(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06F 17/00 (2006.01)
G06Q 20/00A2 (2006.01)

(11) 공개번호 10-2006-0100920
(43) 공개일자 2006년09월21일

(21) 출원번호 10-2006-0006848
(22) 출원일자 2006년01월23일

(30) 우선권주장 11/079,050 2005년03월14일 미국(US)

(71) 출원인 마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이

(72) 발명자 총, 프레더릭 씨.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

(74) 대리인 주성민
이중희
백만기

심사청구 : 없음

(54) 웹 서비스를 위한 신뢰되는 제3자 인증

요약

본 발명은 웹 서비스들을 위한 신뢰되는 제3자 인증으로 확장한다. 웹 서비스들은 신뢰성 있는 웹 서비스들을 위해 신원 제공자로서 동작하는 신뢰되는 제3자에게 사용자 인증 책임을 신뢰하여 위임한다. 신뢰되는 제3자는, 예를 들어, 사용자명/패스워드 및 X.509 증명서와 같은, 일반 인증 메커니즘들을 통해 사용자들을 인증하고, 초기 사용자 인증을 사용하여 웹 서비스들과 후속 보안 세션들을 부트스트랩(bootstrap)한다. 웹 서비스들은 신뢰되는 제3자에 의해 발행되는 서비스 세션 토큰을 사용하여 사용자 신원 컨텍스트를 구성하고, 서버측 분산 캐쉬(cache)를 사용할 필요가 없이 보안 상태들을 재구성한다.

대표도

도 1a

색인어

인증 서비스, 서비스 세션 토큰, 사용자 신원 컨텍스트, 보안 토큰 서비스, 액세스 부여 서비스, 암호화된 대칭적 세션 키, 맞춤 XML 서비스

명세서

도면의 간단한 설명

도 1a는 웹 서비스들을 위한 신뢰되는 제3자 인증을 용이하게 하는 컴퓨터 아키텍처의 일 예를 도시한다.

도 1b는 도 1a의 컴퓨터 아키텍처의 예의 제1 부분의 다른 묘사를 도시한다.

도 1c는 도 1a의 컴퓨터 아키텍처의 예의 제2 부분의 다른 묘사를 도시한다.

도 2는 웹 서비스를 액세스하기 위한 서비스 토큰(token)을 얻는 방법의 순서도의 일 예를 도시한다.

도 3은 웹 서비스 컴포넌트와 웹 서비스 간의 통신을 안전하게 하는 방법의 순서도의 일 예를 도시한다.

도 4는 본 발명의 원리들을 위한 적절한 운영 환경을 도시한다.

<주요도면 부호설명>

101 : 웹 서비스 클라이언트

102 : 보안 토큰 서비스

103 : 인증 서비스

104 : 인증 데이터

105 : 네트워크

106 : 액세스 부여 서비스

107 : 정책 데이터

108 : 웹 서비스

108a, 108b, 108c : 인스턴스

109 : 분산된 캐쉬

161 : 비밀 대칭적 키

163Pu : 공개 키

163Pr : 개인 키

164Pu : 공개 키

164Pr : 개인 키

191, 192 : 신뢰

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 컴퓨터화된 인증에 관한 것이고, 더 구체적으로는, 웹 서비스들을 위한 신뢰되는 제3자 인증에 관한 것이다.

컴퓨터 시스템들과 관련된 기술은 사회의 많은 면들에 영향을 미친다. 실제로, 정보를 프로세스하기 위한 컴퓨터 시스템의 능력은 우리가 생활하고 일하는 방식을 변환시켰다. 예를 들어, 컴퓨터 시스템들은 통상적으로, 컴퓨터 시스템의 도래 이전에 수동으로 수행되었던 다수의 작업들(예를 들어, 문서 편집, 스케쥴링, 및 데이터베이스 관리)을 수행하는 소프트웨어 애플리케이션들을 포함한다. 컴퓨터 시스템은 또한 컴퓨터 시스템이 적절한 운영 상태에 남아 있거나 또는 리턴할 수 있는 것을 확실히 하기 위해 도움을 주는 관리, 진단, 및 보안 애플리케이션들(예를 들어, 백업 애플리케이션, 헬스 검사기, 안티-바이러스 애플리케이션, 방화벽 등)을 포함할 수 있다. 예를 들어, 안티-바이러스 애플리케이션은 컴퓨터 시스템에 임의의 해가 끼쳐지기 전에 컴퓨터 바이러스들을 탐지하여 제거할 수 있다.

다수의 컴퓨터 시스템들은 또한 통상적으로 서로 및 다른 전자 디바이스들에 결합되어 컴퓨터 시스템들과 다른 전자 디바이스들이 전자 데이터를 전송할 수 있는 유선과 무선 컴퓨터 네트워크 모두를 형성한다. 결과적으로, 컴퓨터 시스템에서 수행된 다수의 작업들(예를 들어, 음성 통신, 이메일 접속, 가정 전자기기 제어, 웹 브라우징, 및 문서 프린팅)은 유선 및/또는 무선 컴퓨터 네트워크들을 통해 다수의 컴퓨터 시스템들 및/또는 다른 전자 디바이스들 간의 전자 메시지들의 교환을 포함한다.

사실상 네트워크들은 매우 많아져서 간단하게 네트워크-인에이블되는(enabled) 컴퓨터 시스템은 종종 "인터넷"으로 불리는 네트워크들의 집합체를 통해 전 세계에 분포된 수 억 개의 다른 컴퓨팅 시스템들 중의 임의의 것과도 통신할 수 있다. 그런 컴퓨팅 시스템들은 데스크톱, 랩톱, 또는 태블릿(tablet) 개인용 컴퓨터, PDA(personal digital assistant), 전화, 또는 디지털 네트워크를 통해 통신할 수 있는 임의의 다른 컴퓨터 또는 디바이스를 포함할 수 있다.

또한, 애플리케이션 기능은 다수의 상이한 네트워크된 컴퓨터 시스템들에서 분포되거나 또는 "분산"될 수 있다. 즉, 애플리케이션의 제1 부분은 제1 컴퓨터 시스템에 존재할 수 있고, 애플리케이션의 제2 부분은 제2 컴퓨터 시스템에 존재할 수 있고, 이들 컴퓨터들은 모두 공통 네트워크에 접속된다. 이들 유형들의 애플리케이션들은 "분산된 애플리케이션들"로서 일반적으로 일컬어진다. 분산된 애플리케이션들은 특히 WWW(World Wide Web)(웹)에서 널리 퍼져있다.

다른 플랫폼들에서 상호동작성을 촉진시키기 위해, 웹의 분산된 애플리케이션들은 종종 한 개 이상의 산업 명세들에 따라 개발된다. 더 구체적으로, 웹 서비스들은 인터넷에서 XML(eXtensible Markup Language), SOAP(Simple Object Access Protocol), WSDL(Web Services Description Language), 및 UDDI(Universal Description, Discovery and Integration) 오픈 표준을 사용하는 웹-기반 애플리케이션들을 통합하는 표준화된 방식을 기재한다. XML은 데이터를 태그(tag)하기 위해 사용되고, SOAP는 데이터를 전송하기 위해 사용되고, WSDL은 이용가능한 서비스들을 기재하기 위해 사용되고, 및 UDDI는 무슨 서비스들이 이용가능한 지를 리스팅하기 위해 사용된다.

웹 서비스들은, 종종 비지니스들이 서로 및 클라이언트들과 통신하기 위한 수단으로서 사용되어, 회사들이 서로의 IT 시스템들에 대한 상세한 지식없이 데이터를 통신할 수 있도록 한다. 웹 서비스들은 네트워크에서 프로그래밍 인터페이스를 통해 비지니스 논리, 데이터, 및 프로세스들을 공유한다. 웹 서비스들은 다른 소스들로부터의 상이한 애플리케이션들이 시간-소비적 맞춤(custom) 코딩이 없이 서로 간에 통신하도록 하고, 통신이 XML로 이루어지므로, 웹 서비스들은 임의의 한 개의 운영 시스템 또는 프로그래밍 언어에 묶이지 않는다.

그러나, 웹 서비스들이, 종종 공공 네트워크들에서 서로 간에 통신하므로, 웹 서비스들 간에 데이터를 전송하는 것과 연관된 보안 위험들이 존재한다. 예를 들어, 악의적 사용자들은 데이터가 네트워크에서 전송될 때 웹 서비스 데이터를 가로채려는 시도를 할 수 있고, 한 개의 웹 서비스의 신원을 흉내내는 프로그램들을 구현하여, 다른 웹 서비스들이 웹 서비스 데이터를 그 흉내내는 프로그램으로 전송하도록 시도하게 할 수 있다. 따라서, 예를 들어, WS-보안(WS-Security), WS-보안대화(WS-SecureConversation), 및 WS-신뢰(WS-Trust)와 같은, 다수의 웹 서비스 명세들은, 예를 들어, SOAP 메시지들을 싸인(sign)하고 암호화하는 것 및 보안 토큰들을 요청하고 수신하는 것과 같은, 이들 보안 쟁점들 중의 일부를 해결하기 위한 빌딩 블록(building block)들을 제공한다.

그러나, 웹 서비스 명세들은 웹 서비스들이 모든 그들의 보안 요구사항들을 만족하기 위해 의존할 수 있는 철저한(end-to-end) 보안 프로토콜을 구성하지는 않는다. 즉, 일반 애플리케이션 보안 요구사항들을 인에이블하기 위해, 어떻게 상이한 웹 서비스 명세들이 함께 사용될 수 있는지를 기재하는 규정된 방식이 존재하지 않는다. 예를 들어, 웹 서비스 그룹이, 신뢰성 있는 웹 서비스들을 위한 신원 제공자로서 동작하는 신뢰되는 제3자에게 사용자 인증 책임을 신뢰하여 위임하도록 하는, (만약 있다면) 제한된 메커니즘들이 존재한다. 또한, 신뢰되는 제3자가, 예를 들어, 사용자명/패스워드 및 X.509 증명서들과 같은, 일반 인증 메커니즘들을 통해 사용자들을 인증하도록 하고, 초기 사용자 인증을 사용하여 웹 서비스들과

후속적 보안 세션들을 부트스트랩(bootstrap)하는 (만약 있다면) 제한된 메커니즘들이 존재한다. 또한, 웹 서비스들이, 신뢰되는 제3자에 의해 발행되는 서비스 세션 토큰을 사용하여 사용자 신원 컨텍스트를 구성하도록 하고, 서버측 분산된 캐쉬(cache)를 사용할 필요가 없이 보안 상태들을 재구성하도록 하는 (만약 있다면) 제한된 메커니즘들이 존재한다.

그러므로, 웹 서비스들을 위한 신뢰되는 제3자 인증을 용이하게 하는 시스템, 방법, 및 컴퓨터 프로그램 프로덕트들은 유익할 것이다.

발명이 이루고자 하는 기술적 과제

종래 기술의 전술된 문제들은 웹 서비스들을 위한 신뢰되는 제3자 인증을 위한 방법, 시스템, 및 컴퓨터 프로그램 프로덕트들에 관한 본 발명의 원리들에 의해 극복된다. 웹 서비스 컴포넌트는 인증 서비스로 인증 요청을 전송한다. 인증 서비스는 그 요청을 수신하여, 인증 요청에 포함된 인증 데이터를 유효화한다.

인증 서비스는 웹 서비스 컴포넌트로 인증 응답을 전송한다. 인증 응답은 웹 서비스 컴포넌트와 액세스 부여(granting) 서비스 간의 통신을 안전하게 하기 위한 제1 대칭적 세션 키의 2 개의 인스턴스(instance)들을 포함한다. 세션 키의 제1 인스턴스는 제1 증명 토큰에 포함되고, 웹 서비스 클라이언트로 전달되기 위해 보안화된다. 세션 키의 제2 인스턴스는 토큰 부여 토큰(token granting token)에 포함되고, 보안 토큰 서비스의 비밀 대칭적 키로 암호화된다.

웹 서비스 컴포넌트는 인증 응답을 수신한다. 웹 서비스 컴포넌트는 웹 서비스로의 액세스를 위해, 토큰 부여 토큰을 포함하는, 액세스 요청을 액세스 부여 서비스로 전송한다. 액세스 부여 서비스는 액세스 요청을 수신하고, 웹 서비스 컴포넌트가 토큰 부여 토큰의 내용에 기초하여 보안 토큰 서비스로의 인증된 세션을 가짐을 확인한다.

액세스 부여 서비스는 웹 서비스 컴포넌트에 액세스 부여 응답을 전송한다. 액세스 부여 응답은 웹 서비스 컴포넌트와 웹 서비스 간의 통신을 안전하게 하는 제2 대칭적 세션 키의 2 개의 인스턴스들을 포함한다. 제2 대칭적 세션 키의 제1 인스턴스는 제1 대칭적 세션 키로 암호화되고, 제2 증명 토큰에 포함된다. 제2 대칭적 세션 키의 제2 인스턴스는 웹 서비스에 대응하는 공개/개인 키 쌍으로부터의 공개 키로 암호화되고, 서비스 토큰에 포함된다.

