(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0085143
(43) 공개일자 2016년07월15일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/3263 (2013.01)
H04L 9/3247 (2013.01)
(21) 출원번호 10-2015-0002152
(22) 출원일자 2015년01월07일
심사청구일자 없음

(71) 출원인
주식회사 케이티
경기도 성남시 분당구 불정로 90(정자동)
(72) 발명자
박재성
서울특별시 서대문구 홍제내길 168, 101동 902호 (홍제동, 남양아파트)
김경남
경기도 의왕시 왕곡로 56, 101동 401호 (왕곡동, 충무아파트)
(뒷면에 계속)
(74) 대리인
특허법인필앤온지

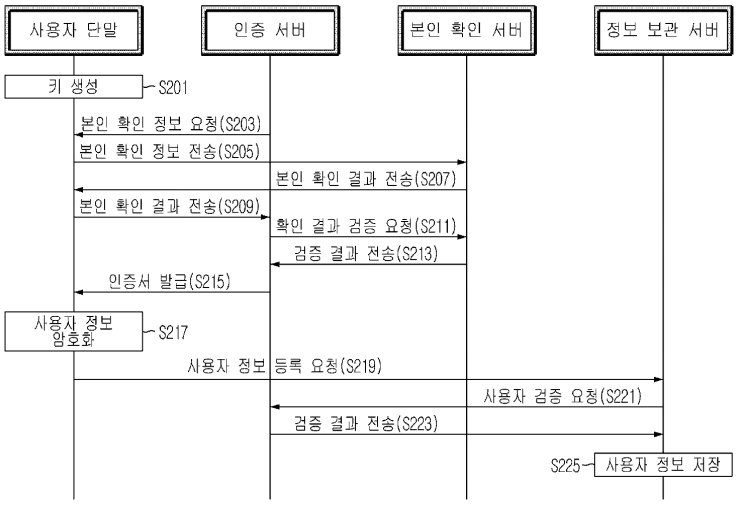
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **익명 서비스 제공 방법 및 사용자 정보 관리 방법 및 이를 위한 시스템**

(57) 요 약

본 발명은 사용자의 개인정보를 노출하지 않고 사용자를 인증하여 온라인 서비스를 제공하는 익명 서비스 제공 시스템 및 방법에 관한 것이다. 본 발명에 따른 사용자의 익명성을 유지하면서 온라인 서비스를 제공하는 시스템은, 익명의 인증정보에 포함된 익명 아이디를 복호화하여 이 익명 아이디에서 사용자 인증서를 추출하며, 상기 사용자 인증서를 검증하고 사용자의 공개키를 이용하여 상기 사용자의 전자 서명을 검증하는 인증 서버; 및 상기 사용자의 단말로부터 수신한 익명 아이디와 전자 서명이 포함된 익명의 인증정보를 상기 인증 서버로 전송하여 상기 사용자의 검증을 상기 인증 서버로 요청하고, 상기 인증 서버로부터 검증 성공 결과를 수신하면 상기 사용자가 요청한 서비스를 상기 사용자의 단말로 제공하는 서비스 서버를 포함한다.

대 표 도



(72) 발명자

김봉기

충청북도 청주시 흥덕구 대농로 17, 108동 2304호 (복대동, 지웰시티1차아파트)

박성철

서울특별시 관악구 봉천로17길 31-17, 403호 (봉천동, 청산주택)

명 세 서

청구범위

청구항 1

사용자의 익명성을 유지하면서 온라인 서비스를 제공하는 시스템으로서,

익명의 인증정보에 포함된 익명 아이디를 복호화하여 이 익명 아이디에서 사용자 인증서를 추출하며, 상기 사용자 인증서를 검증하고 사용자의 공개키를 이용하여 상기 사용자의 전자 서명을 검증하는 인증 서버; 및

상기 사용자의 단말로부터 수신한 익명 아이디와 전자 서명이 포함된 익명의 인증정보를 상기 인증 서버로 전송하여 상기 사용자의 검증을 상기 인증 서버로 요청하고, 상기 인증 서버로부터 검증 성공 결과를 수신하면 상기 사용자가 요청한 서비스를 상기 사용자의 단말로 제공하는 서비스 서버;를 포함하는 익명 서비스 제공 시스템.

청구항 2

제 1 항에 있어서,

상기 익명 아이디에는, 상기 사용자 인증서, 상기 서비스 서버의 도메인 및 랜덤값이 포함된 데이터가 상기 인증 서버의 공개키로 암호화되고,

상기 인증 서버는, 상기 인증 서버의 개인키로 상기 익명 아이디를 복호화한 후에, 복호화된 익명 아이디에 포함된 사용자 인증서를 검증하는 것을 특징으로 하는 익명 서비스 제공 시스템.

청구항 3

제 1 항에 있어서,

상기 서비스 서버는, 상기 서비스 서버의 인증서와 전자 서명이 포함된 서버 인증정보를 상기 인증 서버로 전송하고,

상기 인증 서버는, 상기 서버 인증정보에 포함된 서비스 서버의 인증서와 전자 서명을 검증하여 상기 서비스 서버의 검증을 수행한 후에, 상기 사용자 인증서와 상기 사용자의 전자 서명을 검증하는 것을 특징으로 하는 익명 서비스 제공 시스템.

청구항 4

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 인증 서버는,

상기 사용자의 단말로부터 인증서 발급을 요청받아 상기 사용자의 본인을 인증한 후 인증에 성공하면 상기 사용자 인증서를 상기 사용자의 단말로 발급하는 것을 특징으로 하는 익명 서비스 제공 시스템.

청구항 5

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 익명 아이디는 인증을 시도할 때마다, 상기 사용자의 단말에서 각기 다르게 생성되는 것을 특징으로 하는 익명 서비스 제공 시스템.

청구항 6

사용자의 익명성을 유지하면서 사용자에게 온라인 서비스를 제공하는 익명 서비스 제공 방법에 있어서,

서비스 서버가 사용자의 단말로부터 서비스를 요청받는 단계;

상기 서비스 서버가 상기 사용자의 단말로 인증 정보를 요청하고, 익명 아이디와 상기 사용자의 전자 서명이 포함된 익명의 인증정보를 상기 사용자의 단말로부터 수신하는 단계;

상기 서비스 서버가 상기 익명의 인증정보를 인증 서버로 전송하여, 상기 사용자의 검증을 요청하는 단계;

상기 인증 서버가 상기 익명 아이디를 복호화하여 이 익명 아이디에 포함된 사용자 인증서를 검증하고, 상기 사용자의 공개키를 이용하여 상기 사용자의 전자 서명을 검증하는 단계; 및

상기 서비스 서버가 상기 인증 서버로부터 사용자 검증 결과를 수신하고, 이 검증 결과가 성공에 해당하면, 상기 사용자에 대한 인증을 성공 처리하는 단계;를 포함하는 익명 서비스 제공 방법.

청구항 7

제 6 항에 있어서,

상기 익명 아이디에는, 상기 사용자의 사용자 인증서, 상기 서비스 서버의 도메인 및 랜덤값이 포함된 데이터가 상기 인증 서버의 공개키로 암호화되어 기록되고,

상기 검증하는 단계는,

상기 인증 서버가 상기 인증 서버의 개인키로 상기 익명 아이디를 복호화한 후에, 복호화된 익명 아이디에 포함된 사용자 인증서를 검증하는 것을 특징으로 하는 익명 서비스 제공 방법.

