들의 완전한 데이터 복원이 실행되는 경우, TIME1 이전에 서류 액세스 권한을 부여받은 유저들은 또한 TIME2 이후에 서류를 액세스할 수 있다. 이것은 유저가 TIME1 이전에 권한을 부여받았으나 그 권한이 TIME1 이후 TIME2 이전에 취소된 경우에 유저는 서류 소유자가 ACL 토큰을 검사할 때까지 서류를 액세스할 것임을 의미한다. 그러므로 모든 유저들은 완전한 데이터 복원 이후 ACL 및 능력 리스트를 검사하여야 한다.

서류 데이터베이스만이 복원되었고 ACL, 능력 리스트 및 볼트내에 저장된 토큰들이 그대로인 경우, 유저들은 그들에게 데이터베이스에 존재하지 않는 서류를 액세스하기 위한 권한이 부여 된 사실을 알 수 있는데, 이것은 그 서류가 TIME1 이후에 추가되었지만 이후 데이터베이스 복구시에 손실되었기 때문이다. 모든 토큰들은 최근 것이기 때문에, 예외적인 일은 발생하지 않을 것이다.

또 다른 사례는 능력 리스트들이 사용되지 않으나 ACL들이 애플리케이션 데이터베이스에 저장되는 시스템에 관련된다. 서류 데이터베이스와 ACL은 복원되었으나 볼트에 저장된 토큰들은 그러하지 않은 경우, 유저는 TIME1 이후에 변경된 ACL을 갖는 모든 서류를 액세스할 수 없다는 것을 알게 될 것이다. 이것은 애플리케이션 데이터베이스내의 ACL 토큰들이 개개 소유자들의 볼트에 저장된 토큰들과 일치하지 않기 때문이다. 이를 처리하기 위해서는 모든 서류 소유자들이 ACL을 갱신하여야 할 것인데, 이를 행하기 위한 한 가지 방법은 관리자가 (TIME1 때 실제로 있었던) 구(old) ACL을 서류 소유자들에게 보내어 그들 소유자가 그들의 볼트내의 대응하는 토큰들을 다시 인스톨하도록 하는 것이다. 이러한 갱신은 자동적이 아니라 수동적일 것이며, 소유자의 서류는 소유자가 갱신을 실행할 까지 액세스 불가능하다.

데이터베이스 불일치를 피할 수 없는 상황인 경우, 보관소 관리자는 서류 발원자가 교정 조치를 행할 때까지 복원 이후의 모든 서류에 대한 액세스를 불가능하게 할 수도 있다. 이와 같이 액세스를 불가능하게 하는 것은 보관소에 저장된 모든 서류에 적용될 수도 있고 또는 불일치가 가장 중요한 서류의 일부(subset)에 대해서만 적용될 수도 있다. 이 경우에 있어서, 보관소 관리자는 시스템의 불일치를 보존하려는 의지가 있어야 한다. 그러나, 상술한 바와 같이, 어떤 경우의 관리자는 유저의 서류 액세스를 승인 또는 취소하기 위한 권한을 갖지 못한다.

IBM Vault Registry 제품으로 구현된 본 발명의 바람직한 실시예를 설명하였으나, 당업자라면 명백히 알 수 있듯이, 본 발명을 각 유저의 데스크탑과 함께 지역적으로 배치된 안전한 볼트형 환경과 같은 유사한 기능을 제공하는 다른 제품을 이용하여 구현할 수도 있다. 당업자에게 자명한 이러한 특성과 다른 특성의 변경은 첨부된 특허청구범위에 의해 포괄하고자 한다.

발명의 효과

본 발명에 의하면, 제 3 자에 의해 관리되는 보관소(repository)내에 서류가 물리적으로 저장되어 있지만 유저가 그 보관소내의 어떤 서류에 액세스가능한 지의 판단을 위해 탐색할 수 있게 하며, 또한 보관소에 저장된 데이터에 대한 액세스 권한을 부여받은 유저의 액세스 관련 정보에 대한 완전성 및 액세스가 시스템을 통해 유효하나 제 3 자 보관소 관리자의 행위에는 무관하게 한다.

(57) 청구의 범위

청구항 1

데이터 보관소 시스템(a data repository system)에 저장된 전자 데이터 파일을 탐색하는(searching) 안전 시스템(a secure system)에 있어서,

① 상기 데이터 보관소 시스템내 전자 데이터 파일의 기탁자 컴퓨터(depositor computer)용 제 1 에이전트 프로그램(agent program) 및 상기 전자 데이터 파일에 대한 액세스 특권(access privileges)을 갖는 제 1 유저 컴퓨터(user computer)용 제 2 에이전트 프로그램을 수용하는 통신 환경(a communication environment)과,

② 상기 전자 데이터 파일의 액세스 제어를 수록한 상기 전자 데이터 파일용 목록(a manifest) ― 이 목록은 상기 제 1 에이전트 프로그램에 대해 액세스 가능하고 상기 제 1 에이전트 프로그램에 의해 유지됨 ― 과,

③ 상기 전자 데이터 파일에 대한 상기 제 1 유저 컴퓨터의 액세스 특권에 관한 제 1 기록(a first record) ― 이 제 1 기록은 상기 제 2 에이전트 프로그램에 대해 액세스 가능하고 상기 제 2 에이전트 프로그램에 의해 유지됨 ― 과,

④ 상기 전자 데이터 파일에 대한 상기 제 1 유저 컴퓨터의 액세스 특권에 영향을 미치는 상기 목록의 변경을 상기 제 1 에이전트 프로그램으로부터 상기 제 2 에이전트 프로그램으로 전달하여 상기 제 1 기록을 갱신하기 위한 수단,

⑤ 상기 전자 데이터 파일이 상기 제 2 에이전트 프로그램으로 전달되기 전에 상기 제 1 에이전트 프로그램이 상기 전자 데이터 파일에 대한 상기 제 1 유저 컴퓨터의 액세스 특권을 확인하게 하는 수단

을 포함하는 데이터 보관 시스템에 저장된 전자 데이터 파일을 탐색하는 안전 시스템.

