(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0035147
(43) 공개일자 2020년04월01일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/00* (2006.01)
H04L 9/14 (2006.01)
(52) CPC특허분류
H04L 9/3268 (2013.01)
H04L 9/006 (2013.01)
(21) 출원번호 10-2020-7007314
(22) 출원일자(국제) 2018년10월05일
심사청구일자 2020년03월12일
(85) 번역문제출일자 2020년03월12일
(86) 국제출원번호 PCT/US2018/054670
(87) 국제공개번호 WO 2019/103794
국제공개일자 2019년05월31일
(30) 우선권주장
15/819,605 2017년11월21일 미국(US)

(71) 출원인
퀴랄트, 아이엔씨.
미국 코네티컷 06510-2802 뉴 헤이븐 채플 스트리트 900 플로어 10
(72) 발명자
퀴랄트 마이클
미국 뉴욕 10607 화이트 플레인스 그린에이커스 레인 7
톨버트 존 더블유.
미국 워싱턴 98092 오번 160번가 사우스이스트 37216
(74) 대리인
리앤목특허법인

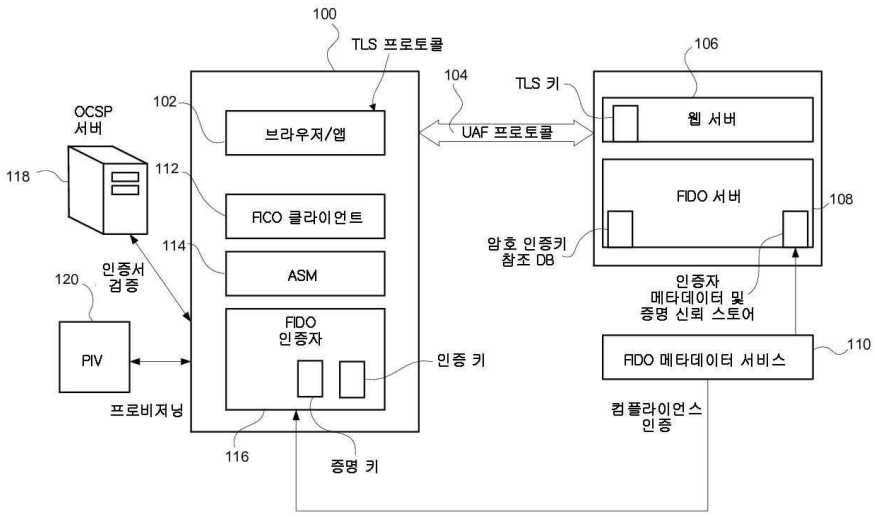
전체 청구항 수 : 총 35 항

(54) 발명의 명칭 **디지털 인증서에 대한 모바일 인증 상호 운용성**

(57) 요 약

계층적 인증 시스템과 비-계층적 인증 시스템을 통합하기 위한 시스템 및 방법. 상기 시스템 및 방법은 하나의 구성에서 모바일 장치가 고도의 기밀 데이터에 액세스하는 것을 허용함과 동시에 계층적 인증 시스템 및 비-계층적 인증 시스템 양자 모두를 이용해 매우 안전한 환경을 보장하여 고도로 신뢰성 있는 인증 프로세스를 제공하도록 기능 하는 모바일 앱으로서 제공된다.

대 표 도



(52) CPC특허분류
H04L 9/14 (2013.01)
H04L 2209/80 (2013.01)

명 세 서

청구범위

청구항 1

네트워크 접속을 통해 온라인 서비스 서버에 액세스하려고 제1 인증 서버 및 제2 인증 서버로부터 인증을 요청하는 모바일 장치를 인증하는 시스템에 있어서,

상기 모바일 장치의 인증 시스템은,

상기 모바일 장치상의 저장 장치상에 저장된 온라인 서비스에 연관된 모바일 앱 - 상기 모바일 앱이 개방될 때, 온라인 서비스에 액세스하기 위한 요청이 생성되고, 상기 요청에는 상기 모바일 장치에 연관된 데이터가 포함되며, 상기 모바일 장치는 상기 요청을 상기 온라인 서비스에 연관된 온라인 서비스 서버에 전송함 -;

상기 온라인 서비스에 액세스하기 위한 요청을 수신하고 상기 제1 인증 서버에 전송되는 제1 인증 요청을 생성하는 상기 온라인 서비스 서버 - 상기 제1 인증 요청은 상기 모바일 장치에 연관된 데이터를 포함함 -;

상기 제1 인증 요청을 수신하고 상기 모바일 장치에 연관된 데이터에 부분적으로 기초하여 제1 인증을 생성하는 상기 제1 인증 서버;

상기 제1 인증을 상기 온라인 서비스 서버에 전송하는 상기 제1 인증 서버;

상기 모바일 장치로 전송되는 신원 증명 요청을 생성하는 상기 온라인 서비스 서버;

제2 인증 서버에 전송되는 제2 인증 요청을 생성하는 상기 모바일 장치 - 상기 제2 인증 요청에는 상기 모바일 장치의 사용자에 연관된 데이터가 포함됨 -;

상기 제2 인증 요청을 수신하고 상기 모바일 장치의 사용자에 연관된 데이터에 부분적으로 기초하여 제2 인증을 생성하는 상기 제2 인증 서버;

상기 제2 인증을 상기 모바일 장치에 전송하는 상기 제2 인증 서버;

상기 제2 인증을 상기 온라인 서비스 서버에 전송하는 상기 모바일 장치; 및

상기 모바일 장치가 상기 제1 인증 및 상기 제2 인증에 기초하여 상기 온라인 서비스 서버를 통해 상기 온라인 서비스에 액세스하는 것을 허용하는 상기 온라인 서비스 서버;

를 포함하는, 모바일 장치의 인증 시스템.

청구항 2

제1항에 있어서,

상기 제1 인증 서버는 비-계층적 인증 시스템을 포함하는, 모바일 장치의 인증 시스템.

청구항 3

제2항에 있어서,

상기 비-계층적 인증 시스템은 고속 신원 온라인 인증 시스템을 포함하는, 모바일 장치의 인증 시스템.

청구항 4

제2항에 있어서,

상기 제1 인증은 전송 계층 보안을 더 포함하는, 모바일 장치의 인증 시스템.

청구항 5

제4항에 있어서,

인증자 포맷의 선택은 상기 모바일 앱이 실행되는 플랫폼에 상응하는, 모바일 장치의 인증 시스템.

청구항 6

제1항에 있어서,

상기 제2 인증 서버는 계층적 인증 시스템을 포함하는, 모바일 장치의 인증 시스템.

청구항 7

제6항에 있어서,

상기 계층적 인증 시스템은 공개키 기반 구조 인증 시스템을 포함하는, 모바일 장치의 인증 시스템.

청구항 8

제1항에 있어서,

상기 제2 인증 요청은 디지털 인증서를 포함하는, 모바일 장치의 인증 시스템.

청구항 9

제8항에 있어서,

상기 디지털 인증서에는 사용자 이름 및 만료 일자가 포함되어 있는, 모바일 장치의 인증 시스템.

청구항 10

제8항에 있어서,

상기 디지털 인증서에는 고유 일련번호가 포함되어 있는, 모바일 장치의 인증 시스템.

청구항 11

제8항에 있어서,

상기 디지털 인증서에는 사용자의 공개키가 포함되어 있는, 모바일 장치의 인증 시스템.

청구항 12

제8항에 있어서,

상기 디지털 인증서에는 상기 디지털 인증서에 연관된 권리 및 사용에 관한 정보가 포함되어 있는, 모바일 장치의 인증 시스템.

청구항 13

제8항에 있어서,

상기 디지털 인증서에는 상기 디지털 인증서를 발행한 인증 기관의 이름이 포함되어 있는, 모바일 장치의 인증 시스템.

청구항 14

제13항에 있어서,

상기 디지털 인증서에는 인증 기관의 서명이 포함되어 있는, 모바일 장치의 인증 시스템.

청구항 15

제14항에 있어서,

상기 디지털 인증서에는 상기 디지털 인증서에 서명하는데 사용된 알고리즘을 식별하는 알고리즘 식별자가 포함되어 있는, 모바일 장치의 인증 시스템.

청구항 16

제8항에 있어서,

상기 디지털 인증서에는 도출한 개인 신원 확인 크리덴셜이 포함되어 있는, 모바일 장치의 인증 시스템.

청구항 17

모바일 앱을 통해 온라인 서비스 서버에 액세스하려고 하는 네트워크 접속을 지니는 사용자의 모바일 장치를 인증하는 방법으로서, 상기 온라인 서비스 서버는 제1 인증 서버 및 제2 인증 서버로부터 인증을 요청하는, 모바일 장치를 인증하는 방법에 있어서,

상기 모바일 장치의 인증 방법은,

모바일 앱을 개방하고 상기 온라인 서비스 서버에 액세스하기 위한 요청을 생성하는 단계 - 상기 요청에는 상기 모바일 장치에 연관된 데이터가 포함됨 -;

상기 네트워크 접속을 통해 상기 요청을 온라인 서비스에 연관된 온라인 서비스 서버에 전송하는 단계;

상기 모바일 장치에 연관된 데이터를 포함하는 제1 인증 요청을 생성하는 단계;

상기 온라인 서비스 서버로부터 상기 제1 인증 서버로 상기 제1 인증 요청을 전송하는 단계;

상기 모바일 장치에 연관된 데이터에 부분적으로 기초하여 제1 인증을 생성하는 단계;

상기 제1 인증을 상기 제1 인증 서버로부터 상기 온라인 서비스 서버로 전송하는 단계;

신원 증명 요청을 생성하는 단계;

상기 신원 증명 요청을 상기 온라인 서비스 서버로부터 상기 모바일 장치로 전송하는 단계;

상기 모바일 장치의 사용자에 연관된 데이터를 포함하는 제2 인증 요청을 생성하는 단계;

상기 제2 인증 요청을 상기 모바일 장치로부터 상기 제2 인증 서버로 전송하는 단계;

상기 모바일 장치의 사용자에 연관된 데이터에 부분적으로 기초하여 제2 인증을 생성하는 단계;

상기 제2 인증을 상기 제2 인증 서버로부터 상기 모바일 장치로 전송하는 단계;

상기 제2 인증을 상기 모바일 장치로부터 상기 온라인 서비스 서버로 전송하는 단계; 및

상기 제1 인증 및 상기 제2 인증을 처리하여 상기 온라인 서비스에 대한 액세스가 상기 온라인 서비스 서버를 통해 상기 모바일 장치에 제공되게 하는 단계;

를 포함하는, 모바일 장치의 인증 방법.

청구항 18

제17항에 있어서,

상기 제1 인증 서버는 비-계층적 인증 시스템을 이용하는, 모바일 장치의 인증 방법.

청구항 19

제18항에 있어서,

상기 비-계층적 인증 시스템은 고속 신원 온라인 인증 시스템을 포함하는, 모바일 장치의 인증 방법.

청구항 20

제18항에 있어서,

상기 제1 인증에는 전송 계층 보안이 더 포함되는, 모바일 장치의 인증 방법.

청구항 21

제20항에 있어서,

인증자 포맷의 선택은 상기 모바일 앱이 실행되는 플랫폼에 상응하는, 모바일 장치의 인증 방법.

청구항 22

제17항에 있어서,

상기 제2 인증 서버는 계층적 인증 시스템을 이용하는, 모바일 장치의 인증 방법.

청구항 23

제23항에 있어서, 상기 계층적 인증 시스템은 공개키 기반 구조 인증 시스템을 사용하는, 모바일 장치의 인증 방법.

청구항 24

제17항에 있어서,

상기 제2 인증 요청에는 디지털 인증서가 포함되는, 모바일 장치의 인증 방법.

청구항 25

제24항에 있어서,

상기 디지털 인증서에는,

사용자 이름;

만료 일자;

고유 일련번호;

사용자의 공개키;

상기 디지털 인증서에 연관된 권리 및 사용에 관한 정보;

상기 디지털 인증서를 발행한 인증 기관의 이름; 및

인증 기관의 서명;

으로 구성되는 그룹으로부터 선택된 데이터가 포함되는, 모바일 장치의 인증 방법.

청구항 26

컴퓨터 판독가능 명령어들을 포함하는 프로그램이 저장된 비-일시적 컴퓨터-이용가능 저장 매체로서, 상기 프로그램이 컴퓨터, 디지털 신호 프로세서, 필드-프로그램가능 게이트 어레이, 주문형 집적 회로, 마이크로프로세서, 마이크로컨트롤러 또는 기타 유형의 프로그램가능 하드웨어 상에서 실행될 때, 상기 컴퓨터 판독가능 명령어들은 청구항 제17항에 따른 방법의 단계들을 수행하도록 구현될 수 있는, 비-일시적 컴퓨터-이용가능 저장 매체.

청구항 27

네트워크 접속을 지니는 사용자의 모바일 장치를 등록하는 방법으로서, 사용자가 모바일 장치상의 저장 장치상에 저장된 앱에 연관된 온라인 서비스에 대한 액세스를 요청하는, 모바일 장치를 등록하는 방법에 있어서,

상기 모바일 장치의 등록 방법은,

상기 모바일 장치상에서 상기 앱을 개시하는 단계;

사용자에게 사용자에 연관된 식별 정보를 입력할 것을 프롬프트하는 단계;

상기 식별 정보를 확인하는 단계;

상기 모바일 장치로부터 제1 인증 서버로 등록 요청을 전송하는 단계;

상기 앱으로부터 상기 온라인 서비스에 연관된 온라인 서비스 서버로 등록 통지를 전송하는 단계;

상기 온라인 서비스 서버로부터 상기 모바일 장치로 등록 신호를 전송하는 단계 - 상기 등록 신호에는 상기 온

라인 서비스에 연관된 데이터가 포함됨 -;

상기 앱으로부터 제2 인증 서버로 확인 요청을 전송하는 단계 - 상기 확인 요청에는 모바일 장치 및 사용자에 연관된 데이터가 포함됨 -;

상기 제2 인증 서버로부터 상기 앱으로 확인 데이터를 전송하는 단계 - 상기 확인 데이터는 상기 확인 요청에 포함된 데이터를 확인하고 상기 제2 인증 서버에 연관된 데이터를 포함함 -;

상기 확인 데이터를 상기 앱으로부터 상기 온라인 서비스 서버로 그리고 상기 제1 인증 서버로 전송하는 단계;

상기 확인 데이터 중 적어도 일부를 상기 제1 인증 서버에 연관된 저장 장치상에 저장하는 단계;

상기 앱에 확인 결과를 전송하는 단계; 및

사용자에게 등록 결과를 통지하는 단계;

를 포함하는, 모바일 장치의 등록 방법.

청구항 28

제27항에 있어서,

상기 제1 인증 서버는 비-계층적 인증 시스템을 이용하는, 모바일 장치의 등록 방법.

