(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0011792
(43) 공개일자 2018년02월02일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 20/32* (2012.01)
G06Q 20/40 (2012.01)
(52) CPC특허분류
G06Q 20/38215 (2013.01)
G06Q 20/322 (2013.01)
(21) 출원번호 10-2017-7036727
(22) 출원일자(국제) 2016년04월22일
심사청구일자 없음
(85) 번역문제출일자 2017년12월20일
(86) 국제출원번호 PCT/CN2016/080017
(87) 국제공개번호 WO 2016/188281
국제공개일자 2016년12월01일
(30) 우선권주장
201510272052.9 2015년05월25일 중국(CN)

(71) 출원인
알리바바 그룹 홀딩 리미티드
케이만군도, 그랜드 케이만, 피오박스 847, 원 캐피탈 플레이스 4층
(72) 발명자
시아 주펑
중국 항저우 310099 완탕 로드 넘버 18 후앙롱 타임스 플라자 빌딩 비 17층 앤츠 패튼 팀 내
(74) 대리인
김태홍, 김진희

전체 청구항 수 : 총 32 항

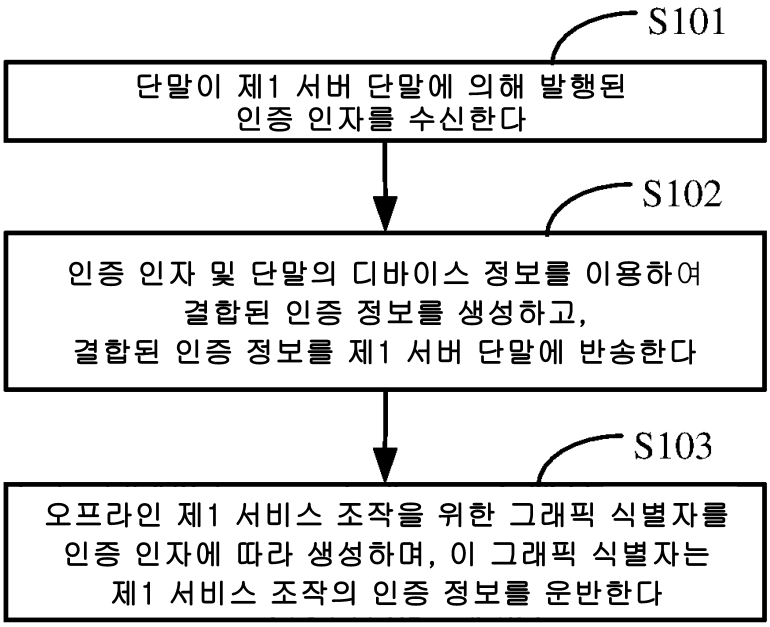
(54) 발명의 명칭 **정보 상호작용 방법, 장치 및 시스템**

(57) 요 약

본 출원은 정보 상호작용 방법, 장치, 및 시스템에 관한 것이다. 본 방법은, 제1 서버 단말에 의해 발행된 인증 인자(authentication factor)(상기 인증 인자는 사용자의 계정 정보와 인증키, 및 동적 시간 인자를 운반함)를 단말에 의해 수신하는 단계 - 상기 인증 인자 및 상기 단말의 디바이스 정보를 이용하여 결합된 인증 정보를 생

(뒷면에 계속)

대 표 도 - 도3a



성하고, 상기 결합된 인증 정보에 따라 상기 제1 서버 단말이 결제에 대한 인가(authorization)를 수행하도록, 상기 결합된 인증 정보를 상기 제1 서버 단말에 반송하는 단계; 및 상기 인증 인자에 따라 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 생성하고, 상기 단말이 상기 그래픽 식별자를 이용하여 오프라인 상태에서 상기 제1 서비스 조작을 완료하도록, 상기 단말에 의해, 상기 그래픽 식별자를 디스플레이하는 단계를 포함한다. 본 출원에서 제공된 정보 상호작용 방법, 장치, 및 시스템은 디바이스가 오프라인 상태에 있을 때 안전하고 편리한 결제를 여전히 달성할 수 있다.

(52) CPC특허분류
G06Q 20/40 (2013.01)

명 세 서

청구범위

청구항 1

정보 상호작용 방법에 있어서,

단말에 의해, 제1 서버 단말에 의해 발행된 인증 인자(authentication factor)를 수신하는 단계 - 상기 인증 인자는 사용자의 계정 정보와 인증키, 및 동적 시간 인자를 운반하고, 상기 제1 서버 단말은, 상기 단말이 제1 서비스 조작을 요청할 때 상기 단말을 인증한 후 상기 제1 서비스 조작을 완료하는 서버 단말임 -;

상기 인증 인자 및 상기 단말의 디바이스 정보를 이용하여 결합된 인증 정보를 생성하고, 상기 결합된 인증 정보에 따라 상기 제1 서버 단말이 상기 제1 서비스 조작에 대한 인가(authorization)를 수행하도록, 상기 결합된 인증 정보를 상기 제1 서버 단말에 반송하는 단계; 및

상기 인증 인자에 따라 상기 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 생성하는 단계

를 포함하고,

상기 그래픽 식별자는 상기 제1 서비스 조작의 인증 정보를 운반하고, 상기 제1 서비스 조작의 인증 정보는 상기 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고, 상기 동적 패스워드는 상기 동적 시간 인자에 따라 생성되며, 상기 디바이스 계정 정보는 상기 단말의 디바이스 정보 및 상기 사용자의 계정 정보에 따라 생성되는 것인, 정보 상호작용 방법.

청구항 2

제1항에 있어서,

상기 인증 인자에 따라 상기 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 생성하는 단계 이전에,

상기 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 디스플레이하기 위한 디스플레이 명령을 수신하는 단계; 및

상기 디스플레이 명령이 수신된 후 상기 인증 인자에 따라 상기 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 생성하는 단계

를 더 포함하고,

상기 인증 인자에 따라 상기 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 생성하는 단계 이후에, 본 방법은,

상기 그래픽 식별자를 이용하여 오프라인 상태에서 상기 제1 서비스 조작을 완료하도록 상기 단말에 의해 상기 그래픽 식별자를 디스플레이하는 단계를 더 포함하는 정보 상호작용 방법.

청구항 3

제2항에 있어서,

상기 그래픽 식별자의 디스플레이 모드는 바코드와 QR 코드 중 하나 또는 이들의 조합을 포함하고,

상기 단말에 의해 상기 그래픽 식별자를 디스플레이하는 단계 이후에, 상기 방법은,

상기 그래픽 식별자의 디스플레이 모드에 대한 전환 명령을 수신할 때 상기 그래픽 식별자의 디스플레이 모드를 전환하는 단계를 더 포함하는 정보 상호작용 방법.

청구항 4

제1항에 있어서,

상기 단말은, 제2 단말을 통해, 상기 제1 서버 단말에 의해 발행된 상기 인증 인자를 수신하고, 상기 결합된 인증 정보를 상기 제2 단말을 통해 상기 제1 서버 단말에 반송하는 것인, 정보 상호작용 방법.

청구항 5

제1항에 있어서,

상기 제1 서버 단말에 의해 발행된 인증 인자를 수신하는 단계 이전에,

상기 단말에 의해, 계정 신원 검증 요청을 상기 제1 서버 단말에 송신하는 단계;

신원 검증이 성공된 후 상기 제1 서버 단말에 의해 송신된 검증 결과를 수신하는 단계;

상기 오프라인 제1 서비스 조작에 대한 인가 검증 요청을 상기 제1 서버 단말에 송신하는 단계; 및

인가 검증이 성공된 후 상기 제1 서버 단말에 의해 발행된 상기 인증 인자를 수신하는 단계

를 더 포함하는 정보 상호작용 방법.

청구항 6

제1항에 있어서,

상기 동적 패스워드는 동일한 시간 창에서 변경되지 않은 상태로 있으며, 다음번 시간 창에서, 상기 동적 패스워드는 상기 동적 시간 인자에 따라 재생성되어 동적으로 변경되는 것인, 정보 상호작용 방법.

청구항 7

제1항에 있어서,

상기 동적 패스워드는 구체적으로, 일회용 패스워드 계산 방법에 따라, 상기 사용자의 인증키, 상기 동적 시간 인자, 상기 디바이스 계정 정보, 및 미리 설정된 패스워드 길이를 이용한 계산을 통해 얻어지는 것인, 정보 상호작용 방법.

청구항 8

정보 상호작용 방법에 있어서,

제2 서버 단말에 의해, 단말 상에서 디스플레이된 그래픽 식별자 내에서 운반된 제1 서비스 조작의 인증 정보를 획득하는 단계 - 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함함 -;

상기 제1 서비스 조작의 인증 정보와 서비스 데이터를 이용하여 제1 서비스 조작 요청을 생성하고, 상기 제1 서버 단말이 상기 제1 서비스 조작 요청 내에서 운반된 상기 제1 서비스 조작의 인증 정보에 따라 인증을 수행하고 상기 인증이 성공된 후 상기 제1 서비스 조작을 완료하도록, 상기 제1 서비스 조작 요청을 상기 제1 서버 단말에 송신하는 단계; 및

상기 제1 서버 단말에 의해 반송된 상기 제1 서비스 조작의 결과를 수신하는 단계

를 포함하는 정보 상호작용 방법.

청구항 9

정보 상호작용 방법에 있어서,

제1 서버 단말에 의해, 제2 서버 단말에 의해 송신된 제1 서비스 조작 요청을 수신하는 단계 - 상기 제1 서비스 조작 요청은, 단말 상에서 디스플레이된 그래픽 식별자 내에서 운반된 상기 제1 서비스 조작의 인증 정보 및 서비스 데이터를 획득함으로써 상기 제2 서버 단말에 의해 생성된 요청이고, 상기 제1 서비스 조작 요청은 상기 제1 서비스 조작의 인증 정보 및 상기 서비스 데이터를 운반하며, 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함함 -; 및

상기 제1 서비스 조작 요청 내에서 운반된 상기 인증 정보에 따라 인증을 수행하고, 상기 인증이 성공된 경우, 상기 제1 서버 단말에 의해 상기 제1 서비스 조작을 완료하는 단계

를 포함하는 정보 상호작용 방법.

청구항 10

제9항에 있어서,

상기 제2 서버 단말에 의해 송신된 제1 서비스 조작 요청을 수신하는 단계 이전에,

상기 제1 서버 단말에 의해, 상기 단말 상의 온라인 계정 결합을 수행하는 단계

를 더 포함하는 정보 상호작용 방법.

청구항 11

제10항에 있어서,

상기 제1 서버 단말에 의해, 상기 단말 상의 온라인 계정 결합을 수행하는 단계는, 구체적으로,

상기 단말에 의해 송신된 계정 신원 검증 요청을 수신하는 단계 - 상기 계정 신원 검증 요청은 상기 사용자의 계정 정보를 운반함 -;

상기 계정 신원 검증 요청이 검증을 통과했는지 여부를 판단하고, 상기 검증이 성공된 경우, 성공된 검증의 검증 결과를 상기 단말에 송신하는 단계;

상기 제1 서비스 조작을 오프라인에서 완료하기 위해, 상기 단말에 의해 송신된 인가 검증 요청을 수신하는 단계;

상기 인가 검증 요청에 대한 검증이 성공되었는지의 여부를 판단하고, 상기 검증이 성공된 경우, 상기 사용자의 인증키를 생성하며, 상기 제1 서버 단말의 동적 시간 인자를 계산하는 단계;

상기 사용자의 인증키, 상기 동적 시간 인자, 및 상기 사용자의 계정 정보를 이용하여 인증 인자를 생성하는 단계;

상기 단말에 상기 인증 인자를 발행하는 단계;

상기 단말에 의해 제출된 결합된 인증 정보를 수신하는 단계 - 상기 결합된 인증 정보는 상기 인증 인자와 상기 디바이스 계정 정보를 결합함으로써 생성됨 -; 및

상기 결합된 인증 정보에 대해 인가 검증을 수행하고, 인가가 성공된 경우, 상기 인가 검증을 완료하는 단계

를 포함한 것인 정보 상호작용 방법.

청구항 12

제10항에 있어서,

상기 제1 서버 단말에 의해, 상기 단말 상의 온라인 계정 결합을 수행하는 단계는, 구체적으로,

상기 제2 단말에 의해 송신된 계정 신원 검증 요청을 수신하는 단계 - 상기 계정 신원 검증 요청은 상기 사용자의 상기 계정 정보를 운반함 -;

상기 계정 신원 검증 요청이 검증을 통과했는지 여부를 판단하고, 상기 검증이 성공된 경우, 성공된 검증의 검증 결과를 상기 제2 단말에 송신하는 단계;

상기 제1 서비스 조작을 오프라인에서 완료하기 위해, 상기 제2 단말에 의해 송신된 인가 검증 요청을 수신하는 단계;

상기 인가 검증 요청에 대한 검증이 성공되었는지의 여부를 판단하고, 상기 검증이 성공된 경우, 상기 사용자의 인증키를 생성하며, 상기 제1 서버 단말의 동적 시간 인자를 계산하는 단계;

상기 사용자의 인증키, 상기 동적 시간 인자, 및 상기 사용자의 계정 정보를 이용하여 인증 인자를 생성하는 단계;

상기 제2 단말이 상기 인증 인자를 상기 단말에 송신하도록, 상기 인증 인자를 상기 제2 단말에 발행하는 단계;

상기 단말에 의해 반송되고 상기 제2 단말에 의해 제출된 결합된 인증 정보를 수신하는 단계 - 상기 결합된 인증 정보는 상기 인증 인자와 상기 단말의 상기 디바이스 계정 정보를 결합함으로써 상기 단말에 의해 생성됨 -; 및

상기 결합된 인증 정보에 대해 인가 검증을 수행하고, 인가가 성공된 경우, 상기 인가 검증을 완료하는 단계

를 포함한 것인 정보 상호작용 방법.

청구항 13

제11항 또는 제12항에 있어서,

상기 사용자의 상기 인증키를 생성하는 단계 후에,

상기 사용자의 인증키 및 상기 사용자의 계정 정보로부터 압축된 문자열을 생성하는 단계 - 상기 압축된 문자열은 상기 인증키 및 상기 사용자의 계정 정보와 일대일 매핑 관계를 가짐 -; 및

상기 사용자의 계정 정보, 상기 사용자의 인증키, 상기 동적 시간 인자를 이용하여 상기 인증 인자를 생성하는 단계 - 이것은, 구체적으로, 상기 사용자의 인증키, 상기 압축된 문자열, 및 상기 동적 시간 인자를 사용하여 상기 인증 인자를 생성하는 것을 포함함 -

를 더 포함하는 정보 상호작용 방법.

청구항 14

제9항에 있어서,

상기 제1 서비스 조작 요청 내에서 운반된 상기 제1 서비스 조작의 상기 인증 정보에 따라 인증을 수행하는 단계는, 구체적으로,

상기 제1 서비스 조작의 상기 인증 정보 내에서 운반된 상기 인증키와 상기 디바이스 계정 정보 사이의 결합 관계가 정확한지 여부를 체크하고, 상기 인증 인자 내의 상기 동적 시간 인자에 따라 상기 동적 패스워드가 유효한지 여부를 체크하는 단계

를 포함하며, 상기 결합 관계가 정확하고 상기 동적 패스워드가 유효한 경우, 상기 인증은 성공된 것인, 정보 상호작용 방법.

