명세서

발명의 명칭: E-Business 거래에서의 전화인증방법, 그리고 E-Business 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체

기술분야

[1] 본 발명은 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법, 그리고 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체에 관한 것으로, 보다 구체적으로는, 종래의 전자상거래 또는 이체와 같은 전자금융거래에서 사용되는 공인인증서의 기능을 전화인증을 통해 대체하도록 하기 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법, 그리고 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체에 관한 것이다.

배경기술

[2] 인터넷상에서의 본인 확인은 일반적으로 주민등록번호를 이용한 실명인증이 이용되었다. 그러나 주민등록번호를 이용한 실명인증은 주민등록번호의 유출의 위험이 존재하여 최근에는 주민등록번호를 대체하는 개인식별번호인 아이핀(I-PIN)이 이용되고 있다.

[3] 인터넷상에서의 금융거래와 같은 전자거래분야에서는 현재 거래 당사자가 본인인지에 대한 본인확인 기능뿐만 아니라, 보안성을 제고시키기 위한 방안으로 이체비밀번호, 계좌비밀번호 등 다양한 비밀번호를 널리 사용하고 있다. 이와 더불어, 전자서명법상 법적 효력을 지닌 인증 수단으로 공인인증서 사용이 일반화되었으며, 최근에는 전자거래마다 비밀번호가 변경되는 일회성 비밀번호인 OTP(One-Time-Password)의 사용이 증가하고 있는 추세이다.

[4] 이러한 종래의 인증방법은, 사용자 단말이 통신망을 경유하여 서비스 제공 서버에 전자거래를 요청하고, 추가로 공인인증 서버에 저장되어 있던 공인인증서 또는 OTP 정보에 상응하는 정보를 제공함으로써 본인 인증이 이루어지는 방식을 취하고 있다.

[5] 그러나, 기술적인 측면에서 메모리 해킹과 같은 해킹 기술이 고도화되면서 공인인증서 및 OTP에 대한 보안 취약성이 사회적으로 문제가 되고 있고, 인증이 일방향이므로 전자거래 수행이 사용자 본인에 의해 수행된 것이 아니라는 부인(否認)의 가능성이 존재하는 문제가 있다.

[6] 이러한 문제를 해결하기 위해 일부에서는 공인인증서 및 OTP에 의한 인증과는

별도로 별도의 콜센터에서 사용자가 지정한 모바일단말 또는 유선단말로 전화를 걸어서 거래의 진위여부를 확인하는 투트랙(Two-Track) 보안 방식이 사용되고 있다. 보다 구체적으로, 이러한 투트랙 보안 방식은 주로 온라인 게임과 같이 특정 계정으로 아이템에 대한 모집이 가능한 경우에 해킹을 피하기 위해서 사용자들이 대거 활용하고 있으며, 게임을 로그인할 때 단순히 아이디/비밀번호를 넣고 마는 것이 아니라, 아이디/비밀번호 넣고 로그인 요청을 하면, 사용자에 의해 설정된 모바일단말 또는 유선단말로 콜센터에 의해 전화가 걸려와서 확인절차를 갖고 사용자가 승인해야 비로소 로그인이 완료되는 것으로 알고리즘화 된다.

[7] 이에 따라 해당 기술분야에 있어서는 종래의 투트랙 보안에 있어서 전화를 통해 확인을 하는 것이 단순히 보충적인 보안수단으로 제약을 극복함으로써, 향후 상술한 공인인증서에 대한 보안의 문제점으로 인해 공인인증서를 대체할 수 있는 수단으로까지 사용할 수 있도록 하기 위한 기술 개발이 요구되고 있는 실정이다.

발명의 상세한 설명

기술적 과제

[8] 본 발명은 상기의 문제점을 해결하기 위한 것으로, 사용자가 지정한 전화인증용 단말에 대한 전화를 통해 전자상거래 및 전자금융거래 등을 모두 포함하는 E-Business 거래에 대한 진위 여부를 확인하도록 하기 위한 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법, 그리고 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체를 제공하기 위한 것이다.

[9] 또한, 본 발명은 사용자와 E-Business 거래를 수행하는 기관 이외의 제 3 자에 해당하는 인증 관련 기관에 E-Business 거래에 대한 부인 방지 정보를 저장하여 기존의 공인인증센터 또는 OTP센터의 역할이 수행되도록 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법, 그리고 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체를 제공하기 위한 것이다.

[10] 또한, 본 발명은 E-Business 거래에 대한 부인 방지 기능뿐만 아니라, 인증정보에 대한 재사용 방지, 인증정보 생성 값 유출 방지, 중간자 공격에 대응하는 기능, 데이터 세션에 대한 가로채기를 방지하도록 하기 위한 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 신뢰기관과의 연계를

통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법, 그리고 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체를 제공하기 위한 것이다.

[11] 그러나 본 발명의 목적들은 상기에 언급된 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

[12] 상기의 목적을 달성하기 위해 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법은, 전화인증요청 단말이, 전화인증서암호(PIN 번호)를 IP망과 연결된 E-Business 서버를 통해 TTP 서버로 전송하여 저장하도록 하여 상기 전화인증서암호(PIN 번호)를 등록하는 제 1 단계; 상기 TTP 서버가 상기 전화인증요청 단말과 상기 E-Business 서버 간의 E-Business 거래에 따라 상기 E-Business 서버로부터 E-Business 내역 정보와, 상기 전화인증요청 단말로부터 상기 E-Business 서버를 거쳐 확인을 위해 다시 입력된 전화인증서암호(PIN 번호)를 수신하여 저장된 전화인증서암호(PIN 번호)와 동일하다고 판단하는 제 2 단계; 상기 TTP 서버가 상기 E-Business 내역 정보와 상기 다시 입력된 전화인증서암호(PIN 번호)를 결합한 데이터를 암호화하여 저장하는 제 3 단계; 및 상기 E-Business 서버가 상기 전화인증요청 단말로부터 수신된 승인전화번호에 해당하는 전화인증용 단말에 대한 전화 승인 요청을 IVR 서버로 전송하여 전화 승인이 수행되도록 하는 제 4 단계; 를 포함한다.

[13] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법은, 상기 제 1 단계 이전에, 상기 전화인증요청 단말이 사용자의 요청에 따라 상기 IP망을 통해 상기 E-Business 서버에 대한 로그인을 수행하는 단계; 상기 전화인증요청 단말이 상기 IP망을 통해 상기 E-Business 서버로 상기 사용자가 소지한 상기 전화인증용 단말을 이용한 전화 인증 서비스를 신청하는 단계; 및 상기 E-Business 서버가 상기 IP망을 통해 상기 전화인증요청 단말로 전화 인증 서비스 등록 요청을 전송하는 단계; 가 더 수행되는 것이 바람직하다.

[14] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법에 있어서, 상기 제 1 단계는, 상기 전화인증요청 단말이 상기 사용자에 의해 상기 전화인증서암호(PIN 번호) 뿐만 아니라, 상기 전화인증용 단말의 전화번호에 해당하는 상기 승인전화번호, 거래승인번호(이체승인번호)의 입력에 따라, 상기 승인전화번호, 상기

전화인증서암호(PIN 번호), 상기 거래승인번호(이체승인번호)를 상기 IP망을 통해 상기 E-Business 서버로 전송하면, 상기 E-Business 서버가 전용선(L1)을 통해 상기 전화인증서암호(PIN 번호)를 상기 TTP 서버로 전송하여 저장하도록 하는 것을 특징으로 한다.

[15] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법은, 상기 제 1 단계와 상기 제 2 단계 사이에, 상기 E-Business 서버가 상기 승인전화번호, 상기 전화인증서암호(PIN번호), 그리고 상기 거래승인번호(이체승인번호)를 상기 IVR 서버와 연결된 전용선(L2)을 통해 상기 IVR 서버로 전송함과 동시에, 상기 IVR 서버로 상기 승인전화번호에 해당하는 상기 전화인증용 단말로 전화 인증 서비스를 위한 가입 전화를 요청하는 제 1-1 단계; 가 더 수행되는 것이 바람직하다.