청구항 8

제 6 항에 있어서,

상기 검증을 요청하는 단계는, 상기 서비스 서버가 상기 서비스 서버의 인증서와 전자 서명이 포함된 서버 인증정보를 상기 인증 서버로 전송하는 단계;를 포함하고,

상기 검증하는 단계는,

상기 인증 서버가, 상기 서버 인증정보에 포함된 서비스 서버의 인증서와 전자 서명을 검증하여 서비스 서버의 검증을 수행한 후에, 상기 익명 아이디와 상기 사용자의 전자 서명을 검증하는 것을 특징으로 하는 익명 서비스 제공 방법.

청구항 9

제 6 항 내지 제 8 항 중 어느 한 항에 있어서,

상기 서비스를 요청받는 단계 이전에,

상기 인증 서버가, 상기 사용자의 단말로부터 인증서 발급을 요청받는 단계; 및

상기 인증 서버가 본인 확인 서버를 통해 상기 사용자의 본인을 인증하고, 인증에 성공하면 상기 사용자 인증서를 상기 사용자의 단말로 발급하는 단계;를 더 포함하는 것을 특징으로 하는 익명 서비스 제공 방법.

청구항 10

사용자 정보를 관리하는 방법에 있어서,

서비스 서버가 상기 사용자의 단말로 사용자 정보를 요청하는 단계;

정보 보관 서버가 상기 사용자의 인증정보가 포함된 접근 권한 변경 요청 메시지를 상기 사용자의 단말로부터 수신하는 단계;

상기 정보 보관 서버가, 상기 사용자의 인증정보에 대한 검증을 진행하는 단계;

상기 정보 관리 서버가, 상기 사용자의 인증정보에 대한 검증에 성공하면 사용자 정보로 접근할 수 있는 참조 링크를 상기 사용자의 단말로 전송하는 단계; 및

상기 정보 보관 서버가, 상기 참조 링크로 접속한 서버로 상기 사용자 정보를 제공하는 단계;를 포함하는 사용자 정보 관리 방법.

청구항 11

제 10 항에 있어서,

상기 정보 보관 서버가, 상기 사용자 정보를 제공받는 서버의 공개키로 암호화된 상기 사용자 정보를 보관하는 단계;를 포함하고,

상기 사용자 정보를 제공하는 단계는, 상기 정보 보관 서버가 상기 암호화된 사용자 정보를 상기 참조 링크로 접속한 서버로 제공하는 것을 특징으로 하는 사용자 정보 관리 방법.

청구항 12

제 11 항 또는 제 12 항에 있어서,

상기 사용자 정보를 제공하는 단계는,

상기 정보 보관 서버가, 상기 참조 링크로 접속한 서버의 정보 접근 권한을 확인하고, 접근 허용된 서버인 경우에 상기 사용자 정보를 제공하는 것을 특징으로 하는 사용자 정보 관리 방법.

청구항 13

제 11 항 또는 제 12 항에 있어서,

상기 검증을 진행하는 단계는,

상기 정보 보관 서버가 상기 사용자의 인증정보를 인증 서버로 전송하는 단계; 및

상기 인증 서버가, 상기 인증정보에 포함된 사용자 인증서를 검증하고 사용자의 전자 서명을 검증하고 이 검증 결과를 상기 정보 보관 서버로 전송하는 단계;를 포함하는 것을 특징으로 하는 사용자 정보 관리 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 익명 기반으로 온라인 서비스를 제공하는 시스템에 관한 것으로서, 더욱 상세하게는 사용자의 개인정보를 노출하지 않고 사용자를 인증하여 온라인 서비스를 제공하는 익명 서비스 제공 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷망의 보급으로 인하여, 다양한 온라인 서비스가 개시되었다. 또한, 웹 사이트에서는 사용자에게 특별한 웹 서비스를 제공하기 위하여, 사용자를 인증하고 인증에 성공한 사용자를 위한 서비스를 제공하기도 한다.

[0003] 이러한 웹 사이트에서는 사용자를 인증하기 위하여, 주민등록번호와 성명을 이용한 인증방법을 사용하고 있으며, 또한 아이디와 패스워드를 이용하여 사용자를 인증하고 있다.

[0004] 그런데 주민등록번호를 이용한 방식은 사용자 고유 정보가 외부에 노출되는 보안상의 문제점이 있으며, 게다가 아이디와 패스워드를 이용하는 방식은 아이디와 패스워드를 사이트별로 관리해야 되는 사용자의 번거로움을 유발하는 문제점이 있다.

[0005] 한편, 이러한 문제점을 착안하여, 아이핀(I-PIN)을 이용한 인증 방식과 공인인증서를 이용한 사용자 인증 방식이 개시되었다. 아래의 특허문헌은 전자 지갑과 아이핀을 활용한 신원확인 시스템에 관해서 개시한다.

[0006] 그런데 아이핀을 이용한 인증방식은 주민등록번호 대신에 사용자에게 부여한 고유 정보(즉, 아이핀)를 이용하는 기법으로서, 웹 사이트가 해킹된 경우에 사용자의 정보(예컨대, 성명, 전화번호, 주소, 아이핀 식별정보 등)가 해커에게 고스란히 노출될 뿐만 아니라 상기 아이핀 식별정보를 이용하여 타 사이트의 사용자의 사용 이력이 노출될 수 있는 문제점이 있다. 즉, 아이핀을 이용한 인증방식은 익명성을 완전하게 보장하지 못하는 문제점이 있다.

[0007] 또한, 공인인증서를 이용한 인증방식은 공인인증서에 사용자 이름과 공개키가 노출되어 사용자 추적이 가능한 구조로서, 사용자의 온라인 활동에 대한 익명성을 보장하지 못하는 문제점이 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 한국공개특허공보 제10-2010-0071679호

발명의 내용

해결하려는 과제

[0009] 본 발명은 이러한 문제점을 해결하기 위하여 제안된 것으로, 사용자 정보를 요구하지 않고 익명성을 보장하여 사용자를 인증하는 익명 서비스 제공 방법 및 이를 위한 시스템을 제공하는데 그 목적이 있다.

[0010] 또한, 본 발명은 사용자 정보의 이용이 허용된 사이트에게만 제공되도록 개인정보를 관리하고 보호하는 사용자 정보 관리 방법 및 이를 위한 시스템을 제공하는데 다른 목적이 있다.

[0011] 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 실시예에 의해 보다 분명하게 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 특허 청구 범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

과제의 해결 수단

[0012] 상기 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 사용자의 익명성을 유지하면서 온라인 서비스를 제공하는 시스템은, 익명의 인증정보에 포함된 익명 아이디를 복호화하여 이 익명 아이디에서 사용자 인증서를 추출하며, 상기 사용자 인증서를 검증하고 사용자의 공개키를 이용하여 상기 사용자의 전자 서명을 검증하는 인증 서버; 및 상기 사용자의 단말로부터 수신한 익명 아이디와 전자 서명이 포함된 익명의 인증정보를 상기 인증 서버로 전송하여 상기 사용자의 검증을 상기 인증 서버로 요청하고, 상기 인증 서버로부터 검증 성공 결과를 수신하면 상기 사용자가 요청한 서비스를 상기 사용자의 단말로 제공하는 서비스 서버를 포함하는 것을 특징으로 한다.