청구항 2

제 1 항에 있어서,

상기 제 1 에이전트 프로그램은 상기 기탁자 컴퓨터의 안전한 확장(a secure extension)이며, 상기 제 2 에이전트 프로그램은 상기 제 1 유저 컴퓨터의 안전한 확장인

데이터 보관 시스템에 저장된 전자 데이터 파일을 탐색하는 안전 시스템.

청구항 3

제 2 항에 있어서,

상기 전자 데이터 파일에 대한 상기 제 1 유저 컴퓨터의 액세스 특권에 영향을 미치는 상기 목록의 변경을 상기 제 2 에이전트 프로그램으로부터 상기 제 1 에이전트 프로그램으로 전달하기 위한 수단을 더 포함하는

데이터 보관 시스템에 저장된 전자 데이터 파일을 탐색하는 안전 시스템.

청구항 4

제 1 항 또는 제 2 항에 있어서,

상기 전자 데이터 파일에 대한 액세스 특권을 갖는 제 2 유저 컴퓨터용 제 3 에이전트 프로그램과,

상기 전자 데이터 파일에 대한 상기 제 2 유저 컴퓨터의 액세스 특권에 관한 제 2 기록 - 이 제 2 기록은 상기 제 3 에이전트 프로그램에 대해 액세스 가능하고 상기 제 3 에이전트 프로그램에 의해 보유됨 -

을 더 포함하며, 상기 전자 데이터 파일에 대한 상기 제 1 유저 컴퓨터의 액세스 특권에 영향을 미치는 상기 목록의 변경을 상기 제 1 에이전트 프로그램으로부터 상기 제 2 에이전트 프로그램으로 전달하여 상기 제 1 기록을 갱신하기 위한 수단은 상기 전자 데이터 파일에 대한 상기 제 2 유저 컴퓨터의 액세스 특권에 영향을 미치는 상기 목록의 변경을 상기 제 1 에이전트 프로그램으로부터 상기 제 3 에이전트 프로그램에 전달하여 상기 제 2 기록을 갱신하기 위한 수단을 포함하며, 상기 전자 데이터 파일이 상기 제 2 에이전트 프로그램으로 전달되기 전에 상기 제 1 에이전트 프로그램이 상기 전자 데이터 파일에 대한 상기 제 1 유저 컴퓨터의 액세스 특권을 확인하게 하는 수단은 상기 전자 데이터 파일이 상기 제 3 에이전트 프로그램에 전달되기 전에 상기 제 1 에이전트 프로그램이 상기 전자 데이터 파일에 대한 상기 제 2 유저 컴퓨터의 액세스 특권을 확인하게 하는 수단을 포함하는

데이터 보관 시스템에 저장된 전자 데이터 파일을 탐색하는 안전 시스템.

청구항 5

제 4 항에 있어서,

상기 제 3 에이전트 프로그램은 상기 제 2 유저 컴퓨터의 안전한 확장인

데이터 보관 시스템에 저장된 전자 데이터 파일을 탐색하는 안전 시스템.

청구항 6

제 5 항에 있어서,

상기 전자 데이터 파일에 대한 상기 제 2 유저 컴퓨터의 액세스 특권에 영향을 미치는 상기 목록의 변경을 상기 제 3 에이전트 프로그램으로부터 상기 제 2 에이전트 프로그램으로 전달하기 위한 수단을 더 포함하는

데이터 보관 시스템에 저장된 전자 데이터 파일을 탐색하는 안전 시스템.

청구항 7

제 2 항 또는 제 5 항에 있어서,

상기 통신 환경은 서버를 포함하는

데이터 보관 시스템에 저장된 전자 데이터 파일을 탐색하는 안전 시스템.

청구항 8

제 1, 2 또는 5 항에 있어서,

상기 안전 시스템은 상기 통신 환경내에 수용된 상기 데이터 보관소 시스템에 대한 인터페이스를 더 포함하며, 상기 인터페이스는 상기 데이터 보관소 시스템 및 상기 에이전트 프로그램들로의 또한 상기 데이터 보관소 시스템 및 상기 에이전트 프로그램들로부터의 모든 통신을 수신하는데 적합한

데이터 보관 시스템에 저장된 전자 데이터 파일을 탐색하는 안전 시스템.

청구항 9

제 8 항에 있어서,

상기 인터페이스는 상기 데이터 보관소 시스템의 안전한 확장인

데이터 보관 시스템에 저장된 전자 데이터 파일을 탐색하는 안전 시스템.