[16] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법은, 상기 제 1 단계와 상기 제 2 단계 사이에 상기 제 1-1 단계 이후에 수행되는, 상기 IVR 서버가 상기 E-Business 서버로부터 수신된 상기 전화인증서암호(PIN번호) 및 상기 거래승인번호(이체승인번호)를 저장하는 제 1-2 단계; 가 더 수행되는 것이 바람직하다.

[17] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법은, 상기 제 1 단계와 상기 제 2 단계 사이에 상기 제 1-2 단계 이후에 수행되는, 상기 IVR 서버가 상기 승인전화번호에 해당하는 상기 전화인증용 단말로 유무선 전화망을 통해 전화 인증 서비스 가입 안내를 음성데이터로 전송하는 제 1-3 단계; 가 더 수행되는 것이 바람직하다.

[18] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법은, 상기 제 1 단계와 상기 제 2 단계 사이에 상기 제 1-3 단계 이후에 수행되는, 상기 전화인증용 단말이 상기 사용자에 의해 전화 인증 서비스 가입 확인을 위해 상기 전화인증서암호(PIN 번호) 및 상기 거래승인번호(이체승인번호)에 대한 동일한 입력을 받은 뒤, 입력받은 전화인증서암호(PIN 번호) 및 거래승인번호(이체승인번호)를 유무선 전화망을 통해 상기 IVR 서버로 반환하는 제 1-4 단계; 가 더 수행되는 것이 바람직하다.

[19] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법은, 상기 제 1 단계와 상기 제 2 단계 사이에 상기 제 1-4 단계 이후에 수행되는, 상기 IVR 서버가 상기 전화인증용 단말로부터 수신된 전화인증서암호(PIN 번호)와 상기 1-2 단계에서 저장된 전화인증서암호(PIN 번호)가 동일함을 확인하고, 상기 전화인증용 단말로부터 수신된

거래승인번호(이체승인번호)와 상기 1-2 단계에서 저장된 거래승인번호(이체승인번호)가 동일함을 확인한 뒤, 전화 인증 서비스 가입 완료 메시지를 상기 전용선(L2)을 통해 상기 E-Business 서버로 통지하여 전화 인증 서비스 신청 과정을 종료하는 제 1-5 단계; 가 더 수행되는 것이 바람직하다.

[20] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법에 있어서, 상기 제 2 단계는, 상기 전화인증요청 단말이 상기 IP망을 통해 상기 E-Business 서버와 데이터 송수신을 통해 상기 E-Business 거래를 수행하는 제 2-1 단계; 상기 전화인증요청 단말이 상기 사용자에 의해 상기 제 1 단계에서 입력받은 동일한 전화인증서암호(PIN 번호)를 다시 입력받아 상기 IP망을 통해 상기 E-Business 서버로 전송하는 제 2-2 단계; 상기 E-Business 서버가 상기 E-Business 내역 정보와, 상기 제 2-2 단계에서 수신된 전화인증서암호(PIN 번호)를 상기 전용선(L1)을 통해 상기 TTP 서버로 전송하는 제 2-3 단계; 및 상기 TTP 서버가 상기 제 2-3 단계에서 수신된 전화인증서암호(PIN 번호)와 상기 제 1 단계에서 저장된 전화인증서암호(PIN 번호)를 비교하여 확인하여 동일한지 여부를 판단하는 제 2-4 단계; 를 포함하는 것을 특징으로 한다.

[21] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법에 있어서, 상기 제 3 단계는, 상기 TTP 서버가 상기 E-Business 내역 정보와 상기 제 2-3 단계에서 수신된 전화인증서암호(PIN 번호)와 결합한 데이터를 암호화하여 거래 부인 방지 정보를 생성하여 저장하며, 상기 E-Business 내역 정보에 대한 저장은 수행하지 않는 것이 바람직하다.

[22] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법은, 상기 제 3 단계와 상기 제 4 단계 사이에, 상기 TTP 서버가 상기 전용선(L1)을 통해 상기 E-Business 서버로 전화인증서암호(PIN 번호)에 대한 확인 결과를 전송하는 단계; 가 더 수행되는 것이 바람직하다.

[23] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법에 있어서, 상기 제 4 단계는, 상기 E-Business 서버가 상기 E-Business 내역 정보를 상기 전용선(L2)을 통해 상기 IVR 서버로 전송하며, 이와 동시에 전화 승인 요청을 상기 IVR 서버로 전송하는 제 4-1 단계; 상기 IVR 서버가 유무선전화망을 통해 음성데이터에 의한 상기 E-Business 내역 정보를 포함하는 전화 승인 요청 안내를 상기 전화인증용 단말로 전송하는 제 4-2 단계; 상기 전화인증용 단말이 상기 제 1 단계에서 상기 전화인증요청 단말로 입력된 거래승인번호(이체승인번호)와 동일한 거래승인번호(이체승인번호)를 상기 사용자로부터 입력받아 상기 유무선전화망을 통해 상기 IVR 서버로 전송하는

제 4-3 단계; 상기 IVR 서버가 상기 전화인증용 단말로부터 수신된 거래승인번호(이체승인번호)와 상기 제 1-2 단계에서 저장된 거래승인번호(이체승인번호)를 비교하여 동일함을 확인한 뒤, 전화 승인 결과를 생성하는 제 4-4 단계; 상기 IVR 서버가 상기 전화 승인 결과를 상기 전용선(L2)을 통해 상기 E-Business 서버로 전송하는 제 4-5 단계; 및 상기 E-Business 서버가 상기 E-Business 거래를 완료한 뒤, 상기 전화 승인 결과를 상기 IP망을 통해 상기 전화인증요청 단말로 전송하는 제 4-6 단계; 를 포함하는 것을 특징으로 한다.

[24] 상기의 목적을 달성하기 위해 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체는 전화인증요청 단말로부터 전화인증서암호(PIN 번호)를 IP망을 통해 수신하여 TTP 서버로 전송하도록 송수신부를 제어하여, 상기 TTP 서버에 상기 전화인증서암호(PIN 번호)를 등록하도록 하는 전화 인증 신청수단; 상기 전화인증요청 단말과 E-Business 거래를 수행하도록 하는 E-business 거래수단; 상기 TTP 서버로 E-Business 내역 정보와, 상기 전화인증요청 단말로부터 상기 E-Business 서버를 거쳐 확인을 위해 다시 입력된 전화인증서암호(PIN 번호)를 전송하도록 상기 송수신부를 제어하여 상기 TTP 서버에 의해 상기 E-Business 내역 정보와 전화인증서암호(PIN 번호)를 결합한 데이터를 암호화하여 저장하도록 하는 E-business 거래 부인 방지수단; 및 상기 전화인증요청 단말로부터 수신된 승인전화번호에 해당하는 전화인증용 단말에 대한 전화 승인 요청을 상기 IVR 서버로 전송하도록 상기 송수신부를 제어하여 상기 전화인증용 단말에 대한 전화 승인이 수행되도록 하는 전화 인증 수행수단; 을 구비하여 이루어진다.

발명의 효과

[25] 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법, 그리고 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체는 사용자가 지정한 전화인증용 단말에 대한 전화를 통해 전자상거래 및 전자금융거래 등을 모두 포함하는 E-Business 거래에 대한 진위 여부를 확인하도록 하는 효과를 제공한다.

[26] 또한, 본 발명의 다른 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법, 그리고 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체는 사용자와 E-Business 거래를 수행하는

기관 이외의 제 3 자에 해당하는 인증 관련 기관에 E-Business 거래에 대한 부인 방지 정보를 저장하여 기존의 공인인증센터 또는 OTP센터의 역할이 수행되도록 하는 효과를 제공한다.

