



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0080576
(43) 공개일자 2017년07월10일

(51) 국제특허분류(Int. Cl.)
G06F 21/35 (2013.01) H04W 4/00 (2009.01)
(52) CPC특허분류
G06F 21/35 (2013.01)
H04W 4/008 (2013.01)
(21) 출원번호 10-2017-7011067
(22) 출원일자(국제) 2015년09월23일
심사청구일자 없음
(85) 번역문제출일자 2017년04월24일
(86) 국제출원번호 PCT/SG2015/050334
(87) 국제공개번호 WO 2016/048240
국제공개일자 2016년03월31일
(30) 우선권주장
10201406045P 2014년09월24일 싱가포르(SG)

(71) 출원인
버티컬 소프트웨어 아시아 피티이 리미티드
싱가포르 에스768160 싱가포르 에이'포쉬 비즈허브 #04-27 1 이슌 인더스트리얼 스트리트 1
(72) 발명자
고 기안 화
싱가포르 에스768160 싱가포르 에이'포쉬 비즈허브 #04-27 1 이슌 인더스트리얼 스트리트 1
탄 춘 웨이 손
싱가포르 에스768160 싱가포르 에이'포쉬 비즈허브 #04-27 1 이슌 인더스트리얼 스트리트 1
(74) 대리인
정홍식, 김태현

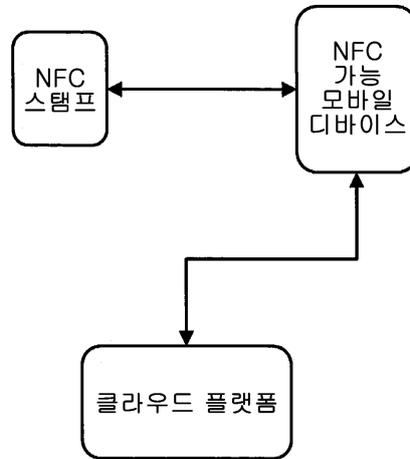
전체 청구항 수 : 총 3 항

(54) 발명의 명칭 **인증 시스템 및 방법**

(57) 요약

클라우드 플랫폼에 접속된 2FA 프로세스를 통해 문서들을 인증 및 검증하기 위한 고무 스탬프에 내장된 NFC 칩을 활용하기 위한 시스템이 본원에 설명되며, 시스템은 NFC 기저대역에 동작가능하게 접속되는 보안 엘리먼트; 및 보안 엘리먼트에 저장된 고유 인증 id를 포함한다.

대표도 - 도1



명세서

청구범위

청구항 1

문서를 인증하기 위한 물체와 커플링가능한(couplable) 내장된(embedded) NFC 칩을 활용하기 위한 인증 시스템으로서,

모바일 통신 디바이스를 포함하고, 상기 모바일 통신 디바이스는, NFC 칩의 상기 모바일 통신 디바이스와의 근접을 검출하는 것 및 상기 모바일 통신 디바이스와 사용자와의 상호작용에 의해 상기 사용자에게 의한 개시 중 적어도 하나를 통해 인증 프로세스의 개시를 가능하게 하는 모바일 애플리케이션을 실행하는 제어기를 포함하고, 상기 인증 프로세스는 상기 사용자로부터의 패스워드 코드, 및 상기 사용자로부터의 사용자 id 및 상기 NFC 칩으로부터의 NFC 칩 id 중 적어도 하나를 프롬프트(prompt)하기 위한 것이고, 상기 패스워드 코드, 및 상기 NFC 칩 id 및 상기 사용자 id 중 적어도 하나는 인증을 위해 클라우드 플랫폼에 제공가능하고,

상기 패스워드 코드, 및 상기 NFC 칩 id 및 상기 사용자 id 중 적어도 하나의 긍정적 인증(positive authentication)시에, 이에 따라 상기 모바일 통신 디바이스 및 상기 모바일 통신 디바이스와 데이터 통신하는 시스템 중 하나에 의해 저장되고 프로세싱가능한 문서에 대한 적용 또는 그와의 연관 중 하나를 위해 상기 클라우드 플랫폼으로부터 이미지가 수신가능한,

NFC 칩을 활용하기 위한 인증 시스템.