청구항 10

전자 데이터 보관소용의 안전한 전자 데이터 탐색 시스템(a secure electronic data search system for an electronic data repository) - 이 시스템은 상기 데이터 보관소에 저장된 각각의 전자 데이터 파일에 대한 액세스 제어를 수록한 목록과 상기 보관소에 저장된 전자 데이터에 대해 액세스하는 각 컴퓨터의 서류 액세스 특권을 수록한 기록을 가짐 - 을 유지하는 방법에 있어서,

① 상기 보관소에 저장된 전자 데이터 파일의 목록을 갱신하는 단계와,

② 상기 갱신에 의해 상기 전자 데이터 파일에 대한 액세스의 변경이 영향을 받는 모든 컴퓨터를 확인하는 단계와,

③ 상기 액세스의 변경을 상기 영향을 받은 모든 컴퓨터에 전달하는 단계와,

④ 상기 영향을 받은 모든 컴퓨터의 상기 액세스 특권 기록을 갱신하는 단계와,

⑤ 상기 갱신된 액세스 특권 기록을 상기 영향을 받은 컴퓨터들에 전달하는 단계

를 포함하는 전자 데이터 보관소의 안전 전자 데이터 탐색 시스템을 유지하는 방법.

청구항 11

데이터 보관소 시스템에 저장된 전자 데이터 파일을 탐색하기 위한 안전 시스템에 있어서,

① 상기 데이터 보관소 시스템에 저장된 각각의 전자 데이터 파일에 대한 액세스 제어를 수록한 목록을 유지하는 수단과,

② 각각의 상기 목록에 대한 액세스를 기탁 특권을 갖는 컴퓨터로 제한하는 수단과,

③ 상기 데이터 보관소 시스템에 저장되어 있는 적어도 하나의 전자 데이터 파일에 대한 액세스 특권을 가진 각각의 컴퓨터와 연관된 상기 전자 데이터 파일에 대한 액세스 특권을 수록한 기록을 유지하는 수단과,

④ 각각의 상기 기록에 대한 액세스를 상기 액세스 특권을 가진 상기 연관된 컴퓨터로 제한하는 수단과,

⑤ 목록내의 액세스 변경에 의해 영향을 받은 각각의 컴퓨터와 연관된 상기 기록을 갱신하는 수단

을 포함하는 안전 시스템.

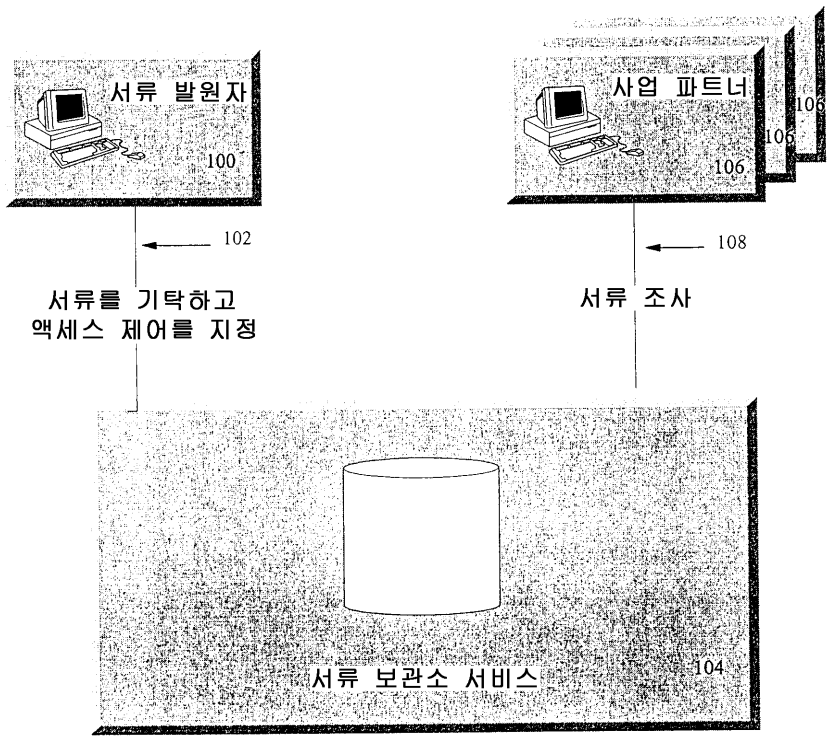
청구항 12

제 10 항의 방법을 컴퓨터에서 실행하는데 사용하기 위한 명령(instruction)들을 저장하는 컴퓨터 판독 가능 메모리.