청구항 15

단말에 있어서,

제1 서버 단말에 의해 발행된 인증 인자를 수신하도록 구성된 수신 유닛 - 상기 인증 인자는 사용자의 계정 정보와 인증키, 및 동적 시간 인자를 운반하고, 상기 제1 서버 단말은, 상기 단말이 제1 서비스 조작을 요청할 때 상기 단말을 인증한 후 상기 제1 서비스 조작을 완료하는 서버 단말임 -;

상기 수신 유닛에 의해 수신된 상기 인증 인자와 상기 단말의 디바이스 정보를 이용하여 결합된 인증 정보를 생성하도록 구성된 결합 유닛;

상기 제1 서버 단말이 상기 결합된 인증 정보에 따라 상기 제1 서비스 조작에 대한 인가를 수행하도록, 상기 결합 유닛에 의해 생성된 상기 결합된 인증 정보를 상기 제1 서버 단말에 반송하도록 구성된 송신 유닛; 및

상기 수신 유닛에 의해 수신된 상기 인증 인자에 따라 상기 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 생성하도록 구성된 처리 유닛

을 포함하고, 상기 그래픽 식별자는 상기 제1 서비스 조작의 인증 정보를 운반하고, 상기 제1 서비스 조작의 인증 정보는 상기 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고, 상기 동적 패스워드는 상기 동적 시간 인자에 따라 생성되며, 상기 디바이스 계정 정보는 상기 단말의 디바이스 정보 및 상기 사용자의 계정 정보에 따라 생성되는 것인, 단말.

청구항 16

제15항에 있어서,

상기 수신 유닛은 또한, 상기 그래픽 식별자를 디스플레이하기 위한 디스플레이 명령을 수신하도록 구성되고,

상기 처리 유닛은, 상기 수신 유닛이 상기 디스플레이 명령을 수신한 후 상기 인증 인자에 따라 상기 제1 서비스 조작을 오프라인에서 완료하기 위한 상기 그래픽 식별자를 생성하도록 구성되며,

상기 단말은,

상기 단말이 상기 그래픽 식별자를 이용하여 상기 제1 서비스 조작을 오프라인 상태에서 완료하도록, 상기 처리 유닛에 의해 생성된 상기 그래픽 식별자를 디스플레이하도록 구성된 디스플레이 유닛

을 더 포함한 것인, 단말.

청구항 17

제16항에 있어서,

상기 디스플레이 유닛에 의해 디스플레이된 상기 그래픽 식별자의 디스플레이 모드는 바코드와 QR 코드 중 하나 또는 이들의 조합을 포함하고,

상기 수신 유닛은 또한, 상기 그래픽 식별자의 디스플레이 모드에 대한 전환 명령을 수신하도록 구성되며,

상기 처리 유닛은 또한, 상기 수신 유닛이 상기 전환 명령을 수신할 때 상기 디스플레이 유닛에 의해 디스플레이된 상기 그래픽 식별자의 디스플레이 모드를 전환하도록 구성된 것인, 단말.

청구항 18

제15항에 있어서,

상기 수신 유닛은, 제2 단말을 통해, 상기 제1 서버 단말에 의해 발행된 상기 인증 인자를 수신하도록 구성되며, 상기 송신 유닛은, 상기 제2 단말을 통해, 상기 결합된 인증 정보를 상기 제1 서버 단말에 반송하도록 구성된 것인, 단말.

청구항 19

제15항에 있어서,

상기 송신 유닛은 또한, 계정 신원 검증 요청을 상기 제1 서버 단말에 송신하도록 구성되고,

상기 수신 유닛은, 신원 검증이 성공된 후 상기 제1 서버 단말에 의해 송신된 검증 결과를 수신하도록 구성되고,

상기 송신 유닛은, 상기 오프라인 제1 서비스 조작에 대한 인가 검증 요청을 상기 제1 서버 단말에 송신하도록 구성되며,

상기 수신 유닛은, 인가 검증이 성공된 후 상기 제1 서버 단말에 의해 발행된 상기 인증 인자를 수신하도록 구성된 것인, 단말.

청구항 20

서버 단말에 있어서,

단말 상에서 디스플레이된 그래픽 식별자 내에서 운반된 제1 서비스 조작의 인증 정보를 획득하도록 구성된 획득 유닛 - 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함함 -;

상기 획득 유닛에 의해 획득된 상기 제1 서비스 조작의 인증 정보와 서비스 데이터를 이용하여 제1 서비스 조작 요청을 생성하도록 구성된 처리 유닛;

상기 제1 서버 단말이 상기 제1 서비스 조작 요청 내에서 운반된 상기 제1 서비스 조작의 인증 정보에 따라 인증을 수행하고 상기 인증이 성공된 후 상기 제1 서비스 조작을 완료하도록, 상기 처리 유닛에 의해 생성된 상기 제1 서비스 조작 요청을 상기 제1 서버 단말에 송신하도록 구성된 송신 유닛; 및

상기 제1 서버 단말에 의해 반송된 상기 제1 서비스 조작의 결과를 수신하도록 구성된 수신 유닛

을 포함하는 서버 단말.

청구항 21

서버 단말에 있어서,

제2 서버 단말에 의해 송신된 제1 서비스 조작 요청을 수신하도록 구성된 수신 유닛 - 상기 제1 서비스 조작 요청은, 단말 상에서 디스플레이된 그래픽 식별자 내에서 운반된 제1 서비스 조작의 인증 정보 및 서비스 데이터를 획득함으로써 상기 제2 서버 단말에 의해 생성된 요청이고, 상기 제1 서비스 조작 요청은 상기 제1 서비스 조작의 인증 정보 및 상기 서비스 데이터를 운반하며, 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함함 -; 및

상기 수신 유닛에 의해 수신된 상기 제1 서비스 조작 요청 내에서 운반된 상기 제1 서비스 조작의 인증 정보에 따라 인증을 수행하도록 구성된 처리 유닛 - 상기 인증이 성공된 경우, 제1 서버 단말이 상기 제1 서비스 조작을 완료함 -

을 포함하는 서버 단말.

청구항 22

제21항에 있어서,

상기 처리 유닛은 또한, 상기 단말 상에서 온라인 계정 결합을 수행하도록 구성된 것인, 서버 단말.

청구항 23

제22항에 있어서,

상기 서버 단말은 송신 유닛을 더 포함하고,

상기 수신 유닛은 또한, 상기 단말에 의해 송신된 계정 신원 검증 요청을 수신하도록 구성되고, 상기 계정 신원 검증 요청은 상기 사용자의 계정 정보를 운반하고;

상기 처리 유닛은 상기 계정 신원 검증 요청이 검증을 통과하였는지 여부를 판단하고, 상기 검증이 성공된 경우, 상기 송신 유닛을 이용하여 상기 성공된 검증의 검증 결과를 상기 단말에 송신하도록 구성되고;

상기 수신 유닛은 상기 제1 서비스 조작을 오프라인에서 완료하기 위해, 상기 단말에 의해 송신된 인가 검증 요청을 수신하도록 구성되고;

상기 처리 유닛은, 상기 인가 검증 요청에 대한 검증이 성공되었는지 여부를 판단하고, 상기 검증이 성공된 경우, 상기 사용자의 인증키를 생성하고, 상기 서버 단말의 동적 시간 인자를 계산하고, 상기 인증키, 상기 동적 시간 인자, 및 상기 사용자의 계정 정보를 이용하여 인증 인자를 생성하도록 구성되고;

상기 송신 유닛은 상기 처리 유닛에 의해 생성된 상기 인증 인자를 상기 단말에 발행하도록 구성되고;

상기 수신 유닛은 상기 단말에 의해 제출된 결합된 인증 정보를 수신하도록 구성되고, 상기 결합된 인증 정보는 상기 인증 인자와 상기 디바이스 계정 정보를 결합함으로써 생성되며;

상기 처리 유닛은, 상기 결합된 인증 정보에 대해 인가 검증을 수행하며, 인가가 성공된 경우, 상기 인가 검증을 완료하도록 구성된 것인, 서버 단말.

청구항 24

제22항에 있어서,

상기 서버 단말은 송신 유닛을 더 포함하고,

상기 수신 유닛은, 상기 제2 단말에 의해 송신된 계정 신원 검증 요청을 수신하도록 구성되고, 상기 계정 신원 검증 요청은 상기 사용자의 계정 정보를 운반하고;

상기 처리 유닛은 상기 계정 신원 검증 요청이 검증을 통과하였는지 여부를 판단하고, 상기 검증이 성공된 경우, 상기 송신 유닛을 이용하여 상기 성공된 검증의 검증 결과를 상기 제2 단말에 송신하도록 구성되고;

상기 수신 유닛은 상기 제1 서비스 조작을 오프라인에서 완료하기 위해, 상기 제2 단말에 의해 송신된 인가 검증 요청을 수신하도록 구성되고;

상기 처리 유닛은, 상기 인가 검증 요청에 대한 검증이 성공되었는지 여부를 판단하고, 상기 검증이 성공된 경우, 상기 사용자의 인증키를 생성하고, 상기 서버 단말의 동적 시간 인자를 계산하고, 상기 인증키, 상기 동적 시간 인자, 및 상기 사용자의 계정 정보를 이용하여 인증 인자를 생성하도록 구성되고;

상기 송신 유닛은 상기 제2 단말이 상기 인증 인자를 상기 단말에 송신하도록, 상기 인증 인자를 상기 제2 단말에 발행하도록 구성되고;

상기 수신 유닛은 상기 단말에 의해 반송되고 상기 제2 단말에 의해 제출된 결합된 인증 정보를 수신하도록 구성되며, 상기 결합된 인증 정보는 상기 인증 인자와 상기 단말의 상기 디바이스 계정 정보를 결합함으로써 상기 단말에 의해 생성되며;

상기 처리 유닛은, 상기 결합된 인증 정보에 대해 인가 검증을 수행하며, 인가가 성공된 경우, 상기 인가 검증을 완료하도록 구성된 것인, 서버 단말.

청구항 25

제23항 또는 제24항에 있어서,

상기 사용자의 인증키를 생성한 후, 상기 처리 유닛은 또한, 상기 사용자의 상기 계정 정보 및 상기 인증키로부터 압축된 문자열을 생성하도록 구성되고, 상기 압축된 문자열은 상기 인증키 및 상기 사용자의 계정 정보와 일대일 매핑 관계를 가지며;

상기 처리 유닛은 상기 사용자의 계정 정보, 상기 인증키, 상기 동적 시간 인자를 이용하여 상기 인증 인자를 생성하도록 구성되며, 이는, 구체적으로, 상기 인증키, 상기 압축된 문자열, 및 상기 동적 시간 인자를 사용하여 상기 인증 인자를 생성하는 것을 포함한 것인, 서버 단말.

청구항 26

제21항에 있어서,

상기 처리 유닛은 구체적으로, 상기 제1 서비스 조작의 상기 인증 정보 내에서 운반된 상기 인증키와 상기 디바이스 계정 정보 사이의 결합 관계가 정확한지 여부를 체크하고, 상기 인증 인자 내의 상기 동적 시간 인자에 따라 상기 동적 패스워드가 유효한지 여부를 체크하도록 구성되며, 상기 결합 관계가 정확하고 상기 동적 패스워드가 유효한 경우, 상기 인증은 성공된 것인, 서버 단말.

청구항 27

전자 디바이스에 있어서,

디스플레이;

프로세서; 및

제1 서버 단말에 의해 발행된 인증 인자, 및 상기 인증 인자에 따라 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 생성하기 위한 프로그램을 저장하도록 구성된 메모리

를 포함하고, 상기 프로그램이 상기 프로세서에 의해 실행될 때, 상기 제1 서비스 조작을 오프라인에서 완료하기 위한 상기 그래픽 식별자가 상기 디스플레이의 디스플레이 영역에서 디스플레이되고, 상기 그래픽 식별자는 상기 제1 서비스 조작의 인증 정보를 운반하고, 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고, 상기 동적 패스워드는 동적 시간 인자에 따라 생성되며, 상기 디바이스 계정 정보는 상기 단말의 디바이스 정보 및 상기 사용자의 계정 정보에 따라 생성되는 것인, 전자 디바이스.

청구항 28

제27항에 있어서,

상기 동적 패스워드는 동일한 시간 창에서 변경되지 않은 상태로 있으며, 다음번 시간 창에서, 상기 동적 패스

워드는 상기 동적 시간 인자에 따라 재생성되어 동적으로 변경되는 것인, 전자 디바이스.

청구항 29

제27항에 있어서,

상기 동적 패스워드는 구체적으로, 일회용 패스워드 계산 방법에 따라, 상기 사용자의 인증키, 상기 동적 시간 인자, 상기 디바이스 계정 정보, 및 미리 설정된 패스워드 길이를 이용한 계산을 통해 얻어지는 것인, 전자 디바이스.

청구항 30

제27항에 있어서,

제2 전자 디바이스와 통신하며, 상기 제1 서버 단말에 의해 발행되고 상기 제2 전자 디바이스에 의해 송신된 상기 인증 인자를 수신하고, 인증을 결합하는 동안, 결합된 인증 정보가 상기 제1 서버 단말에 포워딩되도록, 상기 결합된 인증 정보를 상기 제2 전자 디바이스에 송신하도록 구성된 통신 모듈

을 더 포함하는 전자 디바이스.

청구항 31

제30항에 있어서,

상기 통신 모듈은 블루투스 모듈 또는 WiFi 모듈인 것인, 전자 디바이스.

청구항 32

단말, 제1 서버 단말, 및 제2 서버 단말을 포함하는 정보 상호작용 시스템에 있어서,

상기 단말은, 오프라인 상태에서, 제1 서비스 조작을 완료하기 위한 그래픽 식별자를 디스플레이하고, 상기 그래픽 식별자는 상기 제1 서비스 조작의 인증 정보를 운반하고, 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고,

상기 제2 서버 단말은 상기 그래픽 식별자 내에서 운반된 상기 제1 서비스 조작의 인증 정보를 획득하고,

상기 제2 서버 단말은 상기 제1 서비스 조작의 인증 정보 및 서비스 데이터를 이용하여 제1 서비스 조작 요청을 생성하고, 상기 제1 서비스 조작 요청을 상기 제1 서버 단말에 송신하며,

상기 제1 서버 단말은 상기 제1 서비스 조작 요청 내에서 운반된 상기 제1 서비스 조작의 인증 정보에 따라 인증을 수행하며, 상기 인증이 성공된 경우, 상기 제1 서버 단말은 상기 제1 서비스 조작을 완료하는 것인, 정보 상호작용 시스템.

발명의 설명

기 술 분 야

[0001] 본 출원은 네트워크 정보 상호작용 기술 분야에 관한 것이며, 특히, 정보 상호작용 방법, 장치, 및 시스템에 관한 것이다.

배 경 기 술

[0002] 네트워크 과학과 기술의 끊임없는 발전으로, 안전하고 편리한 네트워크 결제 모드가 지속적으로 보급되어 왔다. 사람들은 네트워크 데이터 처리 기술을 통해, 네트워크에 연결된 상태에 있는 단말 디바이스를 사용하여 실시간으로 데이터 정보를 이미 온라인 처리할 수 있으므로, 결제를 달성할 수 있다.

[0003] 그러나, 네트워크에 연결될 수 없는 단말 디바이스, 예를 들어, (스마트 시계와 같은) 착용가능 디바이스는 결제 서버 단말과의 통신 상호작용을 수행할 수 없으며, 사용자는 단말 디바이스를 통한 정보 상호작용을 수행하여 결제를 달성하는 것이 불가능하다. 대안적으로, (이동 전화기와 같이) 네트워크에 연결될 수 있는 단말 디바이스는, 오프라인 상태에 있을 때, 결제 서버 단말과 온라인 통신을 할 수 없으며, 사용자는 또한, 그러한 오프라인 단말 디바이스를 통해 정보 상호작용을 수행하여 결제를 달성하는 것이 불가능하다. 요약하면, 위 상황들

중 어느 하나에서, 사용자는 결제를 달성하기 위해 이러한 오프라인 단말 디바이스를 통해 정보 상호작용을 수행할 수 없다.