웹 서비스 컴포넌트는 액세스 부여 응답을 수신한다. 웹 서비스 컴포넌트는 웹 서비스로, 웹 서비스 컴포넌트와 서비스 토큰을 위한 신원 정보를 포함하는, 보안 토큰 요청을 전송한다. 웹 서비스는 보안 토큰 요청을 수신하고, 공개/개인 키의 대응하는 개인 키를 사용하여 서비스 토큰에 포함된 제2 대칭적 세션 키의 제2 인스턴스의 암호를 해독한다. 웹 서비스는, 서비스 토큰의 내용에 기초하여 웹 서비스 컴포넌트가 웹 서비스를 액세스하는 것을 승인한다.

웹 서비스는, 웹 서비스 클라이언트와 웹 서비스 간의 통신을 안전하게 하는 마스터 대칭적 세션 키를 생성한다. 웹 서비스는, 제2 대칭적 세션 키를 사용하여 마스터 대칭적 세션 키를 암호화하여, 암호화된 마스터 대칭적 세션 키를 생성한다. 웹 서비스는, 보안 토큰 응답에 보안 컨텍스트 토큰과 함께 암호화된 마스터 대칭적 세션 키를 포함한다. 웹 서비스는, 웹 서비스 컴포넌트로 보안 토큰 응답을 전송하여, 웹 서비스 컴포넌트와 웹 서비스 간의 통신이 마스터 대칭적 세션 키로부터 유도된 대칭적 세션 키들을 사용하여 보안화될 수 있도록 한다. 웹 서비스 컴포넌트는 보안 토큰 응답을 수신하고, 제2 대칭적 세션 키를 사용하여 마스터 대칭적 세션 키의 암호를 해독한다.

본 발명의 이들과 다른 객체들 및 특징들은, 다음 설명과 첨부된 청구범위로부터 더욱 완전히 명백해지거나, 또는 이후에 기재되는 것과 같이 본 발명의 실시에 의해 교시될 수 있다.

발명의 구성 및 작용

본 발명의 위의 그리고 다른 이점들과 특징들을 더 명료하게 하기 위해, 본 발명의 더 구체적 설명이 첨부된 도면들에 도시되는 특정 실시예들을 참조하여 기재될 것이다. 이들 도면들이 단지 본 발명의 통상적 실시예들만을 도시하고, 그러므로 그것의 범위를 제한하는 것으로서 간주되지 않음을 이해해야 한다. 본 발명은 동반하는 도면들의 사용을 통해 추가적 특정성과 상세성으로 기재되어 설명될 것이다.

종래 기술의 전술된 문제들은, 웹 서비스들의 신뢰되는 제3자 인증을 위한 방법, 시스템, 및 컴퓨터 프로그램 프로덕트에 관한 본 발명의 원리들에 의해 극복된다. 웹 서비스 컴포넌트는 인증 서비스로 인증 요청을 전송한다. 인증 서비스는 그 요청을 수신하고, 인증 요청에 포함된 인증 데이터를 유효화한다.

인증 서비스는 웹 서비스 컴포넌트로 인증 응답을 전송한다. 인증 응답은 웹 서비스 컴포넌트와 액세스 부여 서비스 간의 통신을 안전하게 하는 제1 대칭적 세션 키의 2 개의 인스턴스들을 포함한다. 세션 키의 제1 인스턴스는 제1 증명 토큰에 포함되고, 웹 서비스 클라이언트로 전달을 위해 보안화된다. 세션 키의 제2 인스턴스는 토큰 부여 토큰에 포함되고, 보안 토큰 서비스의 비밀 대칭적 키로 암호화된다.

웹 서비스 컴포넌트는 인증 응답을 수신한다. 웹 서비스 컴포넌트는 웹 서비스로의 액세스를 위해, 토큰 부여 토큰을 포함하는, 액세스 요청을 액세스 부여 서비스로 전송한다. 액세스 부여 서비스는 액세스 요청을 수신하고, 토큰 부여 토큰의 내용에 기초하여 웹 서비스 컴포넌트가 보안 토큰 서비스로의 인증된 세션을 가짐을 확인한다.

액세스 부여 서비스는 웹 서비스 컴포넌트로 액세스 부여 응답을 전송한다. 액세스 부여 응답은 웹 서비스 컴포넌트와 웹 서비스 간의 통신을 안전하게 하기 위해 제2 대칭적 세션 키의 2 개의 인스턴스들을 포함한다. 제2 대칭적 세션 키의 제1 인스턴스는 제1 대칭적 세션 키로 암호화되고, 제2 증명 토큰에 포함된다. 제2 대칭적 세션 키의 제2 인스턴스는 웹 서비스에 따라 공개/개인 키 쌍으로부터의 공개 키로 암호화되고, 서비스 토큰에 포함된다.

웹 서비스 컴포넌트는 액세스를 부여하는 응답을 수신한다. 웹 서비스 컴포넌트는 웹 서비스로, 웹 서비스 컴포넌트와 서비스 토큰에 대한 신원 정보를 포함하는, 보안 토큰 요청을 전송한다. 웹 서비스는 보안 토큰 요청을 수신하여, 공개/개인 키의 대응하는 개인 키를 사용하여 서비스 토큰에 포함된 제2 대칭적 세션 키의 제2 인스턴스의 암호를 해독한다. 웹 서비스는 서비스 토큰의 내용에 기초하여 웹 서비스 컴포넌트가 웹 서비스를 액세스하도록 승인한다.

웹 서비스는, 웹 서비스 클라이언트와 웹 서비스 간의 통신을 안전하게 하는 마스터 대칭적 세션 키를 생성한다. 웹 서비스는, 제2 대칭적 세션 키를 사용하여 마스터 대칭적 세션 키를 암호화하여 암호화된 마스터 대칭적 세션 키를 생성한다. 웹 서비스는, 보안 토큰 응답에 보안 컨텍스트 토큰과 함께 암호화된 마스터 대칭적 세션 키를 포함한다. 웹 서비스는, 웹 서비스 컴포넌트로 보안 토큰 응답을 전송하여, 웹 서비스 컴포넌트와 웹 서비스 간의 통신이 마스터 대칭적 세션 키로부터 유도된 대칭적 세션 키들을 사용하여 보안화되도록 할 수 있다. 웹 서비스 컴포넌트는 보안 토큰 응답을 수신하고, 제2 대칭적 세션 키를 사용하여 마스터 대칭적 세션 키의 암호를 해독한다.

본 발명의 범위 내의 실시예들은, 컴퓨터-판독가능 매체에 저장된 컴퓨터-실행가능 명령들 또는 데이터 구조들을 전달하거나 또는 갖는 컴퓨터-판독가능 매체를 포함한다. 이러한 컴퓨터-판독가능 매체는, 일반 목적 또는 특수 목적 컴퓨터 시스템에 의해 액세스가능한, 임의의 이용가능한 매체일 수 있다. 예를 들어, 하지만 이에 제한되지는 않는, 그런 컴퓨터-판독가능 매체는, RAM, ROM, EPROM, CD-ROM이나 다른 광 디스크 저장 장치, 자기 디스크 저장 장치나 다른 자기 저장 디바이스, 또는 컴퓨터-실행가능 명령, 컴퓨터-판독가능 명령, 또는 데이터 구조의 형태로 원하는 프로그램 코드 수단을 전달하거나 또는 저장하기 위해 사용될 수 있고, 일반 목적이나 특수 목적 컴퓨터 시스템에 의해 액세스될 수 있는 임의의 다른 매체와 같은 물리적 저장 매체를 포함할 수 있다.

본 설명과 다음에 오는 청구범위에서, "네트워크"는 컴퓨터 시스템 및/또는 모듈 간에 전자 데이터의 전송을 가능하게 하는 한 개 이상의 데이터 링크들로서 정의된다. 네트워크 또는 다른 통신 접속(유선, 무선, 또는 유선이나 무선의 조합)을 통해 컴퓨터 시스템으로 정보가 전송되거나 또는 제공될 때, 접속은 컴퓨터-판독가능 매체로서 적절하게 보여진다. 그러므로, 이러한 임의의 접속은 컴퓨터-판독가능 매체로서 적절히 용어화된다. 상술한 것의 조합들은 또한 컴퓨터-판독가능 매체의 범위 내에 속해야 한다. 컴퓨터-실행가능 명령들은, 예를 들어, 일반-목적 컴퓨터 시스템 또는 특수-목적 컴퓨터 시스템이 특정 기능이나 기능들의 그룹을 수행하도록 하는 명령들과 데이터를 포함한다. 컴퓨터 실행가능 명령들은, 예를 들어, 이진수, 어셈블리어와 같은 중간 형식 명령, 또는 소스 코드일 수도 있다.

본 설명 및 다음에 오는 청구범위에서, "컴퓨터 시스템"은, 전자 데이터에 연산을 함께 수행하기 위해 동작하는, 한 개 이상의 소프트웨어 모듈들, 한 개 이상의 하드웨어 모듈들, 또는 그것들의 조합들로서 정의된다. 예를 들어, 컴퓨터 시스템의 정의는 개인용 컴퓨터의 하드웨어 컴포넌트들, 및 개인용 컴퓨터의 운영 시스템과 같은, 소프트웨어 모듈들을 포함한다. 모듈들의 물리적 레이아웃은 중요하지 않다. 컴퓨터 시스템은 네트워크를 통해 결합된 한 개 이상의 컴퓨터들을 포함할 수 있다. 유사하게, 컴퓨터 시스템은, (메모리 및 프로세서와 같은) 내부 모듈들이 전자 데이터에 연산들을 수행하기 위해 함께 동작하는 한 개의 물리적 디바이스(모바일 전화 또는 PDA와 같은)를 포함할 수 있다.

당업자들은, 개인용 컴퓨터, 랩톱 컴퓨터, 휴대용 디바이스, 멀티-프로세서 시스템, 마이크로프로세서-기반 또는 프로그램가능한 소비자 전자 제품, 네트워크 PC, 미니 컴퓨터, 메인프레임 컴퓨터, 모바일 전화, PDA, 호출기 등을 포함하는, 다수 유형의 컴퓨터 시스템 구성들을 가진 네트워크 컴퓨팅 환경들에서 본 발명이 실시될 수 있음을 이해할 것이다. 본 발명

은 또한, 네트워크를 통해 링크된(유선 데이터 링크, 무선 데이터 링크, 또는 유선과 무선 데이터 링크들의 조합에 의해), 로컬 및 원격 컴퓨터 시스템들 모두가 작업들을 수행하는 분산 시스템 환경들에서 실시될 수 있다. 분산 시스템 환경에서, 프로그램 모듈들은 로컬과 원격 메모리 저장 디바이스들 모두에 위치될 수 있다.

도 1a는 웹 서비스들을 위한 신뢰되는 제3자 인증을 용이하게 하는 컴퓨터 아키텍처(100)의 일 예를 도시한다. 컴퓨터 아키텍처(100)에서 도시된 것처럼, 웹 서비스 클라이언트(101), 보안 토큰 서비스(102), 및 웹 서비스(108)가 네트워크(105)에 접속된다. 네트워크(105)는 LAN(Local Area Network), WAN(Wide Area Network), 또는 인터넷일 수도 있다. 네트워크(105)에 접속된 컴퓨터 시스템들과 모듈들은 네트워크(105)와 접속된 다른 컴퓨터 시스템들과 모듈들로부터 데이터를 수신하고 송신할 수 있다. 따라서, 웹 서비스 클라이언트(101), 보안 토큰 서비스(102), 및 웹 서비스(108), 및 다른 접속된 컴퓨터 시스템들과 모듈들(도시 안됨)은 메시지 관련된 데이터를 생성하고 네트워크(105)를 통해 메시지 관련된 데이터(예를 들어, 인터넷 프로토콜(Internet Protocol;IP) 데이터그램, 및 전송 제어 프로토콜(Transmission Control Protocol;TCP), 하이퍼텍스트 전송 프로토콜(Hypertext Transfer Protocol;HTTP), 단순 메일 전송 프로토콜(Simple Mail Transfer Protocol;SMTP) 등과 같은 IP 데이터그램들을 사용하는 다른 고층 프로토콜들)를 교환할 수 있다. 예를 들어, 웹 서비스 클라이언트(101)와 웹 서비스(108)는 SOAP 엔벨로프들(envelopes)을 생성할 수 있고, 네트워크(105)를 통해 SOAP 엔벨로프들(XML(eXtensible Markup Language) 데이터를 포함함)을 교환할 수 있다.

컴퓨터 아키텍처(100) 내에서, 레이블(label) 부분 "Pu"를 포함하는 드로잉(drawing) 레이블들은 공개/개인 키 쌍들의 공개 키들을 일컫기 위해 사용되고, 레이블 부분 "Pr"을 포함하는 드로잉 레이블들은 공개/개인 키 쌍들 중의 개인 키들을 일컫기 위해 사용됨을 이해해야 한다. 또한, 레이블 부분 Pu 또는 Pr을 포함하는 유사하게 숫자가 붙여진 드로잉 레이블들은 동일한 공개/개인 키 쌍 중의 공개 키 또는 대응하는 개인 키를 각각 일컫는다. 그러므로, 2 개의 상이한 공개/개인 키 쌍들이 컴퓨터 아키텍처(100)에 도시된다. 한 개의 공개/개인 키 쌍은 공개 키(163Pu)/개인 키(163Pr)로서 도시되고, 다른 공개/개인 키 쌍은 공개 키(164Pu)/개인 키(164Pr)로서 도시된다. 공개/개인 키 쌍들은 공개 키 기반구조(Public Key Infrastructure;PKI)의 일부일 수 있다.