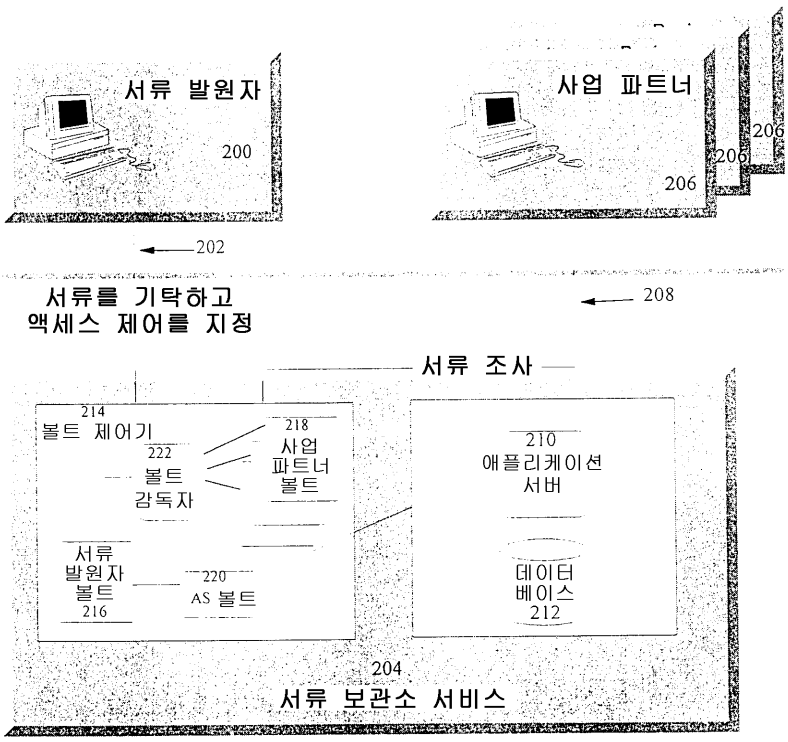
도면

도면1

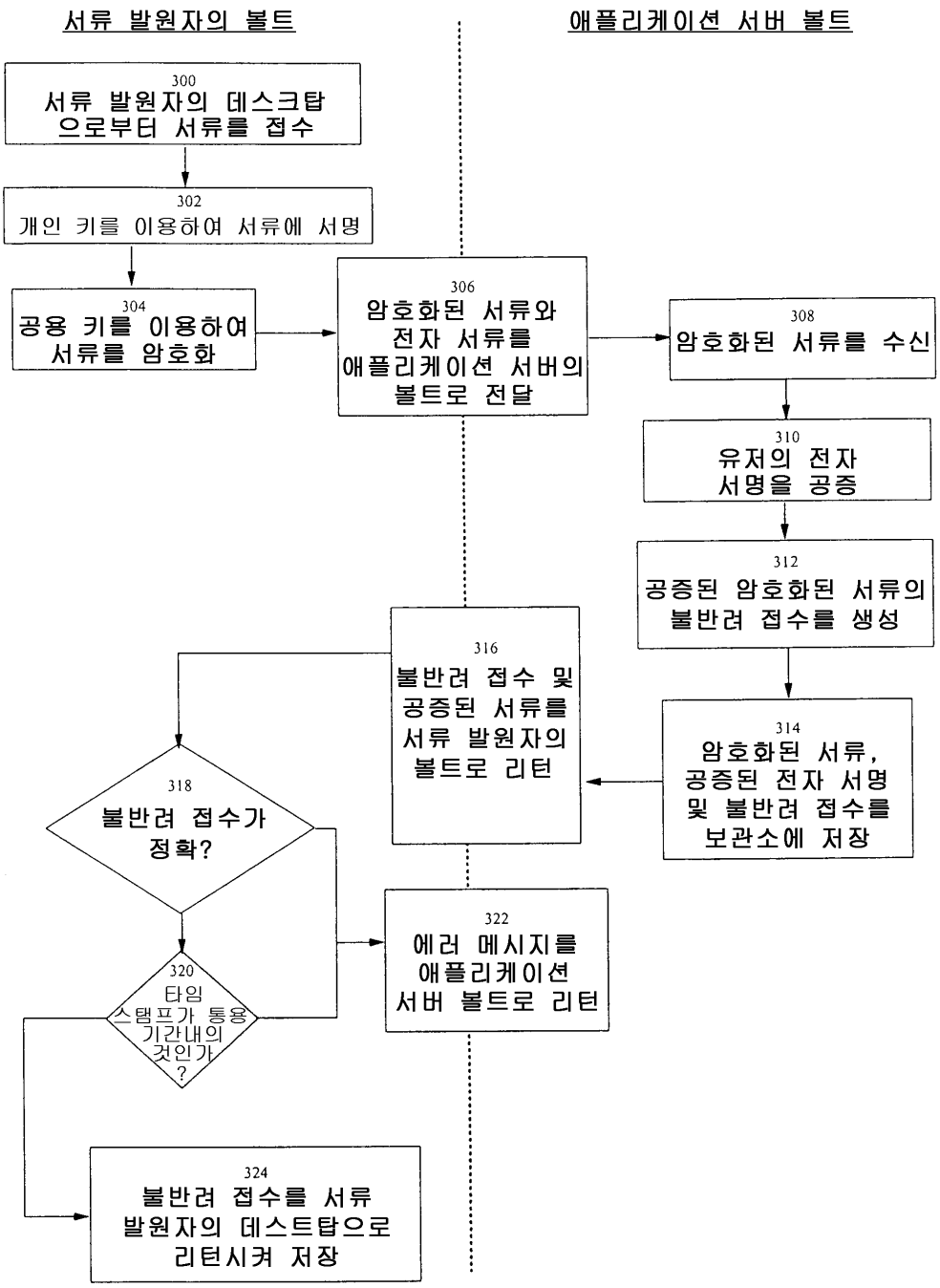
(종래기술)