청구항 2

제 1 항에 있어서,

상기 물체는 고무 스탬프, 신용 카드 및 다른 물체들에 커플링가능한 물질 중 하나인,

NFC 칩을 활용하기 위한 인증 시스템.

청구항 3

클라우드 플랫폼에 접속된 2FA 프로세스를 통해 문서들을 인증 및 검증하기 위한 고무 스탬프에 내장된 NFC 칩을 활용하기 위한 시스템으로서,

- a. NFC 기저대역(baseband)에 동작가능하게 접속되는 보안 엘리먼트; 및
- b. 보안 엘리먼트에 저장된 고유 인증 id를 포함하는,

NFC 칩을 활용하기 위한 시스템.

발명의 설명

기술분야

[0001] 본 발명은 일반적으로, 클라우드-기반 플랫폼을 갖는 인증을 위한 트리거(trigger)로서, 디바이스 예를 들어, 고무 스탬프, 신용 카드에 결합되어, 사용자가 문서들에 보안 서명할 수 있도록 인가할 NFC의 사용에 관한 것이다.

배경기술

[0002] NFC의 사용은 시장에서 보편적이 되었다. 실세계에서 문서들을 인증하기 위한 고무 스탬프들은 문서 프로세싱 및 서명의 전자적 솔루션들이 존재한다는 사실에도 불구하고 여전히 보편적이다.

[0003] 근거리 통신(NFC)은 데이터를 교환하기 위하여 전자파를 사용하는 기술이다. NFC 파들은 단거리(수 인치 정도)를 통해 고주파수로 송신된다. NFC 디바이스들은 이미 매장 디바이스들에서 결제하기 위해 사용되고 있다. NFC는 변조 방식들, 코딩, 전송 속도들 및 RF 인터페이스를 특징하는 공개 표준이다(예를 들어, ISO/IEC 18092 참조). NFC는 금융 거래들 및 액세스 제어를 위한 더 양호한 보안을 입증하기 때문에 통신 플랫폼으로 NFC에

대한 더 넓은 채택들이 존재해 왔다.

[0004] 실세계에서 문제가 되는 것은 어떠한 단일 회사도 문서 진본성(authenticity) 검증 방법을 도입할 수 없다는 것이다. 이것은, 특정 비즈니스 프로세스에서 문서들이 고무 스탬프를 사용하여 회사 검사로 검증될 필요가 있기 때문에, 회사들이 진정한 페이퍼리스(paperless)를 행하지 못하는 것을 초래하였다.

[0005] 따라서, 본 발명은 스탬프에 내장된(embedded) NFC 태그를 갖추으로써 인증 디바이스로서 고무 스탬프 등의 물체들의 사용을 재정의하여 이러한 문제를 해결하고자 한다.

발명의 내용

[0006] 본 발명의 일 양상에 따르면, 모바일 통신 시스템을 포함하는, 문서를 인증하기 위한 물체와 커플링가능한(couplable) 내장된(embedded) NFC 칩을 활용하기 위한 인증 시스템이 개시된다. 모바일 통신 디바이스는, NFC 칩의 모바일 통신 디바이스와의 근접을 검출하는 것 및 모바일 통신 디바이스와 사용자와의 상호작용에 의해 사용자에게 의한 개시 중 적어도 하나를 통해 인증 프로세스의 개시를 가능하게 하는 모바일 애플리케이션을 실행하는 제어기를 포함하고, 인증 프로세스는 사용자로부터의 패스워드 코드, 및 사용자로부터의 id 및 NFC 칩으로부터의 NFC 칩 id 중 적어도 하나를 프롬프트(prompt)하기 위한 것이고, 패스워드 코드, 및 NFC 칩 id 및 사용자 id 중 적어도 하나는 인증을 위해 클라우드 플랫폼에 제공가능하다. 패스워드 코드, 및 NFC 칩 id 및 사용자 id 중 적어도 하나의 긍정적 인증(positive authentication)시에, 이에 따라 모바일 통신 디바이스 및 모바일 통신 디바이스와 데이터 통신하는 시스템 중 하나에 의해 저장되고 프로세싱가능한 문서에 대한 적용 또는 그와의 연관 중 하나를 위해 클라우드 플랫폼으로부터 이미지가 수신가능하다.