개인 키(163Pr)는 보안 토큰 서비스(102)에 대응하는 개인 키일 수 있다. 그러므로, 웹 서비스 클라이언트(101)와 웹 서비스(108)는 대응하는 공개 키, 공개키(163Pu)로의 액세스가 주어질 수 있다. 유사하게, 개인 키(164Pr)는 웹 서비스(108)에 대응하는 개인 키일 수 있다. 그러므로, 웹 서비스 클라이언트(101)와 보안 토큰 서비스(102)는 대응하는 공개 키, 공개키(164Pu)로의 액세스가 주어질 수 있다. 따라서, 보안 토큰 서비스(102), 웹 서비스 클라이언트(101), 웹 서비스(108)는 공개/개인 키 쌍들, 공개 키(163Pu)/개인 키(163Pr) 및 공개 키(164Pu)/개인 키(164Pr)를 사용하여 적절하게 데이터를 싸인하고, 서명을 유효화하고, 데이터를 암호화하고, 데이터의 암호를 해독할 수 있다.

컴퓨터 아키텍처(100) 내에서, 레이블 부분 "Dr"을 포함하는 드로잉 레이블들이 다른 대칭적 키들로부터 유도되는 대칭적 키들을 일컫기 위해 사용됨을 이해해야 한다. 예를 들어, 도 1b를 간략하게 참조하면, 유도된 클라이언트/STS 세션 키(114Dr)가 클라이언트/STS 세션 키(114)로부터 유도된다. 따라서, 보안 토큰 서비스(102), 웹 서비스 클라이언트(101), 웹 서비스(108)는 또한 (잠재적으로 유도된)대칭적 키들(즉, 세션 키들)을 사용하여 데이터를 싸인하고, 서명을 유효화하고, 데이터를 암호화하고, 데이터의 암호를 해독할 수 있다. 대칭적 키들은 컴퓨터 아키텍처(100)의 컴포넌트들 간에 공유될 수 있거나, 또는 특정 컴포넌트에 대해 비밀로 남아있을 수 있다. 예를 들어, 보안 토큰 서비스(102)는 비밀 대칭적 키(161)를 관리할 수 있다.

보안 토큰 서비스(102)는 인증 서비스(103)와 액세스 부여 서비스(106)를 포함한다. 인증 서비스(103)는 웹 서비스 컴포넌트들(예를 들어, 웹 서비스 클라이언트(101))로부터 인증 요청들을 수신하고, 웹 서비스 컴포넌트들을 인증하고, 및 요청하는 웹 서비스 컴포넌트들로 인증 응답들을 리턴하도록 구성된다. 인증 모듈(103)은, 예를 들어, 신임장(credential) 데이터베이스 또는 증명서 유효화 데이터와 같은 인증 데이터(104)를 참조하여 웹 서비스 컴포넌트를 인증할 수 있다. 액세스 부여 서비스(106)는 웹 서비스 컴포넌트들로부터의 액세스 부여 요청들을 수신하고, 웹 서비스에 액세스가 부여되는지를 결정하고, 요청하는 웹 서비스 컴포넌트들로 액세스 부여 응답을 리턴하기 위해 구성된다. 액세스 부여 서비스(106)는, 예를 들어, 웹 서비스 관리자에 의해 설정되는 정책과 같은, 정책 데이터(107)를 참조하여 액세스가 부여되는지를 결정할 수 있다.

웹 서비스 클라이언트(101)는 분산된 애플리케이션의 클라이언트 부분일 수 있다. 신뢰(191)는 웹 서비스 클라이언트(101)가 보안 토큰 서비스(102)와 수립된 신뢰 관계를 가짐을 나타낸다. 즉, 웹 서비스 클라이언트(101)는 보안 토큰 서비스(102)를 신뢰한다. 신뢰(191)는 미리 수립될 수 있고 및/또는 대역 밖의 통신으로부터 나올 수 있다. 예를 들어, 신뢰(191)는 대칭적 키 신뢰 또는 X.509 증명서 신뢰일 수 있다.

웹 서비스(108)는 분산된 애플리케이션의 서버 부분일 수 있다. 일부 실시예들에서, 웹 서비스(108)는, 예를 들어, 인스턴스들(108A, 108B, 및 108C)과 같은, 복수 개의 웹 서비스 인스턴스들을 포함하는 웹 서비스 팜(farm)이다. 각 인스턴스(108A, 108B, 및 108C)에 접속된 웹 서비스 클라이언트들에 대한 상태 정보는 분산된 캐쉬(109)에서 선택적으로 보존되어, 웹 서비스 클라이언트들이 인스턴스들(108A, 108B, 및 108C) 간에 더 효율적으로 이동할 수 있도록 할 수 있다.

신뢰(192)는 웹 서비스(108)가 보안 토큰 서비스(102)와 수립된 신뢰 관계를 가짐을 나타낸다. 즉, 웹 서비스(108)는 보안 토큰 서비스(102)를 신뢰한다. 신뢰(192)는 미리 수립될 수 있고, 및/또는 대역 밖 통신으로부터 나올 수도 있다. 예를 들어, 신뢰(192)는 대칭적 키 신뢰 또는 X.509 증명서 신뢰일 수 있다.

도 1b는 컴퓨터 아키텍처(100)로부터 웹 서비스 클라이언트(101)와 보안 토큰 서비스(102)의 다른 묘사를 도시한다. 도 1b는 또한 웹 서비스 클라이언트(101)와 보안 토큰 서비스(102) 간에 교환되는(즉, 네트워크(105)를 통해) 다수의 전자 메시지들을 도시한다. 도시된 것처럼, 도 1b의 데이터 소자들 중의 일부는 괄호 기재를 포함한다. 예를 들어, 서명(119)은 괄호 기재 "(비밀 대칭적 키(161))"를 포함한다. 이들 괄호 기재들은 암호화 데이터를 암호화하기 위해 또는 싸인된 데이터를 싸인하기 위해 무슨 키가 사용되었는지 또는 어떻게 데이터가 보안화되는 지를 나타내기 위해 사용된다.

그러므로, 서명(119)을 다시 참조하면, 괄호 기재 "(비밀 대칭적 키(161))"는 비밀 대칭적 키(161)가 서명(119)을 생성하기 위해 사용됨을 나타낸다. 유사하게, 이제 암호화된 클라이언트-서비스 세션 키(131B)의 참조에서, 괄호 기재 "(공개 키(164Pu))"는 공개 키(164Pu)가 암호화된 클라이언트-서비스 세션 키(131B)를 암호화하기 위해 사용됨을 나타낸다. 이제 보안화된 클라이언트/STS 세션 키(114A)의 참조에서, 괄호 기재 "(보안 채널 또는 X.509)"는 보안화된 클라이언트/STS 세션 키(114)가 보안 채널 또는 X.509 증명서의 공개 키를 사용하여 보안됨을 나타낸다.

도 2는 웹 서비스를 액세스하기 위한 서비스 토큰을 얻는 방법(200)의 순서도의 일 예를 도시한다. 방법(200)은 도 1b의 컴포넌트들과 데이터에 대해 기재될 것이다.

방법(200)은 인증 요청을 송신하는 동작(동작 201)을 포함한다. 예를 들어, 웹 서비스 클라이언트(101)는 인증 서비스(103)로 인증 요청(111)을 송신할 수 있다. 인증 요청(111)은, 예를 들어, HTTPS와 같은, 보안 채널을 사용하여 보호되는 사용자명과 패스워드를 포함할 수 있다. 다른 경우에, 인증 요청(111)은 웹 서비스 클라이언트(101)에 대응하는 개인 키(도시 안됨)로 싸인되는 X.509 증명서를 포함할 수 있다.

방법(200)은 인증 요청을 수신하는 동작(동작 205)을 포함한다. 예를 들어, 인증 서비스(103)는 인증 요청(111)을 수신할 수 있다. 방법(200)은 인증 데이터를 유효화하는 동작(동작 206)을 포함한다. 예를 들어, 인증 서비스(103)는 인증 요청(111)에 포함된 사용자명과 패스워드를 인증 데이터(104)(즉, 신임장 데이터베이스)와 비교할 수 있다. 다른 경우에, 인증 서비스(103)는 인증 데이터(104)(즉, PKI)를 참조하여 웹 서비스 클라이언트(101)를 위한 공개 키의 위치를 파악하고, 그 공개 키를 사용하여 인증 요청(111)의 서명을 유효화할 수 있다.

방법(200)은 대칭적 세션 키를 포함하는 인증 응답을 송신하는 동작(동작 207)을 포함한다. 예를 들어, 보안 토큰 서비스(102)는 웹 서비스 클라이언트(101)로 인증 응답(112)을 송신할 수 있다. 인증 응답(112)은 증명 토큰(113)과 토큰 부여 토큰(116)을 포함한다. 증명 토큰(113)과 토큰 부여 토큰(116) 모두는, 웹 서비스 클라이언트(101)와 액세스 부여 서비스(106) 간의 통신을 안전하게 하기 위해 사용될 수 있는 클라이언트/STS 세션 키(114)(대칭적 키)의 인스턴스를 포함한다. 증명 토큰(113)은, 보안 채널을 통해 또는 X.509 증명서의 공개 키를 통해 암호화되는 보안화된 클라이언트/STS 세션 키(114A)를 포함한다.

토큰 부여 토큰(116)은 비밀 대칭적 키(161)를 사용하여 암호화되는 암호화된 클라이언트/STS 세션 키(114B)를 포함한다. 토큰 부여 토큰(116)은 또한, 토큰 부여 토큰(118)이 발행될 때를 나타내는 타임 스탬프(time stamp)(118)를 포함한다. 간섭을 막기 위해, 토큰 부여 토큰(116)은 또한 비밀 대칭적 키(161)를 사용하여 생성되는 서명(119)을 포함한다. 다른 경우에, 다른 비밀 대칭적 키가 서명(119)을 생성하기 위해 사용될 수 있다.

인증 응답(112)은 개인 키(163Pr)(보안 토큰 서비스(102)의 개인 키)를 사용하여 생성되는 서명(121)을 포함한다. 서명(121)은 수신하는 컴포넌트에게 보안 토큰 서비스(102)가 인증 응답(112)을 생성하였음을 나타낸다.

방법(200)은 대칭적 세션 키를 포함하는 인증 응답을 수신하는 동작(동작 202)을 포함한다. 예를 들어, 웹 서비스 클라이언트(101)는 인증 응답(112)을 수신할 수 있다. 웹 서비스(101)는 공개 키(163Pu)를 사용하여 서명(121)을 유효화한다(그러므로, 인증 응답(112)을 유효화함). 웹 서비스 클라이언트(101)는 증명 토큰(113)으로부터 클라이언트/STS 세션 키(114A)를 발췌하여, 클라이언트/STS 세션 키(114)의 복사본을 유지할 수 있다.

웹 서비스 클라이언트(101)는 클라이언트/STS 세션 키(114)로부터, 예를 들어, 유도된 클라이언트/STS 세션 키(114Dr)와 같은 다른 세션 키들을 유도할 수 있다. 후속적으로, 예를 들어, 웹 서비스 클라이언트(101)가 웹 서비스와 통신하려 할 때, 웹 서비스 클라이언트(101)는 (잠재적으로 유도된) 세션 키를 사용하여 액세스 부여 서비스(106)와의 통신을 보안화할 수 있다. 또한, 보안 토큰 서비스(102)가 클라이언트/STS 세션 키(114)로부터 다른 세션 키들을 유도하는 것일 수 있다.

웹 서비스 클라이언트(101)와 보안 토큰 서비스(102)는 동일한 키 유도 알고리즘들을 사용하여 웹 서비스 클라이언트(101)와 보안 토큰 서비스(102)에서 유도된 키들이 유도 후에 계속하여 대칭이 되도록 할 수 있다. 그러므로, 보안 토큰 서비스(102)는 또한 클라이언트/STS 세션 키(114)로부터 유도된 클라이언트/STS 세션 키(114Dr)를 유도할 수 있다.

방법(200)은 웹 서비스에 액세스하기 위해 액세스 요청을 송신하는 동작(동작 203)을 포함한다. 예를 들어, 웹 서비스 클라이언트(101)는 액세스 부여 서비스(106)에 액세스 부여 요청(122)을 송신할 수 있다. 액세스 부여 요청(122)은 토큰 부여 토큰(116)을 포함한다. 액세스 부여 요청(122)은 유도된 클라이언트/STS 세션 키(114Dr)를 사용하여 생성되는 서명(127)을 포함한다. 서명(127)은 액세스 부여 요청(122)이 웹 서비스 클라이언트(101)와 보안 토큰 서비스(102) 간의 인증 세션에 포함됨을 나타낸다.

