



**(19) 대한민국특허청(KR)**  
**(12) 공개특허공보(A)**

(11) 공개번호 10-2008-0098492  
 (43) 공개일자 2008년11월10일

- (51) Int. Cl.  
*G06Q 10/00* (2008.03) *G06Q 40/00* (2008.03)  
*H04L 9/00* (2006.01)
- (21) 출원번호 10-2008-7020002  
 (22) 출원일자 2008년08월14일  
 심사청구일자 없음  
 번역문제출일자 2008년08월14일
- (86) 국제출원번호 PCT/US2007/001362  
 국제출원일자 2007년01월19일
- (87) 국제공개번호 WO 2007/097844  
 국제공개일자 2007년08월30일
- (30) 우선권주장  
 11/361,857 2006년02월24일 미국(US)

- (71) 출원인  
**마이크로소프트 코포레이션**  
 미국 워싱턴주 (우편번호 : 98052) 레드몬드 원  
 마이크로소프트 웨이
- (72) 발명자  
**카메론, 킴**  
 미국 98052-6399 워싱턴주 레드몬드 원 마이크로  
 소프트 웨이  
**난다, 아룬 케이.**  
 미국 98052-6399 워싱턴주 레드몬드 원 마이크로  
 소프트 웨이
- (74) 대리인  
**양영준, 백만기**

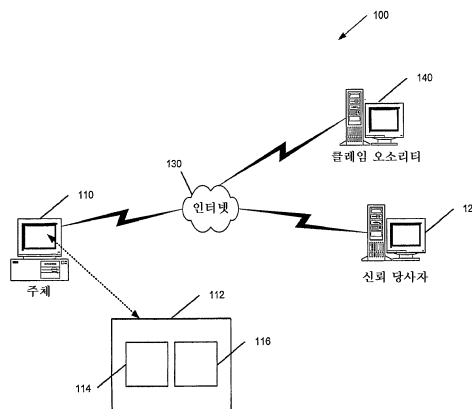
전체 청구항 수 : 총 15 항

**(54) 평판 정보 시스템, 평판 정보 제공 방법 및 컴퓨터 판독가능 매체**

**(57) 요약**

평판 정보를 제공하는 시스템은 당사자와 관련된 평판 정보를 갖는 클레임을 포함하는 보안 토큰을 수신하도록 프로그램된 신뢰 당사자를 포함하고, 상기 신뢰 당사자는 상기 당사자와 거래할지를 결정할 때 상기 평판 정보를 이용하도록 더 프로그램되어 있다. 평판 정보를 제공하는 방법은 당사자로부터 정보에 대한 요청을 수신하는 단계, 평판 정보를 제공하도록 상기 당사자에게 요구하는 단계, 보안 토큰의 클레임에서 상기 평판 정보를 수신하는 단계, 및 상기 평판 정보를 이용하여 상기 당사자와 거래할지를 결정하는 단계를 포함한다. 평판 정보를 제공하는 또 다른 방법은 클레임 오소리티로부터 온라인 서비스와 관련된 평판 정보를 요청하는 단계, 보안 토큰의 클레임에서 상기 평판 정보를 수신하는 단계, 및 상기 평판 정보를 이용하여 상기 온라인 서비스와 거래할지를 결정하는 단계를 포함한다.

**대표도 - 도1**



## 특허청구의 범위

### 청구항 1

평판 정보(reputation information)를 제공하는 시스템으로서,

당사자와 관련된 평판 정보를 갖는 클레임을 포함하는 보안 토큰을 수신하도록 프로그램된 신뢰 당사자(relying party)를 포함하고, 상기 신뢰 당사자는 상기 당사자와 거래할지를 결정할 때 상기 평판 정보를 이용하도록 더 프로그램되어 있는 평판 정보 제공 시스템.

### 청구항 2

제1항에 있어서, 상기 평판 정보는 하나 또는 그 이상의 개인 또는 조직에 의해 평가된 상기 당사자의 인지된 자질(quality) 또는 성격(character)에 관한 정보인 평판 정보 제공 시스템.

### 청구항 3

제1항에 있어서, 상기 보안 토큰은 계산 토큰 및 디스플레이 토큰을 포함하고, 상기 계산 토큰은 상기 당사자와 관련된 상기 평판 정보를 갖는 클레임을 포함하고, 상기 디스플레이 토큰은 상기 평판 정보를 갖는 클레임에 관한 디스플레이 정보를 포함하는 평판 정보 제공 시스템.

### 청구항 4

제1항에 있어서, 상기 신뢰 당사자가 요구하는 상기 평판 정보를 정의하는 상기 신뢰 당사자의 보안 정책(security policy)을 더 포함하고, 상기 신뢰 당사자는 상기 보안 정책을 상기 당사자에게 전송하도록 프로그램되어 있는 평판 정보 제공 시스템.

### 청구항 5

평판 정보를 제공하는 방법으로서,

당사자로부터 정보에 대한 요청을 수신하는 단계;

평판 정보를 제공하도록 상기 당사자에게 요구하는 단계;

보안 토큰의 클레임에서 상기 평판 정보를 수신하는 단계; 및

상기 평판 정보를 이용하여 상기 당사자와 거래할지를 결정하는 단계

를 포함하는 평판 정보 제공 방법.

### 청구항 6

제5항에 있어서, 상기 평판 정보는 하나 또는 그 이상의 개인 또는 조직에 의해 평가된 상기 당사자의 인지된 자질(quality) 또는 성격(character)에 관한 정보인 평판 정보 제공 방법.

### 청구항 7

제5항에 있어서, 상기 보안 토큰은 계산 토큰 및 디스플레이 토큰을 포함하고, 상기 계산 토큰은 상기 당사자와 관련된 상기 평판 정보를 갖는 클레임을 포함하고, 상기 디스플레이 토큰은 상기 평판 정보를 갖는 클레임에 관한 디스플레이 정보를 포함하는 평판 정보 제공 방법.

### 청구항 8

제5항에 있어서, 상기 평판 정보를 제공하도록 상기 당사자에게 요구하는 단계는 상기 신뢰 당사자가 요구하는 상기 평판 정보를 정의하는 보안 정책을 발행하는 단계를 더 포함하는 평판 정보 제공 방법.

### 청구항 9

제5항에 기재된 단계들을 수행하기 위한 컴퓨터 실행가능 명령어들을 갖는 컴퓨터 판독가능 매체.

### 청구항 10

평판 정보를 제공하는 방법으로서는,  
 클레임 오소리티(claims authority)로부터 온라인 서비스와 관련된 평판 정보를 요청하는 단계;  
 보안 토큰의 클레임에서 상기 평판 정보를 수신하는 단계; 및  
 상기 평판 정보를 이용하여 상기 온라인 서비스와 거래할지를 결정하는 단계  
 를 포함하는 평판 정보 제공 방법.

**청구항 11**

제10항에 있어서, 상기 평판 정보는 하나 또는 그 이상의 개인 또는 조직에 의해 평가된 상기 온라인 서비스와 관련된 당사자의 인지된 자질(quality) 또는 성격(character)에 관한 정보인 평판 정보 제공 방법.

**청구항 12**

제10항에 있어서, 상기 평판 정보를 디스플레이하는 단계를 더 포함하는 평판 정보 제공 방법.

**청구항 13**

제12항에 있어서, 상기 평판 정보를 디스플레이하는 단계는 브라우저에서 상기 평판 정보를 디스플레이하는 단계를 더 포함하는 평판 정보 제공 방법.

**청구항 14**

제12항에 있어서, 상기 평판 정보를 요청하는 단계는 상기 온라인 서비스가 액세스될 때 상기 평판 정보를 자동으로 요청하는 단계를 더 포함하는 평판 정보 제공 방법.

**청구항 15**

제11항에 기재된 단계들을 수행하기 위한 컴퓨터 실행가능 명령어들을 갖는 컴퓨터 판독가능 매체.