[0007] 본 발명의 제 2 양상에 따르면, 클라우드 플랫폼에 접속된 2FA 프로세스를 통해 문서들을 인증 및 검증하기 위한 고무 스탬프에 내장된 NFC 칩을 활용하기 위한 시스템이 개시되며, 시스템은 NFC 기저대역에 동작가능하게 접속되는 보안 엘리먼트; 및 보안 엘리먼트에 저장된 고유 인증 id를 포함한다.

도면의 간단한 설명

[0008] 본 개시의 더 양호한 이해를 위해, 비제한적이고 비포괄적인 실시예들이 다음의 도면들을 참조하여 설명된다. 도면들에서, 달리 언급되지 않는 한, 동일한 참조 번호들은 모든 다양한 도면들에 걸친 부분들을 지칭한다.

도 1은 본 발명의 실시예에 따른 클라우드에서의 플랫폼과 고무 스탬프 내의 내장된(embedded) NFC 칩 사이에서 실행되는 인증 방법을 이용하는 인증 시스템의 시스템 도면이다.

도 2는 모바일 애플리케이션에 내장된(embedded) 라이브러리에 의해 트리거링(trigger)될 수 있는 2개의 동작들의 옵션을 갖는 도 1의 인증 시스템의 시스템 흐름도를 도시한다.

도 3은 NFC-가능 고무 스탬프(NFC-Enabled Rubber Stamp) 에 의해 트리거링(trigger) 수 있는 도 2의 인증 방법/프로세스의 옵션들 중 하나의 시스템 흐름도를 도시한다.

도 4는 인증된 모바일 애플리케이션에 의해 트리거링(trigger)될 수 있는 도 2의 인증 방법/프로세스의 옵션들 중 다른 하나의 시스템 흐름도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0009] 본 발명의 예시적인 실시예, 즉, 인증 시스템을 활용한 인증 방법은 이하 도 1, 도 2, 도 3 및 도 4를 참조하여 설명된다.

[0010] 디바이스(예를 들어, 고무 스탬프)의 내장된 NFC 칩

[0011] 본 발명은 PDA의 셀룰러 폰들, 스마트 폰들, 랩탑들, 태블릿 컴퓨터들, 및 소비자 다운로드가능한 애플리케이션들에 대한 바람직한 액세스로서의 셀룰러 데이터 서비스를 포함하는 다른 모바일 디바이스들을 포함하지만 이에 제한되는 것은 아닌 다양한 여러 휴대용 통신 디바이스들과 함께 활용될 수 있는 인증 방법 및 인증 시스템(각각 "시스템" 및 "방법")을 제공한다. 하나의 이러한 디바이스는 iPhone 또는 Samsung S5 일 수 있다. 휴대용 통신 디바이스 기술 플랫폼은 Apple OS, Android OS, Microsoft Windows 모바일, Microsoft Windows Phone 7, RIM Blackberry OS, Samsung Tizen, Symbian, Java 또는 임의의 다른 기술 플랫폼일 수 있다. 본 개시의 목적들을 위해, 본 발명은 일반적으로, 클라우드에서 본 시스템에 접속되는 일반적 플랫폼을 활용하는 스마트 폰에 대해 최적화된 특징들 및 인터페이스들에 따라 설명되지만, 본 기술분야의 당업자는 모든 이러한 특징들 및 인

터페이스들이 또한 임의의 다른 플랫폼 및/또는 디바이스에 대해 사용 및 채택될 수 있음을 이해할 것이다.