청구항 29

제28항에 있어서,

상기 비-계층적 인증 시스템은 고속 신원 온라인 인증 시스템을 포함하는, 모바일 장치의 등록 방법.

청구항 30

제27항에 있어서,

상기 등록 통지에는 전송 계층 보안이 포함되는, 모바일 장치의 등록 방법.

청구항 31

제30항에 있어서,

인증자 포맷의 선택은 상기 모바일 앱이 실행되는 플랫폼에 상응하는, 모바일 장치의 등록 방법.

청구항 32

제27항에 있어서,

상기 제2 인증 서버는 계층적 인증 시스템을 이용하는, 모바일 장치의 등록 방법.

청구항 33

제32항에 있어서,

상기 계층적 인증 시스템은 공개키 기반 구조 인증 시스템을 사용하는, 모바일 장치의 등록 방법.

청구항 34

제27항에 있어서,

상기 확인 요청에는 디지털 인증서가 포함되는, 모바일 장치의 등록 방법.

청구항 35

컴퓨터 판독가능 명령어들을 포함하는 프로그램이 저장된 비-일시적 컴퓨터-이용가능 저장 매체로서, 상기 프로그램이 컴퓨터, 디지털 신호 프로세서, 필드-프로그램가능 게이트 어레이, 주문형 집적 회로, 마이크로프로세서, 마이크로컨트롤러 또는 기타 유형의 프로그램가능 하드웨어 상에서 실행될 때, 상기 컴퓨터 판독가능 명령어들은 청구항 제27항에 따른 방법의 단계들을 수행하도록 구현될 수 있는, 비-일시적 컴퓨터-이

용가능 저장 매체.

발명의 설명

기 술 분 야

[0001] 본원은 모바일 장치상에서 처리되는 리소스(resources)의 보안에 관한 것이다. 구체적으로 기술하면, 본원은 모바일 장치상에서 기밀 데이터를 안전하게 처리하기 위한 인증 시스템에 관한 것이다.

배 경 기 술

[0002] 인증 시스템은 오랫동안 널리 사용되어 왔다. 초기 인증 시스템 중 일부에는 컴퓨터의 사용자에 연관될 수 있는 간단한 패스워드를 사용하는 것이 포함된다. 사용자는 자신을 식별하고 패스워드를 입력한 다음에 개인에 제대로 연관된 정보에 액세스할 수 있게 된다. 여기서 이해할 점은 사람마다 액세스 수준이 다를 수 있다는 점이다.

[0003] 이러한 유형의 시스템에 관련된 주요 문제점은 보안과 관련하여 패스워드가 주지의 사실로 신뢰 가능하지 않다는 점이다. 사람이 컴퓨터를 개방했는지를 시각적으로 식별하기 위한 이미징 소프트웨어를 사용하는 것, 또는 사람을 식별하기 위해 생체 인식(예컨대, 지문, 안구 스캔 등)을 사용하는 것을 포함하여 사용자 인증에 대한 다른 많은 수법이 있다. 패스워드 기반 시스템에서 관측되는 또 다른 문제로는 일상적인 장치의 디폴트 패스워드를 이용하는 사물 인터넷(Internet of Things; IoT)에 의해 자행되는 돌발적인 서비스 거부 공격(Denial of Service attacks)을 들 수 있다.

[0004] 강력하게 검사된 크리덴셜이 필요한 경우 공개키 기반 구조(PKI; Public Key Infrastructure)가 효과적으로 사용되었다. PKI는 그의 아키텍처에 대한 다음과 같은 주요 구성요소들을 이용하여 강력한 신원 증명을 제공한다;

[0005] 1. 디지털 인증서. 사용자와 기기를 식별하는 신뢰할 수 있는 제3 당사자에 의해 발행된 디지털 "신원". 이는 월렛(wallets)에나 또는 디렉토리에 안전하게 저장될 수 있다.

[0006] 2. 공개 및 개인 키. 이들은 비밀 개인키와 수학적으로 관련된 공개키에 기초하여 안전한 통신을 위한 PKI의 기초를 형성한다.

[0007] 3. 인증 기관(Certificate Authority; CA). 신뢰할 수 있는 독립적인 디지털 인증서 공급자로서의 역할을 한다.

[0008] PKI는 매우 강력하게 검사된 크리덴셜을 제공할 수 있는 계층적 시스템으로 설명될 수 있다. PKI는 그와 같이 강력한 표준이므로 개인, 조직 및 기기를 포함한 여러 영역에 대한 신원 인증을 제공하기 위해 정보 보안 영역에서 광범위하게 사용되어 왔다. 신원에 바인딩된 공개키를 사용하고 인증서를 생성한 조직에 관한 정보에 액세스할 수 있는 메커니즘을 제공하며 개인이 자신의 개인키를 제어할 수 있게 함으로써, PKI는 임의의 신뢰 당사자 애플리케이션이 신원의 출처로 되돌려 볼 수 있도록 하는 기능을 제공한다. 이러한 계층적 수법은 신뢰 당사자에게 제시된 신원의 소유권에 관한 높은 수준의 신뢰를 제공하며, 이는 출처가 검증되고 신뢰할 수 있는 엔티티(예컨대, 미국 정부)일 때 강화된다.

[0009] 문제를 더 복잡하게 만드는 것은, 편의, 유연성 및 접근성을 위해 고정 컴퓨터를 모바일 장치로 대체해야 하는 경제의 모든 부문에서 강력한 추세가 나타나고 있다는 것이다. 또한, 인증 기관이 애플리케이션 공급자와 결합해제되고 사용자가 이동 중이며 회사가 자신의 시스템에 액세스하는지 이해하기 위해 어려움을 겪고 있는 다양한 신원 관리 에코시스템이 개발되고 있다. 물리적 워크플레이스(physical workplace)작업 공간에 대해 완탈한(untethered) 이동성은 막대한 효율성을 가져오며 신중하게 구현하면 고용주와 직원 모두에게 이익이 된다. 모바일 컴퓨팅은 최신 아키텍처를 도입하고, 사일로(silo)를 타파하며, 여러 신원과 신뢰에 의존하는 관련없는 당사자 간 피어 투 피어 트랜잭션(peer to peer)을 도입하여 그러한 트랜잭션을 수행하는 것이다. 모바일 컴퓨팅은 사람들이 일하고 업무를 수행하는 방식을 변화시키고 있다. 예를 들어, 과거에는 사람이 매우 안전한 문서에 액세스하기를 원하면 터미널에 앉아 개인이 해당 정보에 액세스할 수 있음을 확인하는 일련의 작업을 통해 로그인해야 했다. 그러나 모바일 장치가 진보함에 따라 훨씬 더 많은 작업을 수행할 수 있게 되면서 개인이 자신의 모바일 장치로 고도의 기밀 정보에 액세스할 수 있도록 하는 압력이 가중되었다.

[0010] 모바일 장치로, 다단계 인증, 고유의 기능(다시 말하면, 앱) 및 웹 브라우징의 빠른 통합이 이루어져 왔다. 최근의 가장 중요한 진보들 중의 하나는 2단계로서의 전화(phone-as-second-factor)이다. 다시 말하면, 셀룰러폰은 "당신이 휴대한 것"이다. 공공연한 물리적 요소는 개인 식별 번호(PIN; Personal Identification Number) 또는 패스워드(당신이 알고있는 것) 또는 점차로 통합 생체인식에 의해 활성화된다.

[0011] 그러나 지금까지는 개인 신원 확인(Personal Identity Verification; PIV)과 같은 강력한 신원 증명 솔루션이 주로 스마트 카드상에 배포되었다. 관행에 따라, PIV 크리덴셜은 보안 개인키가 포함된 스마트 카드상에서 수행된다. 마찬가지로 지금까지는 PIV 크리덴셜의 상호 운용성을 위해서는 클라이언트-측 소프트웨어 구성요소와 백엔드 CA의 특정 PKI 통합이 필요하였다. 정부는 무엇보다도 대부분의 모바일 장치에 기존의 스마트 카드 리더가 없고 모바일 인증을 위해 NFC를 활용하려는 노력이 힘들어지면서 PIV 카드를 모바일 장치와 함께 사용하는 데 어려움을 겪어 왔다. 부분적으로는, 이러한 문제로 인해 미국 정부는 PKI의 보안 모델을 모바일 장치로 확장하는 데 중점을 둔 DPC(Derived PIV Credential) 이니셔티브를 만들었다. 2014년에 출시된 동안, DPC는 여전히 초기 채택 모드에 있으며 배포가 매우 복잡한 것으로 입증되었다. 실제로 이것은 미국 정부의 수백만 대의 모바일 장치가 강력한 인증으로 보호되고 있지 않음을 의미한다.

[0012] 민간 부문 기업은 여러 미국 정부 기관과 유사한 요구에 직면하여 사용자의 모바일 장치로부터 보안 콘텐츠에 대한 액세스를 개방한다. 항공 우주 및 방위 산업을 일 예로 들어 보기로 한다. 이러한 산업의 모든 회사는 자신의 사용자, 공급 업체 및 경우에 따라서는 심지어 고객에게 강력하게 검사된 x.509 신원 크리덴셜을 제공하기 위해 스마트카드(SmartCard) 기술에 상당한 재정 투자를 하였다.

[0013] X.509는 PKI가 디지털 인증서 및 공개키 암호화를 관리하는 표준이며 보안 웹 및 전자메일 통신에 사용되는 전송 계층 보안 프로토콜의 핵심 부분이다. X.509 인증서는 국제 X.509 PKI 표준을 사용하여 공개키가 상기 인증서에 포함된 사용자, 컴퓨터 또는 서비스 신원에 속함을 확인하는 디지털 인증서이다.

[0014] 모바일 장치로 기밀 데이터에 액세스하는 이러한 민간 부문 기업 사용자는 그의 일상 업무를 수행하기 위해 스마트폰과 태블릿에 점차로 의존하고 있다. 그러나 이러한 조직의 데이터 소유자는 (인증에서부터 시작하는) 보안 문제로 인해 모바일 장치로부터 기밀 정보에 대한 액세스를 제공하는 것을 주저하였다.

[0015] 이러한 모든 모바일 장치 이용의 결과로 비-계층적 인증 시스템이 확산되었다. 이러한 비-계층적 인증 시스템은 모바일 장치의 주요 기능과 새로운 컴퓨팅 기법을 활용하여 모바일 장치와 신뢰 당사자(또는 개인, 장치 또는 기타 등등에게 서비스를 제공하는 조직) 간에 더 사용자 친화적이고 마찰이 없는 인증 프로세스를 제공할 수 있다는 이점을 제공한다.

[0016] 강력한 보안 요소와 광범위한 고유 암호 기법의 조합으로 FIDO(Fast Identity Online) 에일리언스(Alliance)가 추진되었고 결과적으로는 본질적으로 모든 모바일 장치로부터의 인증이 탈바꿈되었다. FIDO는 산업 표준, 테스트 및 검사된 암호화 알고리즘을 사용하여 강력한 인증 표준을 사용하는 신원 관리 벤더, 제품 회사 및 서비스 공급업체의 컨소시엄이다. FIDO 표준은 다단계 인증을 위한 새로운 패러다임을 가능하게 하는데, 일단 개인이 자신의 개인 모바일 장치에 인증하게 되면 해당 장치를 사용하여 다른 디지털 서비스에 인증할 수 있어야 한다.

[0017] NIST SP 800-63-3 DIGITAL IDENTITY GUIDELINES의 최근 간행물에는 공개 네트워크를 통해 정부 IT 시스템과 함께 작업하는 직원, 계약자, 민간 개인 및 상업 기관과 같은 사용자의 신원 증명 및 인증에 대한 주목할만한 변경 사항이 요약되어 있다. https://pages.nist.gov/800-63-3/sp800-63-3.html을 참조하기 바란다. 상기 문헌에 요약된 2가지 중요한 변경사항은 (1) 인증자 보증으로부터 신원 보증을 분리하는 것 및 (2) FIDO U2F 및 UAF와 같은 기술을 최고 수준 - AAL3(Authenticator Assurance Level 3) 내에서 인식하는 것이다.

[0018] 결과적으로, FIDO 프로토콜은 인증을 위한 비대칭 공개키(PK) 암호 기법에 대한 정부 지침을 충족하므로 현재 실행 가능한 옵션으로 간주 된다. 이로 인해 이전에는 PKI를 가능하게 하는데 너무 어려웠거나 값비싼 FIDO 가능 레거시 및 클라우드 기반 애플리케이션 및 리소스에 대한 강력한 모바일 인증이 이루어지게 된다.

[0019] FIDO의 제한들 중의 하나는 PIV 크리덴셜을 안전하게 관리하고 인증 전에 신뢰할 수 있는 당사자에게 사용자의 신원을 다시 확인하는 계층적 시스템인 PKI와 직접 통합할 수 없다는 것이다. 이로 인해 FIDO에 의해 제공된 AA3 레벨 인증과 함께 정부 표준 식별 크리덴셜을 직접 사용하는 것이 가능하지 않다.

[0020] 예를 들어, FIDO 에일리언스에 의해 발행된 “FIDO Alliance White Paper: Leveraging FIDO Standards to Extend the PKI Security Model in United States Government Agencies"이라는 제목의 논문에는 FIDO가 미국 정부 인증 에코시스템을 확장할 때 어떠한 방식으로 PKI를 보완할 수 있는지가 기재되어 있다. https://fidoalliance.org/wp-content/uploads/White-Paper-Leveraging-FIDO-Standards-to-Extend-the-PKI-Security-Model-in-US-Govt-Agencies.pdf 상기 논문에는 PKI에 관련된 문제 및 결점이 자세히 기재되어 있지만 PIV가 미국 정부의 선택 크리덴셜로 계속 유지해야 한다는 점이 인정되어 있다.

[0021] 2017년 3월 17일자 “Merging FIDO and PIV could help feds achieve strong authentication goals"이라는 제

목의 또 다른 논문이 SecureID News에 의해 제공되어 있다. https://www.secureidnews.com/news-item/merging-fido-and-piv-could-help-feds-achieve-strong-authentication-goals/ 이러한 논문에는 위에 참조한 white paper가 요약되어 있다. 몇 가지 주요 발췌록에는 "PKI enabling applications - both legacy and new - is not an easy process" 및 "If full-blown PIV card presentment were doable, that would be the preferred route. But in cases where this is not possible, PIV derived credentials would be next followed by FIDO derived credentials." 가 포함되어 있다. 다시 말하면, 계층적 PKI 시스템은 현재 비-계층적 FIDO 세계와 완전히 통합될 수 없다.