[0013] 상기 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 사용자의 익명성을 유지하면서 사용자에게 온라인 서비스를 제공하는 익명 서비스 제공 방법은, 서비스 서버가 사용자의 단말로부터 서비스를 요청받는 단계; 상기 서비스 서버가 상기 사용자의 단말로 인증 정보를 요청하고, 익명 아이디와 상기 사용자의 전자 서명이 포함된 익명의 인증정보를 상기 사용자의 단말로부터 수신하는 단계; 상기 서비스 서버가 상기 익명의 인증정보를 인증 서버로 전송하여, 상기 사용자의 검증을 요청하는 단계; 상기 인증 서버가 상기 익명 아이디를 복호화하여 이 익명 아이디에 포함된 사용자 인증서를 검증하고, 상기 사용자의 공개키를 이용하여 상기 사용자의 전자 서명을 검증하는 단계; 및 상기 서비스 서버가 상기 인증 서버로부터 사용자 검증 결과를 수신하고, 이 검증 결과가 성공에 해당하면, 상기 사용자에 대한 인증을 성공 처리하는 단계를 포함하는 것을 특징으로 한다.

[0014] 상기 목적을 달성하기 위한 본 발명의 제 3 측면에 따른 사용자 정보 관리 방법은, 서비스 서버가 상기 사용자의 단말로 사용자 정보를 요청하는 단계; 정보 보관 서버가 상기 사용자의 인증정보가 포함된 접근 권한 변경 요청 메시지를 상기 사용자의 단말로부터 수신하는 단계; 상기 정보 보관 서버가, 상기 사용자의 인증정보에 대한 검증을 진행하는 단계; 상기 정보 관리 서버가, 상기 사용자의 인증정보에 대한 검증에 성공하면 사용자 정보로 접근할 수 있는 참조 링크를 상기 사용자의 단말로 전송하는 단계; 및 상기 정보 보관 서버가, 상기 참조 링크로 접속한 서버로 상기 사용자 정보를 제공하는 단계를 포함하는 것을 특징으로 한다.

발명의 효과

[0015] 본 발명은 사용자의 개인정보를 요구하지 않고 사용자를 익명으로 인증함으로써, 사용자의 익명성을 보장하고 사용자의 프라이버시를 보호하는 장점이 있다.

[0016] 또한, 본 발명은 사용자 정보 노출을 원천적으로 차단하고, 사용자 선택에 의해서만 사용자 정보를 지정된 웹 사이트에 제공함으로써, 사용자 정보의 노출을 최소화할 수 있는 이점이 있다.

[0017] 게다가, 본 발명은 익명 아이디를 자동적으로 생성하고, 이 익명 아이디와 서명값을 이용하여 사용자를 인증함으로써, 웹 사이트가 해킹되더라도 사용자의 온라인 활동에 대한 추적을 불가능하게 하는 장점이 있다.

도면의 간단한 설명

[0018] 본 명세서에 첨부되는 다음의 도면들은 본 발명의 바람직한 실시예를 예시하는 것이며, 발명을 실시하기 위한

구체적인 내용과 함께 본 발명의 기술사상을 더욱 이해시키는 역할을 하는 것이므로, 본 발명은 그러한 도면에 기재된 사항에만 한정되어 해석되어서는 아니 된다.

도 1은 본 발명의 일 실시예에 따른, 익명 서비스를 제공하고 사용자 정보를 관리하는 통신 시스템의 구성을 나타내는 도면이다.

도 2는 본 발명의 일 실시예에 따른, 통신 시스템에서 사용자 인증서를 발급하고 사용자 정보를 저장하는 방법을 설명하는 흐름도이다.

도 3은 본 발명의 일 실시예에 따른, 통신 시스템에서 익명으로 사용자를 인증하는 방법을 설명하는 흐름도이다.

도 4는 본 발명의 일 실시예에 따른, 통신 시스템에서 사용자의 정보를 필요한 곳에만 최소한으로 제공하는 방법을 설명하는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일 실시예를 상세히 설명하기로 한다.

[0020] 도 1은 본 발명의 일 실시예에 따른, 익명 서비스를 제공하고 사용자 정보를 관리하는 통신 시스템의 구성을 나타내는 도면이다.

[0021] 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 통신 시스템은 사용자 단말(10), 본인 확인 서버(20), 정보 보관 서버(30), 인증 서버(40) 및 다수의 서비스 서버(50-N)를 포함한다. 상기 사용자 단말(10)과 각각의 서버(20, 30, 40, 50-N)는 네트워크(60)를 통해 서로 통신한다. 여기서, 네트워크(60)는 유무선 광대역 인터넷망과 이동통신망을 포함하는 것으로서, 본 발명의 주지의 관용기술에 해당하므로 자세한 설명은 생략한다.

[0022] 사용자 단말(10)은 사용자 개인키와 사용자 공개키를 생성하고, 익명 아이디를 생성하여 익명 기반의 서비스를 수행한다. 상기 사용자 단말(10)은 익명 서비스 어플리케이션이 실행된 경우에, 개인키와 공개키를 생성하여 저장할 수 있다. 또한, 사용자 단말(10)은 사용자의 본인 인증을 1회 수행한 후에, 인증 서버(40)로부터 사용자 인증서를 발급받는다.

[0023] 한편, 사용자 단말(10)은 특정 서비스 서버(50-N)로 사용자 정보를 제공할 때, 정보 보관 서버(30)로 사용자의 공개키 또는 서비스 서버(50-N)의 공개키로 암호화된 사용자 정보를 등록하고, 정보 보관 서버(30)로부터 사용자 정보로 접근할 수 있는 참조 링크를 수신한 후에, 이 참조 링크를 서비스 서버(50-N)로 제공한다. 이러한 사용자 단말(10)은 이동통신단말, 데스크톱 컴퓨터, 노트북, 태블릿 컴퓨터 등을 포함하는 것으로서, 네트워크(60)를 통해 서버와 통신 가능한 장치라면 제한되지 않고 채택 가능하다.

[0024] 본인 확인 서버(20)는 사용자의 주민등록번호, 성명, 전화번호 등을 이용하여 사용자의 본인 인증을 수행하는 기능을 수행한다. 여기서, 본인 확인 서버(20)는 인증 서버(40)와 분리된 본인 인증 기관에 구축된 서버일 수 있다.