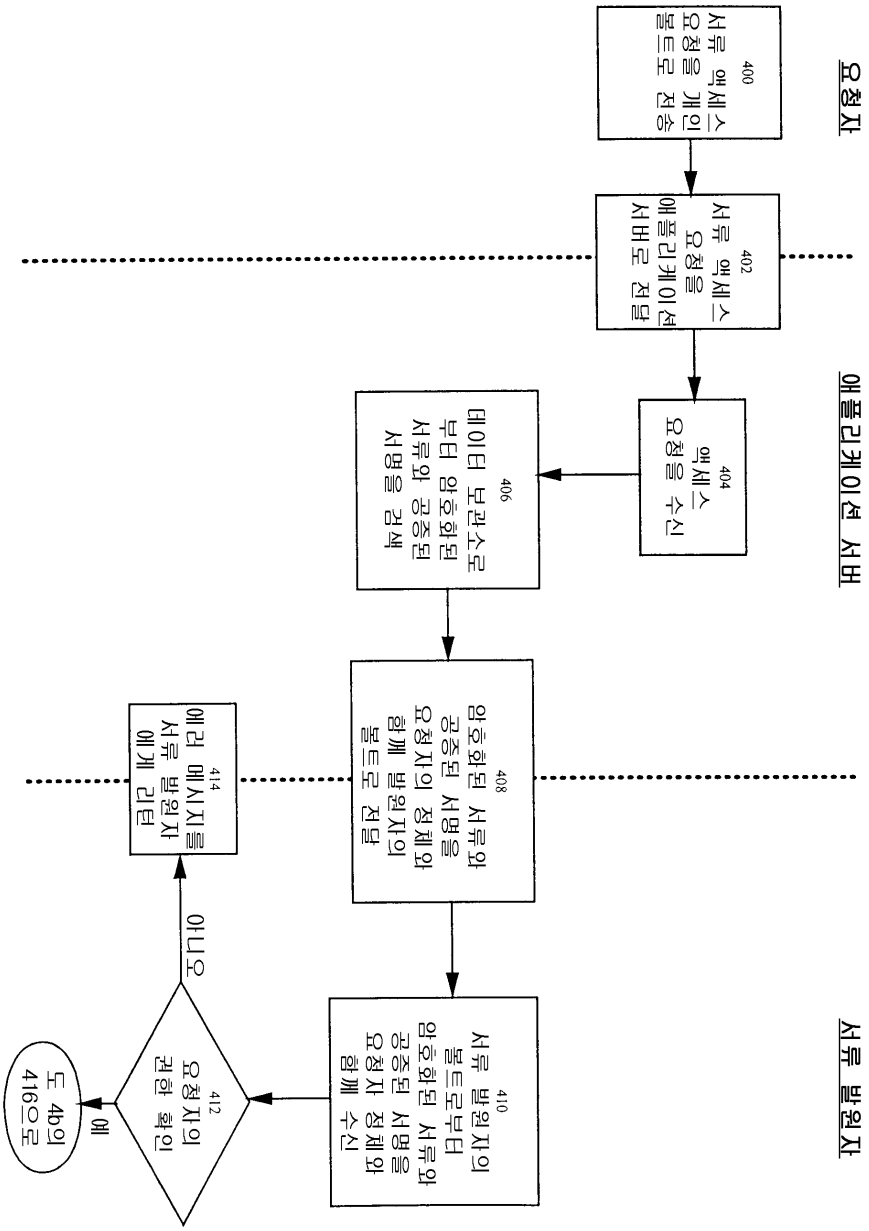
도면2


서류 발원자
200
사업 파트너
206
206
206
202
208
서류를 기탁하고
액세스 제어를 지정
서류 조사
214
볼트 제어기
222
볼트
감독자
218
사업
파트너
볼트
서류
발원자
볼트
216
220
AS 볼트
210
애플리케이션
서버
데이터
베이스
212
204
서류 보관소 서비스

