(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년03월21일
(11) 등록번호 10-1125088
(24) 등록일자 2012년03월02일

(51) 국제특허분류(Int. Cl.)
G06F 15/00 (2006.01)
(21) 출원번호 10-2005-0045325
(22) 출원일자 2005년05월28일
심사청구일자 2010년05월28일
(65) 공개번호 10-2006-0102456
(43) 공개일자 2006년09월27일
(30) 우선권주장
1020050024299 2005년03월23일 대한민국(KR)
(56) 선행기술조사문헌
JP2004240637 A*
KR1020010076121 A*
KR1020000006796 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 비즈모델라인
서울특별시 마포구 와우산로 77, 6층 (서교동, 대창빌딩)
(72) 발명자
김재형
서울특별시 종로구 홍지문길 64, 4동 203호 (구기동, 동익빌라)
홍종철
서울특별시 마포구 동교로38길 8 (연남동)
윤종민
인천광역시 남동구 문화서로49번길 4, 601호 (구월동, 대성아파트)

전체 청구항 수 : 총 2 항 심사관 : 복진요

(54) 발명의 명칭 **고객 인증방법 및 시스템과 이를 위한 서버와 기록매체**

(57) 요 약

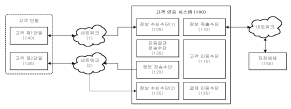
본 발명은 제1단말로 접속한 고객에 대한 인증을 상기 고객의 제2단말을 이용하여 수행하는 고객 인증 시스템에 관한 것이다.

고객 인증 시스템은, 고객이 접속한 제1단말로부터 소정의 고객 식별자 정보를 수신하여, 상기 고객 식별자 정보에 대응하는 상기 고객의 제2단말 정보를 소정의 저장매체로부터 추출하여, 상기 추출된 제2단말로 고객 인증에 필요한 소정의 인증 정보를 요청할 수 있다.

또는, 고객 인증 시스템은, 고객이 접속한 제1단말로부터 상기 고객의 제2단말 정보를 수신하여, 상기 수신한 제2단말로 고객 인증에 필요한 소정의 인증 정보를 요청할 수 있다.

이에 의해, 기존의 피싱(Phishing)이나, 파밍(Pharming), 또는 키보드 해킹 등을 통한 개인 정보 유출을 보다 안전하고 효율적으로 차단할 수 있다는 장점이 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

고객 제1단말 접속시, 고객 제1단말로부터 고객 식별자 정보를 수신하는 정보 수신수단(1);

고객 식별자 정보와 연계 처리된 고객 제2단말 정보를 저장매체로부터 독출하는 정보 독출수단;

상기 독출된 고객 제2단말 정보를 이용하여, 상기 고객 제2단말로 고객 인증정보 요청 정보를 전송하는 정보 전송수단;

고객 제2단말로부터 상기 고객 제2단말에 구비된 고객 공인 인증서 정보를 수신하는 정보 수신수단(2); 및

수신한 고객 공인 인증서 정보를 이용하여 상기 고객 제1단말을 통해 접속한 고객을 인증 처리하는 고객 인증수단;을 구비하여 이루어지는 것을 특징으로 하는 고객 인증 시스템.

청구항 23

고객 제1단말 접속시, 고객 제1단말로부터 고객 제2단말 정보를 수신하는 정보 수신수단(1);

상기 수신한 고객 제2단말 정보를 이용하여, 상기 고객 제2단말로 고객 인증정보 요청 정보를 전송하는 정보 전송수단;

고객 제2단말로부터 상기 고객 제2단말에 저장된 고객 공인 인증서 정보를 수신하는 정보 수신수단(2); 및

수신한 고객 공인 인증서 정보를 이용하여 상기 고객 제1단말을 통해 접속한 고객을 인증 처리하는 고객 인증수단;을 구비하여 이루어지는 것을 특징으로 하는 고객 인증 시스템.

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

청구항 38

삭제

청구항 39

삭제

청구항 40

삭제

청구항 41

삭제

청구항 42

삭제

청구항 43

삭제

청구항 44

삭제

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

청구항 48

삭제

청구항 49

삭제

청구항 50

삭제

청구항 51

삭제

청구항 52

삭제

청구항 53

삭제

청구항 54

삭제

청구항 55

삭제

청구항 56

삭제

청구항 57

삭제

청구항 58

삭제

청구항 59

삭제

청구항 60

삭제

청구항 61

삭제

청구항 62

삭제

청구항 63

삭제

청구항 64

삭제

청구항 65

삭제

청구항 66

삭제

청구항 67

삭제

청구항 68

삭제

청구항 69

삭제

청구항 70

삭제

청구항 71

삭제

청구항 72

삭제

청구항 73

삭제

청구항 74

삭제

청구항 75

삭제

청구항 76

삭제

청구항 77

삭제

청구항 78

삭제

청구항 79

삭제

청구항 80

삭제

청구항 81

삭제

청구항 82

삭제

청구항 83

삭제

청구항 84

삭제

청구항 85

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0025] 본 발명은 제1단말로 접속한 고객에 대한 인증을 상기 고객의 제2단말에 저장된 고객 인증 정보를 통해 보다 안전하고 효율적으로 수행하도록 하는 고객 인증 방법 및 시스템에 관한 것이다.

[0026] 인터넷 인프라 및 금융거래 인프라가 발전하면, 사용자 인증(Authentication)은 웹사이트 접속이나 금융거래에 있어서 매우 중요한 일이 되었다.

[0027] 특히, 최근에 금융기관 등의 웹사이트에서 보낸 e메일로 위장, 링크를 유도해 개인의 인증번호나 신용카드번호, 계좌정보 등을 빼내는 피싱(Phishing)이나, 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인네임시스템(DNS) 이름을 속여 사용자들이 진짜 사이트로 오인하도록 유도, 개인 ID, 패스워드, 계좌정보 등의 개인정보를 훔치는 파밍(Pharming), 또는 사용자 키보드 등으로부터 입력되는 키 입력 정보(예컨대, 개인 ID, 패스워드, 계좌정보 등)를 해킹하는 키보드 해킹 등이 문제가 되면서, 보다 안전하고 효율적인 사용자 인증 문제

는 대두되었다.

[0028] 또한, 일반적으로 로그인이나 금융거래를 위해 요구되는 인증 정보(예컨대, 아이디 및 패스워드 등)는 복수개가 존재하지 않기 때문에, 해킹 등을 통해서 타인에게 유출되는 경우, 사용자는 고스란히 피해를 감당해야 했다.

발명이 이루고자 하는 기술적 과제

[0029] 본 발명의 목적은 상기와 같은 문제점을 해결하기 위해 도출된 것으로서, 고객이 접속한 제1단말로부터 소정의 고객 식별자 정보를 수신하고, 상기 고객 식별자 정보에 대응하는 상기 고객의 제2단말 정보를 소정의 저장매체로부터 추출하여, 상기 추출된 제2단말로 고객 인증에 필요한 소정의 인증 정보를 요청, 상기 제2단말에 저장된 고객 인증 정보를 이용하여 고객 인증 처리를 수행하는 고객 인증 방법 및 시스템을 제공함에 있다.

[0030] 또한, 본 발명의 다른 목적은, 고객이 접속한 제1단말로부터 상기 고객의 제2단말 정보를 수신하여, 상기 수신한 제2단말로 고객 인증에 필요한 소정의 인증 정보를 요청, 상기 제2단말에 저장된 고객 인증 정보를 이용하여 고객 인증 처리를 수행하는 고객 인증 방법 및 시스템을 제공함에 있다.

발명의 구성 및 작용

[0031] 상기 목적을 이루기 위하여 제시되는 고객 인증 방법은, 고객 제1단말 접속시, 소정의 정보 수신수단(1)에서 상기 고객 제1단말로부터 소정의 고객 식별자 정보를 수신하는 고객 식별자 정보 수신 단계와, 소정의 정보 독출수단에서 상기 고객 식별자 정보 수신 단계를 통해 수신한 고객 식별자 정보와 연계 처리된 고객 제2단말 정보를 소정의 저장매체로부터 독출하는 고객 제2단말 정보 독출단계와, 소정의 정보 전송수단에서 상기 고객 제2단말 정보 독출단계를 통해 독출된 고객 제2단말 정보를 이용하여, 상기 고객 제2단말로 소정의 고객 인증정보 요청 정보를 전송하는 고객 인증정보 요청단계와, 상기 고객 제2단말에서 상기 고객 인증정보 요청단계를 통해 전송된 고객 인증정보 요청 정보를 수신하는 고객 인증정보 요청 수신단계와, 상기 고객 제2단말에서 상기 고객 인증정보 요청 수신단계를 통해 수신된 상기 고객 인증정보 요청 정보에 대응하여, 소정의 고객 인증 정보를 입력받거나, 또는 생성하거나 또는 소정의 메모리로부터 추출하는 고객 인증 정보 입력/생성/추출 단계와, 상기 고객 제2단말에서 상기 고객 인증 정보 입력/생성/추출 단계를 통해 입력 또는 생성 또는 추출된 고객 인증 정보를 전송하는 고객 인증 정보 전송단계와, 소정의 정보 수신수단(2)에서 상기 고객 제2단말이 전송한 고객 인증 정보를 수신하는 고객 인증 정보 수신단계 및 소정의 고객 인증수단에서 상기 고객 인증 정보를 근거로 상기 고객 제1단말을 통해 접속한 고객을 인증 처리하는 고객 인증단계를 포함하여 달성된다.

[0032] 바람직하게, 고객 인증 방법은, 소정의 정보 저장수단에서 고객 식별자 정보와 고객 제2단말 정보를 연계 처리하여 소정의 저장매체에 저장하는 정보 저장단계를 더 포함하여 구성될 수 있다.

[0033] 본 발명에 따르면, 상기 정보 수신수단(1)에서 상기 고객 제1단말로부터 수신하는 고객 식별자 정보는, 아이디(ID) 정보와, 패스워드 정보와, 고객 개인정보와, 고객 생체정보와, 고객 통신수단 정보와, 공인인증서 정보를 적어도 하나 이상 포함할 수 있다.

[0034] 한편, 본 발명에 따른 고객 인증 방법은, 고객 제1단말 접속시, 소정의 정보 수신수단(1)에서 상기 고객 제1단말로부터 고객 제2단말 정보를 수신하는 고객 제2단말 정보 수신 단계와, 소정의 정보 전송수단에서 상기 고객 제2단말 정보 수신 단계를 통해 수신된 고객 제2단말 정보를 이용하여, 상기 고객 제2단말로 소정의 고객 인증정보 요청 정보를 전송하는 고객 인증정보 요청단계와, 상기 고객 제2단말에서 상기 고객 인증정보 요청단계를 통해 전송된 고객 인증정보 요청 정보를 수신하는 고객 인증정보 요청 수신단계와, 상기 고객 제2단말에서 상기 고객 인증정보 요청 수신단계를 통해 수신된 상기 고객 인증정보 요청 정보에 대응하여, 소정의 고객 인증 정보

를 입력받거나, 또는 생성하거나 또는 소정의 메모리로부터 추출하는 고객 인증 정보 입력/생성/추출 단계와, 상기 고객 제2단말에서 상기 고객 인증 정보 입력/생성/추출 단계를 통해 입력 또는 생성 또는 추출된 고객 인증 정보를 전송하는 고객 인증 정보 전송단계와, 소정의 정보 수신수단(2)에서 상기 고객 제2단말이 전송한 고객 인증 정보를 수신하는 고객 인증 정보 수신단계 및 소정의 고객 인증수단에서 상기 고객 인증 정보를 근거로 상기 고객 제1단말을 통해 접속한 고객을 인증 처리하는 고객 인증단계를 포함하여 달성될 수 있다.

[0035] 본 발명에 따르면, 전술한 고객 인증 방법은, 상기 고객 인증단계를 통한 인증결과를 상기 고객 제1단말이 접속한 서버로 전송하는 고객 인증결과 전송단계를 더 포함하여 구성될 수 있다.

[0036] 또한, 고객 인증 방법은, 상기 고객 인증 정보 및/또는 상기 고객 인증단계를 통한 인증결과에 대응하는 서버(상기 고객 제1단말이 접속한 서버)를 확인하는 단계 및 상기 고객 인증단계를 통한 인증결과를 상기 확인된 서버로 전송하는 단계를 더 포함하여 구성될 수 있다.

[0037] 또한, 고객 인증 방법은, 상기 고객 인증단계를 통한 인증결과를 근거로, 소정의 결제인증수단에서 상기 제1고객 단말 및/또는 상기 고객 제2단말을 통한 소정의 결제처리를 인증 처리하는 결제처리단계를 더 포함하여 구성될 수 있다.

[0038] 바람직하게, 고객 인증 방법에 있어서, 상기 고객 인증정보 요청단계는, 상기 고객 제2단말로 소정의 고객 인증정보 요청 정보를 전송하는 경우, 고객 인증 정보를 수신하는 소정의 정보 수신수단 접속정보를 상기 고객 제2단말로 더 전송할 수 있다.

[0039] 예컨대, 상기 고객 인증정보 요청단계에서, 상기 고객 제2단말로 소정의 고객 인증정보 요청 정보를 전송시, 고객 인증 정보 수신을 위한 소정의 콜백유알엘을 첨부하여 전송할 수 있다.

[0040] 바람직하게, 상기 고객 인증 정보 입력/생성/추출 단계에 있어서, 상기 고객 인증 정보를 소정의 메모리로부터 추출하는 것은, 상기 고객 제2단말에 구비된 IC칩으로부터 상기 고객 인증 정보를 추출할 수 있다.

[0041] 또한, 상기 고객 인증 정보 입력/생성/추출 단계는, 상기 고객 인증 정보를 소정의 암호화 프로세스에 다라 암호화 처리하는 단계를 더 포함할 수 있다.

[0042] 바람직하게, 상기 고객 인증 정보 전송단계는, 상기 고객 인증 정보를 상기 고객 인증정보 요청 정보에 포함된 콜백유알엘(Callback URL)을 통해 전송하거나, 또는 상기 고객 인증 정보를 무선 통신망에 접속하여 전송하는 것을 포함할 수 있다.

[0043]

[0044] 바람직하게, 상기 고객 인증 정보 수신단계는, 통신사 서버 또는 통신사 서버와 연계된 서버 또는 중계서버에서 상기 고객 인증 정보를 수신하는 경우, 상기 수신한 고객 인증 정보를 상기 고객 제1단말이 접속한 서버 또는 상기 고객 제1단말로 전송하는 단계를 더 포함할 수 있으며, 상기 고객 제1단말은 상기 고객 인증 정보를 임시 저장한 후 고객 인증에 이용할 수 있다.

[0045] 또한, 상기 고객 인증 정보 수신단계는, 통신사 서버 또는 통신사 서버와 연계된 서버 또는 중계서버에서 상기 고객 인증 정보를 수신하는 경우, 상기 고객 인증 정보에 대응하는 서버(상기 고객 제1단말이 접속한 서버)를 확인하는 단계 및 상기 수신한 고객 인증 정보를 상기 확인된 서버로 전송하는 단계를 더 포함할 수 있다.

[0046] 바람직하게, 상기 고객 인증 정보 수신단계 또는 상기 고객 인증단계는, 상기 고객 인증 정보가 소정의 암호화 처리 프로세스에 따라 암호화 처리되어 전송된 경우, 상기 암호화 처리된 고객 인증 정보를 복호화 처리하는 단계를 더 포함할 수 있다.

[0047] 또한, 본 발명은, 상기 고객 제1단말이 제2 내지 제N 웹서버 접속시, 소정의 정보 전송수단에서 상기 제2 내지 제N 웹서버로 상기 고객 인증정보를 전송하는 단계를 더 포함하도록 구성할 수 있다.

[0048] 또한, 상기 고객 인증단계는, 소정의 저장매체에 기 저장된 고객 인증 정보와 상기 고객 제2단말이 전송한 고객 인증정보를 비교하여 고객을 인증하거나, 또는 상기 고객 제1단말로부터 제공받은 소정의 고객 식별정보와 상기 고객 제2단말이 전송한 고객 인증정보를 비교하여 고객을 인증할 수 있다.

[0049] 한편, 본 발명은, 전술한 적어도 하나 이상의 고객 인증 방법을 실행하기 위한 소정의 프로그램을 기록한 기록매체를 구비하는 것을 특징으로 한다.

[0050] 이하 첨부된 도면과 설명을 참조하여 본 발명의 바람직한 실시예에 대한 동작 원리를 상세히 설명한다. 다만, 하기에 도시되는 도면과 후술되는 설명은 본 발명의 특징을 효과적으로 설명하기 위한 여러 가지 방법 중에서 바람직한 실시 방법에 대한 것이며, 본 발명이 하기의 도면과 설명만으로 한정되는 것은 아니다. 또한, 하기에서 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서, 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명에서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0051] 또한, 이하 실시되는 본 발명의 바람직한 실시예는 본 발명을 이루는 기술적 구성요소를 효율적으로 설명하기 위해 각각의 시스템 기능구성에 기 구비되어 있거나, 또는 본 발명이 속하는 기술분야에서 통상적으로 구비되는 시스템 기능구성은 가능한 생략하고, 본 발명을 위해 추가적으로 구비되어야 하는 기능구성을 위주로 설명한다. 만약 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면, 하기에 도시하지 않고 생략된 기능구성 중에서 종래에 기 사용되고 있는 구성요소의 기능을 용이하게 이해할 수 있을 것이며, 또한 상기와 같이 생략된 구성요소와 본 발명을 위해 추가된 구성요소 사이의 관계도 명백하게 이해할 수 있을 것이다.

[0052] 도면1은 본 발명에 따른 바람직한 고객 인증 시스템(100)의 개략적인 구성을 도시한 도면이다.

[0053] 고객 인증 시스템(100)은, 네트워크(1)를 통해 고객 제1단말(140)과 접속되고, 또한 네트워크(2)를 통해 고객 제2단말(145)과 접속한다. 여기서, 네트워크(1) 및 네트워크(2)는 동일하거나 및/또는 서로 상이한 접속환경을 갖는 네트워크일 수 있다.