[27] 뿐만 아니라, 본 발명의 다른 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법, 그리고 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체는 E-Business 거래에 대한 부인 방지 기능뿐만 아니라, 인증정보에 대한 재사용 방지, 인증정보 생성 값 유출 방지, 중간자 공격에 대응하는 기능, 데이터 세션에 대한 가로채기를 방지하는 효과를 제공한다.

도면의 간단한 설명

[28] 도 1은 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법이 구현되는 전체 시스템을 나타내는 도면.

[29] 도 2는 도 1의 전화인증용 단말을 이용한 E-Business 거래 인증 시스템에서의 E-Business 서버를 설명하기 위한 도면.

[30] 도 3은 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법 중 전화 인증 서비스 신청 과정을 나타내는 흐름도.

[31] 도 4는 도 3은 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법 중 전화 인증 서비스에 의한 E-Business 거래 과정을 나타내는 흐름도.

[32] 도 5는 도 4에서의 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법 중 E-Business 거래가 이체 거래인 경우 이체거래 수행을 위한 전화인증요청 단말에 의해 수행되는 입력 과정을 구체적으로 나타내는 흐름도.

발명의 실시를 위한 형태

[33] 이하, 첨부된 도면을 참조하여 본 발명의 각 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법, 그리고 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 기록매체에 대하여 설명하기로 한다.

[34] 이하의 실시 예는 본 발명의 이해를 돕기 위한 상세한 설명이며, 본 발명의 권리 범위를 제한하는 것이 아님은 당연할 것이다. 따라서, 본 발명과 동일한 기능을

수행하는 균등한 발명 역시 본 발명의 권리 범위에 속할 것이다.

[35] 또한 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[36] 본 발명의 실시 예에서 “통신”, “통신망”, "인터넷망" 및“네트워크”는 동일한 의미로 사용될 수 있다. 상기 세 용어들은, 파일을 사용자 단말, 다른 사용자들의 단말 및 다운로드 서버 사이에서 송수신할 수 있는 유무선의 근거리 및 광역 데이터 송수신망을 의미한다.

[37] 이하의 설명에서 “서버”란, 사용자들이 접속하여 컨텐츠를 이용하기 위하여 접속하게 되는 서버 컴퓨터를 의미한다. 용량이 작거나 이용자 수가 적은 경우 하나의 서버에 다수의 프로그램이 운영될 수 있다. 또한, 용량이 매우 크거나 실시간 접속 인원 수가 많은 경우, 서버의 기능에 따라서 하나의 시스템 운영을 위한 서버가 하나 이상 존재할 수도 있다.

[38] 그리고 본 명세서에 있어서 "E-Business 거래"는 전자상거래, 인터넷 뱅킹 이체와 같은 전자금융거래, 그리고 온라인 상에서 수행되는 각종 인증(승인) 거래에 적용되는 광범위한 개념으로, 모든 업체의 온라인상의 업무를 수용할 수 있어야 한다.

[39] 도 1은 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법이 구현되는 전체 시스템(이하, 전화인증용 단말을 이용한 E-Business 거래 인증 시스템)을 나타내는 도면이다. 도 1을 참조하면, 전화인증용 단말을 이용한 E-Business 거래 인증 시스템은 전화인증요청 단말(10), IP망(20), E-Business 서버(30), TTP(Trusted Third Party) 서버(40), IVR(Interactive Voice Response) 서버(50), 유무선 전화망(60), GW(70), 그리고 전화인증용 단말(80)을 포함한다.

[40] 전화인증요청 단말(10)은 웹 또는 왑 브라우저를 구비하여 E-Business 서버(30)에 접속하여 웹 또는 왑 브라우저를 통해 동일한 사용자가 소지한 전화인증을 위한 전화인증용 단말(80)의 전화번호인 "승인전화번호", "전화인증서암호(Personal Identification Number: 이하, PIN 번호)", 그리고 "거래승인번호(이체승인번호)"을 사용자가 입력할 수 있다.

[41] IP망(20)은 대용량, 장거리 음성 및 데이터 서비스가 가능한 대형 통신망의 고속 기간 망이며, 예컨대, 인터넷(Internet)이 될 수 있다. 또한, IP망은 ALL IP(Internet Protocol) 기반의 고속의 멀티미디어 서비스를 제공하기 위한 차세대 유선 망일 수 있으며, 기존의 IP망(20)에 전용선 및 VPN 회선을 포함하는 광범위한 개념이다.

[42] IP망(20)은 전화인증요청 단말(10), E-Business 서버(30), 그 밖의 시스템 상호

간의 신호 및 데이터를 상호 전달하는 역할을 한다.

[43] 유무선 전화망(60)은 공중교환전화망(PSTN)과 같은 서킷(Circuit)망 또는 서킷망과 패킷(Packet)망을 포함하는 WCDMA망을 포함하는 광범위한 개념의 음성 정보를 전달하기 통신망이다. 한편, 무선 전화망의 예로 WCDMA망을 일예로 들었지만, 3G LTE망, 4G망 등 차세대 이동통신망으로 변경될 수 있음은 주지의 사실이다.

[44] 유무선 전화망(60)은 전화인증용 단말(80), IVR 서버(50), 그 밖의 시스템 상호 간의 신호 및 데이터를 상호 전달하는 역할을 한다.

[45] GW(70)는 게이트웨이로 프로토콜 변환기의 하나이며, 유무선 전화망(60)을 통해 유선 또는 무선으로 접속하는 전화인증용 단말(80) 및 IVR 서버(50)와, IP망(20)을 통해 접속하는 전화인증요청 단말(10) 및 E-Business 서버(30) 상호 간의 데이터 송수신을 가능하게 한다. GW(70)는 왑 또는 웹 게이트웨이(Wap/Web Gateway)로서, IP망(20)과 유무선전화망(60) 상호 간에 액세스(Aceess)하기 위한 프로토콜 스택을 포함할 수 있다.

[46] 전화인증용 단말(80)은 전화인증요청 단말(10)을 소지한 사용자가 전화인증을 위해 지정한 단말로, 유선단말 및 무선단말을 포함하는 광범위한 개념이다. 그러나 일반적으로 현재 많이 사용되고 있는 스마트폰으로 설정하는 것이 바람직하나, 이이 한정되진 않으며, 무선링크를 통해 사용자에게 인터넷 데이터를 포함하는 인터넷 서비스를 제공하는 기기로서, 이는 포괄적인 개념의 휴대기기들일 수 있다. 즉, 일반 유무선 전화, VoIP폰, 핸드폰, 무선단말, PDA(Personal Digital Assistant), GSM(Global System for Mobile)폰, W-CDMA(Wideband CDMA)폰, CDMA-2000폰, MBS(Mobile Broad and System)폰, PMP(Portable Multimedia Player), 핸드헬드 컴퓨터(Handheld Computer)와 같이 멀티미디어 폰 및 멀티미디어 플레이어 등을 포함할 수 있다. 여기서, MBS폰은 현재 논의되고 있는 제 4 세대 시스템에서 사용될 핸드폰일 수 있다.

[47] E-Business 서버(30)는 전자금융거래가 수행되는 은행 서버, 또는 전자상거래 서비스가 수행가능한 웹서버 또는 왑서버일 수 있으며, Application 서버 등 모든 서버 및 장비를 포함한다.

[48] 그리고, TTP 서버(40)는 인증센터이며, 본 발명의 다른 실시예로, TTP 서버(40)에는 ARS 시스템이 연동될 수 있다. 즉, 인증센터에 해당하는 TTP 서버(40)에 ARS 시스템이 형성되며, ARS 시스템은 전화 인증 서비스 신청시 전화인증서암호(Personal Identification Number 번호: 이하, PIN 번호)를 관리하기 위한 목적으로 사용된다.