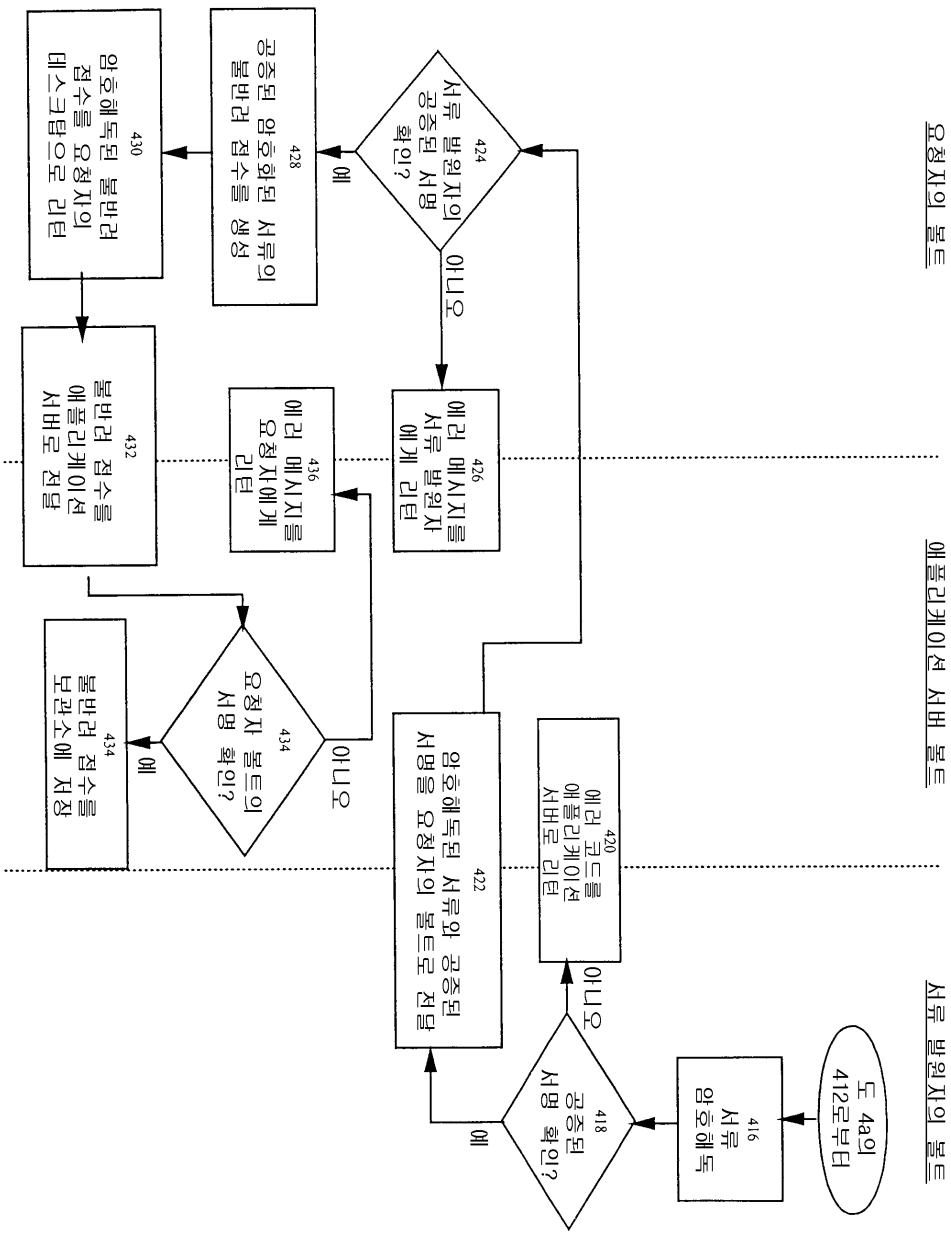
도면3


서류 발원자의 볼트
애플리케이션 서버 볼트
300
서류 발원자의 데스크탑 으로부터 서류를 접수
302
개인 키를 이용하여 서류에 서명
304
공용 키를 이용하여 서류를 암호화
306
암호화된 서류와 전자 서류를 애플리케이션 서버의 볼트로 전달
308
암호화된 서류를 수신
310
유저의 전자 서명을 공증
312
공증된 암호화된 서류의 볼반려 접수를 생성
314
암호화된 서류, 공증된 전자 서명 및 볼반려 접수를 보관소에 저장
316
볼반려 접수 및 공증된 서류를 서류 발원자의 볼트로 리턴
318
볼반려 접수가 정확?
320
타임 스탬프가 통용 기간내의 것인가 ?
322
에러 메시지를 애플리케이션 서버 볼트로 리턴
324
볼반려 접수를 서류 발원자의 데스트탑으로 리턴시켜 저장

