(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년09월30일
(11) 등록번호 10-1658684
(24) 등록일자 2016년09월12일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01) *G06Q 40/02* (2012.01)
(21) 출원번호 10-2011-7017740
(22) 출원일자(국제) 2010년01월06일
심사청구일자 2014년12월26일
(85) 번역문제출일자 2011년07월28일
(65) 공개번호 10-2011-0134381
(43) 공개일자 2011년12월14일
(86) 국제출원번호 PCT/EP2010/050079
(87) 국제공개번호 WO 2010/079182
국제공개일자 2010년07월15일
(30) 우선권주장
0900150.4 2009년01월06일 영국(GB)
12/416,836 2009년04월01일 미국(US)
(56) 선행기술조사문헌
WO2004012036 A2*
WO2008059465 A2*
WO2008100813 A1*
EP0987642 A2
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
비자 유럽 리미티드
영국, 런던 더블류2 6티티, 셀던 스퀘어 1
(72) 발명자
윈필드-치슬렛, 피터
영국, 런던 더블류2 6티티, 셀던 스퀘어 1
레쉬쎄, 이타마르
영국, 런던 더블류2 6티티, 셀던 스퀘어 1
(뒷면에 계속)
(74) 대리인
한양특허법인

전체 청구항 수 : 총 13 항 심사관 : 박장환

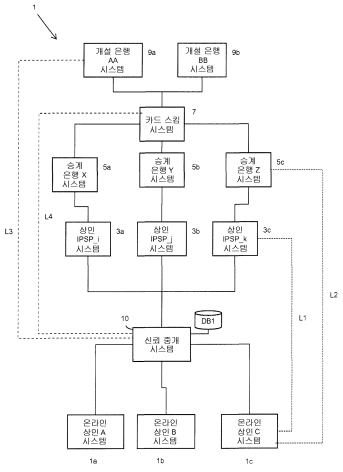
(54) 발명의 명칭 **결제 시스템**

(57) 요 약

본 발명의 실시예들은, 온라인 상인들을 대행하여 데이터 통신 네트워크를 통해 행해질 결제 트랜잭션들에 대한 결제 승인 요청들을 처리하는 방법이고, 상기 결제 승인 요청들은 복수의 상이한 온라인 상인 시스템들을 통한 금융 수단 소유자들에 의한 오더들의 결과로서 행해지며, 상기 온라인 상인들의 각각은 온라인 상인 신원을 갖는

(뒷면에 계속)

대 표 도 - 도2



방법을 제공한다. 상기 방법은, 결제 승인 요청들을 복수의 온라인 상인 인터넷 결제 서비스 제공자 시스템들의 각각에 송신하도록 이루어지는, 신뢰 중앙 중개 시스템에 의해 행해지고; 각각의 상인 IPSP 시스템은 결제 승인 요청들을 복수의 승계 은행 결제 처리기 시스템들 중 적어도 하나에 송신하도록 이루어지며, 상기 복수의 승계 은행 결제 처리기 시스템들의 각각은 상기 승계 은행들 중 적어도 하나에 대해서 결제 승인들을 처리할 책임이 있다. 상기 방법은, 제1 온라인 상인에 대해서 결제 승인 요청들을 발생시킬 책임이 있는 제1 온라인 상인 시스템으로부터 결제 트랜젝션의 승인에 관련된 결제 승인 요청을 수신하는 단계로서, 상기 수신되는 결제 승인 요청은 금융 수단 소유자가 상기 제1 온라인 상인 시스템을 통해 오더를 행하는 것의 결과로서 시작되는, 단계; 상기 요청을 수신한 것에 응답하여: a) 다음의 i), ii) 및 iii)를 포함하는 트랜젝션 데이터를 포함하는 결제 승인 요청을 생성하는 단계; i) 상기 금융 수단 소유자에 의해 상기 결제 트랜젝션에 사용될 금융 수단 신원; ii) 결제 트랜젝션 수익자로서, 상기 제1 온라인 상인과 관련되는, 온라인 상인 신원; 및 iii) 결제 금액을 포함하는 하나 이상의 트랜젝션 명세; b) 상기 제1 온라인 상인과 관련되는 선택된 상인 IPSP 시스템으로의 결제 승인 요청 데이터의 송신을 가능케 하도록 송신 데이터를 검색하는 단계; 및 상기 검색된 송신 데이터에 기초하여, 상기 생성된 결제 승인 요청을 상기 선택된 상인 IPSP 시스템 - 그로부터 추가적인 결제 승인 요청이 생성되어, 상기 제1 온라인 상인이 관련되는 승계 은행에 대한 결제 승인들을 처리할 책임이 있는 승계 은행 결제 처리기 시스템으로 송신될 수 있음 - 에 송신하는 단계를 포함한다. 본 발명의 실시예들은, 사용자로 하여금, 사용자가 개개의 온라인 상인 시스템들에 또는 그것들의 상인 IPSP 시스템들에 지급 명세를 제공하는 요구 사항을 없애면서, 트랜젝션 단위의 결제 방법을 선택할 수 있게 한다. 따라서, 온라인 상인들 또는 그들의 상인 IPSP들이 상기 방법을 행하도록 이루어진 서비스에 기명 승낙하는 것을 조건으로, 사용자들은 그들의 개개의 지급 명세를, 바람직하게 한번만, 분리된 신뢰 엔터티에 제출하는 것만이 필수이다.

(72) 발명자

스트링펠로우, 웨스틀리

영국, 런던 더블류2 6티티, 셸던 스퀘어 1

카사본느, 베로니카

영국, 런던 더블류2 6티티, 셸던 스퀘어 1

탬블린, 레이몬드

영국, 런던 더블류2 6티티, 셸던 스퀘어 1

명 세 서

청구범위

청구항 1

온라인 상인들을 대행하여 데이터 통신 네트워크를 통해 행해질 결제 트랜잭션(payment transaction)들에 대한 결제 승인 요청들을 처리하는 방법이고, 상기 결제 승인 요청들은 복수의 상이한 온라인 상인 시스템들을 통한 금융 수단 소유자(financial instrument holder)들에 의한 오더(order)들의 결과로서 행해지며, 상기 온라인 상인들의 각각은 온라인 상인 신원(online merchant identity)을 갖고, 상기 온라인 상인들의 각각은 복수의 승계 은행(acquiring bank) 중 하나와 관련되는 방법으로서,

상기 방법은, 결제 승인 요청들을 복수의 온라인 상인 인터넷 결제 서비스 제공자(Internet Payment Service Provider; "IPSP") 시스템들의 각각에 송신하도록 이루어지는, 신뢰 중앙 중개 시스템(trusted central intermediary system)에 의해 행해지고,

상기 상인 IPSP 시스템들의 각각은 결제 승인 요청들을 복수의 승계 은행 결제 처리기 시스템들 중 적어도 하나에 송신하도록 이루어지며, 상기 복수의 승계 은행 결제 처리기 시스템들의 각각은 상기 승계 은행들 중 적어도 하나에 대해서 결제 승인들을 처리할 책임이 있고, 그리고

상기 신뢰 중앙 중개 시스템은 선택된 상인 IPSP 시스템에 결제 승인 요청 데이터의 송신을 가능하게 하는 상인 IPSP 시스템 송신 데이터, 및 상기 온라인 상인들의 각각에 대해서 상기 온라인 상인이 등록되는 상인 IPSP 시스템의 식별자와 함께 온라인 상인 신원을 구비하는 상인 프로파일 데이터를 저장하도록 구성된 데이터베이스를 구비하며,

상기 방법은:

제1 온라인 상인에 대해서 결제 승인 요청들을 발생시킬 책임이 있는 제1 온라인 상인 시스템으로부터 결제 트랜젝션의 승인에 관련된 결제 승인 요청을 수신하는 단계로서, 상기 수신되는 결제 승인 요청은 금융 수단 소유자가 상기 제1 온라인 상인 시스템을 통해 오더를 행하는 것의 결과로서 시작되고, 상기 수신되는 결제 승인 요청은 상기 제1 온라인 상인과 관련되는 온라인 상인 신원을 구비하는, 단계;

상기 요청을 수신한 것에 응답하여:

a) 다음의 i), ii) 및 iii)를 포함하는 트랜젝션 데이터를 포함하는 결제 승인 요청을 생성하는 단계:

i) 상기 금융 수단 소유자에 의해 상기 결제 트랜젝션에 사용될 금융 수단 신원;

ii) 결제 트랜젝션 수익자(payment transaction beneficiary)로서, 상기 제1 온라인 상인과 관련되는, 온라인 상인 신원; 및

iii) 결제 금액을 포함하는 하나 이상의 트랜젝션 명세(transaction detail);

b) 상기 제1 온라인 상인과 관련되는 상기 온라인 상인 신원을 사용하여 상기 데이터베이스에서 룩업을 실행함으로써 상기 제1 온라인 상인이 등록된 상기 상인 IPSP 시스템을 선택하는 단계;

c) 상기 선택된 상인 IPSP 시스템과 관련되는 상인 IPSP 시스템 송신 데이터를 검색하는 단계; 및

d) 상기 검색된 상인 IPSP 시스템 송신 데이터에 기초하여, 상기 결제 승인 요청을 상기 온라인 상인의 어플리케이션 프로그래밍 인터페이스(API)의 API 포맷으로 변환하고, 상기 포맷된 결제 승인 요청을 상기 선택된 상인 IPSP 시스템 - 그로부터 추가적인 결제 승인 요청이 생성되어, 상기 제1 온라인 상인이 관련되는 승계 은행에 대한 결제 승인들을 처리할 책임이 있는 승계 은행 결제 처리기 시스템으로 송신될 수 있음 - 에 송신하는 단계를 포함하는 방법.

청구항 2

청구항 1에 있어서,

상기 신뢰 중앙 중개 시스템은 상기 선택된 상인 IPSP 시스템으로부터 결제 승인 응답을 수신하고, 그에 응답하

여 결제 승인 응답을 상기 제1 온라인 상인 시스템에 송신하는, 방법.

청구항 3

삭제

청구항 4

청구항 1 또는 청구항 2에 있어서,

상기 생성된 승인 요청에 포함되는 상기 온라인 상인 신원은 상기 수신되는 온라인 상인 신원에 기초하여 생성되는, 방법.

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

청구항 1에 있어서,

상기 상인 IPSP 시스템 송신 데이터를 검색하는 단계는 상기 선택된 상인 IPSP 시스템에 대한 네트워크 어드레스를 검색하는 것을 포함하고, 상기 생성된 결제 승인 요청을 선택된 상인 IPSP 시스템에 송신하는 단계는 상기 검색된 네트워크 어드레스에 기초하여 상기 생성된 결제 승인 요청을 송신하는 것을 포함하는, 방법.

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

청구항 1, 청구항 2, 및 청구항 8 중 어느 한 항에 있어서,

상기 금융 수단 신원은 상기 금융 수단과 관련된 주 계좌 번호(Primary Account Number; “PAN”)를 포함하는, 방법.

청구항 16

청구항 15에 있어서,

상기 PAN은 신용 카드 번호 또는 직불 카드 번호(debit card number)를 포함하는, 방법.

청구항 17

청구항 1에 있어서,

상기 선택된 상인 IPSP 시스템은, 상기 제1 온라인 상인을 대행하여, 상기 결제 트랜잭션이 행해지는 온라인 상인 계정에 대한 결제 트랜젝션 지불(payment transaction settlement)을 제공하는, 방법.

청구항 18

삭제

청구항 19

청구항 1, 청구항 2, 청구항 8, 및 청구항 17 중 어느 한 항에 있어서,

상기 신뢰 중앙 중개 시스템은, 상기 제1 온라인 상인을 위한 등록 인터페이스를 제공하여, 상기 제1 온라인 상인이 관련된 상인 IPSP 시스템을 상기 제1 온라인 상인이 등록할 수 있는, 방법.

청구항 20

청구항 1, 청구항 2, 청구항 8, 및 청구항 17 중 어느 한 항에 있어서,

상기 신뢰 중앙 중개 시스템은 상기 제1 온라인 상인 시스템으로부터 발생하는 제1 타입의 결제 트랜젝션들에 대한 결제 승인 요청들을 수신 및 처리하며, 그에 응답하여, 생성된 결제 승인 요청을 상기 선택된 상인 IPSP 시스템에 송신하도록 되어 있고, 상기 선택된 상인 IPSP 시스템은 상기 제1 온라인 상인 시스템으로부터 발생하는 상이한 타입의 결제 트랜젝션들에 대한 결제 승인 요청들을 수신 및 처리하며, 상기 상이한 타입의 결제 트랜젝션들에 대한 결제 승인 요청들은 상기 중앙 중개 시스템을 통해 처리되지 않는, 방법.

청구항 21

청구항 20에 있어서,

상기 제1 온라인 상인 시스템으로부터 발생하는 제1 타입의 결제 트랜젝션들에 대한 상기 결제 승인 요청들은 상기 금융 수단 신원을 포함하지 않고, 상기 제1 온라인 상인 시스템으로부터 발생하는 상기 상이한 타입의 결제 트랜젝션들에 대한 상기 결제 승인 요청들은 상기 상이한 타입의 결제 트랜젝션들의 오더 처리 동안에 상기 온라인 상인 시스템에 의해 수집되는 금융 수단 신원을 포함하는, 방법.

청구항 22

청구항 21에 있어서,

상기 상이한 타입의 결제 트랜젝션들의 오더 처리 동안에 상기 온라인 상인 시스템에 의해 수집되는 상기 금융 수단 신원은 신용 카드 번호 또는 직불 카드 번호를 포함하는, 방법.