[49] 한편, E-Business 서버(30), TTP 서버(40) 및 IVR 서버(50)에 대해서는 이하에서 보다 구체적으로 살펴보도록 한다.

[50]

[51] 도 2는 도 1의 전화인증용 단말을 이용한 E-Business 거래 인증 시스템에서의

E-Business 서버(30)를 설명하기 위한 도면이다. 도 2를 참조하면, E-Business 서버(30)는 송수신부(31), 제어부(32), 데이터베이스(33) 그리고 거래인증모듈(34)을 포함한다. 그리고 거래인증모듈(34)은 전화 인증 신청수단(34a), 전화 인증 준비수단(34b), E-business 거래수단(34c), E-business 거래 부인 방지수단(34d), 및 전화 인증 수행수단(34e)을 포함한다. 이하에서는 거래인증모듈(34)의 구성을 중심으로 E-Business 서버(30)에 대해서 구체적으로 살펴보도록 한다.

[52] 전화 인증 신청수단(34a)은 전화인증요청 단말(10)로부터 IP망(20)을 통한 로그인을 수용하도록 송수신부(31)를 제어한다.

[53] 이후, 전화 인증 신청수단(34a)은 전화인증요청 단말(10)로부터 IP망(20)을 통해 전화인증요청 단말(10)의 사용자가 소지한 전화인증용 단말(80)을 이용한 전화 인증 서비스에 대한 신청을 수신하도록 송수신부(31)를 제어한다.

[54] 전화 인증 신청수단(34a)은 IP망(20)을 통해 전화인증요청 단말(10)로 전화 인증 서비스 등록 요청을 전송한 뒤, 전화인증요청 단말(10)로부터 전화인증용 단말(80)의 전화번호에 해당하는 승인전화번호, 전화인증서암호(PIN 번호), 거래승인번호(이체승인번호)를 IP망(20)을 통해 수신하도록 송수신부(31)를 제어한 뒤, 전화인증용 단말(80)의 승인전화번호를 데이터베이스(33)에 저장한다.

[55] 전화 인증 준비수단(34b)은 전화인증서암호(PIN 번호)를 TTP 서버(40)와 연결된 전용선(L1)을 통해 TTP 서버(40)로 전송하도록 송수신부(31)를 제어함으로써, TTP 서버(40)로 전화인증서암호(PIN 번호)가 저장되도록 한다.

[56] 전화 인증 준비수단(34b)은 전화 인증 신청수단(34a)에 의해 수신한 승인전화번호, 전화인증서암호(PIN번호), 그리고 거래승인번호(이체승인번호)를 IVR 서버(50)와 연결된 전용선(L2)을 통해 IVR 서버(50)로 전송함과 동시에, IVR 서버(50)로 승인전화번호에 해당하는 전화인증용 단말(80)로 전화 인증 서비스를 위한 가입 전화를 요청하도록 송수신부(31)를 제어함으로써, IVR 서버(50)로 전화인증서암호(PIN번호) 및 거래승인번호(이체승인번호)가 저장되도록 한다.

[57]

[58] 한편, 전화 인증 신청수단(34a) 및 전화 인증 준비수단(34b)에 의한 상술한 일련의 알고리즘에 의해, IVR 서버(50)는 전화 인증 준비수단(34b)으로부터 수신된 승인전화번호에 해당하는 전화인증용 단말(80)로 유무선 전화망(60)을 통해 전화 인증 서비스 가입 안내를 음성데이터로 전송한다. 이에 따라, 전화인증용 단말(80)은 사용자에 의해 입력된 전화인증서암호(PIN 번호), 거래승인번호(이체승인번호)에 대한 동일한 입력을 받은 뒤, 동일하게 다시 입력받은 전화인증서암호(PIN 번호), 거래승인번호(이체승인번호)를 유무선 전화망(60)을 통해 IVR 서버(50)로 반환한다. 그 후, IVR 서버(50)는 전화 인증 준비수단(34b)으로부터 수신된 전화인증서암호(PIN 번호)와 전화인증용

단말(80)로부터 수신된 전화인증서암호(PIN 번호)가 동일함을 확인하고, 전화 인증 준비수단(34b)으로부터 수신된 거래승인번호(이체승인번호)와 전화인증용 단말(80)로부터 수신된 거래승인번호(이체승인번호)가 동일함을 확인한 뒤, 전화 인증 서비스 가입 완료 메시지를 전용선(L2)을 통해 E-Business 서버(30)로 통지함으로써, 전화 인증 서비스 신청 과정을 종료한다.

[59]

[60] 다시, E-Business 서버(30)의 구성에 대해 살펴보면, E-business 거래수단(34c)은 IP망(20)과 연결된 전화인증요청 단말(10)과 데이터 송수신을 통해 E-Business 거래를 수행하도록 송수신부(31)를 제어한다.

[61] E-business 거래 부인 방지수단(34d)은 전화인증요청 단말(10)의 사용자가 전화 인증 서비스 신청 과정에서 입력한 동일한 전화인증서암호(PIN 번호)에 대한 재입력에 따라 전화인증요청 단말(10)로부터 IP망(20)을 통해 수신하도록 송수신부(31)를 제어한다.

[62] E-business 거래 부인 방지수단(34d)은 E-Business 내역 정보와, 재입력된 전화인증서암호(PIN 번호)를 전용선(L1)을 통해 TTP 서버(40)로 전송하도록 송수신부(31)를 제어함으로써, TTP 서버(40)에 의해 E-Business 내역 정보와 전화인증서암호(PIN 번호)를 결합한 데이터의 암호화에 따른 거래 부인 방지 정보가 생성되도록 한다. 여기서 거래 부인 방지 정보는 종래의 공인인증서의 주요 기능인 전자상거래 또는 전자금융거래에 대한 사용자가 거래 자체를 부인하는 것의 예방과 동일한 기능을 위해 본 발명에서 사용된다. 요약하자면, TTP 서버(40)는 전화인증서암호(PIN 번호)를 이용하여 E-Business 내역 정보를 포함하는 E-Business 거래에 대한 거래 부인 방지 정보를 생성하여 저장하나, TTP 서버(40)에서도 E-Business 내역 정보 자체만으로는 거래 내역에 대한 확인은 불가능한 특징으로 갖는다. 부인 방지 정보의 인자값으로, 거래일시(분초 포함), 출금계좌번호, 이체금액, 입금계좌번호, 입금은행코드. 받는사람을 포함하는 것이 바람직하다.

[63] 전화 인증 수행수단(34e)은 TTP 서버(40)로부터 전용선(L1)을 통해 전화인증서암호(PIN 번호)에 대한 확인 결과를 수신한 뒤, E-Business 내역 정보를 전용선(L2)을 통해 IVR 서버(50)로 전송하며, 이와 동시에 전화 승인 요청을 IVR 서버(50)로 전송하도록 송수신부(31)를 제어한다. 이에 따라, IVR 서버(50)는 유무선전화망(60)을 통해 음성데이터에 의한 E-Business 내역 정보를 포함하는 전화 승인 요청 안내를 전화인증용 단말(80)로 전송한다. 이후, 전화인증용 단말(80)은 전화 인증 서비스 신청시 전화인증요청 단말(10)로 입력된 거래승인번호(이체승인번호)와 동일한 거래승인번호(이체승인번호)를 사용자로부터 입력받아 유무선전화망(60)을 통해 IVR 서버(50)로 전송하면, IVR 서버(50)는 전화 승인 결과를 생성하여 E-Business 서버(30)로 전송한다.

[64] 전화 인증 수행수단(34e)은 전화 승인 결과를 수신하여 E-Business 거래를 완료한 뒤(S42), 전화 승인 결과를 IP망(20)을 통해 전화인증요청 단말(10)로

전송하도록 송수신부(31)를 제어한다.