[0022] 따라서, 이는 본 산업에서 현재 다루어지고 있는 문제, 다시 말하면 PKI와 같은 시스템에서 제공하는 강력한 검사 크리덴셜과 아울러, FIDO와 같은 산업 표준, 테스트 및 검사된 암호화 알고리즘을 사용하는 강력한 인증 표준을 어떠한 방식으로 활용하는 지에 관련된 문제이다. 위에 참조한 논문에서 언급한 바와 같이, 아직 달성된 효과적인 솔루션은 없다.

발명의 내용

[0023] 이리하여 바람직한 것은 모바일 장치를 사용하는 사용자에게 강력한 인증을 제공하는 시스템 및 방법이다.

[0024] 또한, 계층적 인증 시스템과 비-계층적 인증 시스템을 가교(bridging)하는 시스템 및 방법을 제공하는 것이 바람직하다.

[0025] 또한, 모바일 장치상의 디지털 크리덴셜이 계층적 인증 시스템으로 검사될 수 있게 하고, 계층적 인증 시스템의 검사를 이용하는 비-계층적 인증 시스템으로 동일한 신원이 차후에 검사될 수 있게 하는 시스템 및 방법을 제공하는 것이 여전히 바람직하다.

[0026] 또한, FIDO 인증 시스템이 PKI 인증 시스템에 의해 제공되는 신원의 검증 및 확인을 사용하고 그에 의존하도록 모바일 장치용 FIDO 인증 시스템 및 PKI 인증 시스템을 가교하는 시스템 및 방법을 제공하는 것이 바람직하다.

[0027] 따라서, 일 구성에서, FIDO 공개키 암호 기법의 비-계층적 포맷을 PKI의 인증 기관 기반 포맷과 가교하는 시스템이 제공된다.

[0028] PKI의 주요 이점은 개인, 조직 및 기기를 포함한 여러 영역에 대한 신원 인증을 제공하기 위해 정보 보안 영역에서 광범위하게 사용된 강력한 표준을 포함한다는 것이다. PKI는 신원에 바인딩되는 공개키를 사용하기 때문에 매우 강력한 표준으로 간주 된다. 또한, PKI는 인증서를 만든 조직에 관한 정보에 액세스할 수 있는 메커니즘을 제공한다. 여전히 또한, PKI를 사용하면 개인이 개인키를 제어할 수 있다. 이 때문에, PKI를 사용하면 신뢰 당사자 애플리케이션이 연속적인 체인을 통해 신원의 출처로 "되돌려 보는(reach back)" 것이 허용된다. 이는 계층적 인증 시스템의 일 예이다. 이러한 계층적 수법은 신뢰 당사자에게 제시된 신원의 소유권에 대해 매우 높은 수준의 신뢰를 제공하며, 이는 상기 출처가 검증되고 신뢰성이 높은 엔티티일 때 강화된다.

[0029] PKI 수법의 핵심 구성요소는 x.509 포맷의 검증된 디지털 인증서이며, 여기에는 일반적으로 여러 가지 방식(예컨대, 소프트 또는 하드 토큰)으로 신원 소유자에게 제공될 수 있는 이하의 정보 속성, 1) 인증서 사용자 이름; 2) 만료 일자; 3) CA에 의해 상기 인증서에 할당된 고유 일련번호; 4) 사용자의 공개키; 5) 인증서에 연관된 권리 및 사용에 관한 정보; 6) 인증서를 발행한 인증 기관의 이름; 7) CA 서명; 및 8) 인증서 서명에 사용된 알고리즘을 식별하는 알고리즘 식별자;가 포함된다.

[0030] 인증서는 인증서를 소유한 개인 또는 장치의 신원을 검증하는 데 사용할 수 있는 전자 문서가 되며 신뢰 당사자에게 매우 신뢰할 수 있는 응답을 제공한다(다시 말하면, 그것이 계층적이므로 출처로 다시 지속적인 체인을 추적할 수 있음). 그러나 이러한 유형의 시스템을 모바일 장치로 확장하는 데에는 큰 어려움이 있다. 이는 상대적으로 높은 컴퓨팅 요구사항과 인증서 및 그의 정보에 액세스할 때 신뢰 당사자와 사용자 및 개인 정보를 공유하는 PKI의 성향 때문이다.

[0031] 반면에 FIDO 프로토콜은 표준 공개키 암호 기법을 사용하여 장치와 신뢰 당사자(예컨대, 온라인 서비스) 간에 강력한 인증을 제공한다. FIDO UAF 프로토콜은 1) 등록; 2) 인증; 3) 트랜잭션 확인; 및 4) 등록 해제;를 포함한다.

[0032] FIDO 등록 프로세스는 일반적으로 다음과 같이 진행된다.

[0033] 첫째, 사용자에게는 온라인 서비스의 수락 폴리시와 매치(match)하는 사용 가능한 FIDO 인증자를 선택하라고 프롬프트된다.

[0034] 둘째, 사용자는 지문 리더의 스와이핑, 안전한 PIN 입력 또는 다른 어떤 방법으로 신뢰할 수 있는 방법의 사용과 같은 일부 사용자 제스처를 사용하여 FIDO 인증자를 잠금해제한다.

[0035] 셋째, 사용자의 인증자는 인증자, 온라인 서비스 및 사용자 계정에 고유한 새로운 공개/개인 키 쌍을 만든다.

[0036] 넷째, 공개키는 온라인 서비스에 송신되고 사용자 계정에 연관된다. 여기서 유념해야 할 점은 개인키 및 로컬 인증 방법에 관한 정보가 로컬 장치를 떠나지 않는다는 점이다.

[0037] 주요 이점은 FIDO를 통해 에이전시(agency) 및 상용 신뢰 당사자 애플리케이션이 고가인 기존의 CA 모델 없이 공개키 암호 기법의 보안 이점을 얻을 수 있게 된다는 것이다.

[0038] 그러나 FIDO 등록 및 인증 프로세스의 제한은 그것이 인증자 소유자의 신원을 알기 위해 사전 신원-바인딩 단계를 가정한다는 것이다. 다시 말하면, 등록 프로세스 이후로부터는 신원을 전제로 하는 것만으로도 충분하다(예컨대, 시스템이 등록 이후에는 다시 추적하지 않음). PKI가 이러한 취약점을 해결하기 때문에(예컨대, 신뢰성이 높은 출처로 다시 추적될 수 있기 때문에), PKI와 FIDO 양자 모두를 이용하여 하위 CA에 대한 필요 없이 모바일 장치를 사용하여 데이터에 액세스하려는 사용자를 식별하는 것이 좋다. MAIDC(Mobile Authentication Interoperability for Digital Certificates; 디지털 인증서에 대한 모바일 인증 상호 운용성) 시스템은 바로 이를 수행한다.

[0039] MAIDC 시스템은 인증서 크리덴셜을 FIDO 가능 백엔드 서비스에 가입시킨다. MAIDC 시스템은 도출한 PIV 크리덴셜(Derived PIV Credentials; DPC)에 대한 액세스 및 사용자의 모바일 장치(예컨대, 전화, 태블릿 등) 상에서의 DPC의 사용을 제어하는 모바일 인증 앱을 포함한다. 상기 시스템은 또한, 전자 리소스에 대한 액세스를 획득하는 데 이용되는 FIDO UAF(Universal Authentication Framework) 인증 방법을 제공한다.

[0040] 특히, FIDO 인증 도출 크리덴셜(x.509) 인증자는 FIDO UAF 프로토콜을 통해 인증 기관에 의해 발급되고 사용자의 모바일 장치 상에 안전하게 저장된 크리덴셜들 및 기업 웹 리소스들 간의 브리지 역할을 하게 된다.

[0041] 상용 및 정부 서버에 의해 FIDO 프로토콜이 점차 수용됨에 따라, 신뢰할 수 있는 식별을 사용하는 인증자는 예를 들어 개인의 프라이버시(privacy)를 보호하고 다양한 범위의 인증 활동에서 사용될 크리덴셜의 가치를 확장하면서, 비상 대응 관리 파트너, 에너지 유틸리티, 헬스케어 시설, 및 금융 회사에 대한 최초 대응자에 대해 IAL3 신원을 사용하여 NIST SP 800-63-3 AAL3 모바일 인증을 가능하게 할 수 있다.

[0042] MAIDC는 DPC를 이용하는데, 이는 호환 가능한 모바일 장치로 PIV 인증서를 미러링(mirroring)하게 한다. 이것이 의미하는 것은 정확한 사본이 호환 가능한 모바일 장치에 저장되지 않고 오히려 병렬 식별 인증서가 이용된다는 것이다. 그래서, 인증서는 카드 자체로부터 복사되지 않고 오히려 다른 한 위치로부터 복사되는데, 이것이 의미하는 것은 발급자 값이 다르지만 디지털 인증서를 이용하여 표준화된 방식으로 해당 정보를 전달하는 유사한 데이터(예컨대, 동일한 전자 메일, 동일한 이름 등)를 포함한다는 것이다. 액세스 제어 설정에서, 디지털 인증서는 서버에 제공되어 구문 분석되고, 그 속성은 수신 애플리케이션에 의해 인출되어 사용된다. 이는 도출한 크리덴셜의 PIV 속성을 FIDO 속성에 매핑하는 새로운 변환 기능 및 리소스를 허용한다.

[0043] 본원에 대해 이하의 용어와 정의가 적용될 것이다:

[0044] 본원 명세서에서 사용되는 용어 "데이터"는 임의의 표시, 신호, 마크, 심볼, 도메인, 심볼 세트, 표현, 및 영구적이든 일시적이든, 가시적, 청각적, 음향적, 전기적, 자기적, 전기자기적 또는 기타 명시적 정보를 나타내는 임의의 다른 물리적 형태 또는 형태들을 의미한다. 하나의 물리적 형태로 사전에 결정된 정보를 나타내는 데 사용되는 용어 "데이터"는 다른 물리적 형태 또는 형태들로 동일한 사전에 결정된 정보의 임의 및 모든 표현을 포함하는 것으로 간주될 것이다.

[0045] 본원 명세서에서 사용된 용어 "장치"는 전자 통신을 용이하게 하는 임의의 시스템을 의미한다. 이것에는 예를 들어 모바일폰, 호출기, 이메일 시스템, 컴퓨터, 태블릿, 앱, 스마트폰, 개인용 스마트 장치, 웨어러블 기술, 랩톱, 사물 인터넷(Internet of Things; IoT)과 같은 지능 기기가 포함될 수 있다. 종종, 통신 매체는 장치상의 애플리케이션과 관련될 것이다.

[0046] "사용자" 또는 "사용자들"이라는 용어는 단독으로 또는 하나 이상의 그룹에서, 동일하거나 다양한 장소에서, 동시에 또는 다양한 여러 시간에 어떤 방식으로 데이터에 액세스하는 사람 또는 사람들, 기기 또는 프로그램을 의미한다.

[0047] 본원 명세서에서 사용되는 용어 "네트워크"는 인터넷을 포함하여 모든 종류의 네트워크 및 인터-네트워크를 포

함하며, 임의의 특정 네트워크 또는 인터-네트워크에 국한되지 않는다.

[0048] "제1" 및 "제2"라는 용어는 하나의 요소, 세트, 데이터, 객체 또는 사물을 다른 요소, 세트, 데이터, 객체 또는 사물과 구별하기 위해 사용되며, 시간을 두고 상대적인 위치 또는 배치를 지정하는 데 사용되지 않는다.

[0049] 본원 명세서에서 사용된 용어 "결합된", "에 결합된", "접속된", "에 접속된", "와 접속된" 및 "접속"은 각각, (a) 직접적이거나, 하나 이상의 다른 장치, 기기, 파일, 프로그램, 애플리케이션, 매체, 구성요소, 네트워크, 시스템, 서브시스템 또는 수단을 통한 접속; (b) 직접적이거나, 하나 이상의 다른 장치, 기기, 파일, 프로그램, 애플리케이션, 매체, 구성요소, 네트워크, 시스템, 서브시스템 또는 수단을 통한 통신 관계, 및/또는 (c) 하나 이상의 장치, 기기, 파일, 프로그램, 애플리케이션, 매체, 구성요소, 네트워크, 시스템, 서브시스템 또는 수단 중의 어느 하나의 작동이 하나 이상의 다른 것 중의 어느 하나의 작동에 전체적으로 또는 부분적으로 의존하는 기능적 관계 중의 하나 이상을 구성하는, 둘 이상의 장치, 기기, 파일, 프로그램, 애플리케이션, 매체, 구성요소, 네트워크, 시스템, 서브시스템 및/또는 수단 간의 관계를 의미한다.

[0050] 본원 명세서에서 사용된 용어 "프로세스" 및 "프로세싱"은 예를 들어 연속적 또는 비-연속적, 동기식 또는 비-동기식, 데이터 라우팅, 데이터 수정, 데이터의 포맷팅 및/또는 변환, 데이터의 태깅 또는 주석, 데이터의 측정, 비교 및/또는 검토를 포함하지만 이에 국한되지 않는 액션 또는 일련의 액션을 의미하고, 프로그램을 포함하거나 포함하지 않을 수 있다.

[0051] 본원 명세서에서 사용된 "공개키 기반 구조" 및 "PKI"라는 용어는 디지털 인증서를 생성, 관리, 배포, 사용, 저장 및 취소하고 공개키 암호화를 관리하는 데 필요한 한 세트의 역할, 폴리시, 및 절차이다.

[0052] 본원 명세서에서 사용된 "고속 신원 온라인 얼라이언스(Fast Identity On Line Alliance)" 및 "FIDO"라는 용어는 표준 공개키 암호 기법을 사용하여 장치와 신뢰 당사자 간에 인증을 제공하고 등록, 인증, 트랜잭션 확인 및 등록 취소를 포함하는 프로토콜이다.