방법(200)은 웹 서비스로 액세스를 위한 액세스 요청을 수신하는 동작(동작 208)을 포함한다. 예를 들어, 액세스 부여 서비스(106)는 웹 서비스 클라이언트(101)로부터 액세스 부여 요청(122)을 수신할 수 있다. 방법(200)은 인증 세션을 확인하는 동작(동작 209)을 포함한다. 예를 들어, 액세스 부여 서비스(106)는 웹 서비스 클라이언트(101)가 보안 토큰 서비스(102)로의 인증 세션을 가짐을 확인할 수 있다. 액세스 부여 요청(122)의 수령에 후속하여, 액세스 부여 서비스(106)는 유도된 클라이언트/STS 세션 키(114Dr)를 사용하여 서명(127)을 유효화할 수 있다(이에 따라, 액세스 부여 요청(122)을 유효화함).

그 다음, 액세스 부여 서비스(106)는 비밀 대칭적 키(161)를 사용하여 서명(119)을 유효화할 수 있다(이에 따라, 토큰 부여 토큰(116)을 유효화함). 액세스 부여 서비스(106)는 또한 비밀 대칭적 키(116)를 사용하여 암호화된 클라이언트/STS 세션 키(114B)의 암호를 해독하여, 클라이언트/STS 세션 키(114)를 드러낼 수 있다. 클라이언트/STS 세션 키(114)의 인스턴스를 포함하는 토큰 부여 토큰(116)에 기초하여, 액세스 부여 서비스는 웹 서비스 클라이언트(101)가 보안 토큰 서비스(102)로의 인증된 세션을 갖는다고 결정한다.

방법(200)은 액세스 응답을 송신하는 동작(동작 211)을 포함한다. 예를 들어, 액세스 부여 서비스(106)는 웹 서비스 클라이언트(101)에 액세스 부여 응답(128)을 송신할 수 있다. 액세스 부여 응답(128)은 증명 토큰(129)과 서비스 토큰(132)을 포함한다. 증명 토큰(129)과 서비스 토큰(132) 모두는 웹 서비스 클라이언트(101)와 웹 서비스(108) 간의 통신을 안전하게 하기 위해 사용될 수 있는 클라이언트-서비스 세션 키(131)(대칭적 키)의 인스턴스를 포함한다. 증명 토큰(129)은 클라이언트/STS 세션 키(114)(또는 그것의 유도물)를 사용하여 암호화된 클라이언트-서비스 세션 키(131A)를 포함한다. 그러므로, 웹 서비스 클라이언트(101)는 (클라이언트/STS 세션 키(114) 또는 그것의 유도물을 사용하여) 암호화된 클라이언트-서비스 세션 키(131A)를 해독하여 클라이언트-서비스 세션 키(131)를 드러낼 수 있다.

서비스 토큰(132)은 공개 키(164Pu)(웹 서비스(108)를 위한 공개 키)를 사용하여 암호화된 클라이언트-서비스 세션 키(131B)를 포함한다. 서비스 토큰(132)이 보안 토큰 서비스(102)로부터 나온 것을 나타내기 위해, 서비스 토큰(132)은 개인 키(163Pr)(보안 토큰 서비스(102)를 위한 개인 키)를 사용하여 생성되는 서명(134)을 포함한다. 그러므로, 웹 서비스(108)는 공개 키(163Pu)(보안 토큰 서비스(102)를 위한 대응하는 공개 키)를 사용하여 서명(134)을 유효화하여, 서비스 토큰(132)이 보안 토큰 서비스(102)로부터 전송됨을 확인할 수 있다. 웹 서비스(108)는 또한 개인 키(164Pr)(웹 서비스(108)를 위한 대응하는 개인 키)를 사용하여 암호화된 클라이언트-서비스 세션 키(131B)를 해독할 수 있다.

따라서, 클라이언트-서비스 세션 키는 보안 방식으로 클라이언트와 서비스 모두로 전송될 수 있다.

방법(200)은 액세스 응답을 수신하는 동작(동작 204)을 포함한다. 예를 들어, 웹 서비스 클라이언트(101)는 액세스 부여 응답(128)을 수신할 수 있다. 증명 토큰(129)으로부터, 웹 서비스 클라이언트는 암호화된 클라이언트-서비스 세션 키

(131A)(클라이언트/STS 세션 키(114) 또는 그것의 유도물을 사용함)를 해독하여 클라이언트-서비스 세션 키(131)를 드러낼 수 있다. 웹 서비스 클라이언트(101)는 클라이언트-서비스 세션 키(131)를 저장하여 웹 서비스(108)와의 후속적 통신을 용이하게 할 수 있다. 웹 서비스 클라이언트(101)는 또한, 웹 서비스(108)로의 후속적 전송을 위해 서비스 토큰(132)을 저장할 수 있다.

도 1c는 컴퓨터 아키텍처(100)로부터 웹 서비스 클라이언트(101), 보안 토큰 서비스(102), 및 웹 서비스(108)의 다른 묘사를 도시한다. 도 1b는 또한 웹 서비스 클라이언트(101)와 웹 서비스(108) 간에 교환되는(즉, 네트워크(105)를 통해) 다수의 전자 메시지들을 도시한다. 도 3은 웹 서비스 컴포넌트와 웹 서비스 간의 통신을 안전하게 하기 위한 방법(300)의 순서도의 일 예를 도시한다. 방법(300)은 도 1c의 컴포넌트들과 데이터에 대해 기술될 것이다.

방법(300)은 보안 토큰 요청을 송신하는 동작(동작 301)을 포함한다. 예를 들어, 웹 서비스 클라이언트(101)는 웹 서비스(108)의 인스턴스(108A)로 보안 토큰 요청(136)을 송신할 수 있다. 보안 토큰 요청(136)은 서비스 토큰(132)(보안 토큰 서비스(102)로부터 발행됨)을 포함한다. 보안 토큰 요청(136)은 클라이언트-서비스 세션 키(131)를 사용하여 생성되는 서명(141)을 포함한다. 보안 토큰 요청(136)은 또한 웹 서비스(101)에 대응하는 신원 정보를 포함할 수 있다.

방법(300)은 보안 토큰 요청을 수신하는 동작(동작 304)을 포함한다. 예를 들어, 인스턴스(108a)는 웹 서비스 클라이언트(101)로부터 보안 토큰 요청(136)을 수신할 수 있다. 방법(300)은 암호화된 세션 키를 해독하기 위해 개인 키를 사용하는 동작(동작 305)을 포함한다. 예를 들어, 인스턴스(108A)는 개인 키(164Pr)를 사용하여 암호화된 클라이언트-서비스 세션 키(131B)를 해독하여, 클라이언트-서비스 세션 키(131)를 드러낼 수 있다. 인스턴스(108A)는 또한 공개 키(163Pu)를 사용하여 서명(134)을 유효화하여, 서비스 토큰(132)이 보안 토큰 서비스(102)로부터 송신됨을 확인할 수 있다. 후속적으로, 인스턴스(108A)는 (이전에 드러난)클라이언트-서비스 세션 키(131)를 사용하여 서명(141)을 유효화할 수 있다.

방법(300)은 웹 서비스를 액세스하기 위해 웹 서비스 컴포넌트를 승인하는 동작(동작 306)을 포함한다. 예를 들어, (특정한 정책들에 기초한) 웹 서비스(108)는 웹 서비스 클라이언트(101)가 웹 서비스(108)를 액세스하도록 승인할 수 있다. 방법(300)은 마스터 대칭적 세션 키를 생성하는 동작(동작 307)을 포함한다. 예를 들어, 웹 서비스(108)는 웹 서비스 클라이언트(101)와 웹 서비스(108)의 인스턴스들 간의 통신을 안전하게 하기 위해 마스터 클라이언트-서비스 세션 키(193)를 생성할 수 있다.

방법(300)은 마스터 대칭적 세션 키를 암호화하는 동작(동작 308)을 포함한다. 예를 들어, 인스턴스(108A)는 클라이언트-서비스 세션 키(131)를 사용하여 마스터 클라이언트-서버 세션 키(193)를 암호화하여, 암호화된 마스터 클라이언트-서버 세션 키(193A)를 생성할 수 있다. 인스턴스(108A)는 보안 토큰 응답(142)에서 보안 컨텍스트 토큰(146)과 함께 암호화된 마스터 클라이언트-서버 세션 키(193A)를 포함할 수 있다. 보안 토큰 컨텍스트는, 웹 서비스 클라이언트(101)와 웹 서비스(108)의 인스턴스들 간의 보안 통신을 위해 보안 컨텍스트 데이터를 포함한다.

일부 실시예들에서, 보안 컨텍스트 토큰(146)은 선택적 이진 확장(147)을 포함한다. 이진 확장(147)을 수신하는 웹 서비스 인스턴스들은 이진 확장(147)에서 포함된 데이터를 사용하여 서버측 분산된 캐쉬를 참조할 필요가 없이 보안 상태들을 재구성할 수 있다. 따라서, 이진 확장(147)을 사용하는 실시예들에서, 웹 서비스들은 서버측 분산된 캐쉬를 유지해야 하는 것으로부터 해방된다. 또한, 이진 형식으로 보안 컨텍스트 정보를 나타내는 것은, 잠재적으로 자원-집중적, XML 규정화를 수행할 필요가 없이 보안 컨텍스트 토큰 프로세싱을 용이하게 한다.

방법(300)은 보안 토큰 응답을 송신하는 동작(동작 309)을 포함한다. 예를 들어, 인스턴스(108A)는 웹 서비스 클라이언트(101)로 보안 토큰 응답(142)을 송신할 수 있다. 방법(300)은 보안 토큰 응답을 수신하는 동작을 포함한다. 예를 들어, 웹 서비스 클라이언트(101)는 인스턴스(108A)로부터 보안 토큰 응답(142)을 수신할 수 있다. 웹 서비스 클라이언트(101)는 클라이언트-서비스 세션 키(131)를 사용하여 암호화된 마스터 클라이언트-서버 세션 키(193A)를 해독하여, 마스터 클라이언트-서버 세션 키(193)를 드러낼 수 있다. 따라서, 웹 서비스 클라이언트(101)와 웹 서비스(108)의 인스턴스들 간의 후속적 통신은, 마스터 클라이언트-서비스 세션 키 또는 그것의 유도물들을 사용하여 보안화될 수 있다.

일반 키 유도 알고리즘에 따라, 웹 서비스 클라이언트(101)와 웹 서비스(108) 모두는 마스터 클라이언트-서버 세션 키(193)로부터, 예를 들어, 마스터 클라이언트-서버 세션 키들(193Dr1, 193Dr2, 193Dr3, 및 193Dr4)과 같은, 추가 대칭적 세션 키들을 유도할 수 있다. 그 다음, 웹 서비스 클라이언트(101)와 웹 서비스(108)는 서로 간의 통신을 안전하게 하기 위해 유도된 키들을 사용할 수 있다.

방법(300)은 유도된 키들을 사용하는 데이터를 교환하는 동작들(동작(303)과 동작(310))을 포함한다. 예를 들어, 웹 서비스 클라이언트(101)는 유도된 키(193Dr1)를 사용하여 암호화된 서비스 요청(148)을 생성할 수 있다. 암호화된 서비스 요청(148)은 보안 컨텍스트 토큰(146)과 요청 데이터(194)를 포함한다. 암호화된 서비스 요청(148)은 또한 유도된 키(193Dr3)를 사용하여 생성되는 서명(152)을 포함한다.

인스턴스(108C)는 암호화된 서비스 요청(148)을 수신할 수 있다. 인스턴스(108C)는 유도된 키(193Dr1)를 사용하여 보안 컨텍스트 토큰(146)과 요청 데이터(194)를 드러내는 암호화된 서비스 요청(148)을 해독할 수 있다. 인스턴스(108C)는 또한 유도된 키(193Dr3)를 사용하여 서명(152)을 유효화하여, 암호화된 서비스 요청(148)이 웹 서비스 클라이언트(101)와 웹 서비스(108) 간의 보안 통신의 일부임을 확인할 수 있다. 인스턴스(108C)는 보안 컨텍스트 토큰(146)과 요청 데이터(194)를 프로세스하여 어떻게 웹 서비스 클라이언트(101)에 응답할 지를 결정할 수 있다.

인스턴스(108C)는 유도된 키(193Dr2)를 사용하여 암호화된 서비스 응답(153)을 생성할 수 있다. 암호화된 서비스 응답(153)은 요청 데이터(194)에 응답적인 응답 데이터(196)를 포함한다. 암호화된 서비스 응답(153)은 또한 유도된 키(193Dr4)를 사용하여 생성되는 서명(154)을 포함한다.

웹 서비스 클라이언트(101)는 암호화된 서비스 응답(153)을 수신할 수 있다. 웹 서비스 클라이언트(101)는 유도된 키(193Dr2)를 사용하여 응답 데이터(196)를 드러내는 암호화된 서비스 응답(153)을 해독할 수 있다. 웹 서비스(101)는 또한 유도된 키(193Dr4)를 사용하여 서명(154)을 유효화하여, 암호화된 서비스 응답(153)이 웹 서비스 클라이언트(101)와 웹 서비스(108) 간의 보안 통신의 일부임을 확인할 수 있다.

