



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0001112
(43) 공개일자 2014년01월06일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) H04W 12/06 (2009.01)
G06K 17/00 (2006.01)
(21) 출원번호 10-2013-0065693
(22) 출원일자 2013년06월10일
심사청구일자 2013년06월10일
(30) 우선권주장
1020120067945 2012년06월25일 대한민국(KR)

(71) 출원인
주식회사 썬크폴
서울특별시 영등포구 국제금융로 70, 15층(여의도
동, 미원빌딩)
(72) 발명자
김동진
서울특별시 서초구 서초중앙로 200, 12동 901호
(서초동, 삼풍아파트)
김대진
서울특별시 종로구 평창12길 8-22, 금강파크빌리
지 1동 101호 (평창동)
(뒷면에 계속)
(74) 대리인
심충섭

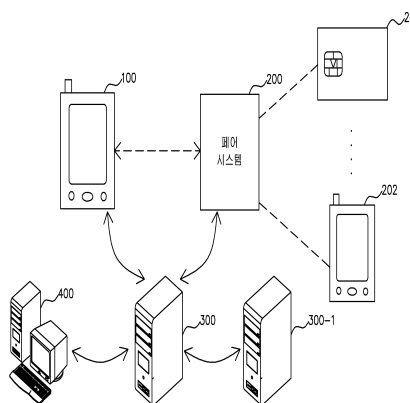
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 NFC 보안 디지털 시스템, 상기 보안 디지털 시스템과 페어를 이루는 페어 시스템, 및 그 제공방법

(57) 요약

NFC 보안 디지털 시스템, 페어 시스템, 및 그 제공방법이 개시된다. 상기 NFC 보안 디지털 시스템은 페어 시스템과 NFC(Near Field Communication) 통신을 수행하기 위한 통신모듈, 상기 통신모듈이 상기 페어 시스템과 적어도 한 번 태깅이 되는 경우, 상기 통신모듈을 통해 상기 페어 시스템으로부터 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 수신하고, 수신된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 인증 시스템으로 전송하는 제어모듈을 포함하며, 전송된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보에 기초하여 상기 인증 시스템에 의해 OTP 또는 인증정보가 생성되며, 상기 인증 시스템에 상기 보안 디지털 시스템의 식별정보 또는 상기 페어 시스템의 식별정보 중 적어도 하나가 미리 등록되어 있는 것을 특징으로 한다.

대표도 - 도1



(72) 발명자

심충섭

서울특별시 용산구 효창원로15길 16, 102동 307호
(신창동, 세방리버하이빌)

이병주

경기도 수원시 장안구 연무로56번길 14-3 (연무동)

특허청구의 범위

청구항 1

OTP 또는 인증정보를 이용해 인증 요청자를 인증하기 위한 보안 디지털 시스템에 있어서,

페어 시스템과 NFC(Near Field Communication) 통신을 수행하기 위한 통신모듈; 및

상기 통신모듈이 상기 페어 시스템과 적어도 한 번 태깅이 되는 경우, 상기 통신모듈을 통해 상기 페어 시스템으로부터 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 수신하고, 수신된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 인증 시스템으로 전송하는 제어모듈을 포함하며,

전송된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보에 기초하여 상기 인증 시스템에 의해 OTP 또는 인증정보가 생성되며,

상기 인증 시스템에 상기 보안 디지털 시스템의 식별정보 또는 상기 페어 시스템의 식별정보 중 적어도 하나가 미리 등록되어 있는 것을 특징으로 하는 NFC 보안 디지털 시스템.

청구항 2

제1항에 있어서, 상기 생성된 OTP 또는 인증정보는 ,

상기 인증 시스템에 의해 상기 보안 디지털 시스템 또는 상기 인증 시스템에 미리 등록된 상기 인증 요청자의 지정 단말기로 전송되는 것을 특징으로 하는 NFC 보안 디지털 시스템.

청구항 3

제1항에 있어서, 상기 제어모듈은,

상기 보안 디지털 시스템과 페어를 이루도록 미리 정의된 상기 페어 시스템의 식별정보를 저장하며,

미리 저장된 식별정보에 상응하는 상기 페어 시스템과 상기 보안 디지털 시스템이 적어도 한 번 태깅하여야, 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 상기 인증 시스템으로 전송하도록 제어하는 NFC 보안 디지털 시스템.

청구항 4

제1항에 있어서, 상기 보안 디지털 시스템은,

상기 보안 디지털 시스템의 식별정보를 더 상기 인증 시스템으로 전송하며,

전송된 상기 보안 디지털 시스템의 식별정보가 상기 인증 시스템에 미리 등록되어 있는 상기 보안 디지털 시스템의 식별정보와 상응하는 경우, 상기 인증 시스템에 의해 상기 OTP 또는 인증정보가 생성되는 것을 특징으로 하는 NFC 보안 디지털 시스템.

청구항 5

제1항에 있어서, 상기 인증 시스템에 의해 생성된 상기 OTP와,

소정의 OTP 인증 시스템에 의해 생성된 상기 인증 요청자에 상응하는 인증용 OTP가 서로 상응하는 경우, 상기 인증 시스템에 의해 상기 인증 요청자가 인증되는 것을 특징으로 하는 NFC 보안 디지털 시스템.

청구항 6

제2항에 있어서, 상기 보안 디지털 시스템 또는 상기 지정 단말기로 전송된 상기 OTP가 상기 보안 디지털 시스템 또는 소정의 데이터 프로세싱 장치를 통해 상기 인증 시스템으로 재전송되면,

상기 인증시스템이 전송한 상기 인증 요청자에 상응하는 인증용 OTP와 재전송된 상기 OTP가 서로 상응하는 경우 상기 인증 시스템에 의해 상기 인증 요청자가 인증되는 것을 특징으로 하는 NFC 보안 디지털 시스템.

청구항 7

제2항에 있어서, 상기 보안 디지털 시스템 또는 상기 지정 단말기로 전송된 상기 인증정보가 상기 보안 디지털 시스템 또는 소정의 데이터 프로세싱 장치를 통해 상기 인증 시스템으로 재전송되면,

상기 인증 시스템이 전송한 상기 인증정보와 상기 인증 시스템으로 재전송된 인증정보가 상응하는 경우, 상기 인증 시스템에 의해 상기 인증 요청자가 인증되는 것을 특징으로 하는 NFC 보안 디지털 시스템.

청구항 8

OTP 또는 인증정보를 이용해 인증 요청자를 인증하기 위한 인증 시스템에 있어서,

보안 디지털 시스템과 페어 시스템이 NFC(Near Field Communication) 통신을 수행하면, 상기 페어 시스템으로부터 상기 보안 디지털 시스템으로 전송된 OTP 정보 또는 상기 페어 시스템의 식별정보를 상기 보안 디지털 시스템으로부터 수신하기 위한 수신부;

수신한 상기 OTP 정보 또는 상기 페어 시스템의 식별정보에 기초하여 OTP또는 인증정보를 생성하기 위한 생성부; 및

상기 생성부에 의해 생성된 OTP 또는 인증정보에 기초하여 상기 인증 요청자의 인증 성공여부를 판단하기 위한 제어부를 포함하는 인증 시스템.

청구항 9

제8항에 있어서, 상기 인증 시스템은,

상기 보안 디지털 시스템의 식별정보 또는 상기 페어 시스템의 식별정보 중 적어도 하나가 미리 등록되어 있는 저장부를 더 포함하는 것을 특징으로 하는 인증 시스템.

청구항 10

제8항에 있어서, 상기 인증 시스템은,

상기 생성부에 의해 생성된 상기 OTP 또는 상기 인증정보를 상기 보안 디지털 시스템 또는 상기 인증 시스템에 미리 등록된 상기 인증 요청자의 지정 단말기로 전송하기 위한 송신부를 더 포함하는 것을 특징으로 하는 인증 시스템.

청구항 11

제9항에 있어서, 상기 생성부는,

상기 수신부를 통해 수신된 상기 보안 디지털 시스템의 식별정보가 상기 인증 시스템에 미리 등록되어 있는 정보와 상응하는 경우에 상기 OTP 또는 상기 인증정보를 생성하는 인증 시스템.

청구항 12

제8항에 있어서, 상기 제어부는,

상기 생성부에 의해 생성된 상기 OTP와 소정의 OTP 인증 시스템에 의해 생성된 상기 인증 요청자에 상응하는 인증용 OTP가 서로 상응하는지 여부를 판단하여 상기 인증 요청자의 인증성공 여부를 판단하는 것을 특징으로 하는 인증 시스템.

청구항 13

제10항에 있어서, 상기 제어부는,

상기 송신부에 의해 상기 보안 디지털 시스템 또는 상기 지정 단말기로 전송된 상기 OTP가 상기 보안 디지털 시스템 또는 소정의 데이터 프로세싱 장치를 통해 상기 수신부로 수신되면,

상기 인증시스템에 의해 생성된 상기 인증 요청자에 상응하는 인증용 OTP와 상기 수신부에 의해 수신된 상기 OTP가 상응하는지 여부를 판단하여 상기 인증 요청자의 인증 성공 여부를 판단하는 인증 시스템.

청구항 14

제10항에 있어서, 상기 제어부는,

상기 송신부에 의해 상기 보안 디지털 시스템 또는 상기 지정 단말기로 전송된 상기 인증정보가 상기 보안 디지털 시스템 또는 소정의 데이터 프로세싱 장치를 통해 상기 수신부로 수신되면,

상기 송신부에 의해 송신된 인증정보와 상기 수신부에 의해 수신된 인증정보가 상응하는지 여부를 판단하여 상기 인증 요청자의 인증 성공 여부를 판단하는 인증 시스템.

청구항 15

OTP 또는 인증정보를 이용해 인증 요청자를 인증하기 위한 보안 디지털 시스템의 제공방법에 있어서,

보안 디지털 시스템이 페어 시스템과 적어도 한 번 태깅을 수행하는 단계;

상기 보안 디지털 시스템이 상기 페어 시스템으로부터 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별 정보를 수신하는 단계; 및

상기 보안 디지털 시스템이 수신된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 인증 시스템으로 전송하는 단계를 포함하며,

전송된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보에 기초하여 상기 인증 시스템에 의해 OTP 또는 인증정보가 생성되며,

상기 인증 시스템에 상기 보안 디지털 시스템의 식별정보 또는 상기 페어 시스템의 식별정보 중 적어도 하나가 미리 등록되어 있는 것을 특징으로 하는 보안 디지털 시스템 제공방법.

청구항 16

OTP 또는 인증정보를 이용해 인증 요청자를 인증하기 위한 인증 시스템의 제공방법에 있어서,

인증 시스템이 보안 디지털 시스템과 페어 시스템이 적어도 한 번 태깅되면, 상기 페어 시스템으로부터 상기 보안 디지털 시스템으로 전송된 OTP 정보 또는 상기 페어 시스템의 식별정보를 상기 보안 디지털 시스템으로부터 수신하는 단계;

상기 인증 시스템이 수신한 상기 OTP 정보 또는 상기 페어 시스템의 식별정보에 기초하여 OTP 또는 인증정보를

생성하는 단계; 및

상기 인증 시스템이 생성된 OTP 또는 인증정보에 기초하여 상기 인증 요청자의 인증 성공여부를 판단하는 단계를 포함하는 인증 시스템 제공방법.

명세서

기술분야

[0001] 본 발명은 NFC 보안 디지털 시스템, 상기 NFC 보안 디지털 시스템과 페어를 이루는 페어 시스템, 및 그 제공방법에 관한 것으로, 보다 상세하게는 개인을 인증하는데 널리 사용되는 보안인증 정보(예컨대, 보안카드 번호 또는 OTP(One Time Password))를 획득하기 위해 서로 독립적인 두 개의 장치를 필요로 하도록 함으로써 보안성을 획기적으로 높일 수 있는 시스템 및 그 제공방법에 관한 것이다.

배경기술

[0002] 유무선 네트워크를 통한 다양한 온라인 서비스가 제공되면서 사용자를 인증하는 다양한 방식이 공지되어 있다. 로그인 정보를 이용한 로그인 인증, 보안카드를 이용한 인증, 공인인증서를 이용한 인증 또는 OTP(One Time Password)를 이용한 인증 등이 그러한 예이다.

[0003] 상기의 다양한 인증 방식 중 로그인 인증은 어떤 특정한 장치를 요구하지 않고, 로그인 정보를 알고 있는 사람을 로그인 정보에 상응하는 계정의 본인이라고 인증하는 방식이며, 공인인증서를 이용한 인증은 공인인증서라는 전자적 데이터를 가지고 있어야 하지만 전자적 데이터이기 때문에 인증을 요청하는 시스템(예컨대, 사용자의 컴퓨터, 모바일 폰 등)이외에 별도의 인증장치를 요구하지 않는다. 공인인증서는 인증을 요청하는 시스템에 저장될 수도 있다. 물론 별도의 장치(예컨대, USB 저장장치 등의 모바일 저장장치)에 상기 공인인증서가 저장될 수도 있지만, 상기 별도의 장치는 범용의 데이터 저장장치이면 족한 것이지 인증을 위해 사용자에게만 할당되는 별도의 장치가 요구되지는 않는다.

[0004] 한편, 보안카드 또는 OTP 생성장치는 특정인(특정 개인뿐만 아니라 법적 독립적 행위가 가능한 법인체 등을 포함하는데, 본 발명에서는 이들 모두를 포함하는 의미로 특정인 또는 특정 개인이라 한다.)을 인증하기 위해 특정인에게 지급되는 인증용 장치로 구현된다. 따라서, 온라인 상에서 소정의 서비스(예컨대, 로그인, 금융거래 등)를 요청하는 사용자가 본인이 상기 특정인임을 증명하기 위해서는 상기 보안카드 또는 OTP 생성장치를 보유하고 있어야 하는 것이 원칙이다.

[0005] 하지만, 보안카드는 주로 사용자들이 지갑 등에 휴대하기 용이하도록 구현되는 반면, 인증방식의 특성상 상기 보안카드에 적힌 정보들이 노출되거나 유출되는 경우, 더 이상 상기 보안카드를 통한 인증 기능은 기대할 수 없게 된다.

[0006] 한편, OTP를 통한 인증은 OTP 인증 시스템과 OTP 생성 장치가 OTP 생성키(비밀키)를 공유하고 있으면서, 각각 동일한 OTP 생성로직(프로그램)을 이용해 동일한 일회용 패스워드 즉, OTP를 생성하는 방식이다. 따라서, OTP 생성 장치는 연산장치, 저장장치, 및 전원을 필요로 하므로 상기 보안카드에 비해서는 상대적으로 휴대성이 낮아진다. 토큰형 OTP 생성장치는 상대적으로 휴대성이 크게 낮아지며, 최근에 카드형 OTP 생성장치가 구현되어 사용자의 지갑에 휴대될 수 있어서 휴대성이 다소 높아지긴 하였다. 하지만, 카드형 OTP 생성장치 역시 OTP를 생성하기 위해서는 전원을 필요로 하므로 사용기간에 제약을 받게 되고, 또한 지갑에서 상기 카드형 OTP 생성장치를 꺼내어서 OTP 생성요청을 하는 행위가 필요하게 된다.

[0007] 따라서 사용자는 현재 인증을 요청하는 시스템에서 필요한 보안정보를 위해 상기 시스템이 아닌 인증을 위한 별도의 보안장치(예컨대, 보안카드 또는 OTP 생성장치 등)를 찾거나 꺼내고, 이를 조작하거나 확인한 후 다시 상기 시스템을 제어하여야 하는 등의 불편한 동작을 수행하여야 하는 문제점이 존재하였다.

[0008] 또한, 어떠한 방식이든 종래의 OTP 생성장치는 상대적으로 휴대성이 낮은 문제점, 전원이 필요하므로 전원이 고갈되면 OTP 생성장치를 새롭게 발급받아야 하는 문제점, 분실되어 부정한 사용자가 점유하게 되는 경우 보안성의 리스크가 현저하게 높아지는 문제점 등이 존재하였다.

[0009] 특히, 보안장치(예컨대, 보안카드 또는 OTP 생성장치 등)를 이용하는 인증 방식은 상기 보안장치가 독립적으로 보안정보(예컨대, 보안카드 번호)를 모두 가지고 있거나 보안정보(OTP)를 생성하므로, 상기 보안장치가 분실 또는 도난에 의해 타인의 손에 넘어가게 되는 경우 보안성에 치명적인 문제점이 발생하게 된다.

[0010] 또한 이러한 분실 또는 도난 등의 위험성은 아니더라도 보안정보를 획득하기 위해 보안장치를 지갑에서 꺼내어서 보안정보를 획득하고 다시 지갑에 넣어야 하는 번거로움이 존재하며, 이러한 행위 자체가 분실 또는 도난을 유발하게 되는 시발점이 되곤 하였다.

발명의 내용

해결하려는 과제

[0011] 따라서, 본 발명이 이루고자 하는 기술적인 과제는 보안정보를 어느 하나의 독립적인 보안장치를 통해 획득할 수 있는 것이 아니라, 페어(pair, 쌍)를 이루도록 정해져 있는 두 개의 시스템(또는 장치)을 모두 가지고 있는 경우에만 사용자가 보안정보를 획득할 수 있도록 하는 시스템 및 그 제공방법을 제공하는 것이다.

[0012] 또한, 보안정보를 핸들링 하는 시스템이 두 개인 경우에 발생할 수 있는 보안정보의 유출 또는 노출의 위험성을 줄일 수 있도록, 보안정보 중 적어도 일부를 획득한 디지털 시스템은 보안정보의 사용이 완료되거나 사용자가 해당 보안정보를 획득하기 위한 제어를 하지 않는 경우, 획득한 정보를 삭제할 수 있는 시스템 및 그 방법을 제공하는 것이다.

[0013] 또한, 페어 시스템이 보안정보(예컨대, 보안코드 즉, 보안카드 번호)를 저장하고 있는 경우, 상기 보안정보를 상기 페어 시스템과 페어를 이루는 디지털 시스템을 통해서만 획득될 수 있도록 하는 시스템 및 그 제공방법을 제공하는 것이다.

[0014] 또한, NFC 태깅을 통해 간편하게 보안정보를 획득할 수 있는 시스템 및 그 제공방법을 제공하는 것이다. 또한, 복수의 태깅을 수행하여야 보안정보를 획득할 수 있도록 함으로써, 사용자가 원하지 않는 태깅이 수행되었을 때 불필요하게 보안정보가 획득되거나, 또는 부정한 사용자가 인식하지 못하는 중에 태깅을 통해 보안정보를 습득할 위험을 줄일 수 있는 시스템 및 그 제공방법을 제공하는 것이다.

[0015] 또한, 모바일 OTP(M-OTP) 생성장치가 가지고 있는 최대의 약점인 보안상의 문제점을 줄일 수 있는 시스템 및 그 제공방법을 제공하는 것이다. 또한 보안카드를 M-OTP처럼 모바일에 저장하여 사용할 수 있도록 하고 그 보안상의 문제점을 해결할 수 있도록 하는 시스템 및 그 제공방법을 제공하는 것이다.

[0016] 또한, 종래 지니고 다녀야 하는 보안카드의 크기의 제약과 인증에 사용될 보안카드 번호를 사람이 직접 찾아서 인증 요청시스템(예컨대, 컴퓨터 또는 모바일 폰 등)에 입력하여야 하는 요인 등으로 인해 보안카드는 통상 수십 개의 보안정보(예컨대, 보안코드)를 담을 수밖에 없었는데, 본 발명은 이러한 보안정보의 숫자의 제약을 해결하여 보안기능을 강화할 수 있는 시스템 및 그 방법을 제공하는 것이다.

[0017] 또한, 서비스를 제공하는 서비스 시스템(예컨대, 금융기관, 웹 사이트 등)들별로 사용되는 보안장치가 상이하여, 특정 개인이 이용하는 보안장치(예컨대, 보안카드 또는 OTP 생성 장치 등)가 복수 개일 수 있는데 이러한 복수 개의 보안장치를 하나로 통합하여 사용할 수 있도록 하는 시스템 및 그 방법을 제공하는 것이다.

[0018] 또한, OTP 생성의 경우, 종래에는 OTP 생성장치 하나에 대응되는 키가 OTP 생성에 이용되었지만, 본 발명에서는 디지털 시스템에 대응되는 생성키를 더 이용하여 OTP를 생성함으로써 보안성을 높일 수 있는 시스템 및 그 방법을 제공하는 것이다.

[0019] 또한, 보안 장치를 지갑에 휴대하고 있는 경우, 지갑에서 상기 보안 장치를 꺼내는 행위 없이 상기 디지털 시스템을 통해 보안정보를 획득할 수 있으므로, 보안장치의 분실의 위험을 낮추고 사용자가 간편하게 보안정보를 획득할 수 있는 시스템 및 그 방법을 제공하는 것이다.

[0020] 또한, 디지털 시스템과 페어 시스템이 일정 거리 이상 멀어지는 경우에는 상기 디지털 시스템 또는 상기 페어 시스템은 사용자에게 알람신호를 줄 수 있어서, 디지털 시스템 또는 페어 시스템의 분실 또는 도난의 경우를 사용자가 용이하게 인지할 수 있도록 하는 시스템 및 그 방법을 제공하는 것이다.

[0021] 또한, 디지털 시스템과 페어 시스템이 일정 거리 이상 멀어지는 경우에 사용자에게 알람신호를 주기 위하여 상기 디지털 시스템과 페어 시스템은 평상시 페어링 상태를 유지하게 함으로써, 상기 디지털 시스템 또는 상기 페

어 시스템의 분실 또는 도난을 예방함과 동시에 상기 디지털 시스템과 페어 시스템이 페어링을 통해 보안정보를 획득함에서 있어서 필요한 페어 형성 절차를 생략 또는 간소화하여 보다 효율적으로 보안정보를 획득할 수 있도록 하는 시스템 및 그 방법을 제공하는 것이다.

[0022] 또한, 보안 디지털 시스템과 페어 시스템이 적어도 한 번 태깅하는 경우, 인증 시스템이 인증 요청자에 상응하는 OTP를 생성할 수 있도록 함으로써, 사용자가 소지하고 있어야 하던 OTP 토큰을 인증 시스템이 대체하는 역할을 수행할 수 있으므로 OTP 토큰의 유출 또는 분실에 의한 위협에 안전하고, 사용자의 편의성 및 보안성이 현저히 높아질 수 있는 시스템 및 그 방법을 제공하는 것이다.

[0023] 또한, 인증 시스템에 미리 등록되어 있는 보안 디지털 시스템의 소유주 또는 기기의 식별정보(예컨대, 디지털 시스템의 핸드폰 번호, 디바이스의 고유 키 값 등 디지털 시스템의 소유주나 기기를 식별할 수 있는 정보, 본 명세서에서는 디지털 시스템의 식별정보로 혼용해서 사용한다.)와 페어 시스템의 식별정보 중 적어도 하나에 해당하는 기기가 페어링되거나 태깅되는 경우에만 인증 시스템이 본인인증을 위한 정보를 수신할 수 있도록 함으로써 사용자의 보안성을 한층 높일 수 있는 시스템 및 그 방법을 제공하는 것이다.

[0024] 또한, 인증 시스템에 의해 생성된 OTP 또는 인증정보를 정당 사용자에게 상응하는 지정 단말기로 전송하고, 전송된 정보를 인증 시스템이 재수신하여 재수신된 OTP 또는 인증정보가 상기 생성된 OTP 또는 인증정보와 일치하는지 여부에 따라 본인인증을 하도록 함으로써 사용자가 상기 지정 단말기를 점유하고 있는지 여부를 확인하고, 사용자 인증의 보안성을 더욱 높일 수 있는 시스템 및 그 방법을 제공하는 것이다.

과제의 해결 수단

[0025] 상기의 기술적 과제를 해결하기 위한 본 발명의 실시 예에 따른 보안 디지털 시스템은 OTP 또는 인증정보를 이용해 인증 요청자를 인증하기 위한 보안 디지털 시스템에 있어서, 페어 시스템과 NFC(Near Field Communication) 통신을 수행하기 위한 통신모듈, 및 상기 통신모듈이 상기 페어 시스템과 적어도 한 번 태깅이 되는 경우, 상기 통신모듈을 통해 상기 페어 시스템으로부터 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 수신하고, 수신된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 인증 시스템으로 전송하는 제어모듈을 포함하며, 전송된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보에 기초하여 상기 인증 시스템에 의해 OTP 또는 인증정보가 생성되며, 상기 인증 시스템에 상기 보안 디지털 시스템의 식별정보 또는 상기 페어 시스템의 식별정보 중 적어도 하나가 미리 등록되어 있는 것을 특징으로 할 수 있다.

[0026] 또한, 상기 생성된 OTP 또는 인증정보는, 상기 인증 시스템에 의해 상기 보안 디지털 시스템 또는 상기 인증 시스템에 미리 등록된 상기 인증 요청자의 지정 단말기로 전송되는 것을 특징으로 할 수 있다.

[0027] 또한, 상기 제어모듈은, 상기 보안 디지털 시스템과 페어를 이루도록 미리 정의된 상기 페어 시스템의 식별정보를 저장하며, 미리 저장된 식별정보에 상응하는 상기 페어 시스템과 상기 보안 디지털 시스템이 적어도 한 번 태깅하여야, 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 상기 인증 시스템으로 전송하도록 제어할 수 있다.

[0028] 또한, 상기 보안 디지털 시스템은, 상기 보안 디지털 시스템의 식별정보를 더 상기 인증 시스템으로 전송하며, 전송된 상기 보안 디지털 시스템의 식별정보가 상기 인증 시스템에 미리 등록되어 있는 상기 보안 디지털 시스템의 식별정보와 상응하는 경우, 상기 인증 시스템에 의해 상기 OTP 또는 인증정보가 생성되는 것을 특징으로 할 수 있다.

[0029] 또한, 상기 인증 시스템에 의해 생성된 상기 OTP와, 소정의 OTP 인증 시스템에 의해 생성된 상기 인증 요청자에 상응하는 인증용 OTP가 서로 상응하는 경우, 상기 인증 시스템에 의해 상기 인증 요청자가 인증되는 것을 특징으로 할 수 있다.

[0030] 또한, 상기 보안 디지털 시스템 또는 상기 지정 단말기로 전송된 상기 OTP가 상기 보안 디지털 시스템 또는 소정의 데이터 프로세싱 장치를 통해 상기 인증 시스템으로 재전송되면, 상기 인증시스템이 전송한 상기 인증 요청자에 상응하는 인증용 OTP와 재전송된 상기 OTP가 서로 상응하는 경우 상기 인증 시스템에 의해 상기 인증 요청자가 인증되는 것을 특징으로 할 수 있다.

[0031] 또한, 상기 보안 디지털 시스템 또는 상기 지정 단말기로 전송된 상기 인증정보가 상기 보안 디지털 시스템 또

는 소정의 데이터 프로세싱 장치를 통해 상기 인증 시스템으로 재전송되면, 상기 인증 시스템이 전송한 상기 인증정보와 상기 인증 시스템으로 재전송된 인증정보가 상응하는 경우, 상기 인증 시스템에 의해 상기 인증 요청자가 인증되는 것을 특징으로 할 수 있다.

