(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년04월25일
(11) 등록번호 10-1388930
(24) 등록일자 2014년04월18일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)
(21) 출원번호 10-2012-0116965
(22) 출원일자 2012년10월19일
심사청구일자 2012년10월19일
(56) 선행기술조사문헌
KR1020060102456 A*
A. Menezes 외 2명, Handbook of Applied Cryptography, Chapter 11. Digital Signatures, CRC Press (1996)*
KR1020120024302 A
KR1020070014159 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
소프트포럼 주식회사
경기도 성남시 분당구 대왕판교로644번길 49 , 9층(삼평동, 한컴타워)
(72) 발명자
심재원
서울특별시 강서구 방화동 청구 푸르뫼마을 아파트 101-503
(74) 대리인
김효성

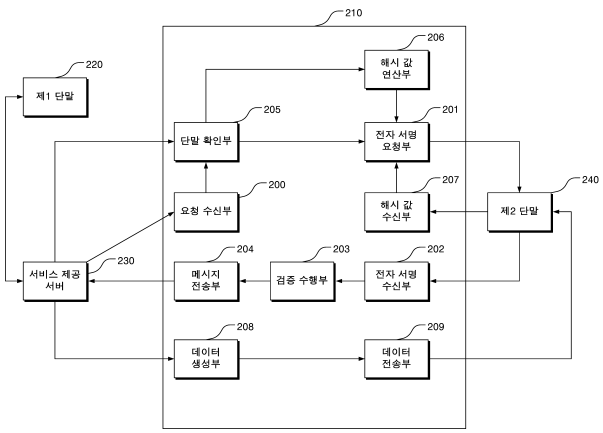
전체 청구항 수 : 총 9 항 심사관 : 양종필

(54) 발명의 명칭 **분리 서명 기반의 사용자 인증 장치 및 방법**

(57) 요 약

분리 서명 기반의 사용자 인증 장치 및 방법이 개시된다. 본 발명의 실시예들은 사용자가 제1 단말을 통해 웹 서비스 등을 제공하는 서비스 제공 서버에 접속하여 사용자 인증을 요청하는 경우, 상기 제1 단말이 아닌 상기 사용자가 보유하고 있는 제2 단말로부터 전자 서명 값을 수신한 후 상기 수신된 전자 서명 값을 검증하여 그 검증 결과에 따라 상기 제1 단말에 대한 사용자 인증여부를 결정하는 분리 서명 기반의 사용자 인증 기법을 제공함으로써, 사용자 인증 절차를 별개의 채널로 분리하여 보안성을 더욱 향상시킬 수 있다.

대 표 도 - 도2



특허청구의 범위

청구항 1

제1 단말이 서비스 제공 서버에 접속하여 사용자 인증을 요청하는 경우, 상기 서비스 제공 서버로부터 상기 제1 단말에 대한 사용자 인증 확인 요청을 수신하는 요청 수신부;

상기 서비스 제공 서버로부터 상기 제1 단말의 사용자 정보를 수신하여 상기 수신된 제1 단말의 사용자 정보를 기초로 상기 제1 단말의 사용자가 보유하고 있는 제2 단말을 확인하는 단말 확인부;

상기 제2 단말에 대한 확인이 완료되면, 상기 사용자 정보에 포함되어 있는 상기 제2 단말에 대한 단말 정보를 선정된(predetermined) 단말 검증용 해시(hash) 함수에 입력으로 인가하여 제1 해시 값을 연산하는 해시 값 연산부;

상기 제2 단말로부터, 상기 제2 단말에 대한 단말 정보를 입력으로 하여 상기 선정된 단말 검증용 해시 함수와 동일한 해시 함수를 기초로 상기 제2 단말에서 연산된 제2 해시 값을 수신하는 해시 값 수신부;

상기 연산된 제1 해시 값과 상기 수신된 제2 해시 값을 비교하여 상기 연산된 제1 해시 값과 상기 수신된 제2 해시 값이 동일한 경우, 상기 수신된 사용자 인증 확인 요청에 대응하여 상기 제2 단말에 대해 전자 서명을 요청하는 전자 서명 요청부;

상기 제2 단말로부터 상기 전자 서명과 연관된 전자 서명 값을 수신하는 전자 서명 수신부;

상기 제2 단말로부터 상기 전자 서명 값이 수신되면, 상기 전자 서명 값에 대한 검증을 수행하는 검증 수행부; 및

상기 전자 서명 값에 대한 검증이 성공하면, 상기 서비스 제공 서버로 사용자 인증 확인 성공 메시지를 전송하는 메시지 전송부

를 포함하는 분리 서명 기반의 사용자 인증 장치.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 서비스 제공 서버에 대해서 상기 제1 단말이 상기 사용자 인증을 통해 액세스(access)하고자 하는 액세스 대상 정보를 확인하여 상기 확인된 액세스 대상 정보를 기초로 상기 전자 서명이 수행되어야 할 전자 서명 대상 데이터를 생성하는 데이터 생성부; 및

상기 생성된 전자 서명 대상 데이터를 상기 제2 단말로 전송하는 데이터 전송부

를 더 포함하고,

상기 전자 서명 요청부는

상기 제2 단말에 대해 상기 생성된 전자 서명 대상 데이터에 대한 전자 서명을 요청하는 분리 서명 기반의 사용자 인증 장치.

청구항 5

제4항에 있어서,

상기 전자 서명 수신부는

상기 제2 단말로부터, 상기 제2 단말에 저장되어 있는 개인키를 기초로 상기 전자 서명 대상 데이터에 대해 전자 서명이 수행되어 생성된 상기 전자 서명 값과 상기 개인키에 대응되는 공개키를 수신하고,

상기 검증 수행부는

상기 제2 단말로부터 상기 전자 서명 값과 상기 공개키가 수신되면, 상기 공개키를 기초로 상기 전자 서명 값을 복호화하여 상기 전자 서명 값에 대한 검증을 수행하는 분리 서명 기반의 사용자 인증 장치.

청구항 6

제5항에 있어서,

상기 전자 서명 수신부는

상기 제2 단말로부터, 상기 전자 서명 대상 데이터에 대해 해시 함수가 적용되어 생성된 해시 값과 상기 해시 값에 대해 상기 개인키를 기초로 전자 서명이 수행되어 생성된 상기 전자 서명 값 및 상기 공개키가 포함되어 있는 공개키 인증서를 수신하고,

상기 검증 수행부는

상기 제2 단말로부터 상기 해시 값과 상기 전자 서명 값 및 상기 공개키 인증서가 수신되면, 상기 공개키 인증서에 포함되어 있는 상기 공개키를 기초로 상기 전자 서명 값에 대해 복호화를 수행하여 복호화 값을 생성한 후 상기 생성된 복호화 값과 상기 수신된 해시 값을 비교하여 상기 생성된 복호화 값과 상기 수신된 해시 값이 동일한 경우, 상기 전자 서명 값에 대한 검증이 성공한 것으로 판단하는 분리 서명 기반의 사용자 인증 장치.