[0054] 네트워크(1)는 고객 제1단말(140)에 의존하여 선택될 수 있으며, 고객 제1단말(140)은, 컴퓨터를 포함하는 유선 단말과, 정보처리기(또는 KIOSK), 현금지급기, 현금입출금기, 결제단말을 적어도 하나 이상 포함하는 단말(또는 기기)과, 텔레비전, 냉장고, 전자레인지, 오디오 등 통신기능이 구비된 가전기기와, 통신기능이 구비된 운동기기와, 휴대폰, PDA, 휴대 인터넷 폰, 텔레메틱스 등 무선 단말과, 유선전화기와, RFID 단말을 적어도 하나 이상 포함하여 이루어질 수 있다.

[0055] 네트워크(2)는 고객 제2단말(145)에 의존하여 선택될 수 있으며, 고객 제2단말(145)은, 휴대폰, PDA, 휴대 인터

넷 폰, 텔레메틱스 등 무선 단말과, 유선전화기와, 컴퓨터를 포함하는 유선 단말과, 정보처리기(또는 KIOSK), 현금지급기, 현금입출금기, 결제단말을 적어도 하나 이상 포함하는 단말(또는 기기)과, 텔레비전, 냉장고, 전자레인지, 오디오 등 통신기능이 구비된 가전기기와, 통신기능이 구비된 운동기기와, RFID 단말을 적어도 하나 이상 포함하여 이루어질 수 있다.

[0056] 특히, 고객 제2단말(145)은, 상기 고객 인증 시스템(100)이 요청하는 고객 인증 정보(210) 요청에 대응하여, 상기 고객 인증 시스템(100)으로 전송할 고객 인증 정보(210)를 포함하고 있다.

[0057] 여기서, 상기 고객 인증 정보(210)는, 고객 제2단말(145)에 구비되는 메모리(1130) 및/또는 IC칩(1135)에 저장되는 것이 바람직하다.

[0058] 또한, 고객 인증 정보(210)는, 아이디(ID) 정보와, 패스워드 정보와, 고객 개인정보와, 고객 생체정보와, 고객 통신수단 정보와, 공인인증서 정보와, 공인 인증서 비밀번호 정보와, 결제수단 정보와, 결제수단 비밀번호 정보와, 고객 계좌정보와, 고객 계좌에 대응하는 비밀번호 정보와, 고객 계좌에 대응하는 계좌이체 비밀번호 정보와, 상기 고객 제2단말(145)에 구비된 IC칩(1135)에 포함된 정보(또는 데이터)와, 상기 고객 제2단말(145)에 구비된 IC칩(1135)에 포함된 공인 인증서 정보와, 상기 고객 제2단말(145)에 구비된 IC칩 고유 정보와, 상기 고객 제2단말(145)에 구비된 소정의 인증키 데이터를 적어도 하나 이상 포함할 수 있다.

[0059] 고객 인증 시스템(100)의 특징은, 고객 제1단말(140)을 통해 접속하는 고객에 대한 인증을 위해, 상기 고객 제1단말(140)로부터 소정의 고객 식별자 정보(200)를 수신하고, 상기 고객 식별자 정보(200)와 연계된 고객 제2단말 정보(205)가 기 저장된 소정의 저장매체(150)와 연동하여, 상기 수신된 고객 식별자 정보(200)에 대응하는 제2단말 정보(205)를 추출한다.

[0060] 또한 고객 인증 시스템(100)은, 상기 추출된 고객 제2단말 정보(205)를 이용하여, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송하고, 상기 고객 제2단말(145)로부터 상기 고객 인증정보 요청 정보에 대응하는 고객 인증 정보(210)를 수신하여, 상기 수신된 고객 인증 정보(210)를 근거로 상기 고객 제1단말(140)을 통해 접속한 고객에 대한 인증 처리를 수행한다.

[0061] 바람직하게, 고객 인증 시스템(100)은, 전술한 고객 인증 처리를 수행하기 위한 적어도 하나 이상의 기능 수단을 구비할 수 있으며, 여기서, 상기 기능 수단들은, 상기 고객 인증 시스템(100) 내에서 단일 서버에 구비되거나, 복수개의 서버(또는 단말)에 구비되도록 구성될 수 있다.

[0062] 도면1을 참조하여, 보다 상세하게, 고객 인증 시스템(100)은, 고객 제1단말(140) 접속시, 고객 제1단말(140)로부터 소정의 고객 식별자 정보(200)를 수신하는 정보 수신수단(1)(105)과, 고객 식별자 정보(200)와 연계 처리된 고객 제2단말 정보(205)를 소정의 저장매체(150)로부터 독출하는 정보 독출수단(110)과, 상기 독출된 고객 제2단말 정보(205)를 이용하여, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송하는 정보 전송수단(120)과, 상기 고객 제2단말(145)이 고객 인증 정보(210) 전송시, 이를 수신하는 정보 수신수단(2)(125) 및 상기 정보 수신수단(2)이 수신한 고객 인증 정보(210)를 근거로 상기 고객 제1단말(140)을 통해 접속한 고객을 인증 처리하는 고객 인증수단(115)을 포함하여 달성될 수 있다.

[0063] 또한, 고객 인증 시스템(100)은, 상기 고객 인증수단(115)의 인증결과를 상기 정보 수신수단(1)(105)으로 전송하는 인증결과 전송수단(130), 및/또는 상기 고객 인증수단(115)을 통한 인증결과를 근거로, 상기 제1고객 단말 및/또는 상기 고객 제2단말(145)을 통한 소정의 결제처리를 인증 처리하는 결제인증수단(135)을 더 구비하여 구성될 수 있다.

[0064] 여기서, 상기 정보 수신수단(1)(105)이 상기 접속한 고객 제1단말(140)로부터 수신하는 고객 식별자 정보(200)는, 아이디(ID) 정보와, 패스워드(Password) 정보와, 고객 개인정보와, 고객 생체정보와, 고객 통신수단 정보와, 공인인증서 정보를 적어도 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0065] 바람직하게, 고객 인증 시스템(100)에 구비되는 정보 전송수단(120)은, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송하는 경우, 고객 인증 정보(210)를 수신하는 소정의 정보 수신수단 접속정보를 상기 고객 제2단말(145)로 더 전송할 수 있다.

[0066] 또한, 상기 정보 전송수단(120)은, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송하는 경우, 고객 인증 정보(210) 수신을 위한 소정의 콜백유알엘(Callback URL)을 첨부하여 전송할 수 있다.

[0067] 또한, 상기 정보 전송수단(120)은, 상기 고객 제1단말(140)이 제2 내지 제N 웹서버 접속시, 상기 제2 내지 제N 웹서버로 상기 고객 인증정보를 전송할 수 있다.

[0068] 바람직하게, 고객 인증 시스템(100)에 구비되는 상기 정보 수신수단(2)(125)은, 상기 정보 수신수단(1)(105)과 동일하거나, 또는 별개로 구성될 수 있으며, 통신사 서버 또는 통신사 서버와 연계된 서버 또는 중계서버에 구비될 수 있다.

[0069] 바람직하게, 고객 인증 시스템(100)은, 상기 고객 인증 정보(210)에 대응하는 서버를 확인하는 정보 확인수단과, 상기 확인된 서버로 상기 고객 인증 정보(210)를 전송하는 정보 전송수단(120)을 더 구비하여 구성될 수 있다.

[0070]

[0071] 바람직하게, 고객 인증 시스템(100)에 구비되는 상기 고객 인증수단(115)은, 통신사 서버 또는 통신사 서버와 연계된 서버에 구비되거나, 또는 네트워크 상의 중계서버에 구비되거나, 또는 상기 고객 제1단말(140)이 접속한 서버에 구비될 수 있다.

[0072] 또한, 상기 고객 인증수단(115)은, 상기 고객 인증 정보(210)가 소정의 암호화 처리 프로세스에 따라 암호화 처리되어 전송된 경우, 상기 암호화 처리된 고객 인증 정보(210)를 복호화 처리하여, 상기 고객 제1단말(140)을 통해 접속한 고객에 대한 인증처리를 수행하는 것이 바람직하다.

[0073] 또한, 바람직한 다른 실시 방법에 따르는 고객 인증 시스템(100)의 특징은, 고객 제1단말(140)을 통해 접속하는 고객에 대한 인증을 위해, 상기 접속하는 고객 제1단말(140)로부터 고객 제2단말 정보(205)를 수신하고, 상기 수신된 고객 제2단말 정보(205)를 이용하여, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송할 수 있다.

[0074] 고객 인증 시스템(100)은, 상기 고객 제2단말(145)로부터 상기 고객 인증정보 요청 정보에 대응하는 고객 인증정보(210)를 수신하여, 상기 수신된 고객 인증 정보(210)를 근거로 상기 고객 제1단말(140)을 통해 접속한 고객에 대한 인증 처리를 수행한다.

[0075] 여기서, 고객 인증 시스템(100)은, 고객 제1단말(140) 접속시, 고객 제1단말(140)로부터 고객 제2단말 정보(205)를 수신하는 정보 수신수단(1)(105)과, 상기 수신한 고객 제2단말 정보(205)를 이용하여, 상기 고객 제2단

말(145)로 소정의 고객 인증정보 요청 정보를 전송하는 정보 전송수단(120)과, 상기 고객 제2단말(145)이 고객 인증 정보(210) 전송시, 이를 수신하는 정보 수신수단(2)(125) 및 상기 정보 수신수단(2)(125)이 수신한 고객 인증 정보(210)를 근거로 상기 고객 제1단말(140)을 통해 접속한 고객을 인증 처리하는 고객 인증수단(115)을 포함하여 달성될 수 있다.

[0076] 도면1을 참조하면, 고객 인증 시스템(100)은, 접속 고객에 대한 소정의 인증 처리를 수행하기 위한 소정의 저장 매체(150)와 연동하는 것을 특징으로 한다.

[0077] 여기서, 저장매체(150)는, 고객 인증 시스템(100) 내부에 데이터베이스 또는 데이터베이스 서버 형태로 구비되거나, 및/또는 소정의 네트워크를 통해 상기 고객 인증 시스템(100)과 연결될 수 있다.

[0078] 또한, 저장매체(150)는, 상기 고객 인증 시스템(100)이 접속한 고객에 대한 인증 처리를 수행하기 위한 다양한 정보들이 저장되는데, 여기서 상기 저장매체(150) 및 저장매체(150)에 저장되는 정보들은 하기의 도면2 내지는 도면5를 통하여 보다 상세하게 설명하기로 한다.

[0079] 도면2는 본 발명에 따른 바람직한 저장매체(150)의 구성을 도시한 도면이다.

[0080] 도면2를 참조하면, 저장매체(150)는, 적어도 하나 이상의 고객 정보(예컨대, 고객정보(1), 고객정보(2), ..., 고객정보(N))를 포함하고 있으며, 상기 고객 정보는, 전술한 도면에 도시된 고객 인증 시스템(100)이 접속한 고객에 대한 인증 처리를 원활하게 수행하기 위하여, 상기 고객에 대한 식별자 정보(200)와, 제2단말 정보(205) 및 고객 인증 정보(210)와 연계되어 있다.

[0081] 여기서, 상기 저장매체(150)에 저장되는 적어도 하나 이상의 고객 정보와, 상기 고객 정보와 연계되는 고객 식별자 정보(200)와, 제2단말 정보(205) 및 고객 인증 정보(210)는, 본 발명에 따라 상기 고객 인증 시스템(100)에 접속한 고객에 대한 인증 처리 작업이 수행되기 이전에 기 저장되어, 그 후 상기 고객의 고객 인증 시스템(100) 접속 시점에서, 상기 고객 인증 시스템(100)의 상기 고객 인증 처리 작업 수행시 참조됨이 바람직하다.

[0082] 이하 도면3 내지는 도면5는, 상기 저장매체(150) 내에서 상기 고객 정보와 연계되어 저장되는 곡객 식별자 정보(200)와, 제2단말 정보(205) 및 고객 인증 정보(210)에 대한 일 예시도이다.

[0083] 도면3은 본 발명의 바람직한 실시예에 따른 고객 식별자 정보(200)에 대한 간단한 예시도이다.

[0084] 도면3을 참조하면, 고객 식별자 정보(200)는, 소정의 단말(예컨대, 고객 제1단말(140))로 고객 인증 시스템(100)에 접속한 고객이 상기 고객 제1단말(140)을 통해 입력 또는 선택하여 상기 고객 인증 시스템(100)으로 전송하는 소정의 고객 식별 정보로서, 상기 고객 인증 시스템(100)에 접속한 고객에 대한 1차 인증에 참조될 수 있으며, 또한, 저장매체(150)로부터 상기 고객 제2단말 정보(205)를 추출하기 위한 제2단말 정보(205) 추출 정보가 될 수 있다.

[0085] 바람직하게, 고객 식별자 정보(200)는, 상기 고객 인증 시스템(100)으로부터 부여된 및/또는 허가된 아이디(ID) 정보와, 패스워드(Password) 정보와, 고객 개인정보(예컨대, 주민등록번호, 보험번호, 운전면허 번호, 홈페이지 정보 등)와, 고객 생체정보(예컨대, 지문, 홍채, 손등, 정맥, 안면, 보이스 등)와, 고객 통신수단 정보(예컨대,

고객 전화번호, 핸드폰 번호, 전자메일 정보 등)와, 공인인증서 정보를 적어도 하나 이상 포함하여 이루어질 수 있다.

[0086] 도면4는 본 발명의 바람직한 실시예에 따른 고객 제2단말 정보(205)에 대한 간단한 예시도이다.

[0087] 저장매체(150)에 저장되는 고객 제2단말 정보(205)는, 본 발명에 따라 고객 인증 시스템(100)에 접속한 고객에 대한 인증 처리를 수행하는 과정에서, 상기 고객 인증 시스템(100)이 상기 고객 제2단말(145)에 저장되는 소정의 고객 인증 정보(210)를 요청하기 위하여 참조되는 정보로서, 고객 전화번호, 핸드폰 번호, 휴대접속 단말번호, 전자메일, 가입자 식별번호, 모바일 IP, 고유 IP 등을 포함할 수 있다.

[0088] 예컨대, 고객 제2단말(145)이 고객 휴대폰인 경우, 상기 고객 제2단말 정보(205)는 상기 휴대폰 번호일 수 있으며, 이 때, 상기 고객 인증 시스템(100)은 전술한 도면3에서 제시된 고객 식별자 정보(200)에 대응하는 휴대폰 번호를 추출하고, 상기 휴대폰 번호를 참조하여 상기 휴대폰으로 고객 인증 정보(210)를 요청하는 메시지를 전송할 수 있다.

[0089] 바람직한 다른 실시 방법에 따르면, 상기 고객 제2단말 정보(205)는 상기 고객 인증 시스템(100)에 접속한 고객으로부터 고객 식별자 정보(200)로서 고객 제2단말 정보(205)가 사용되는 경우, 전술한 도면2와 같이 상기 저장매체(150) 내에 존재하지 않아도 무방하다.

[0090] 도면5는 본 발명의 바람직한 실시예에 따른 고객 인증 정보(210)에 대한 간단한 예시도이다.

[0091] 도면5를 참조하면, 도시된 고객 인증 정보(210)는, 상기 고객 인증 시스템(100)에 접속한 고객에 대한 2차 인증이 수행되는 과정에서 요구되는 정보로서, 상기 저장매체(150)에 외에도 상기 고객의 제2단말(145)의 메모리(1130) 및/또는 IC칩(1135)에 저장되는 것이 바람직하다.

[0092] 바람직한 실시 예에 따르면, 고객 인증 정보(210)는, 아이디(ID) 정보와, 패스워드 정보와, 고객 개인정보와, 고객 생체정보와, 고객 통신수단 정보와, 공인인증서 정보와, 공인 인증서 비밀번호 정보와, 결제수단 정보와, 결제수단 비밀번호 정보와, 고객 계좌정보와, 고객 계좌에 대응하는 비밀번호 정보와, 고객 계좌에 대응하는 계좌이체 비밀번호 정보와, 상기 고객 제2단말(145)에 구비된 IC칩(1135)에 포함된 정보(또는 데이터)와, 상기 고객 제2단말(145)에 구비된 IC칩에 포함된 공인 인증서 정보와, 상기 고객 제2단말(145)에 구비된 IC칩 고유 정보와, 상기 고객 제2단말(145)에 구비된 소정의 인증키 데이터를 적어도 하나 이상 포함하여 이루어질 수 있다.

[0093] 또한, 고객 제2단말(145)에 저장된 고객 인증 정보(210)는, 상기 고객 인증 시스템(100)의 요청에 따라 상기 고객 인증 시스템(100)으로 전송되어, 상기 고객 인증 시스템(100)에서 상기 저장매체(150)에 기 저장된 고객 인증 정보(210)와 상기 제2단말(145)로부터 전송된 고객 인증 정보(210)를 비교하는 작업을 통해 상기 접속 고객에 대한 인증 처리를 수행할 수 있도록 한다.

[0094] 도면6은 본 발명의 바람직한 실시 방법에 따른 고객 인증 과정에 대한 간단한 개념도이다.

[0095] 도면6을 참조하면, 바람직한 실시예에 따른 고객 인증 과정은, 고객 인증 시스템(100)(또는 서버)과, 저장매체(150)와, 고객 제1단말(140) 및 고객 제2단말(145)을 통해 실시될 수 있으며, 고객은 상기 고객 제1단말(140)을 통해 상기 고객 인증 시스템(100)(또는 서버)에 접속하여, 인증 처리를 위한 고객 식별자 정보(200)를 제공하는

것을 특징으로 한다.

[0096] 먼저, 본 발명에 따른 고객 인증 과정을 수행하기 위하여, 고객은 상기 고객 인증 시스템(100)(또는 서버)에 상기 고객 인증 과정에 요구되는 고객 식별자 정보(200)와, 고객 제2단말 정보(205)와, 고객 인증 정보(210)를 등록하고(1), 상기 고객 인증 시스템(100)(또는 서버)은 저장매체(150)에 상기 고객이 제공하는 고객 식별자 정보(200)와, 고객 제2단말 정보(205)와, 고객 인증 정보(210)와 상기 고객 정보를 연계하여 저장하는 것이 바람직하다(2).