그러므로, 본 발명의 실시예들은, 예를 들어, PKI와 같은, 기존 키 기반구조들의 이점을 취하는 보안 통신을 위한 공개/개인 키 쌍들(예를 들어, 공개 키(163Pu)/개인 키(163Pr) 및 공개 키(164Pu)/개인 키(164Pr))를 처음에 사용할 수 있다. 보안 통신을 위해 대칭적 세션 키들(예를 들어, 마스터 클라이언트-서비스 세션 키(193) 및 그것의 유도물들)을 사용하여 후속적 천이가 이루어질 수 있다. 따라서, 본 발명의 실시예들은 기존 공개 키 기반구조들의 키 관리 특징들을 사용하고, 후속하여 효율성을 위해 대칭적 키들로 천이할 수 있다.

토큰 부여 토큰들(예를 들어, 토큰 부여 토큰(116))과 서비스 토큰들(예를 들어, 서비스 토큰(132))은 맞춤 XML 토큰들로서 표현될 수 있다. 다음 XML 명령들은 본 발명의 원리들에 따른 맞춤 XML 토큰의 기재의 예이다:

```
1.      <contoso:IdentityTokenEx contoso:TokenId=... contoso:MajorVersion=...
contoso:MinorVersion=... contoso:Issuer=... contoso:IssueTime=... contoso:Purpose=...>
2.      <contoso:Conditions NotBefore="..." NotOnOrAfter="..." />
3.       <wsp:AppliesTo>
4.          <wsa:EndpointReference>
5.           <wsa:Address>...</wsa:Address>
6.          </wsa:EndpointReference>
7.         </wsp:AppliesTo>
8.          <contoso:TokenStatement contoso:AuthenticationMechanism=...
           contoso:AuthenticationTime=... />
9.          <contoso:SubjectName>...</contoso:SubjectName>
10.        <ds:KeyInfo>
11.        <xenc:EncryptedKey Id=... >
12.         <xenc:EncryptionMethod Algorithm=... />
13.         <ds:KeyInfo >
14.              <wsse:SecurityTokenReference>
15.               <wsse:KeyIdentifier ValueType=... EncodingType=... >
16.         ...
17.              </wsse:KeyIdentifier>
18.             </wsse:SecurityTokenReference>
19.           </ds:KeyInfo>
20.             <xenc:CipherData>
21.              <xenc:CipherValue>
22.              ...
23.             </xenc:CipherValue>
24.             </xenc:CipherData>
25.          </xenc:EncryptedKey>
26.        </ds:KeyInfo>
27.       </contoso:TokenStatement>
28.       <ds:Signature >
29.        <ds:SignedInfo>
30.             <ds:CanonicalizationMethod
                  Algorithm='http://www.w3.org/2001/10/xml-exc-c14n#' />
31.         <ds:SignatureMethod Algorithm=... />
32.        <ds:Reference URI=... >
33.         <ds:Transforms>
34.          <ds:Transform
               Algorithm='http://www.w3.org/2000/09/xmldsig#enveloped_signature' />
35.         <ds:Transform Algorithm='http://www.w3.org/2001/10/xml-exc-c14n#' />
36.              </ds:Transforms>
37.              <ds:DigestMethod Algorithm=... />
38.              <ds:DigestValue>...</ds:DigestValue>
39.             </ds:Reference>
40.        </ds:SignedInfo>
41.        <ds:SignatureValue>...</ds:SignatureValue>
42.        <ds:KeyInfo>
43.             <wsse:SecurityTokenReference>
44.              <wsse:KeyIdentifier ValueType=... EncodingType=... >...
45.              </wsse:KeyIdentifier>
46.             </wsse:SecurityTokenReference>
47.        </ds:KeyInfo>
48.       </ds:Signature>
49.     </contoso:IdentityTokenEx>
```

라인 1에서, IdentityTokenEx\@TokenId 속성은 URI를 사용하여 보안 토큰을 식별한다. 데이터 유형은 xsd:ID이다. 각 보안 토큰 URI는 송신자와 수취인 모두에게 특정한 것일 수 있다. URI 값들은 시간 및 공간에 있어서 전세계적으로 독특한 값이다. 또한 라인 1에서, IdentityTokenEx\@MajorVersion 속성은 이 맞춤 토큰의 주(major) 버전을 식별하고, IdentityTokenEx\@MinorVersion 속성은 이 맞춤 토큰의 부(minor) 버전을 식별한다. 또한 라인 1에서, IdentityTokenEx\@Issuer 속성은 URI를 사용하여 이 토큰의 발행자를 식별한다. 또한 라인 1에서, IdentityTokenEx\@IssueTime 속성은 토큰이 발행된 시간(즉, UTC 형식)을 나타낸다. 이 값을 위한 XML 스키마(schema)는 xsd:dateTime이다,

또한 라인1에서, IdentityTokenEx\@Purpose 속성은, QName을 사용하여, 이 맞춤 토큰의 목적을 식별한다. 값들은 다음을 포함할 수 있다:

QName	설명

contoso:TokenGrantingToken	액세스 부여 서비스에 의해 다른 서비스 토큰을 부여하기 위해 사용되는 토큰
contoso:ServiceToken	애플리케이션 웹 서비스를 액세스하기 위해 사용되는 토큰

라인 2에서, IdentityTokenEx\contoso:Conditions 소자는 이 토큰이 유효한 조건들을 명시한다. 또한 라인 2에서, IdentityTokenEx\Conditions\@NotBefore 속성은 이 토큰이 유효하게 되는 가장 빠른 시간(즉, UTC 형식)을 명시한다. 이 값에 대한 스키마는 xsd:dateTime이다. 또한 라인 2에서, IdentityTokenEx\Conditions\@NotOnOrAfter 속성은 이 토큰이 무효하게 되는 가장 빠른 시간(즉, UTC 형식)을 명시한다. 이 값에 대한 스키마는 xsd:dateTime이다.

라인 3 내지 7에서, IdentityTokenEx\wsp:AppliesTo 소자는 이 토큰이 유효하게 되는 종단점을 명시한다. 라인 4 내지 6에서, IdentityTokenEx\AppliesTo\wsa:EndpointReference 소자는 토큰이 유효한 종단점으로의 참조를 포함한다. 라인 5에서, IdentityTokenEx\AppliesTo\EndpointReference\wsa:Address 소자는 종단점의 URI를 명시한다.

라인 8 내지 27에서, IdentityTokenEx\TokenStatement 소자는 인증된 세션에 관련된 인증 및 신원 정보를 포함한다. 또한 라인 8에서, IdentityTokenEx\TokenStatement\@AuthenticationMechanism 속성은, Qname을 사용하여, 대상을 인증하기 위해 사용되는 인증 메커니즘을 식별한다. 값들은 다음을 포함할 수 있다:

Qname	설명
contoso:password	사용자명과 패스워드가 대상을 인증하기 위해 사용된다.
contoso:x509certificate	X.509 증명서가 대상을 인증하기 위해 사용된다.

또한, 라인 8에서, IdentityTokenEx\TokenStatement\@AuthenticationTime 소자는 인증이 발생할 때 시간(즉, UTC 형식)을 지정한다. 이 값에 대한 XML 스키마는 xsd:dateTime이다.

라인 9에서, IdentityTokenEx\TokenStatement\SubjectName 소자는 인증된 당사자(party)를 식별한다. 라인 10 내지 26에서, IdentityTokenEx\TokenStatement\ds:KeyInf 소자는 이 토큰을 통해 교환되는 세션 키를 포함한다. 라인 11 내지 25에서, IdentityTokenEx\TokenStatement\KeyInfo\xenc:EncryptedKey 소자는 암호화된 세션 키를 포함한다. 라인 28 내지 48에서, IdentityTokenEx\ds:Signature 소자는 맞춤 XML 토큰에 대해 엔벨로프된 서명을 포함한다.

일부 실시예들에서, 웹 서비스 컴포넌트들과 웹 서비스들은 확장된 보안 컨텍스트 토큰들(즉, 보안 컨텍스트 토큰(146))을 교환할 수 있다. 다음 XML 명령들은 본 발명의 원리들에 따라 확장된 보안 컨텍스트 토큰의 기재의 예이다.

```
60.   <wst:SecurityContextToken wsu:Id=... >
61.     <wsu:Identifier>...</wsu:Identifier>
62.      <contoso:SctExtension>
63.      MIIEZzCCA9CgAwIBAgIQEmtJZc0...
64.      </contoso:SctExtension>
65.   </wst:SecurityContextToken>
```

라인 62 내지 64에서, SecurityContextToken\contoso:SctExtension 소자는 base64 이진 형식으로 인코딩된 SCT 맞춤 확장들을 포함한다.

토큰 부여 토큰들, 서비스 토큰, 및 확장된 보안 컨텍스트 토큰들을 기술하는 XML 명령들은, 예를 들어, 컴퓨터 아키텍처(100)의 컴포넌트들 간에 교환되는, 인증 응답(112), 액세스 부여 응답(128), 및 보안 토큰 응답(124)과 같은 SOAP 메시지에 포함될 수 있다.

도 4는 본 발명의 원리들을 위한 적절한 운영 환경을 도시한다. 도 4 및 다음의 논의는 본 발명이 구현될 수 있는 적절한 운영 환경의 간략하고, 일반적인 설명을 제공하려고 의도된다. 요구되지는 않지만, 본 발명은, 컴퓨터 시스템들에 의해 실행되는, 프로그램 모듈들과 같은, 컴퓨터-실행가능한 명령들의 일반 문맥으로 기재될 것이다. 일반적으로, 프로그램 모듈들은, 특정 작업들을 수행하거나 또는 특정 추상 데이터 유형들을 구현하는, 루틴, 프로그램, 객체, 컴포넌트, 데이터 구조 등을 포함한다. 컴퓨터-실행가능한 명령, 연관된 데이터 구조, 및 프로그램 모듈은 본 명세서에 개시된 방법들의 동작들을 실행하는 프로그램 코드 수단의 예들을 나타낸다.

도 4를 참조하면, 본 발명을 구현하는 시스템의 일 예는, 프로세싱 유닛(421), 시스템 메모리(422), 및 시스템 메모리(422)를 포함하는 다양한 시스템 컴포넌트들을 프로세싱 유닛(421)에 결합하는 시스템 버스(423)를 포함하는 컴퓨터 시스템(420)의 형태로 일반-목적 컴퓨팅 디바이스를 포함한다. 프로세싱 유닛(421)은, 본 발명의 특징들을 포함하는, 컴퓨터 시스템(420)의 특징들을 구현하기 위해 고안된 컴퓨터-실행가능 명령들을 실행할 수 있다. 시스템 버스(423)는 메모리 버스나 메모리 제어기, 주변기기 버스, 및 다양한 버스 아키텍처들 중의 임의의 것을 사용하는 로컬 버스를 포함하는 여러 유형의 버스 구조들 중의 임의의 것일 수 있다. 시스템 메모리는 ROM(read only memory;424) 및 RAM(random access memory;425)을 포함한다. 스타트업(start up) 동안에서와 같이, 컴퓨터 시스(420) 내의 소자들 간에 정보 전송을 돕는 기본 루틴들을 포함하는, 기본 입/출력 시스템(basic input/output system;BIOS;426)은 ROM(424)에 저장될 수 있다.

컴퓨터 시스템(420)은 또한 자기 하드 디스크(439)에 읽고 쓰는 자기 하드 디스크 드라이브(427), 분리형 자기 디스크(429)에 읽고 쓰는 자기 디스크 드라이브(428), 및, 예를 들어, CD ROM 또는 다른 광 매체와 같은, 분리형 광 디스크(431)에 읽고 쓰는 광 디스크 드라이브(430)를 포함할 수 있다. 자기 하드 디스크 드라이브(427), 자기 디스크 드라이브(428), 및 광 디스크 드라이브(430)는 하드 디스크 드라이브 인터페이스(432), 자기 디스크 드라이브 인터페이스(433), 및 광 드라이브 인터페이스(434)에 의해 각각 시스템 버스(423)에 접속된다. 드라이브들과 그들의 연관된 컴퓨터-판독가능 매체는 컴퓨터-실행가능 명령, 데이터 구조, 프로그램 모듈, 및 컴퓨터 시스템(420)에 대한 기타 데이터의 비휘발성 저장을 제공한다. 본 명세서에 기재된 환경의 예가 자기 하드 디스크(439), 분리형 자기 디스크(429), 및 분리형 광 디스크(431)를 채택하지만, 자기 카세트, 플래쉬 메모리 카드, DVD(digital versatile disk), 버놀리 카트리지(Bernoulli cartridge), RAM, ROM 등을 포함하는, 데이터를 저장하기 위한 다른 유형들의 컴퓨터 판독가능 매체가 사용될 수 있다.

한 개 이상의 프로그램 모듈들을 포함하는 프로그램 코드 수단은, 운영 시스템(435), 한 개 이상의 애플리케이션 프로그램들(436), 기타 프로그램 모듈들(437), 및 프로그램 데이터(438)를 포함하는, 하드 디스크(439), 자기 디스크(429), 광 디스크(431), ROM(424), 또는 RAM(425)에 저장될 수 있다. 사용자는 키보드(440), 포인팅 디바이스(442), 또는, 예를 들어, 마이크로폰, 조이 스틱, 게임 패드, 스캐너 등과 같은, 다른 입력 디바이스들(도시 안됨)을 통해 컴퓨터 시스템(420)으로 커맨드와 정보를 입력할 수 있다. 상기 및 다른 입력 디바이스들은 시스템 버스(423)에 결합된 입력/출력 인터페이스(446)를 통해 프로세싱 유닛(421)에 접속될 수 있다. 입력/출력 인터페이스(446)는 논리적으로, 예를 들어, 직렬 포트 인터페이스, PS/2 인터페이스, 병렬 포트 인터페이스, USB(Universal Serial Bus) 인터페이스, 또는 IEEE(Institute of Electrical and Electronics Engineers) 1394 인터페이스(즉, 파이어와이어(FireWire) 인터페이스)와 같은, 다양하고 상이한 인터페이스들 중의 임의의 것을 나타내거나, 또는 상이한 인터페이스들의 조합을 논리적으로 나타낼 수도 있다.