청구항 23

복수의 온라인 상인 시스템 및 복수의 상인 IPSP 시스템과 통신하는 신뢰 중앙 중개 시스템으로서,

상기 신뢰 중앙 중개 시스템은 선택된 상인 IPSP 시스템에 결제 승인 요청 데이터의 송신을 가능하게 하는 상인 IPSP 시스템 송신 데이터, 및 온라인 상인들의 각각에 대해서 상기 온라인 상인이 등록되는 상인 IPSP 시스템의 식별자와 함께 온라인 상인 신원을 구비하는 상인 프로파일 데이터를 저장하도록 구성된 데이터베이스를 구비하고,

상기 신뢰 중앙 중개 시스템은,

제1 온라인 상인에 대해서 결제 승인 요청들을 발생시킬 책임이 있는 제1 온라인 상인 시스템으로부터 결제 트

랜젝션의 승인에 관련된 결제 승인 요청을 수신하고, 상기 수신되는 결제 승인 요청은 금융 수단 소유자가 상기 제1 온라인 상인 시스템을 통해 오더를 행하는 것의 결과로서 시작되고, 상기 수신되는 결제 승인 요청은 상기 제1 온라인 상인과 관련되는 온라인 상인 신원을 구비하며,

상기 요청을 수신한 것에 응답하여:

a) 다음의 i), ii) 및 iii)를 포함하는 트랜젝션 데이터를 포함하는 결제 승인 요청을 생성하고:

i) 상기 금융 수단 소유자에 의해 상기 결제 트랜젝션에 사용될 금융 수단 신원;

ii) 결제 트랜젝션 수익자(payment transaction beneficiary)로서, 상기 제1 온라인 상인과 관련되는, 온라인 상인 신원; 및

iii) 결제 금액을 포함하는 하나 이상의 트랜젝션 명세(transaction detail);

b) 상기 제1 온라인 상인과 관련되는 상기 온라인 상인 신원을 사용하여 상기 데이터베이스에서 룩업을 실행함으로써 상기 제1 온라인 상인이 등록된 상기 상인 IPSP 시스템을 선택하고;

c) 상기 선택된 상인 IPSP 시스템과 관련되는 상인 IPSP 시스템 송신 데이터를 검색하고,

d) 상기 검색된 상인 IPSP 시스템 송신 데이터에 기초하여, 상기 결제 승인 요청을 상기 온라인 상인의 어플리케이션 프로그래밍 인터페이스(API)의 API 포맷으로 변환하고, 상기 포맷된 결제 승인 요청을 상기 선택된 상인 IPSP 시스템 - 그로부터 추가적인 결제 승인 요청이 생성되어, 상기 제1 온라인 상인이 관련되는 승계 은행에 대한 결제 승인들을 처리할 책임이 있는 승계 은행 결제 처리기 시스템으로 송신될 수 있음 - 에 송신하도록 이루어지는, 신뢰 중앙 중개 시스템.

청구항 24

삭제

청구항 25

삭제

청구항 26

온라인 상인들을 대행하여 데이터 통신 네트워크를 통해 행해질 결제 트랜잭션들에 대한 결제 승인 요청들을 처리하기 위한 결제 승인 시스템이고, 상기 결제 승인 요청들은 복수의 상이한 온라인 상인 시스템들을 통한 금융 수단 소유자들에 의한 오더들의 결과로서 행해지며, 상기 온라인 상인들의 각각은 온라인 상인 신원을 갖고, 상기 온라인 상인들의 각각은 복수의 상이한 승계 은행(acquiring bank) 중 하나와 관련되는 결제 승인 시스템으로서,

상기 결제 승인 시스템은, 복수의 상이한 온라인 상인 인터넷 결제 서비스 제공자(IPSP) 시스템들과 그리고 복수의 상기 온라인 상인과 통신하도록 이루어지는, 신뢰 중앙 중개 시스템을 포함하고, 상기 신뢰 중앙 중개 시스템은 상기 복수의 상이한 온라인 상인 인터넷 결제 서비스 제공자(IPSP) 시스템들의 각각으로 결제 승인 요청들을 송신하도록 이루어지며,

상기 상인 IPSP 시스템들의 각각은 결제 승인 요청들을 복수의 승계 은행 결제 처리기 시스템들 중 적어도 하나에 송신하도록 이루어지고, 상기 복수의 승계 은행 결제 처리기 시스템들의 각각은 상기 승계 은행들 중 적어도 하나에 대해서 결제 승인들을 처리할 책임이 있으며,

상기 신뢰 중앙 중개 시스템은 선택된 상인 IPSP 시스템에 결제 승인 요청 데이터의 송신을 가능하게 하는 상인 IPSP 시스템 송신 데이터, 및 상기 온라인 상인들의 각각에 대해서 상기 온라인 상인이 등록되는 상인 IPSP 시스템의 식별자와 함께 온라인 상인 신원을 구비하는 상인 프로파일 데이터를 저장하도록 구성된 데이터베이스를 구비하며,

제1 온라인 상인 시스템으로부터의 결제 트랜젝션의 승인에 관련된 결제 승인 요청에 응답하여, 상기 수신되는 결제 승인 요청은 금융 수단 소유자가 상기 제1 온라인 상인 시스템을 통해 오더를 행하는 것의 결과로서 시작되고, 상기 제1 온라인 상인 시스템은 상기 제1 온라인 상인에 대한 결제 승인 요청들을 발생시킬 책임이 있으며, 상기 수신되는 결제 승인 요청은 상기 제1 온라인 상인과 관련되는 온라인 상인 신원을 구비하고,

상기 신뢰 중앙 중개 시스템은,

a) 다음의 i), ii) 및 iii)를 포함하는 트랜젝션 데이터를 포함하는 결제 승인 요청을 생성하고:

i) 상기 금융 수단 소유자에 의해 상기 결제 트랜젝션에 사용될 금융 수단 신원;

ii) 결제 트랜젝션 수익자로서, 상기 제1 온라인 상인과 관련되는, 온라인 상인 신원; 및

iii) 결제 금액을 포함하는 하나 이상의 트랜젝션 명세;

b) 상기 제1 온라인 상인과 관련되는 상기 온라인 상인 신원을 사용하여 상기 데이터베이스에서 룩업을 실행함으로써 상기 제1 온라인 상인이 등록된 상기 상인 IPSP 시스템을 선택하고;

c) 상기 선택된 상인 IPSP 시스템과 관련되는 상인 IPSP 시스템 송신 데이터를 검색하고,

d) 상기 검색된 상인 IPSP 시스템 송신 데이터에 기초하여, 상기 결제 승인 요청을 상기 온라인 상인의 어플리케이션 프로그래밍 인터페이스(API)의 API 포맷으로 변환하고, 상기 포맷된 결제 승인 요청을 상기 선택된 상인 IPSP 시스템 - 그로부터 추가적인 결제 승인 요청이 생성되어, 상기 제1 온라인 상인이 관련되는 승계 은행에 대한 결제 승인들을 처리할 책임이 있는 승계 은행 결제 처리기 시스템으로 송신될 수 있음 - 에 송신하도록 이루어지는, 결제 승인 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은, 온라인 상인들 대행하여 데이터 통신 네트워크를 통해 행해질 결제 트랜젝션(payment transaction)에 대한 결제 승인 요청을 처리하는 시스템 및 방법에 관한 것이며, 특히, 하지만 배타적이지 않게, 금융 수단 소유자(financial instrument holder)에 의해 내어진 오더(order)의 처리에 적합하다.

배 경 기 술

[0002] 사용자들이 온라인에서, 즉, 인터넷 및 관련 기술을 통해서 제품을 구입하는 것에 더욱더 고무되고 있다. 일반적으로 말해서, 기존의 온라인 결제 시스템들은 다음의 3가지 타입의 장치 중 하나에 속한다: 제1 타입의 장치에 있어서, 온라인 상인 시스템(online merchant system)은, 또 하나의 명칭이 구매자(buyer) 또는 카드소지자(cardholder)인 금융 수단 소유자로부터, 트랜젝션에 수반될 수 있는 임의의 다른 엔터티(entity)와 구매자가 직접적으로 상대하지 않고, 지급 명세(payment detail)를 수집하며, 온라인 상인 시스템은 트랜젝션 명세를 그들의 승계 은행(acquiring bank) 시스템에 직접적으로 송신한다. 제2 타입의 장치에 있어서, 온라인 상인 시스템은 트랜젝션에 수반될 수 있는 임의의 다른 엔터티와 구매자가 직접적으로 상대하지 않고 구매자로부터 지급 명세를 수집하며, 온라인 상인 시스템은 상인을 대행하여 결제 승인을 처리하는 온라인 상인 인터넷 결제 서비스 제공자(Internet Payment Service Provider; “IPSP”)에 트랜젝션 명세를 송신한다. 상인 IPSP 시스템은 다음에 온라인 상인의 승계 은행 시스템에 명세를 전송한다; 명세는 승계 은행으로 또는 승계 은행을 대행하는 결제 처리기(payment processor)에 직접적으로 전송될 수 있다. 이러한 제2 타입의 장치에 대한 지원을 제공하는 IPSP 시스템의 예는 Protx™ Veri-Secure Payment system(VSP)을 포함한다.

[0003] 제1 및 제2 타입의 장치에 있어서, 온라인 상인 시스템은 일반적으로 결제 카드 데이터, 은행 계좌 정보 및/또는 다른 금융 데이터를 구매자로부터 획득한다. 온라인 상인 시스템은 그 다음에 이러한 정보를 직접적으로, 또는 상인 IPSP 시스템을 통해서, 승계 은행 처리 시스템으로 패스한다. 각각의 온라인 상인 시스템은 승계 은행에 의해서 온라인 상인 계정 식별자를 할당받고, 이러한 계정 식별자는, 트랜젝션의 승인을 요청할 때, 승계 은행에 온라인 상인을 식별시키는데 사용된다.

[0004] 도 1은 복수의 온라인 상인 시스템(1a, 1b, 1c)을 포함하는 제2 타입의 장치에 따른 일반적인 온라인 결제 시스템의 일예를 나타낸다. 이러한 장치에 있어서, 각각의 온라인 상인들은, 인터넷상의 보안 비즈니스를 행할 목적을 위해 온라인 상인에 의해 선택되고 기명 승낙된 결제 게이트웨이(online merchant)와 협동한다. 도면이 동일한 상인 IPSP 시스템(3)과 관련된 온라인 상인 시스템(1a ... 1c)의 각각을 나타내지만, 대안적으로, 그리고 사실상 실제에 있어서 흔히, 온라인 상인 시스템들은 상이한 상인 IPSP 시스템들(3)에 링크(link)된다. 각각의 상인 IPSP 시스템(3)은 암호화 기술을 이용하여 인터넷을 통해 결제 카드 데이터, 승인 요청, 및 승인 응답을 패스하는 시스템을 제공한다. 트랜젝션 정보는 상인 IPSP 시스템(3)에 의해서 데이터 통신 링크를 통해 승계

은행(5)으로 송신되고, 그리고 거기서부터, 카드의 유효성이 체크되고 그 계정의 자금의 가용성이 검증되는 개설 은행과 중개하는 카드 스킴 시스템(card scheme system)(7)으로 송신된다. 승인 코드가 상인 IPSP 시스템(3)으로 회신된다; 승인은 상인 IPSP 시스템(3)에 의해 암호화되어 오더의 이행을 트리거(trigger)하는 온라인 상인 시스템(1a)에 암호화된 형태로 전송된다.

[0005] 제2 타입의 장치를 이용하고 도 1에 나타낸 엔터티들을 수반하는 일반적인 단 대 단(end-to-end) 온라인 트랜잭션은 다음의 단계들을 포함한다:

[0006] * 온라인 상인의 시스템(1a) 웹사이트는 구매자로부터 하나 이상의 오더 선택을 수집한다. 구매자는 체크하고, 그들의 지급 명세를 입력하며, 상인 웹사이트의 오더 전송 웹페이지상의 '오더를 제출' 또는 등가의 버튼을 누르는 것에 의해 온라인 상인의 시스템(1a)에 오더를 낸다.

[0007] * 구매자의 웹 브라우저는 브라우저와 온라인 상인의 웹 서버간에 송신될 정보를 암호화한다.

[0008] * 온라인 상인은 그 다음에, 일반적으로 상인 IPSP 시스템(3)에 의해 호스팅되는 결제 서버로의 다른 암호화된 연결을 통해서, 그들의 상인 IPSP 시스템(3)에 트랜잭션 명세를 전달한다.

[0009] * 상인 IPSP 시스템(3)은 온라인 상인의 승계 은행 시스템(5)에 의해 사용되는 처리기에, 온라인 상인의 인터넷 계정 식별자를 포함하는, 트랜잭션 정보를 전달한다.

[0010] * 처리기(5)는 트랜잭션 정보를 결제 스킴 시스템(7)(예컨대, Visa/MasterCard)에 전달한다.

[0011] * 결제 스킴 시스템(7)은 트랜잭션을 정확한 카드 개설 은행 시스템(9)으로 라우팅한다.

[0012] * 결제 카드 개설 은행 시스템(9)은 승인 요청을 수신하고, 온라인 상인의 승계 은행 시스템(5)의 처리기에 응답 코드로 응답을 회신한다.

[0013] * 온라인 상인의 승계 은행 시스템(5)의 처리기는 응답을 상인 IPSP 시스템(3)에 전달한다.