[0097] 이후, 고객은 소정의 단말(예컨대, 고객 제1단말(140))을 통해 상기 고객 인증 시스템(100)(또는 서버)에 접속하는 과정에서, 상기 고객 식별자 정보(200)를 상기 고객 인증 시스템(100)(또는 서버)으로 제공하고(3), 상기 고객 인증 시스템(100)은 상기 고객 제1단말(140)로부터 제공된 고객 식별자 정보(200)에 대응하는 고객 제2단말 정보(205)를 상기 저장매체(150)로부터 추출한다(4).

[0098] 그리고, 상기 고객 인증 시스템(100)(또는 서버)은 상기 추출된 고객 제2단말 정보(205)를 참조하여, 상기 고객 제2단말(145)로 상기 고객 인증을 위해 요구되는 고객 인증 정보(210)를 요청한다(5). 이 때, 상기 고객은 상기 고객 제2단말(145)로 수신되는 고객 인증 요청 정보에 대응하는 고객 인증 정보(210)를 상기 고객 제2단말(145)로부터 입력 및/또는 추출하여(6), 상기 입력 및/또는 추출된 고객 인증 정보(210)를 상기 고객 제2단말(145)을 통해 상기 고객 인증 시스템(100)(또는 서버)으로 전송한다(7).

[0099] 그러면, 상기 고객 인증 시스템(100)(또는 서버)은 상기 고객 제2단말(145)로부터 전송된 고객 인증 정보(210)와, 상기 저장매체(150)에 기 저장된 고객 인증 정보(210)를 비교함으로서, 상기 고객에 대한 최종 인증 처리 과정을 수행하고(8), 상기 최종 인증 처리 과정에 대한 내역을 상기 고객 제1단말(140)로 전송함으로서, 상기 고객 제1단말(140)을 통해 접속한 고객에 대한 소정의 인증후 작업(예컨대, 로그인, 컨텐츠 이용, 결제 등)을 개시하도록 한다(9).

[0100] 도면7은 본 발명의 바람직한 실시 방법에 따라 중계서버를 포함하는 고객 인증 과정에 대한 간단한 개념도이다.

[0101] 도면7을 참조하면, 도시된 고객 인증 과정은, 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)과, 저장매체(150)와, 서버와, 고객 제1단말(140) 및 고객 제2단말(145)을 통해 실시될 수 있으며, 고객은 상기 고객 제1단말(140)을 통해 상기 서버에 접속하며, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)은 상기 서버에 접속하는 고객에 대한 인증 처리를 수행하는 것을 특징으로 한다.

[0102] 여기서, 상기 서버는, 고객이 접속하고자 하는 인터넷 상의 웹서버, 컨텐츠 제공 서버 등이 될 수 있으며, 상기 고객 인증 시스템(100)은 상기 서버에 접속하는 고객에 대한 인증 처리를 대행 및/또는 중계하는 중계서버(또는 통신사 서버)가 될 수 있다.

[0103] 전술한 도면6과 같이, 도시된 고객 인증 과정을 수행하기 위하여, 고객은 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)에 상기 고객 인증 과정에 요구되는 고객 식별자 정보(200)와, 고객 제2단말 정보(205)와, 고객 인증 정보(210)를 등록하고(1), 상기 고객 인증 시스템(100)(또는 서버 또는 통신사 서버)은 저장매체(150)에 상기 고객이 제공하는 고객 식별자 정보(200)와, 고객 제2단말 정보(205)와, 고객 인증 정보(210)와 상기 고객 정보를 연계하여 저장한다(2).

[0104] 이후, 고객은 소정의 단말(예컨대, 고객 제1단말(140))을 이용하여, 소정의 서버(예컨대, 인터넷 상의 웹서버,

컨텐츠 제공 서버 등)에 접속하는 과정에서, 상기 고객 식별자 정보(200)를 상기 서버로 제공하고(3), 상기 서버는 상기 고객 제1단말(140)로부터 제공된 고객 식별자 정보(200)를 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)으로 제공하여, 상기 접속한 고객에 대한 인증 처리를 요청한다(4).

[0105] 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)은 상기 서버의 인증 처리 요청에 따라, 상기 서버로부터 제공된 고객 식별자 정보(200)에 대응하는 고객 제2단말 정보(205)를 상기 저장매체(150)로부터 추출하고(5), 상기 추출된 고객 제2단말 정보(205)를 참조하여, 상기 고객 제2단말(145)로 상기 고객 인증을 위해 요구되는 고객 인증 정보(210)를 요청한다(6).

[0106] 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)으로부터 고객 인증 정보(210) 요청 메시지가 상기 고객 제2단말(145)로 전송되면, 고객은 상기 고객 제2단말(145)로 수신되는 고객 인증 요청 정보에 대응하는 고객 인증 정보(210)를 상기 고객 제2단말(145)로부터 입력 및/또는 추출하여(7), 상기 입력 및/또는 추출된 고객 인증 정보(210)를 상기 고객 제2단말(145)을 통해 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)으로 전송한다(8).

[0107] 그러면, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)은 상기 고객 제2단말(145)로부터 전송된 고객 인증 정보(210)와, 상기 저장매체(150)에 기 저장된 고객 인증 정보(210)를 비교함으로서, 상기 고객에 대한 최종 인증 처리 과정을 수행하고(9), 상기 최종 인증 처리 과정에 대한 내역을 상기 고객이 제1단말(140)을 통해 접속한 서버로 전송한다(10).

[0108] 상기 서버는, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)이 제공하는 최종 인증 처리 내역을 상기 고객 제1단말(140)로 전송함으로서, 고객에 대한 소정의 인증후 작업(예컨대, 로그인, 컨텐츠 이용, 결제 등)을 개시하도록 한다(11).

[0109] 도면8은 본 발명의 바람직한 다른 실시 방법에 따른 고객 인증 과정에 대한 간단한 개념도이다.

[0110] 도면8에 도시된 고객 인증 과정은, 고객 인증 시스템(100)(또는 서버)과, 저장매체(150)와, 고객 제1단말(140) 및 고객 제2단말(145)을 통해 실시될 수 있으며, 고객은 상기 고객 제1단말(140)을 통해 상기 고객 인증 시스템(100)(또는 서버)에 접속하여, 인증 처리를 위한 고객 제2단말 정보(205)를 제공하는 것을 특징으로 한다.

[0111] 바람직하게, 도면8에 도시된 고객 인증 과정을 수행하기 위하여, 고객은 상기 고객 인증 시스템(100)(또는 서버)에 상기 고객 인증 과정에 요구되는 고객 인증 정보(210)를 등록하고(1), 상기 고객 인증 시스템(100)(또는 서버)은 저장매체(150)에 상기 고객이 제공하는 고객 인증 정보(210)를 상기 고객 정보와 연계하여 저장한다(2).

[0112] 이후, 고객은 소정의 단말(예컨대, 고객 제1단말(140))을 통해 상기 고객 인증 시스템(100)(또는 서버)에 접속하는 과정에서, 상기 고객 인증 처리에 요구되는 고객 인증 정보(210)가 저장된 고객 제2단말 정보(205)를 상기 고객 인증 시스템(100)(또는 서버)으로 제공하고(3), 상기 고객 인증 시스템(100)(또는 서버)은 상기 고객 제1단말(140)로부터 제공된 고객 제2단말 정보(205)를 참조하여, 상기 고객 제2단말(145)로 상기 고객 인증을 위해 요구되는 고객 인증 정보(210)를 요청한다(4).

[0113] 이 때, 상기 고객은 상기 고객 제2단말(145)로 수신되는 고객 인증 요청 정보에 대응하는 고객 인증 정보(210)를 상기 고객 제2단말(145)로부터 입력 및/또는 추출하여(5), 상기 입력 및/또는 추출된 고객 인증 정보(210)를

상기 고객 제2단말(145)을 통해 상기 고객 인증 시스템(100)(또는 서버)으로 전송한다(6).

[0114] 그러면, 상기 고객 인증 시스템(100)(또는 서버)은 상기 고객 제2단말(145)로부터 전송된 고객 인증 정보(210)와, 상기 저장매체(150)에 기 저장된 고객 인증 정보(210)를 비교함으로서, 상기 고객에 대한 최종 인증 처리 과정을 수행하고(7), 상기 최종 인증 처리 과정에 대한 내역을 상기 고객 제1단말(140)로 전송함으로서, 상기 고객 제1단말(140)을 통해 접속한 고객에 대한 소정의 인증후 작업(예컨대, 로그인, 컨텐츠 이용, 결제 등)을 개시하도록 한다(8).

[0115] 또한, 본 발명의 따른 실시예에 따르면, 상기 고객 인증 시스템(100)(또는 서버)은 상기 고객 제2단말(145)로부터 전송된 고객 인증 정보(210)를 상기 고객 제1단말(140)로 전송함으로서, 상기 고객 제1단말(140)을 통해 접속한 고객에 대한 소정의 인증처리가 이루어지도록 할 수 있다.

[0116] 도면9는 본 발명의 바람직한 다른 실시 방법에 따라 중계서버를 포함하는 고객 인증 과정에 대한 간단한 개념도이다.

[0117] 도면9를 참조하면, 도시된 고객 인증 과정은, 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)과, 저장매체(150)와, 서버와, 고객 제1단말(140) 및 고객 제2단말(145)을 통해 실시될 수 있으며, 고객은 상기 고객 제1단말(140)을 통해 상기 서버에 접속하며, 상기 고객 인증 시스템(100)은 상기 서버에 접속하는 고객에 대한 인증 처리를 수행하는 것을 특징으로 한다.

[0118] 전술한 도면7과 같이, 상기 고객이 제1단말(140)을 통해 접속하는 서버는, 인터넷 상의 웹서버, 컨텐츠 제공 서버 등이 될 수 있으며, 상기 고객 인증 시스템(100)은 상기 서버에 접속하는 고객에 대한 인증 처리를 대행 및/또는 중계하는 중계서버(또는 통신사 서버)가 될 수 있다.

[0119] 도면9에 도시된 고객 인증 과정을 수행하기 위하여, 고객은 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)에 상기 고객 인증 과정에 요구되는 고객 인증 정보(210)를 등록하고(1), 상기 고객 인증 시스템(100)(또는 서버 또는 통신사 서버)은 저장매체(150)에 상기 고객이 제공하는 고객 인증 정보(210)를 상기 고객 정보와 연계하여 저장한다(2).

[0120] 이후, 상기 고객이 소정의 단말(예컨대, 고객 제1단말(140))을 이용하여, 소정의 서버(예컨대, 인터넷 상의 웹서버, 컨텐츠 제공 서버 등)에 접속하는 과정에서, 상기 고객은 인증 처리에 요구되는 고객 인증 정보(210)가 저장된 고객 제2단말 정보(205)를 상기 서버로 제공하고(3), 상기 서버는 상기 고객 제1단말(140)로부터 제공된 고객 제2단말 정보(205)를 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)으로 제공하여, 상기 접속한 고객에 대한 인증 처리를 요청한다(4).

[0121] 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)은 상기 서버의 인증 처리 요청에 따라, 상기 서버로부터 제공된 고객 제2단말 정보(205)를 참조하여, 상기 고객 제2단말(145)로 상기 고객 인증을 위해 요구되는 고객 인증 정보(210)를 요청한다(5).

[0122] 바람직하게, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)으로부터 고객 인증 정보(210) 요청 메시지가 상기 고객 제2단말(145)로 전송되면, 고객은 상기 고객 제2단말(145)로 수신되는 고객 인증 요청 정보에 대응하는 고객 인증 정보(210)를 상기 고객 제2단말(145)로부터 입력 및/또는 추출하여(6), 상기 입력 및/또는 추출된 고객 인증 정보(210)를 상기 고객 제2단말(145)을 통해 상기 고객 인증 시스템(100)(또는 중계서버

또는 통신사 서버)으로 전송한다(7).

[0123] 그러면, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)은 상기 고객 제2단말(145)로부터 전송된 고객 인증 정보(210)와, 상기 저장매체(150)에 기 저장된 고객 인증 정보(210)를 비교함으로서, 상기 고객에 대한 최종 인증 처리 과정을 수행하고(8), 상기 최종 인증 처리 과정에 대한 내역을 상기 고객이 제1단말(140)을 통해 접속한 서버로 전송한다(9).

[0124] 상기 서버는, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)이 제공하는 최종 인증 처리 내역을 상기 고객 제1단말(140)로 전송함으로서, 고객에 대한 소정의 인증후 작업(예컨대, 로그인, 컨텐츠 이용, 결제 등)을 개시하도록 한다(10).

[0125] 또한, 본 발명의 따른 실시예에 따르면, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)은 상기 고객 제2단말(145)로부터 전송된 고객 인증 정보(210)를 상기 고객 제1단말(140)로 전송함으로서, 상기 고객 제1단말(140)을 통해 접속한 고객에 대한 소정의 인증처리가 이루어지도록 할 수 있다.

[0126] 도면10은 본 발명의 바람직한 실시 방법에 따른 고객 인증 시스템(100)에 대한 구성도이다.

[0127] 도면10은, 전술한 도면1 도시된 고객 인증 시스템(100)에 구비되는 적어도 하나 이상의 기능 수단들을 포함하는 고객 인증 서버(1000)와, 상기 서버(1000)에 접속하는 고객 제1단말(140)(예컨대, 개인용 컴퓨터 등)과, 상기 서버(1000)의 고객 인증 정보(210) 요청에 따라 상기 서버(1000)로 제공하는 고객 인증 정보(210)를 저장하는 고객 제2단말(145)(예컨대, 무선 단말 등)을 도시하고 있는 실시예도이다.

[0128] 도면10에 따르면, 도시된 고객 인증 시스템(100)은, 서버에 접속하여 소정의 고객 식별자 정보(200)를 제공하는 고객 제1단말(140)과, 상기 고객 제1단말(140)이 제공한 고객 식별자 정보(200)와 연계 처리된 고객 제2단말 정보(205)를 소정의 저장매체(150)로부터 독출하고, 상기 독출된 고객 제2단말 정보(205)를 이용하여, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송하는 서버(1000)와, 상기 서버(1000)가 전송하는 고객 인증정보 요청 정보를 수신한 후, 상기 서버(1000)로 소정의 고객 인증 정보(210)를 전송하는 고객 제2단말(145)을 구비하여 구성된다.

[0129] 여기서, 상기 서버(1000)는, 인터넷 웹사이트 서버, 인터넷 뱅킹 서버, 통신사 서버, 금융사 서버, VAN사 서버, PG사 서버, 상기 서버들과 연계되는 네트워크 상의 서버를 적어도 하나 이상 포함할 수 있으며, 단일 서버로 이루어지거나, 복수개의 서버(또는 단말) 조합으로 이루어질 수 있다.

[0130] 바람직하게, 상기 서버(1000)는, 상기 고객 제2단말(145)이 전송하는 고객 인증 정보(210)를 근거로 상기 고객 제1단말(140)을 통해 접속한 고객을 인증 처리하는 것을 특징으로 한다.

[0131] 여기서, 상기 서버(1000)는, 상기 고객 제2단말(145)로부터 상기 고객 인증 정보(210)가 소정의 암호화 처리 프로세스에 따라 암호화 처리되어 전송되는 경우, 상기 암호화 처리된 고객 인증 정보(210)를 복호화 처리할 수 있다.

[0132] 바람직하게, 상기 서버(1000)는, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송할 때, 고객 인증 정보(210)를 수신하기 위한 소정의 접속정보를 상기 고객 제2단말(145)로 더 전송할 수 있다.

[0133] 예컨대, 상기 서버(1000)는, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송할 때, 고객 인증 정보(210) 수신을 위한 소정의 콜백유알엘(Callback URL)을 첨부하여 전송할 수 있다.

[0134] 보다 상세하게, 도면10을 참조하면, 상기 서버(1000)는, 정보 수신부(1005), 정보 독출부(1010), 정보 전송부(1020) 및 고객 인증부(1015)를 포함하여 구성될 수 있다.

[0135] 정보 수신부(1105)는, 고객 제1단말(140) 접속시, 상기 서버(1000)에 접속하는 고객 제1단말(140)로부터 상기 저장매체(150)에 저장된 고객 제2단말 정보(205)와 연계되는 고객 식별자 정보(200)를 수신한다.

[0136] 여기서, 상기 고객 식별자 정보(200)는, 전술한 도면3과 같이, 아이디(ID) 정보와, 패스워드 정보와, 고객 개인정보와, 고객 생체정보와, 고객 통신수단 정보와, 공인인증서 정보를 적어도 하나 이상 포함하여 이루어질 수 있으며, 상기 고객 제1단말(140)에 구비된 소정의 입력수단(예컨대, 키보드, 키 패드, 마우스, RF 리더기, 생체정보 리더기 등)을 통해 입력되거나, 상기 고객 제1단말(140)에 구비된 소정의 저장수단(예컨대, EEPROM(Electrically Erasable and Programmable Read Only Memory) 및/또는 FM(Flash Memory) 및/또는 HDD(Hard Disk Drive) 등)으로부터 추출(또는 선택)되어 상기 정보 수신부(1005)로 전송될 수 있다.

[0137] 정보 독출부(1010)는, 상기 정보 수신부(1005)를 통해 상기 고객 제1단말(140)로부터 소정의 고객 식별자 정보(200)가 수신되면, 상기 수신된 고객 식별자 정보(200)와 연계 처리된 고객 제2단말 정보(205)를 소정의 저장매체(150)로부터 독출한다.

[0138] 정보 전송부(1020)는, 상기 정보 독출부(1010)를 통해 상기 고객 식별자 정보(200)와 연계된 고객 제2단말 정보(205)가 독출되면, 상기 독출된 고객 제2단말 정보(205)를 이용하여, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송한다.