[0053] 일 예에서, 네트워크 접속을 통해 온라인 서비스 서버에 액세스하려고 제1 인증 서버 및 제2 인증 서버로부터 인증을 요청하는 모바일 장치를 인증하는 시스템이 제공되며, 상기 모바일 장치의 인증 시스템은 상기 모바일 장치상의 저장 장치상에 저장된 온라인 서비스에 연관된 모바일 앱을 포함한다. 상기 모바일 장치의 인증 시스템은 상기 모바일 앱이 개방될 때, 온라인 서비스에 액세스하기 위한 요청이 생성되도록 제공되고, 상기 요청에는 상기 모바일 장치에 연관된 데이터가 포함되며, 상기 모바일 장치는 상기 요청을 상기 온라인 서비스에 연관된 온라인 서비스 서버에 전송한다. 상기 모바일 장치의 인증 시스템은 상기 온라인 서비스 섭가 상기 온라인 서비스에 액세스하기 위한 요청을 수신하고 상기 제1 인증 서버에 전송되는 제1 인증 요청을 생성하도록 더 제공되고, 상기 제1 인증 요청은 상기 모바일 장치에 연관된 데이터를 포함한다. 여전히 또한, 상기 모바일 장치의 인증 시스템은 상기 제1 인증 요청을 수신하고 상기 모바일 장치에 연관된 데이터에 부분적으로 기초하여 제1 인증을 생성하고, 상기 제1 인증 서버는 상기 제1 인증을 상기 온라인 서비스 서버에 전송하도록 제공된다. 상기 모바일 장치의 인증 시스템은 상기 모바일 장치로 전송되는 신원 증명 요청을 생성하는 상기 온라인 서비스 서버를 제공하며, 상기 모바일 장치는 제2 인증 서버에 전송되는 제2 인증 요청을 생성하고, 상기 제2 인증 요청에는 상기 모바일 장치의 사용자에 연관된 데이터가 포함된다. 상기 모바일 장치의 인증 시스템은 상기 제2 인증 서버가 상기 제2 인증 요청을 수신하고 상기 모바일 장치의 사용자에 연관된 데이터에 부분적으로 기초하여 제2 인증을 생성하는 것과, 상기 제2 인증 서버가 상기 제2 인증을 상기 모바일 장치에 전송하는 것을 추가로 용이하게 한다. 상기 모바일 장치는 상기 제2 인증을 상기 온라인 서비스 서버에 전송하고, 상기 온라인 서비스 서버는 상기 모바일 장치가 상기 제1 인증 및 상기 제2 인증에 기초하여 상기 온라인 서비스 서버를 통해 상기 온라인 서비스에 액세스하는 것을 허용한다.

[0054] 다른 일 예에서, 모바일 앱을 통해 온라인 서비스 서버에 액세스하려고 하는 네트워크 접속을 지니는 사용자의 모바일 장치를 인증하는 방법으로서, 상기 온라인 서비스 서버는 제1 인증 서버 및 제2 인증 서버로부터 인증을 요청하는, 모바일 장치를 인증하는 방법이 제공된다. 상기 모바일 장치의 인증 방법은, 모바일 앱을 개방하고 상기 온라인 서비스 서버에 액세스하기 위한 요청을 생성하는 단계 - 상기 요청에는 상기 모바일 장치에 연관된 데이터가 포함됨 -; 및 상기 네트워크 접속을 통해 상기 요청을 온라인 서비스에 연관된 온라인 서비스 서버에 전송하는 단계;를 포함한다. 상기 모바일 장치의 인증 방법은, 상기 모바일 장치에 연관된 데이터를 포함하는 제1 인증 요청을 생성하는 단계; 상기 온라인 서비스 서버로부터 상기 제1 인증 서버로 상기 제1 인증 요청을 전송하는 단계; 상기 모바일 장치에 연관된 데이터에 부분적으로 기초하여 제1 인증을 생성하는 단계; 및 상기 제1 인증을 상기 제1 인증 서버로부터 상기 온라인 서비스 서버로 전송하는 단계;를 더 포함한다. 상기 모바일 장치의 인증 방법은, 신원 증명 요청을 생성하는 단계; 상기 신원 증명 요청을 상기 온라인 서비스 서버로부터

상기 모바일 장치로 전송하는 단계; 상기 모바일 장치의 사용자에 연관된 데이터를 포함하는 제2 인증 요청을 생성하는 단계; 및 상기 제2 인증 요청을 상기 모바일 장치로부터 상기 제2 인증 서버로 전송하는 단계;를 더 포함한다. 마지막으로, 상기 모방리 장치의 인증 방법은, 상기 모바일 장치의 사용자에 연관된 데이터에 부분적으로 기초하여 제2 인증을 생성하는 단계; 상기 제2 인증을 상기 제2 인증 서버로부터 상기 모바일 장치로 전송하는 단계; 상기 제2 인증을 상기 모바일 장치로부터 상기 온라인 서비스 서버로 전송하는 단계; 및 상기 제1 인증 및 상기 제2 인증을 처리하여 상기 온라인 서비스에 대한 액세스가 상기 온라인 서비스 서버를 통해 상기 모바일 장치에 제공되게 하는 단계;를 포함한다.

[0055] 또 다른 일 예에서, 네트워크 접속을 지니는 사용자의 모바일 장치를 등록하는 방법으로서, 사용자가 모바일 장치상의 저장 장치상에 저장된 앱에 연관된 온라인 서비스에 대한 액세스를 요청하는, 모바일 장치를 등록하는 방법이 제공된다. 상기 모바일 장치의 등록 방법은, 상기 모바일 장치상에서 상기 앱을 개시하는 단계; 사용자에게 사용자에 연관된 식별 정보를 입력할 것을 프롬프트하는 단계; 및 상기 식별 정보를 확인하는 단계;를 포함한다. 상기 모바일 장치의 등록 방법은, 상기 모바일 장치로부터 제1 인증 서버로 등록 요청을 전송하는 단계; 상기 앱으로부터 상기 온라인 서비스에 연관된 온라인 서비스 서버로 등록 통지를 전송하는 단계; 및 상기 온라인 서비스 서버로부터 상기 모바일 장치로 등록 신호를 전송하는 단계를 더 포함하며, 상기 등록 신호에는 상기 온라인 서비스에 연관된 데이터가 포함된다. 상기 모바일 장치의 등록 방법은, 상기 앱으로부터 제2 인증 서버로 확인 요청을 전송하는 단계 - 상기 확인 요청에는 모바일 장치 및 사용자에 연관된 데이터가 포함됨 -; 상기 제2 인증 서버로부터 상기 앱으로 확인 데이터를 전송하는 단계 - 상기 확인 데이터는 상기 확인 요청에 포함된 데이터를 확인하고 상기 제2 인증 서버에 연관된 데이터를 포함함 -; 및 상기 확인 데이터를 상기 앱으로부터 상기 온라인 서비스 서버로 그리고 상기 제1 인증 서버로 전송하는 단계;를 또 포함한다. 마지막으로, 상기 모바일 장치의 등록 방법은, 상기 확인 데이터 중 적어도 일부를 상기 제1 인증 서버에 연관된 저장 장치상에 저장하는 단계; 상기 앱에 확인 결과를 전송하는 단계; 및 사용자에게 등록 결과를 통지하는 단계;를 포함한다.

[0056] 본 발명의 다른 목적 및 그의 특정한 특징 및 이점은 이하 도면들을 고려하면 더 명백해질 것이다.

도면의 간단한 설명

[0057] 도 1은 시스템의 일 예에 따른 시스템과 상호작용하는 FIDO 사용자 장치의 블록도이다.

도 2는 도출한 개인 신원 확인 크리덴셜의 획득을 보여주는 블록도이다.

도 3은 인증서 검증 프로세스를 나타내는 블록도이다.

도 4는 인증 시스템을 통한 모바일 장치의 FIDO UAF 등록을 위한 워크 플로우 프로세스를 보여주는 도면이다.

도 5는 인증 시스템을 통한 모바일 장치의 OCSP 검증을 위한 워크 플로우 프로세스를 보여주는 도면이다.

도 6은 인증 시스템을 통한 모바일 장치의 FIDO UAF 인증을 위한 워크 플로우 프로세스를 보여주는 도면이다.

도 7은 FIDO x.509 스텝-업 인증을 보여주는 블록도이다.

도 8은 인증자 특정 모듈 기능을 나타내는 흐름도이다.

도 9는 인증자 모듈 기능을 나타내는 흐름도이다.

도 10은 인증서 검증 프로세스를 나타내는 흐름도이다.

도 11은 등록 프로세스를 나타내는 흐름도이다.

도 12는 인증 프로세스를 나타내는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0058] 지금부터 도면들을 참조하기로 하고, 상기 도면들 전반에 걸쳐 동일한 참조번호들이 대응 구조를 나타낸다.

[0059] 도 1은 온라인 서비스에 액세스하기 위한 브라우저/앱(102)을 포함하는 임의 유형의 모바일 장치를 포함할 수 있는 FIDO 사용자 장치(100)를 포함한다. 상기 앱(102)은 예를 들어 신뢰 당사자 웹 서버(106)에 의해 수신되는 UAF 프로토콜(104)을 지니는 요청을 전송하도록 활성화될 수 있다. 상기 UAF 프로토콜(104)은 TLS 프로토콜을 포함할 수 있고 상기 신뢰 당사자 웹 서버(106)는 TLS 키를 포함할 수 있다.

[0060] 그 후에, 상기 신뢰 당사자 웹 서버(106)는 FIDO 서버(108)로부터 인증을 요청할 수 있으며, 상기 FIDO 서버(108)는 또 FIDO 요구사항의 준수를 인증하는 FIDO 메타 데이터 서비스(110)를 송신할 수 있다.

[0061] 또한, 도 1에는 상기 브라우저/앱(102)이 FIDO 클라이언트(112), 인증자 특정 모듈(114) 및 FIDO 인증 모듈(116)을 포함하는 것으로 도시되어 있다.

[0062] 본 예에서는, 상기 FIDO 인증 모듈(116)이 인증서 검증을 위해 OCSP 서버(118)와 통신하는 것으로 도시되어 있다. 선택적으로, 이는 PIV 크리덴셜의 프로비저닝을 더 포함할 수 있다.

[0063] 통상의 기술자라면 이해하겠지만, FIDO 인증 DPC 인증자는 강력하게 검증된 크리덴셜로부터 FIDO-가능 엔터프라이즈 서버 측 리소스로의 중요한 브리지를 형성한다. 앞서 검토한 바와 같이, 지금까지 PIV 크리덴셜의 상호 운용성을 위해서는 클라이언트 측 소프트웨어 구성요소 및 백엔드 CA의 특정 PKI 통합이 필요하였다. 제안된 FIDO DPC 인증자는 이러한 통합을 간소화하게 한다. DPC 구현은, 예를 들어 NIST SP 800-157 및 NIST SP 800-63-3 AAL3 수준에 의해 요구되는 바와 같지만 이에 국한되지 않는 정부 표준을 충족하는 승인된 모바일 장치에 대한 디지털 인증서를 생성하고 예를 들어 NIST SP 800-57 및 NIST.SP 800-63-3에 의해 요구되는 바와 같지만 이에 국한되지 않는 정부 표준을 충족하는 모바일 장치의 IAL3 신원을 이용하여 AAL3 인증을 가능하게 한다.

[0064] 도 2는 초기 FIDO 인증자 등록 프로세스(200)를 보여준다. 특히, 이러한 프로세스는 도출한 PIV 크리덴셜 프로비저닝의 선택적 단계를 더 포함하는 것을 보여준다.

[0065] 이러한 예에서, 관리자는 사용자에게 초대장(202)을 보낸다. 그리고 나서, 등록 요청(204)은 신뢰 당사자 앱(206)으로 송신되고, 그리고 나서 FIDO UAF 서버/등록 포털(214)로 전송되며 그럼으로써 FIDO x.509 인증자가 사용자 장치로 다운로드(208) 된다.

[0066] 그리고 나서, 사용자 장치는 신뢰 당사자 앱(206)에 등록 요청(210)을 송신하고, 이는 신뢰 당사자 앱(206)으로부터 FIDO UAF 서버/등록 포털(214)로 등록 요청(212)을 트리거한다. 그리고 나서, FIDO UAF 서버/등록 포털(214)은 신뢰 당사자 앱(206)과 통신하고 그래서 PIN 초기화(216) 및 키 쌍 생성(218)을 위해 사용자 장치와 접촉한다.

[0067] 이 시점에서, 인증 증명 식별(Authentication Attestation Identification; AAID), 공개키, 인증 암호화 및 사용자 이름을 포함하는 키 등록 데이터(Key Registration Data; KRD) 객체는 신뢰 당사자 앱(206)으로 전송된다. 그리고 나서, 신뢰 당사자 앱(206)은 FIDO UAF 서버/등록 포털(214)과 통신하여 공개키(220)를 검증 및 저장한다.

[0068] 도 3은 인증 시스템(300)의 일 예를 보여준다. 이러한 예에서, 액세스 요청(302)은 앱(301)에 의해 생성되고 모바일 장치로부터 FIDO 가능 신뢰 당사자 애플리케이션(304)으로 전송된다.

[0069] 이는 또 인증 요청(306)의 생성을 FIDO UAF 서버(308)에 트리거한다. 인증 요청은 신뢰 당사자 애플리케이션(304)을 통해 사용자 장치(310)로 전송된다. 앱(301)은 인증서 검증 요청(312)을 온-라인 인증서 상태 프로토콜(On-line Certificate Status Protocol; OCSP) 서버(314)로 송신한다. 그리고 나서, 검증 또는 서명된 어서션(signed assertion)(316)은 FIDO 가능 신뢰 당사자 애플리케이션(304)으로 전송된다. 그리고 나서, FIDO 가능 신뢰 당사자 애플리케이션(304)은 결과(318)를 FIDO UAF 서버로 확인하고, 일단 확인되면, 앱(301)이 FIDO 가능 신뢰 당사자 애플리케이션(304)에 액세스하는 것(320)을 허용한다.

[0070] 여기서 유념해야 할 점은 다양한 기능 및 방법이 지금까지 일련의 단계들로 설명되고 제시되었지만, 그러한 일련의 단계들이 단지 하나의 바람직한 실시 예의 예시로 제공되었을 뿐이며, 이러한 기능들을 예시된 특정 순서로 수행할 필요는 없다는 점이다. 여기서 추가로 고려할 점은 이러한 단계들 중 어느 한 단계가 다른 단계들 중 어느 한 단계에 대해 이동 및/또는 결합 될 수 있다는 점이다. 또한, 여기서 더 고려할 점은 애플리케이션에 따라 본원 명세서에 기재된 기능들 중의 전부 또는 일부를 이용하는 것이 바람직할 수 있다는 점이다.

[0071] 도 4를 지금부터 참조하면, FIDO UAF 등록(400) 프로세스의 일 예가 도시되어 있다. 사용자(402)가 신뢰 당사자 모바일 앱(406)을 개방(404)하는 경우를 포함하는 다양한 등록 단계가 도시되어 있다. 모바일 앱(406)은 사용자(402)에게 PIN(408) 및 사용자 이름 및 PIN이 제출될 것(410)을 요청한다. 그리고 나서, 모바일 앱(406)은 로그인(412)을 확인하고 UAF 등록 요청(414)을 FIDO 서버(416)에 트리거하고, FIDO 서버(416)는 신뢰 당사자 모바일 앱(406)으로 UAF 등록 요청(418)을 리턴(return)한다.