[0014] * 상인 IPSP 시스템(3)은 응답을 수신하고, 응답을, 그것이 해석되고, 트랜잭션이 승인되었음을 확인하는 구매자에게 상인을 통해서 관련 응답이 그 다음에 중계 회신되는 온라인 상인의 시스템으로 전달한다.

[0015] * 상인 IPSP 시스템(3)은, 온라인 상인을 대행하여, 모든 그들의 입증된 승인을, 지불을 위해 온라인 상인의 승계 은행 시스템(5)에 제출한다.

[0016] * 승계 은행 시스템(5)은 총 입금된 자금 빼기 임의의 수수료 및 요금을 온라인 상인의 지정된 계정에 넣는다. 이것은, 온라인 상인이 동일한 은행과, 또는 다른 은행의 계정에 그들의 은행 업무를 할 경우, 승계 은행과의 계정이 될 수 있다.

[0017] 도 1에 나타낸 상인 IPSP 시스템과 같은 결제 게이트웨이를 이용하는 장점은, 온라인 상인을 대행하여, 하나 이상의 추가적인 다양한 트랜잭션 처리 기능들, 예컨대 지불, 지불거절(chargeback)의 처리, 환불의 처리, 및 트랜잭션 보고를 제공할 수 있다는 것이다. 지불 프로시져(settlement procedure)에 있어서, 상인 IPSP 시스템(3)은, "배치(batch)"에 있어서, 주어진 기간에 걸쳐 수집된 모든 온라인 상인의 입증된 승인들을 지불을 위해 온라인 상인의 승계 은행 시스템(5)에 제출한다. 지불거절은 구매에 사용된 카드를 개설한 은행 또는 구매자에 의해 시작되는 결제 카드 트랜잭션의 반전이다. 이것은, 상인 IPSP 시스템(3)을 통해, 온라인 상인에 의해 시작되고 동의되는 환불과는 상이하다. 트랜잭션 보고는, 상인 IPSP 시스템(3)을 통해 승인되고 선택적으로 지불된, 축적된 트랜잭션들에 대한 개관 보고 기능을 제공함으로써, 상인은 예컨대, 날짜 범위를 선택하여 선택된 날짜 범위내에서 행해지는 모든 트랜잭션들에 관한 개관을 볼 수 있다. 상인 IPSP 시스템(3)은 보안 온라인 웹사이트를 가진 온라인 상인을 제공할 수 있고, 그에 의해서, 설명된 바와 같이, 지불거절의 허가, 환불의 시작 및/또는 트랜잭션 보고의 관람을 할 수 있다.

[0018] 하지만, 상기한 제1 및 제2 타입의 결제 시스템들의 각각에 있어서, 구매자는, 각각의 상이한 온라인 상인과 시작되는 트랜잭션들에 대해서 별개로 구매자의 결제 정보를 제공하도록 요구받는다. 따라서, 구매자가 상호 작용하는 각각의 새로운 온라인 상인에 대해서, 구매자의 금융 데이터의 부정한 사용, 착복 및/또는 노출의 위험이 증가한다.

[0019] 제3 타입의 장치(도시되지 않음)에 있어서, 온라인 상인 시스템은, 트랜잭션을 완료하기 위해서 구매자가 상호작용하는 대안의 결제 시스템 웹사이트로 구매자를 돌린다. 대안의 결제 시스템은, 그들의 은행 계정으로부터 직접적으로 또는 결제 카드와 같은 메커니즘을 통해서, 결제를 대안의 결제 시스템으로 제공하는 사용자와 직접

적으로 상호 작용한다. 일반적인 결제 스킴으로부터의 결제 카드가 사용되는 경우에, 대안의 결제 시스템이, 승계 은행을 통해 결제 요구를 제출하는, 일반적인 결제 시스템에 있어서의 상인의 역할을 행한다. 사용자로부터의 결제는 대안의 결제 시스템에 대해 이루어진다. 대안의 결제 시스템은 그 다음에 상인의 임의의 변상에 대해 책임이 있다. 제2 사례에 있어서, 대안의 결제 시스템은, 사실상, 사용자의 계정을 직접적으로 인출하는 것에 의해 사용자의 실제 개설 은행 계정으로부터 대안의 결제 시스템내에서의 사용자의 계정을 자금 조달하는, 일반적인 어음 교환소(clearing house)로서 작용한다. 대안의 결제 시스템은 그 다음에, 대개 일반적인 어음 교환소를 통해서, 상인의 개설 은행 계정으로 보내지는 결제를 보장한다. 이러한 상인 은행 계정은, 그들의 일반적인 승계 시스템으로 유지되는 그들의 계정과 동일할 수도 동일하지 않을 수도 있다. 따라서, 대개의 제3 타입의 시간 결제 시스템은 중개자로서 작용을 하여 사용자로부터 실제 자금을 취해서 그것들을, 가장 일반적으로 소비자의 그리고 상인의 개별적인 은행 계정들 - 그것들이 결제 시스템에 의해 유지되는 계정들을 통과함에 따라 그 자금들을 잠재적으로 보유함 - 을 통해서, 상인에게 패스한다: 이러한 제3 타입의 결제 시스템의 일 예는 주지의 PayPal™ 결제 시스템을 포함한다. 그러한 결제 시스템은, 예컨대, 관련 온라인 결제 처리 서비스를 제공하는 것에 의해, 일반적인 IPSP로서 동작할 능력을 또한 가질 수 있다.

[0020] 이러한 타입의 결제 시스템은, 사용자가 온라인 상인 단위로 개별적인 결제 계정들을 설정할 필요를 경감시키지만, 사용자는 대안의 결제 시스템과 관계를 갖고 온라인 상인 시스템과는 관계를 갖지 않으며; 이것은 몇몇의 주목할 만한 단점들을 증가시키는데: 1차적으로, 이러한 트랜젝션들에 대해서, 상인과 카드 결제 스킴간에 직접적인 관계가 없기 때문에, 온라인 상인은 승계 은행으로부터 직접적으로 결제를 받지도 않고, 결제의 결제-스킴 기반의 보증 그 자체가 쓸모 있을 수도 없다. 2차적으로, 카드 결제를 통해 실행되는 트랜젝션들에 대해서, 구매자는, 제품을 구입한 개별적인 온라인 상인을 알지 못한다(대신에 카드 청구서가 대안의 결제 시스템 엔터티를 식별한다). 3차적으로, 트랜젝션이 결제 시스템에 의해서이고, 온라인 상인 시스템에 의해서는 아니기 때문에, 구매자는 카드 스킴의 규칙들에 의해 보호되지 않고 임의의 적용 가능한 소비자 보호에 의해 보호되지 않을 수 있다.

발명의 내용

[0021] 본 발명의 적어도 하나의 실시예에 의하면, 독립 청구항들에 기재되는 바와 같이, 온라인 상인을 대행하여, 데이터 통신 네트워크를 통해 행해질 결제 트랜젝션들에 대한 결제 승인 요청들을 처리하기 위한 시스템 및 소프트웨어가 제공된다. 이것은 각각의 독립 청구항에 열거된 피쳐(feature)들의 조합에 의해 달성된다. 따라서, 종속 청구항들은 본 발명의 보다 상세한 구현들을 규정한다.

[0022] 보다 상세하게, 본 발명의 양태들은, 온라인 상인들을 대행하여 데이터 통신 네트워크를 통해 행해질 결제 트랜잭션(payment transaction)들에 대한 결제 승인 요청들을 처리하는 방법이고, 상기 결제 승인 요청들은 복수의 상이한 온라인 상인 시스템들을 통한 금융 수단 소유자(financial instrument holder)들에 의한 오더(order)들의 결과로서 행해지며, 상기 온라인 상인들의 각각은 온라인 상인 신원(online merchant identity)을 갖고, 상기 온라인 상인들의 각각은 복수의 승계 은행(acquiring bank) 중 하나와 관련되는 방법으로서,

[0023] 상기 방법은, 결제 승인 요청들을 복수의 상이한 온라인 상인 인터넷 결제 서비스 제공자(Internet Payment Service Provider; "IPSP") 시스템들의 각각에 송신하도록 이루어지는, 신뢰 중앙 중개 시스템(trusted central intermediary system)에 의해 행해지고,

[0024] 상기 상인 IPSP 시스템들의 각각은 결제 승인 요청들을 복수의 승계 은행 결제 처리기 시스템들 중 적어도 하나에 송신하도록 이루어지며, 상기 복수의 승계 은행 결제 처리기 시스템들의 각각은 상기 승계 은행들 중 적어도 하나에 대해서 결제 승인들을 처리할 책임이 있고,

[0025] 상기 방법은:

[0026] 제1 온라인 상인에 대해서 결제 승인 요청들을 발생시킬 책임이 있는 제1 온라인 상인 시스템으로부터 결제 트랜젝션의 승인에 관련된 결제 승인 요청을 수신하는 단계로서, 상기 수신되는 결제 승인 요청은 금융 수단 소유자가 상기 제1 온라인 상인 시스템을 통해 오더를 행하는 것의 결과로서 시작되는, 단계;

[0027] 상기 요청을 수신한 것에 응답하여:

[0028] a) 다음의 i), ii) 및 iii)를 포함하는 트랜젝션 데이터를 포함하는 결제 승인 요청을 생성하는 단계:

[0029] i) 상기 금융 수단 소유자에 의해 상기 결제 트랜젝션에 사용될 금융 수단 신원;

[0030] ii) 결제 트랜젝션 수익자(payment transaction beneficiary)로서, 상기 제1 온라인 상인과 관련되는, 온라인 상인 신원; 및

[0031] iii) 결제 금액을 포함하는 하나 이상의 트랜젝션 명세(transaction detail);

[0032] b) 상기 제1 온라인 상인과 관련되는 선택된 상인 IPSP 시스템으로의 결제 승인 요청 데이터의 송신을 가능케 하도록 송신 데이터를 검색하는 단계; 및

[0033] 상기 검색된 송신 데이터에 기초하여, 상기 생성된 결제 승인 요청을 상기 선택된 상인 IPSP 시스템 - 그로부터 추가적인 결제 승인 요청이 생성되어, 상기 제1 온라인 상인이 관련되는 승계 은행에 대한 결제 승인들을 처리할 책임이 있는 승계 은행 결제 처리기 시스템으로 송신될 수 있음 - 에 송신하는 단계를 포함하는 방법을 제공한다.

[0034] 바람직하게 상기 방법은, 상기 결제 트랜젝션에 사용하기 위한 복수의 상이한 금융 수단들 사이에서의 상기 금융 수단 소유자에 의한 선택을 나타내는 데이터를 수신하는 것, 및 상기 나타내어진 선택을 기초로 하여 상기 생성된 결제 승인 요청에 사용될 금융 수단 신원을 검색하는 것을 포함한다. 상이한 금융 수단들은 신뢰 중개 시스템에 의해 로컬 스토어(local store) 또는 사용자 월릿(user wallet)에 유리하게 보유된다. 따라서, 본 발명의 실시예들은 금융 수단 소유자 또는 사용자로 하여금, 사용자가 개개의 온라인 상인 시스템들에 또는 그것들의 상인 IPSP 시스템들에 지급 명세를 제공하는 요구 사항을 없애면서, 트랜젝션 단위의 결제 방법을 선택할 수 있게 한다. 따라서, 온라인 상인들 또는 그들의 상인 IPSP들이 상기 방법을 행하도록 이루어진 서비스에 기명 승낙하는 것을 조건으로, 사용자들은 그들의 개개의 지급 명세를, 바람직하게 한번만, 분리된 신뢰 엔터티에 제출하는 것만이 필수이다. 이것은, 사용자가 각각의 트랜젝션에 관하여 개인적인 그리고 금융의 정보를 입력할 필요가 없기 때문에, 사용자로 하여금 보다 신속하고 편리하게 트랜젝션들을 실행할 수 있게 하면서, 결제 시스템들의 일반적인 장치에 관하여 초래될 수 있는 사기의 위험을 감소시키는 이익을 갖는다.

[0035] 결제 수단 명세들이 있는 사용자 월릿의 개체수에 대해서, 신뢰 중앙 중개 시스템이 금융 수단 소유자를 위한 등록 인터페이스(registration interface)를 바람직하게 제공하여, 금융 수단 소유자가 상기 신뢰 중앙 중개 시스템에 대해서 등록을 위한 금융 수단 신원을 저장된 등록 데이터로서 제공할 수 있다. 결제 승인 요청을 처리할시에, 상기 방법은, 금융 수단 소유자를 승인하고, 그에 응답하여, 상기 저장된 등록 데이터로부터, 상기 생성된 결제 승인 요청에 사용될, 바람직하게 사용자 월릿으로부터의, 등록된 금융 수단 신원을 검색하는 단계를 포함한다.

[0036] “온라인 상인”, “상인 IPSP 시스템”, “신뢰 중앙 중개 시스템” 및 “승계 은행 결제 처리기 시스템”이라는 용어들은 논리적 구성 요소들이라는 것이 이해되어 진다. 그리하여, 각각의 시스템은 서로 물리적으로 분리되어 실시되거나 하나 이상의 다른 시스템에 물리적으로 연결될 수 있다. 예를 들면, 소정의 조직이 상인 IPSP 시스템 및 온라인 상인을 호스팅하는 경우의 장치에 있어서, 구성 요소들은 동일한 네트워크상에 물리적으로 위치되거나 심지어 단일 시스템의 일부로서 통합될 수 있다. 또한, 소정의 조직이 상인 IPSP 시스템 및 승계 은행 결제 처리기 시스템을 호스팅하는 경우에, 구성 요소들은 동일한 네트워크상에 물리적으로 위치되거나 심지어 단일 시스템의 일부로서 통합될 수 있다. 또, 단일 조직이 온라인 상인, 상인 IPSP 시스템 및 승계 은행 결제 처리 시스템을 호스팅할 수 있다. 따라서, 본 발명의 실시예들은, IPSP의 역할 하에 실행되는 기능들이, 상인이기도 한 그리고/또는 승계자이기도 한 조직에 의해 수행될 수 있는 장치들을 포함한다.