청구항 7

제1 단말이 서비스 제공 서버에 접속하여 사용자 인증을 요청하는 경우, 상기 서비스 제공 서버로부터 상기 제1 단말에 대한 사용자 인증 확인 요청을 수신하는 단계;

상기 서비스 제공 서버로부터 상기 제1 단말의 사용자 정보를 수신하여 상기 수신된 제1 단말의 사용자 정보를 기초로 상기 제1 단말의 사용자가 보유하고 있는 제2 단말을 확인하는 단계;

상기 제2 단말에 대한 확인이 완료되면, 상기 사용자 정보에 포함되어 있는 상기 제2 단말에 대한 단말 정보를 선정된(predetermined) 단말 검증용 해시(hash) 함수에 입력으로 인가하여 제1 해시 값을 연산하는 단계;

상기 제2 단말로부터, 상기 제2 단말에 대한 단말 정보를 입력으로 하여 상기 선정된 단말 검증용 해시 함수와 동일한 해시 함수를 기초로 상기 제2 단말에서 연산된 제2 해시 값을 수신하는 단계;

상기 연산된 제1 해시 값과 상기 수신된 제2 해시 값을 비교하여 상기 연산된 제1 해시 값과 상기 수신된 제2 해시 값이 동일한 경우, 상기 수신된 사용자 인증 확인 요청에 대응하여 상기 제2 단말에 대해 전자 서명을 요청하는 단계;

상기 제2 단말로부터 상기 전자 서명과 연관된 전자 서명 값을 수신하는 단계;

상기 제2 단말로부터 상기 전자 서명 값이 수신되면, 상기 전자 서명 값에 대한 검증을 수행하는 단계; 및

상기 전자 서명 값에 대한 검증이 성공하면, 상기 서비스 제공 서버로 사용자 인증 확인 성공 메시지를 전송하는 단계

를 포함하는 분리 서명 기반의 사용자 인증 방법.

청구항 8

삭제

청구항 9

삭제

청구항 10

제7항에 있어서,

상기 서비스 제공 서버에 대해서 상기 제1 단말이 상기 사용자 인증을 통해 액세스(access)하고자 하는 액세스 대상 정보를 확인하여 상기 확인된 액세스 대상 정보를 기초로 상기 전자 서명이 수행되어야 할 전자 서명 대상 데이터를 생성하는 단계; 및

상기 생성된 전자 서명 대상 데이터를 상기 제2 단말로 전송하는 단계

를 더 포함하고,

상기 전자 서명을 요청하는 단계는

상기 제2 단말에 대해 상기 생성된 전자 서명 대상 데이터에 대한 전자 서명을 요청하는 분리 서명 기반의 사용자 인증 방법.

청구항 11

제10항에 있어서,

상기 전자 서명 값을 수신하는 단계는

상기 제2 단말로부터, 상기 제2 단말에 저장되어 있는 개인키를 기초로 상기 전자 서명 대상 데이터에 대해 전자 서명이 수행되어 생성된 상기 전자 서명 값과 상기 개인키에 대응되는 공개키를 수신하고,

상기 검증을 수행하는 단계는

상기 제2 단말로부터 상기 전자 서명 값과 상기 공개키가 수신되면, 상기 공개키를 기초로 상기 전자 서명 값을 복호화하여 상기 전자 서명 값에 대한 검증을 수행하는 분리 서명 기반의 사용자 인증 방법.

청구항 12

제11항에 있어서,

상기 전자 서명 값을 수신하는 단계는

상기 제2 단말로부터, 상기 전자 서명 대상 데이터에 대해 해시 함수가 적용되어 생성된 해시 값과 상기 해시 값에 대해 상기 개인키를 기초로 전자 서명이 수행되어 생성된 상기 전자 서명 값 및 상기 공개키가 포함되어 있는 공개키 인증서를 수신하고,

상기 검증을 수행하는 단계는

상기 제2 단말로부터 상기 해시 값과 상기 전자 서명 값 및 상기 공개키 인증서가 수신되면, 상기 공개키 인증서에 포함되어 있는 상기 공개키를 기초로 상기 전자 서명 값에 대해 복호화를 수행하여 복호화 값을 생성한 후 상기 생성된 복호화 값과 상기 수신된 해시 값을 비교하여 상기 생성된 복호화 값과 상기 수신된 해시 값이 동일한 경우, 상기 전자 서명 값에 대한 검증이 성공한 것으로 판단하는 분리 서명 기반의 사용자 인증 방법.

청구항 13

제7항 또는 제10항 내지 제12항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

명 세 서

기 술 분 야

[0001] 본 발명의 실시예들은 서비스 제공 서버에 접속한 단말 이외의 다른 단말을 통해 전자 서명 값을 수신하여 사용자 인증을 수행하는 기법에 대한 것이다.

배 경 기 술

[0002] 최근, 인터넷 등이 널리 보급됨에 따라, 회원제로 운영되는 웹 사이트가 증가하고 있고, 전자 결제나 온라인 기반의 뱅킹 서비스 사용도 급증하고 있다.

[0003] 보통, 일반적인 회원제 기반의 웹 사이트는 가입자의 아이디와 비밀번호를 수집한 후 웹 사이트에 로그인하고자

하는 사용자의 아이디와 비밀번호를 확인하여 사용자 인증을 수행하는 방식으로 운영되고 있다.

[0004] 또한, 전자 결제나 온라인 기반의 뱅킹 서비스는 사용자의 단말에 소정의 인증서를 발급한 후 사용자가 전자 결제나 온라인 기반의 뱅킹 서비스를 이용하고자 할 때, 상기 단말에 설치되어 있는 인증서를 통해 전자 서명 값을 수신하여 사용자 인증을 수행하는 방식으로 운영되고 있다.

[0005] 이러한 사용자 인증 방식은 일정 수준의 보안성을 유지할 수 있으나, 웹 사이트에 접속하여 서비스를 이용하고 있는 사용자 단말로부터만 사용자 인증 정보를 수신한다는 점에서 상기 사용자 단말이 해킹되거나 비밀번호 등이 제3자에게 노출될 경우, 상기 제3자가 해킹된 사용자 단말 또는 노출된 비밀번호 등을 이용하여 정당한 사용자 몰래 손쉽게 웹 사이트에 로그인하거나 전자 결제 또는 뱅킹 서비스를 이용할 수 있다는 점에서 보안에 취약한 단점이 있다.

[0006] 예컨대, 사용자가 자신의 컴퓨터를 이용하여 인터넷 뱅킹을 통해 계좌 이체를 수행하는 경우, 기존의 인터넷 뱅킹 서비스에서는 보안 서버가 상기 사용자의 컴퓨터로 전자 서명을 요청하고, 상기 사용자가 상기 컴퓨터에 저장되어 있는 인증서를 이용하여 전자 서명을 수행한 후 상기 컴퓨터가 전자 서명 값을 상기 보안 서버로 전송하면, 상기 보안 서버가 상기 전자 서명 값을 검증함으로써, 사용자 인증을 수행한 후 계좌 이체가 실행되는 방식이었다.

[0007] 이러한 방식은 현재 인터넷 뱅킹 서비스를 이용하고 있는 사용자의 컴퓨터로부터 전자 서명 값을 받아오기 때문에 상기 사용자의 컴퓨터가 해킹되거나 인증서의 비밀번호를 알고 있는 제3자가 상기 사용자의 컴퓨터를 이용하여 전자 서명을 수행한다면, 진정한 사용자에게 막대한 금전적인 손해가 발생할 수 있다.

[0008] 따라서, 웹 서비스 등을 제공하는 서비스 제공 서버에 접속한 사용자 단말로부터 인증 데이터를 수신하여 사용자 인증을 수행하는 기존의 사용자 인증 기법보다 보안성을 더욱 강화할 수 있는 사용자 인증 기법에 대한 연구가 필요하다.