발명의 내용

과제의 해결 수단

[0004] 본 출원의 목적은 단말 디바이스가 오프라인 상태에 있을 때 안전하고 편리한 결제가 여전히 달성될 수 있도록 하기 위한, 정보 상호작용 방법, 장치, 및 시스템을 제공하는 것이다.

[0005] 본 출원은 다음을 포함하는 정보 상호작용 방법을 제공한다:

[0006] 제1 서버 단말에 의해 발행된 인증 인자(authentication factor)(상기 인증 인자는 사용자의 계정 정보와 인증키를 운반함), 및 동적 시간 인자를 단말에 의해 수신하는 단계 - 상기 제1 서버 단말은, 상기 단말이 제1 서비스 조작을 요청할 때 상기 단말을 인증한 후 상기 제1 서비스 조작을 완료하는 서버 단말임 -;

[0007] 상기 인증 인자 및 상기 단말의 디바이스 정보를 이용하여 결합된 인증 정보를 생성하고, 상기 결합된 인증 정보에 따라 상기 제1 서버 단말이 제1 서비스 조작에 대한 인가(authorization)를 수행하도록, 상기 결합된 인증 정보를 제1 서버 단말에 반송하는 단계; 및

[0008] 상기 인증 인자에 따라 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 생성하는 단계 - 상기 그래픽 식별자는 제1 서비스 조작의 인증 정보를 운반하고, 상기 제1 서비스 조작의 인증 정보는 상기 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고, 상기 동적 패스워드는 동적 시간 인자에 따라 생성되며, 상기 디바이스 계정 정보는 상기 단말의 디바이스 정보 및 상기 사용자의 계정 정보에 따라 생성됨 -.

[0009] 다른 양태에서, 본 출원은 다음을 포함하는 정보 상호작용 방법을 더 제공한다:

[0010] 제2 서버 단말에 의해, 단말 상에서 디스플레이된 그래픽 식별자 내에서 운반된 제1 서비스 조작의 인증 정보를 획득하는 단계 - 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함함 -;

[0011] 상기 제1 서비스 조작의 인증 정보와 서비스 데이터를 이용하여 제1 서비스 조작 요청을 생성하고, 상기 제1 서버 단말이 상기 제1 서비스 조작 요청 내에서 운반된 제1 서비스 조작의 인증 정보에 따라 인증을 수행하고 인증이 성공된 후 상기 제1 서비스 조작을 완료하도록, 상기 제1 서비스 조작 요청을 상기 제1 서버 단말에 송신하는 단계; 및

[0012] 상기 제1 서버 단말에 의해 반송된 상기 제1 서비스 조작의 결과를 수신하는 단계.

[0013] 또다른 양태에서, 본 출원은 다음을 포함하는 정보 상호작용 방법을 더 제공한다:

[0014] 제1 서버 단말에 의해, 제2 서버 단말에 의해 송신된 제1 서비스 조작 요청을 수신하는 단계 - 상기 제1 서비스 조작 요청은, 단말 상에서 디스플레이된 그래픽 식별자 내에서 운반된 제1 서비스 조작의 인증 정보 및 서비스 데이터를 획득함으로써 제2 서버 단말에 의해 생성된 요청이고, 상기 제1 서비스 조작 요청은 제1 서비스 조작의 인증 정보 및 서비스 데이터를 운반하며, 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함함 -; 및

[0015] 상기 제1 서비스 조작 요청 내에서 운반된 인증 정보에 따라 인증을 수행하고, 상기 인증이 성공된 경우, 상기 제1 서버 단말에 의해, 상기 제1 서비스 조작을 완료하는 단계.

[0016] 또다른 양태에서, 본 출원은 다음을 포함하는 단말을 더 제공한다:

[0017] 제1 서버 단말에 의해 발행된 인증 인자(상기 인증 인자는 사용자의 계정 정보와 인증키, 및 동적 시간 인자를 운반함)를 수신하도록 구성된 수신 유닛 - 상기 제1 서버 단말은, 상기 단말이 제1 서비스 조작을 요청할 때 상기 단말을 인증한 후 상기 제1 서비스 조작을 완료하는 서버 단말임 -;

[0018] 상기 수신 유닛에 의해 수신된 인증 인자와 상기 단말의 디바이스 정보를 이용하여 결합된 인증 정보를 생성하도록 구성된 결합 유닛;

[0019] 상기 제1 서버 단말이 상기 결합된 인증 정보에 따라 제1 서비스 조작에 대한 인가를 수행하도록, 상기 결합 유닛에 의해 생성된 결합된 인증 정보를 제1 서버 단말에 반송하도록 구성된 송신 유닛; 및

[0020] 상기 수신 유닛에 의해 수신된 상기 인증 인자에 따라 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 생성하도록 구성된 처리 유닛 - 상기 그래픽 식별자는 제1 서비스 조작의 인증 정보를 운반하고, 상기 제1 서비스 조작의 인증 정보는 상기 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고, 상기 동적 패스워드는 동적 시간 인자에 따라 생성되며, 상기 디바이스 계정 정보는 상기 단말의 디바이스 정보 및 상기 사용자의 계정 정보에 따라 생성됨 -.

[0021] 또다른 양태에서, 본 출원은 다음을 포함하는 서버 단말을 더 제공한다:

[0022] 단말 상에서 디스플레이된 그래픽 식별자 내에서 운반된 제1 서비스 조작의 인증 정보를 획득하도록 구성된 획득 유닛 - 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함함 -;

[0023] 상기 획득 유닛에 의해 획득된 제1 서비스 조작의 인증 정보와 서비스 데이터를 이용하여 제1 서비스 조작 요청을 생성하도록 구성된 처리 유닛;

[0024] 상기 제1 서버 단말이 상기 제1 서비스 조작 요청 내에서 운반된 제1 서비스 조작의 인증 정보에 따라 인증을 수행하고 인증이 성공된 후 상기 제1 서비스 조작을 완료하도록, 상기 처리 유닛에 의해 생성된 상기 제1 서비스 조작 요청을 상기 제1 서버 단말에 송신하도록 구성된 송신 유닛; 및

[0025] 상기 제1 서버 단말에 의해 반송된 상기 제1 서비스 조작의 결과를 수신하도록 구성된 수신 유닛.

[0026] 또다른 양태에서, 본 출원은 다음을 포함하는 서버 단말을 더 제공한다:

[0027] 제2 서버 단말에 의해 송신된 제1 서비스 조작 요청을 수신하도록 구성된 수신 유닛 - 상기 제1 서비스 조작 요청은, 단말 상에서 디스플레이된 그래픽 식별자 내에서 운반된 제1 서비스 조작의 인증 정보 및 서비스 데이터를 획득함으로써 제2 서버 단말에 의해 생성된 요청이고, 상기 제1 서비스 조작 요청은 제1 서비스 조작의 인증 정보 및 서비스 데이터를 운반하며, 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함함 -; 및

[0028] 상기 수신 유닛에 의해 수신된 상기 제1 서비스 조작 요청 내에서 운반된 상기 제1 서비스 조작의 인증 정보에 따라 인증을 수행하도록 구성된 처리 유닛 - 상기 인증이 성공된 경우, 상기 제1 서버 단말이 상기 제1 서비스 조작을 완료함 -.

[0029] 또다른 양태에서, 본 출원은 다음을 포함하는 전자 디바이스를 더 제공한다:

[0030] 디스플레이;

[0031] 프로세서; 및

[0032] 제1 서버 단말에 의해 발행된 인증 인자, 및 상기 인증 인자에 따라 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 생성하기 위한 프로그램을 저장하도록 구성된 메모리 - 상기 프로그램이 상기 프로세서에 의해 실행될 때, 상기 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자가 상기 디스플레이의 디스플레이 영역에서 디스플레이되고, 상기 그래픽 식별자는 제1 서비스 조작의 인증 정보를 운반하고, 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고, 상기 동적 패스워드는 동적 시간 인자에 따라 생성되며, 상기 디바이스 계정 정보는 상기 단말의 디바이스 정보 및 상기 사용자의 계정 정보에 따라 생성됨 -.

[0033] 또다른 양태에서, 본 출원은 단말, 제1 서버 단말, 및 제2 서버 단말을 포함하는 정보 상호작용 시스템을 더 제공하고;

[0034] 상기 단말은, 오프라인 상태에서, 제1 서비스 조작을 완료하기 위한 그래픽 식별자 - 상기 그래픽 식별자는 상기 제1 서비스 조작의 인증 정보를 운반함 - 를 디스플레이하고, 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고,

[0035] 상기 제2 서버 단말은 상기 그래픽 식별자 내에서 운반된 제1 서비스 조작의 인증 정보를 획득하고,

[0036] 상기 제2 서버 단말은 상기 제1 서비스 조작의 인증 정보 및 서비스 데이터를 이용하여 제1 서비스 조작 요청을 생성하고, 상기 제1 서비스 조작 요청을 상기 제1 서버 단말에 송신하며,

[0037] 상기 제1 서버 단말은 상기 제1 서비스 조작 요청 내에서 운반된 상기 제1 서비스 조작의 인증 정보에 따라 인

증을 수행하며, 상기 인증이 성공된 경우, 상기 제1 서버 단말은 상기 제1 서비스 조작을 완료한다.

발명의 효과

[0038] 본 출원의 실시예들에서 제공된 정보 상호작용 방법, 장치, 및 시스템에서, 오프라인 서비스 조작을 위한 동적 그래픽 식별자가 결합된 인증 정보 및 동적 시간 인자를 통해 생성되고, 오프라인 상태에 있는 단말은 안전한 결제를 달성하기 위해 상기 그래픽 식별자를 이용하여 정보 상호작용을 수행할 수 있거나, 또는 네트워크에 연결될 수 없는 단말 디바이스는 또한 안전한 결제를 달성하기 위해 상기 그래픽 식별자를 이용하여 정보 상호작용을 수행할 수 있다. 본 출원은 단말 디바이스가 오프라인 상태에 있을 때 안전하고 편리한 결제를 달성할 수 있다.

도면의 간단한 설명

[0039] 본 발명의 실시예들에서의 기술적 해결책을 보다 명확하게 설명하기 위해, 이하에서는 실시예들을 설명하기 위해 필요한 첨부 도면을 간단히 소개한다. 명백하게, 이하의 설명에서의 첨부 도면들은 본 출원의 일부 실시예들을 단지 보여줄 뿐이며, 당업자는 창의적인 노력 없이 이들 첨부 도면들로부터 다른 도면들을 계속해서 유도할 수 있다.

도 1은 본 출원의 실시예에 따른 정보 상호작용 시스템의 개략적인 구조도이다.

도 2는 본 출원의 실시예에 따른 다른 정보 상호작용 시스템의 개략적인 구조도이다.

도 3a는 본 출원의 실시예에 따른 단말측에서의 정보 상호작용 방법의 흐름도이다.

도 3b는 본 출원의 실시예에 따른 오프라인 결제 동안의 단말측의 방법 흐름도이다.

도 4는 본 출원의 실시예에 따른 제2 서버 단말측에서의 정보 상호작용 방법의 흐름도이다.

도 5a는 본 출원의 실시예에 따른 제1 서버 단말측에서의 정보 상호작용 방법의 흐름도이다.

도 5b는 본 출원의 실시예에 따른 오프라인 결제 인가 동안의 제1 서버 단말측의 방법 흐름도이다.

도 5c는 본 출원의 실시예에 따른 오프라인 결제 인가 동안의 다른 제1 서버 단말측의 방법 흐름도이다.

도 6은 본 출원의 실시예에 따른 정보 상호작용 방법의 상호작용도이다.

도 7은 본 출원의 실시예에 따른 (이동 전화기) 오프라인 결제 인가 동안의 상호작용도이다.

도 8은 본 출원의 실시예에 따른 다른 (스마트 시계) 오프라인 결제 인가 동안의 상호작용도이다.

도 9는 본 출원의 실시예에 따른 단말의 개략적인 구조도이다.

도 10은 본 출원의 실시예에 따른 제2 서버 단말의 개략적인 구조도이다.

도 11은 본 출원의 실시예에 따른 제1 서버 단말의 개략적인 구조도이다.

도 12는 본 출원의 실시예에 따른 전자 디바이스의 구성의 개략적인 구조도이다.

발명을 실시하기 위한 구체적인 내용

[0040] 본 출원의 목적, 특징, 및 장점을 보다 명백하게 하고 이해하기 쉽게 하기 위해, 본 출원의 실시예들에서의 기술적 해결책들을 본 출원의 실시예들에서의 도면들을 참조하여 아래에서 설명할 것이다. 명백한 바와 같이, 설명된 실시예들은 본 출원의 모든 실시예들이라기 보다는 그 중 일부일 뿐이다. 본 출원의 실시예들에 기초하여, 당업자에 의해 창의적인 노력 없이 획득되는 다른 실시예들은 모두 본 출원의 보호 범위 내에 있다.

[0041] 본 출원의 실시예들에서 제공되는 정보 상호작용 방법 및 장치는 모든 유형의 지능형 이동 단말 디바이스, 예컨대, 스마트 폰, 태블릿 컴퓨터, 및 다른 단말 디바이스에 적용가능하며, 특히, 네트워크 연결 기능을 갖지 않는 스마트 착용식 디바이스들, 예컨대, 스마트 시계, 스마트 팔찌, 및 기타 디바이스에 적용가능하다.

[0042] 도 1은 본 출원의 실시예에 따른 정보 상호작용 시스템의 개략적인 구조도이다. 도 1에서는 단말(1), 판매자 서버 단말(2)(제2 서버 단말), 및 결제 서버 단말(3)(제1 서버 단말)이 도시되어 있다. 본 도면에서의 단말(1)은 네트워크 연결 기능을 갖는 단말, 예컨대, 스마트 폰, 태블릿 컴퓨터 등이며, 단말(1)은 결제 서버 단말(3)과의 네트워크 연결을 가질 수 있다. 도면에서 점선은, 실제 사용 시나리오에서, 단말(1)이 결제 서버 단말(3)에 대

한 네트워크 연결을 구축하는데 실패했음을 나타낸다. 단말(1)은, 온라인 상태에 있는 경우, 결제 서버 단말(3)에 대한 네트워크 연결을 구축할 수 있고, 단말(1)은 결제 서버 단말(3)에게 오프라인 결제 인가를 수행할 것을 요청한다. 결제 서버 단말(3)은, 인가 검증 후, 단말(1)에게 인증 인자를 발행한다. 실제 사용의 시나리오에서, 단말(1)은 오프라인 상태에 있으며, 결제 인증 정보를 운반하고 결제 서버 단말(3)에 의해 발행된 인증 인자에 따라 생성된 그래픽 식별자를 스크린 상에 디스플레이한다. 판매자 서버 단말(2)은 그래픽 식별자를 스캐닝하여 결제 인증 정보를 획득하고, 결제 인증 정보 및 주문 정보로부터 결제 요청을 생성하며, 결제 요청을 결제 서버 단말(3)에 송신한다. 결제 서버 단말(3)은 결제 인증 정보를 검증하고, 검증이 성공된 경우, 결제 서버 단말(3)은 결제를 수행한다.

[0043] 여기서, 판매자 서버 단말(2)은 포그라운드(foreground) 코드 스캐닝 말단기(21) 및 백엔드 서버 단말(22)을 포함한다. 포그라운드 코드 스캐닝 말단기(21)는 단말(1) 상에서 디스플레이되는 그래픽 식별자를 스캔하는 코드 스캐닝 건(code scanning gun)과 함께 주로 설치되어, 그래픽 식별자를 백엔드 서버 단말(22)에 송신한다. 백엔드 서버 단말(22)은 주로 포그라운드 코드 스캐닝 말단기(21)의 파라미터들을 검사하고, 이를 추출하여 그래픽 식별자 내의 결제 인증 정보를 획득한다. 백엔드 서버 단말(22)은, 판매자의 주문 파라미터들을 사전처리한 후, 결제 서버 단말(3)에게 주문 생성 및 결제 요청을 제출한다.