- [0032] 상기의 기술적 과제를 달성하기 위한 본 발명의 실시 예에 따른 인증 시스템은, OTP 또는 인증정보를 이용해 인증 요청자를 인증하기 위한 인증 시스템에 있어서, 보안 디지털 시스템과 페어 시스템이 NFC(Near Field Communication) 통신을 수행하면, 상기 페어 시스템으로부터 상기 보안 디지털 시스템으로 전송된 OTP 정보 또는 상기 페어 시스템의 식별정보를 상기 보안 디지털 시스템으로부터 수신하기 위한 수신부, 수신한 상기 OTP 정보 또는 상기 페어 시스템의 식별정보에 기초하여 OTP 또는 인증정보를 생성하기 위한 생성부, 및 상기 생성부에 의해 생성된 OTP 또는 인증정보에 기초하여 상기 인증 요청자의 인증 성공여부를 판단하기 위한 제어부를 포함할 수 있다.
- [0033] 또한, 상기 인증 시스템은, 상기 보안 디지털 시스템의 식별정보 또는 상기 페어 시스템의 식별정보 중 적어도 하나가 미리 등록되어 있는 저장부를 더 포함하는 것을 특징으로 할 수 있다.
- [0034] 또한, 상기 인증 시스템은, 상기 생성부에 의해 생성된 상기 OTP 또는 상기 인증정보를 상기 보안 디지털 시스템 또는 상기 인증 시스템에 미리 등록된 상기 인증 요청자의 지정 단말기로 전송하기 위한 송신부를 더 포함하는 것을 특징으로 할 수 있다.
- [0035] 또한, 상기 생성부는, 상기 수신부를 통해 수신된 상기 보안 디지털 시스템의 식별정보가 상기 인증 시스템에 미리 등록되어 있는 정보와 상응하는 경우에 상기 OTP 또는 상기 인증정보를 생성할 수 있다.
- [0036] 또한, 상기 제어부는, 상기 생성부에 의해 생성된 상기 OTP와 소정의 OTP 인증 시스템에 의해 생성된 상기 인증 요청자에 상응하는 인증용 OTP가 서로 상응하는지 여부를 판단하여 상기 인증 요청자의 인증성공 여부를 판단하는 것을 특징으로 할 수 있다.
- [0037] 또한, 상기 제어부는, 상기 송신부에 의해 상기 보안 디지털 시스템 또는 상기 지정 단말기로 전송된 상기 OTP가 상기 보안 디지털 시스템 또는 소정의 데이터 프로세싱 장치를 통해 상기 수신부로 수신되면, 상기 인증시스템에 의해 생성된 상기 인증 요청자에 상응하는 인증용 OTP와 상기 수신부에 의해 수신된 상기 OTP가 상응하는지 여부를 판단하여 상기 인증 요청자의 인증 성공 여부를 판단할 수 있다.
- [0038] 또한, 상기 제어부는, 상기 송신부에 의해 상기 보안 디지털 시스템 또는 상기 지정 단말기로 전송된 상기 인증정보가 상기 보안 디지털 시스템 또는 소정의 데이터 프로세싱 장치를 통해 상기 수신부로 수신되면, 상기 송신부에 의해 송신된 인증정보와 상기 수신부에 의해 수신된 인증정보가 상응하는지 여부를 판단하여 상기 인증 요청자의 인증 성공 여부를 판단할 수 있다.
- [0039] 상기의 기술적 과제를 달성하기 위한 본 발명의 실시 예에 따른 보안 디지털 시스템 제공방법은, OTP 또는 인증정보를 이용해 인증 요청자를 인증하기 위한 보안 디지털 시스템의 제공방법에 있어서, 보안 디지털 시스템이 페어 시스템과 적어도 한 번 태깅을 수행하는 단계, 상기 보안 디지털 시스템이 상기 페어 시스템으로부터 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 수신하는 단계, 및 상기 보안 디지털 시스템이 수신된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 인증 시스템으로 전송하는 단계를 포함하며, 전송된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보에 기초하여 상기 인증 시스템에 의해 OTP 또는 인증정보가 생성되며, 상기 인증 시스템에 상기 보안 디지털 시스템의 식별정보 또는 상기 페어 시스템의 식별정보 중 적어도 하나가 미리 등록되어 있는 것을 특징으로 할 수 있다.
- [0040] 상기 기술적 과제를 달성하기 위한 본 발명의 실시 예에 따른 인증 시스템 제공방법은, OTP 또는 인증정보를 이용해 인증 요청자를 인증하기 위한 인증 시스템의 제공방법에 있어서, 인증 시스템이 보안 디지털 시스템과 페어 시스템이 적어도 한 번 태깅되면, 상기 페어 시스템으로부터 상기 보안 디지털 시스템으로 전송된 OTP 정보 또는 상기 페어 시스템의 식별정보를 상기 보안 디지털 시스템으로부터 수신하는 단계, 상기 인증 시스템이 수신한 상기 OTP 정보 또는 상기 페어 시스템의 식별정보에 기초하여 OTP 또는 인증정보를 생성하는 단계; 및 상기 인증 시스템이 생성된 OTP 또는 인증정보에 기초하여 상기 인증 요청자의 인증 성공여부를 판단하는 단계를 포함할 수 있다.

발명의 효과

- [0041] 본 발명의 기술적 사상에 의하면, 사용자는 보안정보를 어느 하나의 독립적인 보안장치를 통해 획득할 수 있는 것이 아니라, 페어(pair, 쌍)를 이루도록 정해져 있는 디지털 시스템 및 페어 시스템을 모두 가지고 있는 경우에만 사용자가 보안정보를 획득할 수 있으므로 어느 하나의 시스템을 분실 또는 도난당하는 경우에도 타인이 보안정보를 획득할 수 없는 효과가 있다.
- [0042] 또한, 본 발명의 기술적 사상에 의하면, 디지털 시스템 및 페어 시스템이 일정 거리 이상 떨어지는 경우에는 상기 디지털 시스템 및/또는 상기 페어 시스템이 소정의 알람신호를 출력함으로써 상기 디지털 시스템 또는 상기 페어 시스템의 분실이나 도난을 예방할 수 있어서 보안성은 더욱 증가되는 효과가 있다.
- [0043] 또한, 본 발명의 실시 예에 따라서는 페어 시스템이 보안정보를 저장하고 있거나 생성하고 디지털 시스템은 단순히 이를 받아 인증에 이용하고 바로바로 삭제할 수 있는 구조를 가질 수 있으므로 해서, 디지털 시스템이 보안정보를 저장하고 있거나 생성함으로써 발생할 수 있는 디지털 시스템을 통한 상기 보안정보의 적어도 일부의 유출 또는 노출의 위험성을 줄일 수 있다. 따라서, 보안정보의 획득에 관여한 시스템(또는 장치)의 개수가 늘어남에 따라 발생할 수 있는 보안정보의 유출의 위험도 동시에 관리될 수 있는 효과가 있다.
- [0044] 또한, 페어 시스템 또는 디지털 시스템이 보안정보(예컨대, 보안코드 즉, 보안카드 번호)를 저장하고 있는 경우, 사용자는 상기 보안정보를 눈으로 확인한 후 요청된 보안정보를 입력하는 것이 아니라 상기 디지털 시스템을 통해 획득할 수 있으므로, 입력할 보안정보 즉, 요청되는 보안코드의 확인에 걸리는 시간이 줄어들고 오확인이 줄어들 뿐만 아니라, 특정인에게 할당될 보안코드의 개수가 종래의 보안카드에 존재하는 보안코드의 개수보다 현저히 많아져도 상기 보안정보를 이용한 인증에 걸리는 시간이 늘어나지 않고 오히려 줄어들 수 있어서, 보안성이 높아짐과 동시에 인증에 소요되는 시간은 오히려 줄어드는 효과가 있다. 또한 실시 예에 따라서는 보안정보를 사람이 입력하는 것이 아니라 디지털 시스템이 입력하도록 할 수 있으므로 고객의 편의성을 더욱 증대하는 효과가 있다.
- [0045] 또한, 페어 시스템이 보안정보를 저장하고 있거나 생성하더라도 디지털 시스템을 통해 상기 보안정보의 적어도 일부를 획득할 수 있으므로, 상기 페어 시스템이 지갑에 휴대되고 있는 경우 상기 페어시스템을 지갑에서 꺼내지 않아도 되어 사용자의 편의성을 높일 뿐만 아니라 분실 또는 도난의 위험을 줄일 수 있는 효과가 있다.
- [0046] 또한, 서비스를 제공하는 서비스 시스템(예컨대, 금융기관, 웹 사이트 등)들 별로 사용되는 보안장치가 상이하여, 특정 개인이 이용하는 보안장치(예컨대, 보안카드 또는 OTP 생성 장치 등)가 복수 개일 수 있는데 이러한 복수 개의 보안장치를 하나로 통합하여 사용할 수 있도록 함으로써 사용자의 편의성을 높이는 효과가 있다.
- [0047] 또한, OTP 생성에 페어 시스템에 대응되는 키만 사용되는 것이 아니라, 디지털 시스템에 대응되는 키도 사용될 수 있으므로, 혹시 발생할지도 모르는 어느 하나의 시스템의 OTP 생성키가 유출되더라도 보안성이 유지되는 효과가 있다.
- [0048] 또한, 본 발명의 기술적 사상에 의하면, 디지털 시스템과 페어 시스템이 일정 거리 이상 떨어지는 경우에 사용자에게 알람신호를 주기 위하여 상기 디지털 시스템과 페어 시스템은 평상시 페어링 상태를 유지하게 함으로써, 상기 디지털 시스템 또는 상기 페어 시스템의 분실 또는 도난을 예방함과 동시에 상기 디지털 시스템과 페어 시스템이 페어링을 통해 보안정보를 획득함에서 있어서 필요한 페어 형성 절차를 생략 또는 간소화하여(이미 특정 시스템간에 페어링이 이루어져 있는 상태이므로) 보다 효율적으로 보안정보를 획득할 수 있는 효과가 있다.
- [0049] 또한, NFC 태깅을 통해 보안 디지털 시스템과 페어 시스템이 통신을 수행하는 경우, 간편하게 보안정보를 획득할 수 있는 효과가 있다. 또한, 복수의 태깅을 수행하여야 보안정보를 획득할 수 있도록 함으로써, 사용자가 원하지 않는 태깅이 수행되었을 때 불필요하게 보안정보가 획득되거나, 또는 부정한 사용자가 사용자가 인식하지 못하는 중에 태깅을 통해 보안정보를 습득할 위험을 줄일 수 있는 효과가 있다.
- [0050] 또한, NFC 태깅 등 무선통신을 통해 보안카드 또는 모바일 OTP(M-OTP) 생성장치가 탑재되어 있는 보안 디지털 시스템과 페어 시스템이 통신을 수행하는 경우에만, 보안 디지털 시스템에 탑재되어 있는 보안카드가 출력되거나 OTP가 생성되도록 함으로써, 모바일 보안카드 또는 OTP 생성장치의 최대 약점인 보안상의 문제점을 해결할 수 있는 효과가 있다.
- [0051] 또한, 보안 디지털 시스템과 페어 시스템이 NFC 통신을 한 경우, 인증 시스템에서 OTP 또는 인증정보를 생성할 수도 있으며, 이러한 경우 거래에 참여하는 매체(예컨대, 상기 보안 디지털 시스템 또는 상기 페어 시스템이 결제수단인 경우의 상기 페어 시스템)와는 독립적인 매체에서 인증에 이용되는 정보를 생성할 수 있어서 보안성이 향상되는 효과가 있다.

[0052] 또한, 보안 디지털 시스템과 페어 시스템이 적어도 한 번 태깅하는 경우, 인증 시스템이 인증 요청자에 상응하는 OTP를 생성할 수 있도록 함으로써, 사용자가 소지하고 있어야 하던 OTP 토큰을 인증 시스템이 대체하는 역할을 수행할 수 있으므로 OTP 토큰의 유출 또는 분실에 의한 위협에 안전하고, 사용자의 편의성 및 보안성이 현저히 높아질 수 있는 효과가 있다.

[0053] 또한, 인증 시스템에 미리 등록되어 있는 보안 디지털 시스템의 식별정보와 페어 시스템의 식별정보 중 적어도 하나에 해당하는 기기가 페어링이 되거나 태깅이 되어야만 상기 인증 시스템이 본인인증을 위한 정보를 수신할 수 있도록 함으로써 사용자의 보안성을 한층 높일 수 있는 효과가 있다.

[0054] 또한, 인증 시스템에 의해 생성된 OTP 또는 인증정보를 정당 사용자에게 상응하는 지정 단말기로 전송하고, 전송된 정보를 인증시스템이 재수신하여 재수신된OTP 또는 인증정보가 상기 OTP에 상응하는 인증용 OTP 또는 전송한 인증정보와 일치하는지 여부에 따라 본인인증을 하도록 함으로써 사용자가 상기 지정 단말기를 점유하고 있는지 여부를 확인하고, 사용자 인증의 보안성을 더욱 높일 수 있는 효과가 있다.

도면의 간단한 설명

[0055] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 간단한 설명이 제공된다.

도 1은 본 발명의 실시 예에 따른 보안 디지털 시스템을 구현하기 위한 개략적인 시스템 구성을 나타내는 도면이다.

도 2는 본 발명의 실시 예에 따른 보안 디지털 시스템의 개략적인 구성을 나타내는 도면이다.

도 3은 본 발명의 일 실시 예에 따라 보안 디지털 시스템 및 페어 시스템이 페어를 형성하는 방식의 일 예를 나타내는 도면이다.

도 4는 본 발명의 다른 실시 예에 따라 보안 디지털 시스템 및 페어 시스템이 페어를 형성하는 방식의 일 예를 나타내는 도면이다.

도 5a는 본 발명의 일 실시 예에 따라 보안 디지털 시스템이 요청 보안코드를 획득하는 과정을 설명하기 위한 도면이다.

도 5b는 본 발명의 다른 실시 예에 따라 보안 디지털 시스템이 요청 보안코드를 획득하는 과정을 설명하기 위한 도면이다.

도 5c는 본 발명의 또 다른 실시 예에 따라 보안 디지털 시스템이 요청 보안코드를 획득하는 과정을 설명하기 위한 도면이다.

도 6은 본 발명의 실시 예에 따른 보안 디지털 시스템에 의해 OTP가 획득되는 방법을 설명하기 위한 도면이다.

도 7은 본 발명의 실시 예에 따라 보안 디지털 시스템이 보안절차를 수행하는 과정을 설명하기 위한 개략적인 플로우 차트이다.

도 8은 본 발명의 실시 예에 따른 페어 시스템의 개략적인 구성을 나타내는 도면이다.

도 9는 본 발명의 실시 예에 따라 보안 디지털 시스템 또는 페어 시스템이 알람신호를 출력하는 개념을 설명하기 위한 도면이다.

도 10은 본 발명의 일 실시 예에 따른 보안 디지털 시스템이 페어 시스템과 태깅을 수행하여 보안정보를 획득하는 경우의 일 예를 나타내는 도면이다.

도 11 내지 도 12는 본 발명의 일 실시 예에 따른 보안 디지털 시스템이 복수의 태깅을 수행하여 보안정보를 획득하는 경우의 일 예를 나타내는 도면이다.

도 13은 본 발명의 다른 실시 예에 따른 OTP 생성 방법을 설명하기 위한 도면이다.

도 14는 본 발명의 실시 예에 따른 인증 시스템의 개략적인 구성을 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0056] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시예에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본

발명의 바람직한 실시 예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용을 참조하여야만 한다.

- [0057] 또한, 본 명세서에 있어서는 어느 하나의 구성요소가 다른 구성요소로 데이터를 '전송'하는 경우에는 상기 구성요소는 상기 다른 구성요소로 직접 상기 데이터를 전송할 수도 있고, 적어도 하나의 또 다른 구성요소를 통하여 상기 데이터를 상기 다른 구성요소로 전송할 수도 있는 것을 의미한다.
- [0058] 반대로 어느 하나의 구성요소가 다른 구성요소로 데이터를 '직접 전송'하는 경우에는 상기 구성요소에서 다른 구성요소를 통하지 않고 상기 다른 구성요소로 상기 데이터가 전송되는 것을 의미한다.
- [0059] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시 예를 설명함으로써, 본 발명을 상세히 설명한다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다.
- [0060] 도 1은 본 발명의 실시 예에 따른 보안 디지털 시스템을 구현하기 위한 개략적인 시스템 구성을 나타내는 도면이다.
- [0061] 도 1을 참조하면, 본 발명의 실시 예에 따른 보안 디지털 시스템을 구현하기 위해서는 보안 디지털 시스템(100) 및 페어 시스템(200)이 구비될 수 있다.
- [0062] 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)과 소정의 통신 프로토콜을 이용해 통신이 가능하며, 본 명세서에서 정의되는 기능들을 수행할 수 있는 데이터 프로세싱 능력이 있는 모든 형태의 데이터 프로세싱 장치를 포함하는 의미로 정의될 수 있다.
- [0063] 예컨대, 상기 디지털 시스템(100)은 도 1에서는 모바일 폰의 형태로만 도시하였지만, 컴퓨터, 노트북, 태블릿, IPTV, 스마트 TV, 셋탑박스, 리모콘, 홈오트메이션 기기 등 그 구현 예는 다양할 수 있다.
- [0064] 상기 보안 디지털 시스템(100)은 유선 또는 무선 네트워크에 접속 가능한 시스템일 수 있다. 그리고, 소정의 서비스 시스템(미도시)에 접속할 수 있다. 그러면, 상기 서비스 시스템은 직접 또는 소정의 인증 시스템(300)을 통해 상기 보안 디지털 시스템(100)으로 인증을 위한 보안정보를 요청할 수 있다. 상기 보안 디지털 시스템(100)과 상기 서비스 시스템은 상기 보안 디지털 시스템(100)에 설치된 웹 클라이언트(예컨대, 브라우저 등)를 통해 연결되거나, 상기 보안 디지털 시스템(100)에 설치된 소정의 애플리케이션을 실행하면 상기 애플리케이션을 통해 연결될 수도 있다. 기타 다양한 방식으로 상기 보안 디지털 시스템(100)과 상기 서비스 시스템은 연결될 수 있음을 본 발명의 기술분야에서 평균적 지식을 가진 자들에 의해 용이하게 추론될 수 있으며, 상기 서비스 시스템 역시 보안정보를 요청하는 시스템이므로 본 발명에서 정의하는 인증 시스템(300)일 수 있다.
- [0065] 또한 상기 보안정보는 예시적으로 보안코드(즉, 보안카드에 기록된 보안카드 번호들) 또는 OTP(One Time Password)일 수 있지만 이에 한정되지는 않으며, 사용자를 인증할 수 있는 어떠한 정보도 상기 보안정보에 포함될 수 있다. 예컨대, 인증 시스템이 페어 시스템(200) 및/또는 보안 디지털 시스템의 식별정보를 저장하고 있는 경우, 상기의 식별정보 또한 보안정보로 활용될 수 있다. 이하에서는 설명의 편의를 위해 상기 보안정보는 주로 보안코드 또는 OTP인 경우를 일 예로 설명하도록 한다.
- [0066] 본 발명의 실시 예들을 정리하여 설명하면 다음과 같을 수 있다.
- [0067] 1. 보안정보 또는 생성정보의 저장에 대한 실시 예
- [0068] 가. 페어 시스템(200)이 보안정보 또는 생성정보를 저장하는 경우
- [0069] 상기 보안정보는 상기 페어 시스템(200)에 저장되어 있거나, 상기 페어 시스템(200)에 저장된 소정의 정보 즉, 생성정보에 의해 생성될 수 있는 정보일 수 있다. 즉, 상기 페어 시스템(200)은 상기 보안정보 자체를 저장하고 있거나, 상기 보안정보를 생성할 수 있는 생성정보를 저장하고 있을 수 있다. 이러한 경우 보안정보의 획득은 상기 보안 디지털 시스템(100)을 통해 또는 상기 페어 시스템(200)을 통해 이루어질 수 있다. 어떠한 경우든 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 페어링이 되어 있는 상태이거나 적어도 한 번은 페어링이 되어야 상기 보안정보는 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)을 통해 사용자에게 제공되거나 인증 시스템(300)에게 제공될 수 있다. 이때 적어도 한 번은 페어링이 되어야 한다고 함은, 예컨대 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 태깅(tagging)을 통한 NFC 통신을 수행하는 경우를 의미할 수 있다. 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 NFC 통신을 하는 경우에는, 태깅이 수행되

는 비교적 짧은 시간 동안에 페어링이 이루어질 수 있다.

- [0070] 상기 페어 시스템(200)이 상기 보안정보 자체를 저장하고 있는 경우는 상기 보안정보가 보안카드에 사용되는 보안코드와 같이 미리 정의되어서 변경되지 않는 정보일 수 있다. 한편, 상기 페어 시스템(200)이 상기 보안정보를 생성할 수 있는 정보를 저장한다고 함은, 상기 보안정보의 생성이 실시간 또는 사용자의 요청 등과 같이 소정의 이벤트가 발생했을 때 수행되는 경우일 수 있다. 이러한 일 예는 OTP를 통한 인증일 수 있다. 이때는 상기 페어 시스템(200)은 상기 보안정보 즉, OTP를 생성하기 위한 정보(예컨대, OTP 생성프로그램(또는 로직), OTP 생성키 등)가 상기 페어 시스템(200)에 저장되어 있을 수 있다. 구현 예에 따라, 상기 페어 시스템(200)에 저장된 정보는 상기 OTP를 생성하기 위해 필요한 정보 모두일 수도 있고, 그 중 일부만일 수도 있다. 상기 페어 시스템(200)에 저장되어 있지 않으면서 상기 OTP의 생성에 사용되는 정보는 상기 보안 디지털 시스템(100) 또는 상기 인증 시스템(300)에 저장되어 있거나 실시간으로 획득될 수 있는 정보(예컨대, 시간정보 등)일 수도 있다.
- [0071] 그러면, 사용자는 상기 보안 디지털 시스템(100)을 통해 상기 보안정보(예컨대, 보안코드 또는 OTP 등)를 획득할 수 있다. 구현 예에 따라서는 상기 페어 시스템(200)을 통해 상기 보안정보를 획득할 수도 있다. 어떠한 경우든 사용자는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 후술할 바와 같이 페어링이 된 상태에서 또는 적어도 한 번 페어링을 수행하여야 상기 보안정보를 획득할 수 있다.
- [0072] 사용자가 상기 보안정보를 획득한다고 함은, 사용자가 인식할 수 있는 상태로 상기 보안정보가 사용자에게 제공되는 것을 의미하거나, 사용자가 비록 상기 보안정보를 인식하지는 못하지만 보안정보가 자동으로 보안정보가 입력되어야 할 입력 UI에 입력되거나 또는 상기 보안정보를 요청한 소정의 인증시스템(300)에 상기 보안정보가 전송되는 경우를 의미할 수 있다.
- [0073] 상기 인증 시스템은 본 발명의 기술적 사상에 따라 획득되는 보안정보를 요청하는 시스템을 의미할 수 있다. 상기 인증 시스템은 본 발명의 기술적 사상에 의해 획득되는 보안정보의 인증을 직접 수행하는 인증서버뿐만 아니라, 상기 인증서버와 연결되어 상기 보안정보가 상기 인증서버로 전송되는 경로상의 적어도 하나의 시스템을 포함하는 의미로 정의될 수 있다. 예컨대, 사용자가 온라인 결제를 수행하는 경우, 소정의 결제 시스템이 보안정보를 요청하고 사용자가 보안정보를 입력하면 입력된 보안정보는 상기 결제 시스템을 통해 소정의 인증 서버로 전송될 수 있는데, 이러한 경우 상기 결제 시스템 및/또는 상기 인증서버가 본 발명의 인증 시스템일 수 있다.
- [0074] 한편, 실시 예에 따라서는 상기 인증 시스템은 상기 보안 디지털 시스템(100) 또는 상기 보안 디지털 시스템(100)의 사용자가 이용하는 별도의 데이터 프로세싱 장치(예컨대, 컴퓨터 등, 400)와 네트워크를 통해 연결될 수 있다.
- [0075] 사용자는 상기 보안 디지털 시스템(100)을 통해 소정의 서비스 시스템에 접속하고, 상기 서비스 시스템은 특정 서비스(예컨대, 로그인, 금융거래 등)를 위해 상기 보안 디지털 시스템(100)으로 보안정보를 요청할 수 있다. 그러면, 사용자는 본 발명의 기술적 사상에 따라 상기 보안정보를 상기 보안 디지털 시스템(100)을 통해 확인하거나 상기 페어 시스템(200)을 통해 확인할 수 있다. 그리고 확인한 보안정보를 직접 상기 서비스 시스템에 입력할 수 있다. 구현 예에 따라서는, 상기 보안정보가 상기 보안 디지털 시스템(100)을 통해 획득되고, 획득된 보안정보가 자동으로 보안정보가 입력되어야 할 입력 UI에 입력되거나 또는 상기 서비스 시스템으로 전송될 수 있다. 그러면, 상기 서비스 시스템은 수신된 보안정보를 직접 인증하거나 인증을 수행할 수 있는 인증서버로 전송할 수 있고, 이를 통해 상기 보안정보는 인증될 수 있다. 이 경우, 상기 서비스 시스템이 인증 시스템(300)일 수 있음은 물론이다.
- [0076] 한편, 다른 실시 예에 의하면, 상기 데이터 프로세싱 장치(400)는 상기 보안 디지털 시스템(100)과는 별도의 독립적인 시스템일 수 있다. 예컨대, 상기 보안 디지털 시스템(100)은 모바일 폰일 수 있고, 상기 데이터 프로세싱 장치(400)는 상기 모바일 폰의 유저가 사용하는 별도의 컴퓨터일 수 있다.
- [0077] 이런 경우, 사용자는 별도의 데이터 프로세싱 장치(400)를 통해 상기 서비스 시스템에 접속할 수 있다. 그러면, 상기 서비스 시스템은 상기 데이터 프로세싱 장치(400)로 보안정보를 요청할 수 있다. 그러면, 사용자는 본 발명의 기술적 사상에 따라 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)을 통해 보안정보를 획득할 수 있고, 획득된 보안정보를 상기 데이터 프로세싱 장치(400)로 입력할 수도 있다. 어떠한 경우든, 사용자는 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200)을 모두 점유하고 있어야 상기 보안정보를 획득할 수 있다.

- [0078] 1) 보안정보가 보안카드인 경우
- [0079] 예컨대, 상기 페어 시스템(200)은 보안코드를 저장하고 있을 수 있다. 그러면, 사용자는 상기 페어 시스템(200)과 페어가 형성된 보안 디지털 시스템(100)을 이용해 상기 보안코드를 획득할 수 있다. 보안 디지털 시스템(100)은 상기 보안코드 전체를 상기 페어 시스템(200)으로부터 수신할 수도 있고, 일부만 수신할 수도 있다. 일부만 수신하는 경우에는 상기 보안 디지털 시스템(100)은 현재 소정의 인증 시스템(300)에 의해 요청되는 요청 보안코드만 수신할 수 있다.
- [0080] 상기 보안코드의 적어도 일부(또는 후술할 바와 같은 OTP 정보의 적어도 일부 또는 OTP)는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 페어링 상태(또는 후술할 바와 같은 알람 페어링 상태)에서 소정의 이벤트가 발생하였을 때 상기 보안 디지털 시스템(100)으로 수신될 수 있다. 상기 소정의 이벤트는 예컨대, 사용자가 상기 보안 디지털 시스템(100)에 보안코드 요청(또는 요청 보안코드 요청)을 입력하는 경우 또는 상기 페어링 상태에서 미리 정의된 행위를 수행하는 경우(예컨대, 알람 페어링 상태에서 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 태깅(tagging)되는 이벤트) 등과 같이 사용자 또는 상기 보안 디지털 시스템(100)이 보안정보를 요청한다고 판단될만한 이벤트일 수 있다. 상기 이벤트가 발생하는지 여부는 상기 제어모듈(110)에 의해 판단될 수 있다.
- [0081] 구현 예에 따라서는, 단순히 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 태깅이 되면, 상기 보안 디지털 시스템(100)은 상기 보안코드의 적어도 일부를 수신할 수 있다. 즉, 이때에는 태깅이 수행되는 동안이 페어링 상태이며, 태깅이라는 행위 자체가 상기 보안코드를 요청하는 이벤트일 수도 있다.
- [0082] 그러면, 사용자는 상기 보안코드 전부 또는 일부를 상기 보안 디지털 시스템(100)에 구비된 디스플레이 장치를 통해 확인하고, 직접 상기 보안 디지털 시스템(100)에서 디스플레이 되고 있는 소정의 입력 UI에 입력할 수도 있다. 구현 예에 따라서는 상기 인증 시스템(300)과 연결된 별도의 데이터 프로세싱 장치(400)가 존재할 수 있다.
- [0083] 구현 예에 따라, 상기 입력 UI는 상기 데이터 프로세싱 장치(400)에 로딩 되어 있을 수도 있다. 즉, 사용자는 상기 데이터 프로세싱 장치(400)를 이용하여 소정의 서비스를 이용하기 위해 서비스 시스템(미도시)에 접속할 수 있고, 상기 서비스 시스템은 소정의 보안정보를 요청할 수 있다. 상기 보안정보의 요청은 상기 서비스 시스템이 상기 데이터 프로세싱 장치(400)로 수행할 수 있다. 그러면, 사용자는 상기 데이터 프로세싱 장치(400)를 이용하다가 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)을 이용해 상기 보안정보를 획득할 수도 있다. 구현 예에 따라서는 상기 보안정보의 요청은 상기 인증 시스템(300)에 의해 수행될 수 있다. 또한, 상기 서비스 시스템과 상기 인증 시스템(300)은 동일한 시스템 또는 서로 연결된 시스템일 수도 있다.
- [0084] 다른 실시 예에 의하면, 수신된 상기 보안코드 중 요청 보안코드가 자동으로 상기 입력 UI에 입력될 수도 있다. 물론, 이러한 경우는 상기 보안 디지털 시스템(100)이 상기 입력 UI를 로딩하는 경우일 수 있다. 이러한 경우에는 입력된 요청 보안코드는 사용자가 인식하지 못하는 형태(예컨대, "***"등)로 표시될 수도 있다. 그러면, 사용자 소정의 UI(예컨대, '확인' 버튼 등)를 선택함으로써 상기 요청 보안코드는 인증 시스템(300)으로 전송되며, 인증 시스템(300)은 수신된 요청 보안코드와 미리 저장된 정보를 비교하여 인증을 수행할 수 있다.
- [0085] 또 다른 실시 예에 의하면, 상기 보안 디지털 시스템(100)은 요청 보안코드를 상기 페어 시스템(200)으로부터 수신한 후, 자동으로 수신된 상기 요청 보안코드를 상기 인증 시스템(300)으로 전송할 수도 있다.
- [0086] 또 다른 실시 예에 의하면, 사용자가 요청 보안코드를 식별할 수 있는 식별정보(예컨대, 도 5c의 부재번호 12)를 입력하면 상기 보안 디지털 시스템(100)은 요청 보안코드만을 상기 페어 시스템(200)으로부터 수신하거나, 또는 상기 보안 디지털 시스템(100)이 보안코드를 전부 수신하고 해당 보안코드만을 디스플레이하거나 요청 보안코드를 자동으로 상기 입력 UI에 입력할 수도 있다.
- [0087] 한편, 사용자는 상기 페어 시스템(200)을 통해 상기 요청 보안코드를 획득할 수도 있다. 이러한 경우, 상기 페어 시스템(200)은 디스플레이 장치를 구비할 수 있다. 또한, 이러한 경우에도 상기 페어 시스템(200)과 상기 보안 디지털 시스템(100)은 페어링이 유지된 상태이거나 또는 적어도 한 번 페어링(즉, 태깅 등이 되어야)을 수행하여야, 상기 페어 시스템(200)을 통해 상기 요청 보안코드를 획득할 수 있다. 그리고, 상기 페어 시스템(200)은 사용자로부터 보안코드를 획득하기 위한 요청이 있는 경우에만, 상기 보안코드의 전부 또는 일부를 상기 페어 시스템(200)에 구비된 디스플레이 장치에 디스플레이할 수 있다. 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 NFC 통신을 수행하는 경우에는, 태깅 행위 자체가 상기 보안코드를 획득하기 위한 요청일 수도 있다.