[65]

[66] 도 3은 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법 중 전화 인증 서비스 신청 과정을 나타내는 흐름도이다. 도 1 내지 도 3을 참조하면, 전화인증요청 단말(10)은 사용자의 요청에 따라 IP망(20)을 통해 E-Business 서버(30)에 대한 로그인을 수행한다(S11).

[67] 단계(S11) 이후, 전화인증요청 단말(10)은 IP망(20)을 통해 E-Business 서버(30)로 사용자가 소지한 전화인증용 단말(80)을 이용한 전화 인증 서비스를 신청한다(S12).

[68] 단계(S12) 이후, E-Business 서버(30)는 IP망(20)을 통해 전화인증요청 단말(10)로 전화 인증 서비스 등록 요청을 전송한다(S13).

[69] 단계(S13) 이후, 전화인증요청 단말(10)은 사용자가 소지한 전화인증용 단말(80)의 전화번호에 해당하는 승인전화번호, 전화인증서암호(PIN 번호), 거래승인번호(이체승인번호)를 입력하면(S14), 입력된 승인전화번호, 전화인증서암호(PIN 번호), 거래승인번호(이체승인번호)를 IP망(20)을 통해 E-Business 서버(30)로 전송한다(S15).

[70] 단계(S15) 이후, E-Business 서버(30)는 사용자가 지정한 전화인증용 단말(80)의 승인전화번호를 데이터베이스(33)에 저장한다(S16).

[71] 단계(S16) 이후, E-Business 서버(30)는 단계(S15)에서 수신한 전화인증서암호(PIN 번호)를 TTP 서버(40)와 연결된 전용선(L1)을 통해 TTP 서버(40)로 전송한다(S17).

[72] 이에 따라, TTP 서버(40)는 전화인증서암호(PIN 번호)를 저장한다(S18).

[73] 단계(S18) 이후, E-Business 서버(30)는 단계(S15)에서 수신한 승인전화번호, 전화인증서암호(PIN번호), 그리고 거래승인번호(이체승인번호)를 IVR 서버(50)와 연결된 전용선(L2)을 통해 IVR 서버(50)로 전송함과 동시에, IVR 서버(50)로 승인전화번호에 해당하는 전화인증용 단말(80)로 전화 인증 서비스를 위한 가입 전화를 요청한다(S19).

[74] 단계(S19) 이후, IVR 서버(50)는 단계(S19)에서 E-Business 서버(30)로부터 수신된 전화인증서암호(PIN번호) 및 거래승인번호(이체승인번호)를 저장한다(S20).

[75] 단계(S20) 이후, IVR 서버(50)는 단계(S19)에서 수신된 승인전화번호에 해당하는 전화인증용 단말(80)로 유무선 전화망(60)을 통해 전화 인증 서비스 가입 안내를 음성데이터로 전송한다(S21).

[76] 단계(S21) 이후, 전화인증용 단말(80)은 사용자에 의해 단계(S10)에서 입력된 전화인증서암호(PIN 번호), 거래승인번호(이체승인번호)에 대한 동일한 입력을 받은 뒤(S22), 단계(S22)에서 입력받은 전화인증서암호(PIN 번호), 거래승인번호(이체승인번호)를 유무선 전화망(60)을 통해 IVR 서버(50)로

반환한다(S23).

[77] 이에 따라, IVR 서버(50)는 단계(S19)에서 수신된 전화인증서암호(PIN 번호)와 단계(S23)에서 수신된 전화인증서암호(PIN 번호)가 동일함을 확인하고, 단계(S19)에서 수신된 거래승인번호(이체승인번호)와 단계(S23)에서 수신된 거래승인번호(이체승인번호)가 동일함을 확인한 뒤, 전화 인증 서비스 가입 완료 메시지를 전용선(L2)을 통해 E-Business 서버(30)로 통지함으로써, 전화 인증 서비스 신청 과정을 종료한다.

[78]

[79] 도 4는 도 3은 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법 중 전화 인증 서비스에 의한 E-Business 거래 과정을 나타내는 흐름도이다. 도 1 내지 도 4를 참조하면, 전화인증요청 단말(10)은 IP망(20)을 통해 E-Business 서버(30)와 데이터 송수신을 통해 E-Business 거래를 수행한다(S31)

[80] 단계(S31) 이후, 전화인증요청 단말(10)은 사용자가 도 3의 전화 인증 서비스 신청 과정에서 입력한 동일한 전화인증서암호(PIN 번호)를 입력받아 IP망(20)을 통해 E-Business 서버(30)로 전송한다(S32).

[81] 단계(S32) 이후, E-Business 서버(30)는 E-Business 내역 정보와, 단계(S32)에서 수신된 전화인증서암호(PIN 번호)를 전용선(L1)을 통해 TTP 서버(40)로 전송한다(S33).

[82] 단계(S33) 이후, TTP 서버(40)는 단계(S33)에서 수신된 전화인증서암호(PIN 번호)와 단계(S18)에서 저장된 전화인증서암호(PIN 번호)를 비교하여 확인한 뒤, 동일한 경우, E-Business 내역 정보와 전화인증서암호(PIN 번호)와 결합한 데이터를 암호화하여 거래 부인 방지 정보를 생성하여 저장한다(S34). 여기서 거래 부인 방지 정보는 종래의 공인인증서의 주요 기능인 전자상거래 또는 전자금융거래에 대한 사용자가 거래 자체를 부인하는 것의 예방과 동일한 기능을 위해 본 발명에서 사용된다. 그리고, TTP 서버(40)는 E-Business 내역 정보와 전화인증서암호(PIN 번호)와 결합한 데이터를 암호화하여 저장시 E-Business에 대한 거래내역을 나타내는 E-Business 내역 정보에 대한 저장을 하진 않는다.

[83] 보다 구체적으로, TTP 서버(40)는 추후에 사용자가 E-Business 거래를 부인하면 E-Business 내역 정보와 전화인증서암호(PIN 번호)가 결합되어 암호화된 데이터를 복호화한 뒤, 분석을 통해 사용자가 전화인증서암호(PIN 번호)을 입력한 것을 부정할 수 없도록 한다. 이때 TTP 서버(40)에는 E-Business에 대한 거래내역인 E-Business 내역 정보가 저장되어 있지 않으므로 자체적으로는 암호화된 데이터를 생성할 수는 없다.

[84]

[85] 이와 같이 TTP 서버(40)는 사용자의 전화인증서암호(PIN 번호), 그리고

E-Business 내역 정보와 사용자의 전화인증서암호(PIN 번호)를 암호화한 데이터를 보관함으로써, 사용자의 액션과 정보의 분산이 가능하도록 한다.

[86] 요약하자면, TTP 서버(40)는 전화인증서암호(PIN 번호)를 이용하여 E-Business 내역 정보를 포함하는 E-Business 거래에 대한 거래 부인 방지 정보를 생성하여 저장하나, TTP 서버(40)에서도 E-Business 내역 정보 자체만으로는 거래 내역에 대한 확인은 불가능한 특징으로 갖는다.

[87] 단계(S34) 이후, TTP 서버(40)는 전용선(L1)을 통해 E-Business 서버(30)로 전화인증서암호(PIN 번호)에 대한 확인 결과를 전송한다(S35).

[88] 단계(S35) 이후, E-Business 서버(30)는 단계(S31)에 따른 E-Business 내역 정보를 전용선(L2)을 통해 IVR 서버(50)로 전송하며, 이와 동시에 전화 승인 요청을 IVR 서버(50)로 전송한다(S36).

[89] 단계(S36) 이후, IVR 서버(50)는 유무선전화망(60)을 통해 음성데이터에 의한 단계(S36)에 따라 수신된 E-Business 내역 정보를 포함하는 전화 승인 요청 안내를 전화인증용 단말(80)로 전송한다(S37).