[0139] 바람직한 실시 방법에 따르면, 상기 정보 전송부(1020)는, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송하는 과정에서, 상기 고객 제2단말(145)이 상기 고객 인증 정보(210) 요청 정보에 대응하는 고객 인증 정보(210)의 전송을 위해 상기 서버(1000)에 접속하기 위한 소정의 정보 수신수단 접속정보를 상기 고객 제2단말(145)로 더 전송할 수 있다.

[0140] 예컨대, 상기 정보 전송부(1020)는, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송하는 과정에서, 상기 고객 제2단말(145)로부터 상기 고객 인증 정보(210) 수신을 위한 소정의 콜백유알엘(Callback URL)을 첨부하여 전송할 수 있다.

[0141] 고객 인증부(1015)는, 상기 고객 제2단말(145)로부터 상기 고객 인증 정보(210) 요청 정보에 대응하는 고객 인증 정보(210)가 전송되는 경우, 및/또는 소정의 서버에서 상기 고객 제2단말(145)이 전송하는 고객 인증 정보(210)를 이용하여 상기 고객을 인증처리하고, 상기 고객 인증 결과 데이터를 전송하는 경우, 상기 고객 인증 정보(210) 및/또는 상기 고객 인증 결과 데이터를 근거로 상기 고객 제1단말(140)을 통해 접속한 고객에 대한 인증 처리를 한다.

[0142] 예컨대, 상기 고객 인증부(1015)가 상기 고객 제2단말(145)로부터 전송되는 고객 인증 정보(210)를 통해 상기 고객에 대한 인증 처리를 하는 것은, 소정의 저장매체(150)에 기 저장된 고객 인증 정보(210)와 상기 고객 제2단말(145)이 전송한 고객 인증정보를 비교하여 상기 고객에 대한 인증 처리를 하거나, 및/또는 상기 고객 제1단

말(140)로부터 제공받은 소정의 고객 식별정보와 상기 고객 제2단말(145)이 전송한 고객 인증정보를 비교하여 상기 고객에 대한 인증 처리를 할 수 있다.

[0143] 또한, 상기 고객 인증 처리 과정에서, 상기 고객 인증부(1015)는, 상기 고객 제2단말(145)로부터 전송된 고객 인증 정보(210)가 소정의 암호화 처리 프로세스에 따라 암호화 처리되어 전송되는 경우, 상기 암호화 처리된 고객 인증 정보(210)에 대한 복호화 처리를 포함할 수 있다.

[0144] 도면10을 참조하면, 상기 서버(1000)는, 결제 처리부(1025)를 더 포함할 수 있는데, 상기 결제 처리부(1025)는, 상기 고객 인증부(1015)를 통한 인증결과를 근거로, 상기 고객 제1단말(140) 및/또는 상기 고객 제2단말(145)을 통한 소정의 결제처리를 인증 처리한다.

[0145] 예컨대, 상기 서버(1000)가 금융 기관 서버이며, 상기 고객이 접속한 제1단말(140)이 현금지급기, 및/또는 정보처리기(또는 KIOSK), 및/또는 현금입출금기, 및/또는 결제단말인 경우, 상기 결제 처리부는 상기 고객 인증부를 통한 인증결과를 근거로, 상기 고객의 현금 입출금, 및/또는 결제 등을 승인할 수 있다.

[0146] 한편, 바람직한 다른 실시 예에 따르면, 도면10에 도시된 서버(1000)는, 고객 제1단말(140) 접속시, 고객 제1단말(140)로부터 고객 제2단말 정보(205)를 수신하는 정보 수신부(1005)와, 상기 수신한 고객 제2단말 정보(205)를 이용하여, 상기 고객 제2단말(145)로 소정의 고객 인증정보 요청 정보를 전송하는 정보 전송부(1020) 및 상기 고객 제2단말(145)이 고객 인증 정보(210) 전송시, 및/또는 소정의 서버에서 상기 고객 제2단말(145)이 전송하는 고객 인증 정보(210)를 이용하여 상기 고객을 인증처리하고, 상기 고객 인증 결과 데이터를 전송시, 상기 고객 인증 정보(210) 및/또는 상기 고객 인증 결과 데이터를 근거로 상기 고객 제1단말(140)을 통해 접속한 고객을 인증 처리하는 고객 인증부(1015)를 구비하여 구성될 수도 있음을 명기한다.

[0147] 또한, 도면10에 도시된 서버(1000)는, 전술한 서버(1000)에 구비되는 적어도 하나 이상의 기능을 실행하기 위한 컴퓨터로 읽을 수 있는 프로그램을 기록한 기록매체를 포함하는 것을 특징으로 한다.

[0148] 도면11은 본 발명의 바람직한 실시 방법에 따른 고객 제2단말(145)에 대한 간단한 구성도이다.

[0149] 도면11은 전술한 도면10에 도시된 서버(1000)에 고객 제1단말(140)을 통하여 접속하는 고객에 대한 인증 처리를 수행하기 위해 요구되는 고객 인증 정보(210)를 구비한 고객 제2단말(145)의 기능 구성에 대한 간단한 예시도로서, 본 도면에 도시되는 고객 제2단말(145)은, 휴대폰, PDA, 휴대 인터넷 폰, 텔레메틱스 등 무선 단말과, 유선 전화기와, 컴퓨터를 포함하는 유선 단말과, 정보처리기(또는 KIOSK), 현금지급기, 현금입출금기, 결제단말을 적어도 하나 이상 포함하는 단말(또는 기기)과, 텔레비전, 냉장고, 전자레인지, 오디오 등 통신기능이 구비된 가전기기와, 통신기능이 구비된 운동기기와, RFID 단말을 적어도 하나 이상 포함하여 이루어지는 것을 특징으로 한다.

[0150] 또한, 고객 제2단말(145)은, 상기 서버(1000)로부터 전송되는 고객 인증 정보(210) 요청 정보에 대응하는 소정의 고객 인증 정보(210)를 저장하고 있는 것을 특징으로 한다.

[0151] 여기서, 상기 고객 제2단말(145)에 저장되는 고객 인증 정보(210)는, 아이디(ID) 정보와, 패스워드 정보와, 고객 개인정보와, 고객 생체정보와, 고객 통신수단 정보와, 공인인증서 정보와, 공인 인증서 비밀번호 정보와, 결제수단 정보와, 결제수단 비밀번호 정보와, 고객 계좌정보와, 고객 계좌에 대응하는 비밀번호 정보와, 고객 계좌에 대응하는 계좌이체 비밀번호 정보와, 상기 고객 제2단말(145)에 구비된 IC칩에 포함된 정보(또는 데이터)

와, 상기 고객 제2단말(145)에 구비된 IC칩에 포함된 공인 인증서 정보와, 상기 고객 제2단말(145)에 구비된 IC칩 고유 정보와, 상기 고객 제2단말(145)에 구비된 소정의 인증키 데이터를 적어도 하나 이상 포함하여 이루어지는 것이 바람직하다.

[0152] 보다 상세하게, 고객 제2단말(145)은, 인증 정보 요청 정보 수신수단(1105)과, 인증 정보 입력수단(1110), 및/또는 인증 정보 추출수단(1115), 및/또는 인증 정보 생성수단(1120)과, 인증 정보 전송수단(1125)과, 메모리(1130), 및/또는 IC칩(1135)과, 제어부(1100)를 포함하여 구성될 수 있다.

[0153] 인증 정보 요청 정보 수신수단(1105)은, 소정의 단말(예컨대, 고객 제1단말(140))을 통해 상기 서버에 접속한 고객에 대한 인증 처리를 위하여, 상기 서버(1000)의 정보 전송부(1020)를 통해 전송되는 고객 인증 정보 요청 정보를 수신한다.

[0154] 여기서, 상기 고객 제2단말(145)(인증 정보 요청 정보 수신수단)과 서버(1000)(정보 전송부)간의 네트워크는, 상기 고객 제2단말(145)에 대응하는 것이 바람직하다. 예컨대, 상기 고객 제2단말(145)이 무선단말인 경우, 상기 고객 제2단말(145)과 서버간 네트워크는 무선 네트워크가 바람직하다.

[0155] 또한, 다른 실시 방법에 따르면, 상기 서버(1000)로부터 상기 고객 제2단말(145)의 인증 정보 요청 정보 수신수단(1105)으로 수신되는 고객 인증 정보 요청 정보를 포함하는 메시지는 상기 고객 제2단말(145)에 구비 가능한 WIPI(Wireless Internet Platform for Interoperability) 플랫폼에 구비된 데이터 통신용 애플리케이션에서 수신 가능한 데이터 통신 규격을 포함하여 이루어지는 것이 바람직하며, 상기 고객 인증 정보 요청 정보를 포함하는 메시지를 수신한 고객 제2단말(145)은 하기의 인증정보 전송 수단(1125)을 통해, 상기 고객 인증 정보 요청 정보에 대응하는 고객 인증 정보를 포함하는 메시지를 상기 서버(1000)로 전송할 수 있다.

[0156] 인증 정보 입력수단(1110)은, 상기 인증 정보 요청 정보 수신수단을 통해 고객 인증 정보요청 정보가 수신되면, 상기 고객 인증 정보 요청 정보에 대응하는 고객 인증 정보(210)를 입력받는다.

[0157] 여기서, 상기 고객 제2단말(145)에 구비되는 인증 정보 입력수단(1110)은, 다수의 숫자키(Number Key), 문자키(Character Key) 및/또는 적어도 하나 이상의 기능키(Function Key)를 구비한 키보드, 키 패드, 마우스, RF 리더기, 생체정보 입력기 등을 적어도 하나 이상 포함하여 구성되는 것을 특징으로 한다.

[0158] 예컨대, 고객 인증 정보(210)가, 숫자, 문자, 기호 등을 포함하는 아이디 및/또는 패스워드이거나, 및/또는 주민등록번호이거나, 및/또는 운전면허번호이거나, 및/또는 보험번호 등일 때, 고객은 상기 인증 정보 입력수단(1110)을 통해 상기 고객 인증 정보(210)를 입력할 수 있다.

[0159] 인증 정보 추출수단(1115)은, 상기 인증 정보 요청 정보 수신수단(1105)을 통해 수신되는 고객 인증 정보 요청 정보에 대응하는 고객 인증 정보(210)가, 예컨대, 상기 고객 제2단말(145)에 구비되는 메모리(1130) 및/또는 IC칩(1135)에 저장되어 있는 경우, 상기 메모리(1130) 및/또는 IC칩(1135)에 저장된 고객 인증 정보(210)를 추출하는 것을 특징으로 한다.

[0160] 여기서, 상기 메모리(1130) 및/또는 IC칩(1135)에 저장되는 고객 인증 정보(210)는, 공인인증서 정보와, 공인인증서 비밀번호 정보와, 결제수단 정보와, 결제수단 비밀번호 정보와, 고객 계좌정보와, 고객 계좌에 대응하는 비밀번호 정보와, 고객 계좌에 대응하는 계좌이체 비밀번호 정보와, 상기 고객 제2단말(145)에 구비된 IC칩(1135)에 포함된 정보(또는 데이터)와, 소정의 인증키 데이터를 포함할 수 있다.

[0161] 인증 정보 생성수단(1120)은, 상기 인증 정보 입력수단(1110)을 통해 입력되는 고객 인증 정보(210) 및/또는 상기 인증 정보 추출수단(1115)을 통해 제2단말(145)의 메모리(1130) 및/또는 IC칩(1135)으로부터 추출되는 고객 인증 정보(210)에 대하여, 예컨대, 상기 고객 인증 정보(210)에 대한 암호화 처리가 요구되는 경우, 상기 입력 및/또는 추출된 고객 인증 정보(210)를 소정의 암호화 처리 프로세스에 의해 암호화하여 상기 서버(1000)로 전송할 소정의 고객 인증 정보(210)를 생성할 수 있다.

[0162] 인증 정보 전송수단(1125)은, 상기 인증 정보 입력수단(1110), 및/또는 인증 정보 추출수단(1115), 및/또는 인증 정보 생성수단(1120)을 통해 입력/추출/생성된 고객 인증 정보(210)를 상기 서버(1000)로 전송하는 것을 특징으로 한다.

[0163] 이 때, 상기 인증 정보 전송수단(1125)은, 상기 서버(1000)로부터 전송된 인증 정보 요청 정보에 상기 서버(1000)로 접속하기 위한 소정의 접속수단 정보(예컨대, 콜백 URL 등)가 포함되어 있는 경우, 상기 인증 정보 요청 정보에 포함된 접속수단 정보를 참조하여, 상기 고객 인증 정보(210)를 전송할 수 있다.

[0164] 본 발명의 바람직한 실시 방법에 따르면, 상기 서버(1000)와 고객 제2단말(예컨대, 무선 단말 등)(145) 사이에는 이동 통신망이 연결되어 있으며, 이에 의해 상기 인증 정보 전송수단(1125)이 상기 서버(1000)로 전송하는 상기 고객 인증 정보를 포함하는 메시지는 SMS 및/또는 EMS 및/또는 MMS를 포함하는 무선 메시지 중에서 적어도 하나 이상의 규격에 따라 이동 통신망을 통해 상기 서버(1000)로 전송되는 것이 바람직하다.

[0165] 메모리(1130)는, 상기 고객 제2단말(145)의 전반적인 동작을 제어하기 위한 소정의 프로그램 루틴(또는 코드) 및/또는 프로그램 데이터(예컨대, 프로그램 루틴(또는 코드)에 의한 동작이 수행될 때 입출력되는 정보 또는 데이터)를 저장하며, 하드웨어적으로 EEPROM(Electrically Erasable and Programmable Read Only Memory) 및/또는 FM(Flash Memory) 및/또는 HDD(Hard Disk Drive)를 포함하는 적어도 하나 이상의 저장수단을 포함하는 것을 특징으로 한다.

[0166] 특히, 상기 메모리(1130)에는, 본 발명에 따라 소정의 서버(1000)에 접속한 고객을 인증하기 위한 적어도 하나 이상의 고객 인증 정보(210)를 저장할 수 있으며, 상기 서버(1000)로부터 고객 제2단말(145)로 고객 인증 정보 요청 정보가 수신되는 경우, 상기 고객 제2단말(145)에 구비되는 제어부(1100)의 명령에 따라 상기 고객 인증 정보 요청 정보에 대응하는 고객 인증 정보(210)를 제공하는 것을 특징으로 한다.

[0167] IC칩(1135)은, 상기 고객 제2단말(145)에 탑재 또는 이탈착될 수 있으며, 바람직하게, ISO/IEC 7816 및/또는 ISO/IEC 14443 등을 포함하는 IC칩 규격과 EMV 규격을 참조하는 IC칩인 것을 특징으로 한다.

[0168] 본 도면11에서는 상기 IC칩(1135)에 대하여 상세하게 도시는 생략하고 있지만, 상기 IC칩(1135)은 전원 공급(VCC), 리셋 신호(RST), 클럭 신호(CLK), 접지(GND), 프로그래밍 전원 공급(VPP), 및/또는 입출력(I/O) 등과 같은 접촉점을 통해 카드 단말 장치와 통신하는 입출력 인터페이스와, CPU(Central Process Unit), MPU(Micro Process Unit), 및/또는 코프로세서(Coprocessor) 등을 포함하는 적어도 하나 이상의 연산 소자로 이루어진 프로세서부와, ROM(Read Only Memory), RAM(Random Access Memory), EEPROM(Electrically Erasable and Programmable Read Only Memory), FM(Flash Memory) 등을 포함하는 적어도 하나 이상의 메모리 소자로 이루어진 메모리부로 이루어지는 것이 바람직하다.

[0169] 또한, 상기 IC칩(1135)의 메모리 소자 중에서 적어도 하나 이상에는 칩 내부 자원을 관리하고 운영하는 칩 운영

체제(Chip Operating System; COS)가 구비되고, 또한 나머지 메모리 소자 중에서 적어도 하나 이상에는 IC칩을 이용한 서비스를 제공하기 위한 적어도 하나 이상의 IC칩 저장 정보가 구비되는 것이 바람직하다.

[0170] 상기 IC칩(1135)의 메모리부에 저장되는 IC칩 저장 정보는, 상기 제어부(1100)에 의해 판독되어 사용되는 데이터 또는 정보에 해당하는 데이터 셋트를 저장하는 데이터 저장부와, 및/또는 상기 제어부(1100)에 의해 사용되는 것이 가능한 프로그램 모듈(예컨대, 자바 애플릿(JAVA Applet)) 등이 저장 및 구동되는 데이터 처리부 등이 구비될 수 있으며, 특히, 상기 IC칩 저장 정보는, 본 발명에 따라 상기 서버로부터 전송되는 고객 인증 정보 요청 정보에 대응하는 적어도 하나 이상의 고객 인증 정보(210)가 저장되는 것을 특징으로 한다.

[0171] 제어부(1100)는, 상기 고객 제2단말(145)의 전반적인 동작을 제어 및 관리하기 위해, 상기 고객 제2단말(145)은 소정의 전원이 입력 및 부팅되는 과정에서 메모리부로부터 운영체제 루틴, 시스템 관리 루틴, 및/또는 시스템 변수들을 상기 실행 메모리로 로딩 및 상기 프로세서에 의해 연산 처리되도록 하여 상기 고객 제2단말(145)에 각 기능수단을 운영하는 것을 특징으로 한다.

[0172] 바람직하게, 상기 제어부(1100)는, 상기 고객 제2단말(145)에 구비되는 인증 정보 요청 정보 수신수단(1105)과, 인증 정보 입력수단(1110), 및/또는 인증 정보 추출수단(1115), 및/또는 인증 정보 생성수단(1120)과, 인증 정보 전송수단(1125)과, 메모리(1130), 및/또는 IC칩(1135)을 제어하고 관리하는 것을 특징으로 한다.

[0173] 또한, 제어부(1100)는, 상기 고객 제2단말(145)에 구비되는 적어도 하나 이상의 기능 수단들을 제어하기 위해, CPU/MPU를 포함하는 프로세서와 실행 메모리를 포함하여 구성될 수 있으며, 또한 소정의 메모리 소자로부터 고객 제2단말(145) 특유의 기능을 제공하기 위한 소정의 프로그램 루틴(Routine) 및/또는 프로그램 데이터를 입출력하는 버스(BUS) 및 이를 위해 구비되는 소정의 전자회로(또는 집적회로)를 포함하여 이루어질 수 있다.

