(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06F 17/00 (2006.01)
G06Q 20/00A2 (2006.01)

(11) 공개번호 10-2006-0032888
(43) 공개일자 2006년04월18일

(21) 출원번호 10-2004-0081890
(22) 출원일자 2004년10월13일

(71) 출원인 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 김수형
대전시 유성구 지족동 열매마을@ 303-1702호
문기영
대전시 서구 월평동 누리아파트 101-1203
장종수
대전시 유성구 전민동 엑스포아파트 303-903
손승원
대전시 유성구 전민동 엑스포아파트 208-902

(74) 대리인 권태복
이화익

심사청구 : 있음

(54) 인터넷 통한 신원정보 관리 장치 및 이를 이용한 서비스제공방법

요약

본 발명은 인터넷 공간에서 전자 신원확인 증명서와 전자 계약서에 의하여 사용자의 신원정보를 용이하게 관리하고, 용이하게 서비스를 제공하기 위한 사용자의 신원정보 관리장치 및 이를 이용한 서비스 제공방법에 관한 것으로, 본 발명의 신원정보 관리장치는 인터넷 상에서 사용자의 신원을 증명하고 보장하기 위한 전자 신원확인 증명서를 발급하는 전자 신원확인 증명서 발급장치, 사용자의 전자 신원확인 증명서에 기반하여 사용자와 전자 계약서를 작성하고 사용자에게 서비스를 제공하는 서비스 제공장치 및 사용자와 전자 계약서가 작성된 서비스 제공장치로부터 서비스를 받기위한 사용자측 서버로 구성된다.

대표도

도 3

색인어

전자 신원확인 증명서, 전자 계약서, 사용자측 서버, 전자 신원확인 증명서 발급장치, 서비스 제공장치

명세서

도면의 간단한 설명

도 1은 본 발명의 전자 신원확인 증명서를 도시한 개략도,

도 2는 본 발명의 전자 계약서를 도시한 개략도,

도 3은 본 발명의 인터넷을 통한 신원정보 관리 시스템의 구성도,

도 4는 본 발명에 따른 전자 신원확인 증명서 발급장치의 구성를 도시한 구성도,

도 5는 본 발명에 따른 서비스 제공장치의 구성을 도시한 구성도,

도 6는 본 발명에 따른 사용자측 서버의 구성을 도시한 구성도,

도 7은 본 발명에 따른 전자 신원확인 증명서의 발급 방법을 개략적으로 도시한 흐름도,

도 8은 본 발명에 따른 사용자와 서비스 제공장치간 전자 계약서의 작성 방법을 개략적으로 도시한 흐름도,

도 9는 본 발명에 의한 서비스 제공장치의 서비스 공급방법을 개략적으로 도시한 흐름도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 인터넷 공간에서 사용자의 신원정보를 관리하기 위한 장치 및 이를 이용한 서비스 제공방법에 관한 것이다.

현재의 인터넷은 정치, 문화, 산업, 모든 분야 전반에서 기업과 기업(B2B), 기업과 개인(B2C), 개인과 개인(P2P)의 상호 거래 및 의사 교환을 위한 주요 매개체가 되었으며, 인터넷을 매개로 한 행위들 중에서 특히, 기업과 개인간의 거래는 무엇보다도 활발히 이루어지고 있다. 그러나 비대면 인터넷 공간에서 기업과 개인간에 이루어지는 행위들의 대부분은, 상호 신뢰를 바탕으로 하지 않음으로 인해, 여러 가지 제약과 해결해야 할 문제점들을 가지고 있다. 기업이 개인을 믿지 못함으로 인해 기업은, 개인에게 제공하는 서비스에 여러 가지 안전 장치를 두어야 하며, 개인에게 더 많은 신원정보를 요구하게 되며, 개인이 제공한 신원정보들을 안전하게 관리해야 하는 부담을 떠안는다. 개인이 기업을 믿지 못함으로 인해 개인은, 특정 서비스(예를 들어, 성인서비스) 사용에 필요한 신원정보를 타인의 것(예를 들어, 주민등록번호)으로 도용해 사용하는 경우가 있고, 신원정보를 상세히 요구하는 기업의 서비스 사용을 꺼려하고, 여러 곳의 기업에게 제공된 신원정보가 제대로 관리되고 있는지에 대한 불안감을 떨치기 어렵다.

서비스 제공자의 개인에 대한 신뢰는, 개인이 기업에게 제공한 신원정보(주민등록번호, 이름, 주소, 전화번호, 이메일 주소 등)에 주로 근간한다. 따라서 기업은 개인에게 재화 혹은 용역을 제공하기 이전에 사용자의 신원정보를 확보하고자 한다. 그리고 사용자가 인터넷을 통해 제공하는 신원정보를, 신뢰할 수 없으므로 인해, 사용자가 기업에게 제공하여야 하는 신원정보는, 사용자 이외의 다른 사람이 파악할 수 없는, 좀 더 구체적인 정보(신용카드정보, 은행계좌정보 등)를 포함하기도 한다. 또한, 은행 업무와 같이 사용자의 신원확인이 절대적으로 중요한 경우에는, 개인을 직접 오프라인에서 대면하고, 신원정보를 입력하는 경우도 있다. 종래에는 사용자가 인터넷을 통해 제공하는 신원정보를 신뢰할 수 있는 기술이 제공되지 않아 기업들은 불법 사용자들의 신원정보 도용을 방지할 수 있는 마땅한 대책을 찾지 못하고 있는 실정이다.

사용자의 서비스 제공자에 대한 신뢰는 서비스 제공자에 대한 다양한 평가 기준에 근간한다. 상기의 평가 기준에는 기업의 크기, 기업에 대한 인지도, 기업이 제공하는 용역 및 제화에 대한 이전 사용자들의 평가, 기업이 제공하는 사이트의 품질 정도 등이 해당되며, 개인의 주관적인 판단에 의해 결정되는 것이 대부분이다. 따라서, 개인의 기업에 대한 신뢰가 기술이나 법제의 보장을 받을 수 있는 시스템에 근간한 것이 아니므로 개인이 기업에게 제공하고자 하는 정보는 크게 제한적일 수 밖에 없으며 개인의 프라이버시가 기업 내에서 안전하게 보호되는지 확신할 수 없었다. 또한 개인 정보가 외부로 불법적으로 유출되었을 때의 책임 소재와 보상의 근거를 마련하기 힘든 실정이다.

앞서의 문제들을 극복하고자 두 가지 연구 방향이 존재한다.

하나는 개인의 프라이버시를 보호하기 위한 기술적 접근으로 P3P(Platform for Privacy Preferences)이며, 다른 하나는 개인과 기업간의 사전에 구축된 신뢰를 바탕으로 개인이 다른 기업과의 거래시에 개인의 신원을 보장하는 방법을 제공하는 Federated Identity와 관련된 연구이다.

P3P는, 사용자들이 자신의 개인정보를 어떻게, 어느 정도에서 보호받을 수 있는지를 스스로 판별할 수 있게 하고, 기업들이 고지하는 개인정보보호정책의 오류 또는 누락된 사항들을 검토하고자 하는 기술적 방안을 제시한다. 그러나 P3P는 특정 사이트가 개인정보보호정책을 준수하는지를 판정하는 수단으로서의 기능을 제공하지만, 기업 내 시스템에서 사용자의 신원정보가 어떻게 보호될 수 있는지를 명확히 설명하고 있지 않으며, 사용자가 제시한 신원정보가 올바른지를 평가할 수 있는 방법은 고려되지 않고 있다.

Federated Identity 관련 연구는, 개인의 신원정보를 한 곳에서 집중 관리하여, 다양한 기업(혹은 조직)에 개인의 신원정보가 산재해서 존재하는 것을 방지하고, 개인이 다른 기업의 서비스를 활용하기 위한 신뢰는, 개인 신원정보를 관리하는 기업의 보증으로 구축되는데, 이러한 보증이 가능하기 위해서는, 사용자가 접근하는 기업들 간의 신뢰 형성이 선행돼 구축되어 있다는 것을 가정한다. Federated Identity 관련 연구는, 기업 간 협력 프로세스를 구축하기 위한 방법을 제공하고, 단일사용승인(Single Sign-On: SSO) 기능을 제공하여 사용자에게 편의성을 제공하며, 사용자 관리에 소유되는 기업의 비용을 절감하는데, 그 목표를 두고 있다. 그러나 Federated Identity 관련 연구는, 기업 내부에서 발생할 수 있는 개인의 프라이버시 오남용과 관련된 문제를 해결하지는 못하며 기업 간의 신뢰가 사전에 구축되어 있어야 한다는 점에서 한계를 가지고 있다.