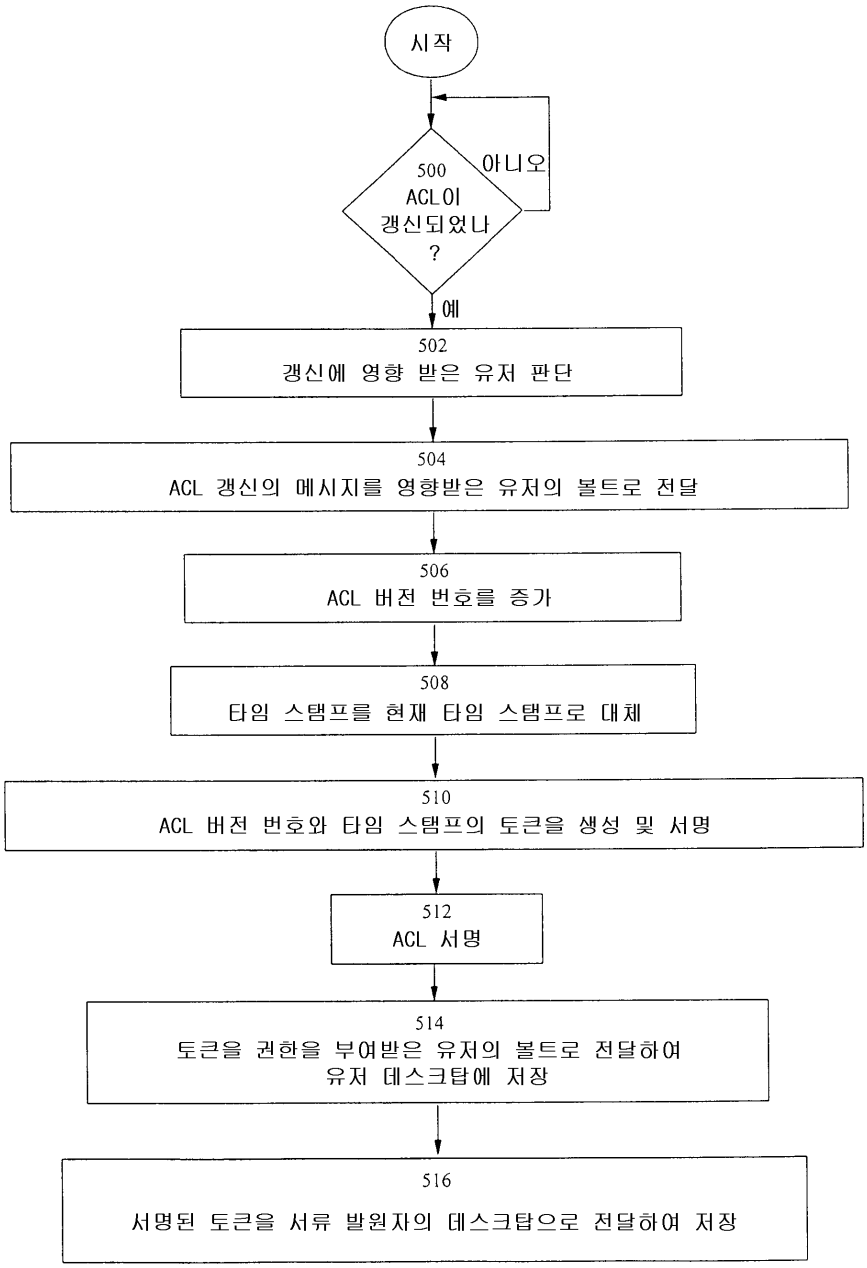
도면4a


요청자
애플리케이션 서버
서류 발원자
400 서류 액세스 요청을 개인 볼트로 전송
402 서류 액세스 요청을 애플리케이션 서버로 전달
404 액세스 요청을 수신
406 데이터 보관소로부터 암호화된 서류와 공증된 서명을 검색
408 암호화된 서류와 공증된 서명을 요청자의 정체와 함께 발원자의 볼트로 전달
410 서류 발원자의 볼트로부터 암호화된 서류와 공증된 서명을 요청자 정체와 함께 수신
412 요청자의 권한 확인
아니오
414 에러 메시지를 서류 발원자에게 리턴
예
도 4b의 416으로

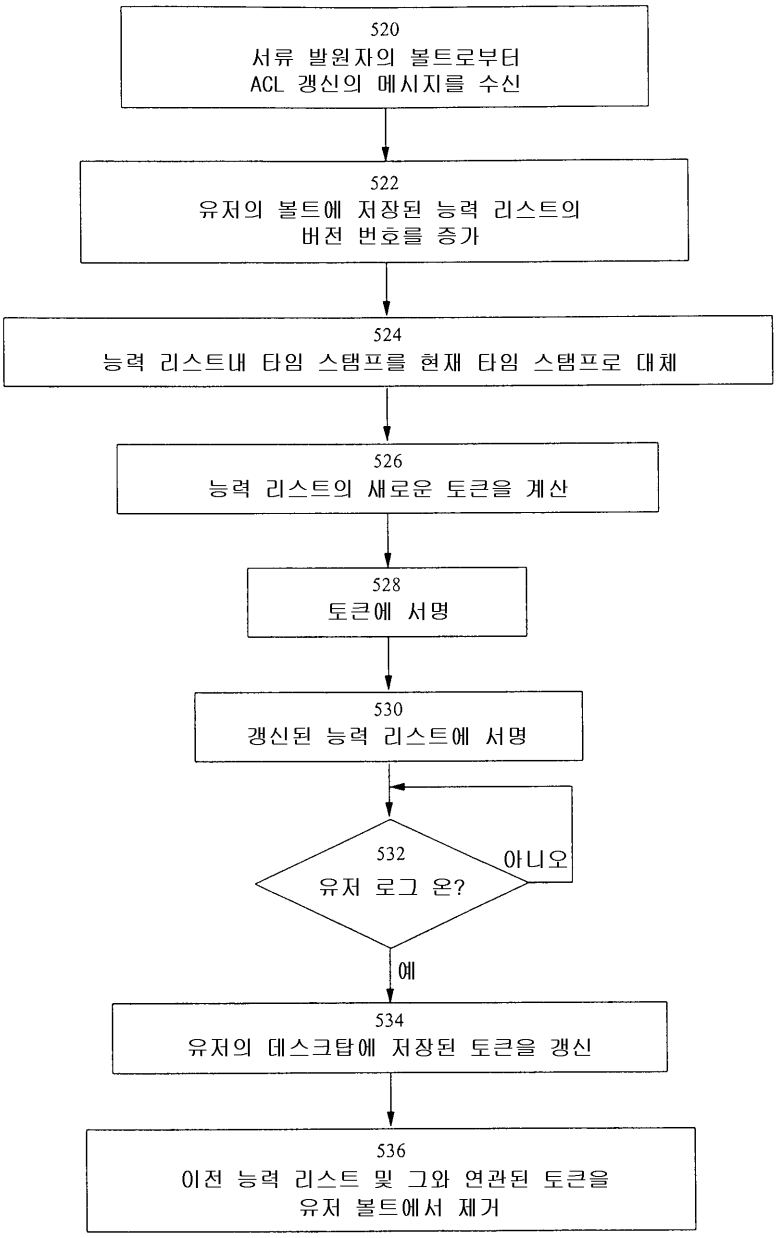
도면4b


서류 발원자의 볼트
애플리케이션 서버 볼트
요청자의 볼트
도 4a의 412로부터
416 서류 암호해독
418 공증된 서명 확인?
아니오
예
420 에러 코드를 애플리케이션 서버로 리턴
422 암호해독된 서류와 공증된 서명을 요청자의 볼트로 전달
424 서류 발원자의 공증된 서명 확인?
아니오
예
426 에러 메시지를 서류 발원자에게 리턴
428 공증된 암호화된 서류의 불반려 접수를 생성
430 암호해독된 불반려 접수를 요청자의 데스크탑으로 리턴
432 불반려 접수를 애플리케이션 서버로 전달
434 요청자 볼트의 서명 확인?
아니오
예
436 에러 메시지를 요청자에게 리턴
434 불반려 접수를 보관소에 저장