[0025] 정보 보관 서버(30)는 사용자의 성명, 생년월일, 집 주소, 전화번호, 이메일 주소 등과 같은 사용자 정보를 사용자별로 구분하여 저장한다. 상기 정보 보관 서버(30)는 사용자 정보를 서비스 서버(50-N)의 공개키 또는 사용자 공개키로 암호화된 사용자 정보를 저장한다. 또한, 정보 보관 서버(30)는 사용자 단말(10)로부터 권한 변경 요청을 수신하면, 사용자의 공개키 또는 서비스 서버(50-N)의 공개키로 암호화된 사용자 정보를 저장하고 저장된 사용자 정보로 접근할 수 있는 참조 링크를 생성하여 사용자 단말(10)로 전송한다. 상기 참조 링크에는 접근 허용된 서비스 서버(50-N)가 사용자 정보를 획득할 수 있는 링크 주소(예컨대, URL)가 포함된다. 상기 정보 보관 서버(30)는 상기 사용자 정보로 접근이 허용된 서비스 서버(50-N)의 도메인, 접근 허용 기간, 접근 허용 항목 등이 포함된 접근 권한 정보를 상기 사용자 단말(10)로부터 수신하여 저장한다. 또한, 정보 보관 서버(30)는 특정 서비스 서버(50-N)가 참조 링크로 접속할 경우, 상기 접근 권한 정보를 토대로 서비스 서버(50-N)가 접근이 허용된 서버인지 여부를 확인한 후, 접근이 허용된 경우에 암호화된 사용자 정보를 서비스 서버(50-N)로 제

공한다.

[0026] 서비스 서버(50-N)는 온라인 쇼핑몰 서비스, 금융 거래 서비스, 이메일 서비스 등과 같은 온라인 서비스를 제공하는 서버로서, 인증 서버(40)와 연동하여 익명 기반의 사용자 인증을 수행한 후에, 인증에 성공하면 해당 서비스를 사용자 단말(10)로 제공한다. 상기 서비스 서버(50-N)는 사용자 단말(10)로부터 익명 아이디와 사용자의 전자 서명이 포함된 익명의 사용자 인증정보를 수신한 경우, 이 사용자 인증정보를 인증 서버(40)로 전송하여, 사용자 검증을 요청한다. 또한, 서비스 서버(50-N)는 사용자 정보가 필요한 온라인 서비스를 사용자 단말(10)이 요청한 경우에, 사용자 단말(10)로 사용자 정보를 요청하고, 이 사용자 정보에 접근할 수 있는 참조 링크를 사용자 단말(10)로부터 수신한다. 게다가, 서비스 서버(50-N)는 상기 참조 링크를 토대로 직접 사용자 정보를 획득할 수 있으며, 또는 서비스 처리를 위해서 상기 참조 링크를 타 서비스 서버로 제공할 수 있다.

[0027] 인증 서버(40)는 익명 기반으로 사용자를 인증하는 기능을 수행한다. 상기 인증 서버(40)는 사용자가 본인 확인에 성공하면, 이 사용자의 단말(10)로 사용자 인증서를 발급하고 상기 사용자 인증서를 관리한다. 또한, 인증 서버(40)는 서비스 서버(50-N) 또는 정보 보관 서버(30)로부터 사용자 검증을 요청받으면, 사용자의 익명 아이디를 복호화하여 사용자 인증서를 검증하고 사용자의 전자 서명을 검증하여, 이 검증 결과를 해당 서버로 제공한다.

[0028] 도 2 내지 4를 참조한 설명을 통해, 본 발명에 따른 통신 시스템의 동작에 대해서 상세하게 설명한다.

[0029] 도 2는 본 발명의 일 실시예에 따른, 통신 시스템에서 사용자 인증서를 발급하고 사용자 정보를 저장하는 방법을 설명하는 흐름도이다.

[0030] 도 2를 참조하면, 사용자 단말(10)은 사용자의 공개키와 개인키를 생성한다(S201). 이때, 사용자 단말(10)은 어플리케이션에 포함된 키 생성 알고리즘에 따라, 상기 사용자의 공개키와 개인키를 생성할 수 있다. 그리고, 사용자 단말(10)은 서비스 서버(50-N)와 정보 보관 서버(30)에서 사용자를 식별하기 위해 이용되는 사용자 식별정보를 생성할 수 있다. 여기서, 임의의 문자열에 대한 해시값이 상기 사용자 식별정보로서 이용될 수 있다. 즉, 상기 사용자 식별정보는 사용자의 고유정보가 아니라, 사용자 정보와는 전혀 관련성이 없는 임의의 문자열이 이용된다. 예를 들면, 사용자의 성명, 생년월일 및 이동통신 전화번호를 연접하여 해시한 값으로 식별정보를 생성할 수 있다.

[0031] 이어서 인증 서버(40)는 본인 확인 정보를 요청하는 메시지를 사용자 단말(10)로 전송한다(S203). 이때, 인증 서버(40)는 본인 확인 서버(40)의 정보를 상기 메시지에 포함시킨다.

[0032] 그러면, 사용자 단말(10)은 사용자로부터 본인 확인 정보(예컨대, 본인인증 기관에서 요구하는 주민등록번호, 성명, 이동통신전화번호 등)를 입력받고, 이 본인 확인 정보를 본인 확인 서버(20)로 전송한다(S205). 그러면, 본인 확인 서버(40)는 상기 본인 확인 정보를 확인하여, 본인 확인 결과를 사용자 단말(10)로 전송한다(S207). 이어서, 사용자 단말(10)은 상기 본인 확인 결과를 인증 서버(40)로 전송한다(S209).

[0033] 다음으로, 인증 서버(40)는 사용자 단말(10)로부터 수신한 본인 확인 결과를 본인 확인 서버(20)로 전송하여, 상기 본인 확인 결과에 대한 검증을 요청한다(S211). 그러면, 본인 확인 서버(20)는 인증 서버(40)로부터 수신한 본인 확인 결과의 진위를 검증하고, 검증 결과를 인증 서버(40)로 전송한다(S213). 즉, 본인 확인 서버(20)는 상기 본인 확인 결과 위조되었는지 여부를 검증한다.

[0034] 이어서, 인증 서버(40)는 본인 확인 서버(20)로부터 수신한 검증 결과가 실패이거나 상기 본인 확인 결과가 실패이면, 사용자 단말(10)로 사용자 인증서 발급이 불가능함을 통보한다. 반면에, 인증 서버(40)는 본인 확인 서버(20)로부터 수신한 검증 결과가 성공이고 상기 본인 확인 결과도 성공이면, 사용자 정보가 전혀 기록되지 않은 사용자 인증서를 생성하고, 이 사용자 인증서를 사용자 단말(10)로 발급한다(S215). 그리고 인증 서버(40)는 사용자의 공개키, 상기 생성한 사용자 인증서, 사용자 식별정보 및 인증서 유효기간을 저장한다. 상기 인증서 유효기간은 사용자 인증서가 발급된 날짜에서부터 특정 날짜(예컨대, 1년)까지의 기간이 기록된다.

[0035] 사용자 단말(10)은 인증 서버(40)로부터 사용자 인증서가 수신되면, 이 사용자 인증서를 저장한다. 그리고 사용자 단말(10)은 사용자 정보를 안전한 장소에 보관하기 위하여, 상기 생성한 사용자 공개키를 이용하여 사용자 정보(즉, 성명, 생년월일, 주소, 전화번호 등)를 암호화한다(S217).