발명이 이루고자 하는 기술적 과제

상기와 같은 문제점을 해결하기 위한 본 발명은 인터넷 상에서 사용자의 신원정보를 관리하기 위한 방법 및 장치를 제공하는 것을 목적으로 한다. 구체적으로, 본 발명은 사용자의 신원정보에 기반하여 사용자와 서비스제공자 사이에 구축된 상호 신뢰를 바탕으로 용이하고 안전하게 서비스의 제공이 가능하도록 유도하며, 이 때 사용자는 서비스 제공자가 제공하는 서비스를 번거로운 인증절차 없이도 자유롭게 접근할 수 있고, 사용자의 신원정보가 서비스제공자에 의하여 오남용 되지 않도록 하는 방법 및 장치를 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

상술한 목적을 달성하기 위한 본 발명의 인터넷 공간에서의 신원정보 관리시스템은 인터넷 상에서 사용자의 신원을 증명하고 보장하기 위한 전자 신원확인 증명서를 발급하는 전자 신원확인 증명서 발급장치, 사용자의 전자 신원확인 증명서에 기반하여 사용자와 전자 계약서를 작성하고 사용자에게 서비스를 제공하는 서비스 제공장치, 및 사용자와 전자 계약서가 작성된 서비스 제공장치로부터 서비스를 받기위한 사용자측 서버로 구성된다.

상술한 목적을 달성하기 위해 본 발명의 인터넷 공간에서의 신원정보를 이용한 서비스 제공방법은 사용자가 신원확인 증명서 발급장치에 전자 신원확인 증명서 발급을 요청하여 전자 신원확인 증명서를 발급하는 제1단계, 전자 신원확인 증명서를 발급받은 사용자가 사용자측 서버를 통하여 서비스 제공장치에 서비스를 요청하고, 상기 서비스 제공장치는 사용자와의 전자 계약서의 발급 유무를 확인하여 전자 계약서가 아직 작성되지 않았으면 전자 계약서 작성장치를 통해 사용자측 서버로부터 정보를 제공받아 전자 계약서를 작성하는 제2단계, 제2단계에서 전자 계약서가 이미 작성된 경우 사용자는 사용자측 서버를 통하여 상기 전자 계약서를 이용해 상기 서비스 제공장치로부터 권한을 부여받아 상기 서비스 제공장치로부터 서비스를 제공받는 제3단계를 포함하여 구성된다.

상술한 바와 같은 본 발명의 목적, 구성 및 효과는 첨부된 도면과 이하의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하. 첨부된 도면을 참조하여 본 발명을 상세히 설명한다.

도 1은 본 발명의 전자 신원확인 증명서를 개략적으로 도시한다.

전자 신원확인 증명서는 전자 신원확인 증명서들을 유일하게 구분할 수 있는 전자 신원확인 증명서 고유번호(11), 전자 신원확인 증명서의 유효 기간(12), 전자 신원확인 증명서를 발급한 전자 신원확인 증명서 발급장치에 대한 정보(13)를 포함한다.

상기 전자 신원확인 증명서는 사용자의 신원정보(14)를 추가로 포함할 수 있다. 예를들어, 사용자의 실명, 전화번호, 주소, 주민등록번호 등을 포함할 수 있으며, 사용자의 사용자측 서버에 대한 정보(IP 혹은 URL 등) 등을 포함할 수 있다. 전자 신원확인 증명서의 발급시 사용자의 신원정보(14)는 사용자의 선택이나 전자 신원확인 증명서 발급장치에 의해 포함될 수 있다. 이러한 전자 신원확인 증명서는 특정한 서비스 제공장치에서 서비스를 제공받기위해 필요한 정보만을 선별적으로 포함할 수 있으므로, 사용자는 다수개의 전자 신원확인 증명서를 발급받아 사용자측 서버를 통해 관리할 수 있다. 즉, 보안의 유지가 불필요한 인터넷 커뮤니티에 참가하기 위해서는 사용자의 신원정보가 포함되지 않은 전자 신원확인 증명서를 이용할 수 있으며, 성인 컨텐츠에 접근하기 위해서는 사용자의 나이를 포함하는 전자 신원확인 증명서를 사용할 수 있다.

본 발명에 따른 전자 신원확인 증명서는 사용자측 서버 정보(15)를 추가로 포함할 수 있다. 사용자측 서버 정보(15)는 사용자측 서버의 IP주소나 URL과 같은 정보가 될 수 있으며, 사용자측 서버 정보(15)에 의하여 결정된 사용자측 서버에서만 이러한 전자 확인 증명서의 사용이 가능하도록 제한 하는 것이 가능하다.

본 발명에 따른 전자 신원확인 증명서는 성인 인증 정보(16)를 추가로 포함할 수 있다. 성인 인증 정보(16)는 전자 신원확인 증명서 발급장치에서 사용자의 신원정보(예를들어, 실명과 주민등록번호)를 확인하여 제공하는 것이다. 이러한 성인 인증 정보(16)을 통하여 서비스 제공장치에 사용자의 실명과 주민등록번호를 노출시키지 않으면서 성인인증이 가능하다.

본 발명에 따른 전자 신원확인 증명서는 전자 신원확인 증명서의 무결성을 보장하기 위한 전자 신원확인 증명서 발급장치의 전자 서명(17)을 추가로 포함할 수 있다.

상기 전자 신원확인 증명서는 바람직하게는 XML 문서로 구현될 수 있으나 이에 한정되지 않는다.

도 2는 본 발명의 전자 계약서를 개략적으로 도시한다.

전자 계약서(20)는 서비스 제공장치에 의해 작성된 전자 계약서들을 유일하게 구분할 수 있는 전자 계약서 고유번호(21), 전자 계약서의 유효 기간(22), 전자 계약서 작성 시에 사용자가 서비스 제공장치에 제공한 사용자 신원정보(23), 전자 계약서를 작성한 서비스 제공장치 정보(24)를 포함한다. 또한, 전자 계약서를 체결한 서비스 제공장치 내에서 유일하게 사용자를 구분할 수 있는 사용자 ID(25), 사용자에게 제시했던 서비스 제공장치의 개인정보보호정책 혹은 사용자가 서비스 제공장치 시스템에서 사용할 수 있는 서비스의 범위 등을 기술한 보안 정책(26), 전자 계약서의 소유자를 증명하는 전자 계약서 소유자 정보(27), 전자 계약서의 실효성을 확보하기 위한 서비스 제공장치의 전자서명(28), 사용자와 서비스 제공장치가 전자 계약서 작성 시에 협상하고 결정한 계약 내용(29)을 추가로 포함할 수 있다.

상기 보안 정책(26)에 기재되는 서비스 제공장치의 개인정보보호정책은 사용자마다 다르게 적용될 수 있다. 예를들어, 사용자가 제공한 개인 신원정보, 사용자가 허락한 개인 정보 수집 방법 및 범위, 사용자가 허락한 개인 정보의 가공 범위등이 클수록, 서비스 제공장치는 사용자에게 좀 더 많은 서비스를 제공하도록 보안 정책(26)을 결정한다.

상기 전자 계약서 소유자 정보(27)는 서비스 제공장치가 제공하는 서비스를 요청한 사용자가, 상기 서비스 제공장치와 전자 계약서를 작성한 적이 있다는 것을 증명하기 위한 정보이다. 사용자의 전자 계약서 체결사실을 증명할 수 있는 정보라면 그 형태와 방법에 제한을 두지 않는다. 예를들어, 사용자와 서비스 제공장치만이 알고 있는 비밀키(symmetric key)를 소유자 증명 정보로 하고, 서비스 제공장치가 임의로 생성된 문자열을 사용자측 서버에 전송하고, 상기 사용자측 서버는 상기 임의의 문자열과 상기 서비스 제공장치와의 전자 계약서를 입력으로 하는 해쉬 함수의 결과를 상기 비밀키로 암호화하고, 상기 암호화된 문자열을 상기 사용자측 서버가 상기 서비스 제공장치로 전송하고, 상기 서비스 제공장치는 상기 임의의 문자열과 상기 서비스 제공장치가 가지고 있는 상기 사용자와의 전자 계약서를 입력으로 하는 해쉬 함수의 결과를 상기 비밀키로 암호화하고, 상기 암호화된 문자열이 상기 사용자측 서버가 보낸 문자열과 일치하는 지를 판정하여, 상기 사용자가 상기 서비스 제공장치와의 전자 계약서를 이미 소유하고 있음을 증명하는 것이다. 이러한 전자 계약서 소유자 정보(27)는 중간자 공격(man-in-the-middle attack) 혹은 재전송 공격(reply attack) 등을 방지하기 위한 것이다.

상기 서비스 제공장치 정보(24)는 서비스 제공장치의 신뢰성을 파악할 수 있는 정보를 포함할 수 있다. 예를 들어, 국내에서 시행되고 있는 전자상거래 인증제도에서의 쇼핑몰에 대한 인증마크를 대체한 신뢰받는 제 3자(Trusted Third Party)에 의한 쇼핑몰 신뢰도 평가 정보 등을 포함할 수 있다.