선행기술문헌

특허문헌

(특허문헌 0001) 대한민국 공개특허공보 제10-2006-0102456호(2006.09.27)

(특허문헌 0002) 대한민국 공개특허공보 제10-2011-0124929호(2011.11.18)

(특허문헌 0003) 대한민국 공개특허공보 제10-2002-0083195호(2002.11.02)

발명의 내용

해결하려는 과제

[0009] 본 발명의 실시예들은 사용자가 제1 단말을 통해 웹 서비스 등을 제공하는 서비스 제공 서버에 접속하여 사용자 인증을 요청하는 경우, 상기 제1 단말이 아닌 상기 사용자가 보유하고 있는 제2 단말로부터 전자 서명 값을 수신한 후 상기 수신된 전자 서명 값을 검증하여 그 검증 결과에 따라 상기 제1 단말에 대한 사용자 인증여부를 결정함으로써, 사용자 인증 절차를 별개의 채널로 분리하여 보안성을 더욱 향상시킬 수 있는 분리 서명 기반의 사용자 인증 기법을 제공하고자 한다.

과제의 해결 수단

[0010] 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 장치는 제1 단말이 서비스 제공 서버에 접속하여 사용자 인증을 요청하는 경우, 상기 서비스 제공 서버로부터 상기 제1 단말에 대한 사용자 인증 확인 요청을 수신하는 요청 수신부, 상기 수신된 사용자 인증 확인 요청에 대응하여 상기 제1 단말의 사용자가 보유하고 있는 제2 단말에 대해 전자 서명을 요청하는 전자 서명 요청부, 상기 제2 단말로부터 상기 전자 서명과 연관된 전자 서명 값을 수신하는 전자 서명 수신부, 상기 제2 단말로부터 상기 전자 서명 값이 수신되면, 상기 전자 서명 값에 대한 검증을 수행하는 검증 수행부 및 상기 전자 서명 값에 대한 검증이 성공하면, 상기 서비스 제공 서버로 사용자 인증 확인 성공 메시지를 전송하는 메시지 전송부를 포함한다.

[0011] 또한, 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 방법은 제1 단말이 서비스 제공 서버에 접속하

여 사용자 인증을 요청하는 경우, 상기 서비스 제공 서버로부터 상기 제1 단말에 대한 사용자 인증 확인 요청을 수신하는 단계, 상기 수신된 사용자 인증 확인 요청에 대응하여 상기 제1 단말의 사용자가 보유하고 있는 제2 단말에 대해 전자 서명을 요청하는 단계, 상기 제2 단말로부터 상기 전자 서명과 연관된 전자 서명 값을 수신하는 단계, 상기 제2 단말로부터 상기 전자 서명 값이 수신되면, 상기 전자 서명 값에 대한 검증을 수행하는 단계 및 상기 전자 서명 값에 대한 검증이 성공하면, 상기 서비스 제공 서버로 사용자 인증 확인 성공 메시지를 전송하는 단계를 포함한다.

발명의 효과

[0012] 본 발명의 실시예들은 사용자가 제1 단말을 통해 웹 서비스 등을 제공하는 서비스 제공 서버에 접속하여 사용자 인증을 요청하는 경우, 상기 제1 단말이 아닌 상기 사용자가 보유하고 있는 제2 단말로부터 전자 서명 값을 수신한 후 상기 수신된 전자 서명 값을 검증하여 그 검증 결과에 따라 상기 제1 단말에 대한 사용자 인증여부를 결정하는 분리 서명 기반의 사용자 인증 기법을 제공함으로써, 사용자 인증 절차를 별개의 채널로 분리하여 보안성을 더욱 향상시킬 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 시스템을 개략적으로 도시한 시스템 개념도이다.

도 2는 본 발명이 일실시예에 따른 분리 서명 기반의 사용자 인증 장치의 구조를 도시한 도면이다.

도 3은 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0015] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0016] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0017] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0018] 이하에서, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.

[0019] 도 1은 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 시스템을 개략적으로 도시한 시스템 개념도이다.

[0020] 도 1을 참조하면, 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 시스템은 분리 서명 기반의 사용자 인증 장치(110), 제1 단말(120), 서비스 제공 서버(130) 및 제2 단말(140)로 구성될 수 있다.

[0021] 여기서, 제1 단말(120)과 제2 단말(140)은 데스크탑 PC, 모바일 단말, PDA, 노트북, 태블릿 PC 등 마이크로프로세서 기반의 장치를 의미한다.

[0022] 그리고, 서비스 제공 서버(130)는 포털 사이트나 인터넷 뱅킹 사이트 등과 같이 서비스 제공 서버(130)에 접속한 단말에 대해 소정의 웹 기반의 서비스를 제공하기 위해 사용되는 서버를 의미한다.

[0023] 예컨대, 서비스 제공 서버(130)는 'www.softforum.co.kr'이라는 URL(Uniform Resource Locator)을 갖는 웹 사이트를 운영하기 위해 사용되는 서버일 수 있고, 'www.softforum.co.kr'라는 URL에 접속한 단말에 대해 인터넷 뱅킹 서비스나 관련 웹 컨텐츠 등을 제공하는데 사용될 수 있다.

[0024] 먼저, 사용자(150)가 데스크탑 컴퓨터 등과 같은 제1 단말(120)을 이용하여 서비스 제공 서버(130)에 접속한 후 인터넷 뱅킹 서비스를 이용하여 계좌 이체를 수행하려고 하는 등의 행위를 수행함으로써, 제1 단말(120)로부터 서비스 제공 서버(130)로 사용자 인증 요청이 전송되는 경우, 서비스 제공 서버(130)는 상기 사용자 인증 요청에 대응하여 분리 서명 기반의 사용자 인증 장치(110)로 제1 단말(120)의 사용자(150)에 대한 사용자 인증 확인 요청을 전송한다.

[0025] 이때, 서비스 제공 서버(130)는 제1 단말(120)의 사용자(150)에 대한 사용자 정보를 확인한 후 상기 확인된 사용자 정보를 분리 서명 기반의 사용자 인증 장치(110)로 전송할 수 있다.

[0026] 여기서, 서비스 제공 서버(130)는 제1 단말(120)의 사용자(150)에 대한 사용자 정보를 확인하기 위해, 제1 단말(120)로부터 상기 사용자 정보를 직접 수신할 수도 있고, 제1 단말(120)로부터 사용자(150)의 회원 아이디를 수신한 후 상기 수신된 회원 아이디를 기초로 서비스 제공 서버(130)에 포함되어 있는 소정의 회원 데이터베이스로부터 상기 사용자 정보를 추출할 수도 있다.

[0027] 또한, 상기 사용자 정보는 사용자(150)의 성명, 주민등록번호 등과 같은 개인 정보뿐만 아니라, 사용자(150)가 보유하고 있는 제2 단말(140)에 대한 정보를 포함할 수 있다.

[0028] 예컨대, 제2 단말(140)이 모바일 단말이라면, 상기 사용자 정보에는 제2 단말(140)에 할당되어 있는 전화번호나 MAC(Media Access Control) 주소와 같은 제2 단말(140)을 식별하기 위한 식별 정보가 포함될 수 있다.

[0029] 이때, 분리 서명 기반의 사용자 인증 장치(110)는 서비스 제공 서버(130)로부터 제1 단말(120)에 대한 사용자 인증 확인 요청과 제1 단말(120)의 사용자(150)에 대한 사용자 정보가 수신되면, 상기 수신된 사용자 정보를 기초로 사용자(150)가 보유하고 있는 제2 단말(140)을 확인할 수 있다.