[0036] 이어서, 사용자 단말(10)은 S201 단계에서 생성한 사용자 개인키와 서명할 원본 메시지를 토대로, 사용자의 전자 서명을 생성한다. 이때, 사용자 단말(10)은 임의의 문자열인 랜덤값을 생성하고, 이 랜덤값과 정보 보관 서

버의 도메인, 서명 목적을 나타내는 데이터 및 사용자 인증서가 조합된 정보를 서명할 원본 메시지로 설정하고, 이 원본 메시지를 해시(hash) 함수에 적용하여 해시값을 생성한 후, 이 해시값을 상기 개인키로 암호화함으로써, 전자 서명을 생성할 수 있다.

[0037] 다음으로, 사용자 단말(10)은 상기 생성한 전자 서명, 암호화된 사용자 정보 및 상기 원본 메시지가 포함된 사용자 정보 등록 요청 메시지를 정보 보관 서버(30)로 전송한다(S219).

[0038] 그러면, 정보 보관 서버(30)는 상기 사용자 정보 등록 요청 메시지에 사용자 전자 서명과 원문 메시지를 추출하고, 상기 추출한 데이터(즉, 전자 서명, 원문 메시지)를 인증 서버(40)로 전송함으로써, 사용자 검증을 인증 서버(40)로 요청한다(S221).

[0039] 이어서, 인증 서버(40)는 상기 사용자 인증서의 유효성을 검증한다. 이때, 인증 서버(40)는 상기 원문 메시지에서 사용자 인증서를 추출한 후, 이 사용자 인증서의 유효기간이 남아있는지 여부를 확인하고, 인명 인증서가 폐기 목록에 등록되어 있는지 여부를 확인함으로써, 사용자 인증서의 유효성을 검증할 수 있다.

[0040] 그리고 인증 서버(40)는 사용자 전자 서명의 진위를 검증한다. 이때, 인증 서버(40)는 사용자 공개키, 상기 원문 메시지 및 전자 서명을 서명 검증 알고리즘에 인자로서 입력함으로써, 상기 전자 서명의 진위를 검증할 수 있다.

[0041] 다음으로, 인증 서버(40)는 사용자 검증 결과를 정보 보관 서버(30)로 전송한다(S223). 이때, 인증 서버(40)는 사용자 인증서의 유효성 검증에 실패하거나 사용자 전자 서명에 대한 검증에 실패하면 검증 실패 메시지를 정보 보관 서버(30)로 전송하고, 반면에 사용자 인증서의 유효성 검증과 사용자 전자 서명 검증에 모두 성공하면 검증 성공 메시지를 정보 보관 서버(30)로 전송한다.

[0042] 이어서, 정보 보관 서버(30)는 인증 서버(40)로부터 검증 실패 메시지를 수신하면, 사용자 단말(10)로 정보 보관을 실행할 수 없음을 통보한다. 반면에. 정보 보관 서버(30)는 인증 서버(40)로부터 검증 성공 메시지를 수신하면, 암호화 처리된 사용자 정보를 저장한다(S225).

[0043] 이렇게 정보 보관 서버(30)에 저장된 사용자 정보는 사용자만이 변경하거나 수정할 수 있다. 즉, 정보 보관 서버(30)에 저장된 사용자 정보는 사용자 단말(10)의 공개키를 통해 암호화되기 때문에, 타 사용자 또는 서버에서는 사용자 정보를 획득하더라도 해독하기가 불가능하고, 사용자 단말(10)에서 보관중인 개인키를 통해서만 해독이 가능하다.

[0044] 도 3은 본 발명의 일 실시예에 따른, 통신 시스템에서 익명으로 사용자를 인증하는 방법을 설명하는 흐름도이다.

[0045] 도 3을 참조하면, 사용자 단말(10)은 서비스 서버(50-N)로 접속하여, 메일 확인, 물품 구매, 금융 거래 등과 같은 온라인 서비스를 요청한다(S301). 그러면, 서비스 서버(50-N)는 임의의 랜덤값(Nonce)를 생성하고, 이 랜덤값이 포함된 인증정보 요청 메시지를 사용자 단말(10)로 전송한다(S303). 상기 랜덤값은 세션값, 시간정보 등 중에서 하나 이상을 포함할 수 있다.

[0046] 이어서, 사용자 단말(10)은 임의의 익명 아이디를 생성한다(S305). 이때, 사용자 단말(10)은 자체적으로 랜덤값을 생성하고, 상기 생성한 랜덤값, 상기 서비스 서버(50-N)의 도메인 및 사용자 인증서가 조합된 데이터를 인증 서버(40)의 공개키로 암호화하여 익명 아이디를 생성한다.

[0047] 그리고 사용자 단말(10)은 서명하고자 하는 원문 메시지와 사용자의 개인키를 이용하여, 사용자의 전자 서명을 생성한다(S307). 이때, 사용자 단말(10)은 서비스 서버(50-N)로부터 수신한 랜덤값, 서비스 서버(50-N)의 도메인 및 서명 목적을 나타내는 데이터(예컨대, LoginRequest)가 조합된 정보를 서명할 원문 메시지로 하여, 전자 서명을 생성할 수 있다.

[0048] 다음으로, 사용자 단말(10)은 암호화된 익명 아이디, 전자 서명 및 원문 메시지가 포함된 사용자 인증정보를 서비스 서버(50-N)로 전송한다(S309).

[0049] 그러면, 서비스 서버(50-N)는 서명 검증을 요청하는 원문 메시지를 해당 서비스 서버의 개인키로 암호화하여 서비스 서버(50-N)의 전자 서명을 생성한다(S311). 또한, 서비스 서버(50-N)는 자신이 보유중인 인증서(즉, 서비스 서버의 인증서), 서명 목적을 나타내는 데이터 및 서비스 서버의 도메인이 조합된 데이터를 서명할 원문 메시지로 설정할 수 있다. 그리고 서비스 서버(50-N)는 자체적으로 생성한 서버의 전자 서명 및 원문 메시지가 포

함된 서버 인증정보를 생성한다.

[0050] 다음으로, 서비스 서버(50-N)는 상기 서버 인증정보 및 상기 사용자 인증정보가 포함된 검증 요청 메시지를 인증 서버(40)로 전송한다(S313).

[0051] 이어서, 인증 서버(40)는 검증 요청 메시지에 포함된 서버 인증정보에서 서비스 서버(50-N)의 인증서를 검증하고, 서비스 서버(50-N)가 서명한 전자 서명에 대한 검증을 수행한다(S315). 즉, 인증 서버(40)는 서비스 서버(50-N)의 인증서의 유효성을 검증하고, 더불어 서비스 서버(50-N)가 서명한 전자 서명의 진위를 검증한다. 이때, 인증 서버(40)는 서비스 서버(50-N)의 전자 서명, 원문 메시지, 공개키를 서명 검증 알고리즘에 인자로서 입력하여, 상기 서비스 서버의 서명을 검증할 수 있다.

[0052] 이어서, 인증 서버(40)는 서비스 서버(50-N)의 인증에 성공하면, 사용자 인증정보에 포함된 익명 아이디를 인증 서버(40)의 개인키로 복호화한 후, 사용자 인증서를 추출한다. 다음으로, 인증 서버(40)는 상기 사용자 인증서와 사용자의 전자서명을 검증한다(S317). 상기 인증 서버(40)는 상기 사용자 인증서의 유효 기간의 만료되었는지 여부와 상기 사용자 인증서가 폐기되었는지 여부를 확인하여 사용자 인증서를 검증할 수 있다. 또한, 상기 인증 서버(40)는 사용자의 전자 서명, 사용자의 공개키 및 원문 메시지를 서명 검증 알고리즘의 인자로서 입력하여, 사용자의 서명을 검증할 수 있다.