**명세서**

**배경 기술**

- <1> 온라인 영역에서의 상업의 존재는 계속 증가하는 추세에 있다. 많은 소비자들이 이제는 벽돌과 모르타르로 이루어진 가게에서 마주보고 거래를 행하기보다는 웹 사이트와 상호작용하여 상품 및 서비스를 구입하고 있다. 상업이 온라인으로 이동하면서, 소비자들은 그들이 상품 및 서비스를 구입하기 위해 방문하고 있는 웹 사이트들을 소유하는 개인들 및 회사들에 관하여 잘 알지 못할 수 있다. 이들 개인 및 회사의 평판은 거래를 심사숙고하는 웹 사이트들을 신뢰하기를 원하는 소비자들에게 중요하게 될 수 있다.
- <2> 다양한 별개의 서비스들이 소비자들이 액세스할 수 있는 당사자들에 관한 평판 정보(reputation information)를 제공한다. 예를 들면, BBB(Better Business Bureau)는 특정 지리적 영역에서 운영중인 다양한 회사들의 평판에 관한 정보를 제공한다. 다른 컨텍스트에서는, 신용 평가 에이전시들(credit rating agencies)에 의해 제공된 신용 점수들(credit scores)이 엔티티들에 관한 또 다른 형태의 평판 정보이다. 또 다른 예에서는, 이베이(eBay) 사용자들이 거래의 완료 후에 다른 이베이 사용자들을 평가할 수 있고, 그 결과의 의견들은 피드백 점수를 생성하고, 그에 의해 각 이베이 사용자에게 대한 평판을 생성하는 데 이용된다. 이베이 사용자들 및 판매자들은 이들 평판을 이용하여 해당 사용자의 평판에 기초하여 특정 이베이 사용자들과 거래할지의 여부에 관한 결정을 행할 수 있다.
- <3> BBB 및 신용 평가 에이전시 등의 서비스들은 당사자들이 어느 정도의 확신을 갖고 정확도를 신뢰할 수 있는 평판 정보를 제공한다. 그러나, 이러한 타입의 조직들에 의해 제공된 평판 정보는 반드시 용이하게 얻어지는 것은 아니다. 예를 들면, BBB로부터 한 회사에 관한 정보를 얻기 위해서는, 그 평판 정보를 얻기 위해 개인이 BBB와 접촉하고 그 회사를 구체적으로 참조할 필요가 있다. 또한, 그러한 조직들은 반드시 모든 당사자에 관한 정보를 갖고 있는 것은 아니다. 예를 들면, BBB는 BBB 조직의 회원인 회사들에 관한 정보만을 포함한다.
- <4> 이베이에 의해 제공되는 피드백 메커니즘 등의 서비스들은, 이베이 사용자들 간의 수천 개의 상호작용 등의, 보다 광범위한 개인들 및 거래들을 커버할 수 있다. 그러나, 이베이 상의 평판 정보는, 예를 들어, BBB의 평판

정보만큼 신뢰할 만한 것이 아닐 수도 있다. 왜냐하면 모든 사용자들이 다 피드백을 제공하는 것이 아닐 수 있고 사용자들이 피드백을 조작할 수도 있기 때문이다. 또한, 평판 정보는 이번에도 이베이 사용자에게만 제한된다.

<5> 이러한 타입의 서비스들의 한계 외에도 온라인 거래와 관련된 고유의 모호함이 있다. 예를 들면, 소비자가 누가 실제로 특정 웹사이트를 운영하는지를 식별하는 것은 어려울 수 있다. 그러한 경우에, 소비자가 그 웹 사이트에 관한 평판 정보를 구하려고 시도하는 것조차 어렵다. 왜냐하면 소비자는 그가 누구와 거래를 심사숙고하고 있는지를 쉽사리 판정할 수 없기 때문이다.

<6> [개요]

<7> 이 개요는 아래 상세한 설명에서 더 설명되는 개념들 중 선택된 것을 간략한 형태로 소개하기 위해 제공된다. 이 개요는 청구된 내용의 중요한 특징들 또는 필수적인 특징들을 식별하기 위한 것도 아니고, 청구된 내용의 범위를 결정하는 데 있어서 보조 수단으로서 이용되기 위한 것도 아니다.

<8> 일 양태는 평판 정보를 제공하는 시스템에 관한 것으로, 이 시스템은 당사자와 관련된 평판 정보를 갖는 클레임을 포함하는 보안 토큰을 수신하도록 프로그램된 신뢰 당사자(relying party)를 포함하고, 상기 신뢰 당사자는 상기 당사자와 거래할지를 결정할 때 상기 평판 정보를 이용하도록 더 프로그램되어 있다.

<9> 다른 양태는 평판 정보를 제공하는 방법에 관한 것으로, 이 방법은 당사자로부터 정보에 대한 요청을 수신하는 단계; 평판 정보를 제공하도록 상기 당사자에게 요구하는 단계; 보안 토큰의 클레임에서 상기 평판 정보를 수신하는 단계; 및 상기 평판 정보를 이용하여 상기 당사자와 거래할지를 결정하는 단계를 포함한다.

<10> 또 다른 양태는 평판 정보를 제공하는 방법에 관한 것으로, 이 방법은 클레임 오소리티로부터 온라인 서비스와 관련된 평판 정보를 요청하는 단계; 보안 토큰의 클레임에서 상기 평판 정보를 수신하는 단계; 및 상기 평판 정보를 이용하여 상기 온라인 서비스와 거래할지를 결정하는 단계를 포함한다.

**발명의 상세한 설명**

<22> 이제 예시적인 실시예들에 대하여 이하에서 첨부 도면들을 참조하여 보다 충실하게 설명한다. 이 실시예들은 이 명세서가 철저하고 완전하도록 하기 위해 제공된다. 유사한 번호들은 전체에 걸쳐서 유사한 요소들을 나타낸다.

<23> 여기 개시된 본 발명의 예시적인 실시예들은 일반적으로 디지털 ID 환경에서 사용하기 위한 온라인 엔티티들에 대한 평판 정보의 생성 및 저장에 관한 것이다. 전형적인 시나리오에서는, 클라이언트 시스템(주체(principal)라고도 불림)이 네트워크를 통하여 서버 시스템(신뢰 당사자(relying party)라고도 불림)과 통신한다. 이 시스템들 사이에 전송되는 정보를 인증하기 위해 이 시스템들 사이에 디지털 "ID들(identities)"이 교환될 수 있다. 또한, 본 발명의 실시예들의 양태들에 따라서, 주체와 신뢰 당사자 사이에 평판 정보도 교환될 수 있다. 평판 정보는 클레임 오소리티 시스템(claims authority system) 등의 다른 독립적인 시스템에 의해 주체에 제공될 수 있다. 평판 정보의 교환을 용이하게 하기 위하여, 예시적인 실시예들에서 평판 정보는, 신뢰 당사자로부터 온 것이든 클레임 오소리티로부터 온 것이든, 보안 토큰 또는 달리 신뢰할 만한 데이터의 부분 내에서 전송된다.

<24> 평판 정보는 하나 또는 그 이상의 개인 또는 조직에 의해 평가된 당사자의 인지된 자질(quality) 또는 성격(character)에 관한 정보이다. 평판 정보의 예로는, 당사자와 이전에 거래한 적 있는 하나 또는 그 이상의 개인에 의한 피드백(예컨대, 평가(ratings)), 신용 에이전시(credit agency)에 의해 보고된 당사자의 신용 점수(credit score), 및/또는 당사자의 상품/서비스에 대한 평가를 제공하거나 또는 복수의 다른 소스들로부터 평판 정보를 집계하기 위해 설립된 조직에 의한 평가를 포함하지만, 이에 제한되는 것은 아니다. 평판 정보의 또 다른 예로는, BBB 또는 던앤드브래드스트리트(Dunn & Breadstreet)로부터의 회사 평가, 및 AAA로부터의 서비스 평가를 포함한다. 다른 형태의 평판 정보도 가능하다.