- [0088] 사용자가 상기 보안 디지털 시스템(100)을 통해 상기 보안코드의 적어도 일부를 획득하거나 또는 상기 페어 시스템(200)을 통해 상기 보안코드의 적어도 일부를 획득하거나, 어떠한 경우든 페어링이 유지된 상태에서 또는 적어도 한 번 페어링을 수행하여야 상기 보안코드의 적어도 일부를 획득할 수 있다.
- [0089] 2) 상기 보안정보가 OTP인 경우
- [0090] 상기 페어 시스템(200)은 OTP 정보를 저장할 수 있다. 상기 OTP 정보는 OTP를 생성하는 주체가 OTP를 생성하기 위해 구비해야 할 정보를 의미할 수 있다. 본 발명의 실시 예들에 의하면, OTP를 생성하는 주체는 상기 페어 시스템(200)일 수도 있고, 상기 보안 디지털 시스템(100)일 수도 있다. 구현 예에 따라서는 상기 인증 시스템(300)일 수도 있다.
- [0091] 상기 OTP 정보는 OTP 생성키를 포함할 수 있다. 또한, 상기 OTP 정보는 OTP 생성 프로그램 정보를 포함할 수 있다. 구현 예에 따라서는, 상기 페어 시스템(200)의 식별정보가 OTP 정보에 포함될 수도 있다.
- [0092] 상기 페어 시스템(200)의 식별정보는 OTP를 생성하기 위한 키 값으로 이용될 수 있다. 즉, OTP 정보에 포함될 수 있다. 구현 예에 따라서는, 상기 페어 시스템(200)의 식별정보는 단순히 인증을 요청하는 자(또는 인증을 요청하는 자 별로 할당된 OTP 생성모듈)을 구분하기 위한 정보로 사용될 수도 있다. 이러한 경우 상기 페어 시스템(200)의 식별정보는 OTP 정보에는 포함되지 않을 수도 있다. 따라서 상기 보안 디지털 시스템(100) 또는 상기 인증 시스템(300)에서 OTP가 생성되는 경우, 상기 페어 시스템(200)의 식별정보는 OTP를 생성하는 키 값으로 이용될 수도 있고, 인증 요청자를 특정하기 위한 정보로 이용될 수도 있다.
- [0093] OTP를 생성하기 위해서는 적어도 상기 OTP 생성 프로그램 정보와 상기 OTP 생성키가 필요할 수 있다. 물론, OTP 생성 알고리즘에 따라 시간정보 등이 키로 더 이용될 수도 있다. 상기 OTP 생성키는 상기 페어 시스템(200)과 상기 인증 시스템(300)이 공유할 수 있다.
- [0094] 이러한 경우, 사용자는 상기 보안 디지털 시스템(100)을 통해 OTP를 획득할 수 있다. 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)으로부터 OTP 정보의 적어도 일부를 획득하고, 획득된 OTP 정보의 적어도 일부를 이용하여 OTP를 생성할 수 있다. 또는 상기 페어 시스템(200)에 의해 생성된 OTP를 상기 보안 디지털 시스템(100)이 수신할 수도 있다. 또는 상기 인증 시스템(300)에 의해 생성된 OTP가 상기 보안 디지털 시스템(100)(또는 미리 지정된 인증 요청자의 지정 단말기)으로 전송될 수도 있다.
- [0095] 어떠한 경우든, 상기 OTP 정보의 적어도 일부 또는 상기 OTP의 수신은 상기 페어 시스템(200)과 상기 보안 디지털 시스템(100)이 페어링이 되어 있는 상태이거나, 페어링(예컨대, 태깅)이 적어도 한 번 수행되어야 수행될 수 있다. 물론, 상기 페어 시스템(200)의 식별정보 역시 상기 페어 시스템(200)과 상기 보안 디지털 시스템(100)이 페어링이 되어 있는 상태이거나, 페어링(예컨대, 태깅)이 적어도 한 번 수행되어야 상기 보안 디지털 시스템(100)으로 수신될 수 있다.
- [0096] 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)으로부터 OTP 정보 또는 페어 시스템(200)의 식별정보를 수신할 수 있다.
- [0097] 이처럼 보안 디지털 시스템(100)으로 상기 페어 시스템(200)의 OTP 정보 또는 페어 시스템(200)의 식별정보가 수신되면, OTP의 생성은 상기 보안 디지털 시스템(100)에 의해 수행될 수도 있고, 상기 인증 시스템(300)에 의해 수행될 수도 있다.
- [0098] 상기 보안 디지털 시스템(100)이 OTP를 생성하는 경우, 상기 OTP 생성프로그램은 상기 페어 시스템(200)으로부터 수신할 수도 있고, 상기 인증 시스템(300)으로부터 수신할 수도 있다. 물론, 상기 보안 디지털 시스템(100)에 OTP 생성프로그램이 미리 저장되어 있을 수도 있다. 그러면, 상기 보안 디지털 시스템(100)은 수신된 상기 OTP 생성키와 상기 OTP 생성프로그램을 이용하여 OTP를 생성할 수 있다.
- [0099] 한편, 상기 보안 디지털 시스템(100)이 OTP를 생성하기 위해 추가 정보가 생성키로 더 이용될 수도 있다. 예컨대, 널리 알려진 바와 같이 시간정보가 추가키로 이용될 수 있다. 특히 본 발명의 일 실시 예에 의하면, 상기 보안 디지털 시스템(100)은 상기 OTP를 생성하기 위해 자신과 인증 시스템(300)이 공유하고 있는 비밀키를 더 이용할 수도 있다. 즉, 이러한 경우, 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)으로부터 수신한 비밀키인 상기 OTP 생성키(이하, 제1OTP 생성키) 및 상기 보안 디지털 시스템(100)과 상기 인증 시스템(300)이 공유하고 있는 비밀키인 제2OTP 생성키, 두 개의 비밀키를 이용하여 OTP를 생성할 수도 있다. 이러한 경우, 어느 하나의 비밀키가 유출되고 OTP 생성프로그램이 알려져 있다고 하더라도 OTP를 생성할 수 없게 되므로 보안성

은 배가된다.

- [0100] 물론, 보안 디지털 시스템(100)에 의해 생성된 OTP의 정당성을 인증하기 위한 인증용 OTP를 생성하는 상기 인증 시스템(300)은 상기 제1OTP 생성키, 상기 제2OTP 생성키, 및 상기 OTP 생성프로그램 정보를 미리 알고 있을 수 있다. 그러면, 생성된 OTP는 상기 보안 디지털 시스템(100)에 구비된 디스플레이 장치를 통해 디스플레이되고, 사용자는 직접 상기 보안 디지털 시스템(100)에서 디스플레이되고 있는 소정의 OTP 입력 UI에 입력할 수도 있다. 공지된 바와 같이 OTP 인증 센터(이하, OTP 인증 시스템)에서 클라이언트(즉, 보안 디지털 시스템(100))에서 생성된 OTP를 인증하기 위한 인증용 OTP를 생성하는 경우, 상기 인증 시스템(300)은 상기 OTP 인증 시스템을 포함하는 의미로 정의될 수 있다. 즉, 클라이언트에서 생성된 OTP를 인증하기 위해 상기 클라이언트에 대응되는 인증용 OTP를 생성하는 시스템 즉, 상기 OTP 인증 시스템(300-1)은 상기 인증 시스템(300)에 설치될 수도 있고, 필요에 따라서는 상기 인증 시스템(300)과 별도의 시스템으로 구현되어 상기 인증 시스템(300)과 유기적으로 결합하여 OTP 인증을 수행할 수도 있다. 즉, 상기 OTP 인증 시스템(300-1)은 필요에 따라 상기 인증 시스템(300) 내부의 한 구성으로 구현될 수도 있고, 독립적으로 구현될 수도 있으므로, 본 명세서에서는 상기 OTP 인증 시스템(300-1) 및 상기 인증 시스템(300)을 모두 합쳐 인증 시스템(300)으로 정의하기로 한다. 따라서, 상기 인증 시스템(300)은 OTP 인증 시스템(300-1)을 포함하며, 상기 인증 시스템(300)은 복수의 물리적 장치가 네트워크를 통해 유기적으로 결합되어 구현될 수도 있다.
- [0101] 상기 보안 디지털 시스템(100)에 의해 생성된 상기 OTP는 자동으로 상기 OTP 입력 UI에 입력될 수도 있다. 이러한 경우에는 입력된 OTP는 사용자가 인식하지 못하는 형태(예컨대, "***")로 표시될 수도 있다. 그러면, 사용자 소정의 UI(예컨대, '확인' 또는 '전송' 버튼 등)를 선택함으로써 상기 OTP는 인증 시스템(300)으로 전송되며, 인증 시스템(300)은 수신된 OTP와 자신이 생성한 OTP를 비교함으로써 인증을 수행할 수 있다.
- [0102] 또 다른 실시 예에 의하면, 상기 보안 디지털 시스템(100)은 OTP를 생성한 후 자동으로 상기 인증 시스템(300)으로 생성된 OTP를 전송할 수도 있다. OTP가 자동으로 입력되거나 전송되는 실시 예들은 상기에서의 보안카드의 실시 예와 유사하게 적용될 수 있음은 물론이다.
- [0103] 한편, 상기 OTP의 생성은 상기 페어 시스템(200)에 의해 수행될 수도 있다. 물론, 이러한 경우에도 상기 페어 시스템(200)은 상기 보안 디지털 시스템(100)과 페어링이 유지되고 있는 상태이거나 적어도 한 번 페어링이 수행된 상태인 경우에만 상기 OTP를 생성할 수 있도록 구현될 수 있다. 이를 위해, 상기 페어 시스템(200)은 전원을 구비하여야 할 수도 있다. 또한, 사용자로부터 OTP 생성 요청을 입력받기 위한 소정의 UI를 구비할 수도 있다.
- [0104] 상기 페어 시스템(200)은 자신이 저장하고 있는 제1OTP 생성키 및 OTP 생성프로그램을 이용하여 상기 OTP를 생성할 수 있다. 구현 예에 따라서는, 상기 보안 디지털 시스템(100)으로부터 제2OTP 생성키를 수신하고, 수신된 상기 제2OTP 생성키를 더 이용하여 OTP를 생성할 수도 있다.
- [0105] 상기 페어 시스템(200)에 의해 생성된 OTP는 사용자에게 의해 확인될 수 있으며, 이를 위해 상기 페어 시스템(200)은 소정의 디스플레이 장치를 구비할 수 있다. 디스플레이된 OTP를 확인하고, 사용자는 상기 보안 디지털 시스템(100) 또는 데이터 프로세싱 장치(400)에 로딩되어 있는 소정의 OTP 입력 UI에 상기 OTP를 입력할 수 있다.
- [0106] 또는, 상기 페어 시스템(200)에 의해 생성된 상기 OTP는 다시 상기 보안 디지털 시스템(100)으로 전송될 수 있다. 전송된 상기 OTP는 자동으로 OTP 입력 UI에 입력되거나, 자동으로 상기 보안 디지털 시스템(100)을 통해 상기 인증 시스템(300)으로 전송될 수 있다.
- [0107] 한편, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 NFC 통신을 수행하도록 구현되는 경우, 사용자는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)을 한 번만 태깅하면 필요한 보안정보를 상기 보안 디지털 시스템(100)을 통해 또는 상기 페어 시스템(200)을 통해 획득할 수 있다. 또는, 복수 번 태깅을 하여야 상기 보안정보가 사용자에게 획득될 수도 있다.
- [0108] 예컨대, 상기 보안 디지털 시스템(100)이 상기 페어 시스템(200)과 태깅을 하면, 상기 보안 디지털 시스템(100)은 상기 한 번의 태깅을 통해 상기 페어 시스템(200)으로부터 보안코드의 적어도 일부, OTP 정보의 적어도 일부, 또는 OTP를 수신할 수 있다. 상기 페어 시스템(200)으로부터 OTP 정보의 적어도 일부를 수신하는 경우에는, 수신된 정보에 기초하여 상기 보안 디지털 시스템(100)은 OTP를 생성할 수 있다. 상기 페어 시스템(200)으로부터 OTP를 수신하는 경우에는, 상기 페어 시스템(200)은 상기 태깅을 OTP 생성요청 신호로 취급하고 OTP를 생성할 수 있으며, 생성된 OTP를 상기 보안 디지털 시스템(100)으로 전송할 수 있다. 또는, 상기 태깅을 통해 상기

보안 디지털 시스템(100)은 상기 보안코드 중 요청 보안코드를 특정할 수 있는 요청 보안코드 식별정보를 상기 페어 시스템(200)으로 전송하고, 상기 페어 시스템(200)은 요청 보안코드 식별정보를 이용하여 요청 보안코드를 추출한 후, 요청 보안코드를 상기 보안 디지털 시스템(100)으로 전송할 수도 있다. 즉, 한 번의 태깅이 수행되는 동안 상술한 바와 같은 요청 보안코드의 추출 또는 OTP 정보의 생성과 같은 페어 시스템(200)의 프로세스와 상기 프로세스가 수행된 후의 요청 보안코드의 전송 또는 OTP의 전송이 모두 수행될 수도 있다.

[0109] 구현 예에 따라서는, 사용자는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)을 복수 번 태깅하여야 최종적으로 필요한 보안정보를 획득할 수도 있다. 예컨대, 한 번 태깅하는 경우에는 전술한 바와 같이 상기 보안 디지털 시스템(100)으로부터 상기 페어 시스템(200)으로의 요청 보안코드 식별정보의 전송, OTP 생성요청의 전송 등이 수행될 수 있다. 그러면, 상기 페어 시스템(200)은 요청 보안코드를 추출하거나 OTP 정보를 생성할 수 있다. 이후 다시 한번 태깅이 되면 요청 보안코드가 상기 보안 디지털 시스템(100)으로 전송되거나 생성된 OTP가 상기 보안 디지털 시스템(100)으로 전송될 수 있다.

[0110] 즉, 어떠한 경우든 상기 보안 디지털 시스템(100)이 보안정보(예컨대, 보안코드 또는 OTP)를 획득하기 위해 수행되어야 할 프로세스가 복수 회에 걸쳐 나누어 수행될 수 있으며, 상기 복수 회에 걸쳐 나누어 수행될 프로세스는 복수 번의 태깅 각각이 수행될 때마다 수행될 수도 있다.

[0111] 예컨대, 상기 보안 디지털 시스템(100)이 상기 페어 시스템(200)으로부터 보안코드 전부를 수신하도록 구현되는 경우, 수행되어야 할 프로세스는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 서로 페어를 이루는 시스템인지를 인증하는 페어 인증 프로세스 및 인증이 성공한 경우 상기 보안코드가 상기 페어 시스템(200)에서 상기 보안 디지털 시스템(100)으로 전송되는 프로세스는 두 개일 수 있다. 이러한 경우, 상기 두 개의 프로세스는 한 번의 태깅으로 모두 수행될 수도 있고, 한 번씩 태깅이 수행될 때마다 각각의 프로세스가 수행될 수도 있다. 상기 페어 인증 프로세스는 수행될 수도 있고, 수행되지 않을 수도 있다.

[0112] 만약, 상기 보안 디지털 시스템(100)이 보안코드의 일부(예컨대, 요청 보안코드)를 상기 페어 시스템(200)으로부터 수신하는 경우, 수행될 수 있는 프로세스는 페어 인증 프로세스, 요청 보안코드 식별정보의 전송, 요청 보안코드의 추출, 추출된 요청 보안코드의 전송일 수 있다. 이 4개의 프로세스가 모두 한 번의 태깅이 수행되는 동안 수행될 수도 있고, 복수 번의 태깅이 수행될 때마다 적어도 하나의 프로세스가 수행될 수도 있다. 이때 요청 보안코드의 추출 프로세스는 반드시 태깅이 수행되는 동안 수행될 필요는 없으며, 태깅이 수행된 후 상기 페어 시스템(200)에 의해 자체적으로 수행될 수도 있다. 또한, 페어 인증 프로세스는 수행될 수도 있고, 수행되지 않을 수도 있다.

[0113] OTP 정보의 적어도 일부를 상기 보안 디지털 시스템(100)이 상기 페어 시스템(200)으로부터 수신하는 경우, 수행될 수 있는 프로세스는 페어 인증 프로세스, OTP 정보의 적어도 일부의 수신, 및 수신된 정보를 이용한 OTP 생성일 수 있다. 이러한 경우에도 위 3개의 프로세스가 모두 한 번의 태깅이 수행되는 동안 수행될 수도 있다. 또는, 한 번의 태깅을 통해 페어 인증 프로세스 및 OTP 정보의 적어도 일부의 수신까지만 수행되고 OTP 생성은 태깅 후에 상기 보안 디지털 시스템(100)에 의해 수행될 수도 있다. 또한, 페어 인증 프로세스는 선택적으로 수행될 수도 있다. 또는, 상기 3개의 프로세스가, 복수 번의 태깅 각각이 수행되는 동안 또는 태깅 각각이 수행된 후에, 나누어져 수행될 수도 있다.

[0114] OTP 정보를 상기 보안 디지털 시스템(100)이 상기 페어 시스템(200)으로부터 수신하는 경우, 수행될 수 있는 프로세스는 페어 인증 프로세스, OTP 생성요청 전송, OTP 생성, 생성된 OTP의 전송일 수 있다. 이러한 경우에도 한 번의 태깅을 통해 모든 프로세스가 수행될 수도 있고, 복수 번의 태깅을 통해 나누어져 수행될 수도 있다. 그리고 각각의 프로세스는 프로세스의 특성에 따라 태깅이 수행되는 동안 수행될 수도 있고, 태깅이 수행된 후에 수행될 수도 있다.

[0115] 한편, 전술한 바와 같이 태깅을 통해 상기 보안 디지털 시스템(100)이 보안정보를 획득하는 경우, 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)은 페어 인증 절차를 수행할 수도 있다. 즉, 미리 페어를 이루도록 결정된 시스템과 태깅이 되어야만 상술한 바와 같은 보안정보를 획득하기 위한 프로세스 또는 페어 시스템(200)으로부터 수신한 정보에 기초한 보안정보의 획득 프로세스가 수행될 수 있다. 이를 위해 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)의 식별정보를 미리 저장하고 있을 수 있다. 그리고, 태깅이 수행되면 상기 페어 시스템(200)의 식별정보를 획득하여 비교함으로써 페어 인증 절차를 수행할 수 있다. 구현 예에 따라서는 상기 페어 시스템(200)에 상기 보안 디지털 시스템(100)의 식별정보가 저장되어 있을 수도 있다. 이러한 경우에도 유사한 방식으로 페어 인증 절차가 수행될 수 있다. 어떠한 경우든, 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)이 페어가 되는 시스템의 식별정보를 미리 기록하고 있는 경우, 페어 인증 절차가

수행될 수 있다.

- [0116] 나. 보안 디지털 시스템(100)이 보안정보 또는 생성정보를 저장하는 경우
- [0117] 1)보안정보가 보안코드인 경우
- [0118] 이러한 경우, 상기 보안 디지털 시스템(100)은 상기 보안코드에 접근 가능할 수 있다. 하지만, 이때에도 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)과 페어링이 유지된 상태 또는 적어도 한 번 페어링(예컨대, 태깅)이 수행된 상태 또는 후에 상기 보안정보에 접근할 수 있다.
- [0119] 상기 보안 디지털 시스템(100)은 인증 시스템(300)으로부터 사용자에게 할당된 보안코드 중 특정 보안카드 번호, 즉, 요청 보안코드의 요청을 받는다. 이러한 요청 보안코드를 요청하는 수단(예컨대, 웹 페이지, 프레임, 또는 소정의 UI 등)이 상기 보안 디지털 시스템(100)에 로딩될 수 있다. 또는 사용자는 상기 보안 디지털 시스템(100)과는 별도의 데이터 프로세싱 장치(400)를 통해 상기 보안코드를 요청 받을 수도 있다.
- [0120] 상기 보안 디지털 시스템(100)은 저장된 보안코드 전체 또는 요청되는 보안코드만을 상기 보안 디지털 시스템(100)에 구비된 디스플레이 장치에 디스플레이할 수 있다. 그러면, 사용자는 디스플레이된 보안코드 중 요청 보안코드를 확인하여 입력 UI에 입력할 수 있다.
- [0121] 또는, 상기 보안 디지털 시스템(100)이 자동으로 상기 요청 보안코드만을 추출하고, 상기 입력 UI에 자동 입력할 수도 있다. 또는 요청 보안코드만을 추출하여 자동으로 상기 인증 시스템(300)으로 전송할 수도 있다.
- [0122] 상기 보안 디지털 시스템(100)이 요청 보안코드가 무엇인지를 확인하기 위해서, 상기 보안 디지털 시스템(100)은 사용자로부터 요청 보안코드를 식별할 수 있는 식별정보(예컨대, 6 : **51, 14 : 75**에서 순번을 나타내는 6, 14)를 입력받을 수도 있고, 상기 인증시스템(300)으로부터 상기 식별정보를 전송받을 수도 있으며, 상기 보안디지털 시스템에 디스플레이된 정보를 분석하여 자동으로 상기 식별정보를 확인할 수도 있다.
- [0123] 이때 상기 페어 시스템(200)은 단순히 상기 보안 디지털 시스템(100)과 페어를 형성할 수 있는 모든 종류의 시스템으로 구현될 수 있다.
- [0124] 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 페어링 상태인 경우(예컨대, 알람 페어링 상태) 또는 적어도 한번의 태깅이 수행된 후 또는 적어도 한 번의 태깅이 수행되는 동안에만, 상기 보안코드 또는 상기 요청 보안코드가 상기 보안 디지털 시스템(100)에 디스플레이되거나, 자동으로 소정의 UI에 입력되거나, 또는 소정의 인증 시스템(300)으로 전송될 수 있다.
- [0125] 2) 보안정보가 OTP인 경우
- [0126] 상기 보안 디지털 시스템(100)은 상기 생성정보 즉, OTP 정보를 미리 저장하고 있을 수 있다. 상기 OTP 정보에는 OTP 생성 프로그램 정보가 더 포함될 수 있다. 이와 관련하여 상기 보안 디지털 시스템(100)이 스마트 폰인 경우 OTP를 생성하는 종래기술은 M(mobile)-OTP 기술로 널리 공지되어 있다. 본 발명에서의 상기 OTP 정보에는 상기 보안 디지털 시스템(100)에 상응하는 제2OTP 생성키가 더 포함될 수 있다. 상기 OTP 생성 프로그램에 대한 정보는 상기 인증 시스템(300) 또는 기타 소정의 시스템(예컨대, 금융기관 시스템, 행정기관 시스템 등)으로부터 수신할 수도 있다.
- [0127] 또한, 종래의 기술과 비교하여 본 발명에서는 상기 보안 디지털 시스템(100)이 내부에 저장하고 있는 상기 OTP 정보만을 이용하여 OTP를 생성할 수 있는 것이 아니라 상기 페어 시스템(200)과 페어링이 유지된 상태(예컨대, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 비페어링 상태 또는 멀리 떨어지는 경우 알람 정보를 제공하기 위해 평상시 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 페어링 상태를 유지하고 있을 수 있다) 또는 적어도 한 번 페어링(예컨대, 태깅)이 수행되는 동안 또는 후에야 상기 OTP를 생성할 수 있는 기술 구성을 가진다. 이러한 기술구성을 가짐으로 해서 종래의 M-OTP의 기술구성이 가지고 있는 최대의 약점이었던 보안상의 문제점을 해결할 수 있는 효과가 있다.
- [0128] 또한, 상기 보안 디지털 시스템(100)은 상기 OTP를 생성하기 위해 상기 제2OTP 생성키 외에도 시간정보 등을 더 생성키로 이용할 수 있다.
- [0129] 또한, 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)과 합동으로 OTP를 생성할 수도 있다. 예컨대, 상

기 보안 디지털 시스템(100)은 제20TP 생성키를 가지고 상기 페어 시스템(200)에 상응하는 비밀키인 제10TP 생성키를 더 이용하여 상기 OTP를 생성할 수도 있다. 이를 위해 상기 보안 디지털 시스템(100)은 상기 제10TP 생성키를 상기 페어 시스템(200)으로부터 수신할 수 있음은 물론이다.

[0130] 또한, 전술한 바와 같이 한 번의 태깅이 아니라 복수 회의 태깅이 수행되어야 상기 보안 디지털 시스템(100)이 OTP를 생성할 수도 있다. 복수 회의 태깅을 수행하는 경우, 각각의 태깅이 수행될 때 수행되는 프로세스는 구현 예에 따라 달라질 수도 있음은 물론이다. 일 예에 의하면, 상기 복수 회의 태깅 중 특정 태깅이 수행되는 경우에는 보안정보를 획득하기 위해 수행되어야 할 프로세스 중 어떠한 프로세스도 수행되지 않을 수도 있다. 이러한 경우에는 상기 특정 태깅은 단순히 미리 정해진 복수 회수의 태깅을 채우기 위한 태깅의 의미만 가질 수 있다.

[0131] 다. 인증 시스템(300)이 OTP 정보 또는 인증정보를 생성하는 경우

[0132] 실시 예에 따라서는 상기 인증 시스템(300)이 OTP를 생성하는 클라이언트(또는 토큰)의 역할을 수행하고, 상기 인증 시스템(300)에 포함된 OTP 인증 시스템(300-1)이 클라이언트에서 생성된 OTP를 인증하는 서버 역할을 할 수 있다. 상기 OTP 인증 시스템(300-1)은 상기 인증 시스템(300)에 설치될 수도 있고, 상기 인증 시스템(300)의 다른 구성과는 별도의 물리적 장치로 구현될 수 있다. 예컨대, 상기 OTP 인증 시스템(300-1)은 공인된 OTP 인증 센터를 의미할 수도 있고, 상기 인증 시스템(300)의 주체가 별도로 운영하는 시스템일 수도 있다. 어떠한 경우든 본 발명에서 인증 시스템(300)이라 하면 상기 OTP 인증 시스템(300-1)을 포함하는 의미로 정의하기로 한다.

[0133] 본 발명의 기술적 사상에 따른 상기 인증 시스템(300)은 OTP 클라이언트와 OTP 클라이언트에서 생성된 OTP를 인증하는 OTP 서버(예컨대, 상기 OTP 인증 시스템(300-1)) 각각이 생성한 OTP를 서로 비교하여 인증 요청자를 인증하는 방식에 이용되는 상기 OTP뿐만 아니라, 소정의 일회용 인증정보를 생성하여 특정 단말기(예컨대, 인증 요청자의 핸드폰 등)로 전송하고 전송된 일회용 인증정보가 다시 재전송되어 오는지에 따라 인증 요청자를 인증하는 방식에 이용되는 상기 일회용 인증정보를 생성할 수도 있다. 상기 일회용 인증정보 역시 넓게는 OTP에 포함될 수 있지만, 본 명세서에서는 전자의 방식의 OTP와 구분하기 위해 상기 일회용 인증정보를 '인증정보'로 정의하기로 한다.

[0134] 본 발명의 기술적 사상을 구현하기 위해, 상기 보안 디지털 시스템(100)은 페어 시스템(200)과 적어도 한 번 태깅이 수행될 수 있다. 그러면 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)으로부터 OTP 정보 중 적어도 일부 및/또는 상기 페어 시스템(200)의 식별정보를 수신할 수 있다. 상기 페어 시스템(200)의 식별정보가 OTP를 생성하는 키로 사용되는 경우, 상기 페어 시스템(200)의 식별정보는 OTP 정보로써 상기 보안 디지털 시스템(100)에 획득될 수 있다. 상기 보안 디지털 시스템(100)은 OTP를 생성하기 위해 필요한 정보 즉, OTP 정보의 전부 또는 일부를 수신할 수 있다.

[0135] 그러면, 상기 보안 디지털 시스템(100)은 수신된 정보(즉, OTP 정보 중 적어도 일부 및/또는 페어 시스템(200)의 식별정보)를 인증 시스템(300)으로 전송할 수 있다.