[0030] 그리고 나서, 분리 서명 기반의 사용자 인증 장치(110)는 제2 단말(140)에 대한 확인이 완료되면, 상기 사용자 정보에 포함되어 있는 제2 단말(140)에 대한 단말 정보를 선정된(predetermined) 단말 검증용 해시(hash) 함수에 입력으로 인가하여 제1 해시 값을 연산한 후 제2 단말(140)에 대해 단말 검증을 위한 제2 해시 값의 전송을 요청할 수 있다.

[0031] 이때, 제2 단말(140)은 상기 제2 해시 값에 대한 전송 요청이 수신되면, 상기 선정된 단말 검증용 해시 함수와 동일한 해시 함수에 대해, 제2 단말(140)에 대한 단말 정보를 입력으로 인가하여 상기 제2 해시 값을 연산한 후 상기 연산된 제2 해시 값을 분리 서명 기반의 사용자 인증 장치(110)로 전송할 수 있다.

[0032] 여기서, 상기 제1 해시 값과 상기 제2 해시 값을 연산하기 위해 입력으로 사용되는 상기 단말 정보는 제2 단말(140)의 전화번호 또는 MAC 주소 등과 같은 단말 고유 식별 번호가 될 수 있다.

[0033] 또한, 제2 단말(140)에는 상기 선정된 단말 검증용 해시 함수와 동일한 해시 함수가 미리 배포되어 저장되어 있을 수 있는데, 이는 사용자(150)가 서비스 제공 서버(130)에서 제공하는 서비스를 이용하기 위해 미리 회원으로 가입할 때, 가입 당시 분리 서명 기반의 사용자 인증 장치(110)가 서비스 제공 서버(130)와의 연동을 통해, 제2 단말(140)에 대해 상기 선정된 단말 검증용 해시 함수와 동일한 해시 함수를 미리 배포함으로써, 구현될 수 있다.

[0034] 분리 서명 기반의 사용자 인증 장치(110)는 제2 단말(140)로부터 상기 제2 해시 값이 수신되면, 앞서 연산된 제1 해시 값과 상기 수신된 제2 해시 값을 비교하여 상기 제1 해시 값과 상기 제2 해시 값이 서로 동일한 경우, 사용자(150)를 제2 단말(140)의 진정한 소유자로 확인할 수 있다.

[0035] 이렇게, 사용자(150)가 제2 단말(140)의 진정한 소유자임이 확인되면, 분리 서명 기반의 사용자 인증 장치(110)는 제2 단말(140)에 대해, 서비스 제공 서버(130)로부터 수신된 제1 단말(120)에 대한 사용자 인증 확인 요청에 대응하여 전자 서명을 요청한다.

[0036] 즉, 기존의 사용자 인증 기법에서는 사용자(150)가 제1 단말(120)을 이용하여 인터넷 뱅킹 서비스를 통해 계좌 이체 등을 수행할 때, 서비스 제공 서버(130)에 접속해 있는 제1 단말(120)에 대해 계좌 이체를 위한 전자 서명

을 요청한 후 제1 단말(120)로부터 전자 서명 값을 수신하여 상기 계좌 이체를 위한 사용자 인증을 진행하는데 반해, 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 시스템에서는 서비스 제공 서버(130)에 접속한 제1 단말(120)에 대해 사용자 인증을 위한 전자 서명을 요청하는 것이 아니라, 사용자(150)가 보유하고 있는 별도의 제2 단말(140)에 대해 상기 전자 서명을 요청할 수 있다.

[0037] 이때, 본 발명의 일실시예에 따르면, 분리 서명 기반의 사용자 인증 장치(110)는 제2 단말(140)에 대해 상기 전자 서명을 요청할 때, 전자 서명이 수행되어야 할 전자 서명 대상 데이터를 생성한 후 이를 제2 단말(140)로 전송할 수 있다.

[0038] 관련하여, 분리 서명 기반의 사용자 인증 장치(110)는 서비스 제공 서버(130)에 대해서 제1 단말(120)이 상기 사용자 인증을 통해 액세스(access)하고자 하는 액세스 대상 정보를 확인하여 상기 확인된 액세스 대상 정보를 기초로 상기 전자 서명이 수행되어야 할 전자 서명 대상 데이터를 생성할 수 있다.

[0039] 예컨대, 제1 단말(120)이 서비스 제공 서버(130)에 대해 계좌 이체를 위한 사용자 인증을 요청하였다면, 분리 서명 기반의 사용자 인증 장치(110)는 서비스 제공 서버(130)에 대해서 제1 단말(120)이 사용자 인증을 통해 액세스하고자 하였던 액세스 대상 정보로 계좌 이체와 관련된 정보인 계좌 정보, 이체 금액, 입금자명 등을 확인한 후 상기 확인된 액세스 대상 정보를 기초로 상기 전자 서명이 수행되어야 할 전자 서명 대상 데이터를 생성할 수 있다.

[0040] 그리고 나서, 분리 서명 기반의 사용자 인증 장치(110)는 상기 생성된 전자 서명 대상 데이터를 제2 단말(140)로 전송할 수 있다.

[0041] 이때, 제2 단말(140)은 상기 수신된 전자 서명 대상 데이터를 디스플레이할 수 있고, 이를 통해 사용자(150)는 제2 단말(140)에서 디스플레이되는 상기 전자 서명 대상 데이터를 확인함으로써, 자신이 제2 단말(140)을 통해 전자 서명을 수행해야할 대상이 정확한지 여부를 확인할 수 있다.

[0042] 이때, 본 발명의 다른 실시예에 따르면, 분리 서명 기반의 사용자 인증 장치(110)는 상기 전자 서명 대상 데이터의 생성을 완료하면, 상기 생성된 전자 서명 대상 데이터를 제2 단말(140)로 직접 전송할 수도 있지만, 상기 생성된 전자 서명 대상 데이터가 삽입된 다차원 코드를 생성한 후 상기 생성된 다차원 코드를 제1 단말(120)로 전송할 수 있다.

[0043] 여기서, 상기 다차원 코드는 QR(Quick Response) 코드가 될 수 있다.

[0044] 이때, 제1 단말(120)은 상기 다차원 코드가 수신되면, 상기 수신된 다차원 코드를 디스플레이할 수 있고, 사용자(150)는 제1 단말(120)을 통해 디스플레이 되는 다차원 코드를 제2 단말(140)로 촬영하여 제2 단말(140)에 상기 다차원 코드를 인식시킬 수 있으며, 제2 단말(140)은 상기 다차원 코드를 인식하여 상기 다차원 코드에 삽입되어 있는 상기 전자 서명 대상 데이터를 추출하여 상기 추출된 전자 서명 대상 데이터를 디스플레이할 수 있다.

[0045] 이를 통해 사용자(150)는 제2 단말(140)에서 디스플레이되는 상기 전자 서명 대상 데이터를 확인함으로써, 자신이 제2 단말(140)을 통해 전자 서명을 수행해야할 대상이 정확한지 여부를 확인할 수 있다.

[0046] 이렇게, 분리 서명 기반의 사용자 인증 장치(110)로부터 제2 단말(140)로 상기 전자 서명 대상 데이터가 전송되고, 상기 전자 서명 대상 데이터에 대한 전자 서명 요청이 전송되면, 제2 단말(140)은 제2 단말(140)에 저장되어 있는 개인키를 기초로 상기 전자 서명 대상 데이터에 대해 전자 서명을 수행하여 전자 서명 값을 생성할 수 있다.