[90] 이에 따라, 전화인증용 단말(80)은 도 3의 단계(S14)에서 전화인증요청 단말(10)로 입력된 거래승인번호(이체승인번호)와 동일한 거래승인번호(이체승인번호)를 사용자로부터 입력받은 뒤(S38), 단계(S38)에서 입력된 거래승인번호(이체승인번호)를 유무선전화망(60)을 통해 IVR 서버(50)로 전송한다(S39).

[91] 단계(S39) 이후, IVR 서버(50)는 전화인증용 단말(80)로부터 수신된 거래승인번호(이체승인번호)와 도 3의 단계(S20)에서 저장된 거래승인번호(이체승인번호)를 비교하여 동일함을 확인한 뒤, 전화 승인 결과를 생성한다(S40).

[92] 단계(S40) 이후, IVR 서버(50)는 단계(S40)에서 생성된 전화 승인 결과를 전용선(L2)을 통해 E-Business 서버(30)로 전송한다(S41).

[93] 단계(S41) 이후, E-Business 서버(30)는 E-Business 거래를 완료한 뒤(S42), 전화 승인 결과를 IP망(20)을 통해 전화인증요청 단말(10)로 전송한다(S43).

[94]

[95] 도 5는 도 4에서의 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법 중 단계(S31) 및 단계(S32)에 의한 E-Business 거래가 이체 거래인 경우 이체거래 수행을 위한 전화인증요청 단말(10)에 의해 수행되는 입력 과정을 구체적으로 나타내는 흐름도이다. 도 1 내지 도 5를 참조하면, 전화인증요청 단말(10)은 사용자의 요청에 의해 IP망(20)을 통해 E-Business 서버(30)에 접속(Access)한 뒤, 사용자에 의해 입력된 아이디(ID) 및 패스워드(PW) 입력에 의한 사용자의 로그인을 E-Business 서버(30)로 수행한다(S51).

[96] 단계(S51)에 따른 로그인 이후, 전화인증요청 단말(10)은 IP망(20)을 통해

E-Business 서버(30)와의 데이터 송수신을 통해 이체 예비거래를 수행한다(S52). 여기서 본 발명의 일 실시예로 이체 예비거래는 전화인증요청 단말(10)은 E-Business 서버(30)로의 데이터 전송에 의해 세부적으로 6가지의 단계를 거쳐 수행된다. 즉, 전화인증요청 단말(10)은 사용자의 입력에 따른 출금계좌번호를 E-Business 서버(30)로 전송한 뒤(S52a), 사용자가 입력하는 출금계좌비밀번호도 전송한다(S52b). 단계(S52b) 이후, 전화인증요청 단말(10)은 사용자의 입력에 따른 이체금액을 E-Business 서버(30)로 전송한 뒤(S52c), 사용자가 입력하는 입금계좌번호도 전송한다(S52d). 단계(S52d) 이후, 전화인증요청 단말(10)은 사용자의 선택 입력에 따른 임금은행을 E-Business 서버(30)로 전송한 뒤(S52e), 사용자가 입력하는 추가이체 또는 이체확인 중 이체확인에 대한 클릭에 따라 이체를 요청하고 있음을 E-Business 서버(30)로 통지한다(S52f).

[97] 단계(S52)에 따른 이체 예비거래가 수행된 이후, 전화인증요청 단말(10)은 IP망(20)을 통해 E-Business 서버(30)와의 데이터 송수신을 통해 이체 본거래를 수행한다(S53). 여기서 본 발명의 일 실시예로 이체 본거래는 전화인증요청 단말(10)이 E-Business 서버(30)로의 데이터 전송에 의한 세부적으로 4가지의 단계를 거쳐 수행된다. 즉, 전화인증요청 단말(10)은 사용자의 입력에 따른 보안카드 비밀번호를 E-Business 서버(30)로 전송한 뒤(S53a), 사용자가 선택 입력하는 승인전화번호도 전송한다(S53b).

[98] 한편, 보안카드 비밀번호 입력을 위해 E-Business 서버(30)는 35개의 지시번호와 난수를 랜덤함수를 통해 생성함으로써, 매 거래시 다른 보안카드 비밀번호를 요구함으로써, "인증정보에 대한 재사용"을 방지할 뿐만 아니라, "인증정보 생성 값 유출"을 방지할 수 있다.

[99] 또한, E-Business 서버(30)는 전화인증요청 단말(10)에 의해 단계(S52b)에서 입력되는 출금계좌비밀번호, 단계(S52d)에서 입력되는 입금계좌번호, 단계(S53a)에서 입력되는 보안카드 비밀번호에 대한 복호화가 불가능하도록 EV SSL(Extended Validation Secure Sockets Layer) 인증서 적용을 통해 보호를 수행함으로써, '중간자 공격에 대응하는 기능'을 수행한다.

[100] 뿐만 아니라, 상술한 EV SSL(Extended Validation Secure Sockets Layer) 인증서 적용을 통해 E-Business 서버(30)는 전화인증요청 단말(10) 간의 데이터 세션에 대한 가로채기를 방지할 수 있다.

[101] 단계(S53b) 이후, 전화인증요청 단말(10)은 사용자의 입력에 따른 전화인증서암호(PIN 번호)를 E-Business 서버(30)로 전송한 뒤(S53c), 사용자가 이체 본거래를 완료하기 위한 확인 버튼이 입력되면, 확인 메시지를 E-Business 서버(30)로 전송함으로써(S53d), 이체 본거래는 완료된다.

[102]

[103] 이상에서 전술한 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체는 E-Business

서버(30)에 기본적으로 설치된 애플리케이션(이는 E-Business 서버(30)에 기본적으로 탑재된 플랫폼이나 운영체제 등에 포함된 프로그램을 포함할 수 있음)에 의해 실행될 수 있고, 사용자가 애플리케이션 스토어 서버, 애플리케이션 또는 해당 서비스와 관련된 웹 서버 등의 애플리케이션 제공 서버를 통해 E-Business 서버(30)에 직접 설치한 애플리케이션(즉, 프로그램)에 의해 실행될 수도 있다. 이러한 의미에서, 전술한 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체는 E-Business 서버(30)에 기본적으로 설치되거나 사용자에 의해 직접 설치된 애플리케이션(즉, 프로그램)으로 구현되고 단말기 등의 컴퓨터로 읽을 수 있는 기록매체에 기록될 수 있다.

[104] 이러한 프로그램은 컴퓨터에 의해 읽힐 수 있는 기록매체에 기록되고 컴퓨터에 의해 실행됨으로써 전술한 기능들이 실행될 수 있다.

[105] 이와 같이, 본 발명의 각 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체를 실행시키기 위하여, 전술한 프로그램은 컴퓨터의 프로세서(CPU)가 읽힐 수 있는 C, C++, JAVA, 기계어 등의 컴퓨터 언어로 코드화된 코드(Code)를 포함할 수 있다.

[106] 이러한 코드는 전술한 기능들을 정의한 함수 등과 관련된 기능적인 코드(Function Code)를 포함할 수 있고, 전술한 기능들을 컴퓨터의 프로세서가 소정의 절차대로 실행시키는데 필요한 실행 절차 관련 제어 코드를 포함할 수도 있다.

[107] 또한, 이러한 코드는 전술한 기능들을 컴퓨터의 프로세서가 실행시키는데 필요한 추가 정보나 미디어가 컴퓨터의 내부 또는 외부 메모리의 어느 위치(주소 번지)에서 참조 되어야 하는지에 대한 메모리 참조 관련 코드를 더 포함할 수 있다.

[108] 또한, 컴퓨터의 프로세서가 전술한 기능들을 실행시키기 위하여 원격(Remote)에 있는 어떠한 다른 컴퓨터나 서버 등과 통신이 필요한 경우, 코드는 컴퓨터의 프로세서가 컴퓨터의 통신 모듈(예: 유선 및/또는 무선 통신 모듈)을 이용하여 원격(Remote)에 있는 어떠한 다른 컴퓨터나 서버 등과 어떻게 통신해야만 하는지, 통신 시 어떠한 정보나 미디어를 송수신해야 하는지 등에 대한 통신 관련 코드를 더 포함할 수도 있다.