[0136] 인증 시스템(300)은 수신된 정보(즉, OTP 정보 중 적어도 일부 및/또는 페어 시스템(200)의 식별정보)에 기초하여 OTP를 생성할 수 있다.

[0137] 상기 인증 시스템(300)이 OTP를 생성하기 위해서는, 인증 요청자별로 미리 결정되어 있는 OTP 정보를 상기 인증 시스템(300)이 모두 획득하여야 한다. 따라서, 상기 보안 디지털 시스템(100)으로부터 OTP 정보 중 일부만 수신한 경우, 나머지 일부는 상기 인증 시스템(300)에 미리 저장되어 있을 수 있다. 상기 인증 시스템(300)은 인증 요청자별로 서로 다른 OTP 정보를 이용해 OTP를 생성할 수 있다. 따라서 인증 요청자별로 OTP를 생성하기 위한 OTP 생성모듈 즉 생성부가 구비될 수 있다. 따라서 OTP를 생성하기 위해서는 인증 요청자를 구분할 필요가 있다. 인증을 요청하는 인증 요청자가 상기 인증 시스템(300) 또는 서비스 시스템에 로그인을 한 경우에는, 로그인 정보에 기초하여 상기 인증 시스템(300)은 인증 요청자를 확인하고, 확인된 인증 요청자에 대응되는 OTP 정보를 이용하여 OTP를 생성할 수 있다. 로그인이 되어 있지 않은 경우에는, 상기 인증 시스템(300)은 보안 디지털 시스템(100)으로부터 수신된 정보에 기초하여 인증 요청자를 확인할 수도 있다. 이를 위해 상기 보안 디지털 시스템(100)은 인증 요청자를 확인할 수 있는 정보를 상기 인증 시스템(300)으로 전송할 수 있다. 인증 요청자를 확인할 수 있는 정보는 예컨대, 페어 시스템(200)의 식별정보일 수도 있고, 상기 보안 디지털 시스템(100)의 식별정보일 수도 있다.

[0138] 인증 시스템(300)에는 미리 보안 디지털 시스템(100)의 식별정보 또는 페어 시스템(200)의 식별정보가 저장되어

있을 수 있다. 본 명세서에서 보안 디지털 시스템(100)의 식별정보라 함은, 상기 보안 디지털 시스템(100) 자체의 단말기를 식별할 수 있는 정보뿐만 아니라, 상기 보안 디지털 시스템(100)의 정당한 사용자를 식별할 수 있는 정보를 포함하는 의미로 정의될 수 있다. 예컨대, 보안 디지털 시스템(100)의 사용자의 식별정보와 단말기의 식별정보가 서로 대응되도록 미리 상기 인증 시스템(300)에 저장되어 있는 경우, 어느 하나의 정보로 나머지 하나의 정보도 인식할 수 있으므로 실질적으로 보안 디지털 시스템(100)의 단말기를 식별할 수 있는 정보는 사용자를 식별할 수 있는 정보로써도 이용될 수 있다.

[0139] 또한, 상기 인증 시스템(300)에는 보안 디지털 시스템(100)의 식별정보 또는 페어 시스템(200)의 식별정보에 대응되는 OTP 정보의 적어도 일부가 미리 저장되어 있을 수 있다. 따라서, 상기 인증 시스템(300)은 인증 요청자에 대응되는 OTP 정보를 이용하여 OTP를 생성할 수 있다.

[0140] 구현 예에 따라서는, 상기 인증 시스템(300)은 상기 보안 디지털 시스템(100)으로부터 페어 시스템(200)의 식별정보만을 수신할 수도 있다. 페어 시스템(200)의 식별정보는 전술한 바와 같이 인증 시스템(300)에 의해 OTP 정보로써 이용될 수도 있고 인증 요청자를 식별할 수 있는 정보로써 이용될 수도 있다. 따라서, 인증 시스템(300)이 페어 시스템(200)의 식별정보를 수신한다고 함은 페어 시스템(200)의 식별정보가 OTP 정보 즉, OTP 생성키로 사용되는 경우를 제외한 경우를 의미할 수 있다. 이처럼 인증 시스템(300)이 상기 페어 시스템(200)의 식별정보를 수신하는 경우에는, 상기 인증 시스템(300)에는 미리 상기 페어 시스템(200)의 식별정보에 대응되는 OTP 정보가 저장되어 있는 경우일 수 있다. 따라서 상기 인증 시스템(300)이 보안 디지털 시스템(100)으로부터 수신된 페어 시스템(200)의 식별정보에 기초하여 OTP를 생성한다고 함은, 보안 디지털 시스템(100)으로부터 페어 시스템(200)의 식별정보가 수신된 경우, 수신된 페어 시스템(200)의 식별정보에 기초하여 인증 요청자에 상응하는 OTP 정보를 특정하고, 특정된 OTP 정보에 기초하여 OTP를 생성함을 의미할 수 있다.

[0141] 구현 예에 따라서는, 상기 인증 시스템(300)은 상기 보안 디지털 시스템(100)으로부터 페어 시스템(200)의 식별정보를 수신할 수 있고, 상기 페어 시스템(200)의 식별정보에 기초하여 OTP와 다른 방식의 인증정보를 생성할 수 있다. 상기 인증정보는 OTP와 같이 OTP 서버 및 클라이언트 각각에서 생성된 OTP를 비교하는데 이용되는 정보가 아닌, 핸드폰 소액 결제 또는 핸드폰 본인인증 등과 같이 소정의 단말기로 전송된 정보가 다시 수신되는지를 판단하는데 이용되는 정보를 의미할 수 있으며 일회용의 정보를 의미할 수 있다. 상기 인증정보는 인증 시스템(300)에 의해 일회용으로 무작위로 생성될 수도 있고, 미리 등록된 많은 정보들 중에서 선택될 수도 있다(예컨대, 종래의 보안카드 방식). 상기의 인증정보는 그 생성방식에 제한을 받지 않으며, 본 발명의 기술적 사상에 따라 다양하게 생성되어질 수 있음은 물론이다.

[0142] 상기 인증 시스템(300)이 인증정보를 생성하는 경우에는, 상기 페어 시스템(200)의 식별정보를 상기 인증정보를 생성하는 키로 이용할 수도 있다. 또는 상기 페어 시스템(200)의 식별정보에 기초하여 미리 인증 시스템(300)에 등록되어 있는 소정의 정보들 중 상기 인증 요청자를 인증하기 위한 정보들이 특정되고 특정된 정보 중에서 상기 인증정보가 생성(즉, 선택)될 수도 있다. 또는, 상기 인증 시스템(300)이 상기 페어 시스템(200)의 식별정보를 수신하면, 수신된 상기 페어 시스템(200)의 식별정보가 미리 상기 인증 시스템(300)에 등록되어 있는지를 판단하고, 등록되어 있는 경우에만 선택적으로 상기 인증정보를 생성할 수도 있다. 그리고 인증정보의 생성 자체에는 상기 페어 시스템(200)의 식별정보가 이용되지 않고, 소정의 알고리즘에 의해 임의로 상기 인증정보가 생성될 수도 있다. 어떠한 경우든 상기 페어 시스템(200)의 식별정보가 상기 인증정보를 생성하는 과정에 이용될 수 있으므로, 상기 인증 시스템(300)은 상기 페어 시스템(200)의 식별정보에 기초하여 상기 인증정보를 생성할 수 있다.

[0143] 결국, 상기 인증 시스템(300)은 보안 디지털 시스템(100)으로부터 수신된 정보(즉, OTP 정보 및/또는 페어 시스템(200)의 식별정보)에 기초하여 OTP 또는 인증정보를 생성할 수 있다.

[0144] 한편, 상기 인증 시스템(300)은 상기 보안 디지털 시스템(100)으로부터 상기 정보(즉, OTP 정보 및/또는 페어 시스템(200)의 식별정보)가 수신되면, 인증 요청자에 상응하는 인증용 OTP를 상기 OTP 인증 시스템(300-1)으로 요청할 수도 있다. 그리고, 상기 OTP 인증 시스템(300-1)에 의해 생성된 인증용 OTP와 상기 인증 시스템(300)이 생성한 OTP가 서로 상응하는지를 판단하여 인증의 성공여부를 판단할 수도 있다.

[0145] 본 발명의 인증 시스템(300)에 의해 생성된 OTP 또는 인증정보를 이용하여 인증 요청자를 인증하는 다양한 실시예를 개시한다.

[0146] 일 실시 예에 의하면, 상기 인증 시스템(300)은 생성된 OTP 인증 시스템(300-1)에 의해 생성된 상기 인증 요청자에 상응하는 OTP와 비교함으로써 인증을 수행할 수도 있다.

- [0147] 다른 실시 예에 의하면, 상기 인증 시스템(300)은 생성된 OTP를 상기 보안 디지털 시스템(100) 또는 상기 인증 요청자의 단말기로 지정된 지정 단말기(상기 보안 디지털 시스템(100)이 지정 단말기일 수 있음은 물론이다.)로 전송하고, 전송에 응답하여 데이터 프로세싱 장치(400) 또는 상기 보안 디지털 시스템(100)으로부터 수신된 OTP와 OTP 인증 시스템(300-1)에 의해 생성된 상기 인증 요청자에 상응하는 OTP와 비교함으로써 인증을 수행할 수도 있다. 이러한 실시 예에 의하면, OTP에 따른 보안성에 인증정보를 이용한 방식의 보안성이 추가로 획득될 수 있다. 즉, OTP 방식에 의해 획득되는 보안성과 더불어, OTP를 전송한 매체(즉, 보안 디지털 시스템(100) 또는 지정 단말기)를 인증 요청자가 소지하고 있는지 여부를 추가로 인증할 수 있는 효과가 있으며, 보안성이 더 높아질 수 있다. 또한, 사용자가 소지하고 있어야 하던 OTP 토큰이나 보안카드 등 보안인증 수단을 인증 시스템(300)이 대체하는 역할을 수행할 수 있으므로 OTP 토큰이나 보안카드 등 보안인증 수단의 유출 또는 분실에 의한 위협에 안전하고, 사용자의 편의성 및 보안성이 현저히 높아지는 효과가 있다.
- [0148] 또 다른 실시 예에 의하면, 상기 인증 시스템(300)은 생성한 인증정보를 상기 보안 디지털 시스템(100) 또는 상기 인증 요청자의 단말기로 지정된 지정 단말기로 전송하고, 전송에 응답하여 데이터 프로세싱 장치(400) 또는 상기 보안 디지털 시스템(100)으로부터 수신할 수 있다. 그리고 수신된 정보와 전송한 정보를 비교함으로써 인증을 수행할 수도 있다.
- [0149] 한편, 상기 인증 시스템(300)이 OTP 또는 인증정보를 전송한 매체와 OTP 또는 인증정보를 수신하는 매체는 서로 다르도록 함으로써 2채널 인증이 수행될 수 있어 보다 높은 보안성이 획득될 수 있다. 예컨대, 인증 시스템(300)이 OTP 또는 인증정보를 보안 디지털 시스템(100)으로 전송한 경우에는, 상기 데이터 프로세싱 장치(400)로부터 OTP 또는 인증정보를 수신하고, 상기 지정 단말기로 OTP 또는 인증정보를 전송한 경우에는 상기 보안 디지털 시스템(100)(상기 보안 디지털 시스템(100)이 상기 지정 단말기가 될 수 있음은 물론이나 본 실시 예에서는 상기 보안 디지털 시스템(100)과 지정 단말기가 상이한 경우를 실시 예로 한다.) 또는 상기 데이터 프로세싱 장치(400)로부터 OTP를 수신하는 경우 보안성은 더 높아질 수 있다.
- [0150] 또한, 인증 시스템(300)이 단순히 인증정보를 전송한 매체로부터 다시 인증정보를 수신하는 경우에도, 종래의 휴대폰 소액결제 등에 이용되는 일회용 인증정보를 이용한 인증에 비해 페어 시스템(200)을 소지하고 있어야 인증이 가능하다는 점에서 보안성의 향상효과는 존재한다. 더구나, 상기 인증 시스템(300)이 OTP 또는 인증정보를 생성하기 위해서는, 미리 서로 페어로 형성되어 있는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 적어도 한 번 태깅을 해야 할 수 있으므로 보안성은 향상될 수 있다.
- [0151] 또한 상기 보안 디지털 시스템(100)의 소유주 또는 기기의 식별정보와 상기 페어 시스템(200)의 식별정보 중 적어도 하나의 식별정보가 상기 인증 시스템(300)에 저장되어 있고, 저장되어 있는 식별정보에 상응하는 상기 보안 디지털 시스템(100) 및/또는 페어 시스템(200)이 적어도 한 번 태깅을 수행하여야 본 발명의 기술적 사상에 따른 인증 요청자의 인증이 구현되는 경우 보안성이 더욱 향상될 수 있다.
- [0152] 또한, 종래의 인증정보를 이용한 인증과 같이 사용자가 휴대폰 번호를 인증 시스템으로 전송할 필요가 없으므로 편의성이 향상되고 휴대폰 번호의 노출에 안전하게 대처할 수 있는 효과도 있다. 또한, 이처럼 인증 시스템(300)이 OTP를 생성하지 않고 인증정보를 생성하는 경우에는 굳이 종래의 OTP 생성 방식 등과 같이 S/KEY OTP 방식, 시간 동기화 방식, 또는 챌린지-리스판스(challenge-response) 방식 등과 같은 상대적으로 복잡한 알고리즘을 통해 인증정보를 생성할 필요 없이, 임의로 생성되는 소정의 자리수의 난수를 인증정보로 이용할 수도 있다.
- [0153] 한편, 상기 인증 시스템(300)은 본 발명의 기술적 사상에 따른 인증을 수행하는데 참여할 수 있는 보안 디지털 시스템(100)의 식별정보를 미리 저장하고 있을 수도 있다. 이러한 경우, 상기 인증 시스템(300)은 상기 보안 디지털 시스템(100)이 상기 페어 시스템(200)과 적어도 한 번 태깅된 후, 상기 보안 디지털 시스템(100)으로부터 상기 보안 디지털 시스템(100)의 식별정보를 더 수신할 수도 있다. 그러면, 상기 인증 시스템(300)은 수신된 식별정보가 미리 등록되어 있는 경우에만, 전송한 바와 같은 방식으로 OTP 또는 인증정보를 생성할 수도 있다. 따라서 본 발명의 기술적 사상에 의하면 미리 등록되어 있는 보안 디지털 시스템(100)을 통해서만 사용자가 OTP 또는 인증정보를 통한 인증을 받을 수 있도록 함으로써 보안성의 향상을 가져올 수도 있다.
- [0154] 또한, 상기 보안 디지털 시스템(100)은 상기 보안 디지털 시스템(100)에 페어 형성절차를 통해 미리 등록된 페어 시스템(200)과 적어도 한 번 태깅이 되어야만, 결과적으로 상기 인증 시스템(300)이 OTP 또는 인증정보를 생성하도록 할 수도 있다. 따라서, 이러한 경우에는 미리 본 발명의 기술적 사상이 적용될 보안 디지털 시스템(100)이 특정되거나 및/또는 상기 보안 디지털 시스템(100)과 페어를 이루는 페어 시스템(200)이 특정될 수 있

으므로 보안성의 향상은 배가될 수 있다.

- [0155] 2. 페어 시스템(200) 및 페어 형성의 실시 예
- [0156] 가. 페어 시스템(200)
- [0157] 상기 페어 시스템(200)은 상기 디지털 시스템(100)과 통신을 수행할 수 있는 시스템 또는 장치일 수 있다.
- [0158] 상기 페어 시스템(200)은 전술한 바와 같이 보안정보 또는 상기 보안정보를 생성하기 위한 생성정보를 저장하고 있을 수 있다. 예컨대, 상기 페어 시스템(200)은 보안코드 및/또는 OTP 정보를 포함할 수 있다. 또한, 상기 페어 시스템(200)의 식별정보를 저장하고 있을 수 있다.
- [0159] 이러한 경우, 상기 페어 시스템(200)은 상기 보안코드 및/또는 OTP 정보를 저장할 수 있는 IC 카드(또는 스마트 카드)로 구현될 수 있다. 즉, 상기 페어 시스템(200)은 자체 전력원이 존재하지 않는 시스템일 수 있다. 예컨대, 상기 페어 시스템(200)은 독자적인 연산능력 및 저장능력이 존재하며, 사용자가 금융거래를 수행할 수 있는 IC 카드 또는 스마트 카드에 본 발명의 기술적 사상을 위한 소정의 RF 통신장치가 추가된 시스템일 수 있다.
- [0160] 또는, 상기 보안코드 및/또는 OTP 정보를 저장하는 저장장치를 포함하며, 전력원이 존재하는 데이터 프로세싱 시스템일 수도 있다. 스마트 폰이나 태블릿 PC 또는 전력원을 가지는 카드형의 OTP 카드나 보안카드 등이 상기 페어 시스템(200)으로 구현될 수도 있다.
- [0161] 한편, 상기 페어 시스템(200)은 보안코드를 선택적으로 사용자에게 제공하거나 또는 OTP를 생성할 수 있는 장치일 수도 있다. 이러한 경우, 상기 페어 시스템(200)은 상기 보안 디지털 시스템(100)과 페어링이 유지된 상태 또는 적어도 한 번 페어링이 된 상태 또는 후에만, 저장하고 있는 상기 보안코드의 적어도 일부 또는 OTP를 생성하여 디스플레이하는 시스템일 수 있다. 따라서, 페어링이 유지된 상태 또는 적어도 한 번 페어링이 된 상태 또는 후가 아니면, 상기 페어 시스템(200)은 상기 보안코드를 사용자에게 제공하지 않거나 OTP를 생성하지 않을 수도 있다.
- [0162] 다른 실시 예에 의하면, 상기 페어 시스템(200)은 단순히 상기 보안 디지털 시스템(100)과 페어를 형성하기 위한 시스템 또는 장치일 수도 있다. 이러한 경우, 상기 페어 시스템(200)은 단순히 상기 보안 디지털 시스템(100)과 통신을 수행할 수 있는 통신장치를 적어도 구비하며, 상기 보안 디지털 시스템(100)이나 상기 페어 시스템(200)의 식별정보를 저장하기 위한 저장장치를 구비할 수 있다.
- [0163] 일 실시 예에 의하면, 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)에는 본 발명의 기술적 사상을 구현하기 위한 소정의 통신장치가 소정의 인터페이스(예컨대, USB 인터페이스 등)를 통해 연결될 수도 있다. 예컨대, 상기 보안 디지털 시스템(100)이 데스크탑 PC인 경우, 본 발명의 기술적 사상을 구현하기 위한 소정의 통신장치가 상기 데스크탑에 연결될 수 있으며, 상기 데스크탑에 연결된 상기 통신장치가 본 발명의 기술적 사상에 따른 페어모듈의 기능을 수행할 수도 있다.
- [0164] 한편, 구현 예에 따라 상기 페어 시스템(200)은 단순히 본 발명의 기술적 사상에 따라 상기 보안 디지털 시스템(100)과 페어만 형성하는 시스템일 수 있다. 예컨대, 상기 페어 시스템(200)은 상기 보안 디지털 시스템(100)과 페어링을 이룰 수 있는 최소한의 기능만을 구비하도록 구현된 시스템(220)으로 구현될 수 있으며, 상기 페어 시스템(200)은 소정의 통신장치(예컨대, RF 통신장치(안테나 등))가 포함된 RF 태그 또는 통신장치 자체일 수도 있다. 물론, 상기 RF 태그 또는 통신장치(예컨대, RF 통신장치 등)에는 소정의 저장장치(예컨대, EEPROM 등) 및/또는 IC 칩 등이 구비될 수 있다.
- [0165] 이러한 경우, 사용자가 상기 페어 시스템(200)을 소정의 물건 또는 장치 등과 같은 타겟 오브젝트에 부착 또는 끼울 수 있도록 구현될 수도 있다. 이를 위해 상기 페어 시스템(200)은 소정의 접촉면을 구비하고 있거나, 상기 타겟 오브젝트에 끼워질 수 있도록 하우징(housing)을 가질 수 있다. 상기 타겟 오브젝트는 사용자의 선택에 의해 다양하게 결정될 수 있다.
- [0166] 또는, 상기 페어 시스템(200)은 별도의 기능을 위해 만들어지는 물건에 상기 페어링 기능을 위한 통신장치(예컨대, RF 통신장치 등)가 내장된 시스템일 수 있다. 예컨대, USB 저장장치, 보안카드, OTP 생성기, 시계, 팔찌, 스마트 카드 등 매우 다양한 실시 예가 가능할 수 있다. 어떠한 경우든, 상기 페어 시스템(200)은 상기 디지털 시스템(100)과 페어링을 수행할 수 있는 통신장치를 포함하기만 하면 매우 다양한 형태로 구현될 수 있다.

- [0167] 일 실시 예에 의하면, 종래의 OTP 생성장치에 본 발명의 기술적 사상을 구현하기 위한 소정의 통신장치가 부착되어 본 명세서에서 정의되는 기능을 수행함으로써 상기 페어 시스템(200)이 구현될 수도 있고, 또는 종래의 보안카드에 본 발명의 기술적 사상을 구현하기 위한 소정의 저장장치, 통신장치 등이 부착되어 본 명세서에서 정의되는 기능을 수행함으로써 상기 페어 시스템(200)이 구현될 수도 있다.
- [0168] 나. 페어 형성
- [0169] 페어 형성이라 함은, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 페어를 이루도록 설정되는 일련의 과정 또는 절차를 의미할 수 있다.
- [0170] 상기 페어 시스템(200)은 미리 특정 보안 디지털 시스템(100)과 페어가 되도록 상기 페어 시스템(200) 또는 상기 보안 디지털 시스템(100)의 제조주체 또는 유통주체에 의해 결정된 시스템일 수도 있고, 사용자에게 의해 선택적으로 상기 디지털 시스템과 페어를 이루도록 구현되는 시스템일 수도 있다.
- [0171] 예컨대, 상기 보안 디지털 시스템(100)의 제조사가 미리 상기 디지털 시스템(100)과 페어를 이룰 수 있는 상기 페어 시스템(200)을 결정할 수 있다. 실시 예에 따라서는 상기 보안 디지털 시스템(100)의 제조사나 유통사가 상기 디지털 시스템(100)과 페어를 이룰 수 있는 태그장치를 제공할 수 있고, 사용자가 소정의 오브젝트에 상기 태그장치를 부착하면, 상기 태그장치가 부착된 오브젝트가 상기 페어 시스템으로 구현될 수도 있다. 또는, 사용자가 상기 보안 디지털 시스템(100)과 페어를 이룰 상기 페어 시스템(200)을 선택할 수도 있다. 또는 금융거래 시스템의 운영주체 또는 상기 인증 시스템(300)의 운영 주체에 의해 상기 페어 시스템(200)이 사용자에게 발급될 수도 있다.
- [0172] 일 실시 예에 의하면, 상기 페어 시스템(200)은 소정의 금융기관에 의해 배포될 수 있는 금융거래 수단일 수도 있다. 예컨대, 금융거래 시스템을 운영하는 주체인 금융기관이 신용카드나 보안카드 등을 상기 페어 시스템(200)으로 구현하여 사용자에게 발급할 수 있다.
- [0173] 또는 OTP나 보안카드, 스마트 카드 등을 생산하고 유통하는 회사들, 또는 인증관련기관 등 다양한 주체에 의해 상기 페어 시스템(200)이나 상기 페어 시스템(200)에 부착되어질 수 있는 태그장치 등이 제공되어질 수도 있다.
- [0174] 어떠한 경우든 페어 형성은 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)이 페어를 이루는 상기 페어 시스템(200) 또는 상기 보안 디지털 시스템(100)을 식별할 수 있는 식별정보를 저장함으로써 수행될 수 있다. 이러한 절차를 페어 형성 절차로 정의할 수 있다. 페어 형성 절차가 수행되면, 이후 본 발명의 기술적 사상을 구현하기 위해 페어링이 형성되기 전에 페어 인증 절차가 수행될 수도 있다.
- [0175] 따라서, 상기 페어 형성 절차는 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)이 상기 페어 시스템(200) 또는 상기 디지털 시스템(100)의 식별정보를 수신하는 과정을 포함할 수 있다. 즉, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 직접 통신(예컨대, 다양한 RF 통신 또는 NFC 통신 등)을 통해 상기 페어 형성 절차를 수행할 수 있다. 구현 예에 따라서는, 상기 페어 형성 절차는 사용자가 소정의 애플리케이션 또는 소프트웨어(예컨대, OS)를 통해 상기 디지털 시스템(100) 또는 상기 페어 시스템(200)으로 상기 페어 시스템(200) 또는 상기 디지털 시스템(100)의 식별정보를 입력함으로써 수행될 수도 있다.
- [0176] 물론, 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)에는 미리 페어를 이루는 상기 페어 시스템(200) 또는 상기 보안 디지털 시스템(100)의 식별정보가 저장되어 있고, 상기 정보는 변경되지 않을 수도 있다.
- [0177] 본 발명의 기술적 사상에 의하면, 보안정보를 획득하고자 하는 자는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)을 모두 소유 또는 점유하고 있어야, 보안정보를 획득할 수 있다. 따라서, 어느 하나의 시스템이 분실 또는 도난되어도 사용자의 인증에 사용되는 보안정보는 유출되지 않을 수 있다.
- [0178] 한편, 상기 페어 시스템(200)이 사용자가 임의로 소정의 물건 등과 같은 타겟 오브젝트에 부착하거나 끼워서 사용할 수 있도록 구현되는 경우에는, 상기 타겟 오브젝트가 무엇인지 타인이 인지하기가 어려우므로 부정한 사용자가 상기 보안정보의 획득에 필요한 상기 페어 시스템(200)이 무엇인지를 특정하기 조차 어려울 수 있다. 따라서, 상기 페어 시스템(200)의 분실 또는 도난 자체를 예방할 수 있는 효과도 존재한다.
- [0179] 또한, 본 발명의 기술적 사상에 의하면, 상기 보안 디지털 시스템(100)과 페어 시스템(200)이 일정 거리 이상 멀어지는 경우에 사용자에게 알람신호를 주기 위하여 상기 보안 디지털 시스템과 페어 시스템은 평상시 페어링 상태(후술하는 바와 같이 본 발명에서는 이를 '알람 페어링 상태'라 함)를 유지하게 함으로써, 상기 보안 디지

터 시스템(100)과 상기 페어 시스템(200)이 페어링을 통해 보안정보를 획득하고자 할 때, 페어 형성 절차가 미리 형성되어 있으므로 해서 보다 효율적으로 보안정보를 획득할 수 있도록 할 뿐만 아니라 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)의 분실 또는 도난 자체를 예방할 수 있는 효과도 존재한다.

[0180] 한편, 상기의 알람 페어링 상태와는 달리 NFC 통신방식 즉, 태깅을 수행하는 동안에 페어링이 수행될 수도 있다.

[0181] 3. 보안 디지털 시스템(100)과 페어 시스템(200)의 통신(페어링)

[0182] 페어링이 된 상태인지 여부는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)간의 통신 상태가 소정의 기준을 만족하는지 여부에 따라 결정될 수 있다. 상기 통신 상태는 상기 디지털 시스템(100)과 상기 페어 시스템(200)간의 거리에 의존할 수 있다.

[0183] 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 무선통신(예컨대, RF 통신)을 수행할 수 있다. 따라서, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200) 간의 통신환경에 영향을 더 받을 수도 있다. 본 명세서에서는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 사람의 일상적인 생활환경을 가정하므로, 상기 통신상태는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)간의 거리에 지배적인 영향을 받는다고 가정할 수 있다. 물론, 상기 페어 시스템(200) 또는 상기 보안 디지털 시스템(100) 사이에 무선통신을 방해할 만한 물체가 존재하는 경우에는, 거리가 충분히 가까워도 페어링이 되지 않을 수도 있다.

[0184] 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 페어링이 된 경우는 예컨대, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 통신을 수행할 수 있는 경우일 수 있다. 또는, 통신이 수행되더라도 일정 크기 이상의 신호가 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)으로 전송될 수 있는 경우를 의미할 수도 있다. 즉, 일반적인 통신환경에서는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 서로 통신을 할 수 있는 통신거리 내에 존재하는 경우, 또는 상기 통신거리보다 짧은 미리 결정된 거리 내에서 존재하는 경우를 의미할 수 있다.

[0185] 한편, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)간의 통신은 다양한 방식으로 수행될 수 있다. 그리고 이러한 방식에 따라, 페어링이 가능한 거리 및/또는 환경은 달라질 수 있음은 널리 공지되어 있다.

[0186] 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)간의 통신은 예컨대, 블루투스, NFC, 적외선 통신, 광통신 등 다양한 실시 예가 가능할 수 있다. 그리고, 이러한 통신을 위한 통신장치가 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200)에 각각 구비될 수 있다.