[0174] 본 발명의 바람직한 일 실시 방법에 따라 상기 고객 제2단말(145)이 이동 통신망에 연결되는 상기 무선 단말인 경우, 상기 고객 제2단말(145)에는 WIPI(Wireless Internet Platform for Interoperability) 플랫폼이 탑재되어 있는 것이 바람직하며, 실시 방법에 따라서는 미국 퀄컴사의 BREW 플랫폼, 또는 WITOP(Wireless Internet Terminal Open Platform)이 탑재되어도 무방하며, 경우에 따라 WIPI 이전의 무선 플랫폼(예컨대, GVM/SK-VM 등)이 탑재될 수 있음을 밝힌다.

[0175] 여기서, 상기 고객 제2단말에 WIPI(Wireless Internet Platform for Interoperability) 플랫폼이 탑재되어 있는 경우, 본 도면11을 통해 기술되는 상기 인증 정보 요청 정보 수신수단(1105)과, 인증 정보 입력수단(1110), 및/또는 인증 정보 추출수단(1115), 및/또는 인증 정보 생성수단(1120)과, 인증 정보 전송수단(1125)과, 메모리(1130), 및/또는 IC칩(1135)은, 예컨대 WIPI 플랫폼 상에서 동작하는 것이 바람직하다.

[0176] 이하, 기술되는 도면12 내지는 도면14는 본 발명에 따라 제1단말(140)(개인용 컴퓨터 등)을 통해 서버에 접속한 고객에 대한 인증 처리를 위해 요구되는 고객 인증 정보(210)로서, 상기 고객의 제2단말(145)(무선 단말)에 구비되는 IC칩(1135)에 저장된 칩 정보를 이용하여, 상기 서버(1000)에 접속한 고객에 대한 인증 처리를 수행하는 것에 대한 실시예이다.

[0177] 도면12는 본 발명의 바람직한 실시 방법에 따른 고객 인증 과정에 대한 간단한 흐름도이다.

[0178] 도면12는 고객이 개인용 컴퓨터(PC 등)를 고객 제1단말(140)로 하여 서버(1000)에 접속하고, 고객 식별자 정보(200)로서 상기 고객의 ID/PW를 상기 서버(1000)로 전송하였을 때, 상기 서버(1000)에서, 상기 고객의 ID/PW와

연계되는 고객 제2단말(145)(본 실시예에서는 무선단말) 정보를 추출하여, 상기 고객 제2단말(145)로 고객 인증 정보(210)를 요청하는 과정에 대한 간단한 실시예이다.

[0179] 또한, 도면12를 통해 기술되는 실시예는, 본 발명에 따라 고객 인증 처리를 수행하는 서버(1000)와 상기 고객이 고객 제1단말(140)로 접속하는 서버(1000)가 동일한 경우에 대한 것임을 밝힌다.

[0180] 도면12를 참조하면, 도시되는 실시예는, 본 발명에 따른 서버에서 고객정보 및/또는 고객 식별자 정보(200)(ID/PW) 및/또는 제2단말(145)(무선단말) 정보 및/또는 고객 인증정보(칩 정보)를 소정의 저장매체(150)에 저장하는 과정으로부터 개시될 수 있다(1200).

[0181] 고객이 개인용 컴퓨터를 통해 인터넷 상의 서버(1000)에 접속하면(1205), 상기 서버(1000)는 본 발명에 따라 상기 접속한 고객에 대한 인증 프로세스를 개시한다(1210). 상기 접속 고객에 대한 인증 프로세스가 개시되면, 상기 서버(1000)는 상기 접속한 고객으로부터 고객 식별자 정보(200)의 입력을 요청하고(1215), 상기 고객은 개인용 컴퓨터에 구비되는 키보드 등을 통해 고객 식별자 정보(200)로 기 등록한 ID/PW를 입력하여 상기 서버로 전송한다(1220).

[0182] 상기 고객 컴퓨터로부터 ID/PW가 수신되면, 상기 서버(1000)는 상기 저장매체(150)와 연동하여, 상기 고객 컴퓨터로부터 수신된 고객 식별자 정보(200)(ID/PW)에 대응하는 고객 제2단말(145)(무선단말) 정보를 상기 저장매체(150)로부터 추출한다(1225).

[0183] 이 때, 상기 고객 컴퓨터로부터 수신된 고객 식별자 정보(200)(ID/PW)에 대응하는 고객 제2단말(145)(무선단말) 정보가 상기 저장매체(150)에 존재하지 않는다면(1230), 상기 서버(1000)는, 본 발명에 따른 고객 인증 프로세스를 계속적으로 수행할 수 없음을 판단하고, 상기 고객 컴퓨터로 고객인증 처리 불가 메시지를 전송한다(1235).

[0184] 여기서, 상기 고객이 본 발명에 따른 고객 인증 프로세스를 수행하기 위해 요구되는 고객 식별자 정보(200)와, 고객 제2단말 정보(205)와 고객 인증 정보(210)를 등록하지 않은 고객이라면, 상기 서버(1000)는 상기 고객에게 본 발명에 따른 고객 인증 프로세스를 수행하기 위한 상기 정보들을 등록하는 소정의 정보 등록 프로세스를 수행하도록 요청할 수 있다(1240).

[0185] 그러나, 상기 고객이 상기 정보 등록 프로세스를 수행하기를 거부한다면, 도시되는 고객 인증 과정은 종료된다(1245).

[0186] 한편, 상기 고객 컴퓨터로부터 수신된 고객 식별자 정보(200)(ID/PW)에 대응하는 고객 제2단말(145)(무선단말) 정보가 상기 저장매체(150)에 존재하여 추출되면(1250), 상기 서버(1000)는 상기 추출된 제2단말 정보(205)(무선단말번호)를 참조하여, 상기 고객 무선단말로 고객 인증 정보(210) 요청 메시지를 전송하는데(1255), 이 때, 상기 고객 인증 정보 요청 메시지에는 상기 무선단말(145)이 상기 서버에 접속하는 과정을 보다 용이하게 수행하기 위한 콜백유알엘(Callback URL)이 포함될 수 있다.

[0187] 또한, 다른 실시 방법에 따르면, 상기 서버(1000)에서 상기 고객 무선단말(145)로 전송하는 고객 인증 정보 요청 정보를 포함하는 메시지는 상기 고객 무선단말(145)에 구비 가능한 WIPI(Wireless Internet Platform for Interoperability) 플랫폼에 구비된 데이터 통신용 애플리케이션에서 수신 가능한 데이터 통신 규격을 포함하여 이루어질 수 있다.

[0188] 또한, 바람직한 다른 실시 방법에 따르면, 상기 고객 컴퓨터로부터 수신되는 고객 식별자 정보(200)로서, 고객 무선단말 정보가 사용되는 경우, 전술한 무선단말 정보 추출 과정(1220 ~ 1250)은 생략되어도 무방할 수 있다.

[0189] 도면13은 본 발명의 바람직한 실시 방법에 따른 고객 인증 과정에 대한 간단한 흐름도이다.

[0190] 도면13은 전술한 도면12에 도시된 실시예를 통해, 고객 제1단말(140)(개인용 컴퓨터(PC 등))로부터 입력된 고객 식별자 정보(200)(ID/PW)에 대응하는 고객 제2단말(145)(본 실시예에서는 무선단말) 정보를 상기 저장매체(150)로부터 추출되어, 상기 고객 제2단말(145)(무선단말)로 소정의 고객 인증 정보(210)를 요청하는 고객 인증 정보 요청 메시지가 전송된 후, 상기 고객 무선단말에서 상기 고객 인증 정보 요청 메시지에 대응하는 고객 인증 정보(210)를 추출하여 상기 서버(1000)로 전송하는 과정에 대한 간단한 실시예이다.

[0191] 특히, 도면13은 서버(1000)로부터 고객 무선단말(145)로 전송되는 고객 인증 요청 메시지에 대응하는 고객 인증 정보(210)로서, 상기 무선단말(145)에 구비되는 IC칩(1135)에 저장된 칩 정보를 이용하는 것을 특징으로 한다.

[0192] 도면13을 참조하면, 고객 제2단말(145)(무선단말)에서 상기 서버(1000)로부터 고객 인증 정보(210) 요청 메시지를 수신하는 과정으로부터 개시될 수 있다(1300).

[0193] 고객 무선 단말(145)에 상기 서버(1000)로부터 고객 인증 정보 요청 메시지가 수신되면, 고객은 상기 고객 인증 요청 메시지에 대응하는 고객 인증 정보(210)가 저장된 IC칩(1135)에 접근하기 위한 PIN 정보를 상기 무선단말(145)에 구비된 키 패드 등을 통해 입력한다(1305).

[0194] 여기서, 상기 서버(1000)로부터 전송되는 고객 인증 정보 요청 메시지는, 상기 고객 무선 단말(145)에 구비 가능한 WIPI(Wireless Internet Platform for Interoperability) 플랫폼에 구비된 데이터 통신용 애플리케이션에서 수신 가능한 데이터 통신 규격을 포함하는 메시지일 수 있으며, 이 경우 상기 수신되는 고객 인증 정보 요청 메시지에 대응하여, 상기 WIPI(Wireless Internet Platform for Interoperability) 플랫폼 상의 상기 인증 정보 요청 정보 수신수단(1105)과, 인증 정보 입력수단(1110), 및/또는 인증 정보 추출수단(1115), 및/또는 인증 정보 생성수단(1120)과, 인증 정보 전송수단(1125)과, 메모리(1130), 및/또는 IC칩(1135) 등은 해당 기능을 수행할 수 있다.

[0195] PIN 정보가 입력되면, 상기 무선단말(145)에 구비된 IC칩(1135)은 상기 키 패드 등을 통해 입력되는 PIN 정보와 상기 IC칩(1135)에 기 저장된 PIN 정보를 비교하여, 상기 입력되는 PIN 정보에 대한 유효성 인증을 실시하는데, 여기서, 상기 입력되는 PIN 정보와 상기 IC칩에 저장된 PIN 정보가 일치하지 않는 경우(1310), 상기 무선 단말(145)에 구비되는 출력수단(예컨대, 화면 출력수단, 음성 출력수단 등)을 통해 PIN입력 실패 메시지 출력하거나, 경고음을 출력할 수 있다(1315).

[0196] 바람직하게, 상기 PIN 정보 입력은 제한된 횟수 내에서 반복적으로 수행될 수 있으며, PIN 정보가 재입력되는 경우(1320), 전술한 PIN 인증 절차는 다시 수행되며, PIN 정보의 재입력이 없는 경우, 도면13에 도시된 고객 인증 과정은 종료된다(1325).

[0197] 한편, 상기 키 패드 등을 통해 입력되는 PIN 정보와 상기 IC칩(1135)에 기 저장된 PIN 정보를 비교결과, 일치하여 상기 입력되는 PIN 정보에 대한 인증이 성공적으로 수행되면(1330), 상기 무선단말(145)은 상기 IC칩(1135)

에 저장된 적어도 하나 이상의 고객 인증 정보(210)를 출력할 수 있다(1335).

[0198] 여기서, 상기 IC칩(1135)에 저장되는 고객 인증 정보(210)는, 공인인증서 정보와, 공인 인증서 비밀번호 정보와, 결제수단 정보와, 결제수단 비밀번호 정보와, 고객 계좌정보와, 고객 계좌에 대응하는 비밀번호 정보와, 고객 계좌에 대응하는 계좌이체 비밀번호 정보와, 상기 고객 제2단말(145)에 구비된 IC칩(1135)에 포함된 정보(또는 데이터)와, 소정의 인증키 데이터를 포함할 수 있다.

[0199] 상기 IC칩(1135)에 다수개의 고객 인증 정보(210)가 저장되어 있는 경우, 고객은 상기 출력된 적어도 하나 이상의 고객 인증 정보(210) 중에서 상기 서버(1000)로부터 수신된 고객 인증 정보 요청 메시지에 대응하여 전송할 고객 인증 정보(210)를 선택할 수 있다(1340).

[0200] 상기와 같이, 상기 고객 인증 정보 요청 메시지에 대응하는 고객 인증 정보(210)가 선택되면, 상기 무선단말(145)은 상기 서버(1000)로부터 수신된 고객 인증 정보 요청 메시지에 포함된 상기 서버의 접속 정보(예컨대, Callback URL 등)를 확인하고(1345), 상기 확인된 서버 접속 정보를 참조하여, 상기 선택된 고객 인증 정보(210)를 전송한다(1350). 그리고, 상기 무선단말(145)은 상기 고객 인증 정보(210) 전송 내역을 상기 화면 출력 수단 등을 통해 출력하여 상기 고객이 인지하도록 한다(1355).

[0201] 도면14는 본 발명의 바람직한 실시 방법에 따른 고객 인증 과정에 대한 간단한 흐름도이다.

[0202] 도면14는 전술한 도면13에 도시된 실시예를 통해, 고객 제2단말(145)(본 실시예에서는 무선단말)로부터 상기 고객 제2단말(145)에 저장된 고객 인증 정보(210)가 서버(1000)로 전송된 후, 상기 서버(1000)에서 상기 고객 제2단말(145)로부터 전송된 고객 인증 정보(210)를 이용하여, 상기 고객에 대한 인증 처리를 수행하는 과정에 대한 간단한 실시예이다.

[0203] 도면14는 서버에서 고객 제2단말(145)(무선단말)로부터 고객 인증 정보(210)(예컨대, 칩 정보 등)를 포함하는 고객 인증 요청 응답 메시지를 수신하는 과정으로부터 개시될 수 있다(1400).

[0204] 상기 도면13의 실시예를 통해, 상기 고객 제2단말(145)(무선단말)로부터 고객 인증 정보(210)(예컨대, 칩 정보 등)를 포함하는 고객 인증 요청 응답 메시지가 수신되면, 상기 서버(1000)는 상기 수신된 고객 인증 요청 응답 메시지에 포함된 고객 인증 정보(210)(예컨대, 칩 정보 등)를 확인한다(1405).

[0205] 그리고, 상기 서버(1000)는 저장매체(150)로부터 상기 고객 정보와 연계되어 저장된 고객 인증 정보(210)를 독출하고(1410), 상기 저장매체(150)로부터 독출된 고객 인증 정보(210)와 상기 고객 인증 요청 응답 메시지로부터 확인된 고객 인증 정보(210)를 비교하여, 고객 인증 정보(210)가 일치하는지 판단한다(1415).

[0206] 만약, 상기 저장매체(150)로부터 독출된 고객 인증 정보(210)와 상기 고객 인증 요청 응답 메시지로부터 확인된 고객 인증 정보(210)가 일치하지 않는다면(1420), 상기 서버(1000)는 상기 고객 제1단말(140) 및/또는 제2단말(145)로 고객 인증 정보(210) 불일치 메시지를 전송할 수 있다(1425).

[0207] 반면에, 상기 저장매체(150)로부터 독출된 고객 인증 정보(210)와 상기 고객 인증 요청 응답 메시지로부터 확인된 고객 인증 정보(210)가 일치한다면(1430), 상기 서버(1000)는 상기 제1단말(140)로 접속한 고객에 대한 인증 처리가 성공적으로 수행되었음을 확인하고, 상기 고객 제1단말(140) 및/또는 제2단말(145)로 고객 인증 처리 내

역을 전송한다(1435).

[0208] 바람직하게, 상기 서버(1000)를 통해 고객 인증 처리가 성공적으로 수행되면, 상기 서버(1000)는 상기 고객의 접속허가 및/또는 컨텐츠 이용에 대한 권한을 부여할 수 있다(1440).

[0209] 도면15는 본 발명의 바람직한 실시 방법에 따른 고객 인증 과정에 대한 간단한 흐름도이다.

[0210] 도면15는 전술한 도면10의 고객 인증 시스템(100)을 참조하여, 고객이 ATM 또는 현금입출금기 또는 결제단말을 고객 제1단말(140)로 하는 경우, 상기 고객 제1단말(140)을 통해 요청되는 일련의 트랜잭션(예컨대, 금융거래 등)에 대하여, 서버(1000)에서 상기 고객의 제2단말(145)(예컨대, 무선단말)과 연동하여 상기 트랜잭션 요청 고객에 대한 고객 인증 정보(210)를 수신, 상기 고객에 대한 인증 처리를 수행하여 상기 고객 제1단말(140)을 통해 요청되는 소정의 트랜잭션을 허여하는 과정에 대한 간단한 실시예이다.

[0211] 도면15에 따르면, 상기 서버(1000)는, 상기 ATM 또는 현금입출금기 또는 결제단말과 연동하는 금융 서버 또는 VAN사 서버인 것을 특징으로 한다.

[0212] 또한, 본 도면에 도시된 실시예를 기술하기 전에, 상기 도면12에 전술한 바와 같이, 본 발명에 따른 서버(1000)에서 고객정보 및/또는 고객 식별자 정보(200)(예컨대, 카드/계좌번호, 카드/계좌 비밀번호 등) 및/또는 제2단말(145)(무선단말) 정보 및/또는 고객 인증정보를 소정의 저장매체(150)에 저장하는 과정이 선행되었음을 명기한다.

[0213] 도면15를 참조하면, 본 실시예는, 고객이 ATM 또는 CD(Cash Dispenser) 또는 결제단말 등을 통해 소정의 금융거래 요청을 하는 과정으로부터 시작될 수 있다(1500). 고객은 상기 ATM 또는 CD 또는 결제단말을 통해 고객 식별자 정보(200)를 입력할 수 있는데(1505), 여기서, 상기 고객 식별자 정보(200)는, 고객 카드 또는 계좌번호, 및/또는 카드 또는 계좌 비밀번호 등이 바람직할 것이다.