[0044] 도 2는 본 출원의 실시예에 따른 다른 정보 상호작용 시스템의 개략적인 구조도이다. 도 1과의 차이점은, 도 2에서의 단말(1)은 네트워크 연결 기능을 갖지 않는 단말, 예를 들어, 스마트 시계, 스마트 팔찌, 및 기타 착용 가능형 디바이스들이고, 단말(1)은 결제 서버 단말(3)과의 네트워크 연결을 구축할 수 없지만, 단말(1)은 (블루투스와 같은) 다른 통신 모듈들을 통해 네트워크 연결 기능을 갖는 제2 단말(4)로의 연결을 구축할 수 있고, 제2 단말(4)을 통해, 결제 서버 단말(3)에 의해 발행된 인증 인자를 획득할 수 있다는 점이다. 도면에서 점선들은, 오프라인 결제 인가 후에, 실제 사용 시나리오에서, 네트워크 연결 기능을 갖는 제2 단말(4)이 필요하지 않을 수 있음을 나타낸다. 이하, 특정 정보 상호작용 프로세스가 소개된다.

[0045] 도 3a는 본 출원의 실시예에 따른 단말측에서의 정보 상호작용 방법의 흐름도이다. 도 3a에서 도시된 바와 같이, 본 출원의 실시예의 정보 상호작용 방법은 다음을 포함한다:

[0046] S101. 단말은 제1 서버 단말에 의해 발행된 인증 인자를 수신한다.

[0047] 인증 인자는 사용자의 계정 정보와 인증키, 및 동적 시간 인자를 운반한다.

[0048] 여기서, 제1 서비스 조작은 (결제 금액 및 바우처 상각(voucher write-off)과 같은) 가상 자원들에 대한 네트워크 교환 조작들을 포함한다.

[0049] 상기 제1 서버 단말은, 상기 단말이 제1 서비스 조작을 요청할 때 상기 단말을 인증한 후 상기 제1 서비스 조작을 완료하는 서버 단말이다.

[0050] 예시를 위해, 본 출원은 제1 서비스 조작의 예로서 결제를 예를 들고, 오프라인 제1 서비스 조작의 예로서 오프라인 결제를 예를 들고, 제1 서비스 조작 요청의 예로서 결제 요청을 예를 들고, 제1 서버 단말의 예로서 결제 서버 단말을 예를 들고, 제2 서버 단말의 일례로서 판매자 서버 단말을 예를 들며, 다른 가상 자원들에 대한 네트워크 교환 조작들이 상기와 마찬가지이다.

[0051] 단말은, 온라인 상태에 있을 때, 제1 서버 단말에 대한 네트워크 연결을 구축하고, 제1 서버 단말로부터 오프라인 결제 인증을 요청한다. 제1 서버 단말은 인증 검증이 성공된 후 단말에 인증 인자를 발행한다.

[0052] 구체적으로, 다음과 같은 단계들이 포함될 수 있다: 단말에 의해, 계정 신원 검증 요청을 제1 서버 단말에 송신하는 단계; 신원 검증이 성공된 후 제1 서버 단말에 의해 송신된 검증 결과를 수신하는 단계; 오프라인 결제 인가에 대한 검증 요청을 제1 서버 단말에 송신하는 단계; 및 인가 검증이 성공된 후 제1 서버 단말에 의해 발행된 인증 인자를 수신하는 단계.

[0053] S102. 인증 인자 및 단말의 디바이스 정보를 이용하여 결합된 인증 정보가 생성되고, 결합된 인증 정보에 따라 제1 서버 단말이 제1 서비스 조작에 대한 인가를 수행하도록, 결합된 인증 정보가 제1 서버 단말에 반송된다.

[0054] 오프라인 상태에서 안전하고 편리한 결제를 달성하기 위해, 단말은, 오프라인 결제 동안에 인가받도록, 온라인 상태에 있을 때, 제1 서버 단말에 의해 발행된 인증 인자와 디바이스 정보의 결합에 대한 인증 검증을 수행할 것을 제1 서버 단말에 요청할 필요가 있다.

[0055] S103. 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자가 인증 인자에 따라 생성되며, 이 그래픽

식별자는 제1 서비스 조작의 인증 정보를 운반한다.

[0056] 제1 서비스 조작의 인증 정보, 즉, 결제 인증 정보는, 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고, 동적 패스워드는 동적 시간 인자에 따라 생성되며, 디바이스 계정 정보는 단말의 디바이스 정보 및 사용자의 계정 정보에 따라 생성된다. 그래픽 식별자는 QR 코드 또는 바코드이다.

[0057] 여기서, 동적 패스워드는 동일한 시간 창에서 변경되지 않은 상태로 있으며, 다음번 시간 창에서, 동적 패스워드는 동적 시간 인자에 따라 재생성되어 동적으로 변경된다. 이는 결제 인증 정보의 안전성을 보장함으로써 위조 방지 목적을 달성할 수 있다.

[0058] 동적 패스워드는 구체적으로, 일회용 패스워드 계산 방법에 따라, 사용자의 인증키, 동적 시간 인자, 디바이스 계정 정보, 및 미리 설정된 패스워드 길이를 이용한 계산을 통해 얻어진다.

[0059] 그래픽 식별정보의 디스플레이 모드가 QR 코드인 경우에는, 많은 양의 정보를 운반할 수 있어서, 일회용 패스워드의 미리 설정된 패스워드 길이를 증가시키고 안전성을 향상시킨다.

[0060] 오프라인 상태에 있는 단말은, 결제를 수행할 필요가 있을 때, 오프라인 결제를 위한 그래픽 식별자 - 이 그래픽 식별자는, 그래픽 식별자 내에서 운반된 결제 인증 정보를 획득하도록 판매자 말단기에 의해 스캐닝됨 - 를 생성하여, 제2 서버 단말을 통해 오프라인 결제를 완료한다.

[0061] 구체적으로, 도 3b에서 도시된 바와 같이, S103은 다음 단계들을 포함할 수 있다:

[0062] S1031. 오프라인 결제를 위한 그래픽 식별자를 디스플레이하기 위한 디스플레이 명령이 수신된다.

[0063] S1032. 오프라인 결제를 위한 그래픽 식별자가 인증 인자에 따라 생성된다.

[0064] S1033. 단말은, 그래픽 식별자를 사용하여 오프라인 상태에서 결제를 수행하도록 그래픽 식별자를 디스플레이한다.

[0065] 그래픽 식별자의 디스플레이 모드는 바코드 및 QR 코드 중 하나 또는 이들의 조합을 포함한다.

[0066] 선택적으로, 단말이 그래픽 식별자를 디스플레이한 후, 본 방법은 다음을 더 포함한다: S1034, 그래픽 식별자의 디스플레이 모드에 대한 전환 명령이 수신될 때 그래픽 식별자의 디스플레이 모드가 전환된다.

[0067] 그래픽 식별자의 디스플레이 모드에 대한 전환 명령이 수신된 경우, 그래픽 식별자의 현재 디스플레이 모드가 QR 코드이면, 디스플레이 모드는 바코드로 전환되고; 반대로, 그래픽 식별자의 현재 디스플레이 모드가 바코드이면, 디스플레이 모드는 QR 코드로 전환된다.

[0068] 제1 서버 단말에 대한 네트워크 연결을 직접 구축할 수 없는 (스마트 시계와 같은) 단말은, 제1 서버 단말에 대한 네트워크 연결을 구축할 수 있는 (스마트 폰과 같은) 제2 단말을 통하여, 제1 서버 단말에 의해 발행된 인증 인자를 수신할 수 있고; 결합된 인증 정보를 제2 단말을 통해 제1 서버 단말에 반송할 수 있다.

[0069] 구체적으로 아래의 단계들이 포함된다: 온라인 상태에 있는 제2 단말에 의해, 계정 신원 검증 요청을 제1 서버 단말에 송신하는 단계; 신원 검증이 성공된 후 제1 서버 단말에 의해 송신된 검증 결과를 제2 단말에 의해 수신하는 단계; 오프라인 결제 인가에 대한 검증 요청을, 온라인 상태에 있는 제2 단말에 의해, 제1 서버 단말에 송신하는 단계; 및 인가 검증이 성공된 후 제1 서버 단말에 의해 발행된 인증 인자를 제2 단말에 의해 수신하는 단계.

[0070] 인증 인자를 획득한 후, 제2 단말은 인증 인자를 단말에 송신한다. 마찬가지로, 단말은, 인증 인자를 획득한 후, 인증 인자를 단말의 디바이스 정보와 결합시키고, 제2 단말을 통해 결합된 인증 정보를 송신하여, 제1 서버 단말은 결합된 인증 정보에 따라 단말의 결제에 대한 인가를 수행함으로써 단말의 오프라인 결제를 달성하게 된다.

[0071] 구체적으로, 단말의 관리 프로그램이 제2 단말에 설치된다. 예를 들어, 스마트 폰에 스마트 시계의 관리 애플리케이션(관리 APP)이 설치되어 있는 경우, 스마트 폰의 APP는 결제 계정 로그인 체크와 같은 로그인, 결제 인증, 및 기타 스마트 폰 기능들을 통합하고, APP를 통해, 스마트 폰은 스마트 시계와의 블루투스 통신, 인증 파라미터들(인증 인자)을 스마트 시계에 송신하는 것, 및 제1 서버 단말 및 스마트 시계와의 안전한 통신을 처리하는 것과 같은 기능들을 수행할 수 있다. 스마트 시계는 스마트 폰과의 안전한 통신을 완료하고, 결제 인증 정보의 생성 파라미터를 저장 및 업데이트하고, 또한 결제 인증 정보의 생성 파라미터에 따라 결제 인증 정보를 생성하고, 결제 인증 정보를 QR 코드 또는 바코드의 형태로 디스플레이한다.

[0072] 도 4는 본 출원의 실시예에 따른 제2 서버 단말측에서의 정보 상호작용 방법의 흐름도이다. 도 4에서 도시된 바와 같이, 본 출원의 실시예의 정보 상호작용 방법은 다음을 포함한다:

[0073] S201. 제2 서버 단말은 단말 상에서 디스플레이된 그래픽 식별자 내에서 운반된 결제 인증 정보를 획득한다.

[0074] 결제 인증 정보는 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함한다.

[0075] 제2 서버 단말은 포그라운드 코드 스캐닝 말단기 및 백엔드 서버 단말을 포함한다. 포그라운드 코드 스캐닝 말단기는 단말 상에서 QR 코드 또는 바코드의 형태로 디스플레이되는 그래픽 식별자를 스캔하는 코드 스캐닝 건(code scanning gun)과 함께 주로 설치되어, 그래픽 식별자를 백엔드 서버 단말에 송신한다. 백엔드 서버 단말은 주로 포그라운드 코드 스캐닝 말단기의 파라미터들을 검사하고, 이를 추출하여 그래픽 식별자 내의 결제 인증 정보를 획득한다.

[0076] S202. 결제 인증 정보 및 서비스 데이터를 이용하여 결제 요청이 생성되고, 제1 서버 단말이 결제 요청 내에서 운반된 결제 인증 정보에 따라 결제 인증을 수행하고 결제 인증이 성공된 경우 결제를 수행하도록, 이 결제 요청은 제1 서버 단말에 송신된다.

[0077] 제2 서버 단말의 백엔드 서버 단말은 서비스 데이터(판매자의 주문 파라미터들)를 사전처리하고, 결제 인증 정보 및 서비스 데이터로부터 주문 및 결제 요청을 생성하고, 주문 및 결제 요청을 제1 서버 단말에 전송한다.

[0078] S203. 제1 서버 단말에 의해 반송된 결제 결과가 수신된다.

[0079] 제1 서버 단말이 결제 인증 검증을 완료하고 결제를 수행한 후, 제2 서버 단말은 제1 서버 단말에 의해 반송된 결제 결과를 수신한다.

[0080] 도 5a는 본 출원의 실시예에 따른 제1 서버 단말측에서의 정보 상호작용 방법의 흐름도이다. 도 5a에서 도시된 바와 같이, 본 출원의 실시예의 정보 상호작용 방법은 다음을 포함한다:

[0081] S301. 제1 서버 단말은 제2 서버 단말에 의해 송신된 결제 요청을 수신하고, 결제 요청은 결제 인증 정보 및 서비스 데이터를 운반한다.

[0082] 결제 인증 정보는 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함한다.

[0083] 단말이 오프라인 상태에 있는 경우, 제1 서버 단말은 제2 서버 단말에 의해 송신된 결제 요청을 수신하고, 결제 요청은 단말의 결제 인증 정보를 운반한다.

[0084] S302. 결제 요청 내에서 운반된 결제 인증 정보에 따라 결제 인증이 수행되며, 결제 인증이 성공된 경우, 제1 서버 단말은 결제를 수행한다.

[0085] 구체적으로, 결제 요청 내에서 운반된 결제 인증 정보에 따라 결제 인증을 수행하는 단계는 구체적으로, 결제 인증 정보 내에서 운반된 디바이스 계정 정보와 인증키의 결합 관계가 정확한지 여부를 체크하는 단계, 및 인증 인자 내의 동적 시간 인자에 따라 동적 패스워드가 유효한지 여부를 체크하는 단계를 포함하고, 상기 결합 관계가 정확하고 상기 동적 패스워드가 유효한 경우, 결제 인증은 성공이다.

[0086] 제2 서버 단말에 의해 송신된 결제 요청을 수신하는 S301 전에, 상기 방법은,

[0087] 제1 서버 단말에 의해, 단말 상의 온라인 계정 결합을 수행하는 단계를 더 포함한다.

[0088] 단말은, 온라인 상태에 있을 때, 먼저 제1 서버 단말과의 온라인 계정 결합을 수행할 필요가 있다.

[0089] 도 5b에서 도시된 바와 같이, 제1 서버 단말에 의해, 단말 상의 온라인 계정 결합을 수행하는 단계는 구체적으로 다음을 포함한다:

[0090] S401. 제1 서버 단말이 단말에 의해 송신된 계정 신원 검증 요청을 수신한다.

[0091] 계정 신원 검증 요청은 사용자의 계정 정보를 운반한다.

[0092] S402. 계정 신원 검증 요청이 검증을 통과하였는지 여부를 판단하고, 상기 검증이 성공된 경우, 성공된 검증의 결과가 단말에 송신된다.

[0093] S403. 단말에 의해 송신된 오프라인 결제 인가 검증을 위한 검증 요청이 수신된다.

[0094] S404. 검증 요청에 대한 검증이 성공되었는지의 여부를 판단하고, 검증이 성공된 경우, 사용자의 인증키가 생성

되고, 제1 서버 단말의 동적 시간 인자가 계산된다.

[0095] S405. 인증 인자가 인증키, 동적 시간 인자, 및 사용자의 계정 정보를 사용하여 생성된다.

[0096] S406. 인증 인자가 단말에 발행된다.

[0097] S407. 단말에 의해 제출된 결합된 인증 정보가 수신되고, 이 결합된 인증 정보는 인증 인자와 디바이스 계정 정보를 결합함으로써 생성된 것이다.

[0098] S408. 결합된 인증 정보에 대해 인가 검증이 수행되고, 인가가 성공된 경우, 오프라인 결제 인가 검증은 완료된다.

[0099] 선택적으로, 사용자의 인증키를 생성하는 S404 후, 본 방법은, 인증키 및 사용자의 계정 정보로부터 압축된 문자열을 생성하는 단계를 더 포함하며, 압축된 문자열은 인증키 및 사용자의 계정 정보와 일대일 매핑 관계를 갖는다. 이러한 방식으로, 저장 공간이 절약될 수 있으므로, 디바이스 계정의 지나치게 긴 식별 정보가 제한된 패스워드 길이에서 디스플레이될 수 없다는 문제점을 피할 수 있다. 결제 인증 정보가 수신되면, 압축된 문자열을 통해 일대일 대응 인증키 및 사용자의 계정 정보가 또한 발견될 수 있다.