[0187] 일 실시 예에 의하면, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 RF 통신을 수행할 수 있다. 예컨대, 상기 디지털 시스템(100)과 상기 페어 시스템(200)은 블루투스(Bluetooth), 지그비(Zigbee) 등의 무선 표준 프로토콜을 이용한 통신을 수행할 수 있다. 물론, 블루투스 통신을 수행하는 경우에는 상기 페어 시스템(200) 역시 자체 전력 공급원을 가지고 있거나 또는 외부에서 전력을 공급받을 수 있는 시스템일 수 있다. 한편, 지그비 통신의 경우에는 블루투스에 비해 저전력으로 통신이 가능하다는 장점이 있을 수 있다. 이외에도 구현 예에 따라 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 다양한 근거리 무선통신(예컨대, IrDA, UWB 등)을 수행할 수 있으며, 무선통신의 종류에 따라 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200)에는 해당 무선통신에 필요한 환경을 위한 소정의 구성들이 구비될 수 있다.

[0188] 일 실시 예에 의하면, 상기 페어 시스템(200)은 자체적인 전력 공급원이 없이 상기 보안 디지털 시스템(100)으로부터 출력된 RF 시그널에 의해 구동되는 시스템일 수도 있다. 즉, RFID 통신 또는 NFC 통신 등을 수행할 수 있다. 예컨대, 상기 페어 시스템(200)은 RFID 태그 등으로 구현되거나, 상기 RFID 태그를 포함하는 소정의 장치일 수 있다. 이러한 경우, 상기 보안 디지털 시스템(100)은 상기 RFID 태그와 통신을 수행할 수 있는 리더기의 역할을 수행할 수도 있다. 그러면, 상기 보안 디지털 시스템(100)은 소정의 RF 시그널을 출력하여, 상기 페어 시스템(200)을 검색하거나, 상기 페어 시스템(200)에 저장된 소정의 정보를 수신할 수도 있다. 또한, 상기 보안 디지털 시스템(100)의 출력 전력에 따라 상기 디지털 시스템(100)과 상기 페어 시스템(200)간의 통신거리는 다양해질 수 있다.

[0189] 일반적으로 상기 페어 시스템(200)은 사용자의 지갑에 휴대될 수 있도록 구현될 수 있다. 그러면, 상기 보안 디지털 시스템(100)을 사용자가 소지하고 있을 때, 지갑 내에 위치한 상기 페어 시스템(200)과 비접촉식 통신을 수행할 수 있는 통신 프로토콜이 본 발명의 기술적 사상을 구현하기 위해 선택될 수 있다. 그리고, 이러한 통신

프로토콜이 적용 가능한 구성이 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)에 구비될 수 있는 것이 바람직하다.

[0190] 일 실시 예에 의하면, 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)은 복수의 서로 다른 통신 프로토콜을 이용해 통신을 수행할 수도 있다. 예컨대, 상기 보안 디지털 시스템(100)에 포함된 상기 통신모듈(120)은 제1통신모듈(121) 및 제2통신모듈(122)을 포함할 수 있다. 예컨대, 상기 제1통신모듈(121)은 후술할 바와 같이 알람 페어링 기능을 수행하기 위한 통신수단일 수 있으며, 제2통신모듈(122)은 보안정보를 획득하기 위한 통신수단일 수 있다. 물론, 상기 제1통신모듈(121) 및 상기 제2통신모듈(122) 각각에 대응되는 제1통신장치(221) 및 제2통신장치(222)가 상기 페어 시스템(200)에 구비될 수도 있다.

[0191] 상기 제1통신모듈(121)은 상기 제2통신모듈(122)에 비해 통신 거리가 긴 통신 수단일 수 있다. 상기 제1통신모듈(121)과 상기 페어 시스템(200)에 구비되는 제1통신장치(221)는 예컨대, 페어링 상태를 유지하다가 비 페어링 상태가 되면 소정의 알람신호를 출력할 수 있다. 또는 상기 제1통신모듈(121)과 상기 제1통신장치(221)의 통신 상태에 따라 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)의 거리가 판단될 수 있으므로, 페어링 상태라도 두 시스템(100, 200)간의 거리가 일정 거리 이상 떨어진 경우에는 알람신호를 출력할 수 있다. 물론, 두 시스템(100, 200)이 통신 가능한 거리내에서도 상기 일정 거리 내에 존재하는 경우에만 페어링 상태라고 판단될 수도 있다.

[0192] 이처럼 상기 제1통신모듈(121)과 상기 제1통신장치(221)는 페어링 상태인지 여부를 주기적으로 판단하고, 비 페어링 상태 또는 일정 거리 이상 이격되었다고 판단하는 경우, 즉, 알람출력 조건이 되는지 여부를 판단하기 위한 수단으로 이용될 수 있다.

[0193] 한편, 이처럼 상기 제1통신모듈(120) 및 상기 제1통신장치(221)가 알람 페어링을 위한 수단으로 구비되는 경우에도 상기 제1통신모듈(120)과 상기 제1통신장치(221)를 통해 본 발명의 기술적 사상을 구현하기 위한 보안정보가 송신 또는 수신될 수 있다. 이러한 경우, 상기 제1통신모듈(120)과 상기 제1통신장치(221)는 페어링 상태인지 여부를 주기적으로 판단하기 때문에, 보안 디지털 시스템(100) 또는 페어 시스템(200)이 페어가 되는 시스템과 페어링을 위해 시스템을 검색하고, 이를 통해 페어를 형성하는 절차를 수행할 필요 없이 바로 보안정보를 송수신할 수 있는 효과가 있다.

[0194] 다른 실시 예에 의하면, 상기 제1통신모듈(121) 및 상기 제1통신장치(221)는 알람 페어링 기능을 수행하는 데에만 관여하고, 제2통신모듈(122) 및 제2통신장치(222)가 보안정보를 송수신하는 데 이용될 수도 있다. 즉, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 서로 다른 통신 프로토콜을 통해 통신을 수행할 수 있다. 이러한 경우, 상기 서로 다른 통신 프로토콜을 통한 통신은 충돌이 없는 경우로 가정할 수 있다. 또는, 충돌이 발생하는 경우라도 충돌을 회피할 수 있는 소정의 수단이 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)에 더 구비될 수 있다. 본 명세서에서는 본 발명의 기술적 특징을 강조하기 위해 동시에 두 시스템(100, 200)이 통신을 하고자 하는 경우의 충돌 또는 이를 회피하기 위한 기술적 사상에 대해서는 고려하지 않기로 한다.

[0195] 제1통신 프로토콜 즉, 상기 제1통신모듈(121)과 상기 제1통신장치(221)가 수행하는 통신 프로토콜은 제2통신 프로토콜 즉, 제2통신모듈(122) 및 상기 제2통신장치(222)가 수행하는 통신 프로토콜에 비해 상대적으로 긴 거리의 통신을 수행할 수 있는 프로토콜일 수 있다. 일 실시 예에 의하면, 상기 제1통신 프로토콜은 블루투스, 지그비 등의 상대적으로 긴 통신을 위한 프로토콜일 수 있으며, 제2통신 프로토콜은 NFC(RFID 통신을 포함함) 통신을 위한 통신 프로토콜일 수 있다. 왜냐하면, 상기 제1통신 프로토콜은 사용자가 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)을 모두 소지하고 있는지를 판단하기 위해 사용될 수 있는 반면, 상기 제2통신 프로토콜은 정보를 교환하기 위해 사용될 수 있고 사용자가 두 시스템(100, 200)을 소지하고 있다는 이유만으로 본 발명의 기술적 사상에 의한 보안정보가 전송될 필요는 없기 때문이다.

[0196] 또한, 제2통신 프로토콜이 NFC인 경우에는 정보 교환에 별도의 페어 형성 절차 또는 페어 인증 절차를 다시 수행할 필요가 없을 수 있고, 태깅을 통해 즉각적으로 정보의 교환이 수행될 수도 있다.

[0197] 또한, 제2통신 프로토콜로 통신을 수행하는 대상이 상기 제1통신 프로토콜로 통신을 수행하고 있는 페어 시스템(200)으로 특정될 수 있는 효과도 있다. 즉, 제2통신 프로토콜을 통해 통신 가능한 페어 시스템(200)은 제1통신 프로토콜을 통해 페어링이 유지되고 있는 상태인 페어 시스템(200)으로 한정될 수 있다. 예컨대, 제1통신 프로토콜을 통해 통신을 수행하는 상기 페어 시스템(200)은 이를 식별할 수 있는 정보를 기록하고, 상기 제2통신모듈(122)은 상기 정보가 기록된 페어 시스템(200)과만 통신을 수행할 수 있다.

- [0198] 어떠한 경우든, 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200)은 하나의 통신수단을 구비하고, 상기 통신수단이 알람 페어링 기능 및/또는 정보 교환 기능을 수행할 수도 있다. 또는, 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200) 각각은 복수의 통신수단을 구비하고, 어느 하나의 통신 수단은 알람 페어링 기능을 수행하며, 나머지 하나는 정보 교환 기능을 수행할 수 있다.
- [0199] 본 발명의 기술적 사상에 의하면, 상기 페어 시스템(200)을 지갑에서 꺼내지 않고도 사용자는 상기 보안 디지털 시스템(100)을 통해 보안정보를 획득할 수 있는 효과가 있다. 이러한 보안정보의 획득은 페어링 상태가 유지되는 상태 또는 적어도 한 번의 태깅이 수행된 경우에만 가능할 수 있다. 페어링 상태가 유지되는 상태에서 사용자는 소정의 입력 또는 요청을 할 수 있고, 그러면 보안정보가 획득될 수 있다. 또는 태깅 자체가 상기 보안정보를 요청하는 행위로 취급될 수도 있다. 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 주기적으로 통신을 수행하면서, 페어링 상태가 유지되는지 여부를 판단할 수 있고, 페어링이 필요한 시점에만 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 소정의 페어 형성 절차 및/또는 페어 인증 절차를 거쳐 페어링이 될 수도 있다.
- [0200] 한편, 본 발명의 기술적 사상에 따르면, 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)은 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 일정 거리 이상 멀어지는 경우 또는 비페어링 상태가 되는 경우(이하, 알람 출력 조건이 만족하는 경우)에는, 소정의 알람신호를 출력할 수 있다. 또한, 본 발명에서는 이처럼 페어링 상태를 유지하고 있다가 알람 출력 조건이 만족되면 소정의 알람 신호를 출력하는 것을 '알람 페어링'기능으로 정의하기로 한다. 상기 알람신호는 소정의 음성신호일 수도 있고, 램프 또는 소정의 디스플레이 정보를 이용한 시각적인 신호일 수도 있으며, 진동 등과 같은 촉각적인 신호일 수도 있다.
- [0201] 이를 통해, 정당한 사용자가 깜빡하고 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)을 놔두고 이동하거나, 분실할 위험을 줄일 수 있는 효과가 있다. 물론, 타인에 의해 도난당할 확률도 줄일 수 있는 효과도 있다.
- [0202] 물론, 정당한 사용자가 의도적으로 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200) 중 어느 하나만을 소지하고자 하는 경우에는 상기 알람신호를 출력하는 기능을 오프 또는 디스에이블 시킬 수 있도록 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)이 구현될 수도 있다.
- [0203] 본 발명의 기술적 사상에 따른 실시 예에 의한 '알람 페어링'은 통상의 경우 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 페어링되어 있음을 전제로 한다. 즉, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 일정 거리 이상 멀어지는 경우 즉 비페어링 상태가 되면 소정의 알람신호를 출력할 수 있다는 것은 통상의 경우에는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 페어링 상태임을 전제로 하는 것이다. 이와 같이 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 이미 페어링이 되어 있는 상태에서는 상기 보안 디지털 시스템(100) 또는 페어 시스템(200)이 보안정보를 획득하기 위한 페어링 형성 절차는 생략되어질 수 있고 상기 보안 디지털 시스템(100) 또는 페어 시스템(200)의 특정 버튼을 통한 신호 수신 방식 등 간단한 방식만으로 보안정보 획득이 가능할 수 있다.
- [0204] 이와 함께 '알람 페어링' 상태에서의 보안정보 획득은 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200) 간의 페어링 형성 절차가 필요하지 않음으로 해서, 보안정보의 획득에 관한 속도 면에서 매우 효율적인 효과를 얻어 본 발명의 실효성을 크게 향상시킨다고 할 수 있다. 이러한 실효성의 차이는 본질적으로 '알람 페어링'의 경우 페어링 상태를 연속적(또는 매우 짧은 시간을 단위로 하는 주기적)으로 유지하는 것에 비해, 단순히 보안정보를 획득하기 위해 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 페어링을 하는 것은 일회적 또는 단발적으로 이루어지기 때문에 발생하는 것이라 할 수 있다.
- [0205] 구현 예에 따라, 즉, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 통신하는 방식에 따라, 사용자는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)을 페어링 시키기 위해 소정의 거리내로 상기 보안 디지털 시스템(100)을 상기 페어 시스템(200)에 위치시키는 행위를 수행하거나, 또는 상기 페어 시스템(200)을 상기 보안 디지털 시스템(100)의 소정의 거리내로 위치시키는 행위를 수행할 수도 있다. 예컨대, 상기 보안 디지털 시스템(100)이 NFC(Near Field Communication) 칩을 구비하며, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 NFC 통신을 수행할 수 있다. 이러한 경우, 사용자는 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200)을 소정의 거리(예컨대, 10cm)내로 위치시키는 행위 즉, 태깅(tagging)을 수행하여야 페어링이 될 수도 있다.
- [0206] 예를 들면, 사용자는 상기 보안 디지털 시스템(100)을 자신의 지갑에 가까이 가져다 댈 수 있다. 즉, 태깅을 수

행할 수 있다. 그러면, 상기 보안 디지털 시스템(100)은 상기 지갑에 있는 페어 시스템(200)과 페어링이 되고, 이때 본 발명의 기술적 사상을 구현하기 위한 소정의 정보들이 교환될 수 있다.

[0207] 그러면, 상기 보안 디지털 시스템(100)을 통해 사용자는 보안정보(예컨대, 보안코드, 요청 보안코드, 또는 OTP)를 획득할 수 있다. 즉, 보안 디지털 시스템(100)에 구비된 디스플레이 장치를 통해 보안정보를 확인할 수 있다. 또는, 전술한 바와 같이 자동으로 보안정보가 소정의 UI에 입력되거나 인증 시스템(300)으로 전송될 수 있다. 보안정보의 획득은 사용자가 태깅을 수행하면 자동으로 발생할 수도 있고, 태깅 후 상기 보안 디지털 시스템(100)을 통해 소정의 입력 또는 요청을 하여야 획득될 수도 있다.

[0208] 또한, 전술한 바와 같이 복수의 태깅을 수행하여야만 사용자는 최종적으로 원하는 보안정보를 획득할 수도 있다. 각각의 태깅이 수행되는 동안 또는 수행된 후 보안정보를 획득하기 위해 필요한 프로세스들 중 일부가 순차적으로 수행될 수도 있다.

[0209] 한편, 상기 보안 디지털 시스템(100)은 알람모듈(130)을 더 포함할 수 있다. 상기 페어 시스템(200) 역시 소정의 알람장치(미도시)를 더 포함할 수도 있다. 상기 알람모듈(130) 또는 상기 알람장치(미도시)는 소정의 알람신호를 출력할 수 있다. 상기 알람신호는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 일정 거리 이상 떨어지는 경우, 사용자에게 이를 알려주기 위한 신호일 수 있다. 상기 알람신호는 음성신호일 수도 있지만, 진동, 디스플레이 신호 등 사용자가 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 일정거리 이상 떨어졌음을 인지하도록 하기 위한 다양한 형태의 신호로 구현될 수 있다.

[0210] 상기 알람모듈(130) 또는 알람장치(미도시)가 상기 알람신호를 출력하는 경우는 예컨대, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 비 페어링 상태로 판단된 경우일 수 있다. 이러한 경우, 상기 제어모듈(110)은 주기적으로 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 페어링 상태인지 여부를 판단하고, 페어링이 되지 않는다고 판단한 경우 알람신호를 출력할 수 있다. 따라서, 이때에는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 일정 거리 내에서는 페어링 상태가 유지될 수 있는 통신 프로토콜이 선택되는 것이 바람직할 수 있다. 상기 일정 거리는 주로 동일인이 상기 페어 시스템(200)과 상기 보안 디지털 시스템(100)을 소지하고 있다고 판단될 정도의 거리일 수 있으며, 수 미터 내외의 거리일 수 있다.

[0211] 한편, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 페어링을 수행하는 통신 방식에 따라, 단순히 비 페어링 상태인 경우에 알람신호를 출력하면 매우 비효율적이거나 비현실적일 수도 있다. 예컨대, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 NFC 통신을 통해 페어링을 수행하는 경우라면, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 약 10cm 내의 근거리에서 존재하지 않으면 비 페어링 상태가 될 수 있다. 이러한 경우 비 페어링 상태에서 알람신호를 출력하도록 상기 알람모듈(130) 또는 알람장치가 구현되는 것은 불합리할 수 있다. 따라서, 이러한 경우에는 상기 알람모듈(130) 또는 알람장치는 페어링 상태여부와는 무관하게 별도로 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)은 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)간의 거리를 판단할 수 있는 거리 판단 수단을 구비할 수 있다. 상기 거리 판단 수단은 전술한 바와 같은 RF 통신모듈일 수도 있지만, 이에 국한되지 않으며 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)의 거리를 판단할 수 있는 모든 형태의 구성을 의미할 수 있다. 판단된 결과 일정거리 이상 떨어졌다고 판단하면 알람신호를 출력할 수 있다. 결국, 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)은 NFC 통신을 위한 통신모듈(120) 및/또는 상기 페어 시스템(200)에 포함된 통신장치(220)와는 별개로 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)과의 거리를 측정하기 위한 상기 거리 판단 수단을 포함할 수 있다. 상기 거리 판단 수단은 예컨대, 페어링을 위한 상기 통신모듈(120) 또는 통신장치와는 별개의 RF 통신을 수행하는 구성일 수도 있으며, 비접촉식으로 통신을 수행하여 거리를 측정할 수 있는 다양한 구성이 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)에 구비될 수 있다.

[0212] 또는, 전술한 바와 같이 서로 다른 통신 프로토콜을 이용해 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 통신을 수행할 수도 있다. 이때 제1통신 프로토콜을 이용해 수행되는 기능 및 제2통신 프로토콜을 이용해 수행되는 기능이 미리 정의되어 있을 수 있다. 예컨대, 제1통신 프로토콜은 전술한 바와 같이 알람 페어링 기능을 수행하며, 제2통신 프로토콜은 보안정보를 송신/수신하기 위해 이용될 수 있다. 이외에도 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200)이 추가적인 기능 예컨대, 결제, 네트워크 접속 등을 위해 통신을 수행하여야 하는 경우, 어떤 통신 프로토콜을 이용할지는 미리 정의될 수 있다. 그리고 이러한 정의의 예는 상기 제1통신 프로토콜 및 상기 제2통신 프로토콜의 구현 예에 따라 다양할 수 있음은 물론이다.

[0213] 결국, 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)은 비 페어링 상태가 되면 알람신호를 출력할 수도 있고, 실시 예에 따라서는 페어링이 되는지 여부와는 무관하게 일정 거리이상 두 시스템이 떨어지면 알

람신호를 출력할 수도 있다. 그리고 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)간의 거리를 판단하기 위해서는 상기 통신모듈(120) 또는 상기 통신장치(도 8의 220)가 이용될 수도 있고, 또는 상기 통신모듈(120) 또는 상기 통신장치(도 8의 220)가 전송한 바와 같이 복수의 통신수단을 포함할 수도 있다. 또는 실시 예에 따라서는 상기 통신모듈(120) 또는 상기 통신장치(도 8의 220)와는 별도로 거리를 판단하기 위한 구성이 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)에 더 구비될 수도 있다.

[0214] 이하에서는, 상술한 바와 같은 본 발명의 기술적 사상을 구현할 수 있는 실시 예들을 도면을 참조하여 보다 구체적으로 설명하기로 한다. 이하에서 설명하는 실시 예는 상술한 기술적 사상의 하나의 실시 예에 불과한 것은 물론이다.

[0215] 도 1을 참조하면, 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)과 페어를 형성할 수 있다. 상기 페어 시스템(200)은 다양한 형태로 구현될 수 있다. 예컨대, IC 칩을 포함한 카드(201)로 구현될 수도 있고, 또 다른 디지털 시스템(202)으로 구현될 수도 있다.

[0216] 한편, 상기 보안 디지털 시스템(100)은 소정의 인증 시스템(300)과 유무선 네트워크를 통해 통신을 수행할 수도 있다. 또는 상기 인증 시스템(300)은 상기 보안 디지털 시스템(100)의 사용자가 이용하는 별도의 데이터 프로세싱 장치(400)와 유무선 네트워크를 통해 통신을 수행할 수도 있다.

[0217] 상기 인증 시스템(300)은 상기 보안 디지털 시스템(100) 또는 상기 데이터 프로세싱 장치(400)로부터 보안정보(예컨대, 보안코드 또는 OTP)를 수신하고, 수신된 보안정보를 인증하는 인증서버 및/또는 상기 인증서버와 상기 보안 디지털 시스템(100) 또는 상기 데이터 프로세싱 장치(400) 상에 존재하는 적어도 하나의 네트워크 시스템을 포함할 수 있다. 상기 인증 시스템(300)은 OTP 인증 시스템(300-1)을 포함하거나 유무선 네트워크를 통해 통신할 수 있다. 상기 OTP 인증 시스템(300-1)은 상기 인증 시스템(300)의 나머지 구성과는 별도의 물리적 장치로 구현될 수도 있으며, 상기 OTP 인증 시스템(300-1)은 널리 이용되고 있는 OTP 인증센터 등일 수도 있다.

[0218] 상기 인증 시스템(300)은 사용자에게 할당된 보안코드에 대한 정보를 기록하고 있을 수 있다. 또는, 상기 인증 시스템(300)은 상기 페어 시스템(200)과 제1OTP 생성키를 공유하고 있을 수 있다. 한편, 구현 예에 따라, 상기 인증 시스템(300)은 상기 보안 디지털 시스템(100)과 제2OTP 생성키를 공유하고 있을 수도 있다.

[0219] 구현 예에 따라서는, 상기 인증 시스템(300)이 OTP를 생성할 수도 있다.

[0220] 상기 인증 시스템(300)은 개별적인 서비스 시스템(예컨대, 웹 사이트를 제공하는 웹 서버, 금융기관의 시스템)별로 구비되는 인증 시스템(300)일 수도 있고, 복수의 서비스 시스템들이 인증을 위해 공통적으로 연결된 시스템일 수도 있다.

[0221] 상기 인증 시스템(300)은 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)과 동일한 방식으로 OTP를 생성할 수 있음은 물론이다.

[0222] 도 2는 본 발명의 실시 예에 따른 보안 디지털 시스템의 개략적인 구성을 나타내는 도면이다.

[0223] 도 2를 참조하면, 본 발명의 실시 예에 따른 보안 디지털 시스템(100)은 제어모듈(110) 및 통신모듈(120)을 포함한다. 구현 예에 따라, 상기 보안 디지털 시스템(100)은 알람모듈(130), 보안모듈(140), 및/또는 디스플레이 모듈(150)을 더 포함할 수 있다.

[0224] 본 명세서에서 모듈이라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스(resource)의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것은 아님은 본 발명의 기술분야의 평균적 전문가에게는 용이하게 추론될 수 있다.

[0225] 상기 제어모듈(110)은 상기 보안 디지털 시스템(100)에 포함된 다른 구성(예컨대, 상기 통신모듈(120), 상기 알람모듈(130), 상기 보안모듈(140), 및/또는 상기 디스플레이 모듈(150))의 기능 및/또는 리소스를 제어할 수 있다. 상기 통신모듈(120)은 상기 보안 디지털 시스템(100)이 NFC 통신을 이용하는 경우에는 NFC 통신모듈로 명명될 수도 있다.

[0226] 상기 통신모듈(120)은 상기 보안 디지털 시스템(100)과 페어를 이루는 페어 시스템(200)과 통신을 수행할 수 있다. 상기 통신모듈(120)이 사용하는 통신 프로토콜은 다양할 수 있음은 상술한 바와 같다.

[0227] 그러면, 상기 제어모듈(110)은 상기 통신모듈(120)과 상기 페어 시스템(200)이 페어링 상태인지 여부를 판단할

수 있다. 또는, 적어도 한 번 페어링이 수행되었는지 판단할 수도 있다. 페어링 상태인지 여부를 판단하는 경우는 전술한 바와 같이 일정 거리 이상 떨어진 상태에서도 상기 통신모듈(120)과 상기 페어 시스템(200)이 통신을 수행할 수 있으며, 상기 통신모듈(120)이 주기적으로 상기 페어 시스템(200)과 통신을 수행하는 경우일 수 있다. 상기 통신모듈(120)이 주기적으로 통신을 수행함으로써 상기 제어모듈(110)은 상기 페어 시스템(200)과 페어링 상태인지 여부를 판단할 수 있다.

[0228] 또는, 상기 제어모듈(110)은 일정 시간 내에 상기 통신모듈(120)이 적어도 한 번 페어링 상태가 되었는지 여부를 판단할 수도 있다. 이러한 경우는 상기 통신모듈(120)이 상기 페어 시스템(200)과 NFC 통신을 수행하는 경우일 수 있다. 이때에는 상기 통신모듈(120)과 상기 페어 시스템(200)이 태깅이 되면 페어링 상태일 수 있다. 상기 제어모듈(110)은 한 번만 태깅이 되어도 보안정보를 사용자가 획득할 수 있는 조건(이하, '보안정보 획득 조건'이라 함)이 만족하였다고 판단할 수 있다. 또는 복수 번 태깅을 수행하여야 상기 보안정보 획득 조건이 만족하였다고 판단할 수도 있다. 상기 보안정보 획득 조건이 만족되면, 그 때부터 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)을 통해 보안정보를 획득하기 위한 소정의 프로세스들이 수행될 수도 있다. 또는, 복수 번 태깅을 수행하는 경우에는 미리 결정된 회수의 태깅이 수행되기 전에 상기 프로세스들 중 일부가 수행될 수도 있음은 전술한 바와 같다.

[0229] 어떠한 경우든 상기 제어모듈(110)은 현재 상기 통신모듈(120)이 상기 페어 시스템(200)과 페어링 상태인 경우에 상기 보안정보 획득 조건이 만족했다고 판단할 수도 있고, 일정 시간 내에 상기 통신모듈(120)과 상기 페어 시스템(200)이 페어링이 적어도 한 번 되었어야 보안정보 획득 조건이 만족했다고 판단할 수 있다. 결국, 상기 제어모듈(110)은 보안정보 획득 조건이 만족하였는지 여부를 판단할 수 있다.

[0230] 보안정보 획득 조건이 만족했다고 판단하면, 상기 제어모듈(110)은 사용자가 상기 보안 디지털 시스템(100)을 통해 보안정보를 획득하도록 제어할 수 있다. 또는 보안정보 획득 조건이 만족하기 전에 보안정보를 획득하기 위한 일부의 프로세스만이 수행될 수도 있다. 상기 제어모듈(110)은 보안정보 획득 조건이 만족했다고 판단하면, 자동으로 상기 보안정보를 획득하도록 소정의 제어를 수행할 수도 있고, 사용자로부터 소정의 입력 또는 요청이 있어야 상기 보안정보를 획득하도록 소정의 제어를 수행할 수도 있다.

[0231] 상기 보안정보는 예컨대, 상기 사용자에게 할당된 보안코드의 적어도 일부일 수도 있고, OTP일 수도 있다.

[0232] 일 실시 예에 의하면, 상기 페어 시스템(200)은 상기 보안코드 정보를 저장하고 있을 수 있다. 또한, 상기 페어 시스템(200)은 상기 OTP를 생성하기 위해 필요한 생성정보 즉, OTP 정보를 저장하고 있을 수 있다.

[0233] 그러면, 상기 제어모듈(110)은 상기 통신모듈(120)을 제어하여 상기 보안코드의 적어도 일부를 수신할 수 있다. 그리고, 수신된 보안코드의 적어도 일부를 사용자가 획득하도록 할 수 있다. 보안코드의 적어도 일부를 사용자가 획득하도록 한다고 함은, 전술한 바와 같이 보안코드의 적어도 일부를 상기 보안 디지털 시스템(100)에 구비되어 있는 디스플레이 모듈(150)로 출력하여 사용자가 눈으로 확인할 수 있도록 하는 경우를 포함한다. 또는, 상기 보안코드의 적어도 일부를 소정의 입력 UI에 자동으로 입력하거나, 자동으로 상기 보안코드의 적어도 일부를 보안코드 중 요청 보안코드를 요청하는 시스템 즉, 인증 시스템(300)으로 전송하는 경우를 포함한다.

[0234] 상기 제어모듈(110)은 상기 페어 시스템(200)으로부터 보안코드 전체를 수신할 수도 있고, 보안코드 중 필요한 보안카드 번호 즉, 요청 보안코드만을 상기 페어 시스템(200)으로부터 수신할 수도 있다.

[0235] 이러한 일 예는 도 5에 도시된다.