[0037] 본 발명의 시스템을 이용하여 승인되는 트랜젝션들이 여전히 상인 IPSP 시스템에 의해 처리되기 때문에, 이러한 트랜젝션들에 관련된 상인 IPSP 기능들은 상이한 트랜젝션 타입들에 공통인 인터페이스를 이용하여 온라인 상인에 의해 액세스될 수 있다. 이러한 트랜젝션 타입들은, 신뢰 중개 시스템을 통해서 발생하는 결제 승인 요청들에 대한 트랜젝션 타입들, 및 신뢰 중개 시스템을 통해 패스하지 않고 상인을 대행하여 IPSP에 의해 처리될 수 있는 다른, 분리적으로 승인되는, 트랜젝션 타입들의 양쪽을 포함할 수 있다. 이러한 공통의 인터페이스는 보안 온라인 웹사이트를 포함할 수 있다.

[0038] 적어도 하나의 장치에 있어서, 신뢰 중앙 중개 시스템은 상기 선택된 상인 IPSP 시스템으로부터 결제 승인 응답을 수신하고, 그에 응답하여 결제 승인 응답을 상기 제1 온라인 상인 시스템에 송신한다. 또한, 상기 방법은 상기 제1 온라인 상인 시스템으로부터 온라인 상인 신원을 수신하는 것을 포함하고, 상기 생성된 승인 요청에 포함되는 상기 온라인 상인 신원은 상기 수신되는 온라인 상인 신원에 기초하여 생성된다. 따라서, 신뢰 중개 시스템이, 새로 바꾸기 보다는, 온라인 상인의 기존의 IPSP 시스템과 인터페이스를 하기 때문에, 그것은 승계 은행에 송신되는 온라인 상인의 계정 식별자이다. 결과적으로, 구매자와 온라인 상인 사이에는, 구매자가 카드

스킴의 규칙들에 의해 보호되고, 일부의 우발성에 있어서, 임의의 적용 가능한 소비자 보호를 준수하는 결과적인 이익이 있는 그러한 트랜젝션들에 대한 관계가 있다. 또한, 온라인 IPSP 시스템은, 온라인 상인 시스템을 대행하여, 하나 이상의 추가적인 다양한 트랜젝션 처리 기능들, 예컨대 지불, 지불거절의 처리, 환불의 처리, 및 트랜젝션 보고를 제공할 수 있다. 특히, 상인 IPSP 시스템은 보안 온라인 웹사이트가 있는 온라인 상인을 제공하여, 그에 의해 본 발명의 시스템을 통해 승인된 트랜젝션들에 관한 트랜젝션 보고들의 관람, 환불의 개시 및/또는 지불거절의 허가를 할 수 있다.

[0039] 바람직하게, 상기 결제 승인 요청 데이터의 제1 온라인 상인과 관련되는 선택된 상인 IPSP 시스템으로 송신을 가능케 하기 위해 송신 데이터를 검색하는 단계는, 상기 제1 온라인 상인에 의해 등록된 상기 상인 IPSP 시스템에 기초하여 상기 선택된 상인 IPSP 시스템에 대한 네트워크 어드레스를 검색하는 것을 포함하고, 상기 생성된 결제 승인 요청을 선택된 상인 IPSP 시스템에 송신하는 단계는 상기 검색된 네트워크 어드레스에 기초하여 상기 생성된 결제 승인 요청을 송신하는 것을 포함한다. 예컨대, 소정의 온라인 상인이 신뢰 중개 시스템에 등록할 때, 네트워크 어드레스가 온라인 상인 단위로 바람직하게 거주됨으로써, 결제 승인 요청들의 흐름을 제어하기 위한 편리하고, 집중화된 메커니즘을 제공한다. 따라서, 신뢰 중앙 중개 시스템이 온라인 상인들을 위한 등록 인터페이스를 제공함으로써, 소정의 온라인 상인이, 온라인 상인이 관련되는 상인 IPSP 시스템을 등록할 수 있다.

[0040] 적어도 일부의 장치에 있어서, 상기 신뢰 중앙 중개 시스템은, 각각이 상이한 개설 은행(issuing bank)에 대해서 승인을 행할 책임이 있는, 복수의 개설 승인 시스템(issuing authentication system)과 협력하고, 상기 방법은 상기 금융 수단 소유자의 신원을 확인하기 위해서 개개의 개설 승인 시스템과 선택적으로 통신하는 단계를 포함한다. 이러한 사용자의 확인은 주지의 3-D 보안 방법을 이용하여 행해질 수 있고, 예컨대, 사용자가 상기한 등록 인터페이스를 통해 그들의 사용자 월릿에 결제 수단을 추가할 때 행해질 수 있다.

[0041] 사용자는: 중개 시스템과 직접적인; 신뢰 써드 파티(third party)를 통해 간접적인: 그리고 온라인 뱅킹 서비스를 통한 전향(re-direction)을 포함하는 몇몇의 상이한 메커니즘을 통해서 신뢰 중개 시스템에 등록할 수 있다. 제3의 대안에 관련하여, 상기 방법은 상기 복수의 개설 승인 시스템 중 선택된 것에 의한 상기 금융 수단 소유자의 승인에 기초하여 상기 생성된 결제 승인 요청에 사용될 금융 수단 신원을 검색하는 단계를 포함한다. 그 후에, 상기 금융 수단 소유자에게 데이터가 송신되어, 상기 금융 수단 소유자가 선택된 승인 시스템에 관한 승인을 행할 수 있게 하며, 상기 선택된 개설 승인 시스템에 의한 상기 금융 수단 소유자의 승인에 응답하여 상기 선택된 승인 시스템으로부터 승인 응답 데이터를 수신한다. 또한, 본 발명의 실시예들은, 상기 선택된 개설 승인 시스템에 의한 상기 금융 수단 소유자의 승인에 응답하여 상기 선택된 개설 승인 시스템으로부터, 상기 생성된 결제 승인 요청에 사용될 금융 수단 신원을 나타내는 데이터를 수신하는 것을 포함할 수 있다.

[0042] 본 발명의 추가적인 양태들에 의하면, 복수의 온라인 상인 시스템 및 복수의 상인 IPSP 시스템과 통신하는 신뢰 중개 시스템이 제공되며, 상기 신뢰 중개 시스템은 상기한 신뢰 중개 시스템 단계들을 행하도록 이루어진다. 또한, 신뢰 중개 시스템 및 복수의 상인 IPSP 시스템과 통신하는 온라인 상인 시스템이 제공되며, 상기 온라인 상인 시스템은 상기한 온라인 상인 시스템 단계들을 행하도록 이루어진다. 또, 신뢰 중개 시스템 및 복수의 온라인 상인 시스템과 통신하는 상인 IPSP 시스템이 제공되며, 상기 상인 IPSP 시스템은 상기한 상인 IPSP 시스템 단계들을 행하도록 이루어진다.

[0043] 본 발명의 양태들은 상기한 방법을 실행하도록 적절히 구성된, 다양한 시스템들간에 배포되는 소프트웨어를 또한 제공한다.

[0044] 본 발명의 추가적인 특징들 및 장점들은, 첨부 도면을 참조하여 이루어지는, 예시로서만 주어지는, 본 발명의 바람직한 실시예들의 하기의 설명으로부터 명백해질 것이다.

도면의 간단한 설명

[0045] 도 1은 일반적인 결제 시스템을 나타내는 개략도이다.

도 2는 본 발명의 일 실시예에 따른 결제 시스템을 나타내는 개략도이다.

도 3은 본 발명의 일 실시예에 따른 도 2의 결제 시스템의 사용 동안의 데이터의 흐름을 나타내는 개략적인 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 도 2의 신뢰 중개 시스템의 구성 요소를 나타내는 대략적인 블록도이다.

도 5는 본 발명의 일 실시예에 따른 도 2의 결제 시스템의 선택된 구성 요소들간의 메시지들의 흐름을 나타내는 개략적인 타이밍도이다.

발명을 실시하기 위한 구체적인 내용

[0046] 상기한 바와 같이, 본 발명의 실시예들은 결제 시스템 및 방법, 특히 온라인 상인을 대행하여 데이터 통신 네트워크를 통해 행해질 결제 트랜젝션들에 대한 결제 승인 요청들을 처리하는 시스템 및 방법에 관한 것이다. 시스템은, 도 1과 관련되는 배경 기술 섹션에서 설명된 일반적인 결제 엔터티들과 협력하는 신뢰 중개 시스템에 대해 여기에 언급되는, 신규한 트랜젝션의 엔터티를 수반한다.

[0047] 도 2는 본 발명의 일 실시예에 따른 결제 시스템(1)의 개략도를 묘사한다. 신뢰 중개 시스템(10)은 복수의 상이한 상인 IPSP 시스템들(3a ... 3c)의 각각에 결제 승인 요청들을 송신하는 것으로서 도시되어 있다. 온라인 상인 처리 시스템들(1a ... 1c)의 각각은 온라인 상인들 중 하나(1c)에 대해 점선(L1)에 의해 표시되는 바와 같이 상인 IPSP 시스템들(3a ... 3c) 중 하나와 관련됨과 더불어, 다시금 온라인 상인(1c)에 대해, 점선(L2)에 의해 표시되는 바와 같이, 승계 은행들 중 하나(5c)와 관련된다. 상인 IPSP 시스템들 중 적어도 일부(3b, 3c)는 하나보다 많은 승계 은행에 결제 승인 요청들을 송신하도록 이루어질 수 있고; 이것은 하나보다 많은 온라인 상인이 주어진 상인 IPSP 시스템을 통해 그들의 결제들을 처리할 수 있다는 사실을 반영하며; 각각의 상인은 특정 승계 은행의 계정을 갖는다.

[0048] 또한, 각각의 온라인 상인 시스템(1a ... 1c) 웹사이트의 오더 송신 웹페이지는, 신규한 결제 옵션으로서, "결제의 보안 시스템(Secure System of Payment)"(SSP)으로서 여기에 칭해지는 것을 포함하며, 이것은 신뢰 중개 시스템(10)을 통한 결제를 식별한다. 일반적인 온라인 결제 옵션들을 포함하는 다른 결제 옵션들이 또한 포함될 수 있고, 그에 의해 구매자는 신뢰 중개 시스템(10)을 통해 처리되는 결제 승인을 수반하지 않는 결제 옵션을 선택할 수 있다. 그와 같이 분리적으로 승인된 트랜젝션들은, 예컨대, 신뢰 중개 시스템(10)을 이용하는 것보다는, 바이어가 그들의 결제 명세들을 온라인 상인 시스템(1c)에 직접적으로, 또는 온라인 IPSP 시스템(1c)에 직접적으로 입력하는 일반적인 온라인 결제 옵션들을 포함할 수 있다. 그러한 트랜젝션들에 관하여, 신뢰 중개 시스템(10)은, 신뢰 중개 시스템(10)에 의해 제공되는 서비스에 가입할 때 온라인 상인의 기존 상인 IPSP 시스템일 수 있는 온라인 상인 IPSP 시스템(3c)과, 그것을 대체하기 보다는, 인터페이싱한다. 이것은, 본 발명의 실시예들에 따른 결제 시스템이 기존의 그리고 주지의 세트의 처리 엔터티들내에 신뢰 중개 시스템(10)의 추가를 수반하기 때문에, 결제들이, 추가적으로, 또는 대안적으로, 신뢰 중개 시스템(10)을 통해, 도 1을 참조하여 설명된 제2 타입 및 제3 타입의 장치를 이용하는 종래의 방법들에 따라 이루어질 수 있다는 것을 말한다.

[0049] 신뢰 중개 시스템(10)은, 트랜젝션 데이터와 함께, 중개 시스템(10)에 등록된 온라인 상인들 및 사용자들(구매자들)에 대응하는 데이터베이스(DB1)에 데이터를 보유한다. 보다 상세히 후술될 바와 같이, 데이터베이스(DB1)는 여기서 리모트 스토어(remote store) 또는 사용자 월릿으로 편의상 칭해지는 저장된 일련의 레코드(record)들의 형태로 사용자에 대한 일련의 결제 명세들을 보유하며; 사용자들이, 신뢰 중개 시스템으로 하여금 유저의 리모트 스토어의 내용들을 갱신시키는, 트랜젝션에 대한 결제를 하게끔 선택할 수 있는 결제 수단들(일반적으로 카드 및 계정)의 명세를 추가할 수 있다. 신뢰 중개 시스템(10)이 사용자에게 가용한 다양한 결제 수단을 보유하기 때문에, 사용자는 트랜젝션 단위의 결제 방법을 선택할 수 있다. 따라서, 온라인 상인들이 신뢰 중개 시스템(10)에 가입한 것을 조건으로, 사용자는 단일 엔터티에 그들 개개의 결제 명세를 1회만 반드시 제출하고, 그에 의해, 사용자가 그들이 온라인을 쇼핑할 때마다 개개의 온라인 상인들에게 결제 명세를 제출할 요구사항을 없앤다. 이것은, (도 1에 나타내어진 것과 같은) 결제 시스템의 일반적인 장치에 관하여 초래될 수 있는 사기의 위험을 감소시키는 이익을 갖는다.