[0100] S405에서는, 인증키, 압축된 문자열, 및 동적 시간 인자를 이용하여 인증 인자가 생성된다. 구체적으로는, SN이 인증 인자를 나타내고, key가 사용자의 인증키를 나타내고, Seq가 디바이스 계정 정보의 압축된 문자열을 나타내고, UserId가 계정 식별 정보를 나타내고, Did가 디바이스 식별 정보를 나타내고, timestamp가 동적 시간 인자를 나타내고, N이 미리 설정된 패스워드 길이를 나타내고, Zip이 일대일 매핑 관계를 나타내고, OTP가 동적 패스워드를 나타내고, Tag가 인증 정보 태그를 나타내면, 인증 인자는 다음의 방정식들을 사용하여 획득될 수 있다:

[0101] Seq = Zip(UserId, Did)

[0102] OTP = HOTP(Key, Tag + Seq + timestamp, N)

[0103] SN = Tag + Seq + OTP

[0104] Seq = Zip(UserId, Did)을 통해, 디바이스 식별 정보 및 계정 식별 정보가 먼저 디바이스 계정 정보의 압축된 문자열 Seq로 압축되고, 이어서 동적 패스워드 OTP가 HMAC(Hash Message Authentication Code) 기반 일회용 패스워드(one-time password; HOTP) 알고리즘에 따른 계산을 통해 획득되며, 인증 인자 SN은 인증 정보 태그 Tag, 압축된 문자열 Seq, 및 동적 패스워드 OTP의 조합을 통해 획득된다는 것을 살펴볼 수 있다.

[0105] 제1 서버 단말에 대한 네트워크 연결을 직접 구축할 수 없는 단말은 제1 서버 단말에 대한 네트워크 연결을 구축할 수 있는 제2 단말을 통해 온라인 계정 결합을 수행한다. 도 5c에서 도시된 바와 같이, 제1 서버 단말에 의해, 단말 상의 온라인 계정 결합을 수행하는 단계는, 도 5b와 유사하며, 구체적으로 다음을 포함한다:

[0106] S501. 제1 서버 단말이 제2 단말에 의해 송신된 계정 신원 검증 요청을 수신한다.

[0107] 계정 신원 검증 요청은 사용자의 계정 정보를 운반한다.

[0108] S502. 계정 신원 검증 요청이 검증을 통과하였는지 여부를 판단하고, 상기 검증이 성공된 경우, 성공된 검증의 결과가 제2 단말에 송신된다.

[0109] S503. 제2 단말에 의해 송신된 오프라인 결제 인가 검증을 위한 검증 요청이 수신된다.

[0110] S504. 검증 요청에 대한 검증이 성공되었는지의 여부를 판단하고, 검증이 성공된 경우, 사용자의 인증키가 생성되고, 제1 서버 단말의 동적 시간 인자가 계산된다.

[0111] S505. 인증 인자가 인증키, 동적 시간 인자, 및 사용자의 계정 정보를 사용하여 생성된다.

[0112] S506. 인증 인자가 제2 단말에 발행된다.

[0113] S507. 단말에 의해 반송되고 제2 단말에 의해 제출된 결합된 인증 정보가 수신되고, 이 결합된 인증 정보는 인증 인자와 디바이스 계정 정보를 결합함으로써 생성된 것이다.

[0114] S508. 결합된 인증 정보에 대해 인가 검증이 수행되고, 인가가 성공된 경우, 오프라인 결제 인가 검증은 완료된다.

[0115] 제1 서버 단말의 성공적인 인가의 결과를 수신한 후, 제2 단말은 이 결과를 단말에 송신한다.

[0116] 도 6은 본 출원의 실시예에 따른 정보 상호작용 방법의 상호작용도이며, 도 6에서 도시된 바와 같이, 본 방법은 다음을 포함한다:

[0117] S601. 단말은 그래픽 식별자를 디스플레이하기 위한 디스플레이 명령을 수신하고, 그래픽 식별자의 프리젠테이션 인터페이스로 전환한다.

[0118] 사용자가 판매자와의 주문 내용 및 금액을 결정한 후, 사용자는 단말을 조작하여 오프라인 결제를 위한 그래픽 식별자를 디스플레이하게 한다. 단말은 사용자의 디스플레이 명령을 수신하고, 그래픽 식별자의 프리젠테이션 인터페이스로 전환한다.

[0119] S602. 단말은 인증 인자에 따라 결제 인증 정보를 생성한다.

[0120] 결제 인증 정보는 QR 코드의 형태로 제공되는 결제 인증 정보일 수 있으며, 바코드의 형태로 제공되는 결제 인증 정보일 수도 있다.

[0121] S603. 단말은 코드 스캐닝의 사용을 위해, 인터페이스 및 코드 스캐닝 건의 유형에 따라 그래픽 식별자를 제공한다.

[0122] 단말은, 사용자의 조작 명령 하에, 필요한 프리젠테이션 모드에 따라 그래픽 식별자를 제공한다.

[0123] S604. 제2 서버 단말의 포그라운드 코드 스캐닝 말단기는 결제 인증 정보를 획득한다.

[0124] S605. 포그라운드 코드 스캐닝 말단기는 주문 정보에 대해 로컬 데이터 처리를 수행한다.

[0125] S606. 포그라운드 코드 스캐닝 말단기는 주문 정보 및 결제 인증 정보로부터 포그라운드 코드 스캐닝 말단기의 결제 요청을 생성하고, 포그라운드 코드 스캐닝 말단기의 결제 요청을 백엔드 서버 단말이 체크하도록, 결제 요청을 제2 서버 단말의 백엔드 서버 단말에 송신한다.

[0126] S607. 백엔드 서버 단말은 결제 인증 정보 및 주문 서비스 정보를 추출하여, 결제 요청을 생성하고, 결제 요청을 제1 서버 단말에 송신한다.

[0127] S608. 제1 서버 단말은, 결제 요청으로부터, 주문 서비스 정보 내의 판매자 정보 및 결제 인증 정보를 추출한다.

[0128] S609. 제1 서버 단말은 결제 인증 정보를 인증한다.

[0129] S610. 제1 서버 단말은, 인증이 성공된 경우, 결제를 수행한다.

[0130] S611. 제1 서버 단말은 결제 결과를 제2 서버 단말에 반송한다.

[0131] S612. 판매자의 직원은 결제 결과를 확인한다.

[0132] 이런 식으로, 사용자는 결제를 완료하고, 판매자는 상품을 인도한다.

[0133] 도 6에서의 단말은 온라인 계정 결합이 수행된 단말이다. 이하, 도 7 및 도 8을 통해 온라인 계정 결합 동안에서의 상호작용 프로세스를 소개한다. 여기서, 도 7의 단말은 제1 서버 단말에 대한 연결을 직접 구축할 수 있는 단말이고, 도 8의 단말은 제1 서버 단말에 대한 연결을 직접 구축할 수 없는 단말이다. 해결책에 대한 보다 상세한 설명을 하기 위해, 도 7의 단말은 이동 전화기이고, 도 8의 단말은 시계이고, 제2 단말은 이동 전화기이다.

[0134] 도 7은 본 출원의 실시예에 따른 (이동 전화기) 오프라인 결제 인가 동안의 상호작용도이며, 도 7에서 도시된 바와 같이, 다음의 단계들이 포함된다:

[0135] S701. 단말은, 온라인 상태에 있을 때, 계정 신원 검증 요청을 제1 서버 단말에 송신한다.

[0136] 계정 신원 검증 요청은 사용자의 계정 정보를 운반한다.

[0137] S702. 제1 서버 단말은 계정 신원 검증 요청이 검증을 통과하였는지 여부를 판단하고, 상기 검증이 성공된 경우, 성공된 검증의 결과가 단말에 송신되며, 그렇지 않은 경우에는, 프로세스는 실패로 끝난다.

[0138] S703. 단말은 오프라인 결제 인가에 대한 검증 요청을 제1 서버 단말에 송신한다.

[0139] S704. 제1 서버 단말은 검증 요청에 대한 검증이 성공되었는지 여부를 판단하고, 검증이 성공된 경우, 프로세스는 S705로 진행하며, 그렇지 않은 경우에는, 프로세스는 실패로 끝난다.

[0140] S705. 제1 서버 단말은 사용자의 인증키를 생성한다.

[0141] S706. 제1 서버 단말은 인증키 및 계정 정보로부터 압축된 문자열을 생성한다.

[0142] S707. 제1 서버 단말은 제1 서버 단말의 동적 시간 인자를 계산한다.

[0143] S708. 제1 서버 단말은 인증키, 동적 시간 인자, 및 사용자의 계정 정보를 이용하여 인증 인자를 생성한다.

[0144] S709. 제1 서버 단말은 인증 인자에 대해 통신 암호화 처리를 수행한다.

[0145] S710. 제1 서버 단말은 인증 인자를 단말에 반송한다.

[0146] S711. 단말은 인가 검증이 성공된 후에 제1 서버 단말에 의해 송신된 인증 인자를 수신한 후 단말의 디바이스 정보 및 인증 인자를 이용하여 결합된 인증 정보를 생성하고, 결합된 인증 정보를 제1 서버 단말에 제출한다.

[0147] S712. 제1 서버 단말은 결합된 인증 정보를 파싱(parse)하고, 계정, 인증키, 및 동적 시간 인자에 따라 인가가 성공되었는지 여부를 체크하며, 성공된 경우, 프로세스는 S713으로 진행하되, 성공되지 않은 경우에는 프로세스는 실패로 끝난다.

[0148] S713. 제1 서버 단말은, 결제 인가가 성공된 경우, 결제를 수행한다.

[0149] 도 8은 본 출원의 실시예에 따른 다른 (스마트 시계) 오프라인 결제 인가 동안의 상호작용도이며, 도 8에서 도시된 바와 같이, 다음의 단계들이 포함된다:

[0150] S801. 제2 단말은, 온라인 상태에 있을 때, 계정 신원 검증 요청을 제1 서버 단말에 송신한다.

[0151] 계정 신원 검증 요청은 사용자의 계정 정보를 운반한다.

[0152] S802. 제1 서버 단말은 계정 신원 검증 요청이 검증을 통과하였는지 여부를 판단하고, 상기 검증이 성공된 경우, 성공된 검증의 결과가 제2 단말에 송신되며, 그렇지 않은 경우에는, 프로세스는 실패로 끝난다.

[0153] S803. 제2 단말은 오프라인 결제 인가에 대한 검증 요청을 제1 서버 단말에 송신한다.

[0154] S804. 제1 서버 단말은 검증 요청에 대한 검증이 성공되었는지 여부를 판단하고, 검증이 성공된 경우, 프로세스는 S805로 진행하며, 그렇지 않은 경우에는, 프로세스는 실패로 끝난다.

[0155] S805. 제1 서버 단말은 사용자의 인증키를 생성한다.

[0156] S806. 제1 서버 단말은 제1 서버 단말의 동적 시간 인자를 계산한다.

[0157] S807. 제1 서버 단말은 인증키, 동적 시간 인자, 및 사용자의 계정 정보를 이용하여 인증 인자를 생성한다.

[0158] S808. 제1 서버 단말은 인증 인자에 대해 통신 암호화 처리를 수행한다.

[0159] S809. 제1 서버 단말은 인증 인자를 제2 단말에 반송하고, 제2 단말은 인증 인자를 획득하기 위해 파싱한다.

[0160] S810. 제2 단말은 인증 인자를 단말(시계)에 기록하고, 단말은 인증 인자를 수신한다.

[0161] S811. 단말은 인증 인자를 암호화된 방식으로 저장한다.

[0162] S812. 단말은 인증 인자와 단말의 디바이스 정보를 이용하여 결합된 인증 정보를 생성한다.

[0163] S813. 단말은 결합된 인증 정보를 제2 단말에 송신한다.

[0164] S814. 제2 단말은 결제 계정의 결합된 인증 정보를 제1 서버 단말에 제출한다.

[0165] S815. 제1 서버 단말은 결합된 인증 정보를 파싱(parse)하고, 계정, 인증키, 및 동적 시간 인자에 따라 인가가 성공되었는지 여부를 체크하며, 성공된 경우, 프로세스는 S816으로 진행하되, 성공되지 않은 경우에는 프로세스는 실패로 끝난다.

[0166] S816. 제1 서버 단말은, 결제 인가가 성공된 경우, 결제를 수행한다.

[0167] 본 출원의 실시예들에서 제공된 정보 상호작용 방법에서, 오프라인 결제를 위한 동적 그래픽 식별자가 결합된 결제 인증 정보 및 동적 시간 인자를 통해 생성되어, 오프라인 상태에 있는 단말 디바이스가 또한 그래픽 식별자를 사용하여 안전한 결제를 수행할 수 있고 안전하고 편리한 결제를 달성할 수 있도록 한다. 본 출원에서, 그래픽 식별자(바코드/QR 코드)는 계정, 디바이스, 동적 시간 인자 타임스탬프, 및 인증키에 관한 정보를 운반하

기 때문에, 결제 체크를 완료할지 여부를 결정함으로써 안전하고 편리한 오프라인 결제를 달성하도록, 제1 서버 단말은 계정, 디바이스, 및 인증키 간의 결합 관계는 물론, HOTP 시그너처 결과에 따라 일회용 패스워드의 유효성을 체크할 수 있다.

[0168] 상기에서는 본 출원의 실시예들에서 제공되는 정보 상호작용 방법에 대하여 상세하게 설명하였으며, 아래에서는 본 출원에 의해 제공되는 정보 상호작용 장치를 상세히 설명할 것이다.

[0169] 도 9는 본 출원의 실시예에 따른 단말의 개략적인 구조도이고, 도 9에서 도시된 바와 같이, 본 출원의 단말은, 수신 유닛(901), 결합 유닛(902), 송신 유닛(903), 및 처리 유닛(904)을 포함한다.

[0170] 수신 유닛(901)은 제1 서버 단말에 의해 발행된 인증 인자를 수신하도록 구성된다.

[0171] 인증 인자는 사용자의 계정 정보와 인증키, 및 동적 시간 인자를 운반한다.

[0172] 결합 유닛(902)은 수신 유닛(901)에 의해 수신된 인증 인자와 단말의 디바이스 정보를 이용하여 결합된 인증 정보를 생성하도록 구성된다.

[0173] 송신 유닛(903)은 제1 서버 단말이 상기 결합된 인증 정보에 따라 결제에 대한 인가를 수행하도록, 결합 유닛(902)에 의해 생성된 결합된 인증 정보를 제1 서버 단말에 반송하도록 구성된다.

[0174] 처리 유닛(904)은 수신 유닛(901)에 의해 수신된 인증 인자에 따라 오프라인 결제를 위한 그래픽 식별자를 생성하도록 구성되며, 그래픽 식별자는 결제 인증 정보를 운반한다.

[0175] 결제 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고, 상기 동적 패스워드는 동적 시간 인자에 따라 생성되며, 상기 디바이스 계정 정보는 상기 단말의 디바이스 정보 및 상기 사용자의 계정 정보에 따라 생성된다.

[0176] 선택적으로, 처리 유닛(904)이 그래픽 식별자를 생성하기 전에, 수신 유닛(901)은 또한 그래픽 식별자를 디스플레이하기 위한 디스플레이 명령을 수신하도록 구성된다. 처리 유닛(904)은, 수신 유닛(901)이 디스플레이 명령을 수신한 후, 인증 인자에 따라 오프라인 결제를 위한 그래픽 식별자를 생성하도록 구성된다.

[0177] 단말은, 단말이 그래픽 식별자를 이용하여 오프라인 상태에서 결제를 수행하도록, 처리 유닛(904)에 의해 생성된 그래픽 식별자를 디스플레이하도록 구성된 디스플레이 유닛(미도시)을 더 포함한다.