[0047] 이와 관련하여, 제2 단말(140)이 상기 전자 서명 값을 생성하는 과정을 좀 더 상세히 설명하면, 다음과 같다.

[0048] 먼저, 제2 단말(140)에는 상기 전자 서명 대상 데이터에 대해 전자 서명이 수행될 수 있도록 공인된 인증 기관에서 발행된 공개키 인증서가 저장되어 있을 수 있다.

[0049] 여기서, 제2 단말(140)에 상기 공개키 인증서가 발급되는 절차는 현재 인터넷 뱅킹 등에서 널리 사용되고 있는 공인인증서 등의 발급 절차 또는 스마트폰에 인증서를 저장하는 절차 등을 통해 널리 알려진 사항이므로, 이에 대한 자세한 설명은 생략하기로 한다.

[0050] 사용자(150)가 제2 단말(140)을 통해 상기 공개키 인증서를 선택한 후 제2 단말(140)에 저장되어 있는 개인키를 로드하기 위한 암호를 입력하면, 제2 단말(140)은 상기 전자 서명 대상 데이터에 대해 해시 함수를 적용하여 해시 값을 생성하고, 상기 생성된 해시 값에 대해 상기 공개키 인증서를 발급받을 때 생성되었던 상기 개인키를

이용하여 전자 서명, 즉 암호화를 수행함으로써, 상기 전자 서명 값을 생성할 수 있다.

[0051] 여기서, 상기 개인키는 제2 단말(140)이 인증 기관으로부터 상기 공개키 인증서를 발급받을 때 생성되며, 상기 개인키로 암호화된 데이터를 복호화할 수 있는 공개키도 상기 공개키 인증서를 발급받을 때 생성되어 상기 공개키 인증서에 포함될 수 있다.

[0052] 그리고 나서, 제2 단말(140)은 상기 해시 값과 상기 전자 서명 값 및 상기 개인키에 대응되는 공개키가 포함되어 있는 상기 공개키 인증서를 분리 서명 기반의 사용자 인증 장치(110)로 전송할 수 있다.

[0053] 이때, 분리 서명 기반의 사용자 인증 장치(110)는 상기 해시 값과 상기 전자 서명 값 및 상기 공개키 인증서가 수신되면, 상기 공개키 인증서에 포함되어 있는 상기 공개키를 기초로 상기 전자 서명 값을 복호화하여 복호화 값을 생성한 후 상기 생성된 복호화 값과 상기 수신된 해시 값을 비교하여 상기 전자 서명 값에 대한 검증을 수행할 수 있다.

[0054] 이때, 본 발명의 일실시예에 따르면, 분리 서명 기반의 사용자 인증 장치(110)는 상기 수신된 공개키 인증서에 포함되어 있는 상기 공개키가 정당한 공개키인지 여부를 검증하기 위해, 상기 공개키 인증서를 발급한 인증 기관의 서버에 접속하여 상기 공개키 인증서에 포함되어 있는 상기 공개키에 대한 검증을 수행할 수 있다.

[0055] 이렇게, 상기 생성된 복호화 값과 상기 수신된 해시 값을 비교한 결과, 상기 생성된 복호화 값과 상기 수신된 해시 값이 서로 동일한 경우, 분리 서명 기반의 사용자 인증 장치(110)는 상기 전자 서명 값에 대한 검증이 성공한 것으로 판단할 수 있고, 상기 생성된 복호화 값과 상기 수신된 해시 값이 서로 동일하지 않은 경우, 분리 서명 기반의 사용자 인증 장치(110)는 상기 전자 서명 값에 대한 검증이 실패한 것으로 판단할 수 있다.

[0056] 그리고 나서, 분리 서명 기반의 사용자 인증 장치(110)는 상기 전자 서명 값에 대한 검증이 성공한 것으로 판단되면, 서비스 제공 서버(130)로 사용자 인증 확인 성공 메시지를 전송할 수 있고, 상기 전자 서명 값에 대한 검증이 실패한 것으로 판단되면, 서비스 제공 서버(130)로 사용자 인증 확인 실패 메시지를 전송할 수 있다.

[0057] 이때, 서비스 제공 서버(130)는 분리 서명 기반의 사용자 인증 장치(110)로부터 상기 사용자 인증 확인 성공 메시지가 수신되면, 제1 단말(120)에 대해 제1 단말(120)이 사용자 인증을 통해 액세스하고자 하였던 서비스에 대한 액세스를 허가할 수 있다.

[0058] 하지만, 서비스 제공 서버(130)는 분리 서명 기반의 사용자 인증 장치(110)로부터 상기 사용자 인증 확인 실패 메시지가 수신되면, 제1 단말(120)에 대해 제1 단말(120)이 사용자 인증을 통해 액세스하고자 하였던 서비스에 대한 액세스를 차단할 수 있다.

[0059] 다시 말해서, 사용자(150)가 제1 단말(120)을 통해 계좌 이체를 수행하고자 하였던 경우, 서비스 제공 서버(130)는 분리 서명 기반의 사용자 인증 장치(110)로부터 상기 사용자 인증 확인 성공 메시지가 수신되면, 제1 단말(120)에 대해 계좌 이체를 실행하고, 상기 사용자 인증 확인 실패 메시지가 수신되면, 제1 단말(120)에 대해 계좌 이체를 중단할 수 있다.

[0060] 결국, 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 시스템은 사용자(150)가 제1 단말(120)을 통해 서비스 제공 서버(130)에 접속하여 사용자 인증을 요청하는 경우, 제1 단말(120)이 아닌 사용자(150)가 보유하고 있는 제2 단말(140)로부터 전자 서명 값을 수신한 후 상기 수신된 전자 서명 값을 검증하여 그 검증 결과에 따라 제1 단말(120)에 대한 사용자 인증여부를 결정함으로써, 사용자 인증 절차를 별개의 채널로 분리하여 보안성을 더욱 향상시킬 수 있다.

[0061] 도 2는 본 발명이 일실시예에 따른 분리 서명 기반의 사용자 인증 장치의 구조를 도시한 도면이다.

[0062] 도 2를 참조하면, 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 장치(210)는 요청 수신부(200), 전자 서명 요청부(201), 전자 서명 수신부(202), 검증 수행부(203) 및 메시지 전송부(204)를 포함한다.

[0063] 요청 수신부(200)는 제1 단말(220)이 서비스 제공 서버(230)에 접속하여 사용자 인증을 요청하는 경우, 서비스 제공 서버(230)로부터 제1 단말(220)에 대한 사용자 인증 확인 요청을 수신한다.

[0064] 전자 서명 요청부(201)는 상기 수신된 사용자 인증 확인 요청에 대응하여 제1 단말(220)의 사용자가 보유하고 있는 제2 단말(240)에 대해 전자 서명을 요청한다.

[0065] 이때, 본 발명의 일실시예에 따르면, 분리 서명 기반의 사용자 인증 장치(210)는 단말 확인부(205)를 더 포함할 수 있다.

[0066] 단말 확인부(205)는 서비스 제공 서버(230)로부터 제1 단말(220)의 사용자 정보를 수신하여 상기 수신된 제1 단말(220)의 사용자 정보를 기초로 제1 단말(220)의 사용자가 보유하고 있는 제2 단말(240)을 확인한다.