전자 계약서는 전자 계약서의 무결성 및 강제성을 보장하기 위해 전자 계약서 작성시에 서비스 제공장치에 의해 작성된 전자서명(28)을 포함한다. 이는 서비스 제공장치가 전자 계약서에 기재된 개인정보보호정책 기타 계약사항을 위반하는 경우에 계약의 이행을 강제하거나 위약에 따른 배상을 청구하는 근거가 된다.

전자 계약서는 바람직하게는 XML 문서로 구현될 수 있으나, 이에 한정되지 않는다.

도 3은 본 발명의 인터넷을 통한 신원정보 관리 시스템의 구성도이다.

전자 신원확인 증명서 발급장치(100)는, 사용자측 서버로부터 전자 신원확인 증명서 발급 요청이 있는 경우에, 사용자의 신원 정보를 입력받아 전자 신원확인 증명서를 발급하기 위한 장치이다. 서비스 제공장치(200)는 사용자측 서버(300)으로부터 전자 신원확인 증명서를 전송받아, 이를 이용하여 사용자와의 전자 계약서를 작성하고, 체결된 전자 계약서에 기반하여 사용자에게 제공할 서비스의 범위를 결정하며, 전자 계약서에 포함된 사용자와의 계약 내용에 의거하여 사용자의 신원정보를 보호하며, 전자 계약서의 유효기간이 만료전까지 사용자에게 서비스를 제공하기 위한 장치이다. 사용자측 서버(300)는 전자 신원확인 증명서 발급장치(100)로부터 발급 받은 전자 신원확인 증명서를 수신하여 저장하며, 서비스 제공장치(200)에 상기 전자 신원확인 증명서를 교부하여 전자 계약서를 작성하고, 전자계약서가 작성된 서비스 제공장치(200)로부터 서비스를 제공받기 위해 상기 서비스 제공장치(200)에 접근하기 위한 장치이다. 아울러, 사용자측 서버(300)는 사용자가 발급받은 다수의 전자 신원확인 증명서 및 다수의 서비스 제공장치(200)와 체결한 전자 계약서의 목록을 관리하고, 사용자가 서비스를 제공받기 위해 서비스 제공장치(200)에 접근한 기록을 작성 및 관리하는 기능을 수행한다.

전자 신원확인 증명서 발급장치(100)는 인터넷에 연결되며, 사용자측 서버를 통한 사용자의 전자 신원확인 증명서 발급요청에 응하여 전자 신원확인 증명서를 발급하여 사용자측 서버(300)로 전송한다. 이러한 전자 신원확인 증명서 발급장치(100)는 전자 신원확인 증명서의 신뢰성을 확보하기 위하여 바람직하게는 공신력 있는 단체에 의하여 운영될 수 있으며, 본 발명이 특정 지역이나 집단에 한정적으로 적용되는 경우에는 해당하는 사설 조직에 의하여 운영될 수도 있다. 이러한 전자 신원확인 증명서 발급장치(100)는 PKI(Public Key Infrastructure)에 있어서, 공인 인증기관과 사설 인증기관에 대응되는 개념으로 이해될 수 있다. 전자 신원확인 증명서 발급장치(100)는 전자 신원확인 증명서를 발급하기 위하여 최초 1회에 한하여 사용자의 신원정보(변경되지 않는 사용자 정보, 예를들어 실명, 주민등록번호)를 입력받아 기록한다. 이때, 바람직하게는 사용자의 신원을 보증할 수 있는 수단, 즉, 공인인증서 또는 사설인증서를 이용하여 입력받는다. 이렇게 기록된 사용자의 신원정보는 그 신뢰성 확보를 위하여 사용자에 의하여 직접 변경될 수 없다.

서비스 제공장치(200)는 사용자에게 인터넷을 경유하여 제공 가능한 서비스 또는 용역 등의 서비스를 제공한다. 상기 서비스 제공장치(200)는 인터넷을 경유하여 제공 가능한 각종 서비스를 위한 웹 서버(web server) 또는 어플리케이션 서버(application server)등을 포함할 수 있다.

상기 사용자측 서버(300)는 인터넷에 연결되며, 퍼스널 컴퓨터 또는 디지털 홈을 위한 홈 서버, 셋탑박스(Set Top Box) 등의 형태로 구현될 수 있다. 상기 사용자측 서버(300)는 특정 사용자만이 사용자측 서버(300)를 이용하여 전자 신원확인 증명서 발급장치(100)로부터 전자 신원확인 증명서를 발급받고, 이를 이용하여 서비스 제공장치(200)로부터 서비스를 제공받을 수 있도록 제한한다. 바람직하게는 단일 사용자에게만 제한적으로 접근가능 하도록 운영되나, 다수의 사용자가 접근가능 하도록 운영되는 것을 제한하지는 않는다. 상기 사용자측 서버(300)는 사용자가 사용자측 서버(300)에 접근하고자 하는 경우 사용자의 보안정보를 확인하여 사용자 인증을 행한다. 상기 보안정보는 서버의 사용자를 확인하기 위한 정보로서, ID와 패스워드, 인증서, 스마트카드에 기록된 신상정보 등이 이에 해당한다. 사용자는 사용자측 서버(300)를 직접 조작할 수도 있으나, 별도의 퍼스널 컴퓨터나 PDA, 모바일 폰 등의 단말기를 이용하여 사용자측 서버(300)에 원격으로 접속하여 이용할 수도 있다.

도 4는 본 발명에 따른 전자 신원확인 증명서 발급장치(100)의 구조를 도시하였다.

전자 신원확인 증명서 발급장치는 사용자가 전자 신원확인 증명서를 발급하기 위한 창구 역할을 수행하는 요청 접수부(110), 사용자 신원정보를 기록하는 신원정보 저장부(120), 사용자의 요청에 따라 상기 등록된 신원정보에 근거하여 사용자 전자 신원확인 증명서를 발급하는 전자 신원확인 증명서 발급부(130), 사용자가 전자 신원확인 증명서 발급장치에 서비스를 요청하였을 때 상기 사용자를 인증하는 사용자 인증부(140), 서비스 제공장치(200)에 의해 특정 사용자의 전자 신원확인 증명서에 대한 검증 요청을 접수하였을 때, 상기 전자 신원확인 증명서의 유효성 여부를 검증하는 전자 신원확인 증명서 검증부(150)를 포함한다.

상기 요청 접수부(110)는 다수의 사용자에 대한 신원 확인 증명서 발급 서비스를 제공하는 창구 역할을 수행한다. 바람직하게는, 상기 서비스 요청 접수부(110)는 사용자와 직접 상호작용 할 수 있는 웹 페이지를 제공하며, 전자 신원확인 증명서의 발급시 사용자측 서버(300) 혹은 서비스 제공장치(200)와 인터넷 프로토콜을 통해 상호작용하는 기능을 제공한다.

상기 신원정보 저장부(120)는 사용자가 전자 신원정보 증명서 발급장치(100)에 최초로 접근하는 경우, 즉, 사용자 정보가 신원정보 저장부(120)에 기록되어있지 않은 경우에 사용자의 신원정보를 입력받아 기록하고, 사용자 정보가 이미 기록되어 있는 경우에 사용자 정보를 전자 신원확인 증명서 발급부(130)로 전달하여 전자 신원확인 증명서를 발급하도록 하는 수단이다. 신원정보 저장부(120)에 저장되는 사용자의 신원정보는 진위의 여부가 매우 중요하므로 공인인증서 기타 본인임을 입증할 수 있는 수단을 이용하여 입력받아 기록한다.

전자 신원확인 증명서 발급부(130)는 사용자의 전자 신원확인 증명서 발급요청시 상기 신원정보 저장부(120)에서 사용자의 신원정보를 입력받아 전자 신원확인 증명서를 유일하게 구분할 수 있는 전자 신원확인 증명서 고유번호, 전자 신원확인 증명서의 유효 기간 및 전자 신원확인 증명서를 발급한 전자 신원확인 증명서 발급장치에 대한 정보가 포함된 신원확인 증명서를 작성하여 요청접수부를 통해 사용자측 서버(300)로 전송한다. 새롭게 부여된 전자 신원확인 증명서 고유번호는 전자 신원확인 증명서 검증부(150)로 전달되어 신원확인 증명서의 유효성의 검증에 이용된다.

상기 전자 신원확인 증명서 검증부(150)는 상기 서비스 요청 접수부(110)에서 서비스 제공장치(200)로부터 전송받은 전자 신원확인 증명서를 넘겨주면 이의 유효성 여부를 검증하는 역할을 수행한다. 예를들어, 신원확인 증명서의 고유번호와 전자 신원확인 증명서 발급장치에 대한 정보를 확인하여 유효성 여부를 판단할 수 있다.

비록 도면에 도시되지는 않았지만, 전자 신원확인 증명서 발급장치(100)는 통상적인 서버가 가지는 기능과 장치들을 포함할 수 있다.

도 5는 본 발명에 따른 서비스 제공장치(200)의 내부 블록을 도시하였다.