[0214] 또한, 상기 고객 식별자 정보(200)를 상기 ATM 또는 CD(Cash Dispenser) 또는 결제단말로 입력 또는 전달하는 과정은, 접촉식 및/또는 비접촉식 인터페이스를 이용하는 것을 포함할 수 있으며, 비접촉식 인터페이스는, 휴대 인터넷 인터페이스, 적외선(Infrared Ray) 인터페이스, RF(Radio Frequency) 인터페이스, 블루투스(BlueTooth) 인터페이스, 무선랜(Wireless LAN) 인터페이스, 와이파이(Wi-Fi) 인터페이스, ZigBee 인터페이스, UWB 인터페이스 등을 적어도 하나 이상 포함하는 근거리 통신 인터페이스가 가능할 수 있다.

[0215] ATM 또는 CD 또는 결제단말에서 상기 고객 식별자 정보(200)가 입력되면, 상기 ATM 또는 CD 또는 결제단말은 상기 고객 식별자 정보(200)를 포함하는 금융거래 요청 전문을 생성하여 네트워크(VAN 등)를 통해 서버(1000)(예컨대, 금융서버 또는 VAN서버)로 전송한다(1510).

[0216] 그러면, 상기 서버(1000)는 상기 ATM 또는 CD 또는 결제단말로부터 수신된 금융거래 요청 전문에 포함된 고객 식별자 정보(200)를 확인하고(1515), 상기 확인된 고객 식별자 정보(200)에 대응하는 고객 제2단말(무선단말) 정보(205)를 저장매체(150)로부터 추출하여(1520), 상기 저장매체(150)로부터 추출된 고객 제2단말 정보(205)를 참조, 상기 고객 제2단말(145)로 고객 인증 정보(210) 요청 메시지를 전송한다(1525).

[0217] 고객 제2단말(145)(무선단말)은 상기 서버(1000)로부터 상기 고객 인증 정보(210) 요청 메시지를 수신하고, 상

기 고객 제2단말(145)(무선단말)에 구비된 메모리(1130) 또는 IC칩(1135)에 탑재된 고객 인증 정보(210)를 추출하고(1530), 상기 추출된 고객 인증 정보(210)가 포함된 고객 인증 정보 응답 메시지를 생성하여 상기 서버로 전송한다(1535).

[0218] 여기서, 상기 고객 인증 정보(210) 추출 과정은, 전술한 도면13을 참조할 수 있으며, 본 도면에서는 생략하기로 한다.

[0219] 서버(1000)는 상기 고객 제2단말(145)(무선단말)로부터 수신된 고객 인증 요청 응답 메시지로부터 고객 인증 정보(210)를 확인하고, 대응하는 고객 인증 정보(210)를 상기 저장매체(150)로부터 추출한다(1540). 그리고, 상기 서버(1000)는 상기 저장매체(150)로부터 추출된 고객 인증 정보(210)와 상기 고객 인증 요청 응답 메시지로부터 확인된 고객 인증 정보(210)를 비교하여, 고객 인증 정보(210) 일치 여부를 판단한다(1545).

[0220] 여기서, 상기 저장매체(150)로부터 추출된 고객 인증 정보(210)와 상기 고객 인증 요청 응답 메시지로부터 확인된 고객 인증 정보(210)가 일치하지 않는다면(1550), 상기 서버(1000)는 상기 고객에 대한 인증 처리를 실패한 것을 판단하고, 상기 고객 제1단말(140) 및/또는 제2단말(145)로 고객 인증 정보(210) 불일치 메시지 및/또는 고객 인증 정보(210) 불일치 내역이 포함된 금융거래 요청 응답 전문을 전송할 수 있다(1555).

[0221] 반면에, 상기 저장매체(150)로부터 추출된 고객 인증 정보(210)와 상기 고객 인증 요청 응답 메시지로부터 확인된 고객 인증 정보(210)가 일치한다면(1560), 상기 서버(1000)는 상기 고객에 대한 인증이 성공적으로 수행되었음을 인지하고, 상기 고객 제1단말(140)로 고객 인증 처리 내역이 포함된 금융거래 요청 응답 전문을 전송함으로서(1565), 상기 ATM 또는 CD 또는 결제단말을 통한 고객 금융거래를 성공적으로 수행할 수 있도록 한다(1570).

[0222] 도면16은 본 발명의 바람직한 다른 실시 방법에 따른 고객 인증 시스템(100)에 대한 구성도이다.

[0223] 도면16은, 전술한 도면1 도시된 고객 인증 시스템(100)에 구비되는 적어도 하나 이상의 기능 수단들을 포함하는 고객 인증 서버(1600)(예컨대, 고객 인증 중계서버)와, 적어도 하나 이상의 고객이 접속하며 상기 고객 인증 서버(1600)로 상기 접속한 고객의 인증을 요청하는 웹서버(1630)와, 상기 웹서버(1630)에 접속하는 고객 제1단말(140)(예컨대, 개인용 컴퓨터 등)과, 상기 고객 인증 서버(1600)의 고객 인증 정보(210) 요청에 따라 상기 서버(1600)로 제공하는 고객 인증 정보(210)를 저장하는 고객 제2단말(145)(예컨대, 무선 단말 등)을 도시하고 있는 실시예도이다.

[0224] 도면16을 참조하면, 서버(1600)는, 고객 제2단말(145)이 전송하는 고객 인증 정보(210)를 수신하는 정보 수신부(1605) 및 상기 정보 수신부(1605)가 수신한 고객 인증 정보(210)를 이용하여 상기 고객을 인증 처리하는 고객 인증부(1615) 및 상기 고객 인증 결과를 상기 고객 제1단말(140)이 접속한 서버(1630)로 전송하는 전송부(1620)를 포함하여 구성될 수 있다.

[0225] 또한, 상기 정보 수신부(1605)는, 상기 수신한 고객 인증 정보(210)를 상기 고객 제1단말(140)로 전송하여, 상기 고객 제1단말(140)에서 상기 고객 인증 정보(210)를 임시 저장하여 이용할 수 있도록 한다.

[0226] 또한, 서버(1600)는, 상기 고객 인증 정보(210)에 대응하는 서버(1630)-상기 고객 제1단말(140)이 접속한 서버(1630)-를 확인하는 정보 확인부(1625)를 더 구비하여 구성될 수 있다.

[0227] 여기서, 고객 인증 처리를 위해 요구되는 고객 인증 정보(210)는, 아이디(ID) 정보와, 패스워드 정보와, 고객 개인정보와, 고객 생체정보와, 고객 통신수단 정보와, 공인인증서 정보와, 공인 인증서 비밀번호 정보와, 결제수단 정보와, 결제수단 비밀번호 정보와, 고객 계좌정보와, 고객 계좌에 대응하는 비밀번호 정보와, 고객 계좌에 대응하는 계좌이체 비밀번호 정보와, 상기 고객 제2단말(145)에 구비된 IC칩(1135)에 포함된 정보(또는 데이터)와, 상기 고객 제2단말(145)에 구비된 IC칩에 포함된 공인 인증서 정보와, 상기 고객 제2단말(145)에 구비된 IC칩 고유 정보와, 상기 고객 제2단말(145)에 구비된 소정의 인증키 데이터를 적어도 하나 이상 포함할 수 있다.

[0228] 또한, 고객 인증 정보(210)는, 소정의 암호화 처리 프로세스에 따라 암호화 처리되어 전송될 수 있는데, 여기서, 상기 서버(1600)의 고객 인증부(1615)는, 상기 고객 인증 정보(210)가 소정의 암호화 처리 프로세스에 따라 암호화 처리되어 전송된 경우, 상기 암호화 처리된 고객 인증 정보(210)를 복호화 처리하는 것을 특징으로 한다.

[0229] 또한, 전술한 바와 같이, 상기 적어도 하나 이상의 고객 인증 정보(210)를 구비할 수 있으며, 상기 고객 인증 정보(210)를 서버(1600)로 전송하는 제2단말(145)은, 휴대폰, PDA, 휴대 인터넷 폰, 텔레메틱스 등 무선 단말과, 유선전화기와, 컴퓨터를 포함하는 유선 단말과, 정보처리기(또는 KIOSK), 현금지급기, 현금입출금기, 결제단말을 적어도 하나 이상 포함하는 단말(또는 기기)과, 텔레비전, 냉장고, 전자레인지, 오디오 등 통신기능이 구비된 가전기기와, 통신기능이 구비된 운동기기와, RFID 단말을 적어도 하나 이상 포함할 수 있다.

[0230] 한편, 도면16에 도시되는 서버(1600)는, 전술한 서버 기능을 실행하기 위한 컴퓨터로 읽을 수 있는 프로그램을 기록한 기록매체를 포함하는 것을 특징으로 한다.

[0231] 도면17은 본 발명의 바람직한 다른 실시 방법에 따른 고객 인증 과정에 대한 간단한 개념도이다.

[0232] 도면17을 참조하면, 도시된 실시예는, 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)과, 저장매체(150)와, 서버와, 고객 제1단말(140) 및 고객 제2단말(145)을 포함하며, 고객은 상기 고객 제1단말(140)을 통해 상기 서버에 접속하고, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)은 상기 서버에 접속하는 고객의 제2단말 정보(205)를 확인하여, 상기 고객 제2단말(145)로부터 소정의 고객 인증 정보(210)를 수신하는 것을 특징으로 한다.

[0233] 또한, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)은, 상기 고객 제2단말(145)로부터 수신한 고객 인증 정보(210)를 상기 고객 제1단말(140)로 전송하여, 상기 고객 제1단말(140)에 임시 저장하는 것을 특징으로 한다.

[0234] 또한, 본 실시예에서는 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)에서 상기 고객 인증 정보(210)가 구비된 고객 제2단말 정보(210)를 상기 고객 제1단말(140)로부터 전송되는 고객 식별자 정보(200)를 이용하여, 소정의 저장매체(150)에서 추출하는 것으로 도시하고 있지만, 전술한 도면8 내지는 도면9와 같이, 상기 고객 제1단말(140)로부터 직접 상기 고객 제2단말 정보(210)를 수신할 수도 있음을 밝힌다.

[0235] 여기서, 상기 서버는, 고객이 접속하고자 하는 인터넷 상의 웹서버, 컨텐츠 제공 서버, 금융서버 등이 될 수 있으며, 상기 고객 인증 시스템(100)은 상기 서버에 접속하는 고객에 대한 인증 처리를 대행 및/또는 중계하는 중계서버(또는 통신사 서버)가 될 수 있다.

[0236] 도면17에 따르면, 도시된 고객 인증 과정을 수행하기 위하여, 고객으로부터 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)에 상기 고객 인증 과정에 요구되는 고객 식별자 정보(200)와, 고객 제2단말 정보(205)와, 고객 인증 정보(210)를 등록하는 과정과(1), 상기 고객 인증 시스템(100)(또는 서버 또는 통신사 서버)에서 저장매체(150)에 상기 고객이 제공하는 고객 식별자 정보(200)와, 고객 제2단말 정보(205)와, 고객 인증 정보(210)와 상기 고객 정보를 연계하여 저장하는 과정이 선행되는 것이 바람직하다(2).

[0237] 또한, 본 실시예에서 이용되며, 고객 제2단말(145)의 메모리(1130) 또는 IC칩(1135)에 저장되는 고객 인증 정보는, 아이디(ID) 정보와, 패스워드 정보와, 고객 개인정보와, 고객 생체정보와, 고객 통신수단 정보와, 공인인증서 정보와, 공인 인증서 비밀번호 정보와, 결제수단 정보와, 결제수단 비밀번호 정보와, 고객 계좌정보와, 고객 계좌에 대응하는 비밀번호 정보와, 고객 계좌에 대응하는 계좌이체 비밀번호 정보와, 상기 고객 제2단말에 구비된 IC칩에 포함된 정보(또는 데이터)와, 상기 고객 제2단말에 구비된 IC칩에 포함된 공인 인증서 정보와, 상기 고객 제2단말에 구비된 IC칩 고유 정보와, 상기 고객 제2단말에 구비된 소정의 인증키 데이터를 적어도 하나 이상 포함할 수 있다.

[0238] 이후, 고객은 소정의 단말(예컨대, 고객 제1단말(140))을 이용하여, 소정의 서버(예컨대, 인터넷 상의 웹서버, 컨텐츠 제공 서버 등)에 접속하는 과정에서, 상기 고객 식별자 정보(200)를 상기 서버로 제공하고(3), 상기 서버는 상기 고객 제1단말(140)로부터 제공된 고객 식별자 정보(200)를 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)으로 제공하여, 상기 접속한 고객에 대한 인증 처리를 요청한다(4).

[0239] 이 때, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)은 상기 서버의 인증 처리 요청에 따라, 상기 서버로부터 제공된 고객 식별자 정보(200)에 대응하는 고객 제2단말 정보(205)를 상기 저장매체(150)로부터 추출하고(5), 상기 추출된 고객 제2단말 정보(205)를 참조하여, 상기 고객 제2단말(145)로 상기 고객 인증을 위해 요구되는 고객 인증 정보(210)를 요청한다(6).

[0240] 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)으로부터 고객 인증 정보(210) 요청 메시지가 상기 고객 제2단말(145)로 전송되면, 고객은 상기 고객 제2단말(145)로 수신되는 고객 인증 요청 정보에 대응하는 고객 인증 정보(210)를 상기 고객 제2단말(145)로부터 입력 및/또는 추출하여(7), 상기 입력 및/또는 추출된 고객 인증 정보(210)를 상기 고객 제2단말(145)을 통해 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)으로 전송한다(8).

[0241] 그러면, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)은 상기 고객 제2단말(145)로부터 전송된 고객 인증 정보(210)와, 상기 저장매체(150)에 기 저장된 고객 인증 정보(210)를 비교함으로서, 상기 고객 인증 정보의 유효성을 확인하고(9), 상기 유효성이 확인된 고객 인증 정보를 상기 고객 제1단말로 전송한다(10).

[0242] 본 실시예에서는, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)에서 상기 고객 제2단말(145)로부터 전송된 고객 인증 정보(210)에 대한 유효성 확인 과정을 수행하지만, 바람직한 다른 실시 방법에 따르면, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)의 고객 인증 정보(210) 유효성 인증 과정은 생략되어도 무방할 것이다. 다만, 이 경우, 상기 고객 인증 정보(210)에 대한 유효성 인증 과정은 상기 고객이 제1단말(140)로 접속한 서버에서 수행될 수 있다.

[0243] 한편, 상기 고객 인증 시스템(100)(또는 중계서버 또는 통신사 서버)으로부터 상기 고객 인증 정보(210)가 고객 제1단말로 전송되면, 상기 고객 제1단말은, 상기 전송된 고객 인증 정보(210)를 상기 고객 제1단말에 구비된 메모리(또는 IC칩) 등에 임시 저장한다(11).

[0244] 바람직하게, 상기 고객 제1단말(140)에 임시 저장된 고객 인증 정보(210)는, 상기 고객 제1단말(140)이 접속하는 서버와 연동하여, 상기 서버에 접속한 고객에 대한 소정의 인증후 작업(예컨대, 로그인, 컨텐츠 이용, 결제 등) 등을 개시하는데 이용될 수 있다.

발명의 효과

[0245] 본 발명에 따르면, 제1단말로 접속한 고객에 대한 인증을 상기 고객의 제2단말에 저장된 고객 인증 정보를 통해 수행하도록 함으로서, 기존의 피싱(Phishing)이나, 파밍(Pharming), 또는 키보드 해킹 등을 통한 개인 정보 유출을 보다 안전하고 효율적으로 차단할 수 있다는 장점이 있다.

[0246] 또한, 본 발명에 따른 고객 인증 정보가 저장된 고객 제2단말이 무선단말인 경우, 통신 사업자는, 통신망 운용에 따르는 부가 수익을 창출할 수 있다는 장점이 있다.

[0247] 또한, 본 발명을 통신 사업자가 유치하는 경우, 다수의 사이트(또는 기관)에 대한 인증 처리를 대행함으로서, 새로운 수익을 창출할 수 있다는 장점이 있다.

[0248] 또한, 본 발명이 금융거래에 적용되는 경우, 금융 기관은, 고객이 안전한 금융거래를 수행하도록 함으로서, 보다 많은 금융거래 고객을 유치할 수 있으며, 기업 이미지를 새롭게 제고할 수 있다는 장점이 있다.

도면의 간단한 설명

[0001] 도1은 본 발명에 따른 바람직한 고객 인증 시스템의 개략적인 구성을 도시한 도면이다.

[0002] 도2는 본 발명에 따른 바람직한 저장매체의 구성을 도시한 도면이다.

[0003] 도3은 본 발명의 바람직한 실시예에 따른 고객 식별자 정보에 대한 간단한 예시도이다.

[0004] 도4는 본 발명의 바람직한 실시예에 따른 고객 제2단말 정보에 대한 간단한 예시도이다.

[0005] 도5는 본 발명의 바람직한 실시예에 따른 고객 인증 정보에 대한 간단한 예시도이다.

[0006] 도6은 본 발명의 바람직한 실시 방법에 따른 고객 인증 과정에 대한 간단한 개념도이다.

[0007] 도7은 본 발명의 바람직한 실시 방법에 따라 중계서버를 포함하는 고객 인증 과정에 대한 간단한 개념도이다.

[0008] 도8은 본 발명의 바람직한 다른 실시 방법에 따른 고객 인증 과정에 대한 간단한 개념도이다.

[0009] 도9는 본 발명의 바람직한 다른 실시 방법에 따라 중계서버를 포함하는 고객 인증 과정에 대한 간단한 개념도이다.

[0010] 도10은 본 발명의 바람직한 실시 방법에 따른 고객 인증 시스템에 대한 간단한 구성도이다.

[0011] 도11은 본 발명의 바람직한 실시 방법에 따른 고객 제2단말에 대한 간단한 구성도이다.

[0012] 도12는 본 발명의 바람직한 실시 방법에 따른 고객 인증 과정에 대한 간단한 흐름도이다.

[0013] 도13은 본 발명의 바람직한 실시 방법에 따른 고객 인증 과정에 대한 간단한 흐름도이다.

[0014] 도14는 본 발명의 바람직한 실시 방법에 따른 고객 인증 과정에 대한 간단한 흐름도이다.