[0067] 이때, 전자 서명 요청부(201)는 상기 확인된 제2 단말(240)에 대해 상기 전자 서명을 요청할 수 있다.

[0068] 또한, 본 발명의 일실시예에 따르면, 분리 서명 기반의 사용자 인증 장치(210)는 해시 값 연산부(206) 및 해시 값 수신부(207)를 더 포함할 수 있다.

[0069] 해시 값 연산부(206)는 제2 단말(240)에 대한 확인이 완료되면, 상기 사용자 정보에 포함되어 있는 제2 단말(240)에 대한 단말 정보를 선정된 단말 검증용 해시 함수에 입력으로 인가하여 제1 해시 값을 연산한다.

[0070] 이때, 제2 단말(240)은 상기 선정된 단말 검증용 해시 함수와 동일한 해시 함수에 대해, 제2 단말(240)에 대한 단말 정보를 입력으로 인가하여 제2 해시 값을 연산할 수 있다.

[0071] 그리고 나서, 해시 값 수신부(207)는 상기 확인된 제2 단말(240)로부터, 제2 단말(240)에 대한 단말 정보를 입력으로 하여 상기 선정된 단말 검증용 해시 함수와 동일한 해시 함수를 기초로 제2 단말(240)에서 연산된 상기 제2 해시 값을 수신한다.

[0072] 이때, 전자 서명 요청부(201)는 상기 연산된 제1 해시 값과 상기 수신된 제2 해시 값을 비교하여 상기 연산된 제1 해시 값과 상기 수신된 제2 해시 값이 동일한 경우, 상기 확인된 제2 단말(240)에 대해 상기 전자 서명을 요청할 수 있다.

[0073] 또한, 본 발명의 일실시예에 따르면, 분리 서명 기반의 사용자 인증 장치(210)는 데이터 생성부(208) 및 데이터 전송부(209)를 더 포함할 수 있다.

[0074] 데이터 생성부(208)는 서비스 제공 서버(230)에 대해서 제1 단말(220)이 상기 사용자 인증을 통해 액세스하고자 하는 액세스 대상 정보를 확인하여 상기 확인된 액세스 대상 정보를 기초로 상기 전자 서명이 수행되어야 할 전자 서명 대상 데이터를 생성한다.

[0075] 데이터 전송부(209)는 상기 생성된 전자 서명 대상 데이터를 제2 단말(240)로 전송한다.

[0076] 이때, 전자 서명 요청부(201)는 제2 단말(240)에 대해 상기 생성된 전자 서명 대상 데이터에 대한 전자 서명을 요청할 수 있다.

[0077] 전자 서명 수신부(202)는 제2 단말(240)로부터 상기 전자 서명과 연관된 전자 서명 값을 수신한다.

[0078] 검증 수행부(203)는 제2 단말(240)로부터 상기 전자 서명 값이 수신되면, 상기 전자 서명 값에 대한 검증을 수행한다.

[0079] 이때, 본 발명의 일실시예에 따르면, 제2 단말(240)은 제2 단말(240)에 저장되어 있는 개인키를 기초로 상기 전자 서명 대상 데이터에 대해 전자 서명을 수행하여 상기 전자 서명 값을 생성할 수 있고, 전자 서명 수신부(202)는 제2 단말(240)로부터, 제2 단말(240)에 저장되어 있는 상기 개인키를 기초로 상기 전자 서명 대상 데이터에 대해 전자 서명이 수행되어 생성된 상기 전자 서명 값과 상기 개인키에 대응되는 공개키를 수신할 수 있다.

[0080] 이때, 검증 수행부(203)는 제2 단말(240)로부터 상기 전자 서명 값과 상기 공개키가 수신되면, 상기 공개키를 기초로 상기 전자 서명 값을 복호화하여 상기 전자 서명 값에 대한 검증을 수행할 수 있다.

[0081] 또한, 본 발명의 일실시예에 따르면, 제2 단말(240)은 상기 전자 서명 대상 데이터에 대해 해시 함수를 적용하여 해시 값을 생성하고, 상기 생성된 해시 값에 대해 상기 개인키를 기초로 전자 서명을 수행하여 상기 전자 서명 값을 생성할 수 있으며, 전자 서명 수신부(202)는 제2 단말(240)로부터, 상기 전자 서명 대상 데이터에 대해 상기 해시 함수가 적용되어 생성된 상기 해시 값과 상기 해시 값에 대해 상기 개인키를 기초로 전자 서명이 수행되어 생성된 상기 전자 서명 값 및 상기 공개키가 포함되어 있는 공개키 인증서를 수신할 수 있다.

[0082] 이때, 검증 수행부(203)는 제2 단말(240)로부터 상기 해시 값과 상기 전자 서명 값 및 상기 공개키 인증서가 수신되면, 상기 공개키 인증서에 포함되어 있는 상기 공개키를 기초로 상기 전자 서명 값에 대해 복호화를 수행하여 복호화 값을 생성한 후 상기 생성된 복호화 값과 상기 수신된 해시 값을 비교하여 상기 생성된 복호화 값과 상기 수신된 해시 값이 동일한 경우, 상기 전자 서명 값에 대한 검증이 성공한 것으로 판단할 수 있다.

[0083] 메시지 전송부(204)는 상기 전자 서명 값에 대한 검증이 성공하면, 서비스 제공 서버(230)로 사용자 인증 확인

성공 메시지를 전송한다.

[0084] 이때, 본 발명의 일실시예에 따르면, 서비스 제공 서버(230)는 상기 사용자 인증 확인 성공 메시지가 수신되면, 제1 단말(220)에 대해 제1 단말(220)이 사용자 인증을 통해 액세스하고자 하였던 서비스에 대한 액세스를 허가할 수 있다.

[0085] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 장치(210)에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 장치(210)는 도 1을 이용하여 설명한 분리 서명 기반의 사용자 인증 장치(110)와 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0086] 도 3은 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 방법을 도시한 순서도이다.

[0087] 단계(S310)에서는 제1 단말이 서비스 제공 서버에 접속하여 사용자 인증을 요청하는 경우, 상기 서비스 제공 서버로부터 상기 제1 단말에 대한 사용자 인증 확인 요청을 수신한다.

[0088] 단계(S320)에서는 상기 수신된 사용자 인증 확인 요청에 대응하여 상기 제1 단말의 사용자가 보유하고 있는 제2 단말에 대해 전자 서명을 요청한다.

[0089] 이때, 본 발명의 일실시예에 따르면, 상기 분리 서명 기반의 사용자 인증 방법은 단계(S320)이전에 상기 서비스 제공 서버로부터 상기 제1 단말의 사용자 정보를 수신하여 상기 수신된 제1 단말의 사용자 정보를 기초로 상기 제1 단말의 사용자가 보유하고 있는 상기 제2 단말을 확인하는 단계를 더 포함할 수 있다.

[0090] 이때, 단계(S320)에서는 상기 확인된 제2 단말에 대해 상기 전자 서명을 요청할 수 있다.

[0091] 또한, 본 발명의 일실시예에 따르면, 상기 분리 서명 기반의 사용자 인증 방법은 단계(S320)이전에 상기 제2 단말에 대한 확인이 완료되면, 상기 사용자 정보에 포함되어 있는 상기 제2 단말에 대한 단말 정보를 선정된 단말 검증용 해시 함수에 입력으로 인가하여 제1 해시 값을 연산하는 단계 및 상기 확인된 제2 단말로부터, 상기 제2 단말에 대한 단말 정보를 입력으로 하여 상기 선정된 단말 검증용 해시 함수와 동일한 해시 함수를 기초로 상기 제2 단말에서 연산된 제2 해시 값을 수신하는 단계를 더 포함할 수 있다.