서비스 제공장치는 사용자에게 재화 및 용역을 제공하기 위한 서비스 공급부(210), 사용자가 제공한 전자 계약서를 검증하는 전자 계약서 검증부(220), 전자 계약서가 작성되지 않은 사용자에 대하여 전자 계약서를 작성하기 위한 전자 계약서 작성부(230), 상기 전자 계약서를 저장하는 전자 계약서 저장부(240), 상기 전자 계약서에 의거하여 사용자의 신원정보를 보호하는 사용자 정보 보호부(250), 상기 전자 계약서에 의거하여 사용자에 대한 서비스 제공 범위를 결정하는 서비스 접근 제어부(260), 전자 계약서 작성시에 사용자가 제시한 전자 신원확인 증명서의 유효성을 확인하는 전자 신원확인 증명서 확인부(270), 전자 계약서에 포함된 내용과 서비스 제공장치의 정책에 따라 전자 계약서를 관리하는 전자 계약서 관리부(280)를 포함한다.

서비스 공급부(210)는 전자 계약서를 작성한 사용자에게 인터넷을 통하여 서비스를 제공하기 위한 수단이다. 상기 서비스 공급부(210)에서 제공하는 서비스는 인터넷을 경유하여 제공 가능한 것이면 서비스의 형태 또는 내용을 가리지 아니한다. 상기 서비스 공급부(210)에서는 사용자의 서비스 공급요청이 있는 경우에, 전자계약서 저장부(240)를 검색하여 전자계약서의 작성여부를 판단하여 유효한 전자 계약서가 존재한다면 서비스를 제공하고, 유효한 전자 계약서가 존재하지 않는다면 사용자측 서버(300)로 전자 신원확인 증명서를 요청하고, 전자 신원확인 증명서 확인부(270)과 전자 계약서 작성부(230)에 전자 계약서의 작성을 지시한다.

상기 사용자 정보 보호부(250)는 전자 계약서에 명시된 서비스 제공장치(200)의 사용자 신원정보의 보호기준을 상기 서비스 공급부(210)에서 준수하고 있는지 여부를 확인한다. 예를들어, 사용자 정보 보호부(250)는 서비스 공급부(210)가 전자 계약서에 포함된 사항과 서비스 제공장치(200)에 대한 사용자의 접근 및 사용 이력을 근거로 하여 사용자에 대한 고객관계관리(Customer Relationship Management) 마케팅을 실시하는 경우에, 사용자의 이력정보를 활용하는 것이 전자 계약서상에 기재된 사용자의 신원정보 보호기준에 위배되는지를 판정할 수 있다. 또한, 서비스 공급부(210)가 사용자의 서비스 사용 이력을 수집하는 경우에도 전자 계약서에 기재된 사용자의 신원정보 보호기준에 위배되는지를 판정할 수 있다.

상기 서비스 접근 제어부(260)는 사용자에 따라서 제공되는 용역이나 서비스를 제한하거나 허용하기 위한 것이다. 예를들어, 서비스 접근 제어부(260)는 전자 계약서 내에 포함된 사용자의 신원정보의 정도에 따라, 또는 전자계약서 상에서 사용자에게 제공하기로 한 서비스나 용역의 범위에 따라서 사용자에게 제공할 서비스나 용역을 제한하거나 허용할 수 있다. 즉, 전자 계약서상에서 특정 서비스에 대해서만 사용자의 접근 권한을 허용하는 경우 나머지 서비스에 대한 이용을 제한하거나, 사용자의 나이에 따라 성인 컨텐츠의 제공여부를 결정할 수 있다.

상기 전자 신원확인 증명서 확인부(270)는 전자 계약서의 작성을 위하여 사용자측 서버(300)로부터 제공받은 전자 신원확인 증명서를 확인하기 위한 수단이다. 전자 신원확인 증명서가 유효한 경우, 상기 전자 신원확인 증명서에 포함된 사용자의 신원정보 기타 전자 신원확인 증명서에 포함된 정보를 추출하여 전자 계약서 작성부(230)로 전송한다. 전자 신원확인

증명서의 유효성을 확인하는 것은 요구되는 정확도에 따라서 상이한 방법이 채용될 수 있다. 예를들어, 주민등록번호의 형식만을 검증한다거나, 입력받은 전자 신원확인 증명서를 발급한 전자 신원확인 증명서 발급장치(100)의 전자 신원확인 증명서 검증부(150)로 전자 신원확인 증명서를 전송하여 유효성 여부를 검증한다거나 하는 방법이 있다.

이외에 도면에 도시 되지는 않았지만, 서비스 제공장치(200)는 통상적인 서버가 가지는 기능과 장치들을 포함하고 있으며, 각종 서비스의 제공에 필요한 부대적인 구성요소를 더 포함 할 수 있다.

도 6는 본 발명에 따른 사용자측 서버(300)의 내부 블록을 도시하였다.

사용자측 서버(300)는 전자 신원확인 증명서 발급장치에서 발급한 전자 신원확인 증명서의 유효성을 확인하는 전자 신원확인 증명서 확인부(310), 전자 신원확인 증명서 발급장치로부터 발급받은 전자 신원확인 증명서를 저장하고 관리하는 전자 신원확인 증명서 저장부(320), 사용자에게 전자 신원확인 증명서와 전자 계약서에 관련된 정보를 제공하는 정보 처리부(330), 상기 사용자측 서버의 사용 주체를 확인하기 위한 사용자 인증부(340), 서비스 제공장치에서 작성한 전자 계약서의 유효성을 확인하는 전자 계약서 확인부(350), 서비스 제공장치에서 작성한 전자 계약서를 저장하고 관리하는 전자 계약서 저장부(360)를 포함한다.

상기 정보처리부(330)는 인터넷에 연결되며, 인터넷을 통하여 사용자측 서버(300)에 접수된 각종 요청을 처리하여 결과값을 반환한다. 즉, 사용자가 사용자측 서버(300)에 접속하는 경우에 사용자 인증부(340)를 통해 사용자를 인증하고, 전자 신원확인 증명서 또는 전자계약서에 대한 정보의 열람요청시 전자 신원확인 증명서 저장부(320) 또는 전자계약서 저장부(360)에 저장된 정보를 검색하여 반환한다. 또한, 사용자가 전자 신원확인 증명서 발급장치(100)로부터 전자 신원확인 증명서를 발급받은 경우 전자 신원확인 증명서 확인부(310)에서 발급받은 전자 신원확인 증명서의 유효성을 확인한 다음 전자 신원확인 증명서 저장부(320)에 저장한다. 서비스 제공장치(200)로부터 서비스를 받고자 하는 경우에 상기 서비스 제공장치(200)에 유효한 전자계약서가 존재하지 않는 경우에는 서비스 제공장치(200)의 요청에 의하여 전자 신원확인 증명서 저장부(320)에 저장된 전자 신원확인 증명서를 서비스 제공장치(200)로 전송하고, 서비스 제공장치(200)로부터 전자 계약서를 발급받아 전자 계약서 확인부(350)을 통해 전자 계약서의 유효성을 판단한 다음 전자 계약서 저장부(360)에 저장한다. 또한, 정보처리부(330)는 사용자의 전자 신원확인 증명서 발급 이력 관리, 서비스 제공장치에 대한 접속 이력 관리 등의 이력 관리를 수행한다. 상기 정보처리부(330)는 보안의 유지를 위하여 전자 신원확인 증명서 발급장치(100) 또는 서비스 제공장치(200)와 보안 통신 채널(예를 들어, SSL/TLS)을 생성하여 통신할 수 있다. 또한, 보안의 확보를 위하여 정보처리부(330)는 사용자가 퍼스널 컴퓨터나 PDA, 모바일 폰 등의 단말기를 이용하여 사용자측 서버(300)에 원격 접속하는 경우 특정 위치 또는 특정 장치에 대해서만 접근을 허용할 수도 있다. 예를들어, 로컬 네트워크에서 접속한 사용자 혹은 지정된 IP 주소를 갖는 단말의 사용자에 대해서만 사용자측 서버(300)에 접속하여 사용자측 서버(300)를 이용할 수 있도록 제한할 수 있다.

사용자 인증부(340)는 사용자측 서버의 사용 주체를 인증하기 위한 수단이다. 사용자가 사용자측 서버(300)에 접근하는 경우, 정보처리부(330)는 사용자 인증부(340)에 사용자의 인증을 요청하고, 이때 사용자 인증부(340)는 사용자의 보안정보를 요구하여 사용자를 인증하고 인증된 사용자에 한하여 사용자측 서버(300)에 대한 접근을 허용한다. 사용자의 인증은 아이디와 패스워드의 입력 또는 공인 인증서를 통한 인증이나, 사용자의 스마트카드를 통한 인증 등의 방식을 채용할 수 있으나 이에 한정되지는 않는다.

이외에 도면에 도시되지는 않았지만, 사용자측 서버는 통상적인 서버가 가지는 구성요소를 포함할 수 있다.