[0072] 모바일 앱(406)은 애플리케이션 식별(신원) 및 전송 계층 보안(Transit Layer Security; TLS) 바인딩들(420)과 함께 UAF 등록 요청을 FIDO 클라이언트(422)에 송신하고, FIDO 클라이언트(422)는 애플리케이션 식별(424)에 의

해 식별된 패싯(facet) 식별 리스트를 신뢰 당사자 모바일 앱(406)에 송신한다. 신뢰 당사자 모바일 앱(406)은 패싯 식별 리스트(426)를 FIDO 클라이언트(422)로 리턴하고, FIDO 클라이언트(422)는 폴리시(policy)(428)에 기초하여 인증자를 선택한다. 이는 다시 FIDO 클라이언트(422)로부터 인증자 특정 모듈(432)로 등록(430)을 트리거한다. 인증자 특정 모듈(432)은 인증자(436)로 KH 액세스 토큰(434)을 포함하는 등록을 트리거한다. 인증자(436)는 사용자(402)로 사용자 확인(438)을 트리거하고, 그럼으로써 사용자(402)는 PIN을 입력하고 인증서 확인 및 검증(440)을 PKI 프로세스(442)에 송신한다.

[0073] PKI 프로세스(442)는 사용자를 확인(444)하고, 이는 애플리케이션 식별 및 인증 식별(446)을 위한 키 쌍의 생성을 위해 인증자(436)로 다시 전송된다.

[0074] 인증자(436)는 증명 및 공개 키(448)를 포함하는 KRD 객체를 인증자 특정 모듈(432)로 리턴하고, 인증자 특정 모듈(432)은 KRD(450)를 FIDO 클라이언트(422)로 리턴한다. FIDO 클라이언트(422)는 KRD(452)를 포함하는 UAF 등록 응답을 신뢰 당사자 모바일 앱(406)으로 리턴하고, 신뢰 당사자 모바일 앱(406)은 KRD(454)를 포함하는 UAF 등록 응답을 FIDO 서버(416)에 송신한다. FIDO 서버(416)는 검증 결과(456)를 신뢰 당사자 모바일 앱(406)으로 리턴하고, 신뢰 당사자 모바일 앱(406)은 다시 성공적인 등록(458)을 사용자(402)에게 알려준다.

[0075] 도 5를 지금부터 참조하여, OCSP 검증 프로세스(500)의 일 예가 제시된다. 사용자(502)가 신뢰 당사자 모바일 앱(506)을 개방(504)하는 경우를 포함하는 다양한 검증 단계가 도시되어 있다. 상기 모바일 앱(506)은 사용자(502)에게 PIN(508)을 입력할 것을 요청한다. 사용자(502)는 자신의 사용자 이름 및 PIN(510)을 입력하며, 이는 인증자(512)에 의해 수신된다. 그리고 나서, 인증자(512)는 로그인(514)을 확인하고 키 스토어(518)로 일자(date)의 유효성을 검사(516)한다. 키 스토어(518)가 유효성을 확인(520)하면, 제어는 인증자(512)로 리턴된다.

[0076] 그리고 나서, 인증자(512)는 인증서로부터 발급자, 일련번호 및 주제를 분석(522)하고 이로부터 키 스토어가 OCSP 쿼리를 구축(524)하게 한다. 그리고 나서, 인증자(512)는 OCSP 쿼리(526)를 OCSP 서버(528)에 제출하게 된다. 그리고 나서, OCSP 서버(528)는 인증 기관(532)으로부터 모든 인증서를 요청한다. 그리고 나서, 인증 기관(532)은 OCSP 서버(528)에 의한 평가(534)를 위해 상기 인증서를 송신한다. 마지막으로, 상기 인증서가 유효하다고 OCSP 서버(528)가 결정하면, FIDO UAF 프로세스(536)의 개시를 위해 제어는 인증자에게 리턴된다.

[0077] 도 6을 지금부터 참조하여, FIDO UAF 인증 프로세스(600)의 일 예가 설명된다. 사용자(602)가 신뢰 당사자 모바일 앱(606)을 개방(604)하는 경우를 포함하는 다양한 인증 단계가 도시되어 있다. 상기 모바일 앱(606)은 UAF 인증 요청(608)을 트리거하며, 이는 FIDO 서버(610)로 전송된다. 일반 인증 요청(612)이 생성되고 UAF 인증 요청은 신뢰 당사자 모바일 앱(606)으로 리턴(614)된다. 그리고 나서, 신뢰 당사자 모바일 앱(606)은 애플리케이션 식별 및 TLS 바인딩들(616)과 함께 UAF 인증 요청을 FIDO 클라이언트(618)에 송신한다.

[0078] FIDO 클라이언트(618)는 애플리케이션 식별(620)에 의해 식별된 패싯 식별 리스트를 검색하려고 시도하고, 이러한 요청은 신뢰 당사자 모바일 앱(606)에 송신된다. 그리고 나서, 신뢰 당사자 모바일 앱(606)은 패싯 식별 리스트(622)를 FIDO 클라이언트(618)로 리턴한다. 그리고 나서, FIDO 클라이언트(618)는 폴리시(624)에 기초하여 인증자를 선택하고, 이는 인증자 특정 모듈(628)에 대한 인증(626)을 트리거한다.

[0079] 그리고 나서, 인증자 특정 모듈(628)은 인증자(632)와 함께 키 핸들(KH) 액세스 토큰(630)을 포함하는 인증을 트리거한다. 이는 사용자 확인(634)을 트리거하고, 그럼으로써 사용자(602)가 자신을 식별할 때 인증서 확인 및 검증 요청(636)이 PKI 프로세스(638)에 송신되게 한다. 그리고 나서, PKI 프로세스(638)는 사용자 인증(640)을 인증자(632)에 다시 송신하게 된다.

[0080] 그리고 나서, 인증자(632)는 사용자 인증을 잠금 해제하고 인증 결과(642)를 계산하며 서명된 데이터(644)를 인증자 특정 모듈(628)에 송신하고, 인증자 특정 모듈(628)은 또 서명된 데이터(646)를 FIDO 클라이언트(618)에 송신한다. FIDO 클라이언트(618)는 서명된 데이터(648)를 포함하는 UAF 인증 응답을 신뢰 당사자 모바일 앱(606)에 송신한다.

[0081] 신뢰 당사자 모바일 앱(606)은 UAF 인증 응답(650)을 FIDO 서버(610)에 송신하고, FIDO 서버(610)는 UAF 인증 응답을 확인(652)한다. 그리고 나서, 확인 결과는 신뢰 당사자 모바일 앱(606)에 송신(654)되고, 신뢰 당사자 모바일 앱(606)은 다시 로그인 정보(656)를 사용자(602)에게 제공한다.

[0082] 도 7은 FIDO x.509 스텝-업 인증을 위한 시스템의 블록도를 제공한다. 상기 블록도는 도 3와 관련하여 설명되고 도 3에 도시된 것과 유사하지만, 이러한 시스템(700)이 모든 애플리케이션에 대해 높은 수준의 보안이 필요할 수 있음을 고려한 것이다. 이러한 예에서, 액세스 요청(702)은 앱(701)에 의해 생성되고 모바일 장치로부터

FIDO 가능 신뢰 당사자 애플리케이션(704)으로 전송된다.

[0083] 이는 다시 인증 요청(706)의 생성을 FIDO UAF 서버(708)로 트리거한다. 인증 요청은 신뢰 당사자 애플리케이션(704)을 통해 사용자 장치(710)로 전송된다.이러한 예에서, 사용자는 얼굴 인식과 같은 생체 인식(712)을 입력해야 한다. 그리고 나서, 서명된 어서션(714) 및 액세스(716)는 신뢰 당사자 애플리케이션(704)에 송신된다. 또한, 기밀(sensitive) 액세스 요청(718)은 기밀 신뢰 당사자 애플리케이션(720)에 송신된다.

[0084] 이는 기밀 기관 요청(722)의 생성을 FIDO UAF 서버(708)로 트리거한다. 또한, x.509 인증 요청(724)은 앱(708)에 전송되며, 앱(708)은 OCSP 서버(728)로부터 인증서 검증(726)을 요청한다. 일단 인증서 검증이 OSCP 서버(728)로부터 리턴되면, 서명된 어서션(730)은 기밀 신뢰 당사자 애플리케이션(720)에 전송된다.

[0085] 그리고 나서, 기밀 신뢰 당사자 애플리케이션(720)은 리턴된 결과(732)를 FIDO UAF 서버(708)로 확인하고 그 후에는 프로세스가 결과를 검증하면 기밀 신뢰 당사자 애플리케이션(720)에 대한 액세스(734)를 허용한다.

[0086] 도 8은 인증자 특정 모듈 기능을 보여주는 흐름도이다. 프로세스(800)는 인증자(804)를 찾아내기 위해 FIDO 클라이언트(802)로부터의 요청에 대한 프로세스를 예시한 것이다.

[0087] 그리고 나서, 프로세스는 인증 요청(806)으로 이동하고, 시스템은 사용자가 인증자에 등록(808)되어 있는지를 결정하게 된다. 사용자가 인증자에 등록(808)되어 있지 않다면, 프로세스는 사용자 등록 프로세스(810)로 이동하고, 사용자가 인증자에 등록(808)되어 있다면, 프로세스는 인증 프로세스(812)로 이동한다.

[0088] 인증 프로세스(812) 후에, 프로세스는 사용자로 이동하여 식별 정보(814)를 입력하게 한다. 여기서 유념해야 하는 점은 이러한 것이 사용자를 식별하기 위해 제공되는 임의의 유형의 식별일 수 있다는 점이다. 일단 정보가 입력되면, 프로세스는 확인(816)으로 이동한다. 신원 정보가 유효하지 않다면, 프로세스는 사용자로 루프백하여 식별 정보(814)를 입력하게 하는데, 이는 프로세스가 종료되기 전에 제한된 횟수의 시도만을 허용하게 된다. 신원 정보가 유효하면, 프로세스는 x.509 검증 프로세스(818)로 이동한다.

[0089] 여기에서부터는 x.509 검증에 합격했는지 실패했는지를 프로세스가 결정(820)한다. 검증에 합격했다면, 프로세스는 긍정 응답(822)을 생성하도록 이동하지만, 검증에 실패했다면, 프로세스는 실패 응답(824)을 생성하도록 이동한다. 그리고 나서, 긍정 또는 실패 응답으로부터, 프로세스는 상기 응답을 FIDO 클라이언트(826)로 리턴하도록 이동한다. 마지막으로, 프로세스는 FIDO 클라이언트 확인응답(828)으로 진행한다.

[0090] 도 9는 인증자 모듈 기능을 보여주는 흐름도이다. 프로세스(900)는 인증자 특정 모듈(902)로부터 수신된 요청을 예시한 것이다. 등록 요청(904)이 수신되면, 프로세스는 키 스토어 검증(906)으로부터 인증서를 추출하도록 진행한다. 그리고 나서, 프로세스는 인증서 검증 프로세스(908)로 이동한다.

[0091] 인증 요청(910)이 수신되면, 프로세스는 로컬 검증(912)을 위해 ASM으로부터 사용자 이름에 기초한 인증서를 검색하도록 진행한다. 그리고 나서, 프로세스는 인증서 검증 프로세스(908)로 이동한다.

[0092] 인증서 검증 프로세스(908)로부터 결과가 결정(914)된다. 결과가 검증되지 않으면 프로세스는 종료(916)된다. 프로세스가 검증되면, 프로세스는 대응하는 응답(918)을 생성한 다음에 ASM(920)으로 되돌아간다.

[0093] 도 10은 인증서 검증 프로세스를 보여주는 흐름도이다. 프로세스(1000)는 인증서(1002)의 발견에서부터 시작하고, 예를 들어 6-8 1004일 수 있는 PIN을 입력하는 사용자로 이동한다. 여기서 유념해야 할 점은 PIN이 일 예로 사용되는 동안, 임의의 유형의 보안이 효과적으로 사용될 수 있다는 점이다.

[0094] 그리고 나서, 프로세스는 입력된 정보가 정확한지를 결정(1006)하게 된다. 만약 입력된 정보가 정확하지 않다면, 사용자에게는 예를 들어, 6번의 시도(1008)로 제한된 것과 같은, 정확한 정보를 입력하도록 하는 제한된 시도 횟수가 제공되게 된다. 제한된 시도 횟수 내에 정확한 정보가 입력되지 않으면, 프로세스는 종료(1010)하게 된다. 정확한 정보가 입력되면, 프로세스는 키 스토어(1012)의 잠금 해제(1012)로 이동하게 된다.

[0095] 키 스토어가 잠금해제된 후에, 프로세스는 인증서 무결성의 검사(1014)로 진행한다. 인증서 무결성의 검사시, 프로세스는 예를 들어 공개키로 서명을 검사하게 되고 발행자 서명을 확인(1016)하게 된다.

[0096] 인증서 무결성이 유효하지 않은 것으로 결정되면, 프로세스는 종료(1018)하게 된다. 인증서 무결성이 유효하다고 결정되면, 프로세스는 인증서 유효 시간의 검사(1020)로 이동하게 된다. 인증서 유효 시간의 검사시, 프로세스는 예를 들어 유효 일자를 검사(1022)하게 된다.

[0097] 인증서 무결성이 유효하지 않다고 결정되면, 프로세스는 종료(1024)하게 된다. 인증서 무결성이 유효하다고 결

정되면, 프로세스는 인증서 서명 알고리즘의 검사(1026)로 이동하게 된다. 상기 서명 알고리즘의 검사시, 프로세스는 비대칭 암호화 알고리즘 또는 ECDSA(Elliptic Curve Digital Signature Algorithm)(1030)인 RSA(Rivest-Shamir-Adleman)(1028)의 검사일 수 있을 것이다.

[0098] 일단 인증서 서명 알고리즘의 검사가 완료되면 프로세스는 인증서 유효성 검사 프로세스(1032)를 수행한다. 인증서 유효성 검사 프로세스에는 서버 기반 인증서 유효성 검사(Server Based Certificate Validation; SCVP)(1034) 또는 온라인 인증서 상태 프로토콜(On-line Certificate Status Protocol; OCSP)(1036)이 포함될 수 있을 것이다.

[0099] 그리고 나서, 프로세스는 인증서가 유효한지를 결정(1038)한다. 인증서가 유효하지 않다고 결정되면, 프로세스는 종료(1040)하게 된다. 인증서가 유효하다고 결정되면, 프로세스는 본 예에서 FIDO UAF 프로세스(1042)로 이동한다.

[0100] 도 11은 등록 프로세스를 보여주는 흐름도이다. 프로세스(1100)는 신뢰 당사자가 사용해야 할 인증자의 식별(1102)에서부터 시작한다. 여기에서부터, 프로세스는 인증자의 선택(1104)으로 그리고 인증자가 발견되었는지의 판정(1106)으로 이동한다.