[0178] 디스플레이 유닛에 의해 디스플레이되는 그래픽 식별자의 디스플레이 모드는 바코드 및 QR 코드 중 하나 또는 이들의 조합을 포함한다.

[0179] 수신 유닛(901)은 또한 그래픽 식별자의 디스플레이 모드에 대한 전환 명령을 수신하도록 구성되고, 처리 유닛(904)은 수신 유닛(901)이 전환 명령을 수신할 때 디스플레이 유닛에 의해 디스플레이된 그래픽 식별자의 디스플레이 모드를 전환하도록 구성된다.

[0180] 선택적으로, 수신 유닛(901)은, 제2 단말을 통해, 제1 서버 단말에 의해 발행된 인증 인자를 수신하도록 구성되며, 송신 유닛(903)은 제2 단말을 통해 제1 서버 단말에 결합된 인증 정보를 반송하도록 구성된다.

[0181] 선택적으로, 송신 유닛(903)은 또한 계정 신원 검증 요청을 제1 서버 단말에 송신하도록 구성되고, 수신 유닛(901)은, 신원 검증이 성공된 후 제1 서버 단말에 의해 송신된 결제 인증을 수신하도록 구성되고, 송신 유닛(903)은 오프라인 결제 인가에 대한 검증 요청을 제1 서버 단말에 송신하도록 구성되며, 수신 유닛(901)은, 인가 검증이 성공된 후 제1 서버 단말에 의해 발행된 인증 인자를 수신하도록 구성된다.

[0182] 상기 유닛들의 기능들은 도 3a 및 도 3b에서 자세히 설명된 상기 정보 상호작용 방법의 처리 단계들에 대응할 수 있다. 상세사항은 여기에서 다시 설명하지 않는다.

[0183] 도 10은 본 출원의 실시예에 따른 서버 단말의 개략적인 구조도이고, 도 10에서 도시된 바와 같이, 서버 단말은, 획득 유닛(1001), 처리 유닛(1002), 송신 유닛(1003), 및 수신 유닛(1004)을 포함한다.

[0184] 획득 유닛(1001)은 단말 상에서 디스플레이된 그래픽 식별자 내에서 운반된 결제 인증 정보를 획득하도록 구성된다.

[0185] 결제 인증 정보는 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함한다.

[0186] 처리 유닛(1002)은 획득 유닛(1001)에 의해 획득된 결제 인증 정보와 서비스 데이터를 이용하여 결제 요청을 생성하도록 구성된다.

[0187] 송신 유닛(1003)은, 제1 서버 단말이 결제 요청 내에서 운반된 결제 인증 정보에 따라 결제 인증을 수행하고 결제 인증이 성공된 경우 결제를 수행하도록, 처리 유닛(1002)에 의해 생성된 결제 요청을 제1 서버 단말에 송신하도록 구성된다.

[0188] 수신 유닛(1004)은 제1 서버 단말(3)에 의해 반송된 결제 결과를 수신하도록 구성된다.

[0189] 도 11은 본 출원의 실시예에 따른 서버 단말의 개략적인 구조도이고, 도 11에서 도시된 바와 같이, 서버 단말은, 수신 유닛(1101), 처리 유닛(1102), 및 송신 유닛(1103)을 포함한다.

[0190] 수신 유닛(1101)은 제2 서버 단말에 의해 송신된 결제 요청을 수신하도록 구성되고, 결제 요청은 결제 인증 정보 및 서비스 데이터를 운반한다.

[0191] 결제 인증 정보는 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함한다.

[0192] 처리 유닛(1102)은 수신 유닛(1101)에 의해 수신된 결제 요청 내에서 운반된 결제 인증 정보에 따라 결제 인증을 수행하도록 구성되며, 서버 단말은, 결제 인증이 성공된 경우, 결제를 수행한다.

[0193] 선택적으로, 처리 유닛(1102)은 또한 단말 상에서 계정 결합을 수행하도록 구성된다.

[0194] 제1 상황:

[0195] 수신 유닛(1101)은 단말에 의해 송신된 계정 신원 검증 요청을 수신하도록 구성되며, 계정 신원 검증 요청은 사용자의 계정 정보를 운반한다.

[0196] 처리 유닛(1102)은 계정 신원 검증 요청이 검증을 통과했는지 여부를 판단하고, 검증이 성공된 경우, 송신 유닛(1103)을 사용하여 성공적인 검증의 결과를 단말에 송신하도록 구성된다.

[0197] 수신 유닛(1101)은 단말에 의해 송신된 오프라인 결제 인가 검증을 위한 검증 요청을 수신하도록 구성된다.

[0198] 처리 유닛(1102)은 검증 요청에 대한 검증이 성공되었는지 여부를 판단하고, 검증이 성공된 경우, 사용자의 인증키를 생성하고, 서버 단말의 동적 시간 인자를 계산하며, 인증키, 동적 시간 인자, 및 사용자의 계정 정보를 이용하여 인증 인자를 생성하도록 구성된다.

[0199] 송신 유닛(1103)은 처리 유닛(1102)에 의해 생성된 인증 인자를 단말에 발행하도록 구성된다.

[0200] 수신 유닛(1101)은 단말에 의해 제출된 결합된 인증 정보를 수신하도록 구성되며, 이 결합된 인증 정보는 인증 인자와 디바이스 계정 정보를 결합함으로써 생성된다.

[0201] 처리 유닛(1102)은 결합된 인증 정보에 대해 인가 검증을 수행하며, 인가가 성공된 경우, 오프라인 결제 인가 검증을 완료하도록 구성된다.

[0202] 제2 상황:

[0203] 수신 유닛(1101)은 제2 단말에 의해 송신된 계정 신원 검증 요청을 수신하도록 구성되며, 계정 신원 검증 요청은 사용자의 계정 정보를 운반한다.

[0204] 처리 유닛(1102)은 계정 신원 검증 요청이 검증을 통과했는지 여부를 판단하고, 검증이 성공된 경우, 송신 유닛(1103)을 사용하여 성공적인 검증의 결과를 제2 단말에 송신하도록 구성된다.

[0205] 수신 유닛(1101)은 제2 단말에 의해 송신된 오프라인 결제 인가 검증을 위한 검증 요청을 수신하도록 구성된다.

[0206] 처리 유닛(1102)은 검증 요청에 대한 검증이 성공되었는지 여부를 판단하고, 검증이 성공된 경우, 사용자의 인증키를 생성하고, 서버 단말의 동적 시간 인자를 계산하며, 인증키, 동적 시간 인자, 및 사용자의 계정 정보를 이용하여 인증 인자를 생성하도록 구성된다.

[0207] 송신 유닛(1103)은 제2 단말이 인증 인자를 단말에 송신하도록, 인증 인자를 제2 단말에 발행하도록 구성된다.

[0208] 수신 유닛(1101)은 단말에 의해 반송되고 제2 단말에 의해 제출된 결합된 인증 정보를 수신하도록 구성되며, 이 결합된 인증 정보는 인증 인자와 디바이스 계정 정보를 결합함으로써 단말에 의해 생성된다.

[0209] 처리 유닛(1102)은 결합된 인증 정보에 대해 인가 검증을 수행하며, 인가가 성공된 경우, 오프라인 결제 인가 검증을 완료하도록 구성된다.

[0210] 선택적으로, 사용자의 인증키를 생성한 후, 처리 유닛(1102)은 또한, 사용자의 계정 정보 및 인증키로부터 압축

된 문자열을 생성하도록 구성되며, 압축된 문자열은 인증키 및 사용자의 계정 정보와 일대일 매핑 관계를 갖는다.

[0211] 처리 유닛(1102)은 사용자의 계정 정보, 인증키, 동적 시간 인자를 이용하여 인증 인자를 생성하도록 구성되며, 이는, 구체적으로, 인증키, 압축된 문자열, 및 동적 시간 인자를 사용하여 인증 인자를 생성하는 것을 포함한다.

[0212] 선택적으로, 처리 유닛(1102)은 구체적으로, 결제 인증 정보 내에서 운반된 디바이스 계정 정보와 인증키 사이의 결합 관계가 정확한지 여부를 체크하고, 인증 인자 내의 동적 시간 인자에 따라 동적 패스워드가 유효한지 여부를 체크하도록 구성되며, 상기 결합 관계가 정확하고 상기 동적 패스워드가 유효한 경우, 결제 인증은 성공된 것이다.

[0213] 상기 유닛들의 기능들은 도 5a 내지 도 5c에서 자세히 설명된 상기 정보 상호작용 방법의 처리 단계들에 대응할 수 있다. 상세사항은 여기에서 다시 설명하지 않는다.

[0214] 도 12는 본 출원의 실시예에 따른 전자 디바이스의 구성의 개략적인 구조도이며, 도 12에서 도시된 바와 같이, 전자 디바이스는, 디스플레이(1201), 프로세서(1202), 메모리(1203), 및 통신 모듈(1204)을 포함한다.

[0215] 메모리(1203)는 제1 서버 단말에 의해 발행된 인증 인자, 및 상기 인증 인자에 따라 오프라인 결제를 위한 그래픽 식별자를 생성하기 위한 프로그램을 저장하도록 구성되며, 상기 프로그램이 상기 프로세서에 의해 실행될 때, 오프라인 결제를 위한 그래픽 식별자가 디스플레이의 디스플레이 영역에서 디스플레이된다. 그래픽 식별자는 결제 인증 정보를 운반하고, 결제 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고, 동적 패스워드는 동적 시간 인자에 따라 생성되며, 디바이스 계정 정보는 단말의 디바이스 정보 및 사용자의 계정 정보에 따라 생성된다.

[0216] 제2 전자 디바이스와 통신하는 통신 모듈(1204)은, 제1 서버 단말에 의해 발행되고 제2 전자 디바이스에 의해 송신된 인증 인자를 수신하고, 인증을 결합하는 동안, 결합된 인증 정보가 제1 서버 단말에 포워딩되도록, 결합된 인증 정보를 제2 전자 디바이스에 송신하도록 구성된다.

[0217] 통신 모듈(1204)은 블루투스 모듈 또는 WiFi 모듈이다.

[0218] 선택적으로, 동적 패스워드는 동일한 시간 창에서 변경되지 않은 상태로 있으며, 다음번 시간 창에서, 동적 패스워드는 동적 시간 인자에 따라 재생성되어 동적으로 변경된다.

[0219] 선택적으로, 동적 패스워드는 구체적으로, 일회용 패스워드 계산 방법에 따라, 사용자의 인증키, 동적 시간 인자, 디바이스 계정 정보, 및 미리 설정된 패스워드 길이를 이용한 계산을 통해 얻어진다.

[0220] 선택적으로, 디바이스 계정 정보는 사용자의 계정 정보 및 그래픽 식별자를 디스플레이하는 단말의 디바이스 정보를 압축함으로써 얻어진 압축된 문자열이다.

[0221] 선택적으로, 그래픽 식별자는 QR 코드 또는 바코드이다.

[0222] 본 출원은 단말, 제1 서버 단말, 및 제2 서버 단말을 포함하는 정보 상호작용 시스템을 더 제공하고;

[0223] 단말은, 오프라인 상태에서, 제1 서비스 조작을 완료하기 위한 그래픽 식별자를 디스플레이하고, 그래픽 식별자는 제1 서비스 조작의 인증 정보를 운반하고, 상기 제1 서비스 조작의 인증 정보는 사용자의 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함하고,

[0224] 상기 제2 서버 단말은 상기 그래픽 식별자 내에서 운반된 제1 서비스 조작의 인증 정보를 획득하고,

[0225] 상기 제2 서버 단말은 상기 제1 서비스 조작의 인증 정보 및 서비스 데이터를 이용하여 제1 서비스 조작 요청을 생성하고, 상기 제1 서비스 조작 요청을 상기 제1 서버 단말에 송신하며,

[0226] 상기 제1 서버 단말은 상기 제1 서비스 조작 요청 내에서 운반된 상기 제1 서비스 조작의 인증 정보에 따라 인증을 수행하며, 상기 인증이 성공된 경우, 상기 제1 서버 단말은 상기 제1 서비스 조작을 완료한다.

[0227] 선택적으로, 단말이 제1 서비스 조작을 오프라인에서 완료하기 위한 그래픽 식별자를 디스플레이하기 전에,

[0228] 단말은 그래픽 식별자를 디스플레이하기 위한 디스플레이 명령을 수신하고;

[0229] 단말은 제1 서버 단말에 의해 발행된 인증 인자에 따라 제1 서비스 조작의 인증 정보를 운반하는 그래픽 식별자를 생성한다.

[0230] 선택적으로, 단말은 제1 서버 단말에 의해 발행된 인증 인자에 따라 제1 서비스 조작의 인증 정보를 운반하는 그래픽 식별자를 생성한다.

[0231] 단말은, 온라인 상태에 있을 때, 제1 서비스 조작을 오프라인에서 완료하기 위한 인가 검증 요청을 제1 서버 단말에 송신하고;

[0232] 제1 서버 단말은 인가 검증 요청을 검증하고, 제1 서버 단말은 검증이 성공된 후 단말에 인증 인자를 송신하며, 인증 인자는 사용자의 인증키, 계정 정보, 및 서버 단말 시간을 포함하며,

[0233] 단말은 인증 인자와 디바이스 계정 정보를 결합하여 결합된 인증 코드를 생성하고, 결합된 인증 코드를 제1 서버 단말에 송신하며,

[0234] 제1 서버 단말은 결합된 인증 코드에 대해 인가 검증을 수행하고, 인가가 성공된 경우, 인가 검증을 완료한다.

[0235] 선택적으로, 단말은 제1 서버 단말에 의해 발행된 인증 인자에 따라 제1 서비스 조작의 인증 정보를 운반하는 그래픽 식별자를 생성한다.

[0236] 온라인 상태에 있는 제2 단말은, 제1 서비스 조작을 오프라인에서 완료하기 위한 인가 검증 요청을 제1 서버 단말에 송신하고;

[0237] 제1 서버 단말은 인가 검증 요청을 검증하고, 제1 서버 단말은 검증이 성공된 후 제2 단말에 인증 인자를 송신하며, 인증 인자는 사용자의 인증키, 계정 정보, 및 서버 단말 시간을 포함하며,

[0238] 제2 단말은 인증 인자를 단말에 송신하며,

[0239] 단말은 인증 인자와 디바이스 계정 정보를 결합하여 결합된 인증 코드를 생성하고, 결합된 인증 코드를 제2 단말에 송신하며,

[0240] 제2 단말은 결합된 인증 코드를 제1 서버 단말에 제출한다.

[0241] 제1 서버 단말은 결합된 인증 코드에 대해 인가 검증을 수행하고, 인가가 성공된 경우, 인가 검증을 완료한다.

[0242] 선택적으로, 제2 단말이 제1 서비스 조작을 오프라인에서 완료하기 위한 인가 검증 요청을 제1 서버 단말에 송신하기 전에,

[0243] 제2 단말은 계정 신원 검증 요청을 제1 서버 단말에 송신하고, 계정 신원 검증 요청은 사용자의 계정 정보를 운반하며,

[0244] 제1 서버 단말은 계정 신원 검증 요청을 검증하고, 상기 검증이 성공된 경우, 제2 단말에게 상기 성공된 검증의 결과를 송신한다.

[0245] 선택적으로, 검증이 성공된 후 제1 서버 단말이 인증 인자를 송신하기 전에,

[0246] 제1 서버 단말은 상기 검증이 성공된 후에 사용자의 인증키를 생성하고 동적 시간 인자를 계산하고;

[0247] 제1 서버 단말은 인증키, 동적 시간 인자, 및 사용자의 계정 정보를 이용하여 인증 인자를 생성한다.