[0053] 다음으로, 인증 서버(40)는 검증 결과를 정보 보관 서버(30)로 전송한다(S319). 이때, 인증 서버(40)는 서비스 서버(50-N)의 인증서의 유효성 검증, 서비스 서버(50-N)의 전자 서명 검증, 사용자 인증서의 유효성 검증, 사용자의 전자 서명 검증 중에서 어느 하라도 실패하면 검증 실패 메시지를 서비스 서버(50-N)로 전송하고, 상기 모든 검증에 성공하면 검증 성공 메시지를 서비스 서버(50-N)로 전송한다.

[0054] 이어서, 서비스 서버(50-N)는 인증 서버(40)로부터 수신한 검증 결과를 확인하고, 이 검증 결과에 따라 선택적으로 온라인 서비스를 사용자 단말(10)로 제공한다(S321, S323). 즉, 서비스 서버(50-N)는 인증 서버(40)로부터 검증 실패 메시지를 수신하면, 사용자 단말(10)로 인증 실패를 통보하고, 사용자 단말(10)이 요청한 서비스를 차단한다. 반면에, 서비스 서버(50-N)는 인증 서버(40)로부터 검증 성공 메시지를 수신하면, 사용자 단말(10)이 요청한 서비스를 실행하여 사용자 단말(10)로 상기 서비스를 제공한다.

[0055] 한편, 사용자 단말(10)은 상기 생성한 익명 아이디를 상기 서비스 서버(50-N)에 대한 유일한 아이디로 설정하여 보관할 수 있으며, 서비스 서버(50-N)는 상기 익명 아이디의 해시값을 사용자 단말(10)의 익명 아이디로서 관리할 수 있다. 또 다른 실시예에서, 사용자 단말(10)은 동일한 도메인이라도 매번 다르게 익명 아이디를 생성할 수 있다. 즉, 사용자 단말(10)은 서비스 서버(50-N)로 서비스를 요청할 때마다 매번 새로운 랜덤값을 생성하고, 매번 다른 익명 아이디를 생성하여 서비스를 요청할 수 있다.

[0056] 도 4는 본 발명의 일 실시예에 따른, 통신 시스템에서 사용자의 정보를 필요한 곳에만 최소한으로 제공하는 방법을 설명하는 흐름도이다.

[0057] 도 4에서는 서비스 서버1(50-1)이 사용자의 온라인 서비스를 제공하는 서버이며 사용자 정보가 불필요한 서버이고, 서비스 서버2(50-2)는 서비스 서버1(50-1)의 요청에 따라 특정 서비스를 제공하는 서버로서 서비스 수행을 위해서는 사용자 정보가 필요한 서버인 것으로 설명된다. 예컨대, 서비스 서버1(50-1)은 사용자 정보가 필요없이 쇼핑 결제를 수행할 수 있는 온라인 쇼핑몰이며, 서비스 서버2(50-2)는 사용자의 성명, 주소, 전화번호 등이 필요한 배송 업체 서버인 것으로 설명될 수 있다. 또한, 도 4에서는 서비스 서버1(50-1)이 도 3과 같은 절차를 통해서, 사용자의 익명 인증에 성공한 것으로 설명된다.

[0058] 도 4를 참조하면, 서비스 서버1(50-1)은 사용자 정보가 필요한 온라인 서비스를 사용자에게 제공하기 위하여, 사용자 단말(10)로 사용자 정보를 요청한다(S401). 이때, 서비스 서버(50-N)1은 사용자 정보가 필요한 서비스 서버2(50-2)의 도메인 정보 및 필요한 사용자 정보 항목(예컨대, 성명, 전화번호, 주소 등)을 사용자 단말(10)로 전송한다.

[0059] 이어서, 사용자 단말(10)은 인증 서버(40)와 통신하여 서비스 서버2(50-2)와 통신하여 서비스 서버2(50-2)의 공개키를 획득하거나, 사용자 단말의 어플리케이션에 저장된 서비스 서버2(50-2)의 공개키를 획득한다. 그리고 사용자 단말(10)은 정보 보관 서버(30)로 접속하여 사용자의 공개키로 암호화된 사용자 정보를 획득하거나, 사용자 단말(10)에 저장된 사용자 정보를 획득한다(S403). 이때, 사용자 단말(10)은 전자 서명을 생성하여 정보 보관 서버(30)로 전송하고, 정보 보관 서버(30)는 사용자 인증서의 유효성을 검증하고 또한 전자 서명을 검증한

후에 검증에 모두 성공한 경우에 사용자 단말(10)로 암호화된 사용자 정보를 전송할 수 있다.

[0060] 이어서, 사용자 단말(10)은 자체 저장중인 사용자의 개인키를 이용하여 암호화된 사용자 정보를 복호화한다. 한편, 사용자 단말(10)은 사용자로부터 직접적으로 사용자 정보를 입력받아, 사용자 정보를 획득할 수도 있으며, 이 경우 정보 보관 서버(30)로 접속하여 사용자 정보를 획득하는 과정과 사용자 정보를 복호화 과정이 생략된다.

[0061] 다음으로, 사용자 단말(10)은 사용자 정보를 상기 서비스 서버2(50-2)의 공개키를 이용하여 암호화한다(S405). 즉, 사용자 단말(10)은 상기 서비스 서버2(50-2)의 공개키를 이용해 암호키(대칭키)를 설정하고, 이렇게 설정된 암호키를 이용하여 사용자 정보를 암호화한다. 그리고 사용자 단말(10)은 서명하고자 하는 원문 메시지 및 사용자 개인키를 토대로 사용자의 전자 서명을 생성한다(S407). 이때, 사용자 단말(10)은 사용자 인증서, 서비스 서버2(50-2)의 도메인, 서명 목적을 나타내는 데이터(예컨대, Access)가 포함된 데이터를 원문 메시지로서 설정하여 사용자의 전자 서명을 생성할 수 있다. 다음으로, 사용자 단말(10)은 사용자 정보로 접근 허용한 서버의 도메인, 접근 허용 기간, 접근 허용 항목 등이 포함된 접근 권한 정보를 생성하고, 이 접근 권한 정보, 상기 암호화한 사용자 정보, 상기 생성한 전자 서명 및 원문 메시지가 포함된 접근 권한 변경 요청 메시지를 정보 보관 서버(30)로 전송한다(S409). 상기 접근 권한 정보는 사용자의 입력을 통해서 상기 사용자 단말(10)에서 생성될 수 있다.