[0101] 인증자가 발견되지 않으면, 프로세스는 종료(1108)한다. 인증자가 발견되면, 프로세스는 애플리케이션 신원의 검사 및 API 키의 생성(1110)으로 이동한다. 일단 이것이 완료되면, 프로세스는 사용자 확인 프로세스(1112)로 이동한 다음에 사용자 확인 프로세스(1112)가 성공적인지의 여부를 프로세스가 결정(1114)한다. 상기 확인 프로세스가 성공적이지 않으면, 프로세스는 종료(1108)한다. 상기 확인 프로세스가 성공적이면, 프로세스는 주제 대체 이름을 사용자 이름에 바인딩하기(1116)로 이동한다.

[0102] 그리고 나서, 프로세스는 키의 생성(1118)으로 이동하고, 상기 키에는 일 예에서 사용자 이름, API 키, 개인 식별 및 발신자 식별이 포함될 수 있다. 그리고 나서, 프로세스는 증명 인증서를 생성(1120)하고, 상기 증명 인증서는 신뢰 당사자(1124)에 송신(1122)된다.

[0103] 도 12는 인증 프로세스를 보여주는 흐름도이다. 프로세스(1200)는 신뢰 당사자(1202)에서부터 시작하고 폴리시에 기초한 인증자 선택(1202)으로 진행하며, 상기 폴리시에는 애플리케이션 식별, tbData 획득, 및 룩업(look up) 키 핸들 및 액세스 키가 포함될 수 있다.

[0104] 그리고 나서, 프로세스는 인증서 검증 프로세스(1204)로 이동하고 여기서 검증이 성공하였는지를 시스템이 결정(1206)한다. 검증이 성공적이지 못하면, 프로세스는 종료(1207)한다. 검증이 성공적이면, 프로세스는 인증자 통지의 생성(1208)으로 이동한다.

[0105] 그리고 나서, 프로세스는 최종 챌린지 파라미터(final challenge parameter; fcp), 결과 n(예 또는 아니오), 카운터(cntr), 서명(s)을 신뢰 당사자(1212)로 송신(1210)한다.

[0106] 본 시스템을 공지된 선행기술과 비교해 볼 때, MAIDC의 많은 이점 중 일부는 다음을 포함한다:

[0107] 1) DPC 가치 및 사용의 증가. 상기 시스템은 FIDO DPC 인증자를 통해 엔터프라이즈 리소스에 모바일 장치를 접속할 수 있는 기능을 제공한다. 상기 시스템은 또한 DPC 사용을 상업적 활동에 이르기까지 확장하고, 이는 개인 정보 및 인증서 정보를 보존하도록 기능 한다.

[0108] 2) 보안 및 개인 정보의 강화. 상기 시스템은 취약한 사용자 이름/패스워드 인증 메커니즘의 사용을 줄이거나 없앤다. 또한, 이는 인증 이벤트로부터 개인 정보를 결합해제하여 인증서의 강도를 잃지 않고 익명 인증을 제공한다. 상기 시스템은 패스워드 재설정 요청을 통한 사회 공학 공격의 가능성을 더 줄인다.

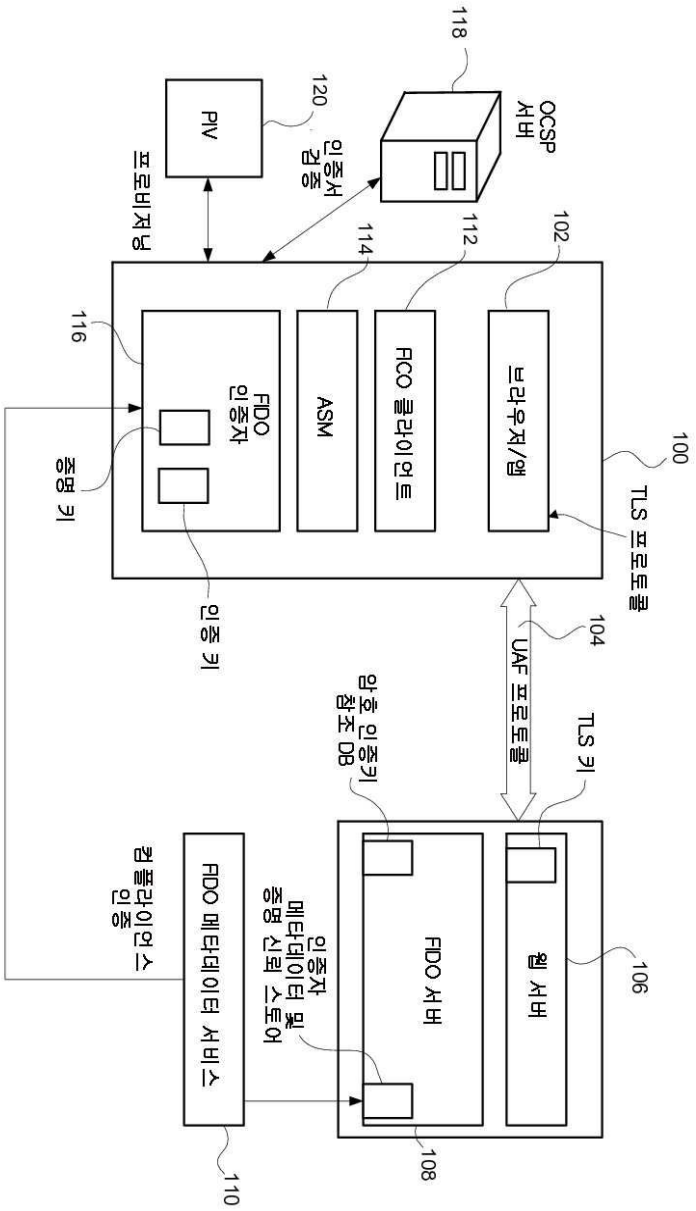
[0109] 3) 운영 비용의 절감. 본 시스템은 PIV 인증 프로세스상에서 이루어지는 현재의 투자를 모바일 장치로 확장하도록 기능 한다. 이는 패스워드의 사용을 줄임으로써 헬프 데스크에 대한 패스워드 재설정 호출 횟수를 줄일 수 있다는 점에서 보안 운영 비용을 절감시킨다.

[0110] 또한 제안된 FIDO DPC 인증자는 모바일 인증을 신속하게 개발하여 정부 및 민간 부문 시스템에 모바일 인증을 통합하는 것을 용이하게 해 준다. FIDO의 제한들 중 하나는 PIV 크리덴셜을 안전하게 관리하고 인증 전에 신뢰할 수 있는 당사자에게 사용자의 신원을 다시 확인하는 계층적 시스템을 PKI와 직접 통합할 수 없다는 것이다. 이로 인해 FIDO에 의해 제공되는 AA3 레벨 인증으로 정부 표준 식별 크리덴셜들을 직접 사용하는 것이 가능하지 않다. 그러나 MAIDC는 모바일 장치상의 인증서 크리덴셜을 FIDO 가능 백엔드 서비스에 결합하는 유일한 시스템이므로 상기 문제를 해결한다.

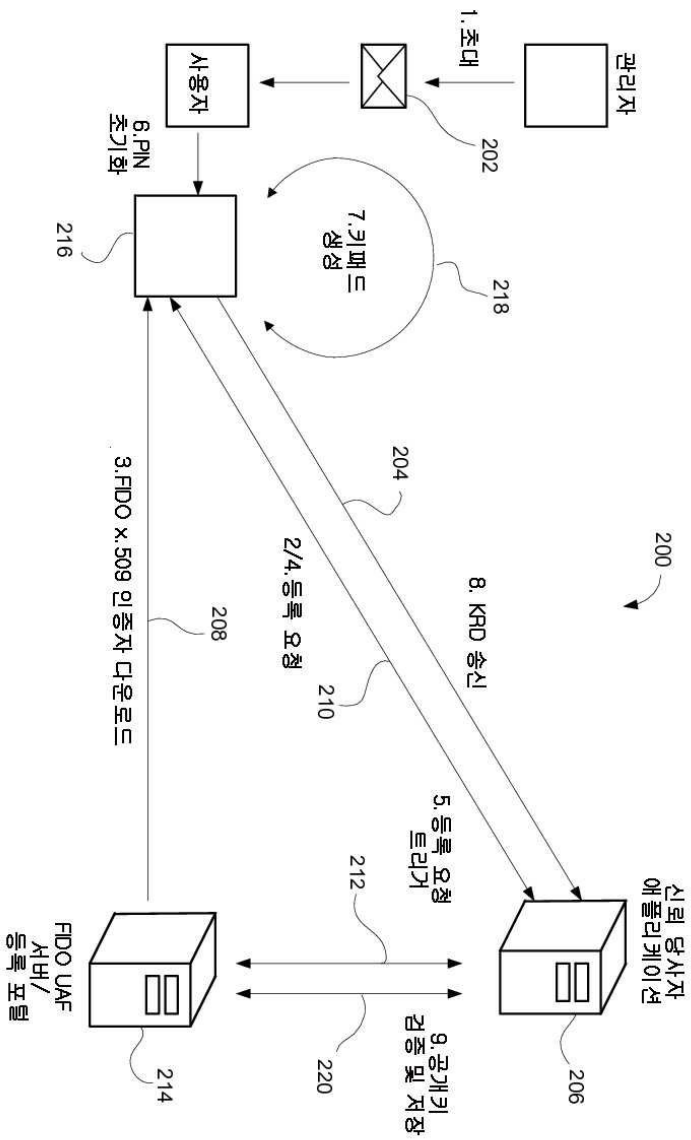
[0111] 본 발명이 부품, 특징 등의 특정한 구성을 참조하여 설명되었지만, 이들은 모든 가능한 구성 또는 특징을 철저하게 다루려는 것이 아니며, 실제로 많은 다른 수정 및 변형이 당업자에게는 명백할 것이다.

도면

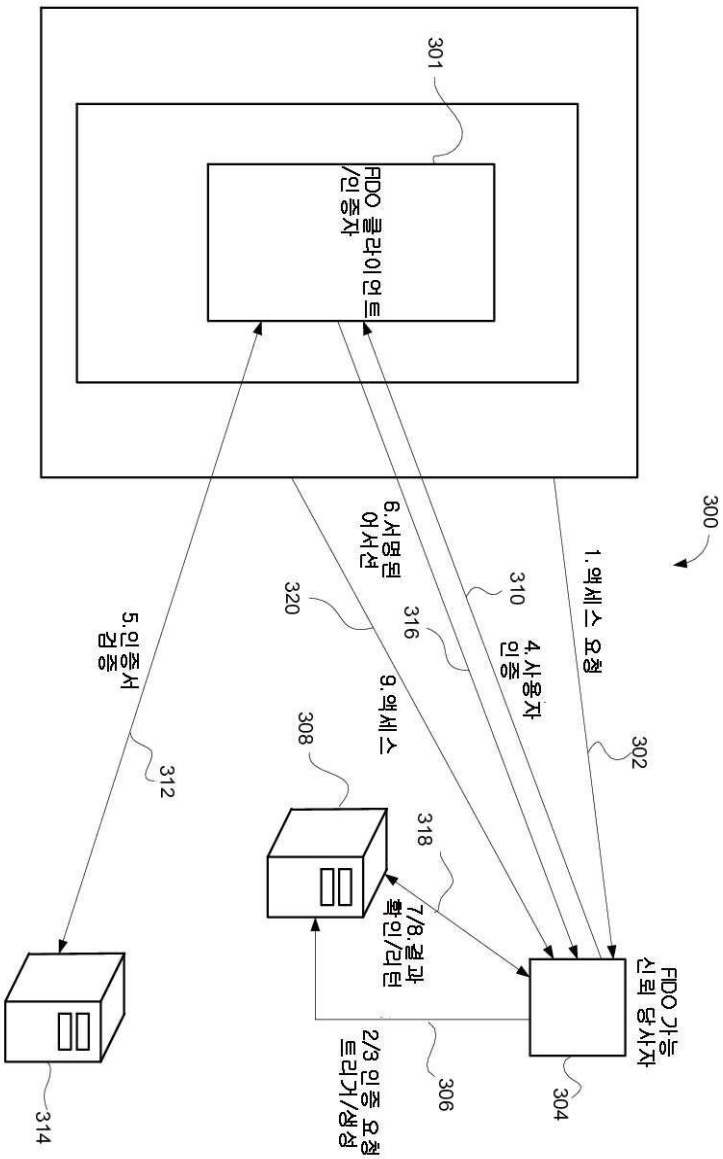
도면1



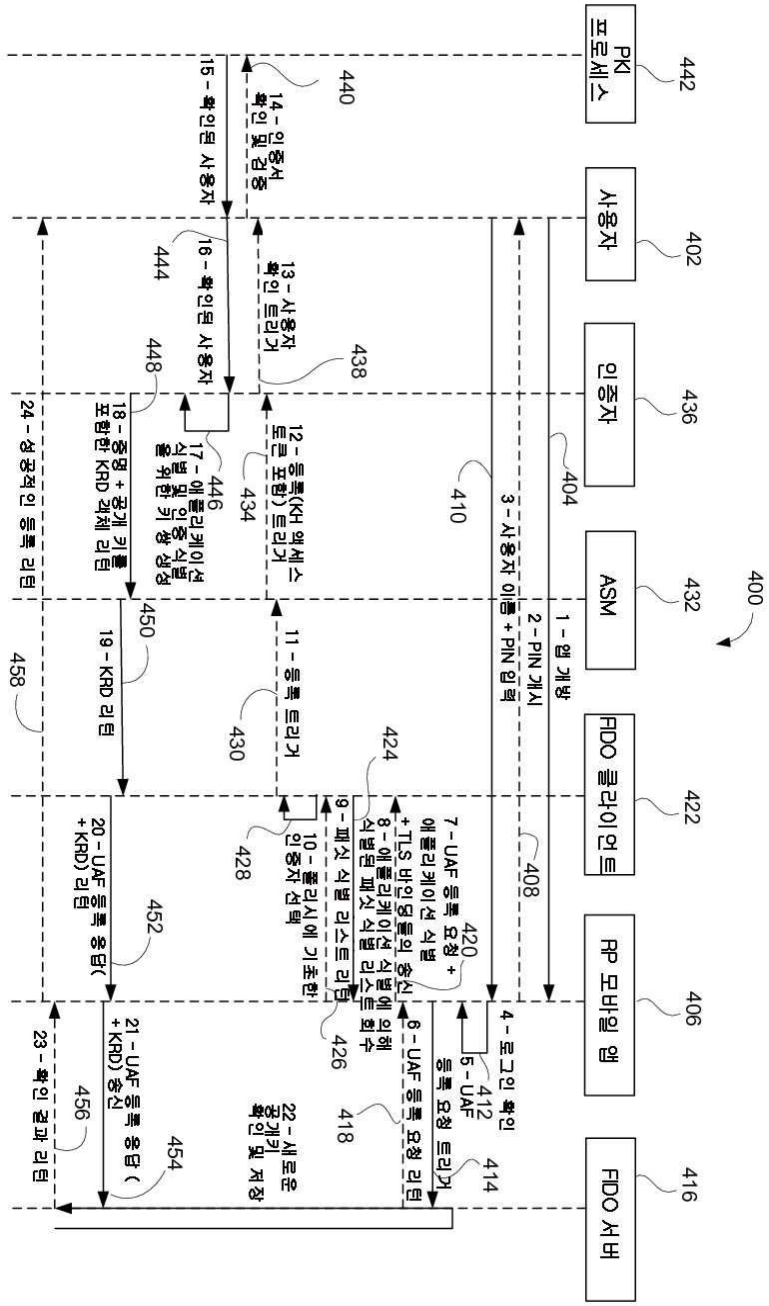
도면2


관리자
1.초대
202
사용자
6.PIN 초기화
216
7.키페드 생성
218
204
8. KRD 송신
200
2/4.등록 요청
210
3.FIDO x.509 인증자 다운로드
208
5.등록 요청 트리거
212
9.공개키 검증 및 저장
220
신뢰 당사자 애플리케이션
206
FIDO UAF 서버/ 등록 포털
214