도 7은 본 발명의 일 실시예에 따른 전자 신원확인 증명서의 발급 방법을 개략적으로 도시한다. 먼저, 사용자는 웹브라우저를 통하여 전자 신원확인 증명서 발급장치에 접속한다(S101). 전자 신원확인 증명서 발급장치에 접속한 사용자는 사용자의 인증을 위하여 보안정보를 제시하여 사용자 인증을 받는다(S102). 인증에 실패하면 전자 신원확인 증명서 발급장치는 사용자의 접근을 거부한다. 상기 인증된 사용자가 상기 전자 신원확인 증명서 발급장치의 서비스 요청 접수부를 통해 전자 신원확인 증명서 발급 요청을 하면(S103), 상기 전자 신원확인 증명서 발급장치는 전자 신원확인 증명서 발급에 필요한 사용자의 신원정보의 입력을 요구한다. 사용자가 이러한 요청에 응하여 전자 신원확인 증명서의 발급에 필요한 신원정보를 입력한다(S104). 이때 사용자 최초등록시 입력된 신원정보와 중첩되는 정보는 생략할 수 있다. 예를들어, 사용자 등록시 입력된 사용자의 성명, 주민등록번호등의 신상정보를 알 수 있으므로 이러한 정보를 재차 입력받지 않을 수 있다. 상기 전자 신원확인 증명서 발급장치는 입력받은 신원정보를 이용하여 전자 신원확인 증명서를 생성한다. 이때 사용자의 성명, 주민등록번호와 같은 기본 정보는 익명성을 요구하는 사용자의 요청에 의해 전자 신원확인 증명서에 포함되지 않을 수 있다. 그리고, 전자 신원확인 증명서의 발급전 또는 발급후에 전자 신원확인 증명서의 내용을 웹 브라우저를 통하여 사용

자에게 확인시킬 수도 있다. 전자 신원확인 증명서 발급장치는 발급된 전자 신원확인 증명서를 사용자측 서버로 전달하고, 사용자측 서버에서 발급받은 전자 신원확인 증명서를 검증하고, 증명서를 저장하는 것으로 전자 신원확인 증명서의 발급이 완료된다(S105).

상기 전자 신원확인 증명서 발급 방법에 있어서, 사용자와 전자 신원확인 증명서 발급장치간의 통신 및 전자 신원확인 증명서 발급장치와 사용자측 서버간의 통신은 보안의 유지를 위하여 SSL(Secure Sockets Layer)/TLS(Transport Layer Security) 채널 상에서 수행되는 것이 바람직하다.

도 8은 본 발명에 따른 사용자와 서비스 제공장치간 전자 계약서의 작성 방법을 개략적으로 도시한다. 서비스 요청장치에서 사용자측 서버를 통해 전자 계약서에 포함될 계약 내용의 전달과 함께 전자 계약서 작성에 필요한 전자 신원확인 증명서 및 사용자의 신원정보를 요청하는 방식으로 전자 계약서 체결요청을 한다(S201). 사용자측 서버에서는 전달받은 계약 내용에 포함된 상기 서비스 제공장치의 개인정보보호정책이 사용자의 신원정보 관리 지침에 위배되지 않는지 여부를 검사한다(S202). 검사결과 신원정보 관리 지침에 위배되지 않는다면, 사용자측 서버에서는 전송받은 전자 계약서의 내용을 웹브라우저상에 표시하여 사용자에게 알리며, 전자 계약서의 작성에 필요한 사용자의 신원정보의 입력을 위한 입력창을 제공한다. 사용자가 전자 계약서의 내용을 확인하고(S203), 전자 계약서 체결에 동의하여 사용자측 서버에 저장된 전자 신원확인 증명서 중 계약내용과 부합되는 전자 신원확인 증명서를 선택하고, 전자 신원확인 증명서에 포함되지 않는 부가적인 신원정보(예를들어, 서비스 제공자측이 제공하는 이메일 수신여부, 관심분야, 결혼여부 등)을 입력한다. 사용자측 서버에서는 입력받은 신원정보와 선정된 전자 신원확인 증명서를 서비스 제공장치로 전송한다(S204). 서비스 제공장치는 상기 전자 신원확인 증명서를 검증하고(S205), 상기 계약 요청서의 내용과 부합되는 전자 계약서를 작성하고, 서명한다(S206). 상기 서비스 제공장치는 상기 작성된 전자 계약서를 상기 사용자측 서버에 전달한다(S207). 사용자측 서버는 전달받은 전자 계약서의 내용이 전자 계약서 체결 요청시 제시된 계약 내용과 일치하는지, 서비스 제공장치의 서명이 정확한지 검증하고, 전자 계약서가 유효하게 작성된 것으로 검증되면 전자 계약서를 저장한다(S208).

사용자측 서버에서 서비스 제공장치의 개인정보보호정책이 사용자의 신원정보 관리 지침에 위배되는지 여부를 검사하는 것(S202)은 서비스 제공장치의 개인정보보호정책이 방대하거나 복잡하여 사용자가 모든 내용을 검토할 수 없으므로 사용자에 의해 미리 정의된 신원정보 관리 지침에 의거, 사용자측 서버가 자동적으로 서비스 제공장치의 개인정보보호정책을 검사하는 것이다. 즉, 신원정보 관리지침은 사용자에 의하여 신원정보의 공개정도나 활용에 대한 허용정도가 미리 정의된 것인데, 사용자측 서버에서는 서비스 제공장치의 개인정보보호정책이 사용자가 미리 정의한 신원정보 관리 지침의 한도를 벗어난 경우에는 계약체결을 거부하거나, 또는 사용자에게 신원정보 관리지침을 벗어난 항목을 알려준다.

상기 사용자와 서비스 제공장치간 전자 계약서의 작성 방법에 있어서, 서비스 제공장치와 사용자측 서버간의 통신은 보안의 유지를 위하여 바람직하게는 SSL(Secure Sockets Layer)/TLS(Transport Layer Security) 채널 상에서 수행된다.

도 9는 본 발명에 의한 서비스 제공장치의 서비스 공급방법을 개략적으로 도시한다.

사용자는 웹 브라우저를 통해 서비스 제공장치에 접속하여 서비스를 요청한다(S301). 이때, 상기 서비스 제공장치는 상기 사용자의 사용자측 서버에 전자 계약서를 요청한다(S302). 요청을 받은 사용자측 서버에서 전자 계약서를 검색하여 유효한 전자 계약서가 존재하지 않는 경우 이를 서비스 제공장치에 알리고, 상기 사용자와 서비스 제공장치간 전자 계약서의 작성 방법에 따라 전자계약서를 작성한다(S303). 만일, 유효한 전자계약서가 존재하는 경우에는 사용자측 서버는 서비스 제공장치로 전자 계약서를 전달하고(S304), 전달받은 서비스 제공장치에서는 전자계약서의 유효성을 검증한다(S305). 서비스 제공장치에서는 유효한 전자계약서가 확인된 경우, 즉, 사용자측 서버로부터 유효한 전자계약서를 전달받았거나, 전자 계약서를 새로 작성한 경우에 필요에 따라 상기 사용자에 대한 사용자 인증 세션을 생성한다(S306). 인증 세션 동안에는 사용중인 사용자의 웹브라우저가 구동중인 한 사용자에 대한 전자 계약서의 확인 절차없이 사용자에게 서비스를 제공할 수 있다. 즉, 인증세션 동안에는 서비스 요청단계(301)에서 바로 서비스 권한 검사단계(S307)로 진행할 수 있다. 사용자가 인증되면 상기 서비스 제공장치는 상기 사용자가 요청한 서비스에 대한 서비스 권한을 갖고 있는지 검사한다. 상기 사용자가 서비스 권한을 갖지 않은 경우, 즉, 전자 계약서상에 특정 서비스에 대한 권한이 포함되어 있지 않은 경우 등 서비스를 할 수 없는 경우에는 서비스를 거절하고, 서비스 권한을 갖는 경우에는 사용자가 요청한 서비스를 제공한다(S308).

상기 서비스 제공장치가 사용자측 서버에 전자 계약서를 요청하는 과정(S302)에서 서비스 제공장치가 사용자측 서버의 위치를 확인하는 방법은 사용자가 직접 서버 위치를 입력하거나 사용자가 서비스 제공장치에 입력한 사용자 아이디를 통해 사전에 등록된 사용자측 서버 위치를 확보하거나 사용자가 웹브라우저에서 서비스 요청시의 요청 메시지에 함께 서버 위치를 포함하여 전달하는 방법 등 다양한 방법들이 사용될 수 있다.

상기에서 사용자측 서버가 서비스 제공장치에 전자 계약서를 전달하고 확인하는 과정(S304 및 S305)은 전자 계약서의 소유자 증명 정보를 전달하고 확인하는 것으로 대체될 수 있다.