[0062] 그러면, 정보 보관 서버(30)는 상기 접근 권한 변경 요청 메시지에서 전자 서명과 원문 메시지를 추출하고, 이 전자 서명과 원문 메시지를 인증 서버(40)로 전송함으로써, 사용자 검증을 인증 서버(40)로 요청한다(S411). 이어서, 인증 서버(40)는 원문 메시지에서 포함된 사용자 인증서를 확인하고, 사용자 인증서의 유효성(예컨대, 유효기간과 폐기 여부에 대한 유효성)을 확인한다. 그리고 인증 서버(40)는 사용자 전자 서명의 진위를 검증한다. 이어서, 인증 서버(40)는 사용자 검증 결과를 정보 보관 서버(30)로 전송한다(S413).

[0063] 다음으로, 정보 보관 서버(30)는 검증 결과로서 검증 성공 메시지를 인증 서버(40)로부터 수신하면, 서비스 서버2(50-2)의 공개키로 암호화된 사용자 정보를 저장하고, 이 사용자 정보에 대한 참조 링크(예컨대, URL)를 생성한다(S415). 바람직하게, 정보 보관 서버(30)는 상기 접근 권한 변경 요청 메시지에서 접근 권한 정보를 확인하고, 이 접근 권한 정보에 근거하여 상기 암호화된 사용자 정보에 대해 접근을 허용하는 서버와 접근 기간, 접근 허용 항목 등을 설정할 수 있다. 이어서, 정보 보관 서버(30)는 상기 참조 링크를 사용자 단말(10)로 전송한다(S417).

[0064] 그러면, 사용자 단말(10)은 서비스 서버1(50-1)에서 인증할 때 이용한 익명 아이디와 상기 참조 링크를 서비스 서버1(50-1)로 전송한다(S419). 다음으로, 서비스 서버1(50-1)은 서비스 서버2(50-2)로 상기 참조 링크를 전송하여, 서비스 처리를 서비스 서버2(50-2)로 요청한다(S421).

[0065] 그러면, 서비스 서버2(50-2)는 해당 참조 링크로 접속하여, 정보 보관 서버(30)로 사용자의 정보를 요청한다(S423). 바람직하게, 서비스 서버1(50-1)은 서비스 서버1(50-1)의 전자 서명을 생성하고 이 전자 서명을 서비스 서버2(50-2)로 전송할 수 있으며, 이 경우 서비스 서버2(50-1)는 인증 서버(40)와 연동하여 서비스 서버1(50-1)의 전자 서명에 대한 검증을 수행하고, 전자 서명에 대한 검증에 성공한 경우에 참조 링크로 접속할 수 있다.

[0066] 이어서, 정보 보관 서버(30)는 상기 참조 링크로 접속한, 서비스 서버2(50-2)가 해당 정보로의 접근이 허용된 서버인지 여부를 접근 권한 정보를 토대로 인증하고, 인증에 성공하면 서비스 서버2(50-2)의 공개키로 암호화된 사용자 정보를 서비스 서버2(50-2)로 전송한다(S425).

[0067] 이어서, 서비스 서버2(50-2)는 정보 보관 서버(30)로부터 수신한 사용자 정보를 자신의 개인키를 이용하여 복호화한다. 그리고 서비스 서버2(50-2)는 사용자 정보를 이용하여 서비스를 제공하고, 서비스 제공 결과를 서비스 서버1(50-1)로 통보한다.

[0068] 한편, 도 4에서 서비스 서버1(50-1)이 직접 참조 링크로 접속할 수도 있다. 즉, 서비스 서버1(50-1)은 사용자 정보가 필요한 서비스를 직접적으로 진행한 경우에, 사용자 단말(10)로부터 참조 링크를 수신하고, 이 참조 링크로 접속하여 정보 보관 서버(30)로부터 사용자 정보를 수신할 수도 있다. 이 경우, 사용자 단말(10)은 사용자 정보가 필요한 서버가 서비스 서버1(50-1)임을 확인하고, 이 서비스 서버1(50-1)의 공개키를 이용하여 사용자 정보를 암호화하고 정보 보관 서버(30)에 저장하고, 서비스 서버1(50-1)은 정보 보관 서버(30)로부터 수신한 암호화된 사용자 정보를 서비스 서버1(50-1)의 개인키를 이용하여 복호화한다.

[0069] 상술한 바와 같이, 본 발명은 사용자의 사용자 정보를 요구하지 않고 사용자를 익명으로 인증함으로써, 사용자의 익명성을 보장하고 사용자의 프라이버시를 보호한다. 또한, 본 발명은 사용자 정보 노출을 원천적으로 차단

하고, 사용자 선택에 의해서만 사용자 정보를 지정된 서비스 서버(50-N)로 제공함으로써, 사용자 정보의 노출을 최소화한다. 게다가, 본 발명은 익명 아이디를 자동적으로 생성하고, 이 익명 아이디를 이용하여 사용자를 인증함으로써, 웹 사이트가 해킹되더라도 사용자의 온라인 활동에 대한 추적을 불가능하게 한다.

[0070] 본 명세서는 많은 특징을 포함하는 반면, 그러한 특징은 본 발명의 범위 또는 특허청구범위를 제한하는 것으로 해석되어서는 안 된다. 또한, 본 명세서에서 개별적인 실시예에서 설명된 특징들은 단일 실시예에서 결합되어 구현될 수 있다. 반대로, 본 명세서에서 단일 실시예에서 설명된 다양한 특징들은 개별적으로 다양한 실시예에서 구현되거나, 적절히 결합되어 구현될 수 있다.

[0071] 도면에서 동작들이 특정한 순서로 설명되었으나, 그러한 동작들이 도시된 바와 같은 특정한 순서로 수행되는 것으로, 또는 일련의 연속된 순서, 또는 원하는 결과를 얻기 위해 모든 설명된 동작이 수행되는 것으로 이해되어서는 안 된다. 특정 환경에서 멀티태스킹 및 병렬 프로세싱이 유리할 수 있다. 아울러, 상술한 실시예에서 다양한 시스템 구성요소의 구분은 모든 실시예에서 그러한 구분을 요구하지 않는 것으로 이해되어야 한다. 상술한 프로그램 구성요소 및 시스템은 일반적으로 단일 소프트웨어 제품 또는 멀티플 소프트웨어 제품에 패키지로 구현될 수 있다.

[0072] 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(시디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다. 이러한 과정은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있으므로 더 이상 상세히 설명하지 않기로 한다.