[0236] 도 5a는 본 발명의 일 실시 예에 따라 보안 디지털 시스템이 요청 보안코드를 획득하는 과정을 설명하기 위한 도면이고, 도 5b는 본 발명의 다른 실시 예에 따라 보안 디지털 시스템이 요청 보안코드를 획득하는 과정을 설명하기 위한 도면이며, 도 5c는 또 다른 실시 예에 따른 요청 보안코드를 획득하는 과정을 설명하기 위한 도면이다.

[0237] 도 5a 내지 도 5c를 참조하면, 상기 인증 시스템(300)은 상기 보안 디지털 시스템(100)으로 사용자를 인증하기 위한 소정의 요청 보안코드를 요청할 수 있다(S10). 이러한 경우는 사용자가 상기 보안 디지털 시스템(100)을 이용하여 소정의 서비스 시스템(미도시)에 서비스를 요청하는 경우일 수 있다. 따라서, 사용자가 상기 보안 디지털 시스템(100)이 아니라 별도의 데이터 프로세싱 장치(예컨대, PC, 노트북 등, 400)를 이용하여 소정의 서비스 시스템(미도시)에 접속하여 서비스를 이용하고자 하는 경우에는, 상기 인증 시스템(300)은 상기 데이터 프로세싱 장치(400)로 요청 보안코드를 요청할 수도 있음은 물론이다. 그러면 사용자는 상기 보안 디지털 시스템(100)을 통해 상기 페어 시스템(200)으로 요청 보안코드를 요청할 수도 있다. 이하에서는 설명의 편의를 위해 상기 보안 디지털 시스템(100)을 이용하여 상기 서비스 시스템(미도시)에 접속하는 경우를 일 예로 설명하기로

한다.

- [0238] 상기 요청 보안코드는 사용자에게 미리 할당된 보안코드(10) 중 현재 인증을 위해 선택된 보안카드 번호를 의미할 수 있다.
- [0239] 상기 인증 시스템(300)이 상기 보안 디지털 시스템(100)으로 요청 보안코드를 요청하면, 상기 보안 디지털 시스템(100)에는 도 5c에 도시된 바와 같은 소정의 요청 수단(예컨대, 페이지, 프레임, UI, 오브젝트 등)이 로딩될 수 있다.
- [0240] 이러한 요청 수단이 로딩되면, 상기 제어모듈(110)은 현재 보안정보 획득 조건이 만족하는지를 판단하고, 만족하였다고 판단하면 상기 페어 시스템(200)으로 보안코드(10)를 요청할 수 있다(S20). 그러면, 상기 통신모듈(120)은 상기 보안코드(10)를 수신할 수 있다(S30). 상기 보안코드가 수신되면, 상기 제어모듈(110)은 상기 보안코드를 상기 디스플레이 모듈(150)을 통해 디스플레이 장치에 디스플레이 할 수 있다(S40). 구현 예에 따라서는, 상기 보안코드 중 요청 보안코드 또는 상기 요청 보안코드를 확인하는데 필요한 정보만을 디스플레이할 수도 있다.
- [0241] 그러면, 사용자는 소정의 입력 UI(예컨대, 도 5c의 부재번호 13)에 요청 보안코드를 입력하고, 상기 인증 시스템(300)으로 상기 요청 보안코드를 전송하도록 상기 보안 디지털 시스템(100)으로 요청할 수 있다.
- [0242] 한편, 상기 보안 디지털 시스템(100)에 포함된 보안모듈(140)은 상기 보안코드의 사용이 완료되거나 현재 사용자가 상기 보안코드를 이용할 의사가 없다고 판단되는 경우에는 수신된 상기 보안코드를 삭제하는 보안절차를 수행할 수도 있다(S50).
- [0243] 상기 보안코드의 사용이 완료되거나 보안코드를 이용할 의사가 없다고 판단되는 경우는, 예컨대, 도 5c에 도시된 바와 같은 보안코드의 요청수단(예컨대, 페이지)가 비활성화되는 경우일 수 있다. 비활성화되는 경우는 상기 요청수단이 상기 보안 디지털 시스템(100)상에서 최소화되어 사용자가 인식하지 못하거나, 상기 요청수단이 종료 또는 클로즈(close)되거나, 디스플레이 레이어(layer) 상 다른 레이어의 하위 레이어에 존재하는 경우든 다양할 수 있다. 어떠한 경우가 상기 요청 수단이 비활성화되는 경우인지는 미리 상기 보안모듈(140)에 정의되어 있을 수 있다.
- [0244] 또는, 상기 보안모듈(140)은 상기 보안코드가 상기 페어 시스템(200)으로부터 수신된 시간이 소정의 시간 경과되면 자동으로 수신된 상기 보안코드를 삭제할 수도 있다.
- [0245] 이처럼 상기 보안모듈(140)이 보안절차를 수행함으로써, 상기 페어 시스템(200)으로부터 수신된 정보는 필요한 경우에만 임시로 상기 보안 디지털 시스템(100)에 저장되었다가 다시 삭제될 수 있다. 따라서, 상기 보안 디지털 시스템(100)에 저장된 후 악의적 공격에 의해 상기 페어 시스템(200)으로부터 수신된 정보가 유출되거나 악용되는 것을 방지할 수 있는 효과가 있다.
- [0246] 이러한 보안절차는 상기 보안 디지털 시스템(100)이 상기 페어 시스템(200)으로부터 OTP를 수신하거나, OTP를 생성할 수 있는 정보(예컨대, 제1OTP 생성기 및/또는 OTP 생성 프로그램 정보 등)를 수신하는 경우도 동일하게 적용될 수 있다.
- [0247] 한편, 도 5a는 상기 페어 시스템(200)으로부터 보안코드 전체를 수신하는 경우를 일 예로 설명하였지만, 도 5b와 같이 상기 인증 시스템(300)으로부터 요청된 정보 즉, 요청 보안코드만을 상기 페어 시스템(200)으로부터 수신할 수도 있다.
- [0248] 도 5b를 참조하면, 상기 인증 시스템(300)은 상기 보안 디지털 시스템(100)으로 요청 보안코드(11)를 요청할 수 있다(S11). 그러면, 도 5c와 같은 요청 수단이 상기 보안 디지털 시스템(100)에 로딩될 수 있다. 이렇게 요청 보안코드(11)가 요청되면(또는 사용자가 보안코드를 요청하면), 상기 제어모듈(110)은 보안정보 획득 조건이 만족하는지를 판단할 수 있다. 그리고, 만족한다고 판단한 경우, 상기 제어모듈(110)은 상기 페어 시스템(200)으로 요청 보안코드(11)를 요청할 수 있다(S21). 그러면, 상기 보안 디지털 시스템(100)은 요청 보안코드(11)를 상기 페어 시스템(200)으로부터 수신할 수 있다(S31).
- [0249] 그러면, 상기 제어모듈(110)은 전송한 바와 같이 상기 요청 보안코드를 사용자가 획득할 수 있도록 소정의 제어를 수행할 수 있다. 예컨대, 상기 디스플레이 모듈(150)을 통해 요청 보안코드(11)를 디스플레이하거나(S41), 입력 UI(13)에 자동으로 입력하거나, 또는 자동으로 상기 인증 시스템(300)으로 전송할 수도 있다(S51).
- [0250] 그러면, 상기 인증 시스템(300)은 수신된 정보 즉, 상기 요청 보안코드(11)를 이용하여 미리 저장된 정보와 비

교환으로써 인증을 수행할 수 있다.

- [0251] 또한, 전술한 바와 같이 상기 보안 디지털 시스템(100)에 포함된 보안모듈(140)은 보안절차를 수행할 수도 있다 (S61). 즉, 일정한 조건이 되면, 상기 페어 시스템(200)으로부터 수신된 요청 보안코드(11)를 삭제할 수 있다.
- [0252] 한편, 상기 제어모듈(110)이 상기 요청 보안코드(11)만을 상기 페어 시스템(200)에 요청하기 위해서는, 요청 보안코드(11)가 무엇인지를 판단할 수 있어야 한다. 이를 위해 상기 인증 시스템(300)이 요청 보안코드(11)의 요청(S11)과는 별도로 상기 요청 보안코드(11)를 식별할 수 있는 보안코드 식별정보(예컨대, 도 5c의 부재번호 12)를 상기 보안 디지털 시스템(100)으로 더 전송할 수 있다.
- [0253] 또는, 전술한 바와 같이 상기 인증 시스템(300)이 별도의 데이터 프로세싱 장치(400)로 요청 보안코드(11)를 요청하는 경우에는, 상기 데이터 프로세싱 장치(400)에 로딩된 요청 수단(예컨대, 도 5c의 웹 페이지 등)을 보고 사용자가 상기 보안 디지털 시스템(100)으로 상기 보안코드 식별정보(예컨대, 12)를 입력할 수도 있다. 그러면, 상기 제어모듈(110)은 요청 보안코드(11)가 무엇인지를 확인할 수 있다.
- [0254] 또는, 상기 보안 디지털 시스템(100)에 요청 수단이 로딩되면, 상기 제어모듈(110)은 상기 요청 수단을 분석(예컨대, 이미지 분석, 텍스트 인식 등)하여 상기 보안코드 식별정보가 무엇인지를 판단하고, 그에 따라 상기 요청 보안코드(11)가 무엇인지를 판단할 수도 있다.
- [0255] 한편, 상기 제어모듈(110)은 상기 보안 디지털 시스템(100)과 페어를 이루는 상기 페어 시스템(200)이 무엇인지를 특정하기 위한 페어 형성 절차를 거칠 수 있다. 그리고, 이러한 페어 형성 절차를 통해 특정된 상기 페어 시스템(200)과만 페어링이 될 수 있다. 구현 예에 따라서는 상기 제어모듈(110)은 소정의 셀프 인증절차를 수행하고, 상기 셀프 인증절차가 성공하여야 페어링이 될 수도 있다. 페어링이 된다고 함은 전술한 바와 같이 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 통신 상태가 소정의 기준을 만족하는 경우를 의미할 수 있다.
- [0256] 상기 소정의 기준은 전술한 바와 같이 상기 통신모듈(120)과 상기 페어 시스템(200)이 통신가능한 상태인 경우이거나, 또는 상기 통신모듈(120)과 상기 페어 시스템(200)간의 통신 파워 즉, 신호세기가 소정의 세기 이상인 경우일 수 있다. 일반적으로 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 통신거리 이내에 존재하는 경우에 통신이 가능한 상태일 수 있으며, 상기 통신거리 이내에서도 미리 정해진 거리 이내에 존재하는 경우에 페어링이 되었다고 판단할 수도 있다. 또는 상기 소정의 기준은 상기 통신모듈(120)과 상기 페어 시스템(200)에 포함된 소정의 통신장치(예컨대, RF 통신장치 등)가 태깅(tagging)을 수행한 경우일 수도 있다. 상기 태깅은 일정한 거리 이하로 상기 통신모듈(120)과 상기 페어 시스템(200)이 접근하는 경우를 의미할 수 있다. 일반적으로 NFC를 통해 상기 페어 시스템(200) 및 상기 통신모듈(120)이 통신을 하는 경우, 약 10cm 정도의 거리내로 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)을 상기 페어 시스템(200) 또는 상기 보안 디지털 시스템(100)으로 근접시키는 일련의 행위를 포함할 수 있다. 이처럼 태깅이 되면, 상기 제어모듈(110)은 페어링이 되었다고 판단할 수 있다.
- [0257] 어떠한 경우든 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 페어링이 되기 위해서는 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)은 페어 형성 절차를 수행할 수 있다. 물론, 상기 보안 디지털 시스템(100)과 페어를 이루는 유일한 페어 시스템(200)이 미리 결정되어 있는 경우에는 별도의 페어 형성절차는 수행되지 않을 수도 있다. 또는 '알람 페어링' 상태에서는 별도의 추가적인 페어 형성절차는 수행되지 않을 수 있다. 알람 페어링 상태에서의 결제나 보안정보 획득을 위한 페어링 과정과 그 효과에 대해서는 앞에서 충분히 설명한 바 있다.
- [0258] 상기 페어 형성 절차는 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)의 사용자에 의해 수행될 수도 있고, 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)의 제공주체(예컨대, 제조사, 유통사, 금융기관, 보안업체 등)에 의해 미리 수행되어 있을 수도 있다.
- [0259] 사용자에 의해 상기 페어 형성 절차가 수행되는 경우에는, 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)이 자신의 페어가 되는 시스템 즉, 상기 페어 시스템(200) 또는 상기 보안 디지털 시스템(100)에 대한 정보를 통신을 통해 송수신하는 절차를 통해 수행될 수 있다. 또는, 상기 보안 디지털 시스템(100)에 설치된 소정의 애플리케이션을 통해 상기 페어 시스템(200)에 대한 정보가 입력되는 절차를 통해 수행될 수도 있다.
- [0260] 이러한 일 예는 도 3 내지 도 4를 참조하여 설명하도록 한다.
- [0261] 도 3은 본 발명의 일 실시 예에 따라 보안 디지털 시스템 및 페어 시스템이 페어를 형성하는 방식의 일 예를 나

타내는 도면이고, 도 4는 본 발명의 다른 실시 예에 따라 보안 디지털 시스템 및 페어 시스템이 페어를 형성하는 방식의 일 예를 나타내는 도면이다.

- [0262] 먼저, 도 3은 보안 디지털 시스템(100)과 페어 시스템(200)이 통신을 통해 페어 형성 절차를 수행하는 경우를 나타내고, 도 4는 보안 디지털 시스템(100)에 설치될 수 있는 소정의 애플리케이션을 통해 페어 형성 절차를 수행하는 경우를 나타낸다.
- [0263] 먼저, 도 3을 참조하면, 소정의 페어 시스템(200)이 구비될 수 있다. 상기 페어 시스템(200)은 예컨대, 상기 RF 통신이 가능한 RF 통신장치 그 자체이거나, 상기 RF 통신장치에 소정의 구성이 추가된 장치일 수 있다. 또한, 상기 RF 태그는 자신의 식별정보를 보안 디지털 시스템(100)으로 전송할 수도 있다.
- [0264] 어떠한 경우든, 초기에 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)과는 페어를 이루지 않고 있는 상태일 수 있다. 즉, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 관계가 없는 상태로 독자적으로 이용될 수 있다. 물론, 구현 예에 따라서는 페어 형성 절차가 수행되어야 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)이 정상적으로 동작하도록 구현될 수도 있다.
- [0265] 이후, 페어 형성 절차가 수행되기 위해 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 서로 통신을 수행할 수 있다. 또한, 상기 페어 형성 절차를 수행하기 위해서는 미리 사용자가 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)으로 페어 형성 절차의 수행을 요청하는 소정의 신호를 입력할 수도 있다. 이러한 신호가 입력되면 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)은 페어 형성 절차가 수행됨을 미리 알 수 있다. 이후, 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200)이 서로 통신을 할 수 있다. 그러면, 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)으로부터 상기 페어 시스템(200)을 식별할 수 있는 식별정보를 수신할 수 있다. 구현 예에 따라서는 상기 보안 디지털 시스템(100)이 상기 페어 시스템(200)으로 상기 보안 디지털 시스템(100)의 식별정보를 전송할 수도 있다. 또는, 이 두 가지의 과정이 모두 수행될 수도 있다. 그러면, 전송된 상기 페어 시스템(200)의 식별정보 또는 상기 보안 디지털 시스템(100)의 식별정보는 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)에 각각 기록될 수 있다.
- [0266] 이처럼 어느 하나의 시스템에 페어가 되는 다른 시스템의 식별정보가 기록되면, 페어 형성 절차가 완료될 수 있다. 페어 형성 절차가 완료되면, 이후에는 상기 보안 디지털 시스템(100)(또는 상기 페어 시스템(200))은 자신에게 기록된 식별정보에 해당하는 페어 시스템(200)(또는 디지털 시스템(100))과 통신이 가능한 경우, 일정 거리 이내인 경우, 또는 태깅이 되는 경우에 페어링이 될 수 있다.
- [0267] 한편, 이러한 페어 형성 절차를 위해 서로의 식별정보를 송수신하기 위한 통신은 단순히 페어링이 될 수 있는 거리(이하, 페어링 거리) 이내에만 두 시스템이 존재하면 수행될 수도 있지만, 상기 페어링 거리 이내보다 더 근접해야 수행될 수도 있다. 예컨대, 두 시스템이 페어링 거리(즉, 통신가능한 거리 또는 이보다 짧은 소정의 거리)이내에 존재하더라도 페어 형성 절차는 수행되지 않을 수 있다. 예컨대, NFC 태깅 등과 같이 미리 결정된 근접 거리(예컨대, 10cm 등) 이내로 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200)이 근접하여야만 상기 페어 형성 절차가 수행될 수도 있다.
- [0268] 한편, 본 발명의 일 실시 예에 의하면, 상기 페어 시스템(200)과 페어를 형성할 수 있는 디지털 시스템이 한정되어 있을 수도 있다. 예컨대, 상기 페어 시스템(200)이 특정 사용자의 금융 IC 카드인 경우, 상기 페어 시스템(200)과 페어를 이룰 수 있는 시스템은 상기 특정 사용자의 명의의 디지털 시스템만 가능할 수 있다.
- [0269] 즉, 상기 페어 시스템(200)과 페어를 이룰 수 있는 보안 디지털 시스템(100)이 미리 정의되어 있을 수 있다. 이처럼 상기 보안 디지털 시스템(100)에 포함된 제어모듈(110)이 상기 보안 디지털 시스템(100)이 상기 페어 시스템(200)과 페어를 이룰 수 있는 시스템인지를 스스로 확인하는 절차를 셀프 인증절차로 정의할 수 있다.
- [0270] 셀프 인증절차를 수행하기 위해 상기 제어모듈(110)은 상기 인증 시스템(300) 또는 상기 페어 시스템(200)에 저장된 정보를 이용할 수 있다. 즉, 상기 페어 시스템(200)과 페어 가능한 보안 디지털 시스템(100)을 식별할 수 있는 정보는 상기 인증 시스템(300) 또는 상기 페어 시스템(200)에 저장될 수 있다.
- [0271] 예컨대, 상기 제어모듈(110)은 상기 보안 디지털 시스템(100)에 저장된 사용자 식별정보(예컨대, 이름, 전화번호 등) 또는 기기 식별정보(예컨대, 특정 하드웨어의 시리얼 넘버 등)를 파악할 수 있다. 그러면, 상기 제어모듈(110)은 파악된 정보가 상기 인증 시스템(300)에 저장된 정보와 상응하는지를 파악할 수 있다. 예컨대, 상기 인증 시스템(300)에는 사용자 식별정보(예컨대, 전화번호) 또는 기기 식별정보 및 이에 대응되는 소유주 정보가 저장되어 있을 수 있다. 그러면, 상기 사용자 식별정보를 이용하여 상기 보안 디지털 시스템(100)의 소유주가 누구인지를 파악할 수 있으며, 파악한 결과에 기초하여 상기 제어모듈(110)은 상기 보안 디지털 시스템(100)이

상기 페어 시스템(200)과 페어를 형성할 수 있는지 여부를 판단할 수 있다. 만약, 상기 페어 시스템(200)에 사용자를 특정할 수 있는 정보가 존재하는 경우, 상기 제어모듈(110)은 상기 정보와 상기 소유주 정보가 서로 상응하는지를 판단하는 셀프 인증절차를 수행할 수 있다. 상기 보안 디지털 시스템(100)에 상기 보안 디지털 시스템(100)의 소유주를 식별할 수 있는 소유주 정보(예컨대, 이름, 별칭 등)가 저장되어 있는 경우, 상기 제어모듈(110)은 상기 소유주 정보와 상기 페어 시스템(200)에 저장된 소유주 식별정보를 비교함으로써 셀프 인증절차를 수행할 수도 있다.

[0272] 이처럼 수행된 셀프 인증절차가 성공하면, 최종적으로 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 페어를 형성할 수 있다.

[0273] 한편, 도 4를 참조하면, 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)에 페어가 되는 시스템의 식별정보가 직접 입력됨으로써 페어 형성 절차가 수행될 수 있다.

[0274] 일 실시 예에 의하면, 상기 보안 디지털 시스템(100)에는 본 발명의 기술적 사상을 구현하기 위한 소정의 애플리케이션(30)이 설치될 수 있다. 상기 애플리케이션은 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)의 제공주체 또는 활용주체가 운영하는 소정의 웹 서버 등에서 다운로드 가능할 수 있다.

[0275] 사용자는 상기 애플리케이션(30)을 실행시킬 수 있으며, 그러면 도 4에 도시된 바와 같은 UI가 사용자에게 제공될 수 있다. 그러면, 사용자는 상기 UI를 통해 상기 보안 디지털 시스템(100)과 페어가 되는 페어 시스템(200)의 식별정보를 입력할 수 있다. 입력된 식별정보는 소정의 저장장치에 저장될 수 있으며, 상기 통신모듈(120)은 저장된 상기 식별정보를 확인할 수 있다.

[0276] 예컨대, 상기 보안 디지털 시스템(100)이 모바일 폰이고, 상기 페어 시스템(200)이 상기 보안 디지털 시스템(100)과 페어링 될 수 있는 스마트카드인 경우가 존재할 수 있다. 이러한 경우, 상기 보안 디지털 시스템(100)은 상기 스마트카드를 제공하는 카드사나 금융기관의 웹 사이트에 또는 소정의 앱 스토어(app store) 등에서 상기 애플리케이션(30)을 다운로드 할 수 있다. 그러면, 상기 보안 디지털 시스템(100)의 사용자는 상기 애플리케이션(30)을 실행한 후, 상기 스마트카드의 식별정보를 입력함으로써 페어 형성 절차를 수행할 수 있다.

[0277] 한편, 구현 예에 따라서는 상기 페어 시스템(200) 역시 소정의 애플리케이션이 구동 가능한 시스템일 수 있다. 이러한 경우에는 상기 페어 시스템(200)에 설치되어 실행될 수 있는 소정의 애플리케이션을 통해 상기 보안 디지털 시스템(100)의 식별정보가 입력됨으로써 페어 형성 절차가 수행될 수도 있음은 물론이다.

[0278] 이처럼 사용자에 의해 페어 형성 절차가 수행되는 경우에는, 사용자는 자신의 보안 디지털 시스템(100)과 페어를 이루는 페어 시스템(200)을 선택할 수 있으며, 본 발명의 기술적 사상을 구현할 수 있는 페어 시스템(200)을 복수 개 가지고 있는 경우에는 상기 보안 디지털 시스템(100)과 페어를 이루는 페어 시스템(200)을 변경할 수도 있고, 복수 개를 페어 시스템으로 이용할 수도 있다.

[0279] 한편, 상기 보안 디지털 시스템(100) 또는 상기 페어 시스템(200)의 제공주체에 의해 미리 페어가 되는 시스템이 결정되어 있을 수도 있다. 이러한 경우에는 상기 보안 디지털 시스템(100)에 상기 페어 시스템(200)에 대한 정보가 미리 저장되어 있거나, 상기 페어 시스템(200)에 상기 보안 디지털 시스템(100)에 대한 정보가 미리 저장되어 사용자에게 판매 또는 유통될 수 있다. 구현 예에 따라 상기 제공주체는 상기 보안 디지털 시스템(100) (또는 페어 시스템(200))을 사용자에게 판매 또는 유통하면서, 상기 페어 시스템(200)(또는 디지털 시스템(100))을 같이 판매 또는 유통할 수 있다. 특히, 클라우드 시스템으로 고객이나 커뮤니티를 관리하거나, 더 나아가 본 발명의 기술적 사상을 활용하여 인증이나 결제 관련 비즈니스를 진행하고자 하는 제조사나 유통사의 경우에는 더욱 그러할 수 있다. 또한 알람 페어링이 먼저 이루어지고 알람 페어링 상태에서 본 발명의 기술적 사상에 의한 보안정보 획득을 위한 페어링이 이루어지는 경우에는, 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200) 각각의 페어가 되는 시스템이 유통이나 제조단계에서 미리 결정되어 있을 가능성이 더욱 높다.

[0280] 한편, 상기 보안 디지털 시스템(100)에 의해 사용자가 획득하는 보안정보가 OTP 인 경우, 상기 제어모듈(110)은 상기 페어 시스템(200)에 의해 생성된 OTP를 수신할 수도 있고, 상기 페어 시스템(200)으로부터 OTP 생성에 필요한 정보를 수신한 후, 상기 제어모듈(110)이 직접 상기 OTP를 생성할 수도 있다. 그러면, 생성된 OTP를 사용자가 획득할 수 있도록 할 수 있다. OTP를 획득할 수 있도록 하는 경우도 역시, 상기 OTP를 소정의 디스플레이 모듈(150)로 출력하여 디스플레이하거나, OTP를 입력할 수 있는 소정의 입력 UI에 자동으로 입력하거나, 또는 생성된 OTP를 인증 시스템(300)으로 전송하는 경우를 포함할 수 있다.

[0281] 이러한 일 예는 도 6을 참조하여 설명하도록 한다.

- [0282] 도 6은 본 발명의 실시 예에 따른 보안 디지털 시스템에 의해 OTP가 획득되는 방법을 설명하기 도면이다.
- [0283] 도 6을 참조하면, 상기 제어모듈(110)은 보안정보 획득 조건이 만족하는지 여부를 판단하고, 자동으로 또는 사용자로부터 입력되는 OTP 생성요청에 응답하여(S12), 상기 페어 시스템(200)으로 상기 OTP 생성에 필요한 생성 정보를 요청할 수 있다(S22).
- [0284] 상기 생성정보는 상기 페어 시스템(200)에 저장된 OTP 정보(20) 중 적어도 일부일 수 있다. 상기 OTP 정보(20)는 OTP 생성프로그램 정보(21) 및/또는 제10TP 생성키(22)를 포함할 수 있다.
- [0285] 일 실시 예에 의하면, 상기 제어모듈(110)은 상기 페어 시스템(200)으로부터 상기 제10TP 생성키(22)를 수신할 수 있다(S32). 한편, 상기 OTP 생성프로그램 정보(21)는 상기 보안 디지털 시스템(100)에 저장되어 있을 수 있다.
- [0286] 상기 보안 디지털 시스템(100)에 저장된 OTP 생성프로그램 정보(21)는 상기 정보를 요청(S22)하기 전에 미리 상기 보안 디지털 시스템(100)에 저장되어 있을 수 있으며, 상기 보안 디지털 시스템(100)은 인증 시스템(300)으로부터 상기 OTP 생성프로그램 정보(21)를 미리 수신해둘 수도 있다.
- [0287] 그러면, 상기 제어모듈(110)은 상기 OTP 생성프로그램 정보(21) 및 상기 페어 시스템(200)으로부터 수신하는 제10TP 생성키(22)를 이용하여 OTP를 생성할 수 있다(S42). 생성된 상기 OTP는 인증 시스템(300)으로 전송될 수 있다. 또한, 인증 시스템(300)은 자신이 보유하고 있던 상기 OTP 생성프로그램 정보(21) 및 상기 제10TP 생성키(22)를 이용하여 별도로 OTP를 생성하고, 자신이 생성한 OTP와 상기 보안 디지털 시스템(100)으로부터 수신한 OTP를 비교하여 인증을 수행할 수 있다.
- [0288] 상기 보안모듈(140)은 생성된 OTP를 일정 조건에 따라 삭제하는 보안절차를 수행할 수 있다(S52).
- [0289] 다른 실시 예에 의하면, 상기 제어모듈(110)이 생성정보를 상기 페어 시스템(200)으로 요청하면(S22), 상기 페어 시스템(200)은 상기 OTP 생성프로그램 정보(21)를 더 상기 보안 디지털 시스템(100)으로 전송할 수도 있다(S32-1).
- [0290] 그러면, 상기 제어모듈(110)은 상기 페어 시스템(200)으로부터 수신한 상기 OTP 생성프로그램 정보(21) 및 상기 제10TP 생성키(22)를 이용하여 상기 OTP를 생성할 수도 있다(S42).
- [0291] 한편, 본 발명의 기술적 사상에 의하면, 상기 보안 디지털 시스템(100)은 제20TP 생성키(23)를 더 이용하여 OTP를 생성할 수도 있다. 상기 제20TP 생성키(23)는 상기 인증 시스템(300)과 공유하고 있는 비밀키일 수 있다.
- [0292] 그러면, 상기 제어모듈(110)은 상기 페어 시스템(200)으로부터 상기 제10TP 생성키(22)를 수신하고, 상기 보안 디지털 시스템(100)으로부터 획득할 수 있는 상기 제20TP 생성키(23)를 이용하여 상기 OTP를 생성할 수 있다. 이러한 경우, OTP 생성프로그램(21)은 상기 제20TP 생성키(23)를 추가로 입력변수로 이용하여 상기 OTP를 생성할 수 있다. 구현 예에 따라서는, 상기 제10TP 생성키(22) 및 상기 제20TP 생성키(23)를 이용하여 어느 하나의 새로운 키를 생성하고, 상기 키를 입력변수로 하여 상기 OTP를 생성할 수도 있다. 물론, 이때에는 상기 인증 시스템(300)도 상기 제10TP 생성키(22) 및 상기 제20TP 생성키(23)를 이용하여 상기 제어모듈(110)이 생성하는 상기 새로운 키와 동일한 키를 생성할 수 있어야 하는 것이 바람직하다.
- [0293] 상기 제20TP 생성키(23)는 미리 상기 인증 시스템(300)과 공유된 비밀키일 수 있다. 일 실시 예에 의하면, 상기 제20TP 생성키(23)는 상기 보안 디지털 시스템(100)의 유니크한 식별정보에 기초하여 소정의 알고리즘을 통해 생성될 수 있으며, 상기 인증 시스템(300) 또는 상기 보안 디지털 시스템(100) 중 적어도 하나에 의해 생성될 수 있다.
- [0294] 이처럼 제20TP 생성키(23)도 이용하여 상기 OTP를 생성하는 경우에는, OTP를 생성하기 위해 알아야 하는 비밀키가 늘어나서 보안성이 현저히 증가할 수 있다. 또한, 어느 하나의 비밀키(예컨대, 제10TP 생성키(22) 또는 제20TP 생성키(23))가 유출되더라도 유출된 하나의 비밀키만으로는 상기 인증 시스템(300)과 동일한 OTP를 생성할 수 없게 되는 효과가 있다.
- [0295] 이처럼 다양한 방식으로 상기 OTP가 상기 보안 디지털 시스템(100)에 의해 생성되어 사용자에게 획득될 수 있다.
- [0296] 또한, 다른 실시 예에 의하면, 상기 페어 시스템(200)이 자신이 저장하고 있는 OTP 생성프로그램 정보(21) 및 제10TP 생성키(22)를 이용하여 OTP를 생성할 수도 있다. 이런 경우, 상기 제어모듈(110)은 상기 페어 시스템(200)에 의해 생성된 OTP를 수신할 수도 있다. 물론, 이러한 경우에도 보안정보 획득 조건이 만족하는 경우에만

상기 OTP를 수신할 수 있음은 물론이다.