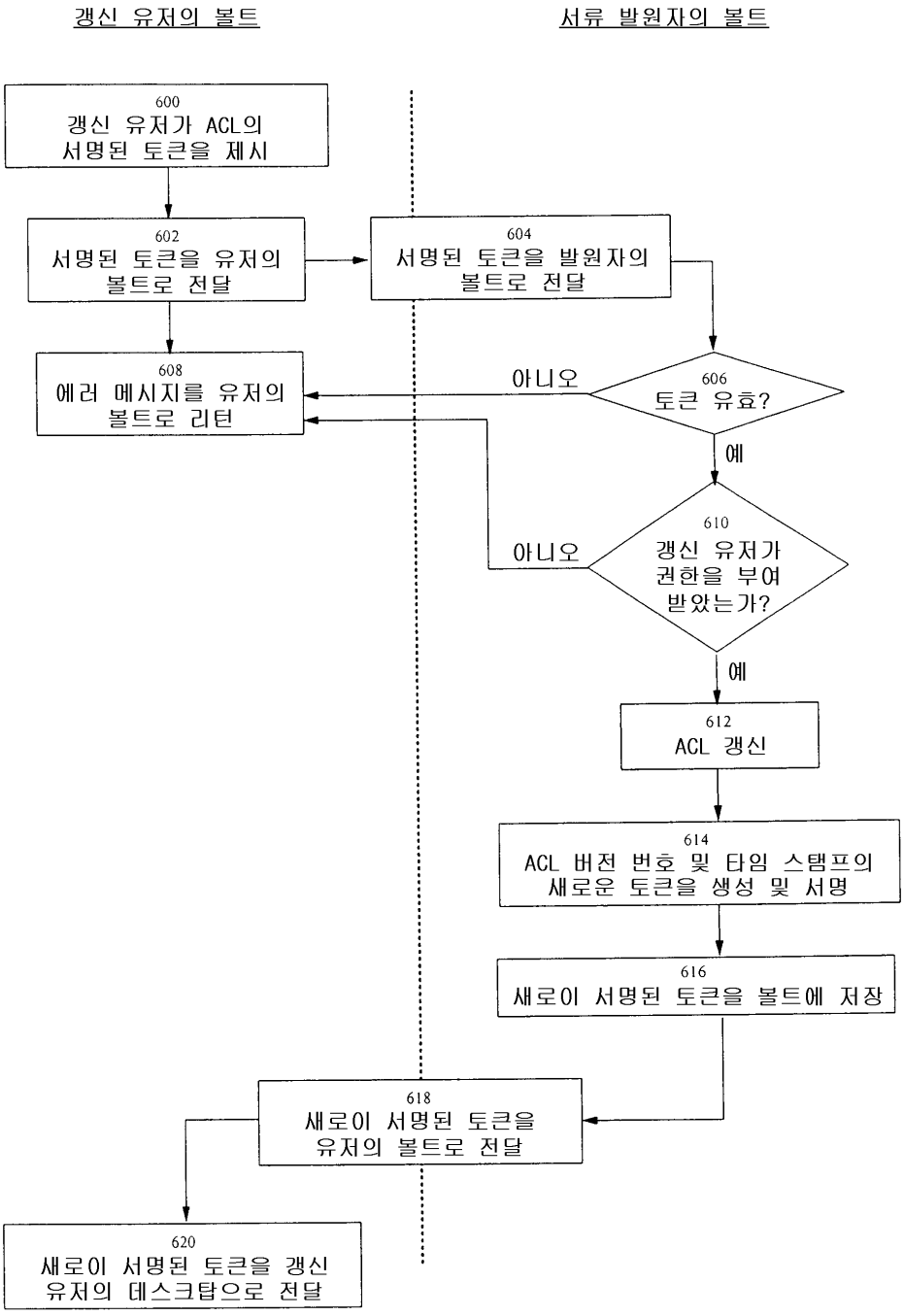
도면5a


시작
500
ACL이
갱신되었나
?
아니오
예
502
갱신에 영향 받은 유저 판단
504
ACL 갱신의 메시지를 영향받은 유저의 볼트로 전달
506
ACL 버전 번호를 증가
508
타임 스탬프를 현재 타임 스탬프로 대체
510
ACL 버전 번호와 타임 스탬프의 토큰을 생성 및 서명
512
ACL 서명
514
토큰을 권한을 부여받은 유저의 볼트로 전달하여
유저 데스크탑에 저장
516
서명된 토큰을 서류 발원자의 데스크탑으로 전달하여 저장

도면5b


520
서류 발원자의 볼트로부터
ACL 갱신의 메시지를 수신
522
유저의 볼트에 저장된 능력 리스트의
버전 번호를 증가
524
능력 리스트내 타임 스탬프를 현재 타임 스탬프로 대체
526
능력 리스트의 새로운 토큰을 계산
528
토큰에 서명
530
갱신된 능력 리스트에 서명
532
유저 로그 온?
아니오
예
534
유저의 데스크탑에 저장된 토큰을 갱신
536
이전 능력 리스트 및 그와 연관된 토큰을
유저 볼트에서 제거

도면6


갱신 유저의 볼트
서류 발원자의 볼트
600
갱신 유저가 ACL의 서명된 토큰을 제시
602
서명된 토큰을 유저의 볼트로 전달
604
서명된 토큰을 발원자의 볼트로 전달
606
토큰 유효?
아니오
예
608
에러 메시지를 유저의 볼트로 리턴
610
갱신 유저가 권한을 부여 받았는가?
아니오
예
612
ACL 갱신
614
ACL 버전 번호 및 타임 스탬프의 새로운 토큰을 생성 및 서명
616
새로이 서명된 토큰을 볼트에 저장
618
새로이 서명된 토큰을 유저의 볼트로 전달
620
새로이 서명된 토큰을 갱신 유저의 데스크탑으로 전달