<25> 이제 도 1을 참조하면, 주체(110), 신뢰 당사자(120), 및 클레임 오소리티(140)를 포함하는 예시적인 디지털 ID 시스템(100)이 도시되어 있다. 도시된 예에서, 주체(110)는 개인, 회사, 조직, 컴퓨터 또는 다른 장치, 서비스, 또는 임의의 다른 타입의 엔티티일 수 있다. 신뢰 당사자(120)는 주체(110)가 액세스하고 및/또는 획득하고자 하는 상품, 서비스, 또는 기타 정보를 갖는 온라인 서비스일 수 있다. 주체(110), 신뢰 당사자(120), 및 클레임 오소리티(140)는 인터넷(130)을 통하여 서로 통신할 수 있다.

- <26> 예시적인 실시예들에서, 주체(110)는 적어도 하나의 프로세서 및 메모리를 포함하는 퍼스널 컴퓨터를 제어하는 개인일 수 있다. 컴퓨터 시스템(110)은 컴퓨터 판독가능 명령어들, 데이터 구조들, 프로그램 모듈들, 또는 기타 데이터와 같은 정보의 저장을 위해 임의의 방법 또는 기술로 구현된 이동식 및 비이동식 매체뿐만 아니라, 휘발성 및 비휘발성 컴퓨터 저장 매체 중 하나 이상을 포함한다. 컴퓨터 시스템(110)은 마이크로소프트사로부터의 윈도우(WINDOWS) 운영 체제와 같은 운영 체제, 및 컴퓨터 판독가능 매체 상에 저장된 하나 또는 그 이상의 프로그램을 포함한다. 컴퓨터 시스템(110)은 또한 사용자가 컴퓨터 시스템(110)과 통신할 수 있게 하고, 또한 컴퓨터 시스템(110)이 인터넷(130) 및 신뢰 당사자(120) 등의 다른 장치들과 통신할 수 있게 하는 하나 또는 그 이상의 입력 및 출력 통신 장치들을 포함한다. 도 1에 도시된 하나의 예시적인 출력 장치는 디스플레이(112)이다.
- <27> 도시된 실시예에서, 주체(110)는 브라우저(114) 등의 프로그램을 이용하여 신뢰 당사자(120)와 관련된 웹 사이트에 액세스할 수 있다. 브라우저의 일례는 마이크로소프트사에 의해 제공된 인터넷 익스플로러(Internet Explorer) 브라우저이다. 일 실시예에서, 브라우저(114)는 HTTP(hypertext transport protocol)과 같은 하나 또는 그 이상의 공지된 프로토콜을 이용하여 신뢰 당사자(120)와 통신한다. 다른 프로토콜들이 이용될 수도 있다.
- <28> 예시적인 실시예들에서, 주체(110)는 신뢰 당사자(120)로부터 상품, 서비스, 또는 기타 정보를 요청할 수 있고, 신뢰 당사자(120)는 요청된 상품, 서비스, 또는 정보를 제공하기 전에 또는 제공하는 것과 관련하여 주체(110)에 관한 정보를 요구할 수 있다. 신뢰 당사자(120)가 요구하는 정보는 주체(110)에 관한 평판 정보를 포함한다.
- <29> 도시된 예에서, 클레임 오소리티(140)는 주체(110)에 관한 하나 또는 그 이상의 클레임 또는 어설션(assertions)을 제공할 수 있는 하나 또는 그 이상의 엔티티들을 포함한다. 클레임은 주체의 ID 또는 주체에 관한 정보, 예를 들면, 이름, 주소, 사회보장번호(social security number), 나이 등에 관계된 주체에 관하여 행해진 문(statement)이다. 본 명세서에서 설명된 예들에서, 클레임은 주체에 관한 평판 정보를 포함할 수 있다.
- <30> 예시적인 실시예들에서, 클레임 오소리티(140)는 다른 개인들 또는 조직들로부터의 피드백 또는 평가들을 수집하여 평판 정보를 생성한다. 다른 실시예들에서, 클레임 오소리티(140)는, 예를 들면, 주체에 관한 정보를 추적함으로써 평판 정보를 개발한다. 또 다른 실시예들에서, 클레임 오소리티(140)는 하나 또는 그 이상의 제3자들(예컨대, BBB, AAA 등)로부터 평판 정보를 집계한다. 만일 평판 정보가 복수의 소스들로부터 집계되면, 그 평판 정보를 특정 스케일로 표준화함으로써 2 또는 그 이상의 소스들로부터의 평판 정보가 비교될 수 있고 표준화된 평판이 계산될 수 있도록 할 수 있다.
- <31> 하나의 예에서, 클레임 오소리티(140)는 서명된 보안 토큰을 발행할 수 있는 보안 토큰 서비스를 포함한다. 예를 들면, 아래에서 더 설명되는 바와 같이, 클레임 오소리티(140)는 클레임들을 서명된 보안 토큰의 형태로 주체(110) 및/또는 신뢰 당사자(120)에게 제공할 수 있다. 클레임들 중 하나 또는 그 이상이 평판 정보를 포함할 수 있다. 예시적인 실시예들에서, 클레임 오소리티(140)는 신뢰 당사자(120)와 신뢰 관계(trusted relationship)에 있고, 따라서 신뢰 당사자(120)는 클레임 오소리티(140)로부터의 서명된 보안 토큰 내의 클레임들을 신뢰한다.
- <32> 본 명세서에서 개시된 예시적인 실시예들에서, 시스템(100)은 워싱턴주, 레드먼드의 마이크로소프트사가 개발한 WINFX 애플리케이션 프로그래밍 인터페이스에서 제공되는 InfoCard 시스템으로서 구현된다. 이 InfoCard 시스템은 주체들이 각종 클레임 오소리티들로부터의 복수의 디지털 ID들을 관리할 수 있게 한다. InfoCard 시스템은 WINFX 애플리케이션 프로그래밍 인터페이스에서 윈도우 커뮤니케이션 파운데이션(Windows Communication Foundation)과 같은 웹 서비스 플랫폼을 이용한다. 또한, InfoCard 시스템은 워싱턴주, 레드먼드의 마이크로소프트사에 의해 적어도 일부가 보급된 웹 서비스 보안 사양들(Web Service Security Specifications)를 이용하여 구축된다. 이들 사양은 메시지 보안 모델 WS-Security, 종점 정책(endpoint policy) WS-SecurityPolicy, 메타데이터 프로토콜 WS-MetadataExchange, 및 신뢰 모델 WS-Trust를 포함한다. 본 명세서에서 설명된 예시적인 실시예들은 위에서 설명된 웹 서비스 보안 사양들을 참조한다. 대안 실시예들에서는, 시스템(100)의 각종 컴포넌트들 간의 통신을 용이하게 하기 위해 하나 또는 그 이상의 다른 사양들이 이용될 수 있다.
- <33> 이제 도 2를 참조하면, 예시적인 주체(110), 신뢰 당사자(120), 및 클레임 오소리티(130)가 다시 도시되어 있다. 도시된 실시예에서, 주체(110)는 상품, 서비스, 또는 기타 정보에 대한 요청을 신뢰 당사자(120)에게 송신한다. 예를 들면, 일 실시예에서, 주체(110)는 주체(110)가 원하는 신뢰 당사자(120)로부터의 정보에의 액세스

스에 대한 요청을 신뢰 당사자(120)에게 송신한다. 주체(110)가 송신하는 요청은 또한, 예를 들면, WS-MetadataExchange에서 제공된 메커니즘들을 이용한 신뢰 당사자(120)의 보안 정책(아래 참조)에 대한 요청을 포함할 수 있다.