[0015] 도15는 본 발명의 바람직한 실시 방법에 따른 고객 인증 과정에 대한 간단한 흐름도이다.

[0016] 도16은 본 발명의 바람직한 다른 실시 방법에 따른 고객 인증 시스템에 대한 구성도이다.

[0017] 도17은 본 발명의 바람직한 다른 실시 방법에 따른 고객 인증 과정에 대한 간단한 개념도이다.

[0018] <도면의 주요부분에 대한 설명>

[0019] 100 : 고객 인증 시스템 105 : 정보 수신수단(1)

[0020] 110 : 정보 독출수단 115 : 고객 인증수단

[0021] 120 : 정보 전송수단 125 : 정보 수신수단(2)

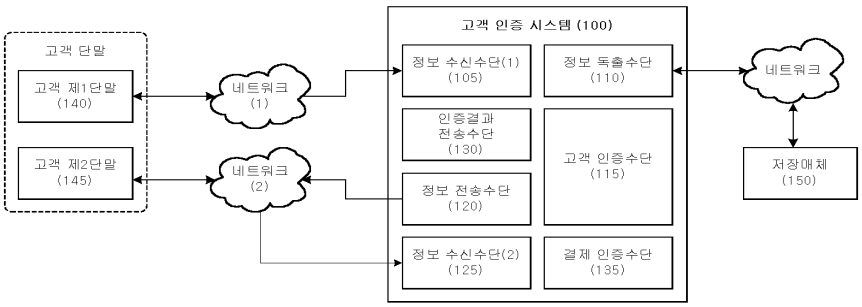
[0022] 130 : 인증결과 전송수단 135 : 결제 인증수단

[0023] 140 : 고객 제1단말 145 : 고객 제2단말

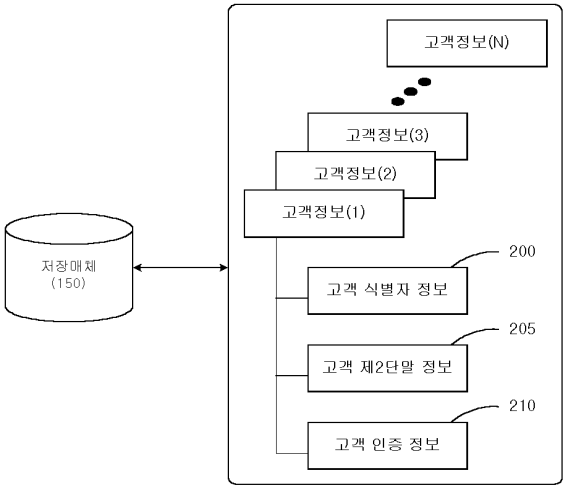
[0024] 150 : 저장매체

도면

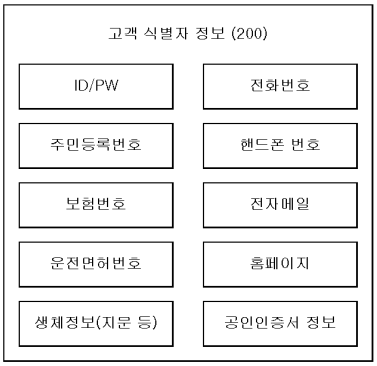
도면1



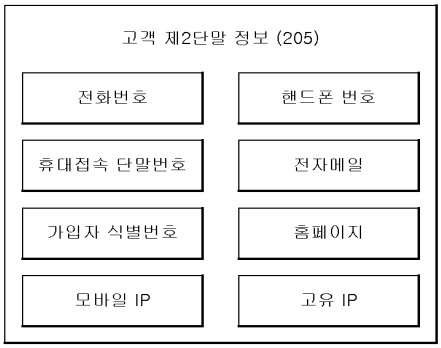
도면2


고객정보(N)
고객정보(3)
고객정보(2)
고객정보(1)
저장매체
(150)
200
고객 식별자 정보
205
고객 제2단말 정보
210
고객 인증 정보

도면3


고객 식별자 정보 (200)
ID/PW
전화번호
주민등록번호
핸드폰 번호
보험번호
전자메일
운전면허번호
홈페이지
생체정보(지문 등)
공인인증서 정보

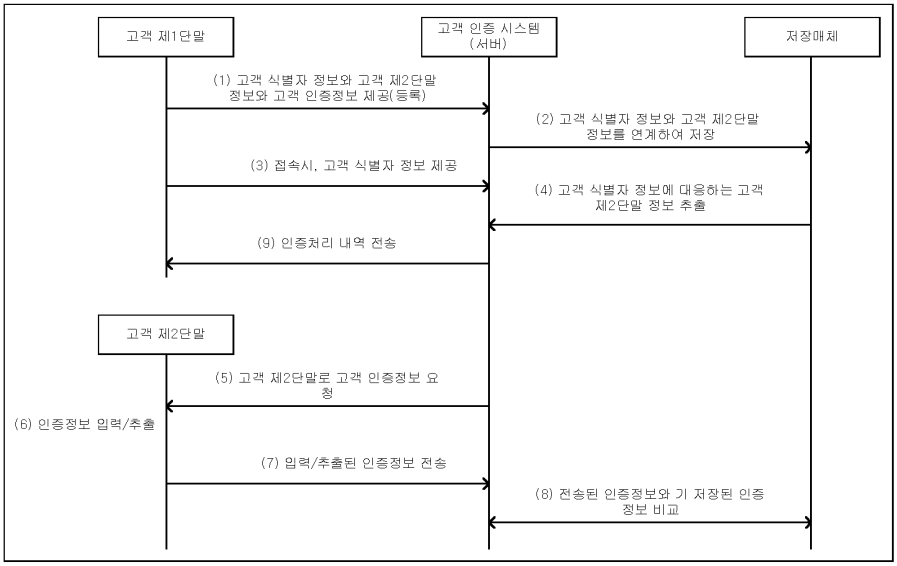
도면4


고객 제2단말 정보 (205)
전화번호
핸드폰 번호
휴대접속 단말번호
전자메일
가입자 식별번호
홈페이지
모바일 IP
고유 IP

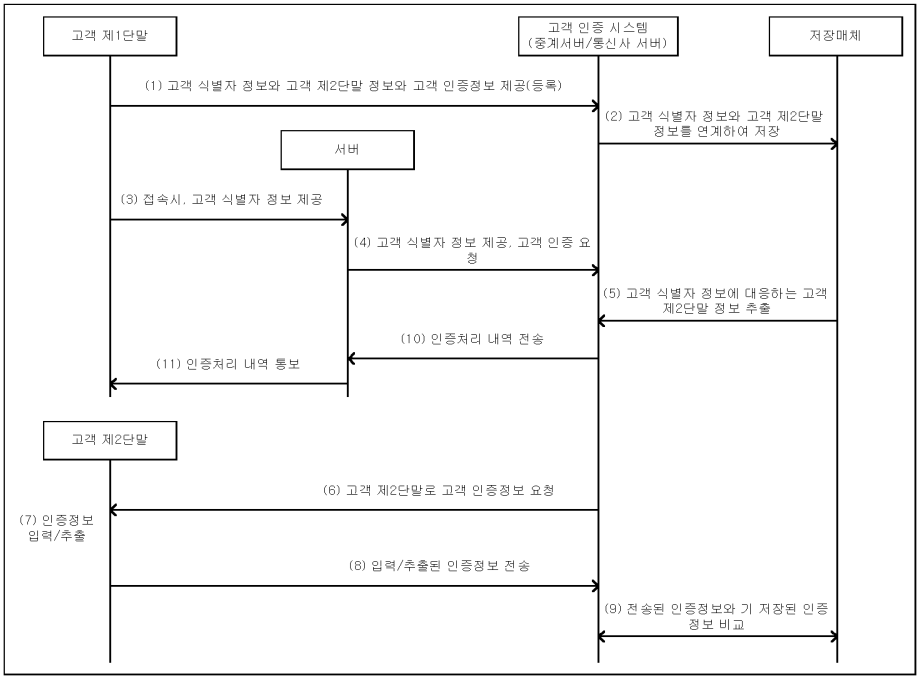
도면5


고객 인증 정보 (210)
ID/PW
전화번호
주민등록번호
핸드폰 번호
보험번호
전자메일
운전면허번호
홈페이지
생체정보(지문 등)
공인인증서 정보
모바일 IP
고유 IP
휴대접속 단말번호
가입자 식별번호
카드번호
계좌번호
IC칩 시리얼번호
IC칩 비밀번호

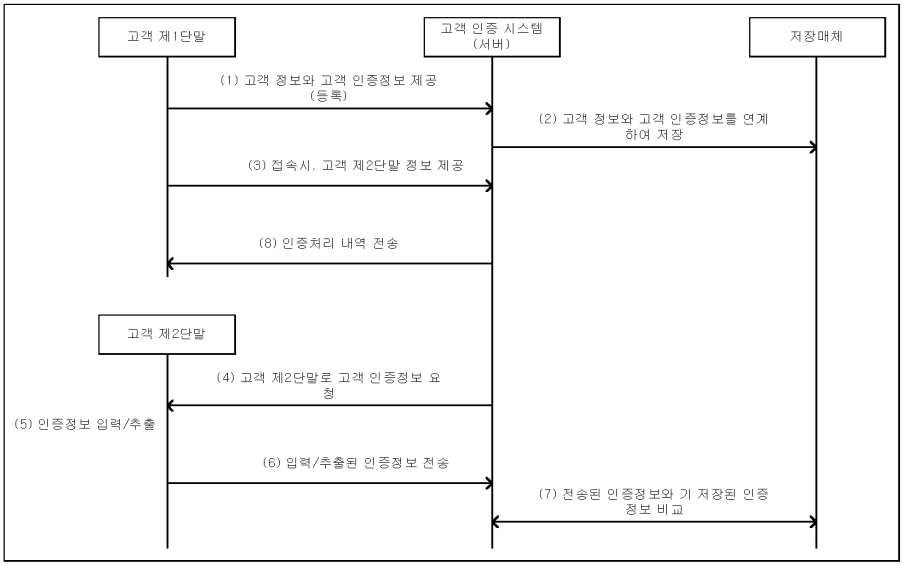
도면6


고객 제1단말
고객 인증 시스템
(서버)
저장매체
(1) 고객 식별자 정보와 고객 제2단말 정보와 고객 인증정보 제공(등록)
(2) 고객 식별자 정보와 고객 제2단말 정보를 연계하여 저장
(3) 접속시, 고객 식별자 정보 제공
(4) 고객 식별자 정보에 대응하는 고객 제2단말 정보 추출
(9) 인증처리 내역 전송
고객 제2단말
(5) 고객 제2단말로 고객 인증정보 요청
(6) 인증정보 입력/추출
(7) 입력/추출된 인증정보 전송
(8) 전송된 인증정보와 기 저장된 인증정보 비교

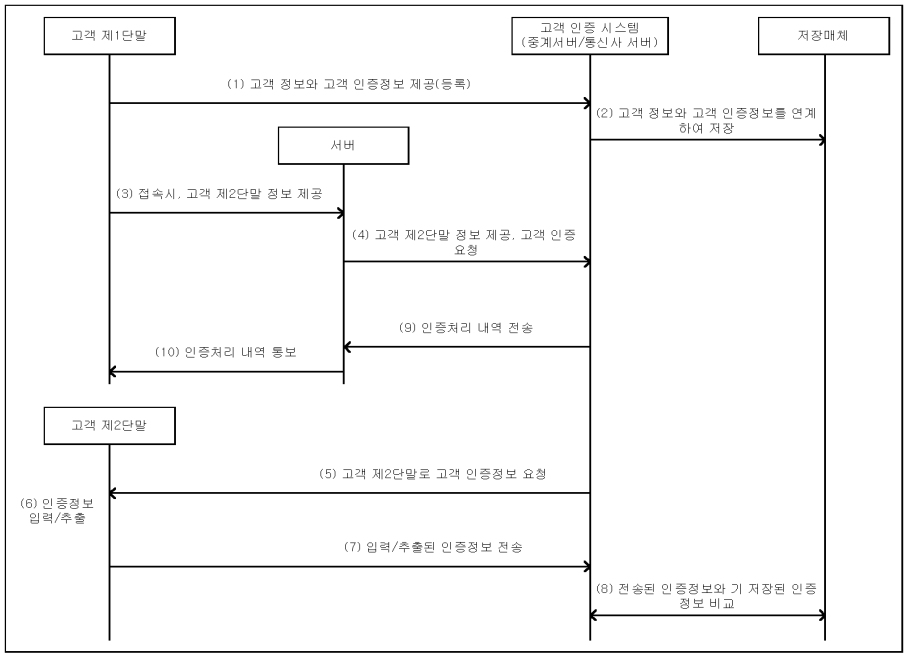
도면7


고객 제1단말
고객 인증 시스템
(중계서버/통신사 서버)
저장매체
(1) 고객 식별자 정보와 고객 제2단말 정보와 고객 인증정보 제공(등록)
(2) 고객 식별자 정보와 고객 제2단말 정보를 연계하여 저장
서버
(3) 접속시, 고객 식별자 정보 제공
(4) 고객 식별자 정보 제공, 고객 인증 요청
(5) 고객 식별자 정보에 대응하는 고객 제2단말 정보 추출
(10) 인증처리 내역 전송
(11) 인증처리 내역 통보
고객 제2단말
(6) 고객 제2단말로 고객 인증정보 요청
(7) 인증정보 입력/추출
(8) 입력/추출된 인증정보 전송
(9) 전송된 인증정보와 기 저장된 인증정보 비교

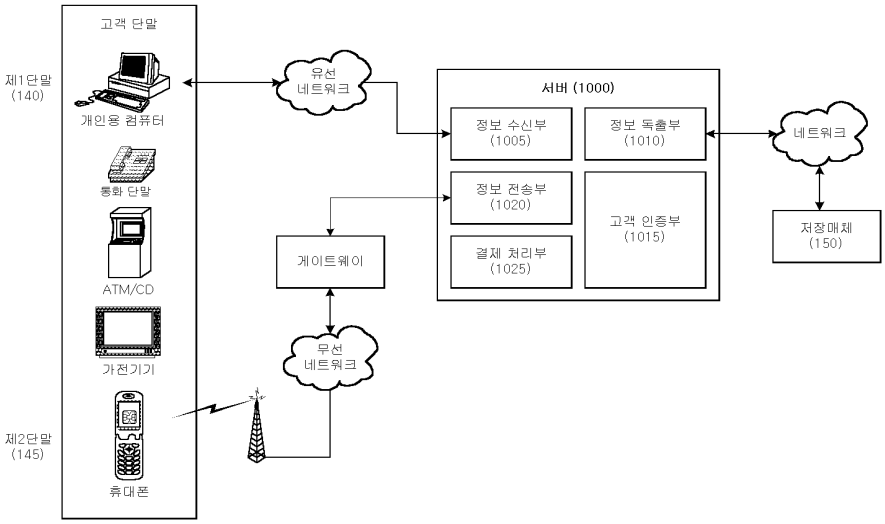
도면8


고객 제1단말
고객 인증 시스템
(서버)
저장매체
(1) 고객 정보와 고객 인증정보 제공
(등록)
(2) 고객 정보와 고객 인증정보를 연계
하여 저장
(3) 접속시, 고객 제2단말 정보 제공
(8) 인증처리 내역 전송
고객 제2단말
(4) 고객 제2단말로 고객 인증정보 요
청
(5) 인증정보 입력/추출
(6) 입력/추출된 인증정보 전송
(7) 전송된 인증정보와 기 저장된 인증
정보 비교

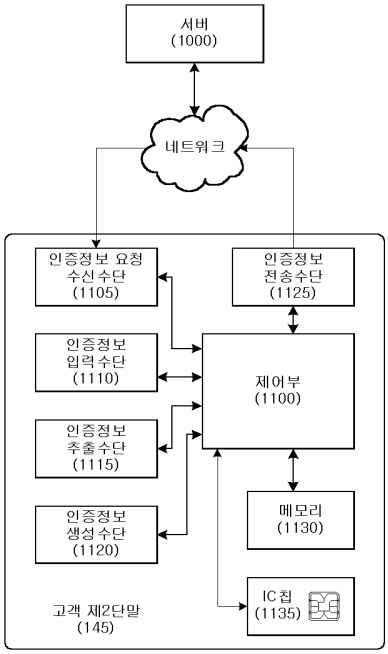
도면9


고객 제1단말
고객 인증 시스템
(중계서버/통신사 서버)
저장매체
(1) 고객 정보와 고객 인증정보 제공(등록)
(2) 고객 정보와 고객 인증정보를 연계하여 저장
서버
(3) 접속시, 고객 제2단말 정보 제공
(4) 고객 제2단말 정보 제공, 고객 인증 요청
(9) 인증처리 내역 전송
(10) 인증처리 내역 통보
고객 제2단말
(5) 고객 제2단말로 고객 인증정보 요청
(6) 인증정보 입력/추출
(7) 입력/추출된 인증정보 전송
(8) 전송된 인증정보와 기 저장된 인증정보 비교