[0092] 이때, 단계(S320)에서는 상기 연산된 제1 해시 값과 상기 수신된 제2 해시 값을 비교하여 상기 연산된 제1 해시 값과 상기 수신된 제2 해시 값이 동일한 경우, 상기 확인된 제2 단말에 대해 상기 전자 서명을 요청할 수 있다.

[0093] 또한, 본 발명의 일실시예에 따르면, 상기 분리 서명 기반의 사용자 인증 방법은 단계(S320)이전에 상기 서비스 제공 서버에 대해서 상기 제1 단말이 상기 사용자 인증을 통해 액세스하고자 하는 액세스 대상 정보를 확인하여 상기 확인된 액세스 대상 정보를 기초로 상기 전자 서명이 수행되어야 할 전자 서명 대상 데이터를 생성하는 단계 및 상기 생성된 전자 서명 대상 데이터를 상기 제2 단말로 전송하는 단계를 더 포함할 수 있다.

[0094] 이때, 단계(S320)에서는 상기 제2 단말에 대해 상기 생성된 전자 서명 대상 데이터에 대한 전자 서명을 요청할 수 있다.

[0095] 단계(S330)에서는 상기 제2 단말로부터 상기 전자 서명과 연관된 전자 서명 값을 수신한다.

[0096] 단계(S340)에서는 상기 제2 단말로부터 상기 전자 서명 값이 수신되면, 상기 전자 서명 값에 대한 검증을 수행한다.

[0097] 이때, 본 발명의 일실시예에 따르면, 단계(S330)에서는 상기 제2 단말로부터, 상기 제2 단말에 저장되어 있는 개인키를 기초로 상기 전자 서명 대상 데이터에 대해 전자 서명이 수행되어 생성된 상기 전자 서명 값과 상기 개인키에 대응되는 공개키를 수신할 수 있다.

[0098] 이때, 단계(S340)에서는 상기 제2 단말로부터 상기 전자 서명 값과 상기 공개키가 수신되면, 상기 공개키를 기초로 상기 전자 서명 값을 복호화하여 상기 전자 서명 값에 대한 검증을 수행할 수 있다.

[0099] 또한, 본 발명의 일실시예에 따르면, 단계(S330)에서는 상기 제2 단말로부터, 상기 전자 서명 대상 데이터에 대해 해시 함수가 적용되어 생성된 해시 값과 상기 해시 값에 대해 상기 개인키를 기초로 전자 서명이 수행되어 생성된 상기 전자 서명 값 및 상기 공개키가 포함되어 있는 공개키 인증서를 수신할 수 있다.

[0100] 이때, 단계(S340)에서는 상기 제2 단말로부터 상기 해시 값과 상기 전자 서명 값 및 상기 공개키 인증서가 수신되면, 상기 공개키 인증서에 포함되어 있는 상기 공개키를 기초로 상기 전자 서명 값에 대해 복호화를 수행하여 복호화 값을 생성한 후 상기 생성된 복호화 값과 상기 수신된 해시 값을 비교하여 상기 생성된 복호화 값과 상

기 수신된 해시 값이 동일한 경우, 상기 전자 서명 값에 대한 검증이 성공한 것으로 판단할 수 있다.

[0101] 단계(S350)에서는 상기 전자 서명 값에 대한 검증이 성공하면, 상기 서비스 제공 서버로 사용자 인증 확인 성공 메시지를 전송한다.

[0102] 이때, 본 발명의 일실시예에 따르면, 상기 서비스 제공 서버는 상기 사용자 인증 확인 성공 메시지가 수신되면, 상기 제1 단말에 대해 상기 제1 단말이 사용자 인증을 통해 액세스하고자 하였던 서비스에 대한 액세스를 허가할 수 있다.

[0103] 이상, 도 3을 참조하여 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 방법은 도 1과 도 2를 이용하여 설명한 분리 서명 기반의 사용자 인증 장치(110, 210)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0104] 본 발명의 일실시예에 따른 분리 서명 기반의 사용자 인증 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0105] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0106] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0107] 110: 분리 서명 기반의 사용자 인증 장치