- <34> 그 요청에 응답하여, 신뢰 당사자(120)는 신뢰 당사자(120)가 주체(100)에 관한 ID 또는 기타 정보를 인증하기 위한 필요 조건들을 주체(110)에게 송신한다. 인증을 위한 신뢰 당사자(120)의 필요 조건들은 본 명세서에서 보안 정책(security policy)이라고 불린다. 보안 정책은 신뢰 당사자(120)가 주체(110)를 인증하기 위해 주체(110)가 신뢰 당사자(120)에게 제공해야 하는 클레임들의 세트를 정의한다. 하나의 예에서, 신뢰 당사자(120)는 그것의 보안 정책을 WS-SecurityPolicy를 이용하여 기술하지만, 다른 프로토콜들도 이용될 수 있다. 도시된 예에서, 신뢰 당사자(120)의 보안 정책은 주체(110)의 평판과 관련된 클레임에 대한 필요 조건을 포함한다.
- <35> 일단 주체(110)가 신뢰 당사자(120)로부터 보안 정책을 수신하면, 주체(110)는 그 정책이 요구하는 클레임들을 수집하기 위해 하나 또는 그 이상의 클레임 오소리티와 통신한다. 도시된 예에서, 주체(110)는 보안 정책의 필요 조건들을 클레임 오소리티(140)에 통신한다. 예를 들면, 주체(110)는 WS-Trust에서 기술된 발행 메커니즘을 이용하여 클레임 오소리티(140)로부터 하나 또는 그 이상의 보안 토큰을 요청할 수 있다.
- <36> 클레임 오소리티(140)는 신뢰 당사자(120)로부터의 정책에 따라 요구되는 클레임들 중 하나 이상을 제공할 수 있다. 예를 들면, 클레임 오소리티(140)는 주체(110)와 관련된 평판 정보를 포함하는 하나 또는 그 이상의 클레임을 생성하도록 프로그램되어 있다. 예시적인 실시예들에서, 클레임 오소리티(140)는 아래에서 설명되는 바와 같이 평판 정보를 갖는 하나 또는 그 이상의 클레임을 포함하는 하나 또는 그 이상의 서명된 보안 토큰(150)을 생성한다.
- <37> 그 후 평판에 관련한 하나 또는 그 이상의 클레임을 포함하는 보안 토큰(150)이 클레임 오소리티(140)에 의해 주체(110)에게 전송될 수 있다. 예시적인 실시예들에서, 클레임 오소리티(140)는 WS-Trust에서 기술된 응답 메커니즘들을 이용하여 보안 토큰(150)을 주체(110)에게 전송한다.
- <38> 일단 주체(110)가 보안 토큰(150)을 수신하면, 주체(110)는 신뢰 당사자(120)의 보안 정책의 전부 또는 일부를 만족시키기 위해 토큰(150)을 신뢰 당사자(120)에게 전송할 수 있다. 하나의 예에서, 주체(110)는 WS-Security에서 기술된 보안 바인딩 메커니즘들을 이용하여 보안 토큰(150)을 애플리케이션 메시지에 바인딩함으로써 보안 토큰(150)을 신뢰 당사자(120)에게 전송할 수 있다.
- <39> 일단 신뢰 당사자(120)가 보안 토큰(150)을 수신하면, 신뢰 당사자(120)는 서명된 보안 토큰(150)의 출처(origin)를 암호화로 확인할 수 있다. 신뢰 당사자(120)는 보안 토큰(150) 내의 평판 클레임들을 이용하여 신뢰 당사자(120)의 보안 정책을 만족시킬 수 있다. 예를 들면, 신뢰 당사자(120)는 보안 토큰(150) 내의 평판 클레임들을 검사하여 주체(110)를 신뢰하거나 또는 주체(110)와의 거래를 계속할지의 여부를 결정할 수 있다.
- <40> 이제 도 3을 참조하면, 예시적인 보안 토큰(150)이 도시되어 있다. 도시된 실시예에서, 보안 토큰(150)은 계산 토큰(152) 및 디스플레이 토큰(154)을 포함한다. 계산 토큰(152)은 암호화된 포맷으로 클레임 오소리티(140)에 의해 제공된 클레임들을 포함한다. 예시적인 실시예들에서, 클레임 오소리티(140)는 후술하는 바와 같이 신뢰 당사자(120)가 이해(즉, 암호 해독)할 수 있는 암호화된 포맷으로 계산 토큰(152)을 생성한다.
- <41> 클레임 오소리티(140)는 또한 디스플레이 토큰(154)을 생성한다. 일반적으로, 디스플레이 토큰(154)은, 평판 클레임들의 요약을 포함하여, 보안 토큰(150)의 계산 토큰(152)에 포함되어 있는 클레임들의 요약을 적어도 포함한다. 예를 들면, 일부 실시예들에서, 디스플레이 토큰(154)은 계산 토큰(152)에 포함된 모든 클레임들의 목록을 포함한다.
- <42> 디스플레이 토큰(154)은, 예를 들어, 디스플레이(112)를 이용하여 주체(110)에 의해 검토될 수 있는 포맷으로 생성될 수 있다. 일부 예들에서, 디스플레이 토큰(154)은 일반 텍스트 포맷 또는 HTML(Hypertext Markup Language) 포맷으로 생성된다. 보안 토큰 응답의 일부로서 포함되는 디스플레이 토큰(154)의 하나의 예시적인 실시예가 아래 제시된다. 이 예에서, 디스플레이 토큰은 평판에 관련한 클레임에 관한 정보를 포함한다(즉, 평판(reputation) = "중간(medium)").

<ic:RequestedDisplayToken>

<34>                   <ic:DisplayToken xml:lang="en-us">

```

    <ic:DisplayClaim
      URI="http://.../ws/2005/05/identity/claims/reputation">
        <ic:DisplayTag>Reputation</ic:DisplayTag>
        <ic:DisplayValue>Medium</ic:DisplayValue>
      </ic:DisplayClaim>
    <ic:DisplayToken>

```

<44> </ic:RequestedDisplayToken>

<45> 다음은 디스플레이 토큰에서 위에 제시된 요소들에 대한 일반 설명이다:

<46> • /ic:RequestedDisplayToken/ic:DisplayToken - 반환된 디스플레이 토큰;

<47> • /ic:RequestedDisplayToken/ic:DisplayToken/@xml:lang - 이 속성은, 디스플레이 토큰 콘텐츠가 지역화되는, RFC 3066에서 지정된 언어 코드를 이용한, 언어 식별자를 지시한다;

<48> • /ic:RequestedDisplayToken/ic:DisplayToken/ic:DisplayClaim - 이 요소는 보안 토큰에서 반환되는 개별 클레임을 지시한다;

<49> • /ic:RequestedDisplayToken/ic:DisplayToken/ic:DisplayClaim/@URI - 이 속성은 보안 토큰에서 반환되는 개별 클레임의 고유 식별자(URI)를 제공한다;

<50> • /ic:RequestedDisplayToken/ic:DisplayToken/ic:DisplayClaim/ic:DisplayTag - 이 옵션 요소는 보안 토큰에서 반환되는 클레임에 대한 공통의 또는 친화적인 이름(friendly name)을 제공한다;

<51> • /ic:RequestedDisplayToken/ic:DisplayToken/ic:DisplayClaim/ic:Description - 이 옵션 요소는 보안 토큰에서 반환되는 클레임에 대한 의미(semantics)에 대한 설명을 제공한다;

<52> • /ic:RequestedDisplayToken/ic:DisplayToken/ic:DisplayClaim/ic:DisplayValue - 이 옵션 요소는 보안 토큰에서 반환되는 클레임에 대한 하나 이상의 디스플레이 가능한 값들을 제공한다;

<53> • /ic:RequestedDisplayToken/ic:DisplayToken/ic:DisplayTokenText(제시되지 않음) - 이 옵션 요소는 토큰 콘텐츠가 개별 클레임들로서 디스플레이하기에 적합하지 않은 경우 전체로서의 토큰 전체의 대안적인 텍스트 표현을 제공한다.