모니터(447) 또는 다른 디스플레이 디바이스는 또한 비디오 인터페이스(448)를 통해 시스템 버스(423)에 접속된다. 예를 들어, 스피커들과 프린터들과 같은, 다른 주변 출력 디바이스들(도시 안됨)이 또한 컴퓨터 시스템(420)에 접속될 수 있다.

컴퓨터 시스템(420)은, 예를 들어, 사무실-전반이나 기업-전반 컴퓨터 네트워크, 홈 네트워크, 인트라넷, 및/또는 인터넷과 같은 네트워크들에 접속할 수 있다. 컴퓨터 시스템(420)은 그런 네트워크들을 통해, 예를 들어, 원격 컴퓨터 시스템, 원격 애플리케이션, 및/또는 원격 데이터베이스와 같은 외부 소스들과 데이터를 교환할 수 있다.

컴퓨터 시스템(420)은, 컴퓨터 시스템(420)이 외부 소스들로부터 데이터를 수신하고 및/또는 외부 소스들로 데이터를 전송하는 네트워크 인터페이스(453)를 포함한다. 도 4에 도시된 것처럼, 네트워크 인터페이스(453)는 링크(451)를 통해 원격 컴퓨터 시스템(483)과의 데이터의 교환을 용이하게 한다. 네트워크 인터페이스(453)는, 예를 들어, 네트워크 인터페이스 카드 및 대응하는 NDIS(Network Driver Interface Specification) 스택과 같은, 한 개 이상의 소프트웨어 및/또는 하드웨어 모듈들을 논리적으로 나타낼 수 있다. 링크(451)는 네트워크의 일부(예를 들어, 이더넷 세그먼트)를 나타내고, 원격 컴퓨터 시스템(483)은 네트워크의 노드를 나타낸다.

유사하게, 컴퓨터 시스템(420)은, 컴퓨터 시스템(420)이 외부 소스들로부터 데이터를 수신하고 및/또는 외부 소스들로 데이터를 전송하는, 입력/출력 인터페이스(446)를 포함한다. 입력/출력 인터페이스(446)는, 컴퓨터 시스템(420)이 외부 소스들로부터 데이터를 수신하고 및/또는 전송하는 링크(459)를 통해 모뎀(454)(예를 들어, 표준 모뎀, 케이블 모뎀, 또는 DSL(Digital Subscriber Line) 모뎀)에 접속된다. 도 4에 도시된 것처럼, 입력/출력 인터페이스(446) 및 모뎀(454)은 링크(452)를 통해 원격 컴퓨터 시스템(493)과의 데이터 교환을 용이하게 한다. 링크(452)는 네트워크의 일부를 나타내고, 원격 컴퓨터 시스템(493)은 네트워크의 노드를 나타낸다.

도 4가 본 발명을 위한 적절한 운영 환경을 나타내는 한편, 본 발명의 원리들은, 필요하면 적절히 수정되는, 본 발명의 원리들을 구현할 수 있는 임의의 시스템에 채택될 수 있다. 도 4에 도시된 환경은 단지 설명적일 뿐이고, 본 발명의 원리들이 구현될 수 있는 다양한 환경들의 매우 작은 부분만을 나타내는 것이다.

본 발명에 따라, 인증 데이터, 정책 데이터, 증명 토큰, 토큰 부여 토큰, 서비스 토큰, 보안 컨텍스트 토큰, 이진 확장, 대칭적 키, 공개 키, 개인 키, 및 유도된 키를 포함하는 연관된 데이터 뿐만 아니라, 보안 토큰 서비스, 인증 서비스, 액세스 부여 서비스, 웹 서비스 클라이언트, 웹 서비스, 및 웹 서비스 인스턴스를 포함하는 모듈들은, 컴퓨터 시스템(420)과 연관된 컴퓨터 판독가능 매체 중의 임의의 것에 저장되고 액세스될 수 있다. 예를 들어, 이러한 모듈들의 부분들 및 연관된 프로그램 데이터의 부분들은, 시스템 메모리(422)에 저장되기 위해, 운영 시스템(435), 애플리케이션 프로그램들(436), 프로그램 모듈들(437), 및/또는 프로그램 데이터(438)에 포함될 수 있다.

예를 들어, 자기 하드 디스크(439)와 같은, 대용량 저장 디바이스가 컴퓨터 시스템(420)에 결합될 때, 그런 모듈들과 연관된 프로그램 데이터는 또한 대용량 저장 디바이스에 저장될 수 있다. 네트워크 환경에서, 컴퓨터 시스템(420), 또는 그것의 일부에 관련되어 도시된 프로그램 모듈들은, 시스템 메모리 및/또는 원격 컴퓨터 시스템(483) 및/또는 원격 컴퓨터 시스템(493)과 연관된 대용량 저장 디바이스들과 같은, 원격 메모리 저장 디바이스들에 저장될 수 있다. 이러한 모듈들의 실행은 이전에 기재된 것처럼 분산 환경에서 수행될 수 있다.

본 발명은 그것의 취지 또는 기본 특성들로부터 벗어나지 않고 다른 특정 형태들로 구현될 수 있다. 기재된 실시예들은 단지 설명적이고, 제한적이지는 않게 모든 면에서 고려되어야 한다. 그러므로, 본 발명의 범위는 전술된 설명보다는 첨부된 청구범위에 의해 나타내진다. 청구범위의 동등물의 의미와 범위 내에 속하는 모든 변경들은 그것들의 범위 내에 포함되어야 한다.

발명의 효과

웹 서비스를 액세스하기 위해 신뢰되는 제3자 인증을 위한 본 발명의 방법 및 시스템을 통해서, 웹 서비스들이 공공 네트워크들에서 서로 간에 통신할 때 데이터 전송과 관련된 보안 위험의 문제점을 극복할 수 있다.

(57) 청구의 범위

청구항 1.

컴퓨터 시스템에서, 웹 서비스 컴포넌트를 인증하는 방법으로서,

인증 서비스에 인증 요청을 송신하는 단계;

상기 인증 서비스로부터 인증 응답을 수신하는 단계 -상기 인증 응답은, 상기 웹 서비스 컴포넌트와 액세스 부여(granting) 서비스 간의 통신을 안전하게 하기 위한 제1 대칭적 세션 키의 2 개의 인스턴스(instance)들을 포함하고, 상기 제1 대칭적 세션 키의 제1 인스턴스는, 상기 웹 서비스들로의 전달을 위해 보안화되어 제1 증명 토큰에 포함되고, 상기 제1 대칭적 세션 키의 제2 인스턴스는, 상기 보안 토큰 서비스의 비밀 대칭적 키로 암호화되어 토큰 부여 토큰(token granting token)에 포함됨-;

웹 서비스로의 액세스를 위한 액세스 요청을 상기 액세스 부여 서비스에 송신하는 단계 -상기 액세스 요청은 상기 토크 부여 토큰을 포함함-; 및

상기 액세스 부여 서비스로부터 액세스 부여 응답을 수신하는 단계 -상기 액세스 부여 응답은, 상기 웹 서비스 컴포넌트와 상기 웹 서비스 간에 통신을 안전하게 하기 위해 제2 대칭적 세션 키의 2 개의 인스턴스들을 포함하고, 상기 제2 대칭적 세션 키의 제1 인스턴스는, 상기 제1 대칭적 세션 키로 암호화되어 제2 증명 토큰에 포함되고, 상기 제2 대칭적 세션 키의 제2 인스턴스는, 상기 웹 서비스에 대응하는 공개/개인 키 쌍으로부터의 공개 키로 암호화되어 서비스 토큰에 포함됨-

를 포함하는 방법.

청구항 2.

제1항에 있어서, 인증 서비스로의 인증 요청을 송신하는 상기 단계는 상기 인증 서비스로 사용자명과 패스워드를 송신하는 단계를 포함하는 방법.

청구항 3.

제1항에 있어서, 인증 서비스로 인증 요청을 송신하는 상기 단계는 상기 인증 서비스로 디지털적으로 싸인된(signed) X.509 증명서를 송신하는 단계를 포함하는 방법.

청구항 4.

제1항에 있어서, 상기 인증 서비스로부터 인증 응답을 수신하는 상기 단계는 맞춤(custom) XML 토큰 부여 토큰을 포함하는 SOAP(Simple Object Access Protocol) 메시지를 수신하는 단계를 포함하는 방법.

청구항 5.

제1항에 있어서, 상기 액세스 부여 서비스로부터 액세스 부여 응답을 수신하는 상기 단계는, 맞춤 XML 서비스 토큰을 포함하는 SOAP 메시지를 수신하는 단계를 포함하는 방법.

청구항 6.

제1항에 있어서,

상기 웹 서비스로 보안 토큰 요청을 송신하는 단계 -상기 보안 토큰 요청은 상기 웹 서비스 컴포넌트와 상기 서비스 토큰을 위한 신원 정보를 포함함-;

상기 웹 서비스로부터 보안 토큰 응답을 수신하는 단계 -상기 보안 토큰 응답은, 상기 웹 서비스 컴포넌트와 상기 웹 서비스 간의 통신을 안전하게 하기 위한 보안 컨텍스트 토큰 및 마스터 대칭적 세션 키를 포함함-

를 더 포함하는 방법.

청구항 7.

제6항에 있어서,

상기 마스터 대칭적 세션 키로부터 한 개 이상의 유도된 대칭적 세션 키들을 유도하는 단계; 및

상기 웹 서비스로 서비스 요청을 송신하는 단계 -상기 서비스 요청은, 상기 한 개 이상의 유도된 세션 키들 중에서 제1 유도된 대칭적 세션 키를 사용하여 암호화되고, 상기 한 개 이상의 유도된 세션 키들 중에서 제2 유도된 대칭적 세션 키를 사용하여 싸인됨-

를 더 포함하는 방법.

청구항 8.

제7항에 있어서,

상기 웹 서비스로부터 서비스 응답을 수신하는 단계 -상기 서비스 응답은 상기 한 개 이상의 유도된 세션으로부터 제3 유도된 대칭적 세션 키를 사용하여 암호화되고, 상기 서비스 응답은 상기 한 개 이상의 유도된 세션 키들 중에서 제4 유도된 대칭적 세션 키를 사용하여 디지털 서명으로 싸인됨-;

상기 제3 유도된 대칭적 세션 키를 사용하여 상기 서비스 응답을 해독하는 단계; 및

상기 제4 유도된 대칭적 세션 키를 사용하여 상기 디지털 서명을 유효화하는 단계

를 더 포함하는 방법.

청구항 9.

보안 토큰 서비스를 포함하는 컴퓨터 시스템에서, 웹 서비스 컴포넌트를 인증하는 방법으로서,

웹 서비스 컴포넌트로부터 인증 요청을 수신하는 단계;

상기 인증 요청에 포함된 인증 데이터를 유효화하는 단계;

상기 웹 서비스 클라이언트에 인증 응답을 송신하는 단계 -상기 인증 응답은, 상기 웹 서비스 컴포넌트와 액세스 부여 서비스 간의 통신을 안전하게 하기 위한 대칭적 세션 키의 2 개의 인스턴스들을 포함하고, 상기 대칭적 세션 키의 제1 인스턴스는 상기 웹 서비스 컴포넌트로 전달되기 위해 보안화되어 제1 증명 토큰에 포함되고, 상기 대칭적 세션 키의 제2 인스턴스는, 상기 보안 토큰 서비스의 비밀 대칭적 키로 암호화되어 토큰 부여 토큰에 포함됨-; 및

상기 웹 서비스 컴포넌트로부터 웹 서비스로의 액세스를 위한 액세스 요청을 수신하는 단계 -상기 액세스 요청은 상기 토큰 부여 토큰을 포함함-;

상기 토큰 부여 토큰의 내용에 기초하여, 상기 웹 서비스 컴포넌트가 상기 보안 토큰 서비스로의 인증된 세션을 가짐을 확인하는 단계; 및

상기 웹 서비스 컴포넌트에 액세스 부여 응답을 송신하는 단계 -상기 액세스 부여 응답은, 상기 웹 서비스 컴포넌트와 상기 웹 서비스 간의 통신을 안전하게 하기 위해 제2 대칭적 세션 키의 2 개의 인스턴스들을 포함하고, 상기 제2 대칭적 세션 키의 제1 인스턴스는, 제1 대칭적 세션 키로 암호화되어 제2 증명 토큰에 포함되고, 상기 제2 대칭적 세션 키의 제2 인스턴스는, 상기 웹 서비스에 대응하는 공개/개인 키 쌍으로부터의 공개 키로 암호화되어 서비스 토큰에 포함됨-

를 포함하는 방법.