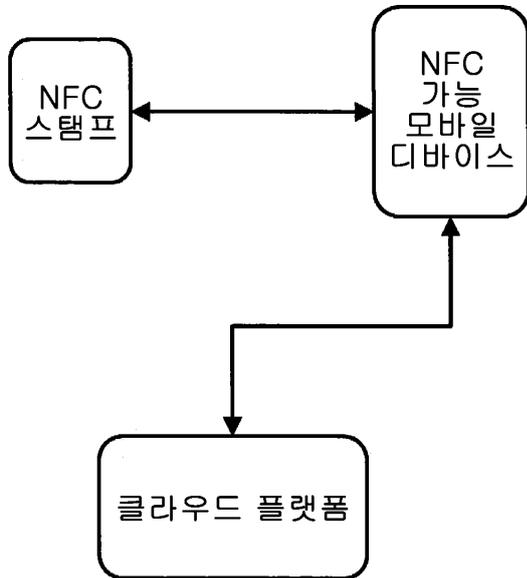
- [0012] 사용자는 본 클라우드 기반 플랫폼에 고유한 회사 id를 갖는 계정을 생성한다. 이러한 회사 id를 생성하도록 인가받은 사용자의 적법성(legitimacy)의 진본성(authenticity)을 제공한 후, 관리자 권한들이 이러한 사용자에게 할당될 것이다.
- [0013] 디바이스, 예를 들어, 전통적인 고무 스탬프, 신용 카드, 물체들 등의 채택물들에 부착가능한 물질에 내장되는 NFC 칩은 먼저, NFC 기능을 갖는 모바일 디바이스 또는 NFC 판독기를 갖는 컴퓨터의 모바일 애플리케이션 다운로드를 사용하여 최초로 인증될 것이다. 본 출원의 목적은 NFC 칩에 저장된 고유한 id를 애플리케이션 상에서 사용자에게 의해 입력된(keyed) 회사 id를 페어링(pair)하는 것이다.
- [0014] 모바일 통신 디바이스 상에 상주하는(residing) 모바일 애플리케이션에 의해 인증의 개시가 용이하게 되고 제어되는 것이 바람직하며, 모바일 애플리케이션은 최초의 사용 등록 및 인증, 모바일 통신 디바이스와 NFC 칩의 근위(proximal) 상호작용/신호 통신을 통한 인증 프로세스의 개시, 모바일 애플리케이션을 통한 및/또는 (바람직하게는 다른 모바일 통신 디바이스 상에 상주하는(residing)) 인증된 모바일 애플리케이션을 통한 인증 프로세스의 개시를 관리하고, 이미지, 예를 들어, 모바일 통신 디바이스 상에 상주하는 라이브러리에 저장되거나 또는 모바일 통신 디바이스 상에 상주하거나 그에 의해 액세스되고 있는 전자 문서에 적용될 회사 스탬프 이미지의 다운로드 및 암호해독을 관리한다.
- [0015] 모바일 애플리케이션 및 모바일 통신 디바이스는 인증 시스템의 적어도 일부를 구성하는 것이 바람직하다. 추가로, 인증 시스템은 모바일 애플리케이션이 모바일 통신 디바이스를 통해 통신 및 상호작용하는 클라우드 기반 플랫폼을 더 포함할 수 있다.
- [0016] 관리 사용자는 상이한 사용자들에게 그들의 고유한 핀으로 문서들을 인증 및 검증하기 위하여 이러한 특정 스탬프를 사용할 수 있는 권한들을 할당할 수 있다.