<54> 일부 실시예들에서는, 계산 토큰(152)을 포함하는 보안 토큰(150)이 OASIS(Organization for the Advancement of Structured Information Standards)에 의해 공표된 SAML(Security Assertion Markup Language) 표준에 따라 발행된다. 예를 들면, 보안 토큰(150)은 SAML 1.1 또는 SAML 2.0 표준에 따라 발행될 수 있다. 제한이 아니라 예로서 X.509 인증서, XrML 토큰, 또는 커베로스 티켓(Kerberos ticket) 등의 다른 표준들이 이용될 수도 있다.

<55> 또한, 보안 토큰(150)은 알려진 알고리즘을 이용하여 클레임 오소리티(140)에 의해 암호화로 서명 또는 배서(cryptographically signed or endorsed)될 수 있다. 일 실시예에서는, 2048-비트 비대칭 RSA 키가 이용된다. 다른 실시예들에서는, 예를 들면, base64 인코딩된 대칭 암호화 키와 같은 다른 암호화 알고리즘이 이용될 수 있다. 일 실시예에서는, 대칭 키가 기본(befault)으로 이용된다. 이런 식으로, 도시된 예에서, 신뢰 당사자(120) 등의 당사자는 보안 토큰(150)이 클레임 오소리티(140)로부터 유래한 것을 암호화로 확인할 수 있다.

<56> 예시적인 실시예들에서, 계산 토큰(152)은, 제한이 아니라 예로서, 계산 토큰(152)과 디스플레이 토큰(154)의 양자를 포함하는 클레임 오소리티(140)로부터의 전체 응답 메시지 상에 디지털 서명을 이용하는 것과 같이, 하나 이상의 알려진 알고리즘을 이용하여 디스플레이 토큰(154)에 암호화로 바인딩된다(cryptographically bound).

<57> 주체(110)는 보안 토큰(150)을 신뢰 당사자(120)에게 전송하기 전에 디스플레이 토큰(154)의 내용을 검토할 수 있다. 예를 들면, 디스플레이 토큰(154)의 내용은 도 1에 도시된 디스플레이(112) 상의 브라우저(114)에서 및/또는 별도의 그래픽 사용자 인터페이스(116)에서 디스플레이될 수 있다. 일부 실시예들에서, 주체(110)는 디스플레이 토큰(154)의 내용의 검토에 기초하여 보안 토큰(150)을 신뢰 당사자(120)에게 전송할지의 여부를 결정할 수 있다.

- <58> 디스플레이 토큰을 포함하는 보안 토큰에 관련한 추가 상세는 2005년 12월 19일에 출원된 미국 특허 출원 11/312,920호에서 발견할 수 있고, 상기 특허 출원의 전체가 본 명세서에 참고로 통합된다.
- <59> 대안 실시예들에서, 클레임 오소리티(140)로부터의 보안 토큰(150)은 디스플레이 토큰을 포함할 필요가 없다. 예를 들면, 다른 실시예들에서, 보안 토큰(150)은 신뢰 당사자(120)에 의해 이용되는 계산 토큰(152)만을 포함한다. 보안 토큰(150)은 주체(110)를 통하여 신뢰 당사자(120)에게 전송되거나, 또는 클레임 오소리티(140)에 의해 바로 신뢰 당사자(120)에게 전송될 수 있다.
- <60> 예를 들면, 하나의 대안 실시예에서, 신뢰 당사자(120)는 클레임 오소리티(140)로부터 바로 주체(110)에 관한 평판 정보를 요청하여 수신할 수 있다. 이러한 구성은 신뢰 당사자(120)가 주체(110)에 의해 필터링되지 않은 평판 정보를 얻을 수 있게 한다.
- <61> 이제 도 4를 참조하면, 주체가 평판 정보를 포함하는 보안 토큰을 이용하는 예시적인 방법(200)이 도시되어 있다. 오퍼레이션 210에서는, 주체가 신뢰 당사자로부터 정보를 요청한다. 예를 들면, 일 실시예에서, 주체는 개인이고, 신뢰 당사자는 은행 기관(banking institution)이다. 주체는 컴퓨터를 이용하여 은행 기관의 웹 사이트에 액세스하여 주택 담보(home mortgage)에 대한 승인을 요청한다.
- <62> 다음으로, 오퍼레이션 220에서, 은행은 그 은행의 보안 정책을 그 개인의 컴퓨터에 전송한다. 그 정책은 개인이 그 담보의 자격을 얻기 위해 주어진 값 이상의 신용 점수(credit score)를 갖는 필요 조건을 포함한다. 그 후 컨트롤은 오퍼레이션 230으로 넘겨지고, 그 개인은 그 개인의 신용 점수와 관련된 하나 또는 그 이상의 클레임을 갖는 보안 토큰에 대한 요청을 신용 보고 에이전시(credit reporting agency)에 송신한다. 다음으로, 오퍼레이션 250에서, 그 개인은 보안 토큰의 디스플레이 토큰에서 지시된 신용 점수를 검토한다.
- <63> 다음으로, 오퍼레이션 260에서, 그 개인은 그 신용 점수를 포함하는 보안 토큰을 은행에 전송할지의 여부를 결정한다. 만일 그 개인이 토큰을 전송하지 않기로 결정하면, 컨트롤은 오퍼레이션 280으로 넘겨지고, 토큰은 은행에 전송되지 않는다. 대안적으로, 만일 그 개인이 오퍼레이션 260에서 토큰을 은행에 전송하기로 결정하면, 컨트롤은 오퍼레이션 265로 넘겨지고, 보안 토큰은 은행에 전송된다. 다음으로, 신용 점수가 은행이 요구하는 조건을 만족시킨다고 가정하여, 컨트롤은 오퍼레이션 270으로 넘겨지고 그 개인은 요청된 담보에 대한 승인을 수신한다.
- <64> 이제 도 5를 참조하면, 클레임 오소리티가 평판 토큰을 포함하는 보안 토큰을 생성하는 예시적인 방법(300)이 도시되어 있다. 방법(200)에서 설명된 것과 동일한 예를 가정하여, 방법(300)은 오퍼레이션 310에서 시작하고, 거기서는 클레임 오소리티가 개인의 컴퓨터로부터 그 개인의 신용 점수를 갖는 보안 토큰을 제공하기를 원하는 요청을 수신한다. 일 실시예에서, 클레임 오소리티는 신용 보고 에이전시의 보안 토큰 서비스이다. 다음으로, 오퍼레이션 320 및 330에서는, 신용 보고 에이전시의 보안 토큰 서비스가 신용 점수를 포함하는 계산 및 디스플레이 토큰들을 생성한다. 그 후 컨트롤은 오퍼레이션 340으로 넘겨지고, 거기서는 디스플레이 토큰이 계산 토큰에 논리적으로 바인딩되어 보안 토큰을 생성하게 된다. 다음으로, 오퍼레이션 350에서는, 신용 보고 에이전시의 보안 토큰 서비스가 보안 토큰을 개인에게 전송한다.
- <65> 이제 도 6을 참조하면, 신뢰 당사자가 평판 정보를 이용하는 예시적인 방법(400)이 도시되어 있다. 오퍼레이션 410에서 시작하여, 신뢰 당사자 은행이 개인으로부터 주택 담보에 대한 요청을 수신한다. 다음으로, 오퍼레이션 420에서는, 은행이 신용 점수를 요구하는 그 은행의 보안 정책을 그 개인에게 전송한다. 다음으로, 오퍼레이션 430에서는, 은행이 그 개인으로부터(또는 신용 보고 에이전시의 보안 토큰 서비스로부터 직접) 보안 토큰을 수신한다. 그 후 컨트롤은 오퍼레이션 440으로 넘겨지고, 거기서는 은행이 보안 토큰 내의 신용 점수를 심사한다. 다음으로, 오퍼레이션 450에서는, 은행이 그 신용 점수가 은행의 조건을 만족시키는지의 여부를 결정한다. 만일 신용 점수가 충분하다면, 컨트롤은 오퍼레이션 460으로 넘겨지고, 그 개인은 요청된 담보에 대하여 승인받는다. 대안적으로, 만일 오퍼레이션 450에서 신용 점수가 충분하지 않다면, 컨트롤은 오퍼레이션 470으로 넘겨지고, 그 개인은 요청된 담보에 대하여 승인받지 못한다.
- <66> 이제 도 7을 참조하면, 사용자(510), 제3자 웹 사이트(520)와 같은 온라인 서비스, 및 클레임 오소리티(540)를 포함하는 시스템(500)의 다른 실시예가 도시되어 있다. 도시된 예에서, 사용자(510)는 인터넷(130)을 통하여 제3자 웹 사이트(520)에 액세스하여 웹 사이트(520)로부터 상품, 서비스, 또는 기타 정보를 요청할 수 있다.
- <67> 제3자 웹 사이트(520)에 액세스하기 전에 또는 액세스하는 것과 관련하여, 사용자(510)는 또한 클레임 오소리티(540)에 액세스하여 클레임 오소리티(540)로부터 제3자 웹 사이트(520)에 관한 평판 정보를 요청할 수도 있다. 예시적인 실시예들에서, 사용자(510)는 클레임 오소리티(540)에 송신되는 평판 정보에 대한 요청에서 제3자 웹