- [0297] 한편, 상기 보안 디지털 시스템(100)이 상기 OTP를 생성하기 위해 상기 페어 시스템(200)으로부터 생성정보(즉, OTP 생성프로그램 정보(21) 및/또는 제1OTP 생성키(22))를 수신하는 경우에는 상기 생성정보는 가급적 상기 보안 디지털 시스템(100)에 저장되지 않는 것이 바람직할 수 있다.
- [0298] 이를 위해 보안모듈(140)은 상기 생성정보를 일정한 조건이 되면 상기 보안 디지털 시스템(100)에서 삭제함으로써 보안절차를 수행할 수 있음은 전술한 바와 같다.
- [0299] 이러한 보안절차의 개략적인 과정은 도 7에 도시된다.
- [0300] 도 7은 본 발명의 실시 예에 따라 보안 디지털 시스템이 보안절차를 수행하는 과정을 설명하기 위한 개략적인 플로우 차트이다.
- [0301] 도 7을 참조하면, 상기 보안 디지털 시스템(100)은 인증 시스템(300)으로부터 요청 보안코드(11) 또는 OTP 즉, 보안정보를 요청받을 수 있다. 그러면, 상기 보안 디지털 시스템(100)에는 소정의 요청 수단(예컨대, 도 5c에 도시된 바와 같은 웹 페이지, 또는 소정의 애플리케이션, 프레임, UI 등)이 로딩될 수 있다(S13).
- [0302] 그러면, 상기 제어모듈(110)은 상기 페어 시스템(200)으로부터 상기 보안정보(예컨대, 보안코드)의 적어도 일부 또는 상기 보안정보(예컨대, OTP)를 생성하기 위한 생성정보(예컨대, 제1OTP 생성키(22) 및/또는 OTP 생성프로그램 정보(21))를 요청하고, 수신할 수 있다(S23).
- [0303] 이처럼 수신된 정보는 상기 보안 디지털 시스템(100)에 의해 사용되고 나면, 상기 보안 디지털 시스템(100)에는 저장되지 않는 것이 보안상 유리할 수 있다.
- [0304] 이를 위해 상기 보안모듈(140)은 수신된 정보가 수신된 시점으로부터 일정 시간이 경과했는지를 판단하고(S33), 판단결과 상기 일정 시간이 경과했다고 판단하면 상기 수신된 정보를 삭제할 수 있다(S53).
- [0305] 다른 실시 예에 의하면, 상기 보안모듈(140)은 상기 요청 수단이 비활성화되는지 여부를 판단할 수도 있다(S43). 판단결과 상기 요청 수단이 비활성화되었다고 판단되면, 상기 보안모듈(140)은 상기 수신된 정보를 삭제할 수 있다(S53). 상기 요청 수단이 비활성화되는 경우 즉, 상기 수신된 정보를 삭제할 경우나 조건은 미리 상기 보안모듈(140)에 의해 정의될 수 있음은 전술한 바와 같다.
- [0306] 상술한 바와 같은 방식으로 사용자는 인증에 필요한 보안정보를 상기 보안 디지털 시스템(100)을 통해 획득할 수 있다. 또한, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 비접촉 통신을 수행할 수 있다.
- [0307] 따라서, 상기 페어 시스템(200)이 상기 사용자의 지갑에 보관되고 있는 경우라도, 상기 사용자는 간편하게 자신이 사용하고 있는 보안 디지털 시스템(100)을 통해 상기 보안정보를 획득할 수 있다. 따라서, 상기 페어 시스템(200)을 상기 사용자의 지갑에서 꺼낼 필요가 없는 효과가 있다.
- [0308] 한편, 본 발명의 실시 예에 따른 상기 보안 디지털 시스템(100)은 알람모듈(130)을 더 포함할 수 있다.
- [0309] 상기 알람모듈(130)은 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 비 페어링 상태인 경우(즉, 일정 거리 이상 떨어지는 경우), 알람신호를 출력할 수 있다.
- [0310] 이러한 일 예는 도 9를 참조하여 설명하도록 한다.
- [0311] 도 9는 본 발명의 실시 예에 따라 디지털 시스템 또는 페어 시스템이 알람신호를 출력하는 개념을 설명하기 위한 도면이다.
- [0312] 도 9를 참조하면, 상기 보안 디지털 시스템(100)에 포함된 상기 제어모듈(110)은 상기 페어 시스템(200)과 페어링이 유지되고 있는지를 판단할 수 있다(S14). 즉, 상기 제어모듈(110)은 알람 페어링 상태인지 여부를 확인할 수 있다. 물론, 알람 페어링 기능은 사용자의 요청에 의해 활성화되거나 비활성화 될 수도 있다.
- [0313] 알람 페어링 상태에서 소정의 이벤트가 발생하면(예컨대, 사용자로부터 요청이 입력되면), 상기 제어모듈(110)은 전술한 바와 같은 방식으로, 즉 상기 페어 시스템(200)으로부터 OTP 생성에 필요한 생성정보를 수신하여 OTP를 생성할 수 있다(S24). 구현 예에 따라서는 상기 보안 디지털 시스템(100)이 OTP 정보(40)를 저장하고 있으며, 상기 OTP 정보(40)를 이용하여 OTP를 생성할 수도 있다. 이때 상기 OTP 정보(40)는 OTP 생성프로그램 정보 및 제2OTP 생성키를 포함할 수 있다. 결국, 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)과는 무관하게 독립적으로 OTP를 생성할 수 있는 장치일 수도 있다. 이러한 경우에도 상기 보안 디지털 시스템(100)

은 보안정보 획득 조건이 만족하는 경우에만 상기 OTP를 생성할 수 있도록 구현될 수 있다.

- [0314] 한편, 페어링 상태(즉, 알람 페어링 상태)가 유지되다가, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 비페어링 상태가 되는 경우 또는 일정 거리 이상 두 시스템(100, 200)이 멀어지는 경우, 알람 출력 조건이 만족할 수 있다. 그러면, 상기 제어모듈(110)은 상기 알람모듈(130)을 제어하여 소정의 알람신호를 출력하도록 할 수 있다(S34). 구현 예에 따라서는, 상기 페어 시스템(200) 역시 소정의 알람신호를 출력할 수도 있다(S34-1).
- [0315] 상기 페어 시스템(200) 역시 상기 보안 디지털 시스템(100)과 페어링 상태(즉, 알람 페어링 상태)가 유지되는지 여부를 주기적으로 판단할 수도 있다. 예컨대, 주기적으로 상기 보안 디지털 시스템(100)과 소정의 신호를 수신하다가, 더 이상 상기 신호가 수신되지 않으면 상기 페어 시스템(200)은 알람 출력 조건이 만족했다고 판단하고 알람신호를 출력할 수도 있다.
- [0316] 물론, 이러한 경우에는 상기 페어 시스템(200)과 상기 보안 디지털 시스템(100)간의 통신 프로토콜은 동일한 사용자가 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)을 보유하고 있는 경우에는 통신이 가능한 통신 프로토콜일 수 있다.
- [0317] 한편, 전술한 바와 같이 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)은 페어링이 되고 있는지와는 무관하게, 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200)이 일정 거리 이상 떨어졌다고 판단한 경우에 상기 알람신호를 출력할 수도 있다.
- [0318] 예컨대, 상술한 바와 같이 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 제1거리(예컨대, 10cm) 내에서만 페어링 될 수 있고, 알람신호는 제2거리(예컨대, 수 미터) 이상 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 떨어지는 경우 출력될 수도 있다.
- [0319] 일 실시 예에 의하면, 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)이 알람 페어링 기능을 제공하며, 상기 보안 디지털 시스템(100) 또는 상술한 바와 같이 알람 페어링으로 그 기준 거리를 일정거리(예컨대, 10미터) 이상으로 하고, 보안정보 획득을 위한 페어링 기준 거리를 보다 좁은 거리(예컨대, 1미터, NFC의 경우 10센티미터)로 달리 설정하고, 알람 페어링의 기준 거리를 벗어나는 경우에만 알람신호를 출력할 수도 있다.
- [0320] 알람 페어링 기능이 비활성화되어 있는 상태 또는 상기 알람 페어링 기능이 제공되지 않는 경우에는, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 알람 출력 조건을 만족하는 경우에도 알람신호가 출력되지 않는 점을 제외하고는 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 동일 또는 유사한 동작을 수행할 수 있다.
- [0321] 도 8은 본 발명의 실시 예에 따른 페어 시스템의 개략적인 구성을 나타내는 도면이다.
- [0322] 도 8을 참조하면, 상기 페어 시스템(200)은 보안코드 및/또는 OTP 정보 중 적어도 하나를 저장하는 저장장치(211) 및 상기 보안 디지털 시스템(100)에 구비된 통신모듈(120)과 통신을 수행할 수 있는 통신장치(220)를 포함할 수 있다.
- [0323] 구현 예에 따라, 상기 페어 시스템(200)은 스스로 데이터 처리 능력을 가질 수 있으며, 이러한 경우에는 소정의 제어장치(212)가 더 구비될 수도 있다.
- [0324] 일 실시 예에 의하면, 상기 페어 시스템(200)은 상기 저장장치(211) 및 상기 제어장치(212)를 포함하는 스마트 카드로 구현될 수도 있다. 이러한 경우, 상기 페어 시스템(200)은 상기 스마트 카드는 종래의 제어장치(212) 및 저장장치(211)에 본 발명의 기술적 사상을 구현하기 위한 통신장치(220)가 더 구비되는 시스템일 수도 있다.
- [0325] 한편, 다른 실시 예에 의하면, 상기 페어 시스템(200)에는 상기 보안코드 및 상기 OTP 정보는 저장되어 있지 않을 수도 있다. 즉, 상기 페어 시스템(200)은 단순히 상기 보안 디지털 시스템(100)과 페어를 형성하는 기능만 수행할 수도 있다. 이러한 경우에는 상기 제어장치(212) 및/또는 상기 저장장치(211) 중 적어도 하나는 상기 페어 시스템(200)에 포함되지 않을 수도 있다.
- [0326] 예컨대, 상기 페어 시스템(200)은 통신장치(예컨대, RF 통신장치 등, 220)를 포함할 수 있다. 구현 예에 따라서는 상기 통신장치(예컨대, RF 통신장치 등, 220) 자체가 상기 페어 시스템(200)일 수 있다. 일 실시 예에 의하면, 상기 통신장치(예컨대, RF 통신장치 등, 220)는 소정의 RF 안테나를 포함할 수 있다.
- [0327] 상기 통신장치(220)는 예컨대, RFID 태그로 구현될 수도 있다. 구현 예에 따르면, 상기 페어 시스템(200) 자체

가 상기 RFID 태그일 수도 있다. 다른 실시 예에 의하면, 상기 통신장치(220)는 RF 리더기를 포함할 수도 있다. 어떠한 경우든 상기 통신장치(220)는 보안 디지털 시스템(100)에 포함된 통신모듈(120)과 통신을 수행할 수 있도록 구현될 수 있다.

- [0328] 한편, 본 발명의 실시 예에 따른 상기 디지털 시스템(100) 또는 상기 페어 시스템(200)은 페어링이 되지 않은 경우에도 보안정보를 생성할 수 있다. 즉, 한정된 상황에서는 페어링이 되지 않아도 사용자가 보안정보를 획득하도록 할 수도 있다. 이를 위해서는 소정의 추가 인증이 수행되어야 할 필요가 있을 수 있다.
- [0329] 따라서, 사용자가 의식적으로 또는 무의식적으로 상기 보안 디지털 시스템(100) 및 상기 페어 시스템(200)을 페어링 거리 이내로 모두 점유하고 있지 않은 경우는, 한정된 조건 즉, 추가 인증이 성공하는 조건 하에 보안정보를 사용자에게 획득하도록 허락할 수도 있다.
- [0330] 상기 추가 인증은 페어링이 되지 않은 경우에는, 상기 추가 인증이 수행되어 성공되어야만 상기 보안정보 획득 절차를 수행할 수 있도록 하는 모든 형태의 인증을 포함할 수 있다. 예컨대, 비밀번호를 통한 인증, 비밀패턴을 이용한 인증, 생체정보(예컨대, 지문, 홍채 등)를 이용한 인증, 위치정보나 하드웨어의 고유한 식별정보에 의한 인증, 및/또는 공인인증서 등 중 적어도 하나가 상기 추가 인증으로 이용될 수도 있다. 그 밖에 추가 인증의 방법은 더 다양할 수 있다.
- [0331] 또한, 본 발명의 실시 예에 따른 상기 디지털 시스템(100) 및/또는 상기 페어 시스템(200)은 페어링이 되지 않는 경우 또는 소정의 거리 이상에 상기 디지털 시스템(100) 및 상기 페어 시스템(200)이 위치하는 경우에는 사용자가 이를 인식할 수 있도록 소정의 알람신호를 출력하기 위한 수단을 더 포함할 수 있다.
- [0332] 한편, 본 발명의 기술적 사상에 의하면, 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)은 복수의 보안정보 또는 보안정보를 생성하기 위한 생성정보를 저장하고 있을 수도 있다.
- [0333] 예컨대, 상기 페어 시스템(200)은 복수의 보안코드들 또는 상기 OTP 정보를 포함하는 복수의 OTP 정보들을 저장하고 있을 수 있다. 이러한 경우는, 상기 페어 시스템(200)이 종래의 복수의 보안카드 또는 복수의 OTP 생성장치의 역할을 통합적으로 수행할 수 있음을 의미할 수 있다. 복수의 보안코드들 또는 상기 복수의 OTP 정보들은 각각 서로 다른 주체가 이용하거나 배포하는 보안코드일 수 있다. 예컨대, 금융기관 1과 금융기관 2는 서로 다른 보안카드를 이용할 수 있다. 또는 서로 다른 OTP 생성장치를 이용할 수 있다.
- [0334] 이러한 경우, 상기 페어 시스템(200)은 서로 다른 보안카드들 또는 서로 다른 OTP 생성장치에 대응되는 보안코드들 또는 OTP 정보들을 저장하고 있을 수 있다.
- [0335] 그러면, 상기 보안 디지털 시스템(100)에 포함된 제어모듈(110)은 사용자로부터 상기 복수의 보안코드들 중 특정 보안코드(예컨대, 금융기관 1에서 사용되는 보안코드)를 선택하는 보안코드 선택신호가 입력되거나, 상기 보안코드에 대응되는 애플리케이션(예컨대, 금융기관 1에 의해 배포된 애플리케이션)이 상기 보안 디지털 시스템에 의해 실행되면, 상기 복수의 보안코드들 중 상기 보안코드가 선택될 수 있다. 그러면, 선택된 상기 보안코드의 적어도 일부를 수신하도록 상기 제어모듈(110)은 제어를 수행할 수 있다. 또는, 상기 사용자로부터 상기 복수의 OTP 정보들(예컨대, 금융기관 1 또는 2에서 사용되는 OTP 정보들) 중 특정 OTP 정보(예컨대, 금융기관 1에서 사용)를 선택하는 OTP 정보 선택신호가 입력되거나 상기 OTP 정보에 대응되는 애플리케이션(예컨대, 금융기관 1에 의해 배포된 애플리케이션)이 상기 보안 디지털 시스템에 의해 실행되면, 상기 복수의 OTP 정보들 중 상기 OTP 정보의 적어도 일부를 수신하거나 상기 OTP 정보에 기초하여 생성된 상기 OTP를 수신하도록 제어할 수 있다.
- [0336] 도 10은 본 발명의 일 실시 예에 따른 보안 디지털 시스템이 페어 시스템과 태깅을 수행하여 보안정보를 획득하는 경우의 일 예를 나타내는 도면이다.
- [0337] 도 10을 참조하면, 상기 보안 디지털 시스템(100)은 한 번의 태깅을 수행(S15)하여 상기 페어 시스템(200)으로부터 원하는 보안정보(예컨대, 보안코드 전체 또는 요청 보안코드, OTP)를 수신할 수 있다(S25). 또는, 상기 보안정보를 생성하기 위한 생성정보 즉, OTP 정보의 적어도 일부를 수신할 수 있다(S25).
- [0338] 또한, 상기 태깅이 수행되면(S15) 자동으로 페어 인증 절차가 수행되고, 페어 인증 절차가 성공되지 않으면 상기 보안 디지털 시스템(100)은 보안정보 또는 생성정보를 수신할 수 없을 수도 있다.
- [0339] 보안코드 전체를 수신하는 경우에는 태깅(S15)이 수행되는 동안, 상기 페어 시스템(200)은 보안코드 전체를 상기 보안 디지털 시스템(100)으로 전송하는 과정이 수행될 수 있다. 보안코드 일부를 수신하는 경우에는 태깅(S15)이 수행되는 동안, 상기 보안 디지털 시스템(100)은 요청 보안코드 식별정보를 전송하고, 전송된 정보에

기초하여 상기 페어 시스템(200)에 저장된 보안코드 중 상기 요청 보안코드가 추출되고, 추출된 요청 보안코드가 상기 보안 디지털 시스템(100)에 의해 수신되는 과정이 수행될 수 있다. OTP 정보의 적어도 일부를 상기 보안 디지털 시스템(100)이 수신하는 경우에는 상기 태깅(S15)이 수행되는 동안, OTP 정보의 적어도 일부가 상기 보안 디지털 시스템(100)에 의해 수신될 수 있다. 그러면, OTP 생성은 상기 보안 디지털 시스템(100)에 의해 수행되는데, 이러한 경우는 상기 태깅이 수행(S15)되는 동안일 수도 있고, 태깅이 수행(S15)된 후일 수도 있다. 상기 보안 디지털 시스템(100)이 OTP를 수신하는 경우에는 상기 태깅이 수행(S15)되는 동안, OTP 생성요청신호가 상기 페어 시스템(200)으로 전송되고, 전송에 응답하여 상기 페어 시스템(200)이 OTP를 생성하며, 생성된 OTP가 상기 보안 디지털 시스템(100)으로 전송되는 과정이 수행될 수 있다. 상기 OTP 생성요청 신호는 태깅 행위 자체일 수도 있고, 별도로 상기 보안 디지털 시스템(100)으로부터 상기 페어 시스템(200)으로 전송되는 신호일 수도 있다.

[0340] 한편, 전송한 바와 같이 태깅 즉, NFC 통신을 통해 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 통신을 수행하는 경우에는 복수 번의 태깅이 수행되어야 사용자는 원하는 보안정보를 획득할 수도 있다. 이러한 일 예는 도 11 내지 도 12를 참조하여 설명하도록 한다.

[0341] 도 11 내지 도 12는 본 발명의 일 실시 예에 따른 보안 디지털 시스템이 복수의 태깅을 수행하여 보안정보를 획득하는 경우의 일 예를 나타내는 도면이다.

[0342] 도 11 내지 도 12는 두 번의 태깅을 통해 보안정보를 획득하는 경우를 예시적으로 나타내지만, 본 발명의 권리 범위가 이에 한정되지는 않는다.

[0343] 먼저, 도 11을 참조하면, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 제1태깅을 수행할 수 있다(S16). 상기 제1태깅이 수행(S16)되는 동안 또는 수행된 후 페어 인증절차(S26)가 수행될 수 있다. 페어 인증절차가 성공(또는 실패)하면, 다음 태깅 즉, 제2태깅때 미리 정의된 프로세스가 수행될 수 있음(또는 없음)을 나타내는 소정의 정보가 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)에 기록될 수도 있다.

[0344] 이후, 제2 태깅이 수행되면(S36), 상기 제2태깅이 수행되는 동안 보안코드의 적어도 일부, OTP 정보의 적어도 일부, 또는 OTP가 상기 보안 디지털 시스템(100)으로 전송될 수 있다(S46). 또한, 제2태깅이 수행된 후, 소정의 프로세스 예컨대, 수신된 OTP 정보의 적어도 일부에 기초하여 OTP 생성이라는 프로세스가 상기 보안 디지털 시스템(100)에 의해 수행될 수도 있다.

[0345] 도 12를 참조하면, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)은 제1태깅을 수행할 수 있다(S17). 그러면, 상기 보안 디지털 시스템(100)은 요청 보안코드를 특정할 수 있는 정보 또는 OTP 생성요청 신호를 상기 페어 시스템(200)으로 전송할 수 있다(S27). 또한, 상기 제1태깅이 수행(S17)되는 동안 또는 후에 페어 인증절차가 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)에 의해 수행될 수도 있다. 구현 예에 따라서는 상기 제1태깅 전에 별도의 태깅을 통해 상기 페어 인증절차가 수행될 수도 있다.

[0346] 그러면, 상기 페어 시스템(200)은 요청 보안코드를 추출하거나 OTP를 생성할 수 있다(S37). 이러한 과정은 상기 제1태깅이 수행되는 동안(S17) 또는 그 후에 수행될 수 있다.

[0347] 이후, 제2태깅이 수행되면(S47), 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)으로부터 요청 보안코드 또는 OTP를 수신할 수 있다(S57).

[0348] 구현 예에 따라서는 상기 제1태깅이 수행되면(S17), OTP 정보의 적어도 일부를 요청하는 신호가 상기 페어 시스템(200)으로 전송되고, 상기 제2태깅이 수행되면(S47), OTP 정보의 적어도 일부가 상기 보안 디지털 시스템(100)으로 전송될 수도 있다.

[0349] 한편, 복수의 태깅이 수행되어야 상술한 바와 같은 보안정보가 획득될 수 있는 경우, 상기 복수의 태깅 중 각각의 태깅이 수행되는 동안 또는 후에 수행될 프로세스는 미리 정의될 수 있으며, 각각의 태깅이 수행되는 동안 또는 후에 어떠한 프로세스가 수행될지는 구현 예에 따라 다양하게 정의될 수 있음은 물론이다. 일 실시 예에 의하면 특정 태깅이 수행되는 경우에는 보안정보를 획득하기 위해 수행되어야 할 프로세스 중 어떠한 프로세스도 실질적으로 수행되지 않을 수도 있다. 또한, 필요한 경우에는 일정 시간 동안 몇 번의 태깅이 수행되었는지를 카운트하는 정보가 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)에 기록 및/또는 유지될 수도 있다. 물론, 일정 시간 내에 수행되는지 여부를 판단하기 위한 소정의 타이머가 상기 보안 디지털 시스템(100) 및/또는 상기 페어 시스템(200)에 구비될 수도 있다.

[0350] 도 14는 본 발명의 실시 예에 따른 인증 시스템의 개략적인 구성을 나타내는 도면이다.

- [0351] 도 2 및 도 14를 참조하면, 본 발명의 일 실시 예에 따른 보안 디지털 시스템(100)은 OTP(또는 인증정보)를 이용해 인증 요청자를 인증할 수 있다. 이때 상기 OTP(또는 인증정보)는 인증 시스템(300)에 의해 생성될 수도 있다.
- [0352] 이를 위해 상기 보안 디지털 시스템(100)은 제어모듈(110) 및 통신모듈(120)을 포함할 수 있다. 상기 통신모듈(120)은 상기 페어 시스템(200)과 NFC 통신을 수행할 수 있다. 즉, 적어도 한 번 태깅을 통해 상기 통신모듈(120)은 상기 페어 시스템(200)으로부터 소정의 정보(예컨대, OTP 정보 중 적어도 일부 및/또는 상기 페어 시스템(200)의 식별정보)를 수신할 수 있다.
- [0353] 상기 제어모듈(110)은 상기 보안 디지털 시스템(100)과 페어를 이루도록 미리 상기 보안 디지털 시스템(100)에 저장된 상기 페어 시스템(200)의 식별정보에 상응하는 상기 페어 시스템(200)과 상기 보안 디지털 시스템(100)이 적어도 한 번 태깅하는지를 판단할 수 있다. 즉, 페어로 형성된 페어 시스템(200)과 적어도 한 번 태깅되는지를 판단할 수 있다. 그리고 판단결과 페어로 형성된 상기 페어 시스템(200)과 적어도 한 번 태깅되어야, 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템(200)의 식별정보를 상기 인증 시스템(300)으로 전송하도록 제어할 수 있다.
- [0354] 일 실시 예에 의하면, 상기 제어모듈(110)은 적어도 한 번 태깅을 수행한 페어 시스템(200)이 미리 페어로 형성되어 있는 시스템이 아닌 경우에는, 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템(200)의 식별정보를 수신하지 않을 수도 있다. 또는, 수신하는 경우라도 수신된 정보를 상기 인증 시스템(300)으로 전송하지 않음으로써 결과적으로 상기 인증 시스템(300)이 상기 OTP(또는 인증정보)를 생성하지 못하도록 제어할 수도 있다.
- [0355] 상기 제어모듈(110)은 상기 통신모듈(120)이 상기 페어 시스템과 적어도 한 번 태깅이 되는 경우, 상기 통신모듈(120)을 통해 상기 페어 시스템으로부터 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 수신하고, 수신된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 인증 시스템으로 전송할 수 있다.
- [0356] 또한, 상기 제어모듈(110)은 상기 보안 디지털 시스템(100)의 식별정보를 상기 인증 시스템(300)으로 더 전송할 수 있다. 그러면, 상기 인증 시스템(300)은 수신된 상기 보안 디지털 시스템(100)의 식별정보에 기초하여 상기 보안 디지털 시스템(100)이 미리 등록된 시스템인지를 판단하고, 미리 등록된 시스템이어야 상기 OTP(또는 인증정보)를 생성할 수도 있다.
- [0357] 상기 인증 시스템(300)은 수신부(310), 생성부(320), 및 송신부(330)를 포함할 수 있다. 상기 인증 시스템(300)은 제어부(340)를 더 포함할 수 있고, 저장부(미도시)도 더 포함할 수 있다.
- [0358] 설명의 편의를 위해 도 14에서는 상기 인증 시스템(300)을 하나의 물리적 장치로 도시하였지만, 상기 인증 시스템(300)은 복수의 물리적 장치가 유무선 네트워크를 통해 유기적으로 결합되어 구현될 수도 있다. 예컨대, 상기 인증 시스템(300)은 OTP 인증 시스템(300-1)을 포함하는 것으로 정의될 수 있으며, 상기 OTP 인증 시스템(300-1)은 상기 인증 시스템(300)의 나머지 구성들과 하나의 물리적 장치로 구현될 수도 있고, 상기 OTP 인증 시스템(300-1)은 상기 인증 시스템(300)과는 별개의 물리적 장치로 구현되고 유무선 네트워크를 통해 통신으로 연결될 수도 있다.
- [0359] 상기 인증 시스템(300)의 수신부(310)는 상기 제어모듈(110)에 의해 전송된 상기 OTP 정보 중 적어도 일부 또는 상기 페어 시스템의 식별정보를 수신할 수 있다. 또한, 상기 수신부(310)는 상기 제어모듈(110)로부터 상기 보안 디지털 시스템(100)의 식별정보를 더 수신할 수도 있다.
- [0360] 그러면, 상기 생성부(320)는 상기 수신부(310)를 통해 수신된 정보에 기초하여 OTP(또는 인증정보)를 생성할 수 있다. 또한, 상기 생성부(320)는 상기 보안 디지털 시스템(100)의 식별정보에 기초하여 상기 보안 디지털 시스템(100)이 미리 등록된 시스템인지를 판단하고, 판단 결과에 따라 선택적으로 상기 OTP(또는 인증정보)를 생성할 수도 있다. 또한, 상기 수신부(310)를 통해 상기 정보가 수신되면, 상기 제어부(340)는 OTP 인증 시스템(300-1)으로 인증용 OTP를 요청할 수도 있다.
- [0361] 일 실시 예에 의하면, 상기 제어부(340)는 생성부(320)에 의해 생성된 상기 OTP와 상기 인증용 OTP를 비교함으로써 인증 요청자의 인증 성공 여부를 결정할 수 있다.
- [0362] 다른 실시 예에 의하면, 상기 송신부(330)는 상기 생성부(320)에 의해 생성된 상기 OTP를 상기 보안 디지털 시스템(100) 또는 상기 인증 시스템(300)의 소정의 저장부(미도시)에 미리 등록된 인증 요청자의 지정 단말기로 전송할 수 있다. 그리고 전송에 응답하여 상기 보안 디지털 시스템(100) 또는 상기 데이터 프로세싱 장치(400)

로부터 OTP가 상기 수신부(310)를 통해 수신되면, 상기 제어부(340)는 수신된 OTP와 상기 인증용 OTP를 비교함으로써 인증 요청자의 인증 성공 여부를 결정할 수도 있다. 물론, 수신된 OTP와 상기 송신부(330)가 전송한 OTP가 상응하는지 여부가 판단될 수 있다.