상기 본 발명에 의한 서비스 제공장치의 서비스 공급방법에 있어, 서비스 제공장치와 사용자측 서버간의 통신은 바람직하게는 SSL(Secure Sockets Layer)/TLS(Transport Layer Security) 채널 상에서 수행된다.

이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 한정되는 것은 아니다.

발명의 효과

이상에서 설명한 바와 같이, 본 발명은 유무선 인터넷 공간에서 사용자의 신원정보를 관리하고, 이에 근거하여 서비스 제공자와 사용자간에 전자 계약서를 작성하여 서비스의 제공을 용이하게 하기 위한 방법 및 장치를 제공한다.

이러한 본 발명에 의하면, 사용자가 서비스 제공자에게 제공한 신원정보가 오남용 되거나 불법적으로 유통되는 것을 막을 수 있으며, 사용자가 제공한 신원정보를 신뢰할 수 있어 타인의 신원정보를 도용하는 불법행위를 원천적으로 방지할 수 있다는 뛰어난 효과가 있다.

또한, 본 발명에 의하면, 사용자가 인터넷을 통해 서비스를 제공받기 위해 선행하였던 종래의 회원 가입, 아이디와 패스워드의 입력, 회원 탈퇴등의 번거로운 절차를 대체하여 보다 안전하고 용이하게 인터넷상의 서비스를 제공받을 수 있다는 뛰어난 효과가 있다.

(57) 청구의 범위

청구항 1.

전자 신원확인 증명서들을 유일하게 구분할 수 있는 전자 신원확인 증명서 고유번호;

전자 신원확인 증명서를 유효하게 사용할 수 있는 기간을 결정하는 전자 신원확인 증명서 유효 기간;

전자 신원확인 증명서를 발급한 전자 신원확인 증명서 발급장치에 대한 정보;

전자 신원확인 증명서의 사용자의 신원정보; 및

전자 신원확인 증명서를 사용할 사용차측 서버에 관한 정보를 구비하는 것을 특징으로 하는 전자 신원확인 증명서.

청구항 2.

제 1 항에 있어서,

상기 사용자에 대한 성인 인증 정보를 추가로 구비하는 것을 특징으로 하는 전자 신원확인 증명서.

청구항 3.

제 1 항에 있어서,

전자 신원확인 증명서를 발급한 전자 신원확인 증명서 발급장치의 전자 서명을 추가로 구비하는 것을 특징으로 하는 전자 신원확인 증명서.

청구항 4.

서비스 제공장치에 의해 작성된 전자 계약서들을 유일하게 구분할 수 있는 전자 계약서 고유번호;

전자 신원확인 증명서를 유효하게 사용할 수 있는 기간을 결정하는 전자 계약서의 유효 기간;

전자 계약서 작성 시에 사용자가 서비스 제공장치에 제공한 사용자 신원정보;

전자 계약서를 작성한 서비스 제공장치에 관한 정보;

전자 계약서를 체결한 서비스 제공장치 내에서 유일하게 사용자를 구분할 수 있는 사용자 ID;

서비스 제공장치의 개인정보보호정책 혹은 사용자가 서비스 제공장치 시스템에서 사용할 수 있는 서비스의 범위 등을 기술한 보안 정책; 및

사용자와 서비스 제공장치가 전자 계약서 작성 시에 협상하고 결정한 계약 내용을 구비하는 것을 특징으로 하는 전자 계약서.

청구항 5.

제 4 항에 있어서,

전자 계약서의 소유자를 증명하는 전자 계약서 소유자 정보를 추가로 구비하는 것을 특징으로 하는 전자 계약서.

청구항 6.

제 4 항에 있어서,

전자 계약서의 실효성을 확보하기 위한 서비스 제공장치의 전자서명을 추가로 구비하는 것을 특징으로 하는 전자 계약서.

청구항 7.

인터넷 상에서 사용자의 신원을 증명하고 보장하기 위한 전자 신원확인 증명서를 발급하는 전자 신원확인 증명서 발급장치;

사용자의 전자 신원확인 증명서에 기반하여 사용자와 전자 계약서를 작성하고 사용자에게 서비스를 제공하는 서비스 제공장치; 및

사용자와 전자 계약서가 작성된 서비스 제공장치로부터 서비스를 받기위한 사용자측 서버를 구비하는 것을 특징으로 하는 신원정보 관리시스템.

청구항 8.

제 7 항에 있어서,

상기 신원확인 증명서 발급장치는 사용자의 전자 신원확인 증명서 발급요청을 접수하는 요청 접수부;

사용자 신원정보를 기록하는 신원정보 저장부;

사용자의 요청에 따라 상기 등록된 신원정보에 근거하여 사용자 전자 신원확인 증명서를 발급하는 전자 신원확인 증명서 발급부;

사용자가 전자 신원확인 증명서 발급장치에 서비스를 요청하였을 때 상기 사용자를 인증하는 사용자 인증부;

상기 서비스 제공장치에 의해 특정 사용자의 전자 신원확인 증명서에 대한 검증 요청을 접수하였을 때, 상기 전자 신원확인 증명서의 유효성 여부를 검증하는 전자 신원확인 증명서 검증부를 구비하는 것을 특징으로 하는 신원정보 관리시스템.

청구항 9.

제 7 항에 있어서,

상기 서비스 제공장치는 사용자에게 재화 및 용역을 제공하기 위한 서비스 공급부;

사용자가 제시한 전자 계약서를 검증하는 전자 계약서 검증부;

전자 계약서가 작성되지 않은 사용자에 대하여 전자 계약서를 작성하기 위한 전자 계약서 작성부;

상기 전자 계약서 작성부에서 작성된 전자계약서를 저장하는 전자 계약서 저장부;

상기 전자 계약서에 의거하여 사용자의 신원정보를 보호하는 사용자 정보 보호부;

상기 전자 계약서에 의거하여 사용자에 대한 서비스 제공 범위를 결정하는 서비스 접근 제어부;

전자 계약서 작성시에 사용자가 제시한 전자 신원확인 증명서의 유효성을 확인하는 전자 신원확인 증명서 확인부; 및

전자 계약서에 포함된 내용과 서비스 제공장치의 정책에 따라 전자 계약서를 관리하는 전자 계약서 관리부를 구비하는 것을 특징으로 하는 신원정보 관리시스템.

청구항 10.

제 7 항에 있어서,

사용자측 서버는 전자 신원확인 증명서 발급장치에서 발급한 전자 신원확인 증명서의 유효성을 확인하는 전자 신원확인 증명서 확인부;

전자 신원확인 증명서 발급장치로부터 발급받은 전자 신원확인 증명서를 저장하고 관리하는 전자 신원확인 증명서 저장부;

사용자에게 전자 신원확인 증명서와 전자 계약서에 관련된 정보를 제공하는 정보 처리부;

상기 사용자측 서버의 사용 주체를 확인하기 위한 사용자 인증부;

서비스 제공장치에서 작성한 전자 계약서의 유효성을 확인하는 전자 계약서 확인부;

서비스 제공장치에서 작성한 전자 계약서를 저장하고 관리하는 전자 계약서 저장부를 구비하는 것을 특징으로 하는 신원정보 관리시스템.

청구항 11.

신원확인 증명서 발급장치에서 사용자에게 전자 신원확인 증명서를 발급하는 제 1 단계;

사용자가 전자 신원확인 증명서를 제시하여 서비스 제공장치에 서비스를 요청하면, 상기 서비스 제공장치는 사용자와 전자 계약서를 작성한 적이 없는 경우 전자 계약서를 작성하는 제 2 단계; 및

전자 계약서가 이미 존재하거나, 새롭게 작성한 경우에 서비스 제공장치로부터 서비스를 제공받는 제 3 단계로 구성되는 것을 특징으로 하는 인터넷 공간에서의 신원정보를 이용한 서비스 제공방법.

청구항 12.

제 11 항에 있어서,

상기 제 1 단계는 웹브라우저를 통하여 전자 신원확인 증명서 발급장치에 접속하는 단계;

사용자의 인증을 위하여 보안정보를 제시하고 사용자 인증을 받는 단계;

정상적으로 사용자 인증이 된 경우, 전자 신원확인 증명서 발급에 필요한 사용자의 신원정보를 입력하는 단계; 및

전자 신원확인 증명서를 사용자측 서버로 전달하는 단계로 구성되는 것을 특징으로 하는 인터넷 공간에서의 신원정보를 이용한 서비스 제공방법.

청구항 13.

제 11 항에 있어서,

상기 제 2 단계는 사용자측 서버로 개인정보보호정책을 포함한 전자 계약서에 포함될 계약 내용을 전달하고 전자 계약서 작성에 필요한 전자 신원확인 증명서 및 사용자의 신원정보를 요청하는 단계;

전달받은 서비스 제공장치의 개인정보보호정책이 사용자의 신원정보 관리 지침에 위배되지 않는지 여부를 검사하는 단계;

신원정보 관리 지침에 위배되지 않는 경우 전자 계약서의 작성에 필요한 사용자의 신원정보 및 전자 신원확인 증명서를 서비스 제공장치로 전달하는 단계;

상기 사용자의 신원정보를 전송받은 서비스 제공장치에서 전자 신원확인 증명서를 검증하고, 전자 계약서를 작성 및 서명하는 단계; 및

상기 작성된 전자 계약서를 사용자측 서버로 전달하는 단계로 구성되는 것을 특징으로 하는 인터넷 공간에서의 신원정보를 이용한 서비스 제공방법.