[0248] 선택적으로, 제1 서버 단말이 결합된 인증 코드에 대해 인증 검증을 수행하는 것은 구체적으로 다음을 포함한다:

[0249] 결합된 인증 코드를 파싱하여, 인증키, 디바이스 계정 정보, 및 서버 단말 시간을 획득하는 단계; 및

[0250] 파싱을 통해 획득된 인증키, 디바이스 계정 정보, 및 서버 단말 시간에 따라 인가 검증이 성공되었는지 여부를 체크하는 단계를 포함한다.

[0251] 선택적으로, 제1 서버 단말이 제1 서비스 조작을 완료한 후,

[0252] 제2 서버 단말이 제1 서비스 조작의 결과를 확인하도록, 제1 서버 단말은 제1 서비스 조작의 결과를 제2 서버 단말에 반송한다.

[0253] 본 출원의 실시예들에서 제공된 정보 상호작용 방법, 장치, 및 시스템에서, 오프라인 결제를 위한 동적 그래픽 식별자가 결합된 결제 인증 정보 및 동적 시간 인자를 통해 생성되어, 오프라인 상태에 있는 단말 디바이스가 또한 그래픽 식별자를 사용하여 안전한 결제를 수행할 수 있고 안전하고 편리한 결제를 달성할 수 있도록 한다.

[0254] 전문가는 또한 여기에 개시된 실시예들을 참조하여 설명된 예시들에서 유닛들 및 알고리즘 단계들이 전자 하드

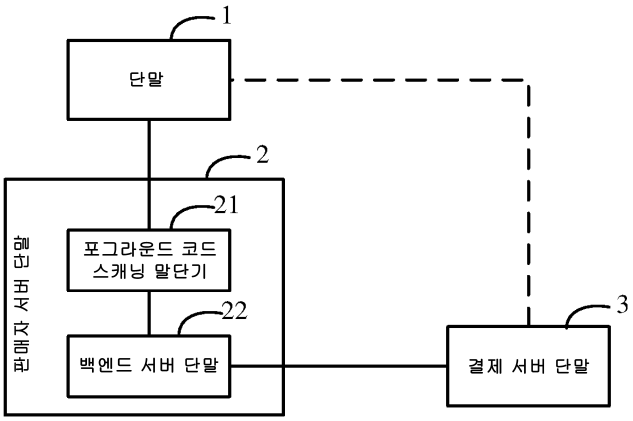
웨어, 컴퓨터 소프트웨어, 또는 이들의 조합에 의해 구현될 수 있음을 알아야 한다. 하드웨어와 소프트웨어 간의 상호교환가능성을 명확하게 설명하기 위해, 전술한 설명의 기능에 따라 각각의 예시의 구성 및 단계들이 일반적으로 설명되었다. 이러한 기능들이 하드웨어 또는 소프트웨어를 사용하여 실행되는지 여부는 기술적 해결책의 특정 응용 및 설계 제약 조건에 좌우된다. 각각의 특정 응용마다, 전문가는 설명된 기능들을 구현하기 위해 상이한 방법을 사용할 수 있다. 그러나, 그러한 구현은 본 출원의 범위를 초과하는 것으로서 간주되어서는 안된다.

[0255] 본 명세서에 개시된 실시예들을 참조하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어, 프로세서에 의해 실행되는 소프트웨어 모듈, 또는 이들의 조합에 의해 구현될 수 있다. 소프트웨어 모듈은 랜덤 액세스 메모리(RAM), 메모리, 판독 전용 메모리(ROM), 전기적 프로그래밍가능 ROM, 전기적 소거가능 프로그래밍가능 ROM, 레지스터, 하드 드라이브, 착탈식 디스크, CD-ROM, 또는 본 기술 분야에서 통상적으로 알려진 임의의 다른 형태의 저장 매체 내에 배치될 수 있다.

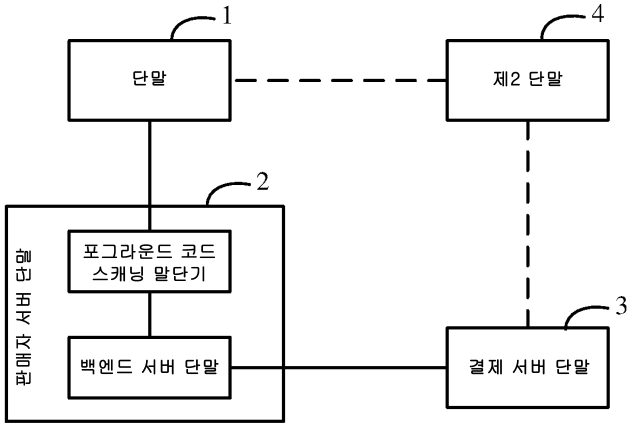
[0256] 전술한 특정 구현예들은 본 출원의 목적, 기술적 해결책, 및 이로운 효과에 대한 더 상세한 설명을 제공한다. 상술한 것은 본 출원의 특정 구현예일 뿐이며, 이는 본 출원의 보호 범위를 제한하려는 것이 아니라는 것을 이해해야 한다. 본 출원의 사상과 원리 내에서 이루어지는 임의의 수정, 등가적 대체물, 개선물 등은 본 출원의 보호 범위에 포함된다.

도면

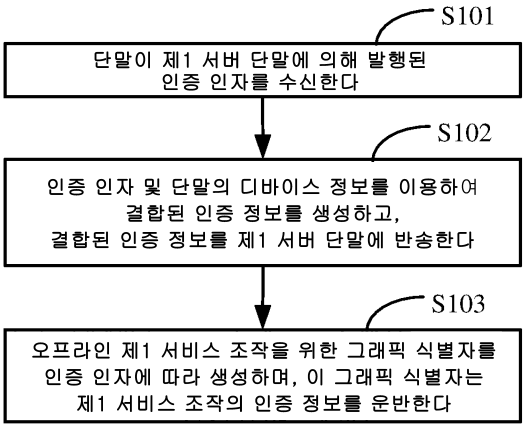
도면1



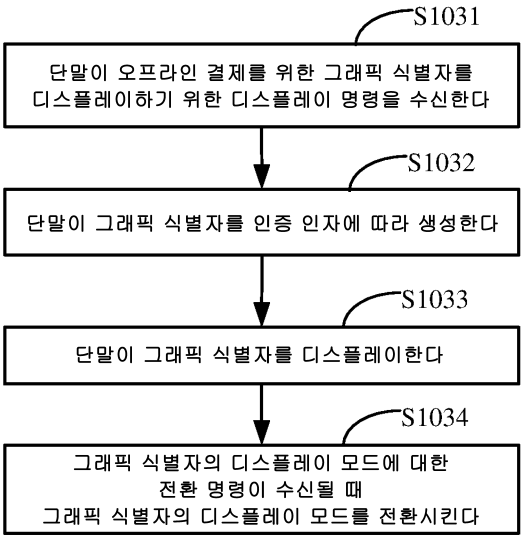
도면2



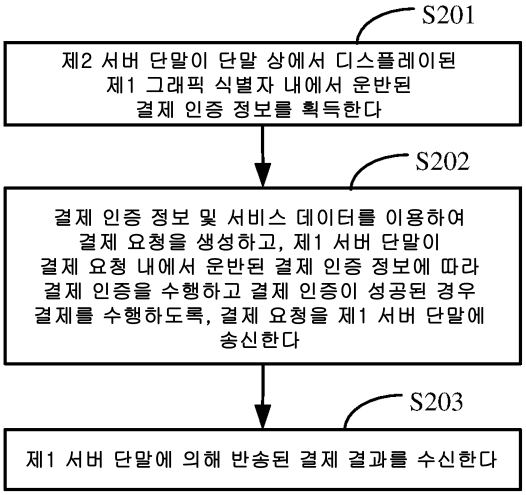
도면3a



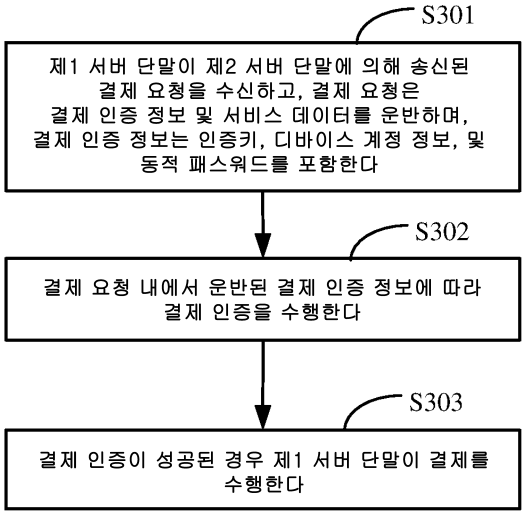
도면3b



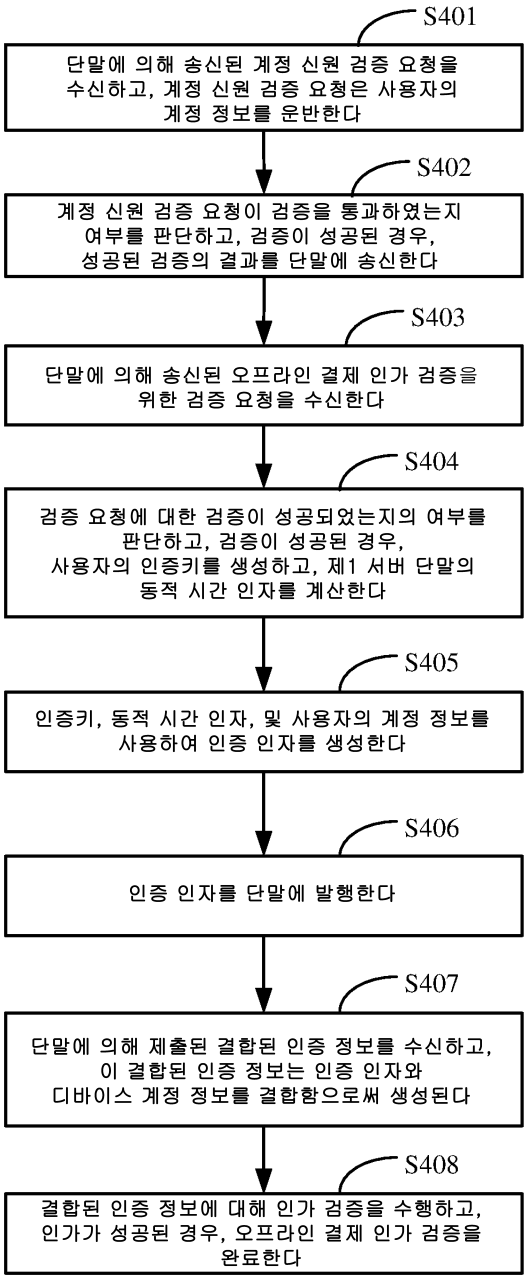
도면4



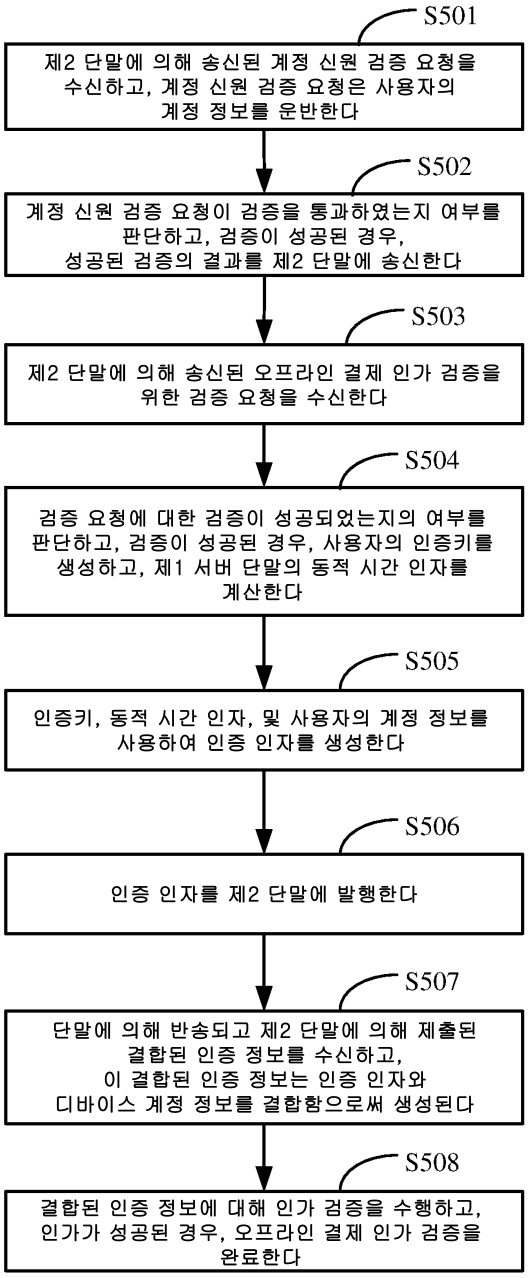
도면5a


S301
제1 서버 단말이 제2 서버 단말에 의해 송신된 결제 요청을 수신하고, 결제 요청은 결제 인증 정보 및 서비스 데이터를 운반하며, 결제 인증 정보는 인증키, 디바이스 계정 정보, 및 동적 패스워드를 포함한다
S302
결제 요청 내에서 운반된 결제 인증 정보에 따라 결제 인증을 수행한다
S303
결제 인증이 성공된 경우 제1 서버 단말이 결제를 수행한다