[0073] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

부호의 설명

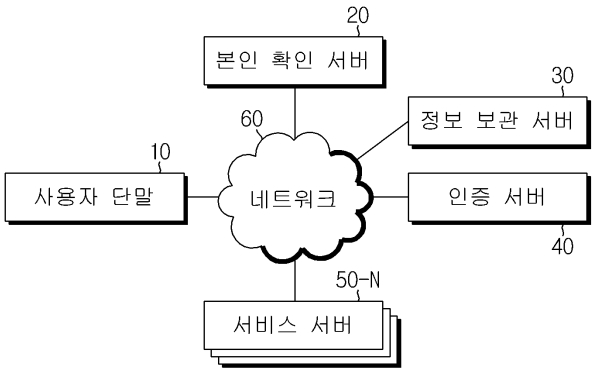
[0074] 10 : 사용자 단말 20 : 본인 확인 서버

30 : 정보 보관 서버 40 : 인증 서버

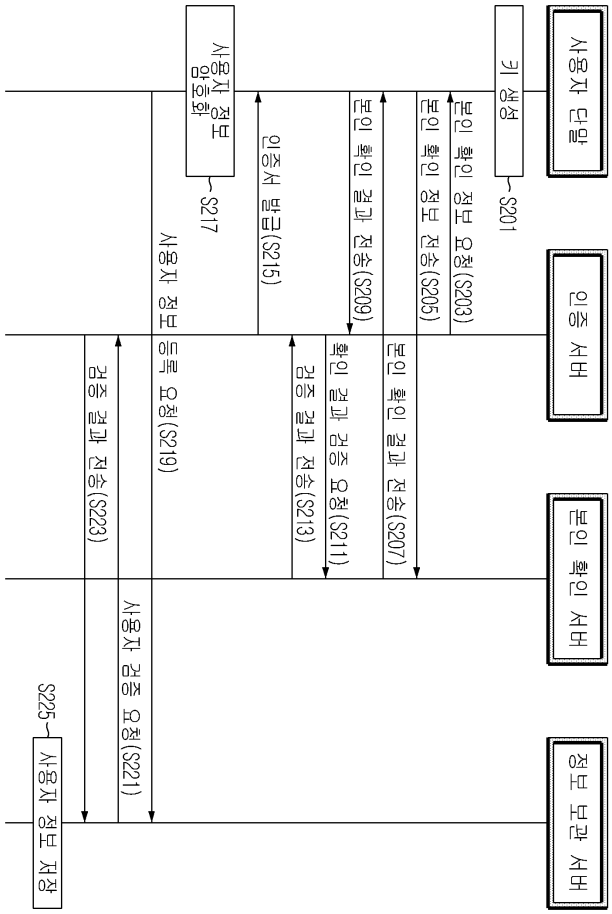
50 : 서비스 서버 60 : 네트워크

도면

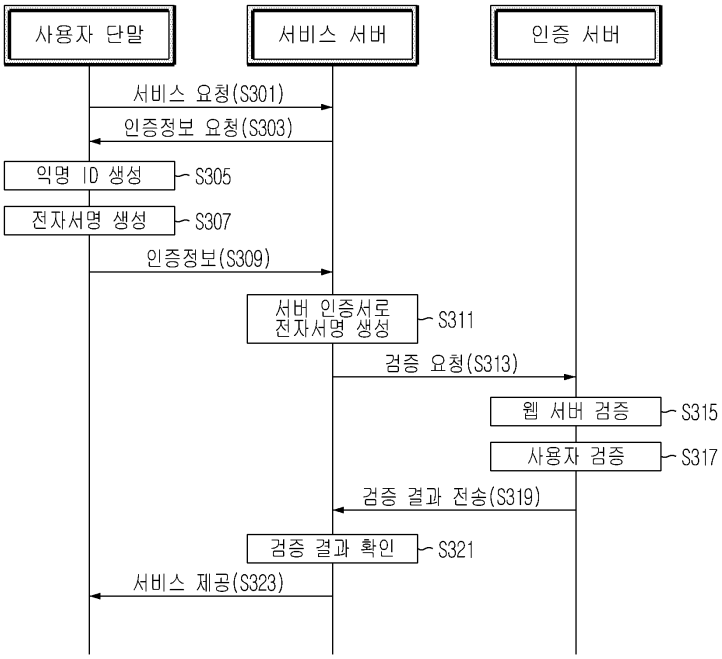
도면1



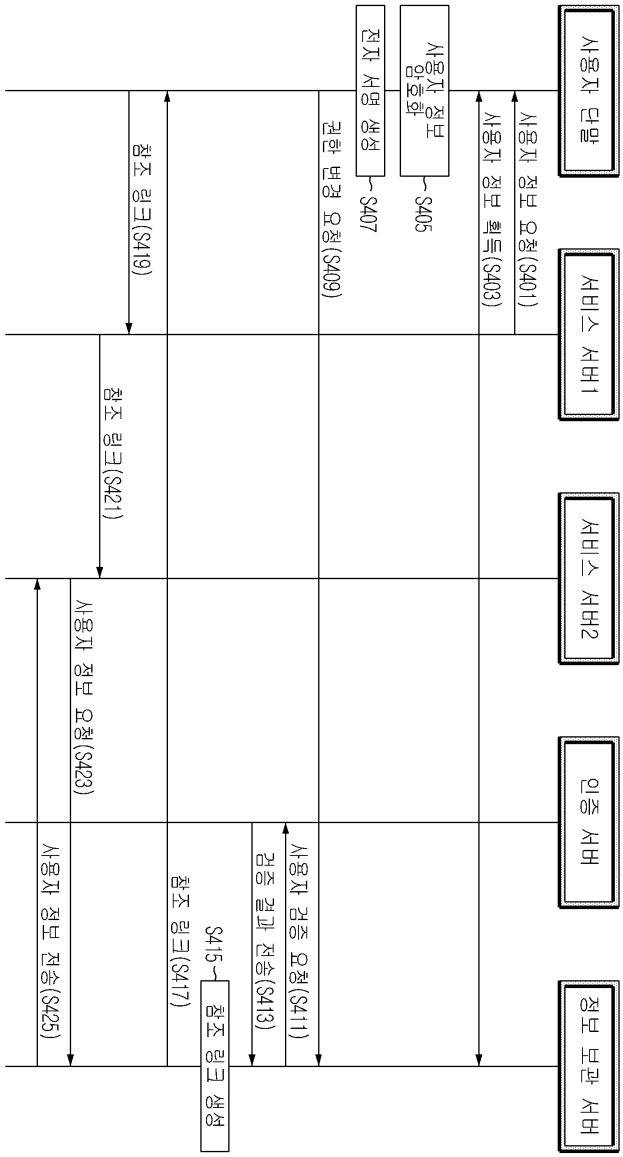
도면2


사용자 단말
인증 서버
본인 확인 서버
정보 보관 서버
키 생성
S201
본인 확인 정보 요청(S203)
본인 확인 정보 전송(S205)
본인 확인 결과 전송(S207)
확인 결과 검증 요청(S211)
검증 결과 전송(S213)
인증서 발급(S215)
사용자 정보 암호화
S217
사용자 정보 등록 요청(S219)
검증 결과 전송(S223)
사용자 검증 요청(S221)
S225
사용자 정보 저장

도면3


사용자 단말
서비스 서버
인증 서버
서비스 요청(S301)
인증정보 요청(S303)
익명 ID 생성
S305
전자서명 생성
S307
인증정보(S309)
서버 인증서로 전자서명 생성
S311
검증 요청(S313)
웹 서버 검증
S315
사용자 검증
S317
검증 결과 전송(S319)
검증 결과 확인
S321
서비스 제공(S323)

도면4


사용자 단말
서비스 서버1
서비스 서버2
인증 서버
정보 보관 서버
사용자 정보 요청(S401)
사용자 정보 획득(S403)
사용자 정보 암호화 S405
전자 서명 생성 S407
권한 변경 요청(S409)
사용자 검증 요청(S411)
검증 결과 전송(S413)
S415 참조 링크 생성
참조 링크(S417)
참조 링크(S419)
참조 링크(S421)
사용자 정보 요청(S423)
사용자 정보 전송(S425)