청구항 14.

제 11 항에 있어서,

상기 제 3 단계는 전자계약서를 서비스 제공장치로 전달하는 단계;

상기 전달받은 전자 계약서의 유효성을 검증하는 단계;

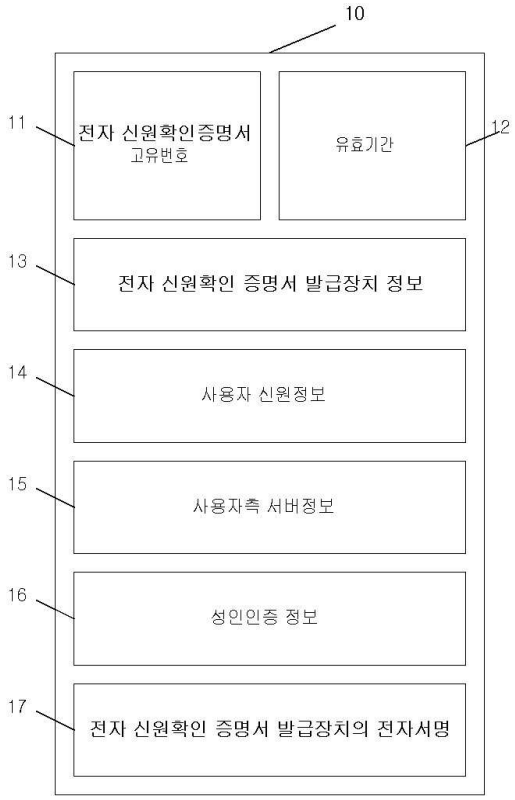
전자 계약서가 유효한 경우 사용자에 대한 사용자를 인증하는 단계;

상기 전자 계약서를 분석하여 인증된 사용자가 요청한 서비스에 대한 서비스 권한을 갖고 있는지 검사하는 단계;

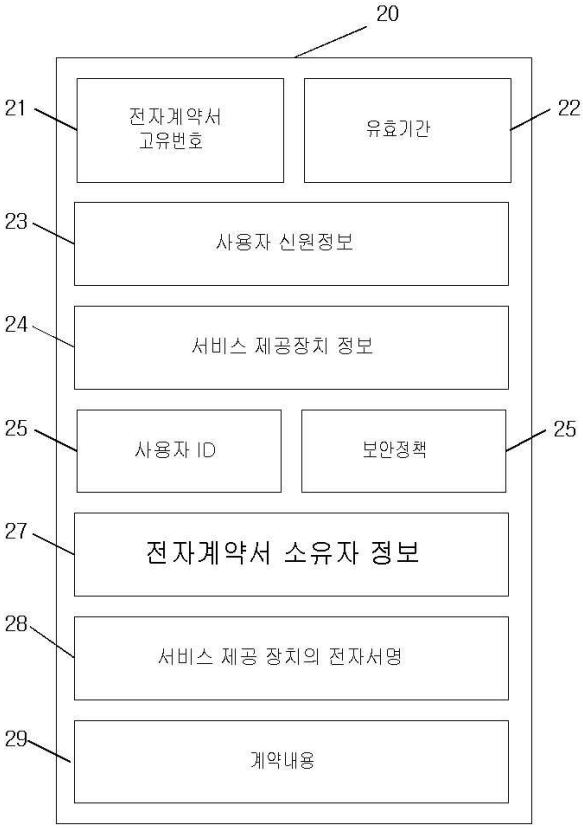
상기 사용자가 서비스 권한을 갖는 경우 사용자가 요청한 서비스를 제공하는 단계로 구성되는 것을 특징으로 하는 인터넷 공간에서의 신원정보를 이용한 서비스 제공방법.

도면

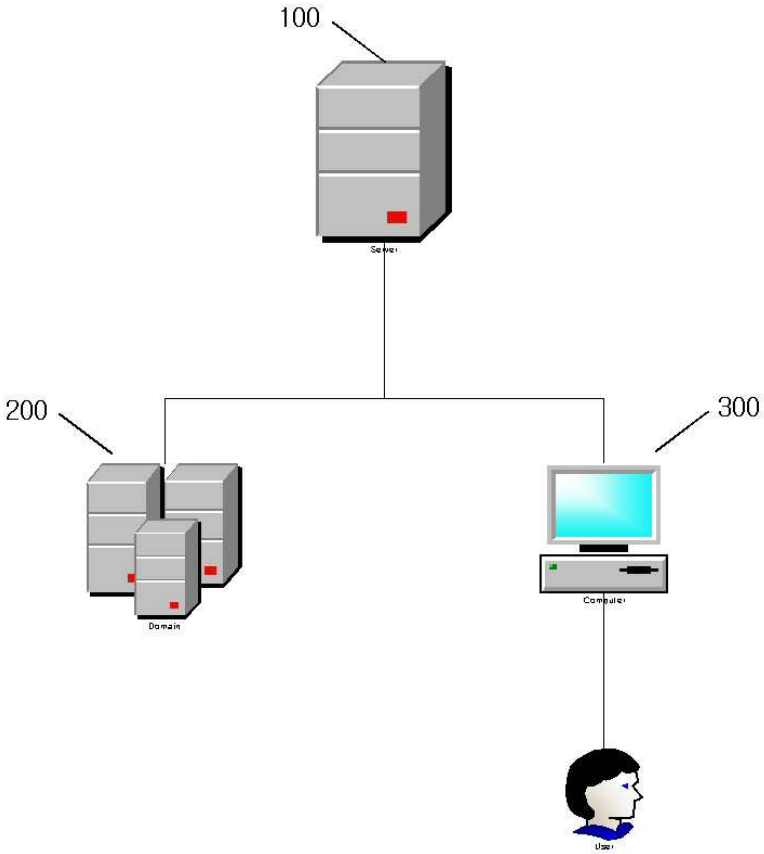
도면1



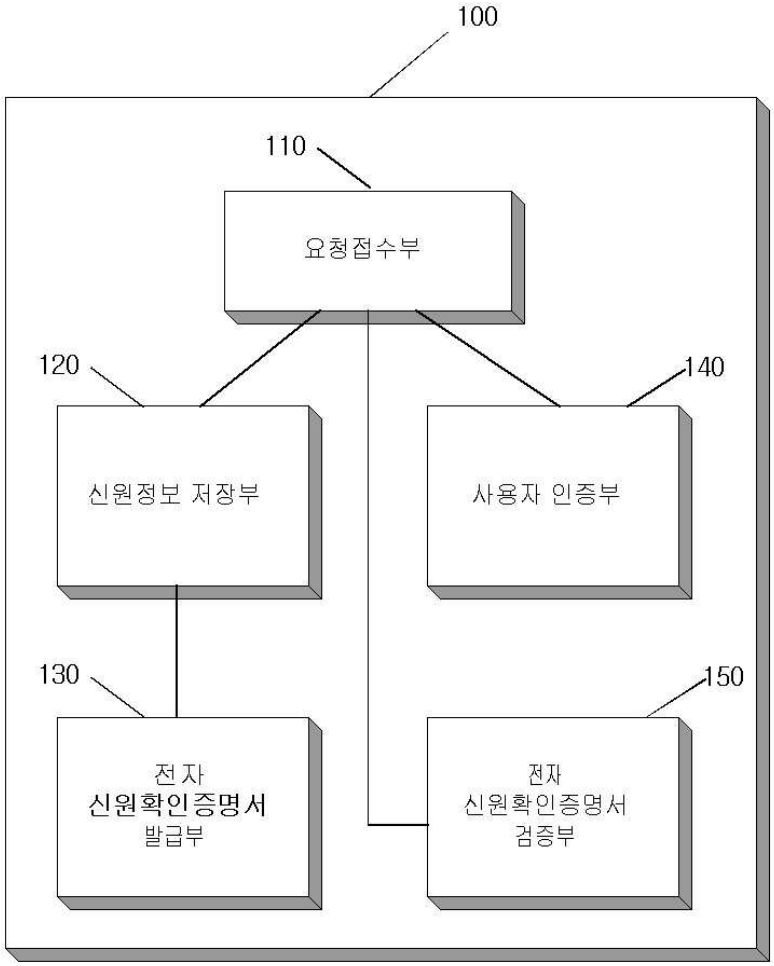
도면2


20
21
전자계약서
고유번호
유효기간
22
23
사용자 신원정보
24
서비스 제공장치 정보
25
사용자 ID
보안정책
25
27
전자계약서 소유자 정보
28
서비스 제공 장치의 전자서명
29
계약내용