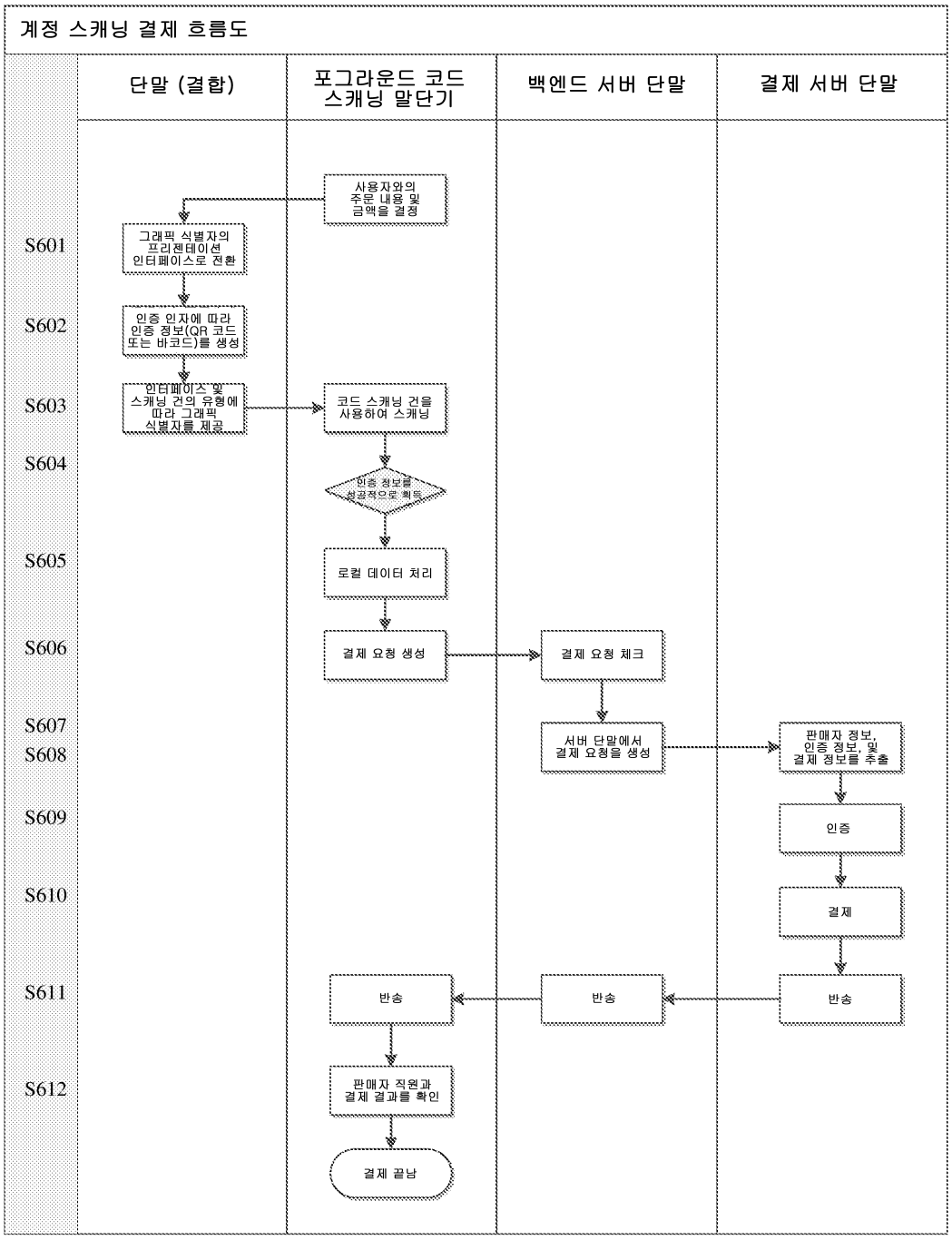
도면5b


S401
단말에 의해 송신된 계정 신원 검증 요청을 수신하고, 계정 신원 검증 요청은 사용자의 계정 정보를 운반한다
S402
계정 신원 검증 요청이 검증을 통과하였는지 여부를 판단하고, 검증이 성공된 경우, 성공된 검증의 결과를 단말에 송신한다
S403
단말에 의해 송신된 오프라인 결제 인가 검증을 위한 검증 요청을 수신한다
S404
검증 요청에 대한 검증이 성공되었는지의 여부를 판단하고, 검증이 성공된 경우, 사용자의 인증키를 생성하고, 제1 서버 단말의 동적 시간 인자를 계산한다
S405
인증키, 동적 시간 인자, 및 사용자의 계정 정보를 사용하여 인증 인자를 생성한다
S406
인증 인자를 단말에 발행한다
S407
단말에 의해 제출된 결합된 인증 정보를 수신하고, 이 결합된 인증 정보는 인증 인자와 디바이스 계정 정보를 결합함으로써 생성된다
S408
결합된 인증 정보에 대해 인가 검증을 수행하고, 인가가 성공된 경우, 오프라인 결제 인가 검증을 완료한다

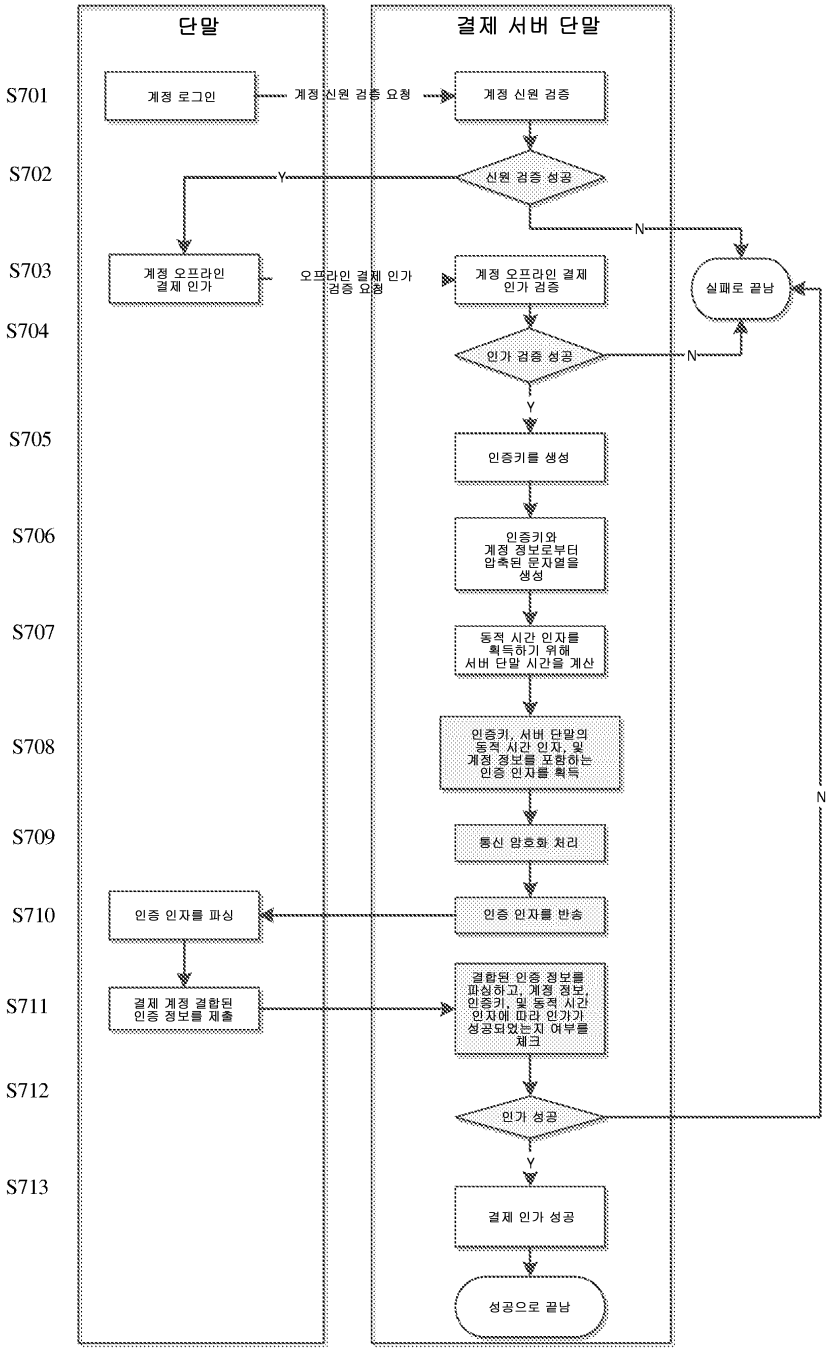
도면5c


S501
제2 단말에 의해 송신된 계정 신원 검증 요청을 수신하고, 계정 신원 검증 요청은 사용자의 계정 정보를 운반한다
S502
계정 신원 검증 요청이 검증을 통과하였는지 여부를 판단하고, 검증이 성공된 경우, 성공된 검증의 결과를 제2 단말에 송신한다
S503
제2 단말에 의해 송신된 오프라인 결제 인가 검증을 위한 검증 요청을 수신한다
S504
검증 요청에 대한 검증이 성공되었는지의 여부를 판단하고, 검증이 성공된 경우, 사용자의 인증키를 생성하고, 제1 서버 단말의 동적 시간 인자를 계산한다
S505
인증키, 동적 시간 인자, 및 사용자의 계정 정보를 사용하여 인증 인자를 생성한다
S506
인증 인자를 제2 단말에 발행한다
S507
단말에 의해 반송되고 제2 단말에 의해 제출된 결합된 인증 정보를 수신하고, 이 결합된 인증 정보는 인증 인자와 디바이스 계정 정보를 결합함으로써 생성된다
S508
결합된 인증 정보에 대해 인가 검증을 수행하고, 인가가 성공된 경우, 오프라인 결제 인가 검증을 완료한다

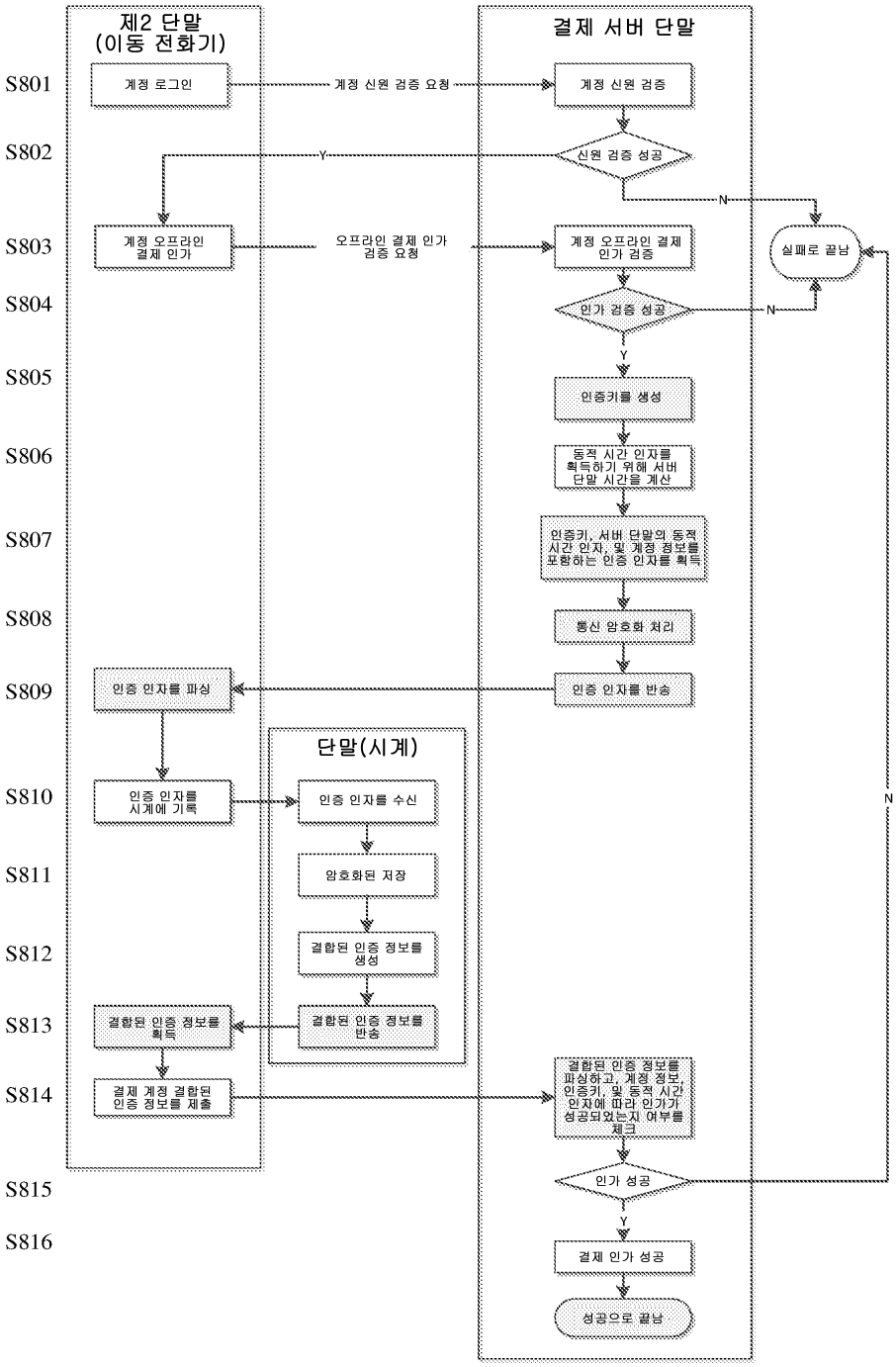
도면6


계정 스캐닝 결제 흐름도
단말 (결합)
포그라운드 코드 스캐닝 말단기
백엔드 서버 단말
결제 서버 단말
S601
S602
S603
S604
S605
S606
S607
S608
S609
S610
S611
S612
사용자와의 주문 내용 및 금액을 결정
그래픽 식별자의 프리젠테이션 인터페이스로 전환
인증 인자에 따라 인증 정보(QR 코드 또는 바코드)를 생성
인터페이스 및 스캐닝 건의 유형에 따라 그래픽 식별자를 제공
코드 스캐닝 건을 사용하여 스캐닝
인증 정보를 성공적으로 획득
로컬 데이터 처리
결제 요청 생성
결제 요청 체크
서버 단말에서 결제 요청을 생성
판매자 정보, 인증 정보, 및 결제 정보를 추출
인증
결제
반송
반송
반송
판매자 직원과 결제 결과를 확인
결제 끝남

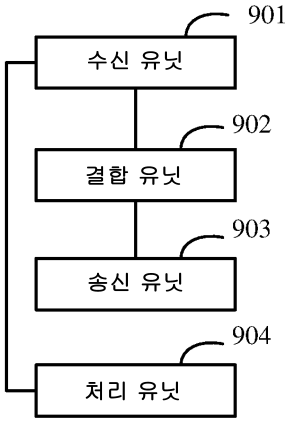
도면7


단말
결제 서버 단말
S701
계정 로그인
계정 신원 검증 요청
계정 신원 검증
S702
신원 검증 성공
Y
N
S703
계정 오프라인 결제 인가
오프라인 결제 인가 검증 요청
계정 오프라인 결제 인가 검증
실패로 끝남
S704
인가 검증 성공
N
Y
S705
인증키를 생성
S706
인증키와 계정 정보로부터 압축된 문자열을 생성
S707
동적 시간 인자를 획득하기 위해 서버 단말 시간을 계산
S708
인증키, 서버 단말의 동적 시간 인자, 및 계정 정보를 포함하는 인증 인자를 획득
N
S709
통신 암호화 처리
S710
인증 인자를 파싱
인증 인자를 반송
S711
결제 계정 결합된 인증 정보를 제출
결합된 인증 정보를 파싱하고, 계정 정보, 인증키, 및 동적 시간 인자에 따라 인가가 성공되었는지 여부를 체크
S712
인가 성공
Y
S713
결제 인가 성공
성공으로 끝남

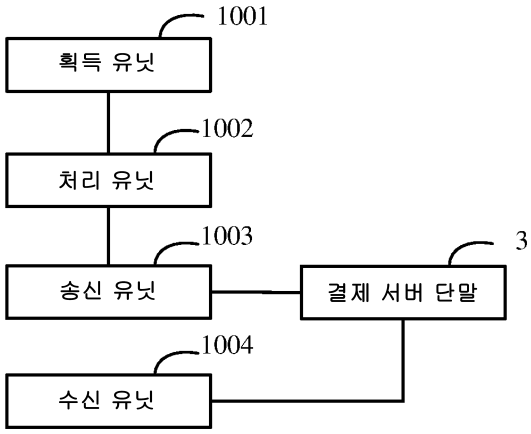
도면8


제2 단말
(이동 전화기)
결제 서버 단말
단말(시계)
S801
S802
S803
S804
S805
S806
S807
S808
S809
S810
S811
S812
S813
S814
S815
S816
계정 로그인
계정 신원 검증 요청
계정 신원 검증
신원 검증 성공
Y
N
계정 오프라인
결제 인가
오프라인 결제 인가
검증 요청
계정 오프라인 결제
인가 검증
실패로 끝남
인가 검증 성공
N
Y
인증키를 생성
동적 시간 인자를
획득하기 위해 서버
단말 시간을 계산
인증키, 서버 단말의 동적
시간 인자, 및 계정 정보를
포함하는 인증 인자를 획득
통신 암호화 처리
인증 인자를 반송
인증 인자를 파싱
인증 인자를
시계에 기록
인증 인자를 수신
암호화된 저장
결합된 인증 정보를
생성
결합된 인증 정보를
반송
결합된 인증 정보를
획득
결제 계정 결합된
인증 정보를 제출
결합된 인증 정보를
파싱하고, 계정 정보,
인증키, 및 동적 시간
인자에 따라 인가가
성공되었는지 여부를
체크
인가 성공
N
Y
결제 인가 성공
성공으로 끝남

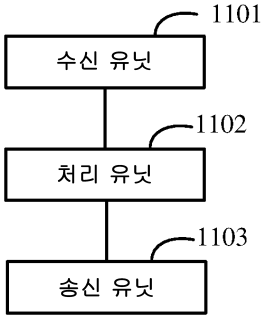
도면9



도면10



도면11



도면12