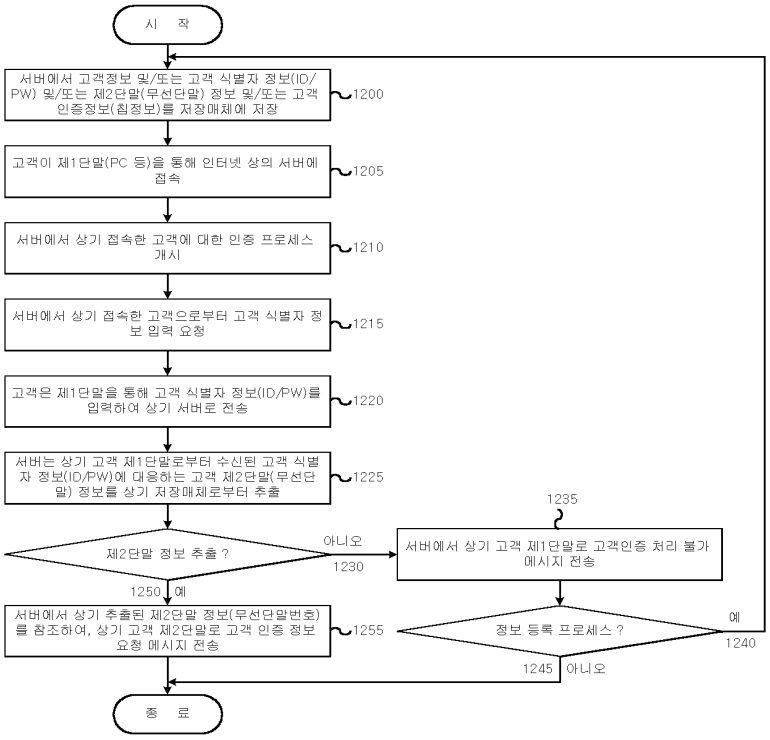
도면10


고객 단말
제1단말
(140)
개인용 컴퓨터
통화 단말
ATM/CD
가전기기
제2단말
(145)
휴대폰
유선
네트워크
무선
네트워크
게이트웨이
서버 (1000)
정보 수신부
(1005)
정보 독출부
(1010)
정보 전송부
(1020)
고객 인증부
(1015)
결제 처리부
(1025)
네트워크
저장매체
(150)

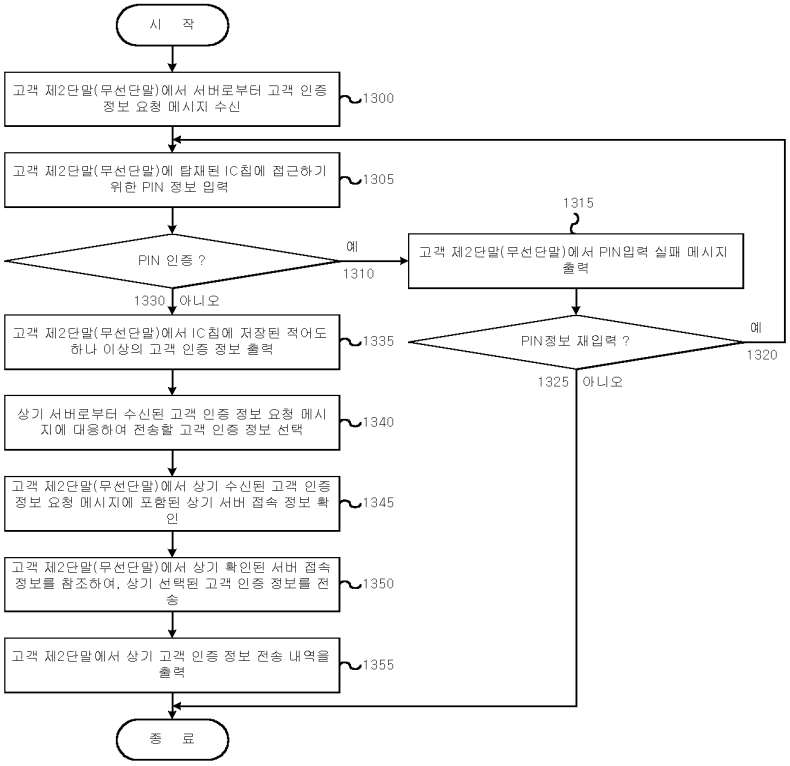
도면11


서버
(1000)
네트워크
인증정보 요청
수신수단
(1105)
인증정보
전송수단
(1125)
인증정보
입력수단
(1110)
제어부
(1100)
인증정보
추출수단
(1115)
메모리
(1130)
인증정보
생성수단
(1120)
IC칩
(1135)
고객 제2단말
(145)

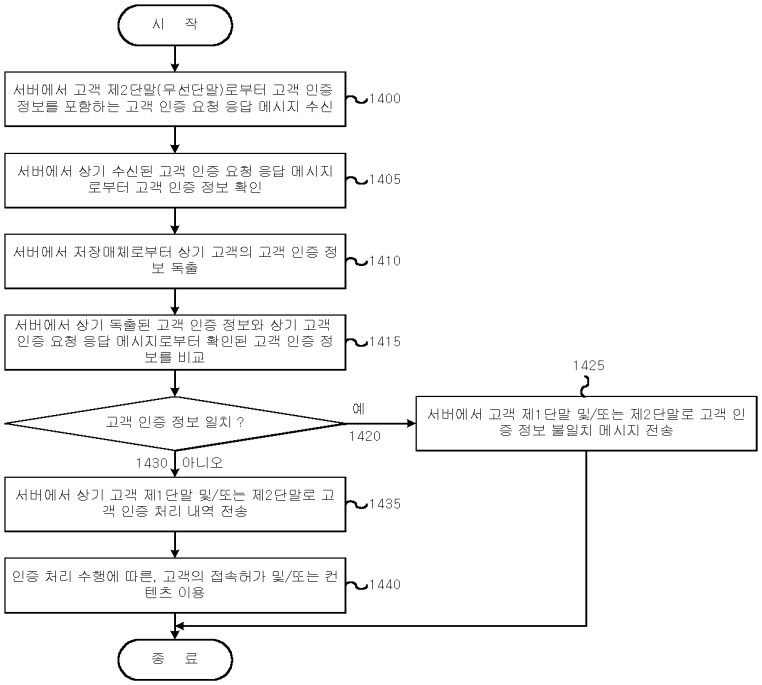
도면12


시 작
서버에서 고객정보 및/또는 고객 식별자 정보(ID/PW) 및/또는 제2단말(무선단말) 정보 및/또는 고객 인증정보(침정보)를 저장매체에 저장
1200
고객이 제1단말(PC 등)을 통해 인터넷 상의 서버에 접속
1205
서버에서 상기 접속한 고객에 대한 인증 프로세스 개시
1210
서버에서 상기 접속한 고객으로부터 고객 식별자 정보 입력 요청
1215
고객은 제1단말을 통해 고객 식별자 정보(ID/PW)를 입력하여 상기 서버로 전송
1220
서버는 상기 고객 제1단말로부터 수신된 고객 식별자 정보(ID/PW)에 대응하는 고객 제2단말(무선단말) 정보를 상기 저장매체로부터 추출
1225
제2단말 정보 추출 ?
아니오
1230
1235
서버에서 상기 고객 제1단말로 고객인증 처리 불가 메시지 전송
정보 등록 프로세스 ?
예
1240
1245
아니오
1250
예
서버에서 상기 추출된 제2단말 정보(무선단말번호)를 참조하여, 상기 고객 제2단말로 고객 인증 정보 요청 메시지 전송
1255
종 료

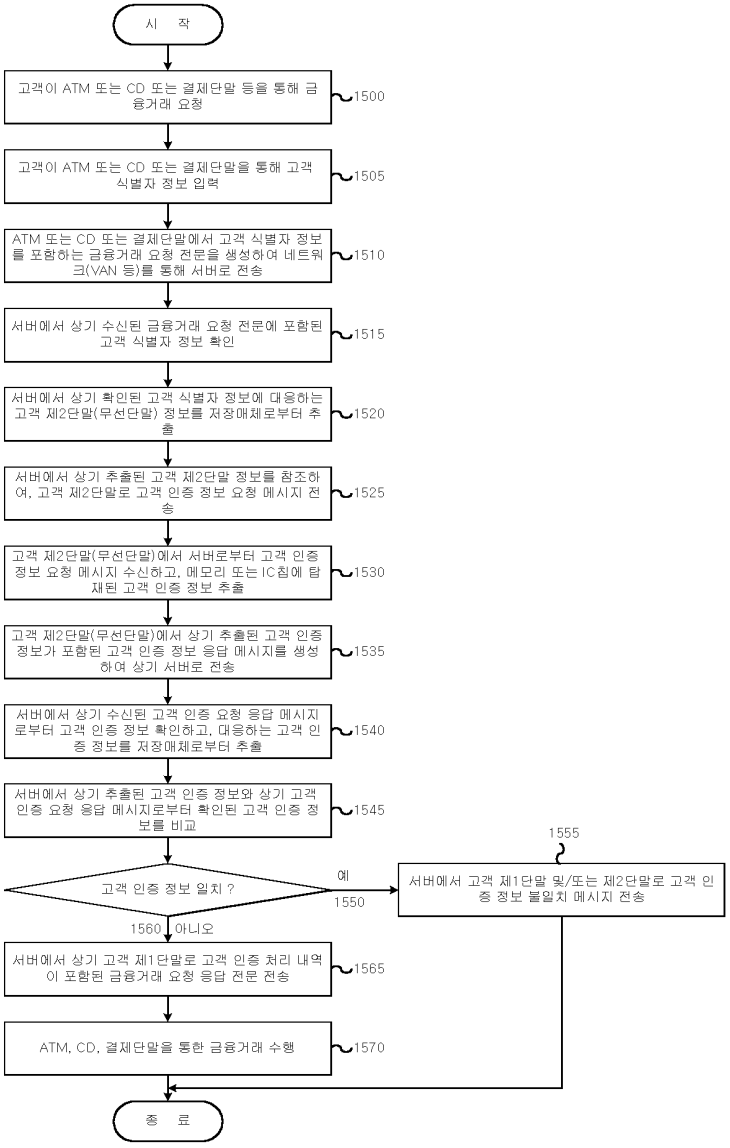
도면13


시 작
고객 제2단말(무선단말)에서 서버로부터 고객 인증 정보 요청 메시지 수신
1300
고객 제2단말(무선단말)에 탑재된 IC칩에 접근하기 위한 PIN 정보 입력
1305
PIN 인증 ?
예
1310
1315
고객 제2단말(무선단말)에서 PIN입력 실패 메시지 출력
1330 아니오
고객 제2단말(무선단말)에서 IC칩에 저장된 적어도 하나 이상의 고객 인증 정보 출력
1335
PIN정보 재입력 ?
예
1320
1325 아니오
상기 서버로부터 수신된 고객 인증 정보 요청 메시지에 대응하여 전송할 고객 인증 정보 선택
1340
고객 제2단말(무선단말)에서 상기 수신된 고객 인증 정보 요청 메시지에 포함된 상기 서버 접속 정보 확인
1345
고객 제2단말(무선단말)에서 상기 확인된 서버 접속 정보를 참조하여, 상기 선택된 고객 인증 정보를 전송
1350
고객 제2단말에서 상기 고객 인증 정보 전송 내역을 출력
1355
종 료

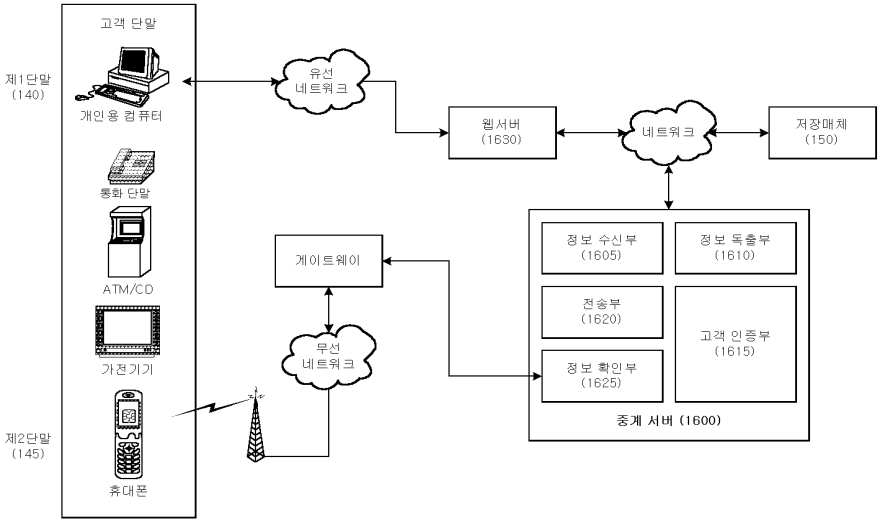
도면14


시 작
서버에서 고객 제2단말(무선단말)로부터 고객 인증 정보를 포함하는 고객 인증 요청 응답 메시지 수신
1400
서버에서 상기 수신된 고객 인증 요청 응답 메시지로부터 고객 인증 정보 확인
1405
서버에서 저장매체로부터 상기 고객의 고객 인증 정보 독출
1410
서버에서 상기 독출된 고객 인증 정보와 상기 고객 인증 요청 응답 메시지로부터 확인된 고객 인증 정보를 비교
1415
고객 인증 정보 일치 ?
예
1420
1425
서버에서 고객 제1단말 및/또는 제2단말로 고객 인증 정보 불일치 메시지 전송
1430
아니오
서버에서 상기 고객 제1단말 및/또는 제2단말로 고객 인증 처리 내역 전송
1435
인증 처리 수행에 따른, 고객의 접속허가 및/또는 컨텐츠 이용
1440
종 료

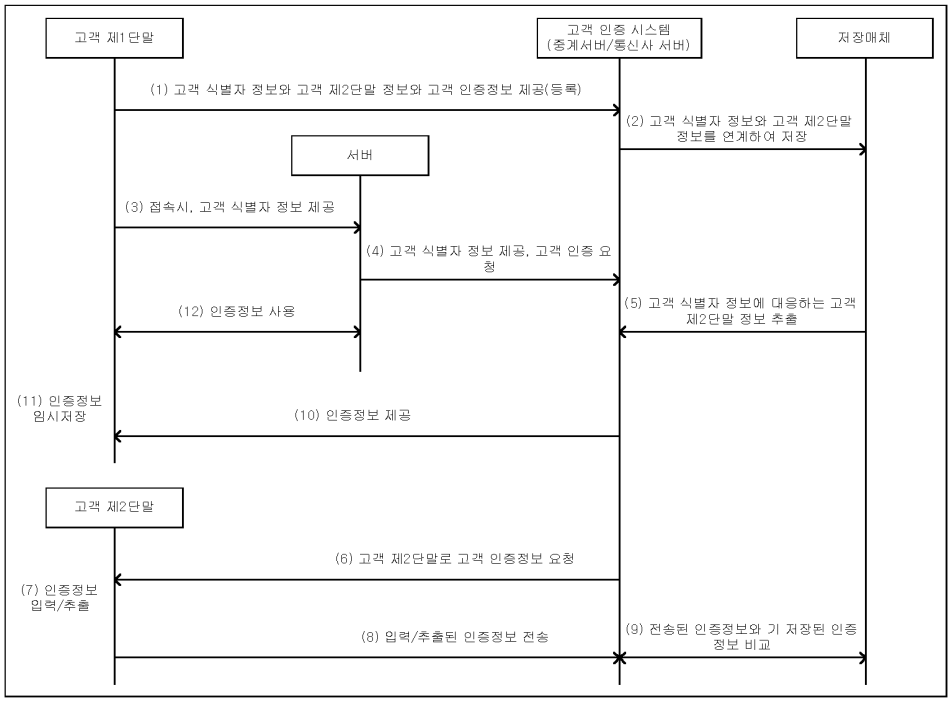
도면15


시 작
고객이 ATM 또는 CD 또는 결제단말 등을 통해 금융거래 요청
1500
고객이 ATM 또는 CD 또는 결제단말을 통해 고객 식별자 정보 입력
1505
ATM 또는 CD 또는 결제단말에서 고객 식별자 정보를 포함하는 금융거래 요청 전문을 생성하여 네트워크(VAN 등)를 통해 서버로 전송
1510
서버에서 상기 수신된 금융거래 요청 전문에 포함된 고객 식별자 정보 확인
1515
서버에서 상기 확인된 고객 식별자 정보에 대응하는 고객 제2단말(무선단말) 정보를 저장매체로부터 추출
1520
서버에서 상기 추출된 고객 제2단말 정보를 참조하여, 고객 제2단말로 고객 인증 정보 요청 메시지 전송
1525
고객 제2단말(무선단말)에서 서버로부터 고객 인증 정보 요청 메시지 수신하고, 메모리 또는 IC칩에 탑재된 고객 인증 정보 추출
1530
고객 제2단말(무선단말)에서 상기 추출된 고객 인증 정보가 포함된 고객 인증 정보 응답 메시지를 생성하여 상기 서버로 전송
1535
서버에서 상기 수신된 고객 인증 요청 응답 메시지로부터 고객 인증 정보 확인하고, 대응하는 고객 인증 정보를 저장매체로부터 추출
1540
서버에서 상기 추출된 고객 인증 정보와 상기 고객 인증 요청 응답 메시지로부터 확인된 고객 인증 정보를 비교
1545
고객 인증 정보 일치 ?
예
1550
1555
서버에서 고객 제1단말 및/또는 제2단말로 고객 인증 정보 불일치 메시지 전송
1560
아니오
서버에서 상기 고객 제1단말로 고객 인증 처리 내역이 포함된 금융거래 요청 응답 전문 전송
1565
ATM, CD, 결제단말을 통한 금융거래 수행
1570
종 료

도면16


고객 단말
제1단말
(140)
개인용 컴퓨터
통화 단말
ATM/CD
가전기기
제2단말
(145)
휴대폰
유선
네트워크
무선
네트워크
게이트웨이
웹서버
(1630)
네트워크
저장매체
(150)
정보 수신부
(1605)
정보 독출부
(1610)
전송부
(1620)
고객 인증부
(1615)
정보 확인부
(1625)
중계 서버 (1600)

도면17


고객 제1단말
고객 인증 시스템
(중계서버/통신사 서버)
저장매체
(1) 고객 식별자 정보와 고객 제2단말 정보와 고객 인증정보 제공(등록)
(2) 고객 식별자 정보와 고객 제2단말 정보를 연계하여 저장
서버
(3) 접속시, 고객 식별자 정보 제공
(4) 고객 식별자 정보 제공, 고객 인증 요청
(5) 고객 식별자 정보에 대응하는 고객 제2단말 정보 추출
(12) 인증정보 사용
(11) 인증정보 임시저장
(10) 인증정보 제공
고객 제2단말
(6) 고객 제2단말로 고객 인증정보 요청
(7) 인증정보 입력/추출
(8) 입력/추출된 인증정보 전송
(9) 전송된 인증정보와 기 저장된 인증정보 비교