청구항 10.

제9항에 있어서, 웹 서비스 컴포넌트로부터 인증 요청을 수신하는 상기 단계는, 상기 웹 서비스 컴포넌트로부터 사용자명과 패스워드를 수신하는 단계를 포함하는 방법.

청구항 11.

제9항에 있어서, 웹 서비스 컴포넌트로부터 인증 요청을 수신하는 상기 단계는, 상기 웹 서비스 컴포넌트로부터 싸인된 X.509 증명서를 수신하는 단계를 포함하는 방법.

청구항 12.

제9항에 있어서, 상기 웹 서비스 클라이언트로 인증 응답을 송신하는 상기 단계는, 맞춤 XML 토큰 부여 토큰을 포함하는 SOAP 메시지를 송신하는 단계를 포함하는 방법.

청구항 13.

제9항에 있어서, 상기 웹 서비스 컴포넌트로 액세스 부여 응답을 송신하는 상기 단계는, 맞춤 XML 서비스 토큰을 포함하는 SOAP 메시지를 송신하는 단계를 포함하는 방법.

청구항 14.

웹 서비스를 포함하는 컴퓨터 시스템에서, 상기 웹 서비스로의 액세스를 부여하는 방법으로서,

웹 서비스 컴포넌트로부터 보안 토큰 요청을 수신하는 단계 -상기 요청은 보안 토큰 서비스로부터 발행된 서비스 토큰을 포함하고, 상기 서비스 토큰은, 상기 웹 서비스 클라이언트와 상기 웹 서비스 간의 통신을 안전하게 하기 위해 상기 웹 서비스 컴포넌트와 암호화된 대칭적 세션 키를 위한 신원 정보를 포함하고, 상기 암호화된 대칭적 세션 키는, 상기 웹 서비스에 따라 공개/개인 키 쌍으로부터의 공개 키를 사용하여 암호화됨-;

상기 공개/개인 키 쌍으로부터의 개인 키로 상기 암호화된 대칭적 세션 키를 해독하는 단계;

상기 서비스 토큰의 내용에 기초하여 상기 웹 서비스 컴포넌트가 상기 웹 서비스를 액세스하도록 승인하는 단계;

상기 웹 서비스 클라이언트와 상기 웹 서비스 간의 통신을 안전하게 하기 위한 마스터 대칭적 세션 키를 생성하는 단계;

상기 대칭적 세션 키를 사용하여 상기 마스터 대칭적 세션 키를 암호화하여, 암호화된 마스터 대칭적 세션 키를 생성하는 단계;

보안 토큰 응답에, 보안 컨텍스트 토큰과 함께 상기 암호화된 마스터 대칭적 세션 키를 포함하는 단계; 및

상기 웹 서비스 컴포넌트로 상기 보안 토큰 응답을 송신하여, 상기 웹 서비스 컴포넌트와 상기 웹 서비스 간의 통신이 상기 마스터 대칭적 세션 키로부터 유도된 대칭적 세션 키들을 사용하여 보안화될 수 있도록 하는 단계

를 포함하는 방법.

청구항 15.

제14항에 있어서, 보안 토큰 요청을 수신하는 상기 단계는, 신뢰되는 제3자로부터 발행되는 맞춤 XML 서비스 토큰을 포함하는 SOAP 메시지를 수신하는 단계를 포함하는 방법.

청구항 16.

제14항에 있어서, 보안 토큰 응답에, 보안 컨텍스트 토큰과 함께 상기 암호화된 마스터 대칭적 세션 키를 포함하는 상기 단계는, SOAP 메시지에 확장된 보안 컨텍스트 토큰을 포함하는 단계를 포함하고, 상기 확장된 보안 컨텍스트 토큰은 이진 확장을 포함하여, 상기 웹 서비스가 분산된 서비스측 캐쉬(cache)를 참조하지 않고 상기 이진 확장으로부터 상기 웹 서비스 클라이언트에 대한 보안 세션 상태를 재생성할 수 있도록 하는 방법.

청구항 17.

제16항에 있어서,

상기 웹 서비스의 인스턴스가 상기 웹 서비스 클라이언트로부터 웹 서비스 요청을 수신하는 단계 -상기 웹 서비스 요청은 상기 확장된 보안 컨텍스트 토큰을 포함함-; 및

상기 인스턴스가, 상기 확장된 보안 컨텍스트 토큰을 사용하여, 분산된 서비스측 캐쉬를 참조하지 않고 상기 웹 서비스 클라이언트에 대한 보안 세션 상태를 재생성하는 단계

를 더 포함하는 방법.

청구항 18.

제14항에 있어서, 상기 웹 서비스 컴포넌트로 상기 보안 토큰 응답을 송신하는 상기 단계는, 확장된 보안 컨텍스트 토큰을 포함하는 SOAP 메시지를 송신하는 단계를 포함하는 방법.

청구항 19.

제14항에 있어서,

상기 웹 서비스 컴포넌트로부터 서비스 요청을 수신하는 단계를 더 포함하고, 상기 서비스 요청은 상기 마스터 대칭적 세션 키로부터 유도된 제1 유도된 대칭적 세션 키를 사용하여 암호화되고, 상기 마스터 대칭적 세션 키로부터 유도된 제2 유도된 대칭적 세션 키를 사용하여 디지털 서명으로 싸인되는 방법.

청구항 20.

제19항에 있어서,

상기 제1 유도된 대칭적 세션 키를 사용하여 상기 서비스 요청을 해독하는 단계;

상기 제2 유도된 대칭적 세션 키를 사용하여 상기 디지털 서명을 유효화하는 단계;

서비스 응답에, 상기 웹 서비스 컴포넌트로 리턴하기 위한 응답 데이터를 포함하는 단계; 및

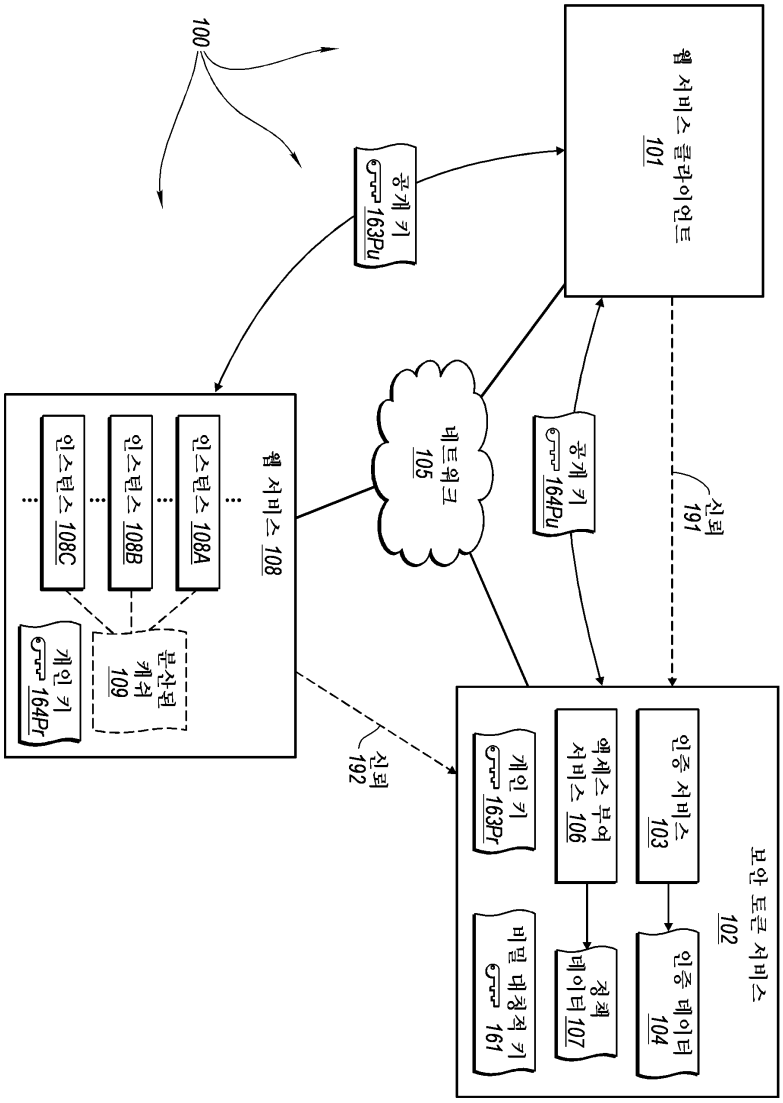
상기 웹 서비스 컴포넌트로 상기 서비스 응답을 송신하는 단계

를 더 포함하고,

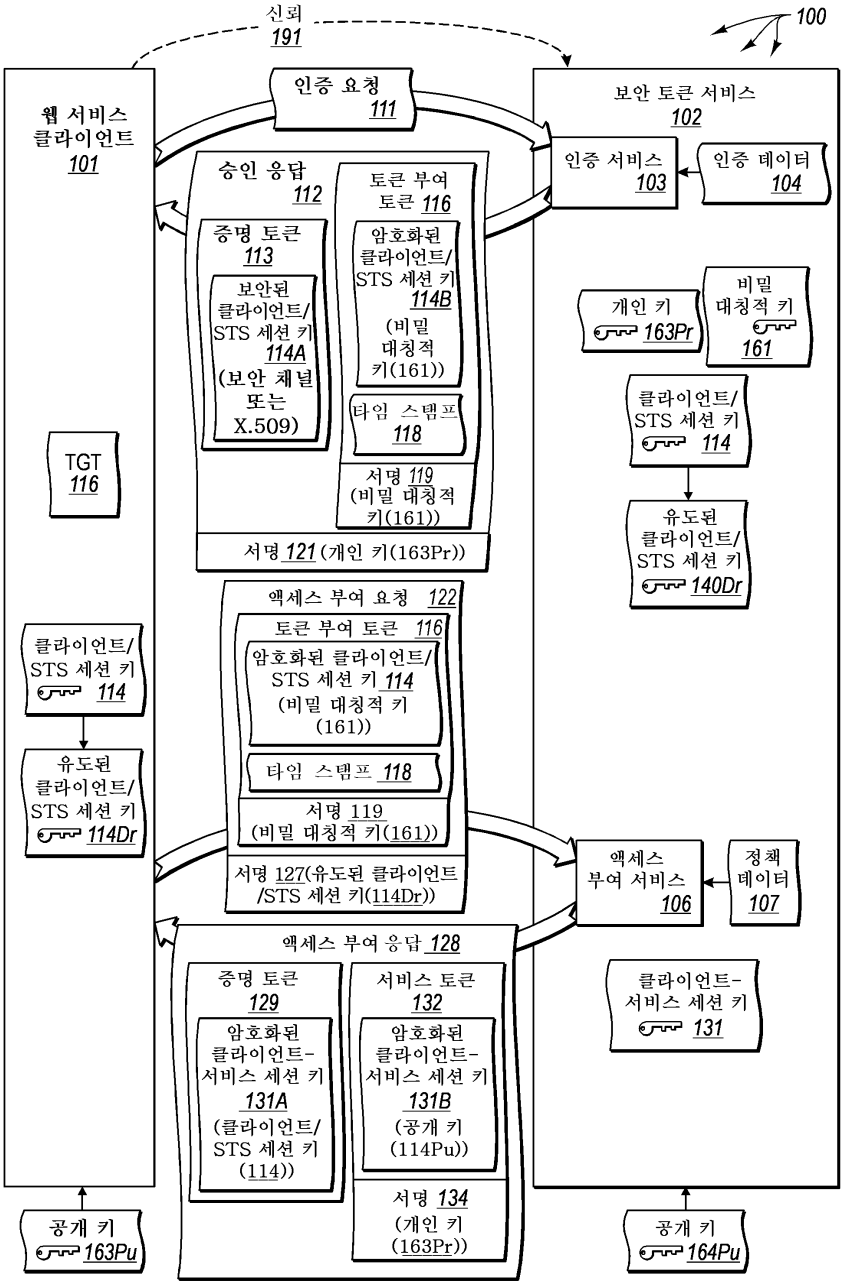
상기 서비스 응답은 상기 마스터 대칭적 세션 키로부터 유도되는 제3 유도된 대칭적 세션 키를 사용하여 암호화되고, 상기 마스터 대칭적 세션 키로부터 유도된 제4 유도된 대칭적 세션 키를 사용하여 디지털 서명으로 싸인되는 방법.