[109] 그리고, 본 발명을 구현하기 위한 기능적인(Functional) 프로그램과 이와 관련된 코드 및 코드 세그먼트 등은, 기록매체를 읽어서 프로그램을 실행시키는 컴퓨터의 시스템 환경 등을 고려하여, 본 발명이 속하는 기술분야의 프로그래머들에 의해 용이하게 추론되거나 변경될 수도 있다.

[110] 이상에서 전술한 바와 같은 프로그램을 기록한 컴퓨터로 읽힐 수 있는 기록매체는, 일 예로, ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광

미디어 저장장치 등이 있다.

[111] 또한 전술한 바와 같은 프로그램을 기록한 컴퓨터로 읽힐 수 있는 기록매체는 네트워크로 커넥션된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 이 경우, 다수의 분산된 컴퓨터 중 어느 하나 이상의 컴퓨터는 상기에 제시된 기능들 중 일부를 실행하고, 그 결과를 다른 분산된 컴퓨터들 중 하나 이상에 그 실행 결과를 전송할 수 있으며, 그 결과를 전송받은 컴퓨터 역시 상기에 제시된 기능들 중 일부를 실행하여, 그 결과를 역시 다른 분산된 컴퓨터들에 제공할 수 있다.

[112] 특히, 본 발명의 각 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체를 실행시키기 위한 프로그램인 애플리케이션을 기록한 컴퓨터로 읽을 수 있는 기록매체는, 애플리케이션 스토어 서버(Application Store Server), 애플리케이션 또는 해당 서비스와 관련된 웹 서버 등의 애플리케이션 제공 서버(Application Provider Server)에 포함된 저장매체(예: 하드디스크 등)이거나, 애플리케이션 제공 서버 그 자체일 수도 있다.

[113] 본 발명의 각 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체를 실행시키기 위한 프로그램인 애플리케이션을 기록한 기록매체를 읽을 수 있는 컴퓨터는, 일반적인 데스크 탑이나 노트북 등의 일반 PC 뿐만 아니라, 스마트 폰, 태블릿 PC, PDA(Personal Digital Assistants) 및 이동통신 단말기 등의 모바일 단말기를 포함할 수 있으며, 이뿐만 아니라, 컴퓨팅(Computing) 가능한 모든 기기로 해석되어야 할 것이다.

[114] 또한, 본 발명의 실시예에 따른 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체를 실행시키기 위한 프로그램인 애플리케이션을 기록한 기록매체를 읽을 수 있는 컴퓨터가 스마트 폰, 태블릿 PC, PDA(Personal Digital Assistants) 및 이동통신 단말기 등의 모바일 단말기인 경우, 애플리케이션은 애플리케이션 제공 서버에서 일반 PC로 다운로드 되어 동기화 프로그램을 통해 모바일 단말기에 설치될 수도 있다.

[115] 이상에서, 본 발명의 실시예를 구성하는 모든 구성 요소들이 하나로 결합되거나 결합되어 동작하는 것으로 설명되었다고 해서, 본 발명이 반드시 이러한 실시예에 한정되는 것은 아니다. 즉, 본 발명의 목적 범위 안에서라면, 그 모든 구성 요소들이 하나 이상으로 선택적으로 결합하여 동작할 수도 있다. 또한, 그 모든 구성 요소들이 각각 하나의 독립적인 하드웨어로 구현될 수 있지만, 각 구성 요소들의 그 일부 또는 전부가 선택적으로 조합되어 하나 또는 복수 개의 하드웨어에서 조합된 일부 또는 전부의 기능을 수행하는 프로그램

모듈을 갖는 컴퓨터 프로그램으로서 구현될 수도 있다. 그 컴퓨터 프로그램을 구성하는 코드들 및 코드 세그먼트들은 본 발명의 기술 분야의 당업자에 의해 용이하게 추론될 수 있을 것이다. 이러한 컴퓨터 프로그램은 컴퓨터가 읽을 수 있는 저장매체(Computer Readable Media)에 저장되어 컴퓨터에 의하여 읽혀지고 실행됨으로써, 본 발명의 실시예를 구현할 수 있다. 컴퓨터 프로그램의 저장매체로서는 자기 기록매체, 광 기록매체, 등이 포함될 수 있다.

[116] 또한, 이상에서 기재된 "포함하다", "구성하다" 또는 "가지다" 등의 용어는, 특별히 반대되는 기재가 없는 한, 해당 구성 요소가 내재될 수 있음을 의미하는 것이므로, 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것으로 해석되어야 한다. 기술적이거나 과학적인 용어를 포함한 모든 용어들은, 다르게 정의되지 않는 한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 사전에 정의된 용어와 같이 일반적으로 사용되는 용어들은 관련 기술의 문맥 상의 의미와 일치하는 것으로 해석되어야 하며, 본 발명에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[117] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

청구범위

[청구항 1] 전화인증요청 단말이, 전화인증서암호(PIN 번호)를 IP망과 연결된 E-Business 서버를 통해 TTP(Trusted Third Party) 서버로 전송하여 저장하도록 하여 상기 전화인증서암호(PIN 번호)를 등록하는 제 1 단계;
상기 TTP 서버가 상기 전화인증요청 단말과 상기 E-Business 서버 간의 E-Business 거래에 따라 상기 E-Business 서버로부터 E-Business 내역 정보와, 상기 전화인증요청 단말로부터 상기 E-Business 서버를 거쳐 확인을 위해 다시 입력된 전화인증서암호(PIN 번호)를 수신하여 저장된 전화인증서암호(PIN 번호)와 동일하다고 판단하는 제 2 단계;
상기 TTP 서버가 상기 E-Business 내역 정보와 상기 다시 입력된 전화인증서암호(PIN 번호)를 결합한 데이터를 암호화하여 저장하는 제 3 단계; 및
상기 E-Business 서버가 상기 전화인증요청 단말로부터 수신된 승인전화번호에 해당하는 전화인증용 단말에 대한 전화 승인 요청을 IVR(Interactive Voice Response) 서버로 전송하여 전화 승인이 수행되도록 하는 제 4 단계; 를 포함하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 2] 청구항 1에 있어서, 상기 제 1 단계 이전에,
상기 전화인증요청 단말이 사용자의 요청에 따라 상기 IP망을 통해 상기 E-Business 서버에 대한 로그인을 수행하는 단계;
상기 전화인증요청 단말이 상기 IP망을 통해 상기 E-Business 서버로 상기 사용자가 소지한 상기 전화인증용 단말을 이용한 전화 인증 서비스를 신청하는 단계; 및
상기 E-Business 서버가 상기 IP망을 통해 상기 전화인증요청 단말로 전화 인증 서비스 등록 요청을 전송하는 단계; 더 포함하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 3] 청구항 2에 있어서, 상기 제 1 단계는,
상기 전화인증요청 단말이 상기 사용자에 의해 상기 전화인증서암호(PIN 번호) 뿐만 아니라, 상기 전화인증용 단말의 전화번호에 해당하는 상기 승인전화번호,
거래승인번호(이체승인번호)의 입력에 따라, 상기 승인전화번호,