[0363] 또 다른 실시 예에 의하면, 상기 제어부(340)는 인증정보를 생성할 수도 있다. 이러한 경우, 상기 송신부(330)는 상기 생성부(330)에 의해 생성된 상기 인증정보를 상기 보안 디지털 시스템(100) 또는 상기 인증 시스템(300)의 소정의 저장부(미도시)에 미리 등록된 인증 요청자의 지정 단말기로 전송할 수 있다. 그러면, 전송에 응답하여 상기 보안 디지털 시스템(100) 또는 상기 데이터 프로세싱 장치(400)로부터 인증정보가 상기 수신부(310)를 통해 수신될 수 있다. 그러면 제어부(340)는 상기 송신부(330)에 의해 전송된 인증정보와 상기 수신부(310)에 의해 수신된 인증정보를 비교함으로써 인증 성공 여부를 결정할 수도 있다. 또한, 이러한 경우에 상기 인증정보는 종래의 OTP 방식과 달리 일회성으로 생성되는 소정의 자리수의 정보이지만 하면 상기 인증정보로 이용될 수 있음은 전술한 바와 같다.

[0364] 이처럼 상기 인증 시스템(300)이 OTP(또는 인증정보)를 생성하는 과정의 일 실시 예는 도 13에 도시된다.

[0365] 도 13은 본 발명의 다른 실시 예에 따른 OTP 생성 방법을 설명하기 위한 도면이다. 도 13은 보안 디지털 시스템(100)이 페어 시스템(200)으로부터 OTP 정보 중 적어도 일부를 수신하는 경우를 도시하고 있다. 하지만, 페어 시스템(200)의 식별정보를 수신할 수도 있음은 전술한 바와 같다.

[0366] 도 13을 참조하면, 상기 보안 디지털 시스템(100)과 상기 페어 시스템(200)이 적어도 한 번 태깅이 되면, 상기 보안 디지털 시스템(100)은 상기 페어 시스템(200)으로부터 OTP 정보 중 적어도 일부(및/또는 페어 시스템(200)의 식별정보)를 수신할 수 있다(S100). 그러면, 상기 보안 디지털 시스템(100)은 수신된 OTP 정보 중 적어도 일부(및/또는 페어 시스템(200)의 식별정보)를 상기 인증 시스템(300)으로 전송할 수 있다(S110). 구현 예에 따라서는 상기 보안 디지털 시스템(100)은 상기 보안 디지털 시스템(100)의 식별정보를 더 전송할 수도 있다(S110-1).

[0367] 그러면 상기 인증 시스템(300)은 수신된 정보에 기초하여 인증 요청자에 상응하는 OTP 정보(OTP 생성 프로그램, OTP 생성키 등) 및/또는 페어 시스템(200)의 식별정보를 특정할 수 있다. 그리고 특정된 OTP 정보 및/또는 페어 시스템(200)의 식별정보에 기초하여 상기 인증 요청자에 상응하는 OTP를 생성할 수 있다(S120).

[0368] 한편, 상기 인증 시스템(300)은 OTP 인증 시스템(300-1)으로 상기 인증 요청자에 상응하는 인증용 OTP를 요청할 수 있다(S110-2). 인증 요청자를 특정하기 위해 인증 요청자를 식별할 수 있는 정보(예컨대, 로그인 정보, 페어 시스템(200)의 식별정보, 및/또는 보안 디지털 시스템(100)의 식별정보 등)를 상기 OTP 인증 시스템(300-1)으로 전송할 수 있음은 물론이다.

[0369] 그러면, 상기 OTP 인증 시스템(300-1)은 인증용 OTP를 생성하고, 생성한 인증용 OTP를 상기 인증 시스템(300)으로 전송할 수 있다(S110-3, S110-4).

[0370] 상기 인증 시스템(300)은 생성한 OTP(S120에 의해)와 수신한 인증용 OTP를 비교함으로써 인증 성공 여부를 판단할 수도 있다(S150).

[0371] 구현 예에 따라서는, 생성한 OTP를 보안 디지털 시스템(100)으로(또는 미리 등록된 인증 요청자의 지정 단말기로) 전송할 수도 있다(S130). 그러면, 사용자는 전송된 OTP를 확인하고, 확인한 OTP를 소정의 데이터 프로세싱 장치(400)로 입력하여 상기 인증 시스템(300)으로 전송할 수 있다(S140). 지정 단말기로 OTP가 전송된 경우, 상기 보안 디지털 시스템(100)을 통해 상기 OTP를 상기 인증 시스템(300)으로 전송할 수도 있다. 구현 예에 따라서는, 상기 보안 디지털 시스템(100)으로 OTP가 전송된 경우, 상기 보안 디지털 시스템(100)을 통해 다시 상기 OTP를 재전송할 수도 있다.

[0372] 어떠한 경우든 상기 인증 시스템(300)으로 다시 OTP가 전송되면, 상기 인증 시스템(300)은 수신된 OTP와 인증용 OTP를 비교함으로써 인증 성공 여부를 판단할 수 있다(S150).

[0373] 구현 예에 따라서는, 상기 인증 시스템(300)이 전송한 OTP와 수신된 OTP가 서로 상응하는지를 판단함으로써 인증 성공 여부를 판단할 수 있다(S150).

[0374] 본 발명의 실시 예에 따른 보안 디지털 시스템, 페어시스템, 또는 인증 시스템 제공방법은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 하드 디스크, 플로피 디스크, 광 데이터 저장장치 등

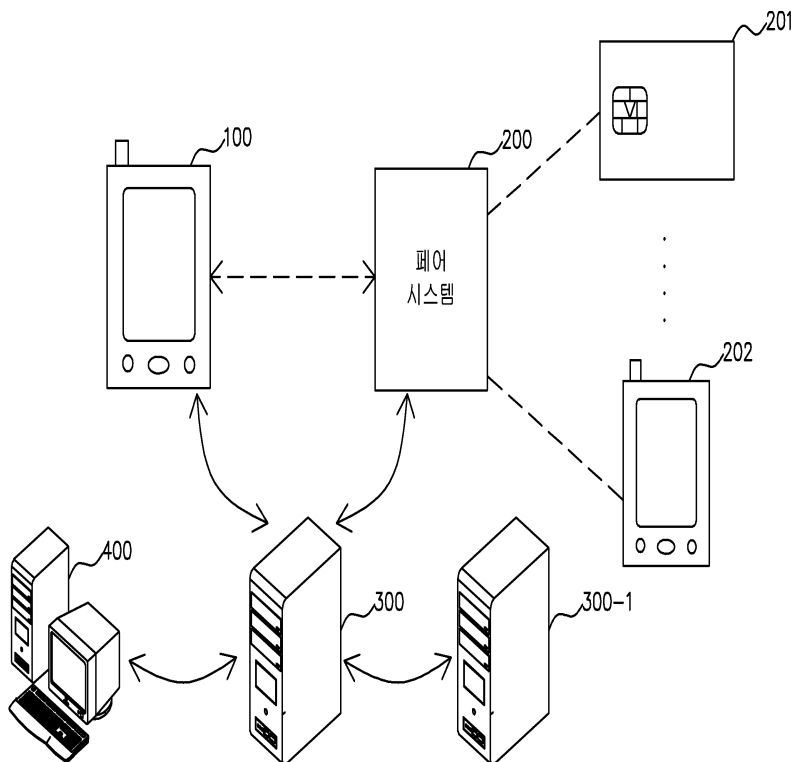
이 있으며, 또한 캐리어 웨이브(예를 들어, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

[0375]

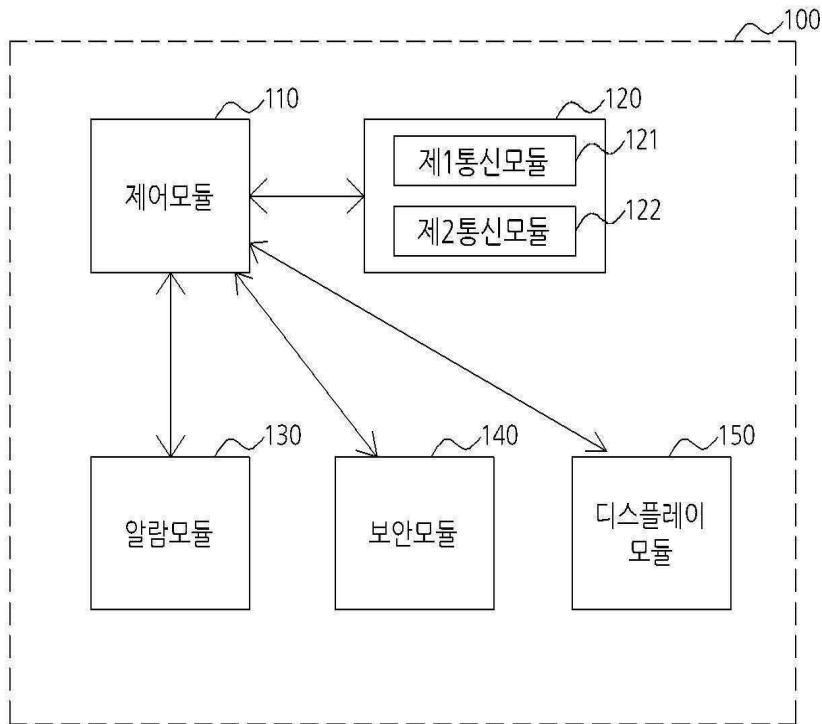
본 발명은 도면에 도시된 일 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

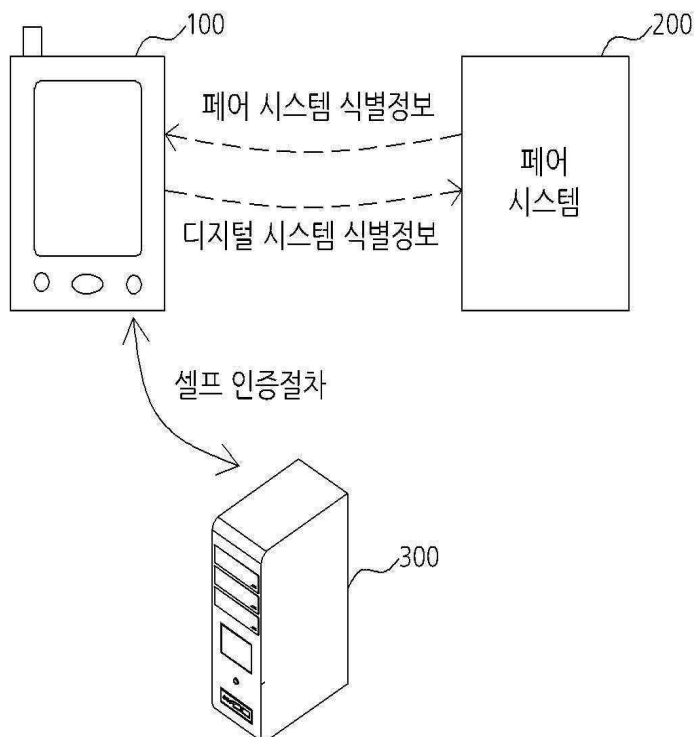
도면1



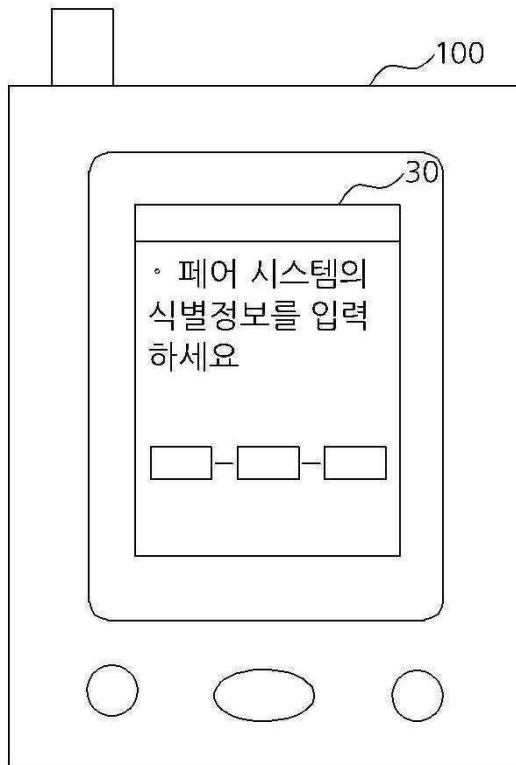
도면2



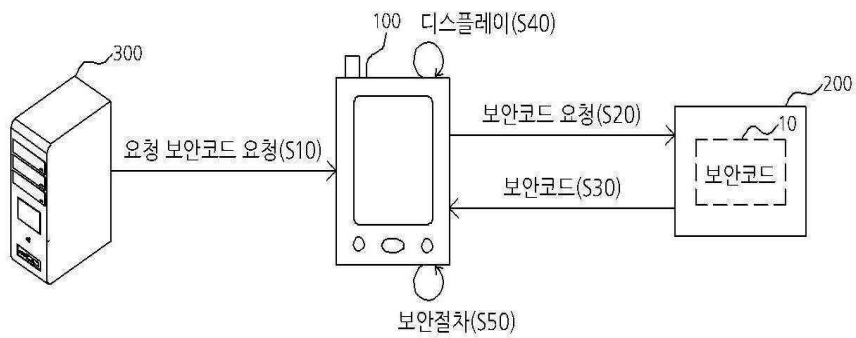
도면3



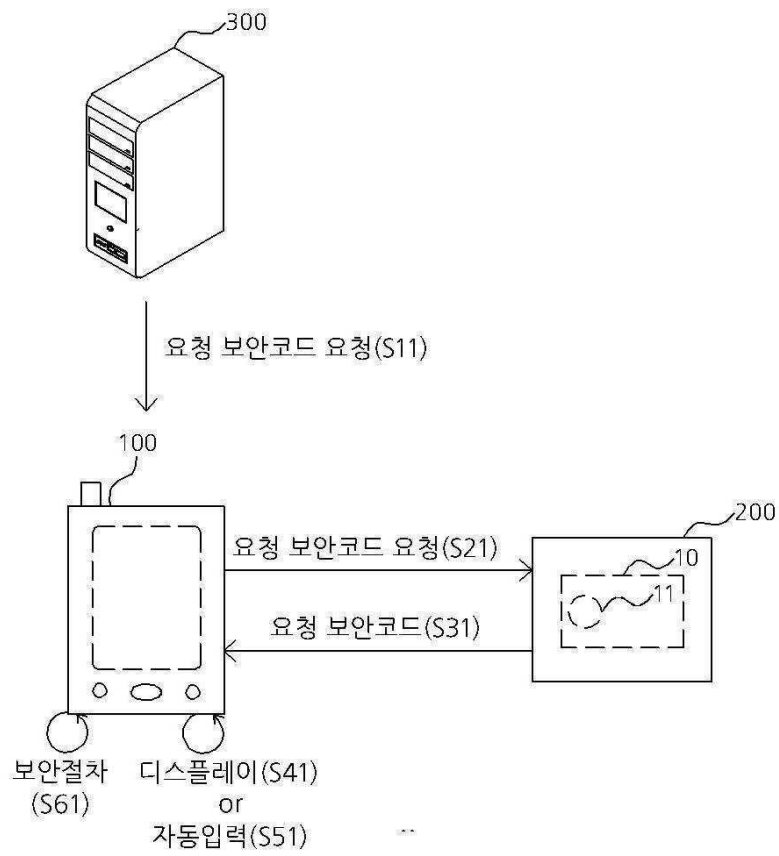
도면4



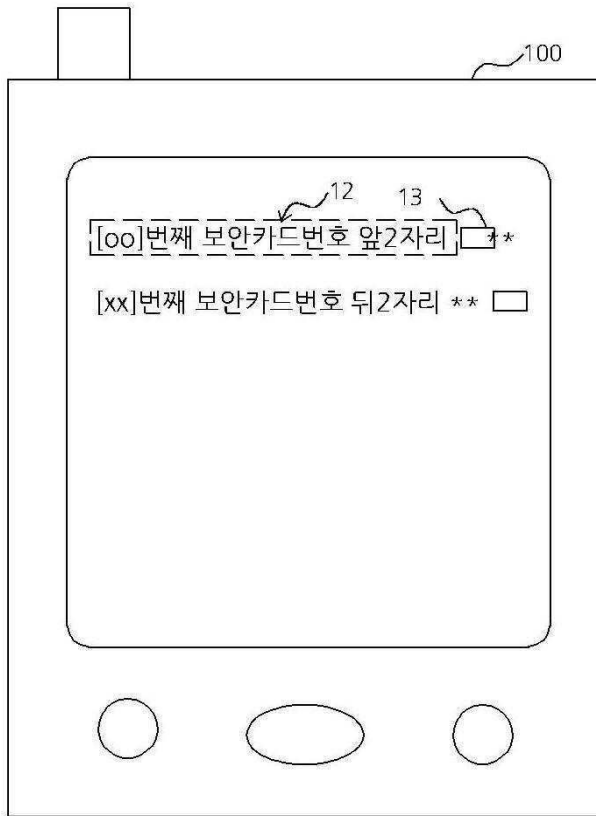
도면5a



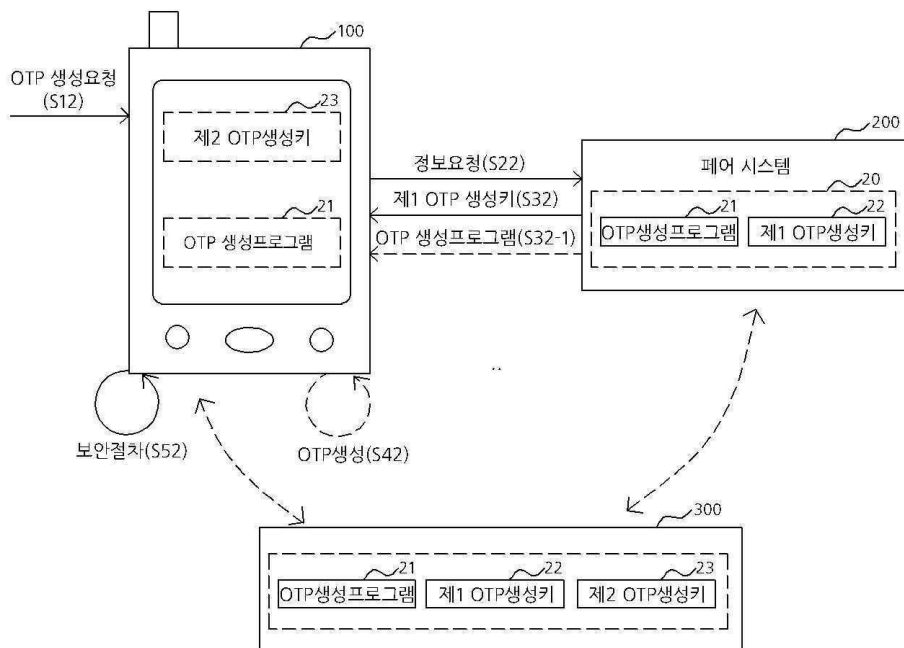
도면5b



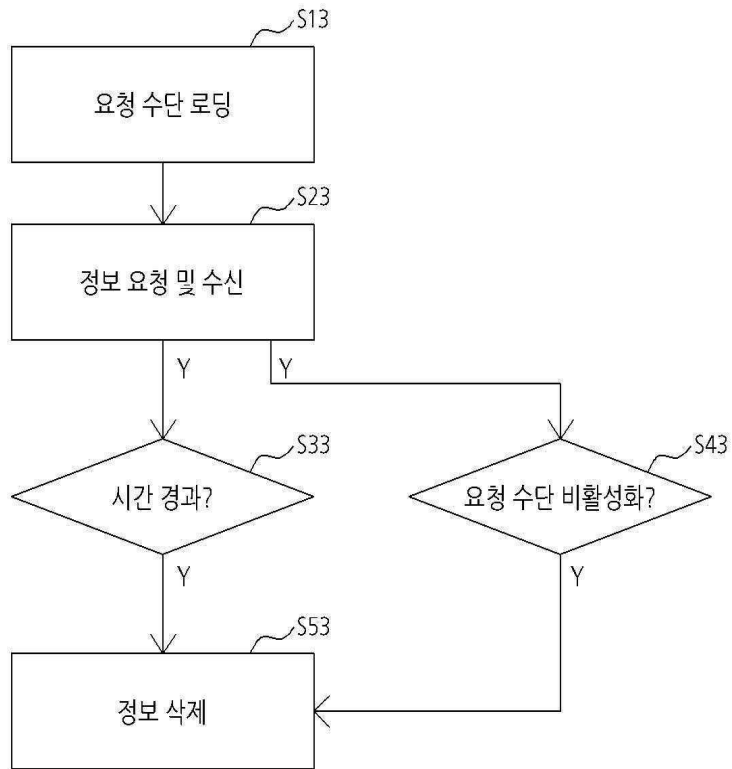
도면5c



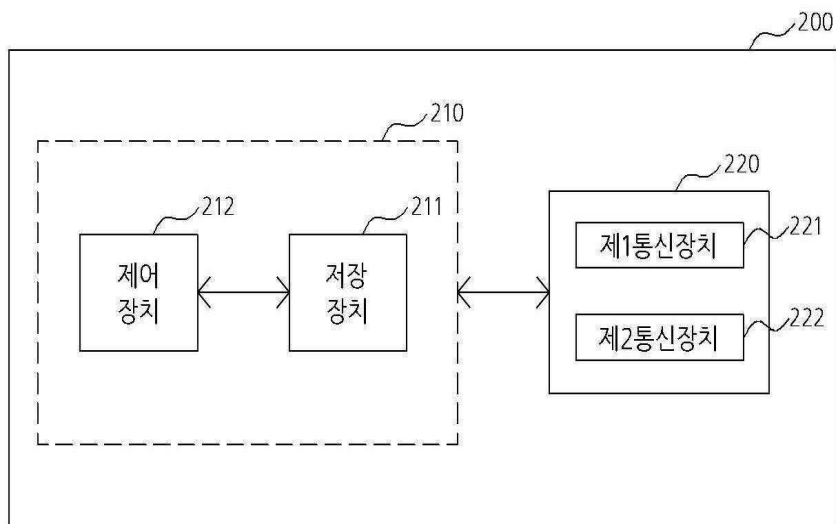
도면6



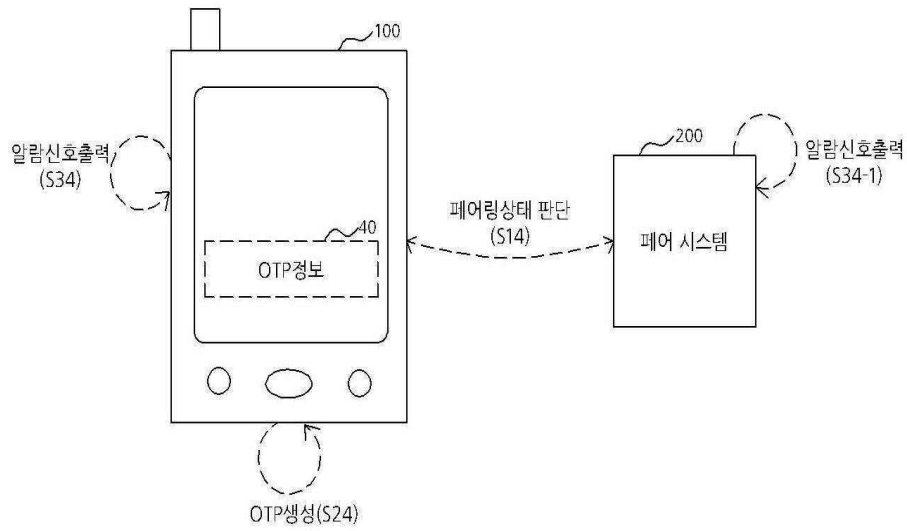
도면7



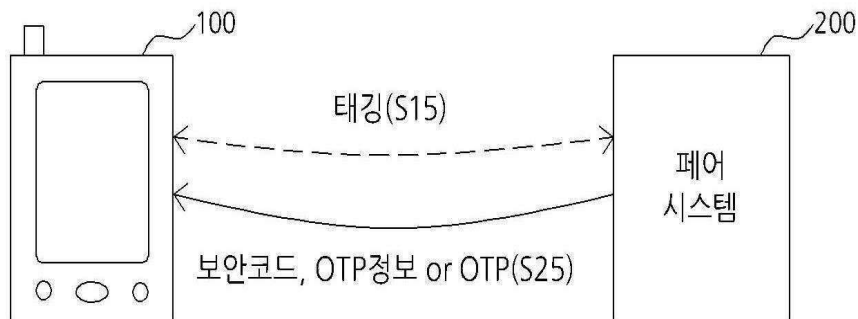
도면8



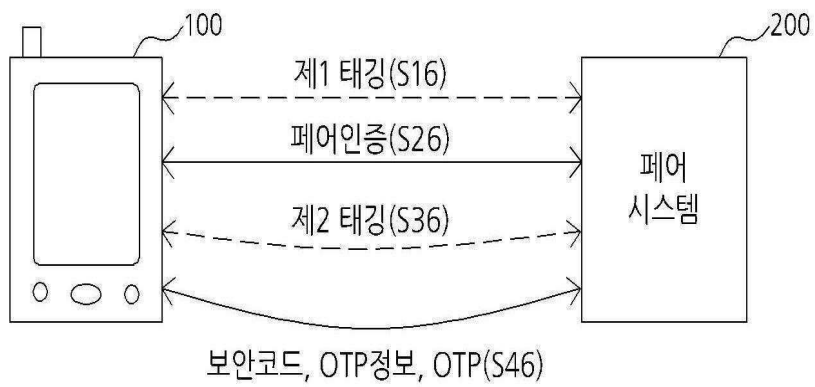
도면9



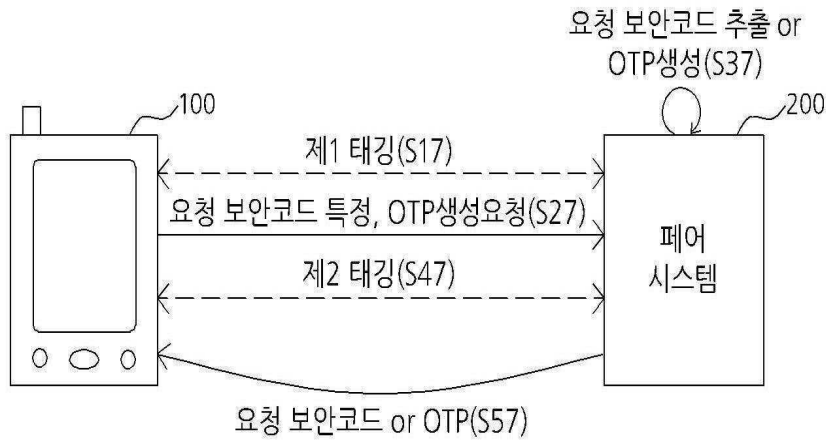
도면10



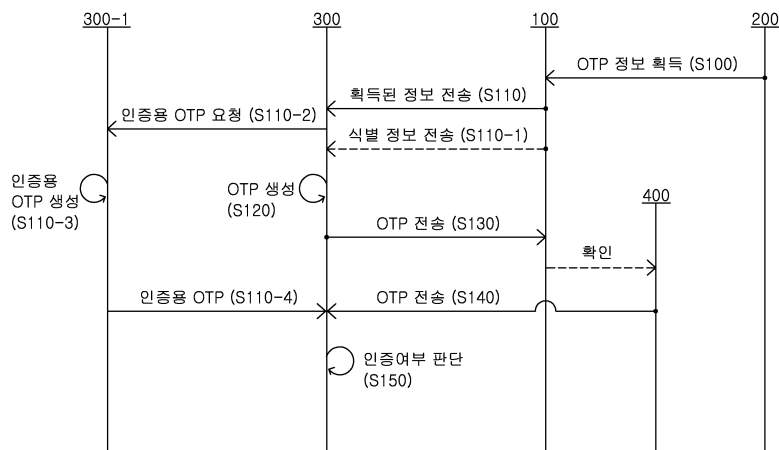
도면11



도면12



도면13



도면14