- [0017] 본 출원인들에 의해 사용자들에게 제공된 소프트웨어 라이브러리가 내장된 NFC 가능 모바일 통신 디바이스를 터치함으로써 스탬프가 사용될 때마다, 클라우드에서 본 플랫폼과 통신할 라이브러리에 의해 제 2 팩터(factor) 인증 프롬프트(prompt)가 트리거링(trigger)될 것이고, 이에 의해 사용자들은 인가받은 사용자로서의 자신들을 검증하기 위해 자신들의 핀을 입력하도록 요구받을 것이다. 이러한 핀은 클라우드-기반 플랫폼에 의한 검증을 위해 인증 id 및 회사 id와 함께 전송될 것이다.
- [0018] 일단 인증되면, 회사 스탬프의 디지털 이미지는 임의적인 서명 프로세스(즉, 습식 잉크 서명 또는 전자 이미지 서명)와 함께 문서에 중첩되거나, 태그되거나 병합되도록 라이브러리로 전송될 것이다.
- [0019] 이러한 서명된 문서는 검증된 사용자들에 의한 보관 및 검색을 위해 다시 클라우드에 저장될 것이다.
- [0020] 인증된 모바일 애플리케이션
- [0021] 대안적인 인증 방법은 도 4에 도시된 바와 같이 존재한다. 사용자는 모바일 인증 애플리케이션을 사용하여 회사 id로 모바일 디바이스를 클라우드 플랫폼에 페어링(pair)해야 한다.
- [0022] 사용자가 도 2 및 도 4에 도시된 바와 같이 "모바일 애플리케이션을 통한 인증" 옵션을 선택하는 경우, 사용자는 모바일 애플리케이션에 회사 id를 입력하도록 라이브러리에 의해 프롬프트된다.
- [0023] 회사 ID에 페어링된 모바일 인증 디바이스에 푸시 통지가 트리거링될 것이다. 이것은 시스템에 의해 트리거링되는 인증 프로세스를 도출할 것이다. 푸시 통지는 모바일 인증된 디바이스에 전송될 것이다. 이것은, 사용자에게 의한 인증 핀에 대해 요청하기 위해 애플리케이션에 의한 프롬프트를 트리거링할 것이다. 정확한 핀이 시스템에 입력되면, 클라우드 플랫폼은 암호화된 회사 이미지를 본 라이브러리에 의해 내장된 모바일 애플리케이션에 푸시할 것이다.
- [0024] 암호화된 회사 스탬프
- [0025] 사용자가 도 3 또는 도 4를 통해 성공적으로 인증되는 경우, 회사 스탬프 이미지를 포함하는 디지털 회사 스탬프가 생성될 뿐만 아니라, 스탬프의 일회성 사용을 인가받은 사용자의 이름 뿐만 아니라 타임스탬프가 캡슐화(encapsulated)되고 내장(embedded)될 것이다.
- [0026] 재생성된 이미지는 암호화되고, 클라우드 플랫폼으로부터 인터넷을 통해 라이브러리로 전송되고, 모바일 애플리케이션 상의 소프트웨어 라이브러리에 전송될 것이다. 소프트웨어 라이브러리에 도달하는 경우, 재생성된 이미