사이트(520)의 도메인 이름, 그 웹 사이트와 관련된 공개 키, 및/또는 그 웹 사이트와 관련된 회사의 이름에 의해 제3자 웹 사이트(520)를 식별할 수 있다. 다른 타입의 식별이 이용될 수도 있다.

- <68> 예시적인 실시예들에서, 클레임 오소리티(540)는 하나 또는 그 이상의 제3자들에 관한 평판 정보를 포함하는 클레임 오소리티이다. 클레임 오소리티(540)는 평판 정보를 생성할 수 있고, 또는 클레임 오소리티(540)는 하나 또는 그 이상의 제3자 소스들로부터 평판 정보를 집계할 수 있다. 예시적인 실시예들에서, 클레임 오소리티(540)는 사용자(510)와 신뢰 관계에 있다. 사용자(510)는 클레임 오소리티(540)로부터의 제3자(520)와 관련된 평판 정보를 이용하여, 예를 들면, 제3자(520)과 거래할지의 여부를 결정할 수 있다.
- <69> 일부 실시예들에서, 클레임 오소리티(540)는 클레임 오소리티(540)가 서명한 보안 토큰에서 평판 정보를 사용자(510)에게 송신할 수 있다. 보안 토큰은 디스플레이 토큰을 포함할 수 있지만, 필수적인 것은 아니다.
- <70> 일부 실시예들에서, 평판 정보는 시각적 지시자(visual indicator)(예컨대, 텍스트, 컬러, 및/또는 평판이 우수할수록 수 또는 사이즈가 증가하는 별(star) 또는 바(bar) 등의 스케일 마커(scaled markers))의 형태로 사용자에게 제시된다. 아래에서 설명되는 도 9 및 10을 참조한다. 수치 값 또는 가청 지시자(audible indicators) 등의 다른 지시들이 이용될 수도 있다.
- <71> 이제 도 8을 참조하면, 사용자가 클레임 오소리티로부터 웹 사이트에 관한 평판 정보를 요청하는 예시적인 방법(600)이 도시되어 있다. 오퍼레이션 610에서는, 사용자가 클레임 오소리티에게 제3자에 관한 평판 정보에 대한 요청을 송신한다. 예시적인 실시예들에서, 요청은 사용자가 웹 사이트를 방문할 때 자동으로 생성될 수 있다. 다른 예에서, 요청은 사용자에게 의해 수동으로 개시될 수 있다.
- <72> 일 실시예에서, 사용자는 카메라를 구입하기 위해 온라인으로 쇼핑하는 개인이고, 제3자는 온라인 판매를 위해 카메라들을 제공하는 웹 사이트를 운영한다. 사용자의 브라우저(114)는 제3자 웹 사이트와 같은 웹 사이트가 브라우저(114)에 로딩될 때 그 웹 사이트에 관한 평판 정보를 자동으로 찾도록 프로그램되어 있다.
- <73> 다음으로, 오퍼레이션 620에서는, 개인이 제3자 웹 사이트에 관하여 클레임 오소리티로부터 응답을 수신한다. 예를 들면, 사용자는 제3자 웹 사이트에 관한 평판 정보를 갖는 보안 토큰을 수신한다. 다음으로, 오퍼레이션 630에서는, 사용자를 위해 평판 정보가 디스플레이된다. 다음으로, 오퍼레이션 640에서는, 사용자가 그 평판이 제3자와 거래를 계속하기에 충분한지의 여부를 결정한다. 예를 들어, 만일 사용자가 카메라 구입과 같이 웹 사이트와의 금융 거래를 심사숙고하고 있다면, 사용자는 단순히 뉴스 등의 정보를 웹 사이트로부터 얻기를 원하는 경우보다는 더 큰 특정 평판을 요구할 수 있다.
- <74> 만일 사용자가 그 평판 정보가 충분하다고 결정하면, 컨트롤은 오퍼레이션 650으로 넘겨지고, 사용자는 카메라를 구입하기 위해 제3자 웹 사이트와의 거래를 시작하거나 계속한다. 대안적으로, 만일 오퍼레이션 640에서 그 평판 정보가 충분하지 않다면, 컨트롤은 오퍼레이션 660으로 넘겨지고, 사용자는 카메라를 구입하기 위해 제3자 웹 사이트와의 거래를 중지하거나 하지 않는다.
- <75> 다시 도 7을 참조하여, 사용자가 클레임 오소리티(540)로부터 평판 정보를 수신하면, 그 평판 정보는 디스플레이(112) 상의 브라우저(114) 또는 별도의 인터페이스(116)에서 디스플레이될 수 있다. 평판 정보는 값(예컨대, 수치 값) 또는 스케일(예컨대, 등급 "A"- "F")의 형태로 사용자에게 디스플레이될 수 있다. 예를 들면, 평판 정보는 컬러 코딩된 및/또는 "별(star)" 스케일로 사용자에게 디스플레이될 수 있다. 일부 실시예들에서, 평판 정보는 사용자에게 디스플레이될 수 있는 이미지의 형태로 사용자에게 제공된다. 예를 들면, 일 실시예에서, 평판 정보는 제3자의 평판의 크기를 지시하기 위해 마커들(예컨대, 별) 및/또는 컬러들(예컨대, 적색, 황색, 녹색)을 갖는 이미지(예컨대, 비트맵 또는 JPEG)의 형태로 클레임 오소리티에 의해 제공된다. 그 이미지는 디스플레이(112) 상에서 사용자에게 디스플레이될 수 있다.
- <76> 예를 들면, 이제 도 9를 참조하여, 일 실시예에서, 브라우저(114)는 브라우저(114)의 상태 표시줄(status bar)(710)에서 클레임 오소리티(540)로부터의 평판 정보를 제공하도록 프로그램되어 있다. 도시된 실시예에서, 상태 표시줄(710) 내의 평판 정보는 브라우저(114)에서 보여지는 웹 사이트가 "별이 다섯인(five star)" 평판을 갖고 있음을 지시한다.
- <77> 이제 도 10을 참조하여, 대안 실시예에서, 평판 정보는 별도의 그래픽 사용자 인터페이스(116)에서 보여진다. 예를 들면, 사용자 인터페이스(116)는 평판 정보(810)(예컨대, "우수함(Excellent)")를 포함한다. 다른 구성들도 가능하다.
- <78> ID 시스템(identity systems)의 일부로서 평판 정보를 제공하는, 본 명세서에서 설명된 시스템들 및 방법들과

관련된 하나 이상의 이점들이 있다. 예를 들면, ID 시스템의 일부로서 평판 정보를 이용함으로써 평판 정보가 보다 용이하게 소비될 수 있는 표준화된 포맷으로 공유 및 집계될 수 있다. 신뢰 당사자들은 주체와 거래할지의 여부를 결정할 때 신뢰할 만한 제3자들로부터의 평판 정보를 이용할 수 있고, 그에 의해 거래에 대한 신뢰 당사자의 확신을 증가시킬 수 있다. 게다가, 사용자들은 제3자들과 거래할지의 여부를 결정할 때 그 제3자들에 관한 평판 정보를 이용할 수 있고, 그에 의해 거래에 대한 사용자의 확신을 증가시킬 수 있다.