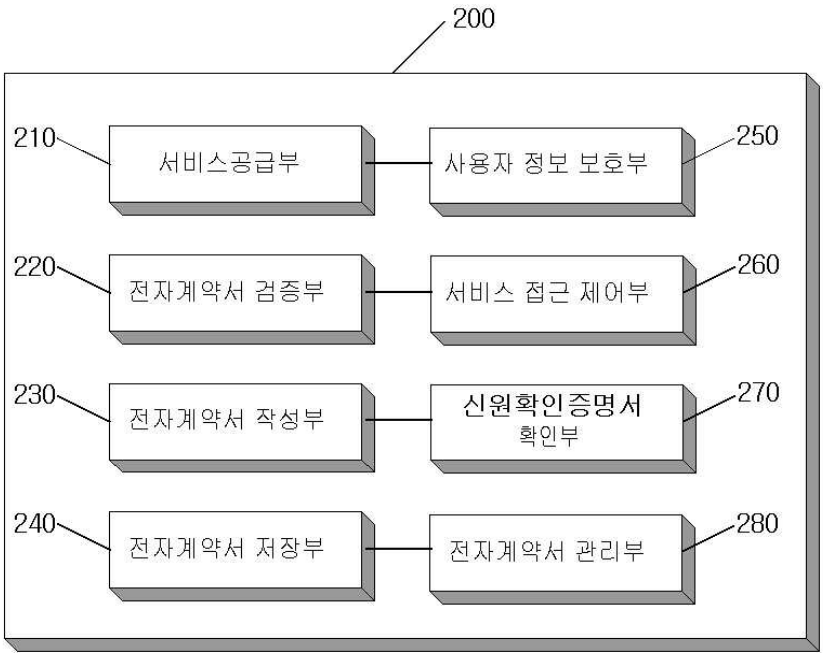
도면3


100
200
300
Server
Domain
Computer
User

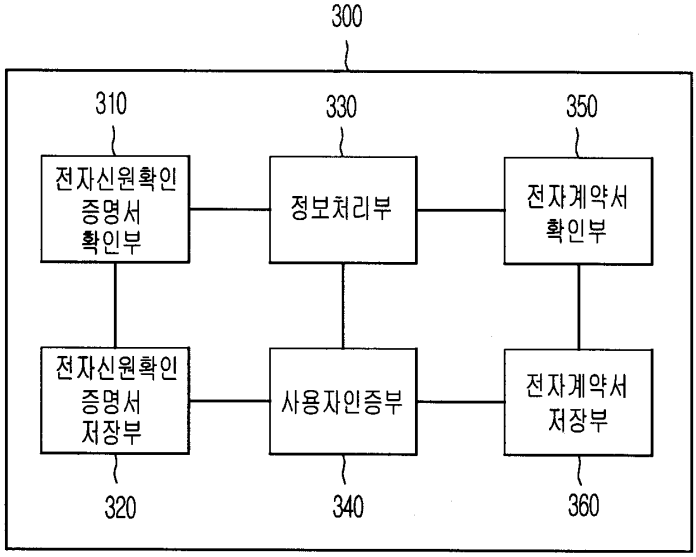
도면4


100
110
요청접수부
120
신원정보 저장부
140
사용자 인증부
130
전자
신원확인증명서
발급부
150
전자
신원확인증명서
검증부

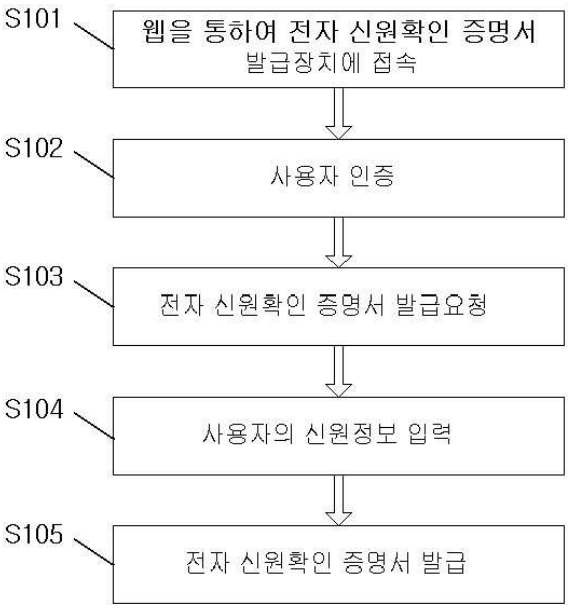
도면5


200
210
서비스공급부
사용자 정보 보호부
250
220
전자계약서 검증부
서비스 접근 제어부
260
230
전자계약서 작성부
신원확인증명서
확인부
270
240
전자계약서 저장부
전자계약서 관리부
280

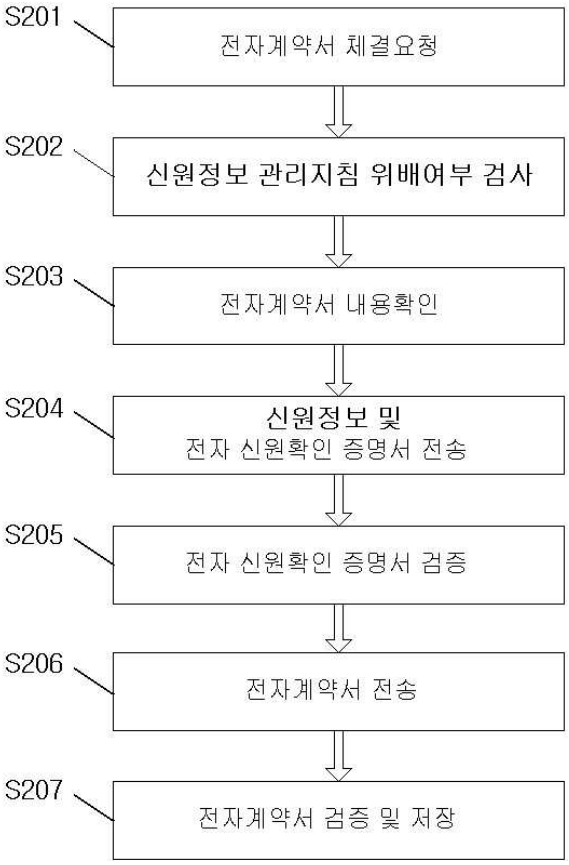
도면6


300
310
330
350
전자신원확인 증명서 확인부
정보처리부
전자계약서 확인부
전자신원확인 증명서 저장부
사용자인증부
전자계약서 저장부
320
340
360

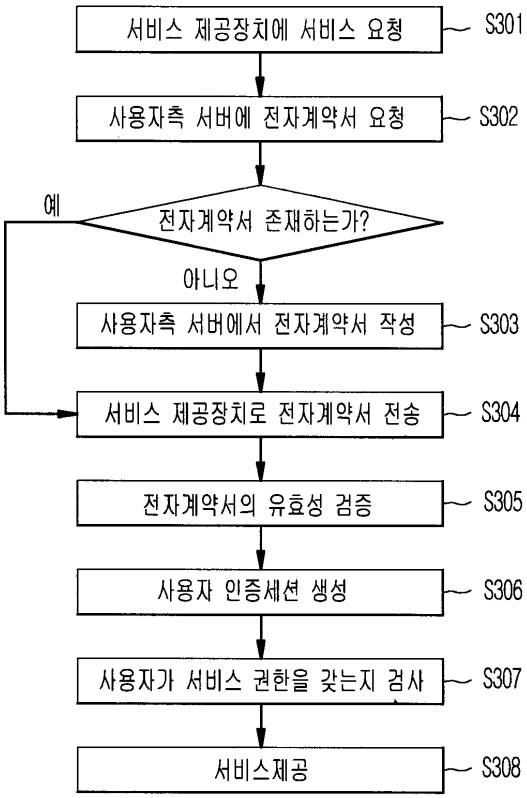
도면7


S101
웹을 통하여 전자 신원확인 증명서 발급장치에 접속
S102
사용자 인증
S103
전자 신원확인 증명서 발급요청
S104
사용자의 신원정보 입력
S105
전자 신원확인 증명서 발급

도면8


S201
전자계약서 체결요청
S202
신원정보 관리지침 위배여부 검사
S203
전자계약서 내용확인
S204
신원정보 및
전자 신원확인 증명서 전송
S205
전자 신원확인 증명서 검증
S206
전자계약서 전송
S207
전자계약서 검증 및 저장

도면9


서비스 제공장치에 서비스 요청
S301
사용자측 서버에 전자계약서 요청
S302
예
전자계약서 존재하는가?
아니오
사용자측 서버에서 전자계약서 작성
S303
서비스 제공장치로 전자계약서 전송
S304
전자계약서의 유효성 검증
S305
사용자 인증세션 생성
S306
사용자가 서비스 권한을 갖는지 검사
S307
서비스제공
S308