[0050] 신뢰 중개 시스템(10)을 이용하여 발생되는 트랜젝션 승인 요청들이 IPSP 시스템(3c)에 패스되고, IPSP 시스템(3c)에 의해 처리되기 때문에, 이러한 트랜젝션들에 관한 IPSP 기능들을 처리하는 추가적인 다양한 트랜젝션이 신뢰 중개 시스템(10)을 통해 온라인 상인에 의해 엑세스될 수 있다. 상인 IPSP 시스템(3c)은, 온라인 상인 시스템(1c)을 대행하여, 기능들, 예컨대, 지불, 지불거절의 처리, 환불의 처리, 및 트랜젝션 보고를 처리하는 하나 이상의 그러한 추가적인 트랜젝션을 제공할 수 있다. 상인 IPSP 시스템(3c)은 보안 온라인 웹사이트가 있는 온라인 상인을 바람직하게 제공하여, 그에 의해서, 신뢰 중개 시스템(10)을 통해 승인된 트랜젝션들에 관한 트랜젝션 보고의 관람, 환불의 시작 및/또는 지불거절의 허가를 한다.

[0051] 또한, 신뢰 중개 시스템(10)을 이용하여 발생하는 트랜젝션 승인 요청들이 IPSP 시스템(3c)에 패스되고 IPSP 시스템(3c)에 의해 처리되므로, 이러한 트랜젝션들에 관한 IPSP 기능들은, 신뢰 중개 시스템(10)을 통해 승인되는

트랜젝션 타입들, 및 신뢰 중개 시스템(10)을 통해 패스하지 않고 상인을 대행하는 IPSP에 의해 처리될 수 있는 다른, 분리적으로 승인되는, 트랜젝션 타입들의 양쪽을 포함하는, 상이한 트랜젝션 타입들에 공통인 IPSP 시스템 인터페이스를 이용하여 온라인 상인에 의해 액세스될 수 있다. 그러한 분리적으로 승인되는 트랜젝션들은, 예컨대, 상인 IPSP 시스템(1c)에 의해 수행되는 결제 승인들에 사용하기 위해, 구매자가 그들의 결제 명세를 온라인 상인 시스템(1c)에 직접적으로, 또는 상인 IPSP 시스템(3c)에 직접적으로 입력하는 트랜젝션들을 포함할 수 있다.

[0052] 또한, 결제 승인 요청의 일부로서 상인 IPSP 시스템(3c)에 의해 승계 은행(5c)에 송신되는 것이 온라인 상인 인터넷 계정 식별자이다. 이것은, 구매자가 카드 스킴의 규칙에 의해 보호되고, 일부의 우발성에 있어서, 임의의 적용 가능한 소비자 보호를 준수하는 것을 보장하는 이익을 갖고; 추가적으로 각각의 트랜젝션은 사용자의 카드 청구서를 기초로 온라인 상인마다 식별될 수 있다.

[0053] 도 2로부터, 특히 점선(L3)로부터 알 수 있는 바와 같이, 신뢰 중개 시스템(10)은 개설 은행 시스템(9a)에 연결되어 있다(하나의 연결만이 도시되었지만, 신뢰 중개 시스템(10)과 임의의 개수의 개설 은행 시스템들간에 연결이 있을 수 있다는 것이 이해되어 진다). 이러한 연결은 주지의 3-D 보안 승인 메커니즘을 이용하여 카드 소지자(구매자)의 확인을 촉진시킨다. 3-D 보안에 대한 프로토콜은, 그 내용이 그 전체로서 참조로 이 명세서에 통합되어 있는 비자 국제 서비스 협회(Visa International service Association)의, 공개 번호 US2002/0194138하에 공개된, 미국 특허 출원 10/156,271에 기록되어 있다. 상기 프로토콜은 상기한 특허 공개 공보에서 지불인 승인 서비스(Payer Authentication Service; “PAS”)로서 기록되어 있는 바와 같은, 보안 소켓 층(Secure Sockets Layer; “SSL”)을 통해 송신되는 메시지들(일반적으로 XML 메시지들)을 이용한다. 이러한 서비스는, 신뢰 중개 시스템(10)이, 고가의 제품의 외국으로의 선적을 수반하는 트랜젝션에 대한 사례일 수 있는 바와 같이, 미리 정해진 레벨의 위험에 대응하는 소정의 요청된 트랜젝션을 판정할 때, 채용될 수 있다. 위험 평가가 행해지는 수단 및 게다가 소정의 트랜젝션에 대해 판정되는 위험 레벨이 보다 상세하게 후술된다.

[0054] 카드 스킴 시스템(7)은 점선(L4)에 의해 개략적으로 나타내어진 바와 같이 신뢰 중개 시스템(10)에 통신적으로 연결되어 있으며, 이것은, 신뢰 중개 시스템(10)이 카드 스킴 시스템(7)에 의해 제공되는 계정 갱신 서비스(도 2에 참조 번호가 부여되어 있지 않지만, 부분(415d)으로서 후술되는 도 4를 참조하여 설명됨)에 가입되었고, 그렇기 때문에, 예컨대, 카드가 분실되거나, 도난당하거나 만료되었고, 따라서 사용자에게 재발행되었을 때의, 갱신된 카드 정보를 수신하는 것을 나타낸다. 그러한 서비스의 일 예는 비자 계정 갱신기 서비스(Visa Account Updater service; “VAU”)이고, 다른 서비스가 마스터카드 자동 과금 갱신기(Mastercard Automatic Billing Updater)이다. 하나의 장치에 있어서 카드 스킴 시스템(7)에 의해 제공되는 계정 갱신 서비스에 대한 인터페이스는 배치(batch) 지향이다: 신뢰 중개 시스템(10)은 요청 또는 요청들을 카드 스킴 시스템(7)에 제출하며, 상기 요청은 시스템(10)에 등록된 특정 사용자들의 명세들을 포함한다. 배치 인터페이스는 일반적으로, 재발행된 카드들의 명세들을 수집할 책임이 있는 계정 갱신 서비스에 요청 파일(들)을 송신하는데 사용된다(예컨대, 보안 파일 이송 프로토콜(Secure File Transfer Protocol; “SFTP”) 또는 Connect:Direct(™)). 시간을 둔 후에, 신뢰 중개 시스템(10)은 계정 갱신 서비스를 액세스하여 응답 파일(들)을 수집하며, 그 후 SSP 시스템에 대한 관련 가입자들에 대한 갱신 결제 수단들을 국소적으로 수집한다. 대안적으로 인터페이스는 메시지-기반일 수 있고, 그래서 개개의 주 계정 번호가 실시간으로 확인되거나 갱신될 수 있다. 카드 스킴 시스템(7)에 직접적으로 요청을 송신하는 것에 대한 대안으로서, 신뢰 중개 시스템(10)은, 예컨대, 카드 스킴 시스템(7)으로의 후속의 포워딩(forwarding)에 대해서, 주지의 승계 은행 시스템들(5a ... 5c)에 요청을 송신하는 온라인 상인의 동작을 대리 실행(emulate)할 수 있다.

[0055] 이제 도 3을 참조하여 보면, 본 발명의 일 실시예에 따른 결제 시스템(1)의 동작이 이제 설명될 것이다. 단계(S301)에서, 사용자는 온라인 상인 C의 온라인 상인 시스템과의 그들의 쇼핑 체험을 완료하고, 온라인 상인 시스템을 이용하는 체크아웃(checkout)을 시작하며, 당업자에게 주지되어 있는 체크아웃 소프트웨어 패키지 및 공통적으로 사용할 수 있는 쇼핑 카트를 통해 가용한 일반적인 방법들에 따라, 가상의 체크아웃을 진행한다. 사용자가 결제 옵션으로서 “결제를 위한 보안 시스템(Secure System for Payment)”(SSP)을 선택하여(단계 S301), 온라인 상인 시스템(1c)으로 하여금, 발생한 결제 인증 요청 메시지를 신뢰 중개 시스템(10)에 송신하게 한다(단계 S303); 상기 발생한 요청 메시지는 오더를 위한 식별자, 온라인 상인 계정 식별자 및 선택된 제품에 대한 결제 금액을 적어도 포함한다. 신뢰 중개 시스템(10)은 그 다음에 로그인 URL을 사용자에게 송신하여(단계 S305), 사용자에게 로그인하도록 프롬프트(prompt)하고, 또는, 이것이 결제 옵션으로서 SSP를 선택하는 그들의 첫 번째 시간일 경우에, 신뢰 중개 시스템(10)에 등록하도록 프롬프트한다. 본 예의 목적을 위해 사용자가 사전에 서비스에 등록했다는 것을 가정하면, 사용자는 그들의 로그인 자격 증명서(예컨대, 신뢰도는 중개 시스

템(10)에 의해 활용되는 승인 메커니즘에 따라, 사용자 이름, 패스워드, 또는 다른 승인 명세들)를 입력한다(단계 S307).

[0056] 신뢰 중개 시스템(10)은 그 다음에 사용자의 자격 증명서 및 식별 명세에 의거하여 룩업(lookup)을 실행하고(단계 S309), 데이터베이스(DB1)로부터 사용자의 리모트 스토어로부터의 명세들을 검색하며, 사용자에게, 그들의 결제 방법의 선택을 위해, 검색된 명세들을 프리젠테이션한다(단계 S310). 사용자의 리모트 스토어로부터 검색되는 명세들에 따라 제공되는 옵션들로부터 희망하는 결제 방법의 선택시에, 신뢰 중개 시스템(10)은 결제 승인 요청 메시지를 온라인 상인의 IPSP 시스템(3c)에 송신하며, 결제 승인 요청 메시지는 선택된 결제 수단 명세, 요구되는 결제 금액 및 온라인 상인 식별자를 포함한다(단계 S311). 상인 IPSP 시스템(3c)은 추가적인 결제 승인 요청을 관련 승계 은행(5c)에 송신하여(단계 S313), 일반적인 방벌들에 대한 승인(또는 그 외)을 프롬프트하고(단계 S315) 및 승계 은행(5c)로부터의 응답 메시지의 상인 IPSP 시스템(3c)로의 송신을 프롬프트한다(단계 S317). 단계(S319)에서, 승인된 결제의 확인을 포함하는 응답을 가정하여 보면, 상인 IPSP 시스템(3c)은 결제 성공 통지 메시지를 신뢰 중개 시스템(10)에 송신한다. 이러한 결제 성공 통지 메시지는 카드 스킴 승인에 대한 레퍼런스(reference) 및 카드 스킴 트랜젝션에 대한 트랜젝션 식별자를 포함한다.

[0057] 그 후, 신뢰 중개 시스템(10)은 결제 성공 확인 메시지를 온라인 상인 시스템(1c)에 송신하고(단계 S321), 그것은 사용자에게 오더 상태를 확약시키도록 온라인 상인 시스템을 프롬프트한다(단계 S323).

[0058] 상기한 것으로부터, 일반적인 온라인 상인 시스템들(그것들의 상인 IPSP 시스템을 포함)이 결제 옵션으로서 "결제를 위한 보안 시스템"(SSP)을 포함하도록 그리고 게다가 신뢰 중개 시스템(10)과 인터페이싱하도록 수정할 것을 요구한다는 것이 이해될 것이다. 따라서, 상인 IPSP 시스템은, 결제 수단(일반적으로 카드 및 은행 계정)에 대한 결제 및 지불을 가능케 하는 결제 승인 서비스를 신뢰 중개 시스템(10)에 노출한다. 또한, 신뢰 중개 시스템(10)이 많은 상인 IPSP 시스템들과 일체화하기 때문에, 그것은 따라서, 각각이 개개의 상인 IPSP 시스템에 대응하는, 복수의 인터페이스 포맷 및 프로토콜을 포함한다는 것이 이해될 것이다. 추가적으로, 각각의 온라인 상인의 시스템은, 결제 방법으로서 SSP를 이용하는 결제 트랜젝션을 시작하기 위한 목적으로, 온라인 상인으로 하여금 신뢰 중개 시스템(10)과 일체화하는 것을 가능케 하는, 예컨대, 플러그인(plugin) 형태의, 통합 소프트웨어 구성 요소들로 구성되어 있다.

[0059] 신뢰 중개 시스템(10)의 구성 및 처리 능력의 세부가 이제 도 4를 참조하여 설명될 것이다. 신뢰 중개 시스템(10)은 다양한 사용자-특정의 그리고 상인-특정의 데이터를 송신 및 관리하도록 구성되어 있는, 프리젠테이션(presentation) 및 연결성 처리 구성 요소들을 포함한다; 이러한 처리 구성 요소들은 보다 상세히 후술될 것이지만, 개략적으로 그것들은 다음을 포함한다:

[0060] **사용자 등록 요소 및 데이터**

[0061] 사용자가 신뢰 중개 시스템(10)에 등록하기를 원할 때, 그들은 사용자가 SSP 서비스에 계정을 생성하는 것을 가능케 하는 계정 등록 처리를 완료하도록 요구받는다. 계정은, 서비스를 제공하는 온라인 상인 시스템으로부터 SSP 서비스로부터의 결제를 하는데 사용될 수 있는 적절한 데이터와 거주될 것이 요구된다.