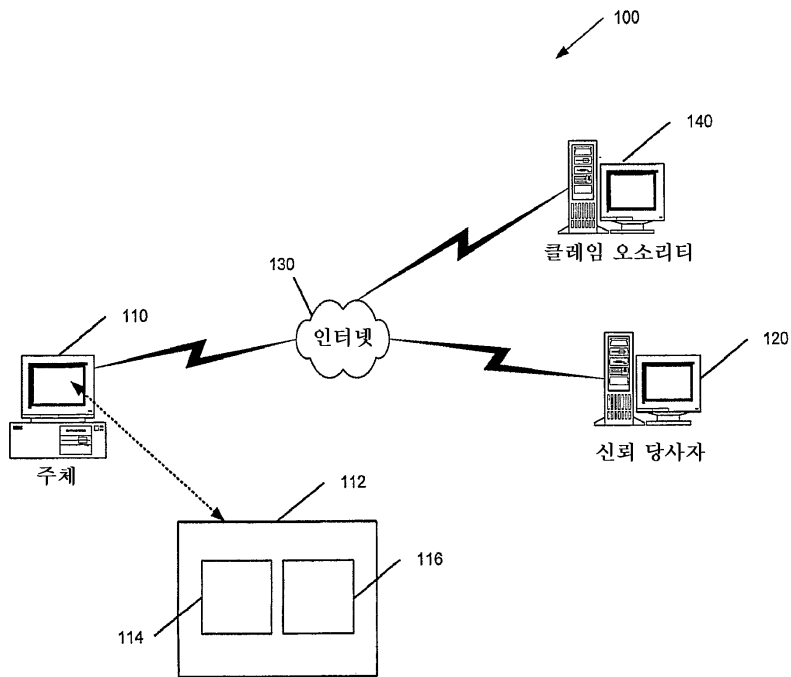
<79> 위에서 설명된 다양한 실시예들은 단지 예시로서 제공된 것으로 제한적인 것으로 해석되어서는 안 될 것이다. 숙련된 당업자라면 본 명세서 또는 다음의 청구항들의 진정한 정신 및 범위에서 벗어남이 없이 위에서 설명된 실시예들에 대해 행해질 수 있는 다양한 수정들 및 변경들을 쉽사리 인지할 것이다.

**도면의 간단한 설명**

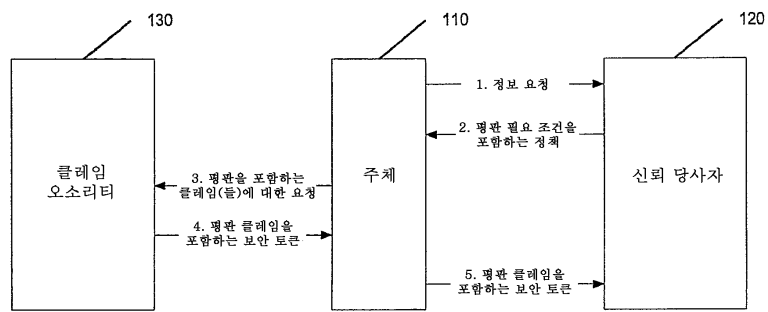
- <11> 이제 첨부 도면들을 참조한다. 이 도면들은 반드시 일정한 비례로 그려져 있지는 않다.
- <12> 도 1은 신뢰 당사자의 일 실시예가 클레임 오소리티(claims authority)로부터 주체(principal)에 관한 평판 정보를 수신하도록 프로그램되어 있는 예시적인 컴퓨팅 환경을 도시한다.
- <13> 도 2는 도 1로부터의 주체, 신뢰 당사자, 및 클레임 오소리티를 도시한다.
- <14> 도 3은 계산 토큰 및 디스플레이 토큰을 포함하는 예시적인 보안 토큰을 도시한다.
- <15> 도 4는 주체가 평판 정보를 ID(identity) 클레임으로서 이용하는 예시적인 방법을 도시한다.
- <16> 도 5는 클레임 오소리티가 평판 정보를 포함하는 보안 토큰을 생성하는 예시적인 방법을 도시한다.
- <17> 도 6은 신뢰 당사자가 ID 클레임으로부터의 평판 정보를 이용하는 예시적인 방법을 도시한다.
- <18> 도 7은 컴퓨터 시스템의 하나의 예시적인 실시예가 클레임 오소리티로부터 평판 정보를 수신하도록 프로그램되어 있는 또 다른 예시적인 컴퓨팅 환경을 도시한다.
- <19> 도 8은 사용자가 클레임 오소리티로부터의 제3자 웹 사이트에 관한 평판 정보를 이용하는 예시적인 방법을 도시한다.
- <20> 도 9는 평판 정보의 디스플레이를 포함하는 도 7의 컴퓨터 시스템의 예시적인 그래픽 사용자 인터페이스를 도시한다.
- <21> 도 10은 평판 정보의 디스플레이를 포함하는 도 7의 컴퓨터 시스템의 또 다른 예시적인 그래픽 사용자 인터페이스를 도시한다.