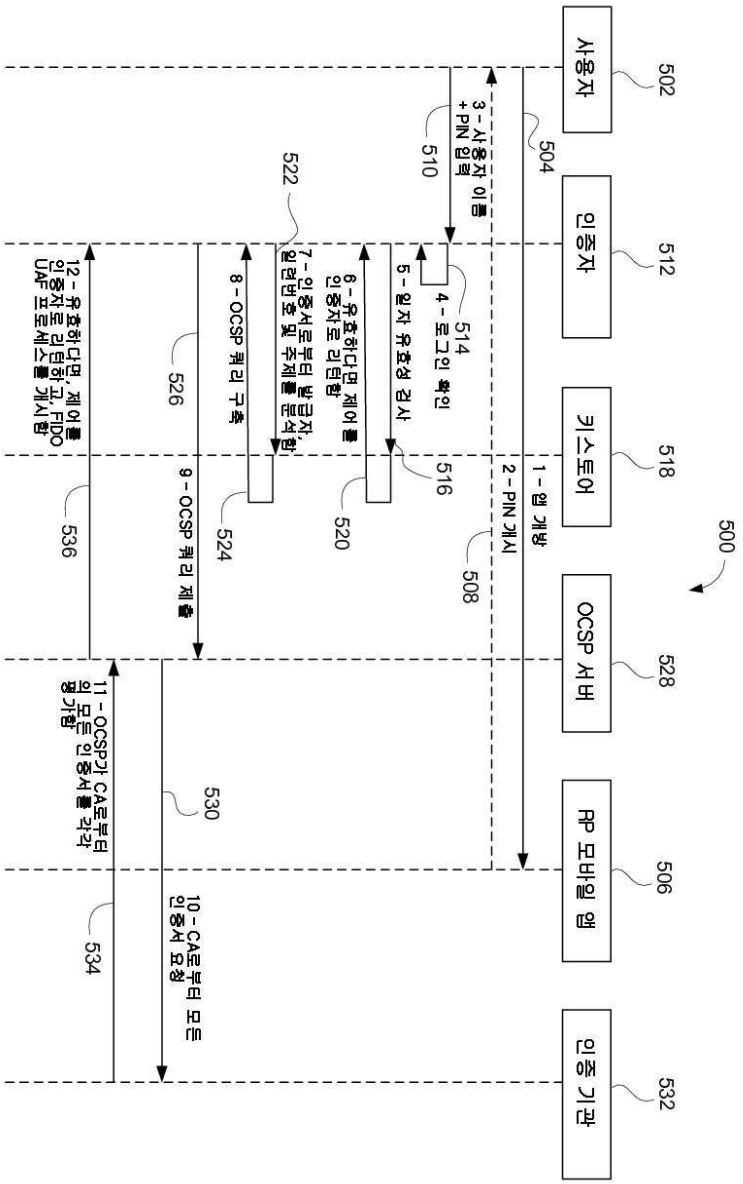
도면3


301
FIDO 클라이언트
/인증자
300
1.액세스 요청
302
FIDO 가능
신뢰 당사자
304
2/3 인증 요청
트리거/생성
306
7/8.결과
확인/리턴
308
318
9.액세스
320
316
4.사용자
인증
310
6.서명된
어서션
5.인증서
검증
312
314

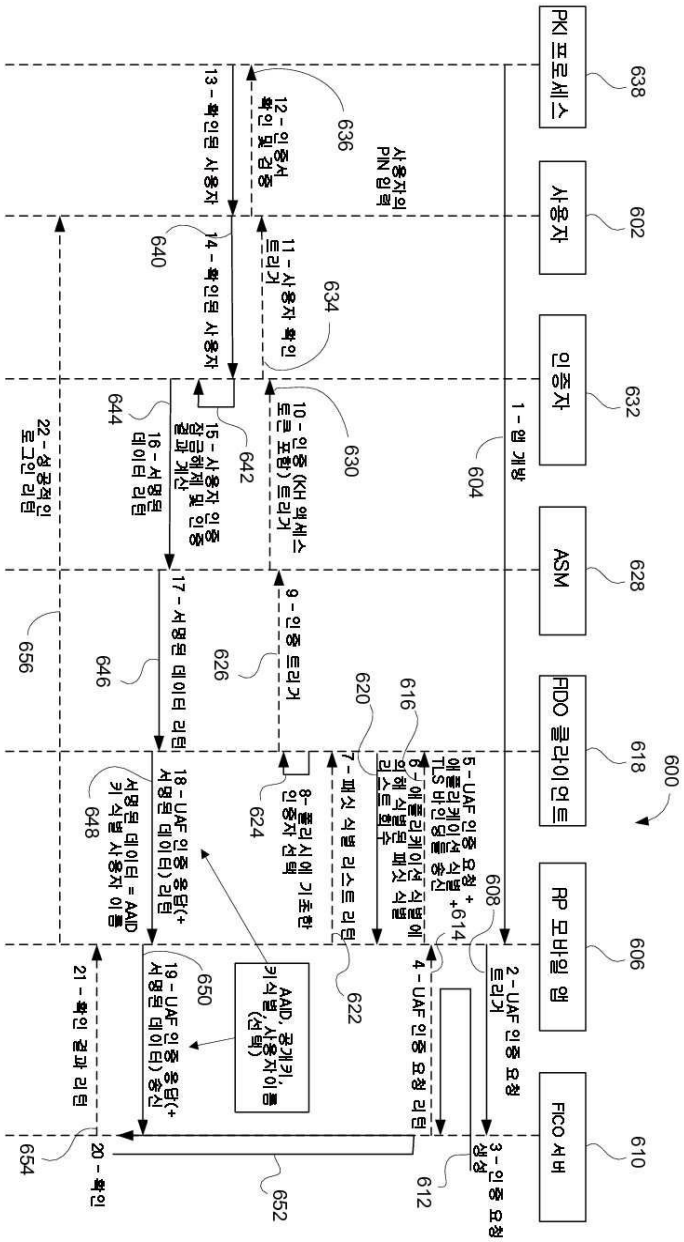
도면4


400
PKI 프로세스
442
사용자
402
인증자
436
ASM
432
FIDO 클라이언트
422
RP 모바일 앱
406
FIDO 서버
416
1 - 앱 개방
2 - PIN 게시
3 - 사용자 이름 + PIN 입력
4 - 로그인 확인
5 - UAF 등록 요청 트리거
412
6 - UAF_등록_요청 리턴
414
7 - UAF 등록 요청 + 애플리케이션 식별
420
8 - 애플리케이션 식별된 피싱 식별 리스트를 + TLS 바인딩들의 송신
9 - 피싱 식별 리스트 리턴
426
10 - 폴리시에 기초한 인증자 선택
428
11 - 등록 트리거
430
12 - 등록(KH 액세스 토큰 포함) 트리거
434
13 - 사용자 확인 트리거
438
14 - 인증서 확인 및 검증
440
15 - 확인된 사용자
16 - 확인된 사용자
444
17 - 애플리케이션 식별 및 인증 키쌍 생성
446
18 - 증명 + 공개 키를 포함한 KRD 객체 리턴
448
19 - KRD 리턴
450
20 - UAF 등록 응답(+ KRD) 리턴
452
21 - UAF 등록 응답 (+ KRD) 송신
454
22 - 새로운 공개키 및 저장
418
23 - 확인 결과 리턴
456
24 - 성공적인 등록 리턴
458
410
404
408
424

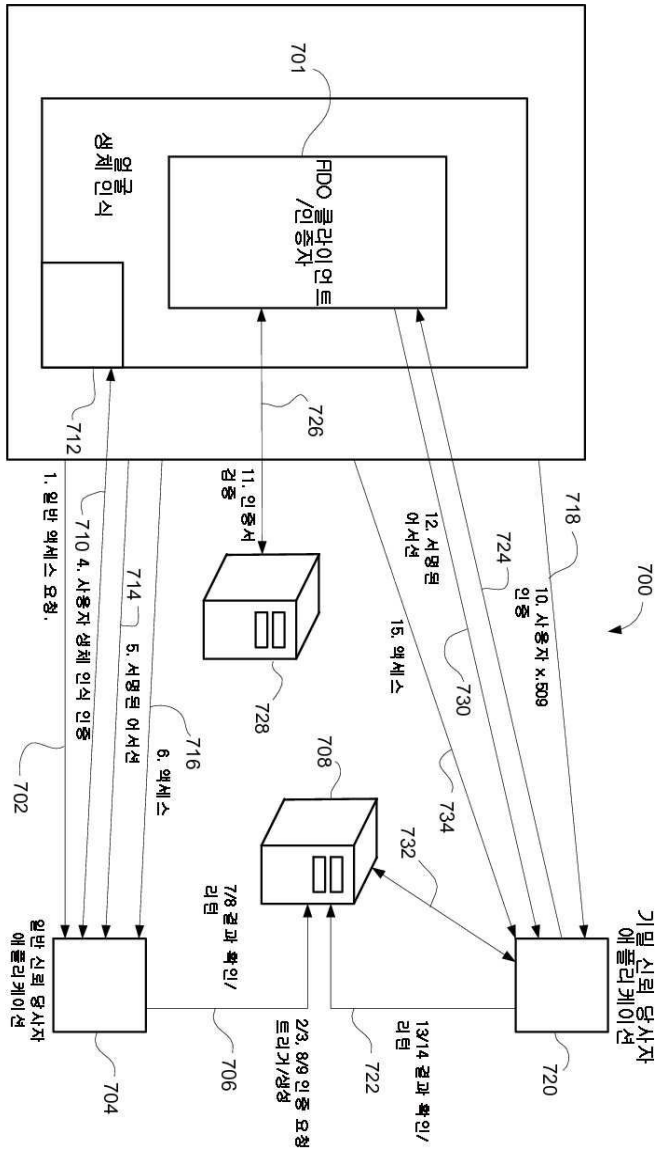
도면5


사용자
인증자
키스토어
OCSP 서버
RP 모바일 앱
인증 기관
500
502
504
506
508
510
512
514
516
518
520
522
524
526
528
530
532
534
536
1 - 앱 개방
2 - PIN 게시
3 - 사용자 이름 + PIN 입력
4 - 로그인 확인
5 - 일자 유효성 검사
6 - 유효하다면, 제어를 인증자로 리턴함
7 - 인증서로부터 발급자, 일련번호 및 주제를 분석함;
8 - OCSP 쿼리 구축
9 - OCSP 쿼리 제출
10 - CA로부터 모든 인증서 요청
11 - OCSP가 CA로부터 의 모든 인증서를 각각 평가함
12 - 유효하다면, 제어를 인증자로 리턴함, FIDO UAF 프로세스를 개시함

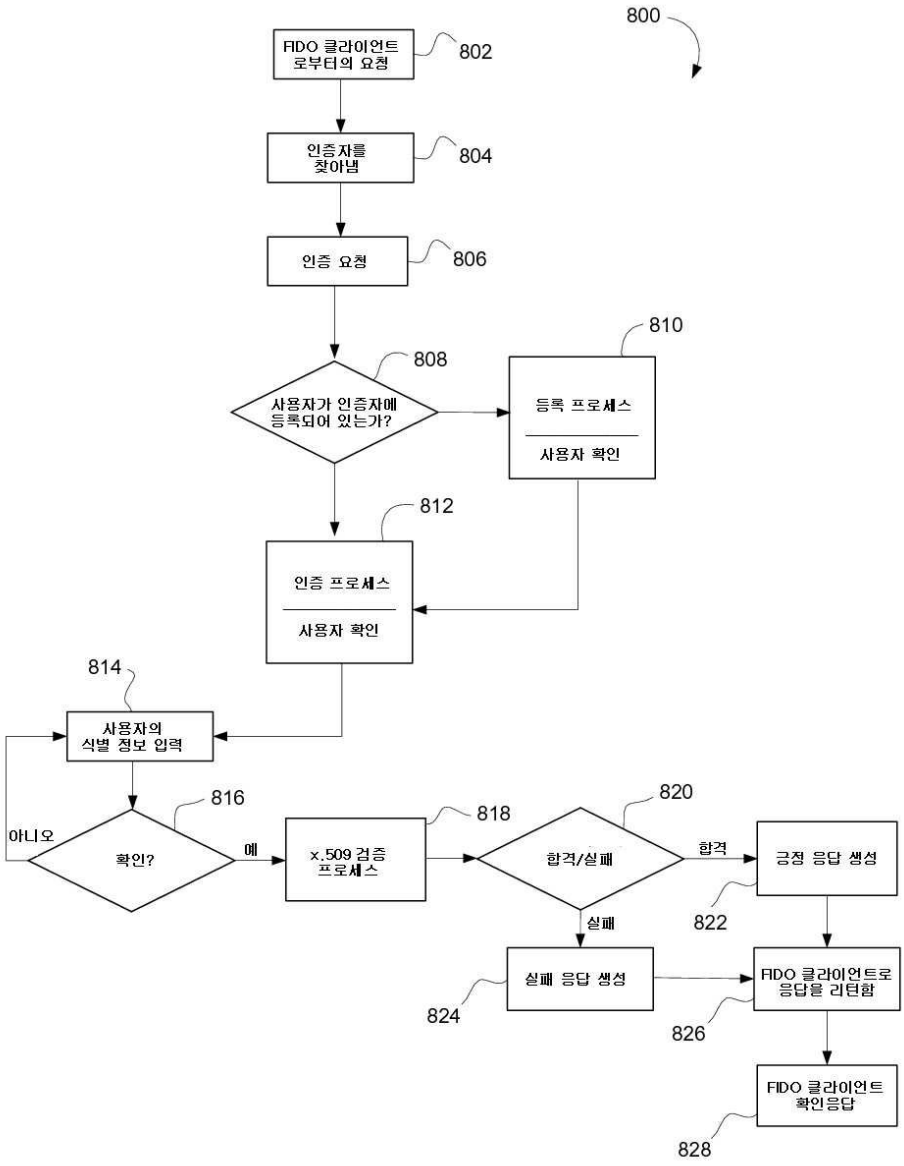
도면6


PKI 프로세스
638
사용자
602
인증자
632
ASM
628
FIDO 클라이언트
618
600
RP 모바일 앱
606
FICO 서버
610
1 - 앱 개방
604
2 - UAF 인증 요청 트리거
3 - 인증 요청 생성
612
4 - UAF 인증 요청 리턴
5 - UAF 인증 요청 + 에플리케이션 식별 + TLS 바인딩을 송신
608
614
6 - 에플리케이션 식별에 의해 식별된 페싯 식별 리스트 획득
616
620
7 - 페싯 식별 리스트 리턴
622
8 - 플리시에 기초한 인증자 선택
624
9 - 인증 트리거
626
10 - 인증 (KH 액세스 토큰 포함) 트리거
630
11 - 사용자 확인 트리거
634
12 - 인증서 확인 및 검증
636
13 - 확인된 사용자
640
14 - 확인된 사용자
사용자의 PIN 입력
15 - 사용자 인증 챌린지 계산 및 인증 결과 리턴
642
16 - 서명될 데이터 리턴
644
17 - 서명될 데이터 리턴
646
18 - UAF 인증 응답(+ 서명될 데이터) 리턴
서명될 데이터 = AAID + 키 식별 + 사용자 이름
648
AAID, 공개키, 사용자 이름 (선택)
650
19 - UAF 인증 응답(+ 서명될 데이터) 송신
652
20 - 확인
654
21 - 확인 결과 리턴
22 - 성공적인 로그인 리턴
656