[0062] 일단 등록되면, 각각의 사용자는, 금융 트랜젝션을 실행할 때 그들이 차변할 것을 희망하는 계정들의 명세들을 저장하는, 그와 관련된 일련의 레코드들을 갖는다. 이것은, 은행 계정, 결제 카드 또는 고유한 계정 레퍼런스가 주어질 수 있는 임의의 결제 수단과 같은 다른 계정일 수 있다. 신뢰 중개 시스템(10)은, 사용자로 하여금 결제 수단들의 목록으로부터 선택 및 추가/제거를 할 수 있게 하는 프리젠테이션 요소(404)를 포함한다. 추가적으로, 사용자는 선적 세부를 보유하는 어드레스 북(address book) 엔터티를 갖는다; 프리젠테이션 요소(404)는 사용자로 하여금 선적 세부를 수정할 수 있게 한다. 각각의 사용자는, 사용자에 대한 인구학 및 식별 데이터를 포함하고 프리젠테이션 요소들(404)을 통해 수정될 수 있는 프로파일(profile)을 갖고, 사용자 트랜젝션 데이터는 사용자에 의한 리뷰(review)를 위해 표시될 수 있다. 도 4에 도시되고 보다 상세히 후술될 바와 같이, 신뢰 중개 시스템(10)은 웹 서버로서 구현될 수 있고, 그 경우에 있어서 프리젠테이션 요소들(404)은 지금 설명되는 방식으로 사용자 데이터의 선택 및 수정을 가능케 하도록 사용자의 브라우저와 상호 운용한다. 하지만, 사용자의 신뢰 중개 시스템(10)에 대한 등록은 임의의 대안적인 적절한 인터페이스를 통해 행해질 수 있다.

[0063] 등록은 다수의 채널들을 통해 실행될 수 있다:

[0064] ● SSP 사이트를 통한 등록 - 사용자는 신뢰 중개 시스템(10)의 웹 사이트에 로그온하며 사용자의 신원 및 바람직한 결제 수단 세부를 캡쳐하도록 설계된 등록 페이지를 프리젠테이션 받는다.

[0065] ● 오더 시스템으로부터의 전향 - 사용자가 온라인 상인의 오더 시스템에 속하고 SSP 옵션을 이용하여 결제를 실행하기를 희망하는 경우에, 그들은, 그들이 이미 등록을 하지 않았다면, 등록을 필요로 할 것이다. 사용자는 신뢰 중개 시스템(10)과 관련된 등록 스크린에 전향되고 그 다음에 온라인 상인의 시스템으로 되 전향된다.

[0066] ● 온라인 은행을 통한 등록 - 신뢰 중개 시스템(10)이 필요한 통합 기능성을 포함한다고 가정하면, 사용자는 그들의 은행의 온라인 계정 서비스내로부터 SSP 서비스에 대한 등록을 할 수 있다.

[0067] **사용자 승인 요소들**

[0068] 결제 트랜젝션들에 대한 신뢰 중개 시스템(10)으로의 사용자의 승인은 하기에 목록화된 3개의 알려진 카테고리들 중 임의의 것에 따라 행해질 수 있다:

[0069] ***1중 승인(1-factor authentication)*** - 사용자가 알고 있는 어떤 것(예컨대, 사용자명 및 패스워드, 패스 프레이즈(pass phrase), 또는 개인 식별 번호(personal identification number; "PIN"))

[0070] ***2중 승인(2-factor authentication)*** - 1중 승인으로서, 더하기, 사용자가 갖는 어떤 것(예컨대, ID 카드, 보안 토큰(token), 소프트웨어 토큰, 전화, 또는 휴대 전화)

[0071] ***3중 승인(3-factor authentication)*** - 2중 승인으로서, 더하기, 사용자가 되어 있거나 하는 어떤 것(예컨대, 지문 또는 망막 패턴, DNA 서열(충분히 다채로운 정의가 있음), 서명 또는 음성 인식, 고유한 생체 전기적 신호, 또는 다른 생물 측정의 식별자)

[0072] 승인을 가능케 하는 메커니즘의 일 예는 상기한 3-D 보안 서비스 - 신뢰 중개 시스템(10)에 의해 촉진됨 - 이고, 개설 은행은 은행 또는 구매자에게만 알려져 있는 패스워드에 대해 구매자에게 프롬프트한다. 상인이 이러한 패스워드만을 알고 그것을 캡쳐하는 것에 대해 책임이 없기 때문에, 그것은 구입자가 사실상 그 카드 소지자라는 증거로서 개설 은행에 의해 사용될 수 있다.

[0073] 일 실시예에 있어서, 신뢰 중개 시스템(10)은 승인 처리를 구현한다. 대안적으로, 사용자는 그 온라인 뱅킹 명세를 통해 로그인할 수 있고, 그 경우에 있어서, 사용자는 그 온라인 뱅킹 계정에 로그인할 것이고, 그로부터 뱅킹 시스템 소프트웨어는 사용자를 신뢰 중개 시스템(10)에 되 전향시킬 것이다. 추가적인 대안으로서, 승인은, 사용자-특정 입력에 기반하여, 사용자를 대행하여 사용자의 계정의 식별을 실행하도록 중개자로서 작용하고 신뢰 중개 시스템(10)과 협력할 수 있는, 계정 식별 엔터티를 수반할 수 있다.

[0074] **온라인 상인 데이터 스토어:**

[0075] 신뢰 중개 시스템(10)은 온라인 상인 프로파일 및 등록 데이터를 저장한다. 이들 데이터는 온라인 상인 시스템이 등록되는 상인 IPSP 시스템(3c)의 트랜젝션 및 네트워크 식별자와 함께 온라인 상인 인터넷 계정 식별자를 포함한다. 이들 데이터는, 온라인 상인 시스템을 대행하여 신뢰 중개 시스템(10)을 상인 IPSP 시스템(3c)과 통신할 수 있게 하도록 보유되고, 상인 IPSP 시스템 송인 데이터, 또는 간단히 송신 데이터로서 집합적으로 칭해진다. 또한, 신뢰 중개 시스템(10)은, 신뢰 중개 시스템(10)은 온라인 상인을 대행하여 결제를 실행하는 결제 승인 서비스를 포함한다. 또한, 신뢰 중개 시스템(10)은 많은 상인 IPSP 시스템들과 일체화하기 때문에, 그것은 복수의 인터페이스 포맷 및 프로토콜을 포함한다. 각각의 상인 IPSP 시스템에 대한 관련 포맷 및 프로토콜의 세부는 온라인 상인 데이터 스토어에 보유되어 있다. 따라서, 상기한 송신 데이터는, 소정의 온라인 상인 시스템으로부터, 결제 승인 요청들이 관련 상인 IPSP 시스템에 라우팅될 수 있게 하는 네트워크 프로토콜, 네트워크 어드레스 및/또는 IPSP 식별자로 나오는 결제 승인 요청의 매핑을 포함한다.

[0076] 따라서, SSP 서비스를 제공하는 임의의 주어진 상인의 등록이, 상인이 그들이 가입한 상인 IPSP 시스템을 식별하는 것을 수반한다는 것이 이해될 것이다. 편리하게, 신뢰 중개자(10)는 활성의 상인 IPSP 시스템들에 대응하는 일련의 레코드들을 보유할 수 있다: 각 세트의 레코드들은 신뢰 중개자(10)에 의해 데이터베이스(DB1)내의 저장을 위한 요구되는 통신 프로토콜 및 네트워크 식별자를 포함할 수 있다. 따라서, SSP에 대한 등록 동안에, 소정의 온라인 상인은, 예컨대, 신뢰 중개자(10)의 프리젠테이션 요소들(404)에 의해 조정되는 드롭 다운(drop down) 목록을 통해서, 온라인 상인이 가입한 상인 IPSP 시스템을 선택할 수 있다; 대응하는 송신 데이터(또는 그에 대한 링크)는 그 다음에 데이터베이스(DB1)에 보유되는 상인 레코드들과 함께 저장될 수 있다. 따라서, 소정의 온라인 상인이 지금 설명하는 방식으로 그 대응하는 상인 IPSP 시스템을 특정하는 것을 조건으로, 그 다음에, 상인 시스템으로부터의 결제 승인 요청의 수신에 응답하여, 신뢰 중개자(10)는 데이터베이스로부터 적절한 룩업을 실행하여 대응하는 상인 IPSP 시스템의 네트워크 식별자, 프로토콜 요건 등을 검색할 수 있다.

[0077] **어플리케이션 프로그래밍 인터페이스(Application Programming Interface; API) 서비스 어댑터(services**

adaptor)

[0078] 신뢰 중개 시스템(10)은 결제 시스템의 메시징 인프라스트럭처와 신뢰 중개 시스템(10)사이의 연결성을 가능케 하는 API 서비스 어댑터를 포함한다. 어댑터는, 상인 IPSP 시스템(3c)에 대한 결제 승인들과 같이, 외부 서비스에 대한 신뢰 중개 시스템(10) 요청의 이행을 관리하고, 상인 IPSP 시스템(3c)과 같이 외부 기능들에 의해 사용될 수 있는 일련의 신뢰 중개 시스템(10) 서비스를 노출하도록 구성되어 있다.

[0079] **트랜젝션-특정 요소들 및 데이터:**

[0080] 신뢰 중개 시스템(10)은, 신뢰 중개 시스템(10)에 의해 관리되는 결제 승인 및 지불과 같은 트랜젝션의 데이터를 저장한다. 또한, 신뢰 중개 시스템(10)은, 사용자 및 온라인 상인 온라인 활동과 함께 일반적인 시스템 활동과 관련된 감사 데이터를 저장할 수 있다.

[0081] **메시징 서비스**

[0082] 신뢰 중개 시스템(10)은, 어드레스 승인과 사용자 활성화 및 구입 오더 확인의 목적을 위한 이메일을 만들어 송신하는, 이메일 에이전트(email agent)와 더불어 구성되어 있다.

[0083] 상기와 같이 신뢰 중개 시스템(10)은, 웹 어플리케이션 서버로서, 예컨대, 플랫폼(platform)의 공통의 비즈니스 로직(common business logic)에 대한 액세스를 관리하고 제공하는 J2EE 준수 어플리케이션 서버(401), 및 온라인 상인으로부터 그리고 사용자의 브라우저로부터 신뢰 중개 시스템(10)으로의 외부 HTTP 요청들에 대한 입구로서 작용을 하는 웹 서버 & J2EE 서블릿 엔진(servlet engine)(403)으로서 바람직하게 실시된다.

[0084] 웹 서버 및 서블릿 엔진(403)은, 웹 서비스-기반 결제 API들 또는 API 래퍼(wrapper)들을 온라인 시스템들에 노출시키는 프리젠테이션 요소들을 포함한다. 또한, 웹 서버 및 서블릿 엔진(403)은, 예컨대, 사용자가 상기한 방식으로 결제 방식을 선택할 때, 사용자에 대한 인터페이스를 생성 및 관리하도록 구성되어 있는 프리젠테이션 처리 요소들(404)을 포함한다.

[0085] J2EE 어플리케이션 서버(401)는 웹 플랫폼 및 어플리케이션들에 대한 모든 비즈니스 로직을 관리한다. 비즈니스 로직은, 예컨대, 세션(Session) EJBs(Enterprise Java Beans)로서 구현될 수 있는 기능성 소프트웨어 요소들(411a ... 411e)을 포함한다. 이러한 기능성 그룹들은, 예컨대, 이메일 처리 모듈들, 어드레스 확인 모듈과, 프로드(fraud) 및 보안 서비스 모듈을 포함한다; 또한, 서버(401)는, 예컨대, 상기한 사용자 데이터, 감사 데이터 및 트랜젝션 데이터와 같은 DB1에 저장된 정적 및 영속적 데이터에 대한 액세스를 제공하는 EJB 3.0 특정 자바 객체(Java object)들(411f ... 411h)로서 구현되는 객체들을 포함한다. 신뢰 중개 시스템(10)은, 결제 시스템(1)의 다른 요소들에 세션 EJBs를 노출하는 래퍼의 형태의 웹 서비스들을 포함한다. 보다 상세하게, 기능성 소프트웨어 요소들(411a ... 411e)은, 특히 어드레스 확인 서비스들(415a), (이메일 서버에 대한 액세스를 포함하는) 이메일 어플리케이션들(415b), 3-D 보안 서비스들(415c), 계정 갱신 서비스들(415d), 및 프로드 서비스들(415e)과 같은, 외부 서비스 인에이블러(enabler)(405)와 상호 운용한다. 어플리케이션 서버(401) 요소들(411a ... 411e)은 파트(413a ... 413e)들에 관하여 그와 같이 일반적으로 칭해지는, 일련의 API들을 통해 어플리케이션 요소들(415a ... 415e)과 통신한다. 웹 서버로서 구현될 때, 신뢰 중개 시스템(10)과 결제 시스템(1)의 요소들(즉, 도 2 및 3에 나타내어진 것들) 사이의 데이터는, 예컨대, 보안 소켓 층 프로토콜(Secure Socket Layer protocol)(HTTPS)를 통해, 보안 메커니즘을 이용하여 송신된다.

[0086] 3-D 보안 서비스 기능성 요소(411c)의 경우에 있어서, 이러한 요소는, 요소가 사용자와 신뢰 중개자(10)간의 상호 작용들에 수반되어야 할지 아닐지의 여부를 판정하기 위해서 불러지는 위험-기반 규칙들을 사용하거나 협력한다. 규칙들은 프로드 서비스(415e)의 제어하에 일반적으로 구성되고, 예컨대, (사용자가 적법한 카드 소지인 것을 보장하기 위해) 사용자가 SSP 서비스에 결제 수단을 등록할 때, 3-D 보안 방법이 불러져야 한다는 것을 지정할 수 있다; 구매자가 만든 제1 트랜젝션에 대해서; 특정 값을 초과하는 트랜젝션들에 대해서; 구매자의 자기 지역 밖의 상품의 선적을 수반하는 트랜젝션들에 대해서; 그리고 특정 타입의 상품 및/또는 서비스에 대해서이다. 모든 트랜젝션들에 대한 서비스를 불러오는 것을 포함하는 3-D 보안 서비스를 트리거(trigger)할 수 있는 다른 이벤트(event)들이 당업자에게 명백해질 것이다.