지는 암호해독(decrypted)되고 모바일 애플리케이션 또는 모바일 형태로 내장(embedded)된다.

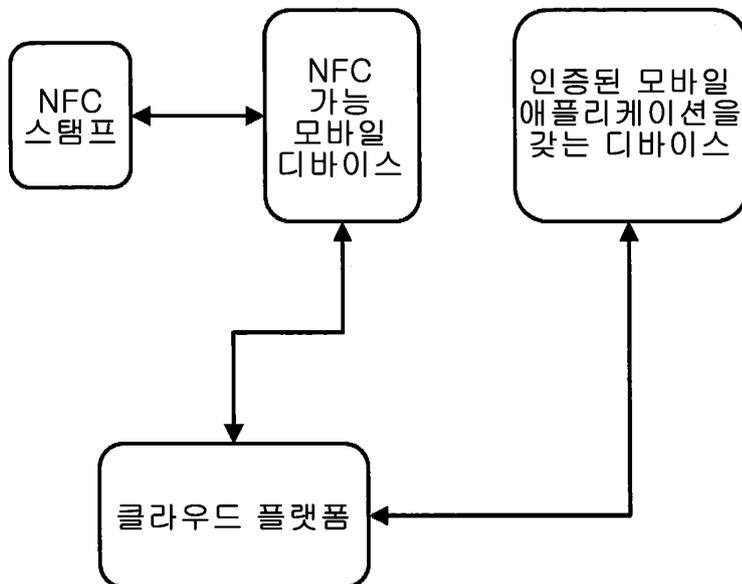
- [0027] 예들
- [0028] 구체적으로는 NFC 칩의 사용에 의한 인증 시스템 및 인증 방법의 적용의 예에서, 물류 트럭 운전사가, 본 소프트웨어 라이브러리가 내장된(embedded) 모바일 애플리케이션을 포함하는 태블릿을 휴대한다. 여기서, 태블릿은 전송된 바와 같이 모바일 통신 디바이스로서 기능한다.
- [0029] 운전사가 고객의 장소에 도달하는 경우, 그는 고객의 서명 및 회사 스탬프를 요청하는 애플리케이션을 론칭(launch)할 것이다.
- [0030] 발생할 수 있는 2개의 상황들(또는 선택가능한 2개의 옵션들)이 존재한다:
- [0031] 상황 1: (고객이 "NFC 가능 스탬프를 통한 인증"을 선택한다) <도 3 참조>
- [0032] 고객은 NFC 가능 스탬프(NFC enabled Stamp)를 사용하고 본 소프트웨어 라이브러리가 내장된 본 모바일 애플리케이션을 포함하는 NFC 가능 태블릿(NFC enabled Tablet)을 터치할 것이다. 이것은 프로세스를 트리거(trigger)할 것이고, 그에 따라 소프트웨어 라이브러리가 고객의 핀을 요청할 것이다. 회사 id, NFC 고유 id, 고객의 핀이 암호화될 것이고, 인증을 위해 클라우드에 전송될 것이다.
- [0033] 세부사항들이 성공적으로 인증되면, 회사 스탬프 이미지는 사용자 이름 뿐만 아니라 타임스탬프가 내장된(embedded) 클라우드로부터 소프트웨어 라이브러리로 전송되어, 모바일 애플리케이션 또는 모바일 형태로 전자 문서 상에 중첩될 것이다.
- [0034] 상황 2: (고객이 "모바일 인증된 디바이스를 통한 인증"을 선택한다) <도 4 참조>
- [0035] 회사 ID에 페어링(pair)된 모바일 인증 디바이스에 푸시 통지(notification)가 전송될 것이다. 고객은 디지털 회사 스탬프의 일회성 사용을 승인하기 위해 애플리케이션을 론칭(launch)할 수 있다.
- [0036] 애플리케이션은 핀 검증을 위해 프롬프트(prompt)할 것이다. 사용자가 성공적으로 인증되면, 클라우드 플랫폼은 사용자 이름 및 타임스탬프(timestamp) 세부사항들이 내장된(embedded) 암호화된 이미지를, 이러한 프로세스를 트리거링(trigger)한 모바일 애플리케이션 상의 소프트웨어 라이브러리에 푸시할 것이다.
- [0037] 본 개시의 특정 실시예들의 양상들은 기존의 컴퓨터-구현된 방법들 및 시스템들과 연관된 적어도 하나의 양상, 문제, 제한 및/또는 단점을 처리한다. 특정 실시예들과 연관된 특징들, 양상들 및/또는 이점들이 본 개시에서 설명되었지만, 다른 실시예들이 또한 이러한 특징들, 양상들 및/또는 이점들을 나타낼 수 있고, 반드시 모든 실시예들이, 본 개시의 범위에 속하는 이러한 특징들, 양상들 및/또는 이점들을 나타낼 필요는 없다. 앞서 개시된 구조들, 컴포넌트들 또는 이들의 대안들 중 몇몇이 바람직하게는 대안적인 구조들, 컴포넌트들 및/또는 애플리케이션들로 결합될 수 있음이 당업자에 의해 인식될 것이다. 또한, 본 개시의 범위 내에서 당업자에 의해 개시되는 다양한 실시예들에 대해 다양한 수정들, 변경들 및/또는 개선들이 행해질 수 있으며, 이는 하기 청구항들에 의해서만 제한된다.

도면

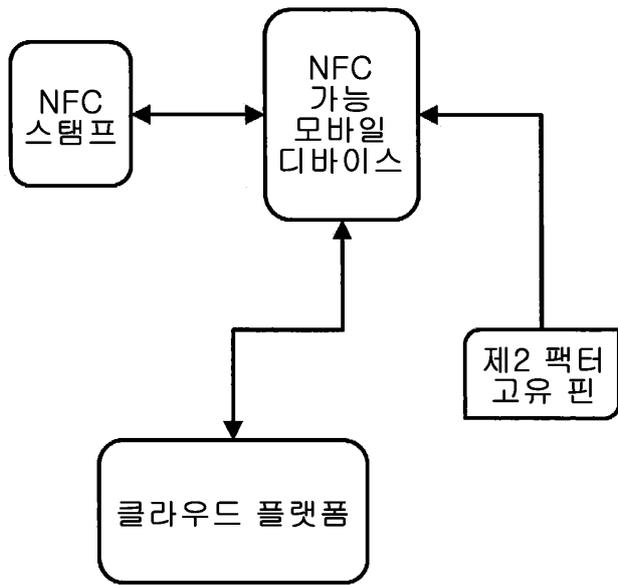
도면1



도면2



도면3



도면4