도면

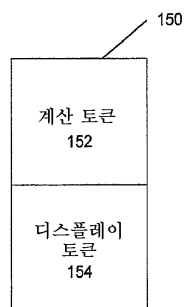
도면1



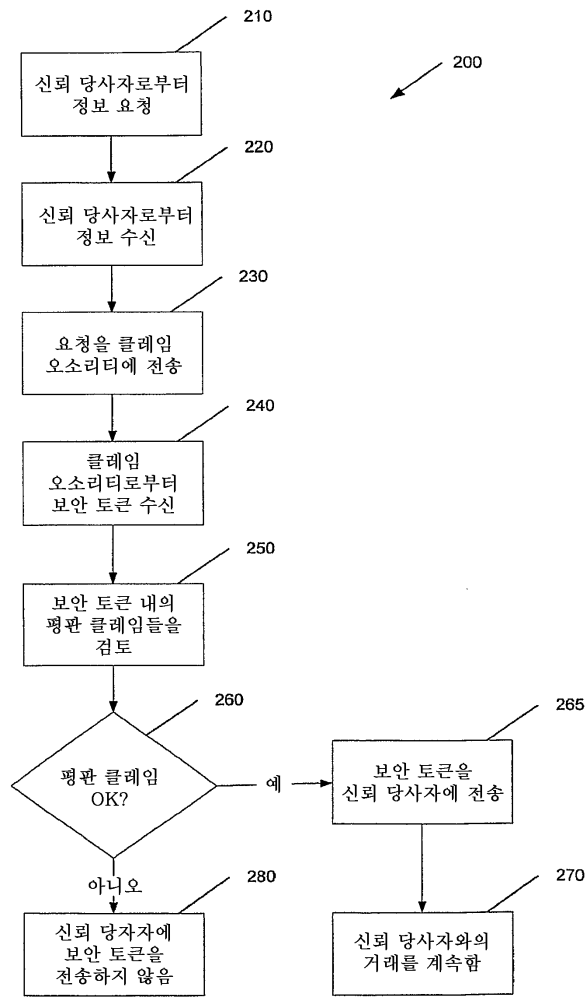
도면2



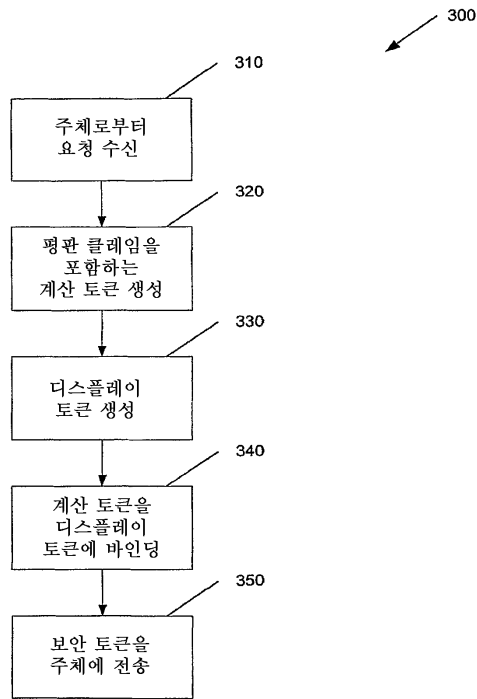
도면3



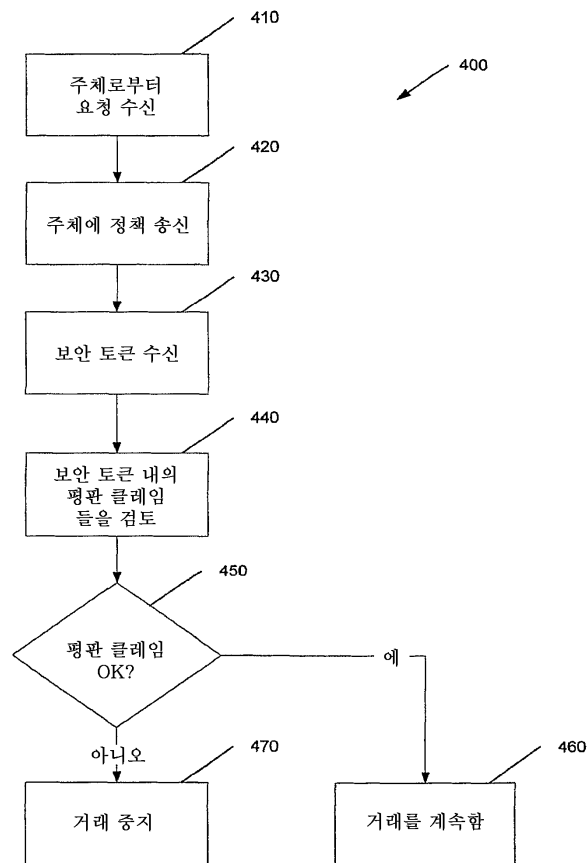
도면4



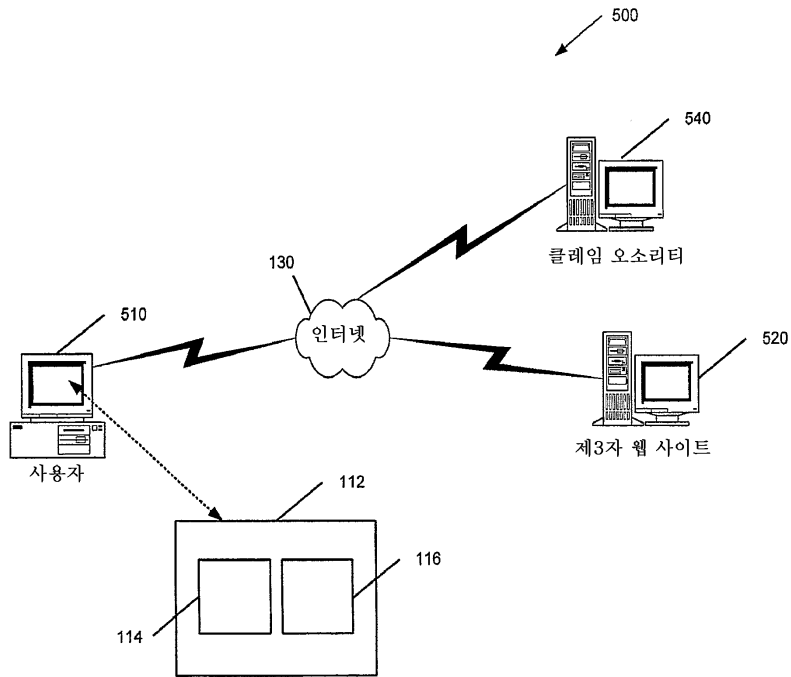
도면5



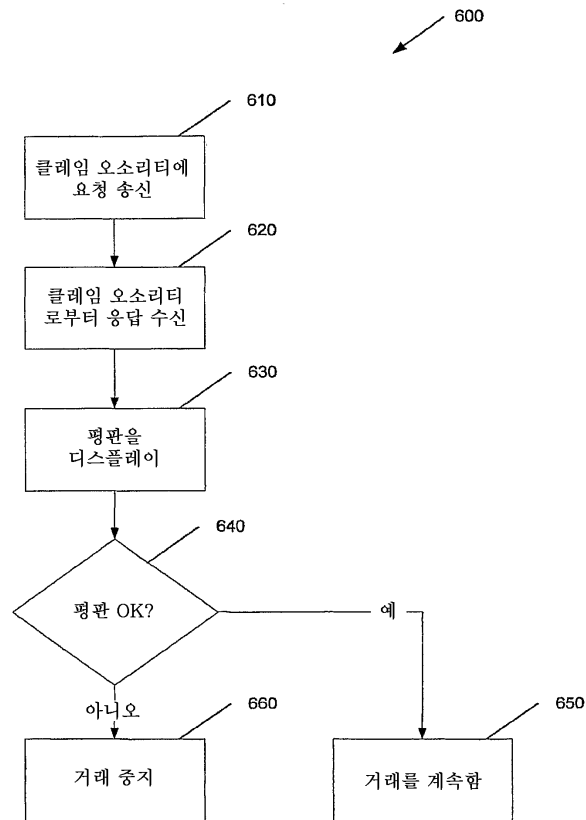
도면6



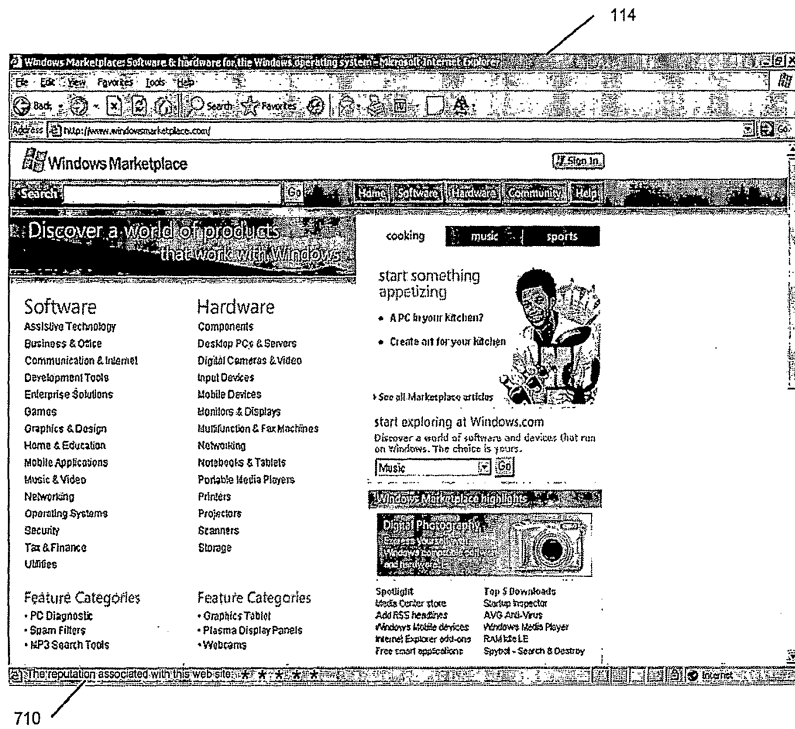
도면7



도면8



도면9



도면10