120: 제1 단말 130: 서비스 제공 서버

140: 제2 단말 150: 사용자

210: 분리 서명 기반의 사용자 인증 장치

200: 요청 수신부 201: 전자 서명 요청부

202: 전자 서명 수신부 203: 검증 수행부

204: 메시지 전송부 205: 단말 확인부

206: 해시 값 연산부 207: 해시 값 수신부

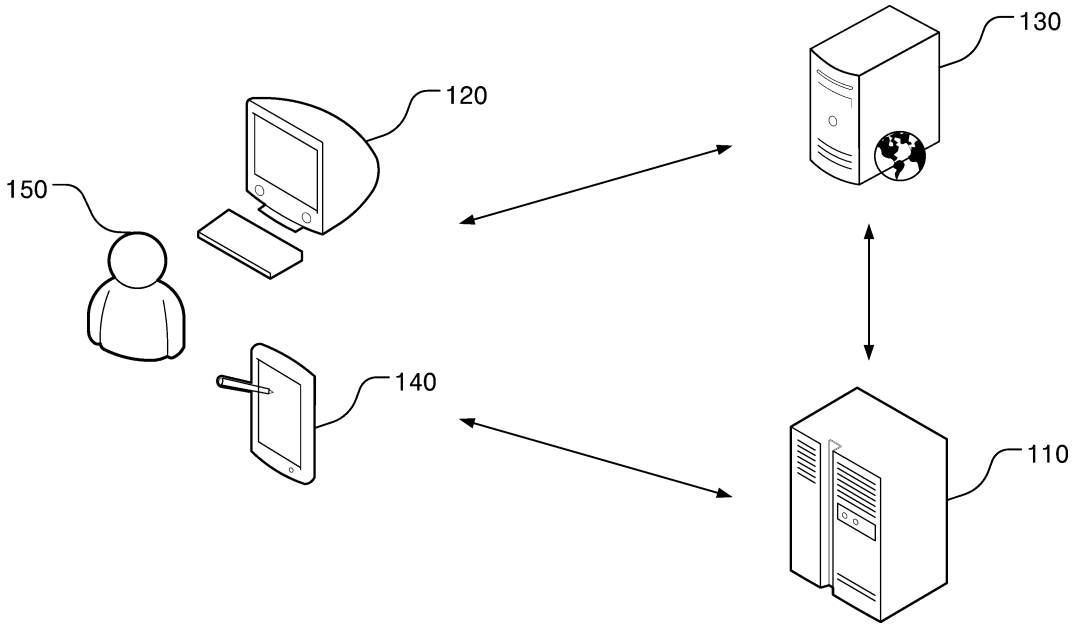
208: 데이터 생성부 209: 데이터 전송부

220: 제1 단말 230: 서비스 제공 서버

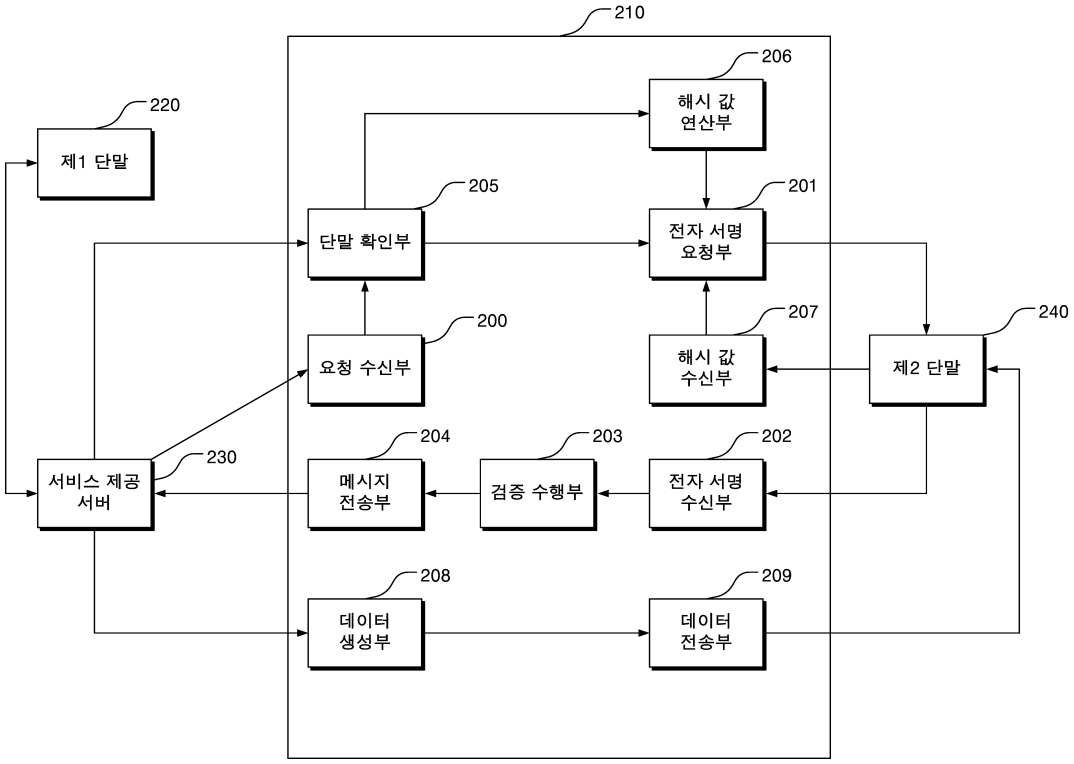
240: 제2 단말

도면

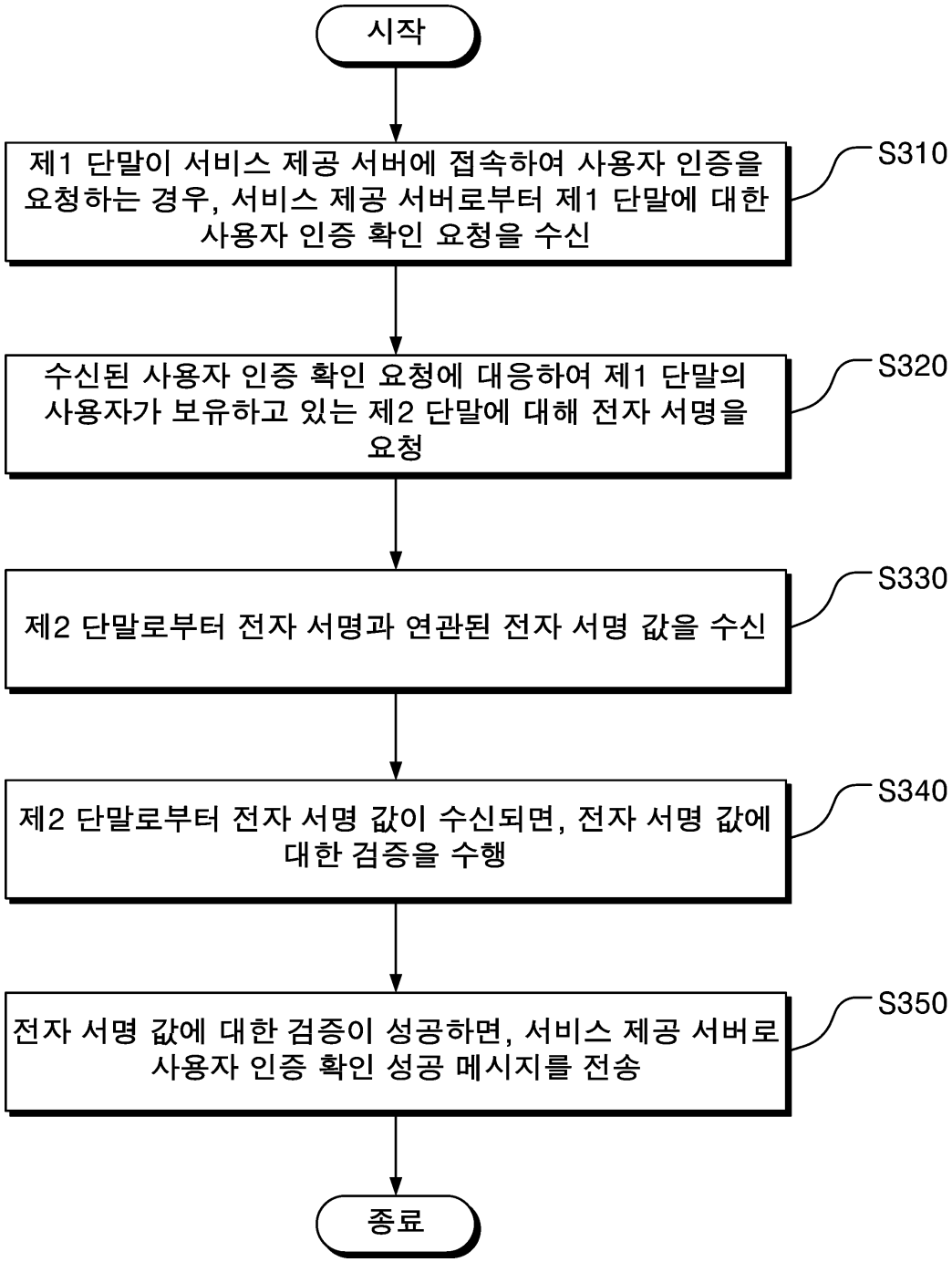
도면1


130
120
150
140
110

도면2


210
206
해시 값
연산부
220
제1 단말
205
201
단말 확인부
전자 서명
요청부
207
240
200
요청 수신부
해시 값
수신부
제2 단말
204
203
202
230
서비스 제공
서버
메시지
전송부
검증 수행부
전자 서명
수신부
208
209
데이터
생성부
데이터
전송부

도면3


시작
제1 단말이 서비스 제공 서버에 접속하여 사용자 인증을 요청하는 경우, 서비스 제공 서버로부터 제1 단말에 대한 사용자 인증 확인 요청을 수신
S310
수신된 사용자 인증 확인 요청에 대응하여 제1 단말의 사용자가 보유하고 있는 제2 단말에 대해 전자 서명을 요청
S320
제2 단말로부터 전자 서명과 연관된 전자 서명 값을 수신
S330
제2 단말로부터 전자 서명 값이 수신되면, 전자 서명 값에 대한 검증을 수행
S340
전자 서명 값에 대한 검증이 성공하면, 서비스 제공 서버로 사용자 인증 확인 성공 메시지를 전송
S350
종료