상기 전화인증서암호(PIN 번호), 상기
거래승인번호(이체승인번호)를 상기 IP망을 통해 상기 E-Business 서버로 전송하면,
상기 E-Business 서버가 전용선(L1)을 통해 상기
전화인증서암호(PIN 번호)를 상기 TTP 서버로 전송하여
저장하도록 하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 4] 청구항 3에 있어서, 상기 제 1 단계와 상기 제 2 단계 사이에,
상기 E-Business 서버가 상기 승인전화번호, 상기
전화인증서암호(PIN번호), 그리고 상기
거래승인번호(이체승인번호)를 상기 IVR 서버와 연결된
전용선(L2)을 통해 상기 IVR 서버로 전송함과 동시에, 상기 IVR 서버로 상기 승인전화번호에 해당하는 상기 전화인증용 단말로 전화 인증 서비스를 위한 가입 전화를 요청하는 제 1-1 단계; 를 더 포함하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 5] 청구항 4에 있어서, 상기 제 1 단계와 상기 제 2 단계 사이에 상기 제 1-1 단계 이후에 수행되는,
상기 IVR 서버가 상기 E-Business 서버로부터 수신된 상기
전화인증서암호(PIN번호) 및 상기 거래승인번호(이체승인번호)를 저장하는 제 1-2 단계; 를 더 포함하는 것을 특징으로 하는
신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 6] 청구항 5에 있어서, 상기 제 1 단계와 상기 제 2 단계 사이에 상기 제 1-2 단계 이후에 수행되는,
상기 IVR 서버가 상기 승인전화번호에 해당하는 상기 전화인증용 단말로 유무선 전화망을 통해 전화 인증 서비스 가입 안내를 음성데이터로 전송하는 제 1-3 단계; 를 더 포함하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 7] 청구항 6에 있어서, 상기 제 1 단계와 상기 제 2 단계 사이에 상기 제 1-3 단계 이후에 수행되는,
상기 전화인증용 단말이 상기 사용자에 의해 전화 인증 서비스 가입 확인을 위해 상기 전화인증서암호(PIN 번호) 및 상기 거래승인번호(이체승인번호)에 대한 동일한 입력을 받은 뒤,

입력받은 전화인증서암호(PIN 번호) 및
거래승인번호(이체승인번호)를 유무선 전화망을 통해 상기 IVR 서버로 반환하는 제 1-4 단계; 를 더 포함하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 8] 청구항 7에 있어서, 상기 제 1 단계와 상기 제 2 단계 사이에 상기 제 1-4 단계 이후에 수행되는,
상기 IVR 서버가 상기 전화인증용 단말로부터 수신된 전화인증서암호(PIN 번호)와 상기 1-2 단계에서 저장된 전화인증서암호(PIN 번호)가 동일함을 확인하고, 상기 전화인증용 단말로부터 수신된 거래승인번호(이체승인번호)와 상기 1-2 단계에서 저장된 거래승인번호(이체승인번호)가 동일함을 확인한 뒤, 전화 인증 서비스 가입 완료 메시지를 상기 전용선(L2)을 통해 상기 E-Business 서버로 통지하여 전화 인증 서비스 신청 과정을 종료하는 제 1-5 단계; 를 더 포함하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 9] 청구항 8에 있어서, 상기 제 2 단계는,
상기 전화인증요청 단말이 상기 IP망을 통해 상기 E-Business 서버와 데이터 송수신을 통해 상기 E-Business 거래를 수행하는 제 2-1 단계;
상기 전화인증요청 단말이 상기 사용자에 의해 상기 제 1 단계에서 입력받은 동일한 전화인증서암호(PIN 번호)를 다시 입력받아 상기 IP망을 통해 상기 E-Business 서버로 전송하는 제 2-2 단계;
상기 E-Business 서버가 상기 E-Business 내역 정보와, 상기 제 2-2 단계에서 수신된 전화인증서암호(PIN 번호)를 상기 전용선(L1)을 통해 상기 TTP 서버로 전송하는 제 2-3 단계; 및
상기 TTP 서버가 상기 제 2-3 단계에서 수신된 전화인증서암호(PIN 번호)와 상기 제 1 단계에서 저장된 전화인증서암호(PIN 번호)를 비교하여 확인하여 동일한지 여부를 판단하는 제 2-4 단계; 를 포함하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 10] 청구항 9에 있어서, 상기 제 3 단계는,
상기 TTP 서버가 상기 E-Business 내역 정보와 상기 제 2-3 단계에서 수신된 전화인증서암호(PIN 번호)와 결합한 데이터를 암호화하여 거래 부인 방지 정보를 생성하여 저장하며, 상기 E-Business 내역 정보에 대한 저장은 수행하지 않는거나 저장을

하는 것을 선택적으로 적용가능한 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 11] 청구항 10에 있어서, 상기 제 3 단계는,
상기 TTP 서버에 의해 생성되는 거래 부인 방지 정보에는 인자값으로, 거래일시(분초 포함), 출금계좌번호, 이체금액, 입금계좌번호, 입금은행코드. 받는사람을 포함하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 12] 청구항 10에 있어서, 상기 제 3 단계와 상기 제 4 단계 사이에,
상기 TTP 서버가 상기 전용선(L1)을 통해 상기 E-Business 서버로 전화인증서암호(PIN 번호)에 대한 확인 결과를 전송하는 단계; 를 더 포함하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 13] 청구항 12에 있어서, 상기 제 4 단계는,
상기 E-Business 서버가 상기 E-Business 내역 정보를 상기 전용선(L2)을 통해 상기 IVR 서버로 전송하며, 이와 동시에 전화 승인 요청을 상기 IVR 서버로 전송하는 제 4-1 단계;
상기 IVR 서버가 유무선전화망을 통해 음성데이터에 의한 상기 E-Business 내역 정보를 포함하는 전화 승인 요청 안내를 상기 전화인증용 단말로 전송하는 제 4-2 단계;
상기 전화인증용 단말이 상기 제 1 단계에서 상기 전화인증요청 단말로 입력된 거래승인번호(이체승인번호)와 동일한 거래승인번호(이체승인번호)를 상기 사용자로부터 입력받아 상기 유무선전화망을 통해 상기 IVR 서버로 전송하는 제 4-3 단계;
상기 IVR 서버가 상기 전화인증용 단말로부터 수신된 거래승인번호(이체승인번호)와 상기 제 1-2 단계에서 저장된 거래승인번호(이체승인번호)를 비교하여 동일함을 확인한 뒤, 전화 승인 결과를 생성하는 제 4-4 단계;
상기 IVR 서버가 상기 전화 승인 결과를 상기 전용선(L2)을 통해 상기 E-Business 서버로 전송하는 제 4-5 단계; 및
상기 E-Business 서버가 상기 E-Business 거래를 완료한 뒤, 상기 전화 승인 결과를 상기 IP망을 통해 상기 전화인증요청 단말로 전송하는 제 4-6 단계; 를 포함하는 것을 특징으로 하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증방법.

[청구항 14] 전화인증요청 단말로부터 전화인증서암호(PIN 번호)를 IP망을 통해 수신하여 TTP(Trusted Third Party) 서버로 전송하도록 송수신부를 제어하여, 상기 TTP 서버에 상기 전화인증서암호(PIN 번호)를 등록하도록 하는 전화 인증 신청수단;
상기 전화인증요청 단말과 E-Business 거래를 수행하도록 하는 E-business 거래수단;
상기 TTP 서버로 E-Business 내역 정보와, 상기 전화인증요청 단말로부터 상기 E-Business 서버를 거쳐 확인을 위해 다시 입력된 전화인증서암호(PIN 번호)를 전송하도록 상기 송수신부를 제어하여 상기 TTP 서버에 의해 상기 E-Business 내역 정보와 전화인증서암호(PIN 번호)를 결합한 데이터를 암호화하여 저장하도록 하는 E-business 거래 부인 방지수단; 및
상기 전화인증요청 단말로부터 수신된 승인전화번호에 해당하는 전화인증용 단말에 대한 전화 승인 요청을 IVR(Interactive Voice Response) 서버로 전송하도록 상기 송수신부를 제어하여 상기 전화인증용 단말에 대한 전화 승인이 수행되도록 하는 전화 인증 수행수단; 을 구비하여 이루어지는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 신뢰기관과의 연계를 통해 부인방지 기능을 제공하는 전화인증용 단말을 이용한 E-Business trade 거래에서의 전화인증프로그램을 기록한 컴퓨터로 판독가능한 기록매체.