[0087] 계정 갱신(account updating; "AU") 기능성 요소(411d) 및 카드 스킴 시스템(7)에 의해 제공되는 대응 서비스(415d)에 대해 검토하여 보면, AU 요소(411d)는 데이터베이스(DB1)내의 개별적인 사용자 월릿에 저장되는 결제 수단의 만료 일자를 루틴하게 리뷰하고, 결제 수단들이 지정된 시간 윈도우(time window)내에 만료하기로 되어

있는, 사용자의 세부를 가진 카드 스킴 시스템(7)에 요청들을 제출하기 위한 루틴(routine)들을 포함한다. AU 요소(411d)는 다음에 계정 갱신 서비스(415d)를 액세스하여 그에 의해 생성된 응답 파일을 수집하며, 응답 파일의 내용에 기초하여 관련 사용자 월릿들내의 결제 수단들을 갱신한다.

[0088] 도 3을 참조하여 상기한 처리 단계들, 특히 다양한 결제 엔터티들과 인터페이싱할 때 신뢰 중개 시스템(10)에 의해 특정적으로 실행되는 단계들이 이제 보다 상세히 설명될 것이다. 도 5를 검토하여 보면, 단계(S5.1)에서, 사용자는 결제 방법으로서 SSP 결제 서비스를 선택하고, 그들의 선택을 온라인 상인 웹 사이트에 제출한다. 이것은, 온라인 상인 시스템으로부터의 요청, 신뢰 중개 시스템(10)의 사인-인 페이지(sign-in page)에 대응하는 URL의 온라인 상인 시스템에 의한 검색, 및 그 다음에, 보안 세션의 생성 및 리턴(return) URL(단계 S5.3)을 포함하는 온라인 상인 필드 더하기 키 오더(key order)의 송신을 트리거한다. 신뢰 중개 시스템(10)으로부터 사인-인 URL을 수신하면, 온라인 상인 시스템은 사인-인 페이지를 사용자에게 표시한다(단계 S5.5). 일 장치에 있어서, 사인-인 페이지는 사용자로 하여금 온라인 상인의 온라인 환경내에 남아 있으면서 신뢰 중개 시스템(10)과 직접적으로 통신할 수 있게 하는 i프레임(iFrame)으로서 구현된다. 사용자는 그들의 사인-인 세부를 입력하고(단계 S5.7), 상기한 승인 메커니즘 중 하나에 따라 승인된다(단계 S5.9); 승인이 성공적이면, 웹 서버 및 서블릿 엔진(403)은 표시 및 그 내부의 선택을 위해 사용자의 리모트 스토어로부터 데이터 내용을 I프레임에 송신한다(단계 S5.11). 일단 사용자가 다운로드된 리모트 스토어 내용내에서의 옵션들로부터 그들의 결제 방법을 선택하면, 사용자는 그들의 선택된 옵션을 웹 서버 및 서블릿 엔진(403)에 제출하여(단계 S5.13), 확인 페이지가 i프레임에 송신되는 결과를 가져온다(단계 S5.15).

[0089] 일단 사용자가 결제 선택 및 제출된 결제 선택을 확인하면(단계 S5.17), 웹 서버 및 서블릿 엔진(403)은, 신뢰 중개 시스템(10)이 온라인 상인을 대행하여 결제를 실행하는 결제 승인 서비스를 통해 온라인 상인의 IPSP 시스템(3c)에 결제 명세를 송신한다(단계 S5.19). 특정 상황하에서, 어플리케이션 서버(401)는 단계(S5.17)에서의 결제 선택의 수신에 응하는 3-D 보안 처리를 불러온다. 예를 들면, 어플리케이션 서버(401)는, 결제 요청 메시지의 내용에 기초하여, 트랜젝션의 처리와 계속하기 전에, 사용자가 대응하는 개설 은행에 의해 확인되는지 아닌지의 여부를 판정하는, 3-D 보안 요소(411c)를 불러올 수 있다. 3-D 보안 요소(411c)가 (요소(411c)에 액세스할 수 있는 규칙에 기초하여) 트랜젝션이 미리 정해진 레벨의 위험을 제공하는 것으로 판정하는 이벤트에 있어서, 3-D 보안 요소(411c)는 사용자와 대응하는 3-D 보안 개설 은행 승인 시스템(415c)간의 보안 통신을 구성한다. 예를 들면, 비자/보안코드(Visa/SecureCode)에 의해 확인되는 것을 이용하는 트랜젝션은, 트랜젝션을 승인하기 위해, 개설 은행의 웹 사이트로의 전향을 시작할, 또는 인라인 프레임 세션(inline frame session)의 로딩(loading)을 시작할 것이다.

[0090] 사용자가 확인되는 것을 가정하거나, 질문의 트랜젝션에 대해서 확인이 불필요하다고 간주되는 경우에 있어서, 단계(S5.19)는, 결제 API들(406)에 의한 수신을 위한 승인 요청을 생성하는 것, 결제 승인 요청을 온라인 상인의 API의 API 포맷으로 변환하는 것 및 포맷된 요청을 상인 IPSP 시스템(3c)에 송신하는 것을 수반한다. 지불 요청은 결제 API들(406)에 또한 송신되고, 결제 API들(406)은 지불 요청의 온라인 상인의 API의 API 포맷으로의 변환을 실행하고 그것을 상인 IPSP 시스템(3c)에 송신한다. 통신은 단일 또는 2중의 메시지 임플러먼테이션(implementation)에 의해 실행될 수 있다는 것이 이해될 것이다. 이러한 포맷 및 송신 동작은 온라인 상인 시스템에 대응하는 신뢰 중개 시스템(10)에 의해 보유되는 트랜젝션 데이터 스토어내에 기록된다.

[0091] 결제 요청의 승인의 통지시에(단계 S5.21), 웹 서버 및 서블릿 엔진(403)은 리턴 온라인 상인 URL을 i프레임에 송신하고(단계 S5.23), 성공적인 승인의 통지와 함께, i프레임을 비우고 온라인 상인 시스템으로부터 자바스크립트 코드(Javascript code)로 재장전시키며, 따라서 i프레임을 제거하고 사용자를 온라인 상인 시스템의 웹 사이트로 되돌린다. 마지막으로, 온라인 상인 시스템의 웹 사이트는 성공적인 오더 웹페이지를 단계(S5.27)에서 표시한다.

[0092] 단계들(S5.13~S5.19)과 나란히, 어플리케이션 서버(401)는 사용자의 활동을 기록하여 그것을 감사 데이터 스토어에 송신하면서, 대응 시스템 및 이벤트 정보를 써드 파티 프로드 통지 시스템에 송신할 수 있다(이것은 도 4에 나타낸 공통 서비스 인에이블러들(415e) 중 하나에 의해 표현된다). 프로드 통지 시스템은, 트랜젝션에 대한 위험 점수 및 권장 동작을 생성하기 위해서 그것의 분석을 실행하는, 프로드 위험 엔진(fraud risk engine)을 포함하지만, 이에 한정되지 않는다; 그 프로드 방지 스위트(fraud prevention suite)의 RSA™에 의해 제공되는 것과 같은 적절한 프로드 통지 시스템이 알려져 있고 여기서는 임의의 보다 세부적인 것으로 설명되지 않을 것이다. 위험 점수 및 동작은 온라인 상인 및 사용자에 대한 다른 트랜젝션 세부와 함께, 데이터베이스(DB1)에 저장된다.

[0093] 상기 실시예들은 본 발명의 예시적인 예들로서 이해되어진다. 본 발명의 추가적인 실시예들이 직시된다. 예를 들면, 상기한 예들에 있어서, 신뢰 중개 시스템(10)은 온라인 상인 시스템들로부터 결제 요청들을 수신하는 것으로 기술되었지만, 중개자(10)는, 그러한 상인 IPSP 시스템들이 결제 옵션으로서 SSP를 제공한 경우에 있어서, 배경 섹션에서 기술된 제3 타입의 장치의 상인 IPSP 시스템으로부터 추가적으로 또는 대안적으로 결제 요청들을 수신할 수 있다.

[0094] 또한, 바람직한 실시예들이, 사용자로 하여금 상이한 웹 사이트들을 항행시키기 위해 i프레임 웹 기술을 이용하지만, 표준 웹 전향이 대신 채용될 수 있다는 것이 이해될 것이다. 그러한 대안적인 장치에 있어서, 사용자의 브라우저는, 사용자의 브라우저가 임의의 시점에 통신하고 있는 엔터티(또는 오히려 그에 대응하는 URL)에 따라, SSP 웹 사이트로부터 멀리 또는 SSP 웹 사이트로 돌아가도록 항행될 것이다. 예를 들면, 사용자에 의한 승인 및/또는 계정 선택시에, 사용자의 브라우저는 SSP 웹사이트에 의해서, 사용자의 개설 은행에 의해 또는 사용자의 개설 은행을 대행하여 제공되는 웹사이트에 전향될 수 있고, 일단 사용자 승인 및/또는 계정 선택이 완료되면, 사용자의 브라우저는 개설 은행 웹사이트에 의해 SSP 웹 사이트로 돌아가도록 전향될 수 있다.

[0095] 상기 실시예들에 있어서, 신뢰 중개 시스템(10)은 선적 세부를 일련의 사용자 레코드에 저장하는 것으로 기술되었다: 이러한 정도까지, 신뢰 중개 시스템(10)은 체크아웃 도구와 관련된 기능성을 일부를 제공하는 것으로 보여질 수 있다: 데이터베이스(DB)에 저장된 관련 필드들이, 상인 시스템들로 하여금 체크아웃 처리시에 데이터를 참조하도록 그리고 필드를 적절히 거주시키게 할 수 있게끔 인터페이스를 통해 사용 가능할 수 있다. 하지만, 이것은 중개자(10)의 선택적인 양태이라는 것이 이해되어진다. 사실상, 체크아웃 기능성이 온라인 상인 시스템(1c)에 의해 제공될 수 있고, 그 경우에 있어서, 신뢰 중개 시스템(10)은 단순히 결제 도구의 역할을 수행할 것이고, 데이터베이스(DB1)는 그 다음에 사용자-특정의 정보의 더 적은 항목들을 저장할 것이다.

[0096] 상기에 있어서, 용어 “시스템”, 상인 시스템과 같은 엔터티에 적용될 경우, 상인 IPSP 시스템, 신뢰 중개 시스템 및 다른 엔터티들은, 하나 이상의 물리적 사이트들 중 하나에 의해 제공되는, 데이터 통신 링크들을 통해 다른 데이터 처리 기능들에 연결되는 데이터 처리 기능을 의미하는 것으로 이해되어야 한다. 각각의 기능은, 단일의 데이터 처리 노드, 예컨대, 서버 컴퓨터, 또는 서버 컴퓨터들의 클러스터(cluster)와 같은, 상호 페일-오버 백업(fail-over backup)을 제공하는 일련의 데이터 처리 노드들, 및/또는 세트의 다른 부재들에 관하여 상이한 모듈의 서브-기능들을 제공하는 일련의 상호 연결된 데이터 처리 노드들, 예컨대 일련의 상호 작용하는 상이한 서버 컴퓨터들에 의해 제공될 수 있다.

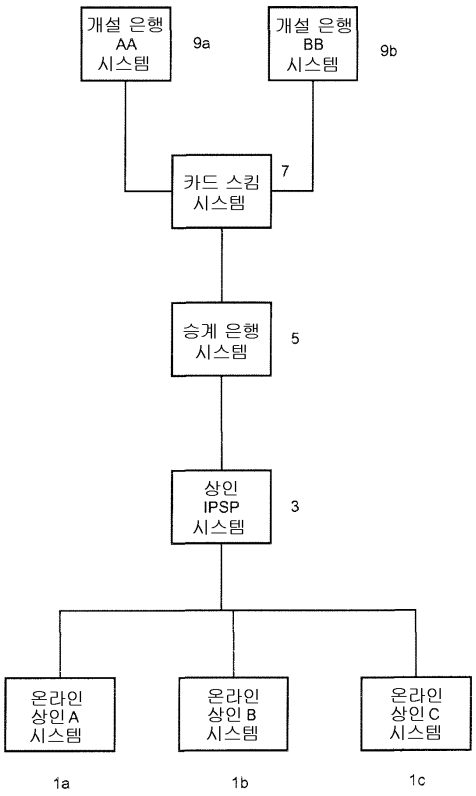
[0097] 상기로부터 이해될 바와 같이, 결제 시스템(1)을 포함하는 다양한 엔터티들간의 통신들은 인터넷과 같은 데이터 통신 네트워크를 통해 바람직하게 진행된다. 결제 시스템(1)의 각각의 엔터티들(개설 은행; 신뢰 중개자; 승계 은행 처리기; 상인 IPSP 시스템; 및 온라인 상인 시스템)은 인터넷 프로토콜(IP) 어드레스 또는 다른 적절한 식별자와 같은 네트워크 식별자를 통해 식별될 수 있다.