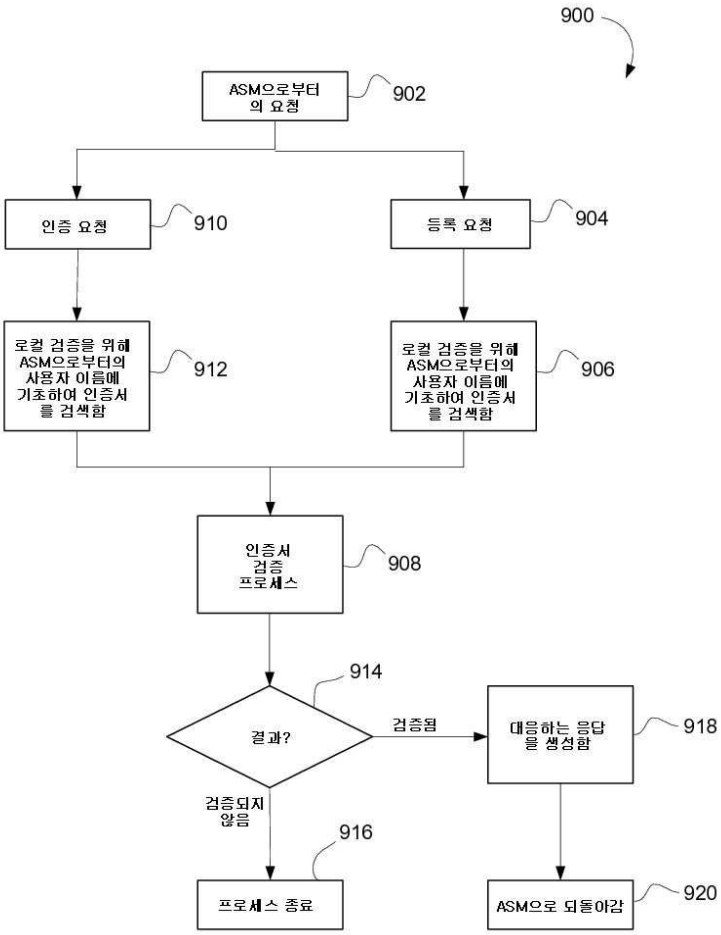
도면7


701
생체 인식
FIDO 클라이언트/인증자
726
712
1. 일반 액세스 요청.
710 4. 사용자 생체 인식 인증
714
5. 서명된 어서션
716
6. 액세스
702
11. 인증서 검증
728
12. 서명된 어서션
15. 액세스
730
718
10. 사용자 x.509 인증
724
700
708
734
732
7/8 결과 확인/리턴
일반 신뢰 당사자 애플리케이션
704
706
2/3, 8/9 인증 요청 트리거/생성
13/14 결과 확인/리턴
722
720
기밀 신뢰 당사자 애플리케이션

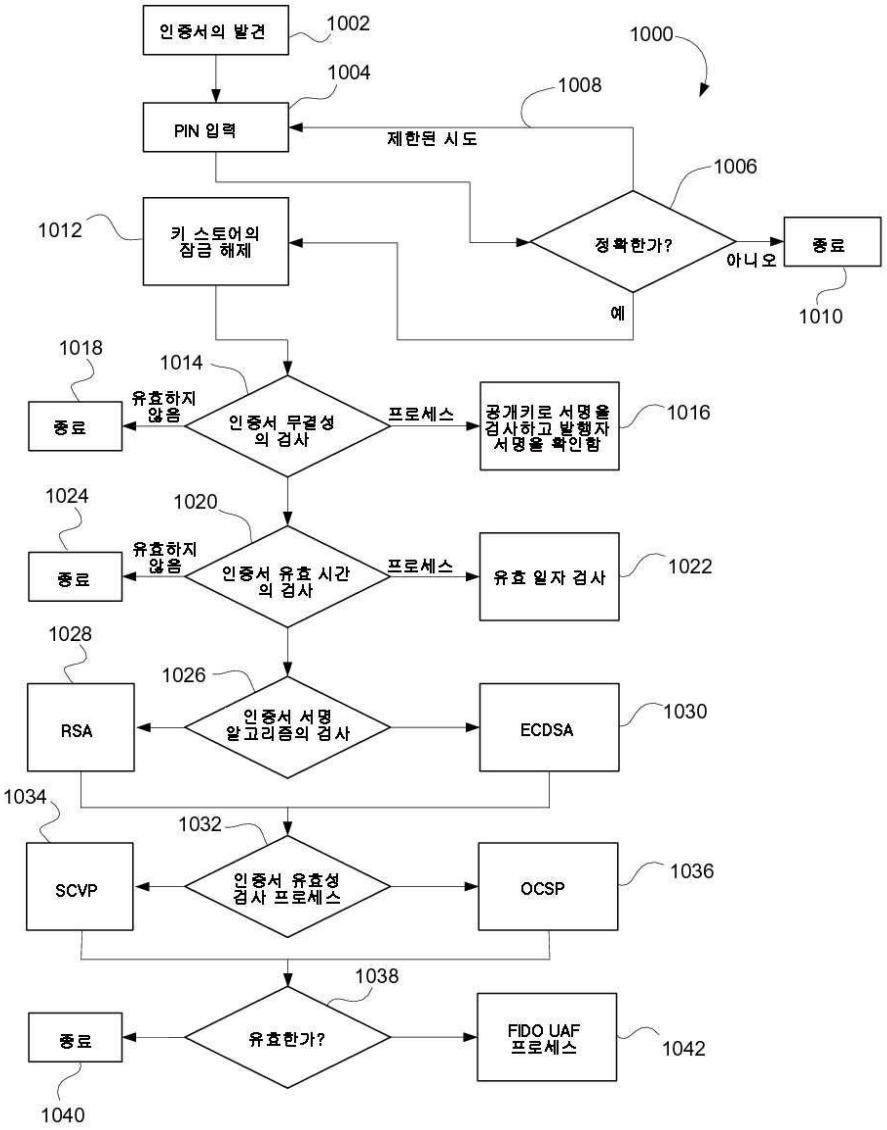
도면8


800
FIDO 클라이언트 로부터의 요청
802
인증자를 찾아냄
804
인증 요청
806
사용자가 인증자에 등록되어 있는가?
808
등록 프로세스
사용자 확인
810
인증 프로세스
사용자 확인
812
사용자의 식별 정보 입력
814
확인?
816
아니오
예
x.509 검증 프로세스
818
합격/실패
820
합격
긍정 응답 생성
822
실패
실패 응답 생성
824
FIDO 클라이언트로 응답을 리턴함
826
FIDO 클라이언트 확인응답
828

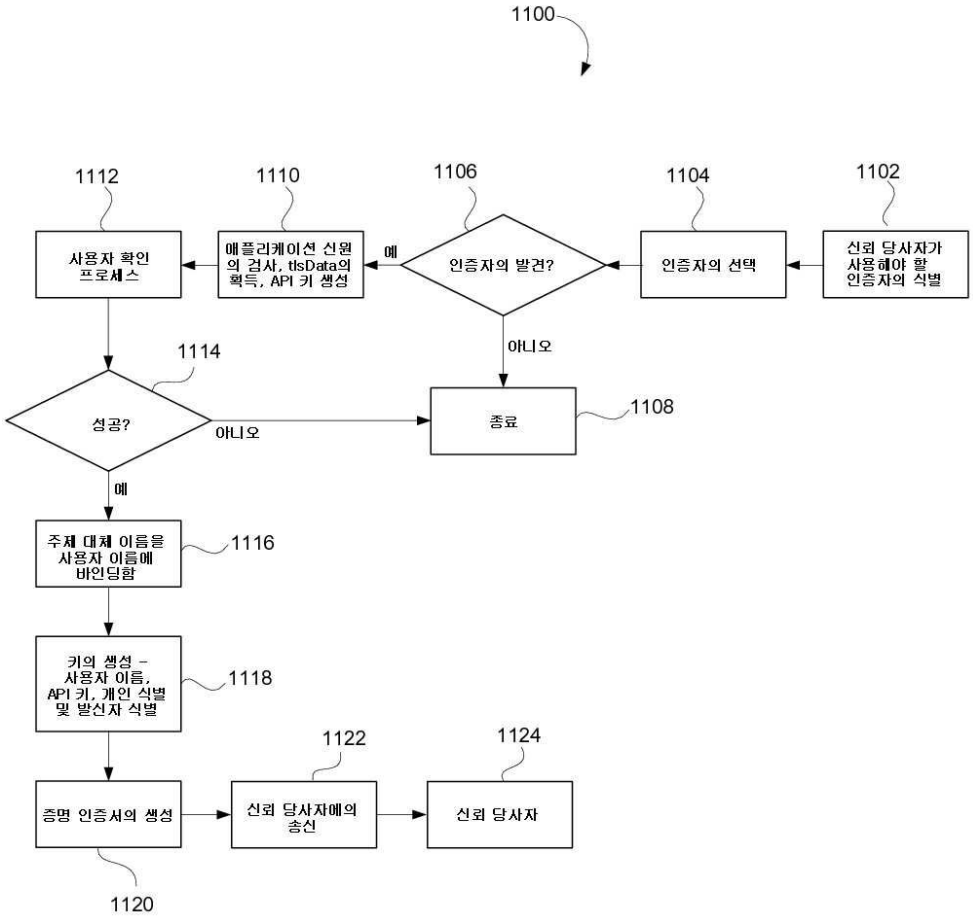
도면9


900
ASM으로부터 의 요청
902
인증 요청
910
등록 요청
904
로컬 검증을 위해 ASM으로부터의 사용자 이름에 기초하여 인증서를 검색함
912
로컬 검증을 위해 ASM으로부터의 사용자 이름에 기초하여 인증서를 검색함
906
인증서 검증 프로세스
908
914
결과?
검증됨
대응하는 응답을 생성함
918
검증되지 않음
916
프로세스 종료
ASM으로 되돌아감
920

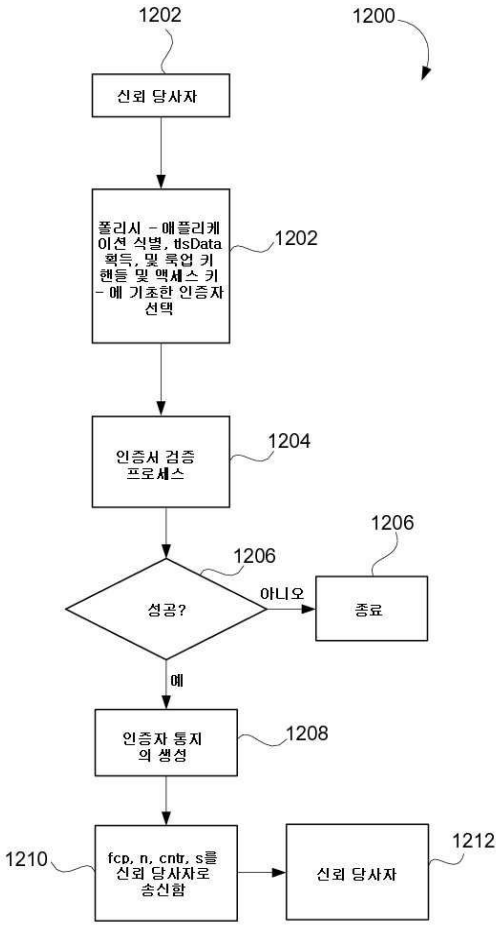
도면10


인증서의 발견
1002
1000
1004
1008
PIN 입력
제한된 시도
1006
1012
키 스토어의 잠금 해제
정확한가?
아니오
종료
1010
예
1018
1014
유효하지 않음
종료
인증서 무결성의 검사
프로세스
공개키로 서명을 검사하고 발행자 서명을 확인함
1016
1024
1020
유효하지 않음
종료
인증서 유효 시간의 검사
프로세스
유효 일자 검사
1022
1028
1026
RSA
인증서 서명 알고리즘의 검사
ECDSA
1030
1034
1032
SCVP
인증서 유효성 검사 프로세스
OCSP
1036
1038
종료
유효한가?
FIDO UAF 프로세스
1042
1040

도면11


1100
1112
사용자 확인 프로세스
1110
애플리케이션 신원의 검사, tlsData의 획득, API 키 생성
예
1106
인증자의 발견?
1104
인증자의 선택
1102
신뢰 당사자가 사용해야 할 인증자의 식별
아니오
1114
성공?
아니오
1108
종료
예
주체 대체 이름을 사용자 이름에 바인딩함
1116
키의 생성 - 사용자 이름, API 키, 개인 식별 및 발신자 식별
1118
1122
증명 인증서의 생성
신뢰 당사자에의 송신
1124
신뢰 당사자
1120

도면12


1202
1200
신뢰 당사자
폴리시 - 애플리케이션 식별, tlsData 획득, 및 룩업 키 핸들 및 액세스 키 - 에 기초한 인증자 선택
1202
인증서 검증 프로세스
1204
1206
1206
성공?
아니오
종료
예
인증자 통지의 생성
1208
1210
fcp, n, cntr, s를 신뢰 당사자로 송신함
신뢰 당사자
1212