[0098] 따라서, 통신 네트워크는 하나 이상의 기술들을 포함하는 네트워크, 즉 하이브리드 통신 네트워크를 포함할 수 있다; 예컨대, 네트워크는 인터넷과 함께 공중 전화망(Public Switched Telephone Network; “PSTN”) 및/또는, 예컨대 하나 이상의 하기의 통신 프로토콜을 지원할 수 있는 모바일 통신 네트워크를 포함할 수 있다: GSM(Global System Mobile), WCDMA(Wideband Code Division Multiple Access), GPRS(General Packet Radio Service). 모바일 통신 네트워크에 더하여 또는 그 대신에, 무선 로컬 영역 네트워크(WLAN)와 같은 로컬 영역 네트워크 또는 블루투스®(BlueTooth®)(BT) 및/또는 WiMax와 같은 다른 기술들이 결재 승인 요청 및 응답 apl 지들의 일부를 수행하도록 사용될 수 있다. 이러한 식으로, 이러한 식으로, 사용자들은 휴대형, 원격 장치들을 사용하는 온라인 상인 시스템들과 상호 작용할 수 있다. 데이터 통신 네트워크는 임의의 운송 방법을 이용하여 일반적인 인터넷 액세스를 지원하도록 이루어질 수 있다. 추가적으로, 또는 대안적으로, 확인 메시지를 이메일 메시지로서 송신하기 위해서, 결제 확인 메시지들이 SMS-메시지(Short Message Service), MMS-메시지(Multi Media Service), 무선 어플리케이션 프로토콜(Wireless Application Protocol; “WAP”) 페이지, 인터넷 페이지, HTML(Hypertext Mark-up Language) 페이지, XHTML(extended HTML) 페이지, 또는 IP-데이터그램(Internet Protocol datagram)로서 전해질 수 있다.

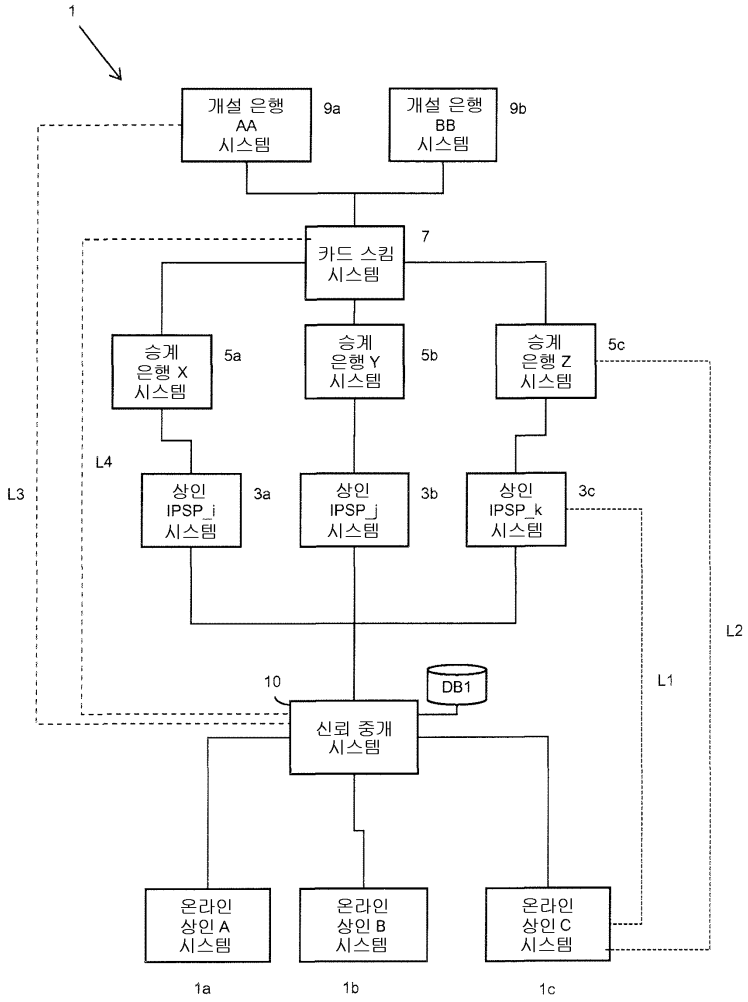
[0099] 임의의 하나의 실시예에 관하여 기술된 임의의 피처가 단독으로, 또는 다른 설명된 피처들과 함께 사용될 수 있고, 임의의 다른 실시예들의 하나 이상의 피처들 또는 임의의 다른 실시예들의 임의의 조합과 함께 또한 사용될 수 있다. 또한, 상술하지 않은 등가 및 수정이 또한, 첨부된 청구 범위에서 규정되는 본 발명의 권리 범위로부터 벗어나지 않고 채용될 수 있다.

도면

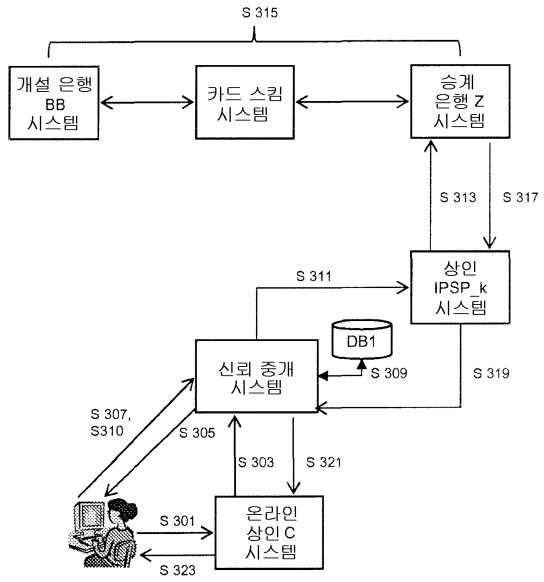
도면1


개설 은행
AA
시스템
9a
개설 은행
BB
시스템
9b
카드 스킴
시스템
7
승계 은행
시스템
5
상인
IPSP
시스템
3
온라인
상인 A
시스템
온라인
상인 B
시스템
온라인
상인 C
시스템
1a
1b
1c

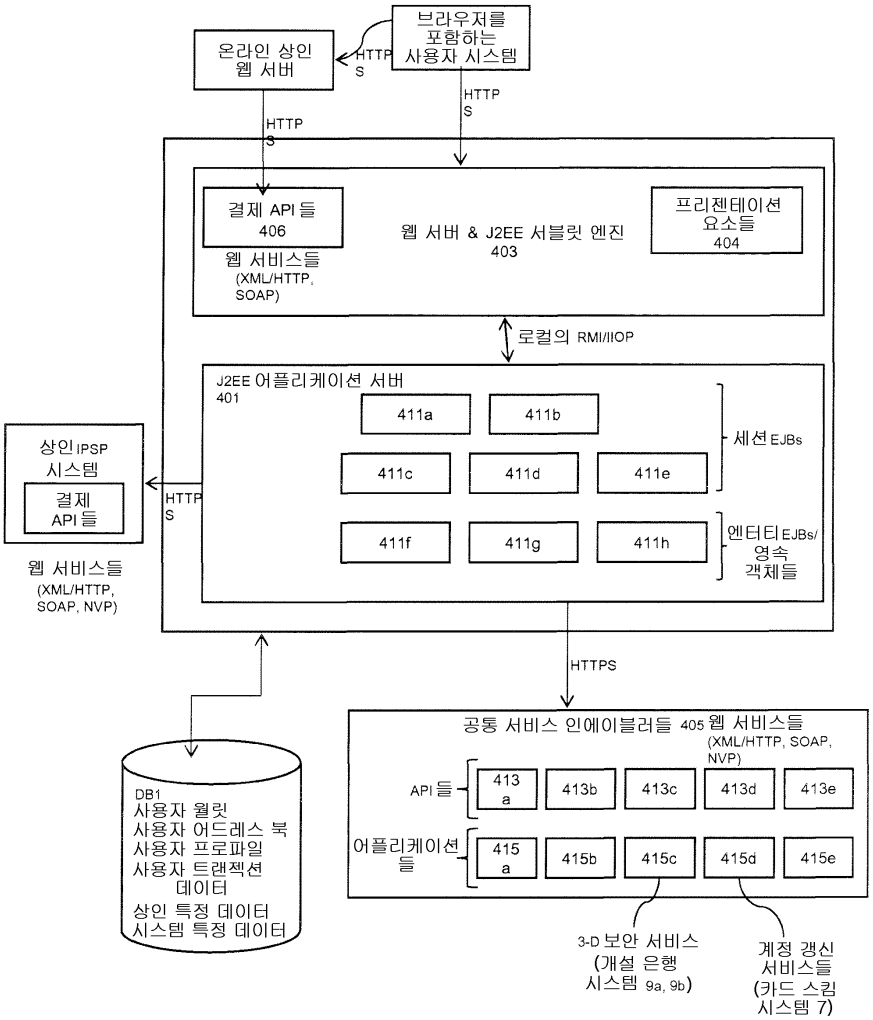
도면2


1
개설 은행 AA 시스템
9a
개설 은행 BB 시스템
9b
카드 스킴 시스템
7
승계 은행 X 시스템
5a
승계 은행 Y 시스템
5b
승계 은행 Z 시스템
5c
L4
L3
상인 IPSP_i 시스템
3a
상인 IPSP_j 시스템
3b
상인 IPSP_k 시스템
3c
L2
L1
10
DB1
신뢰 중개 시스템
온라인 상인 A 시스템
온라인 상인 B 시스템
온라인 상인 C 시스템
1a
1b
1c

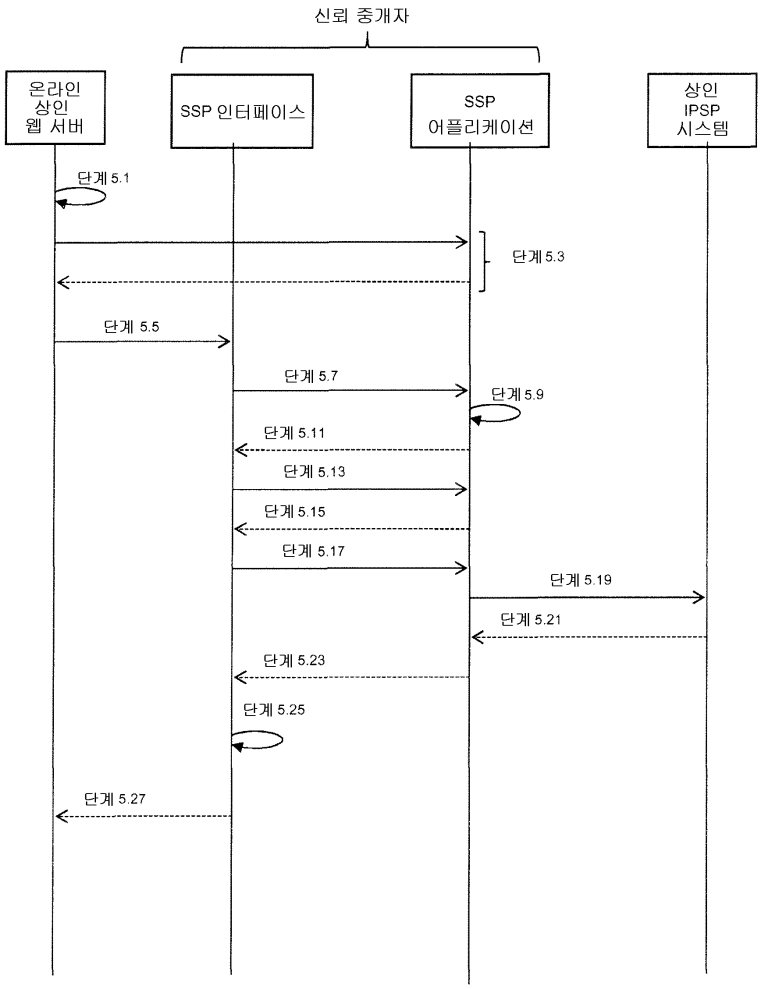
도면3


S 315
개설 은행 BB 시스템
카드 스킴 시스템
승계 은행 Z 시스템
S 313
S 317
S 311
상인 IPSP_k 시스템
DB1
신뢰 중개 시스템
S 309
S 319
S 307, S310
S 305
S 303
S 321
S 301
온라인 상인 C 시스템
S 323

도면4


온라인 상인 웹 서버
HTTPS
브라우저를 포함하는 사용자 시스템
HTTPS
HTTPS
결제 API 들 406
웹 서비스들 (XML/HTTP, SOAP)
웹 서버 & J2EE 서블릿 엔진 403
프리젠테이션 요소들 404
로컬의 RMI/IIOP
J2EE 어플리케이션 서버 401
411a
411b
411c
411d
411e
411f
411g
411h
세션 EJBs
엔터티 EJBs/ 영속 객체들
상인 IPSP 시스템
결제 API 들
HTTPS
웹 서비스들 (XML/HTTP, SOAP, NVP)
HTTPS
공통 서비스 인에이블러들 405
웹 서비스들 (XML/HTTP, SOAP, NVP)
API 들
413a
413b
413c
413d
413e
어플리케이션 들
415a
415b
415c
415d
415e
DB1
사용자 월릿
사용자 어드레스 북
사용자 프로파일
사용자 트랜잭션 데이터
상인 특정 데이터
시스템 특정 데이터
3-D 보안 서비스 (개설 은행 시스템 9a, 9b)
계정 갱신 서비스들 (카드 스킴 시스템 7)

도면5



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 26, 27줄

【변경전】

상기 신뢰 중개 시스템은

【변경후】

상기 신뢰 중앙 중개 시스템은