도면

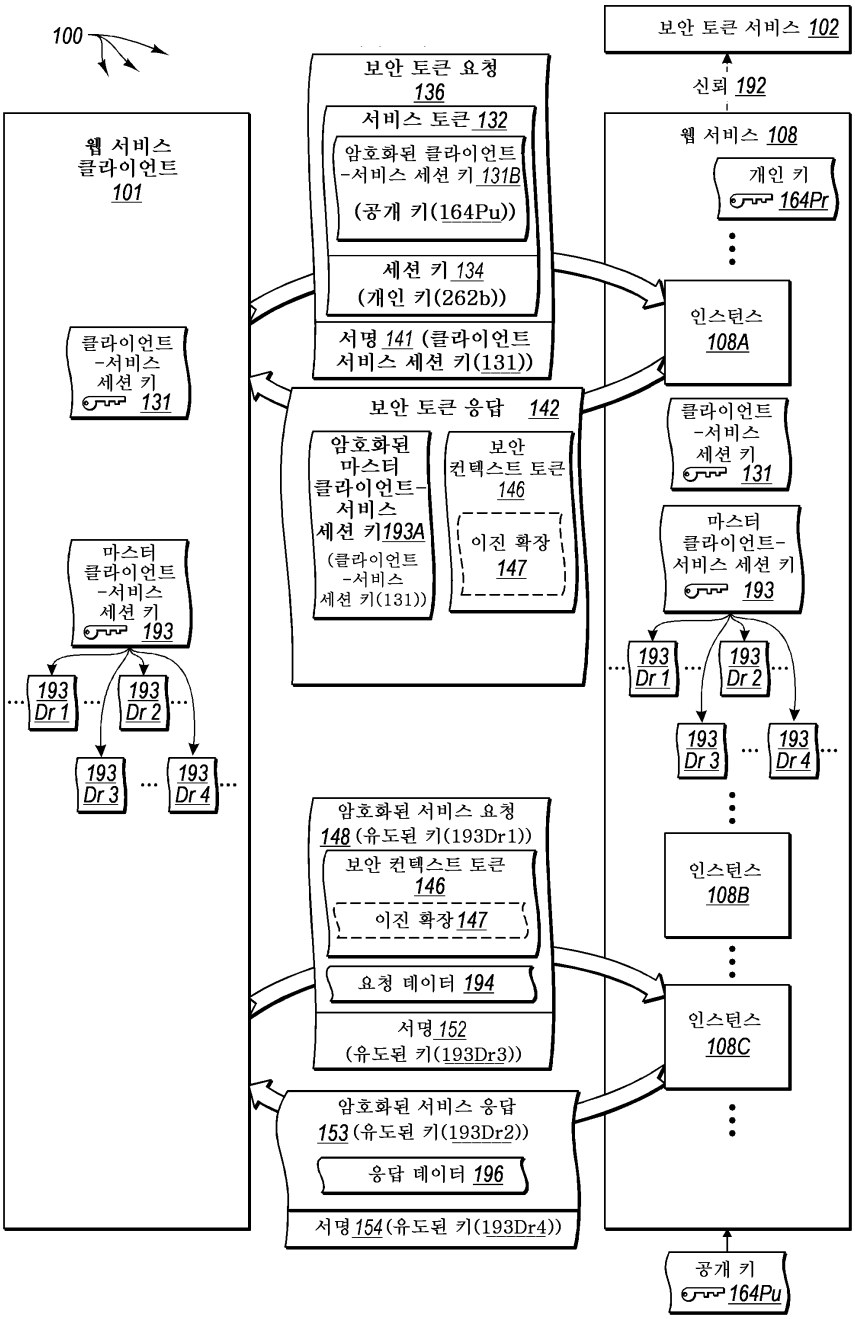
도면1a


100
웹 서비스 클라이언트
101
공개 키
163Pu
네트워크
105
공개 키
164Pu
신뢰
191
보안 토큰 서비스
102
인증 서비스
103
인증 데이터
104
액세스 부여
서비스 106
정책
데이터 107
개인 키
163Pr
비밀 대칭적 키
161
웹 서비스 108
인스턴스 108A
인스턴스 108B
인스턴스 108C
분산된
캐쉬
109
개인 키
164Pr
신뢰
192

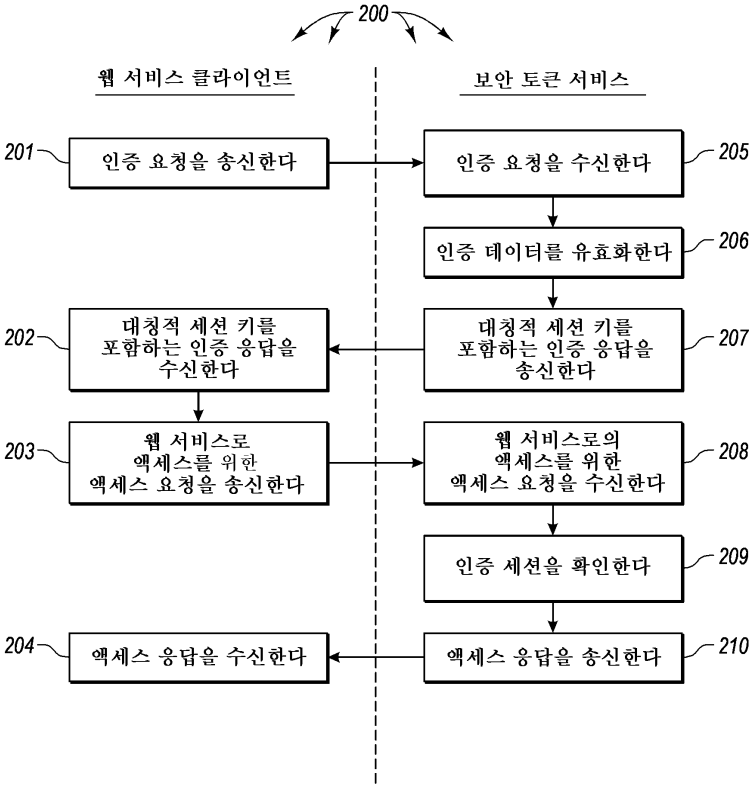
도면1b


신뢰
191
100
웹 서비스
클라이언트
101
인증 요청
111
보안 토큰 서비스
102
인증 서비스
103
인증 데이터
104
승인 응답
112
토큰 부여
토큰 116
증명 토큰
113
보안된
클라이언트/
STS 세션 키
114A
(보안 채널
또는
X.509)
암호화된
클라이언트/
STS 세션 키
114B
(비밀
대칭적
키(161))
타임 스탬프
118
서명 119
(비밀 대칭적
키(161))
서명 121 (개인 키(163Pr))
개인 키
163Pr
비밀
대칭적 키
161
클라이언트/
STS 세션 키
114
유도된
클라이언트/
STS 세션 키
140Dr
TGT
116
액세스 부여 요청 122
토큰 부여 토큰 116
암호화된 클라이언트/
STS 세션 키 114
(비밀 대칭적 키
(161))
타임 스탬프 118
서명 119
(비밀 대칭적 키(161))
서명 127(유도된 클라이언트
/STS 세션 키(114Dr))
클라이언트/
STS 세션 키
114
유도된
클라이언트/
STS 세션 키
114Dr
액세스
부여 서비스
106
정책
데이터
107
클라이언트-
서비스 세션 키
131
액세스 부여 응답 128
증명 토큰
129
암호화된
클라이언트-
서비스 세션 키
131A
(클라이언트/
STS 세션 키
(114))
서비스 토큰
132
암호화된
클라이언트-
서비스 세션 키
131B
(공개 키
(114Pu))
서명 134
(개인 키
(163Pr))
공개 키
163Pu
공개 키
164Pu

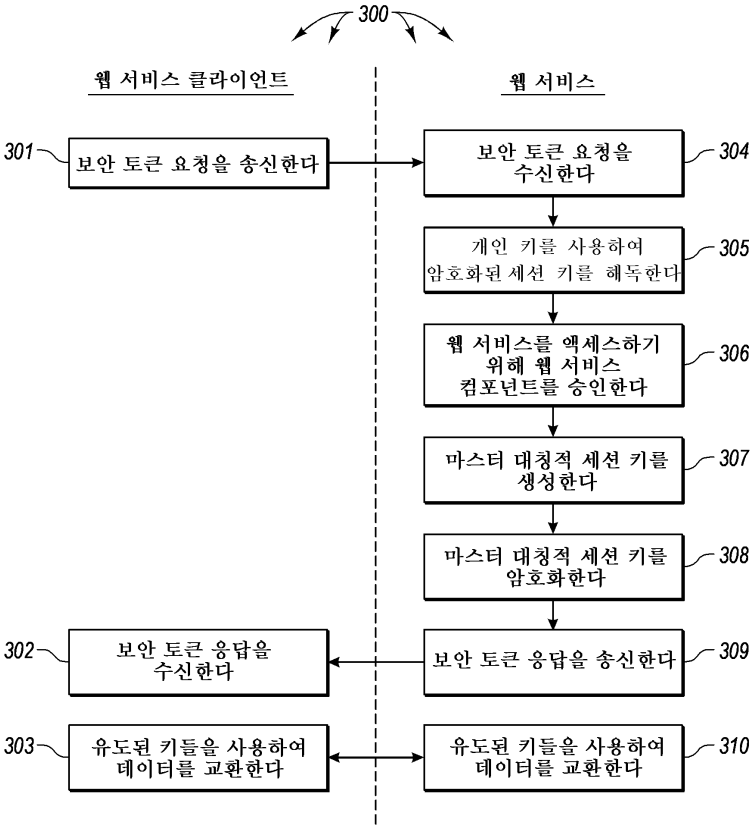
도면1c


100
보안 토큰 서비스 102
신뢰 192
보안 토큰 요청 136
서비스 토큰 132
암호화된 클라이언트-서비스 세션 키 131B
(공개 키(164Pu))
세션 키 134
(개인 키(262b))
서명 141 (클라이언트 서비스 세션 키(131))
웹 서비스 클라이언트 101
웹 서비스 108
개인 키 164Pr
인스턴스 108A
클라이언트-서비스 세션 키 131
보안 토큰 응답 142
암호화된 마스터 클라이언트-서비스 세션 키193A
(클라이언트-서비스 세션 키(131))
보안 컨텍스트 토큰 146
이진 확장 147
마스터 클라이언트-서비스 세션 키 193
193 Dr 1
193 Dr 2
193 Dr 3
193 Dr 4
암호화된 서비스 요청 148 (유도된 키(193Dr1))
보안 컨텍스트 토큰 146
이진 확장 147
요청 데이터 194
서명 152 (유도된 키(193Dr3))
인스턴스 108B
인스턴스 108C
암호화된 서비스 응답 153 (유도된 키(193Dr2))
응답 데이터 196
서명 154 (유도된 키(193Dr4))
공개 키 164Pu

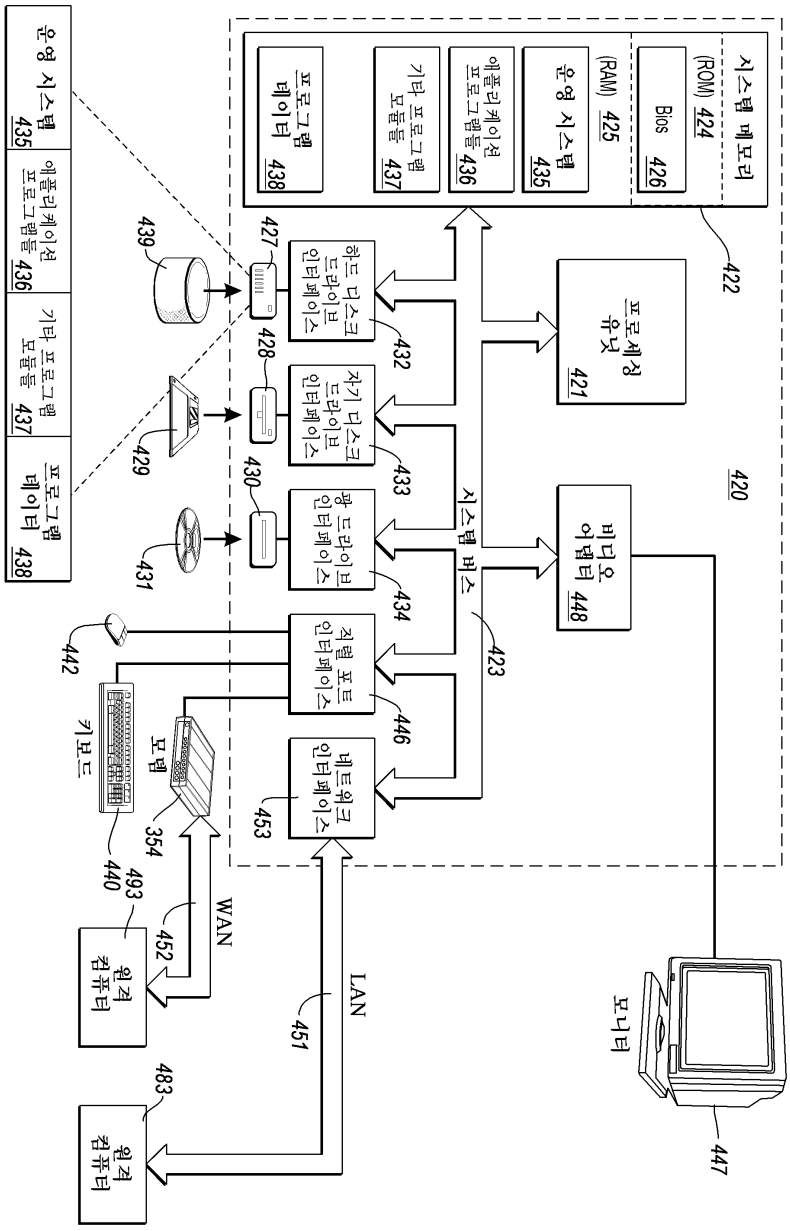
도면2


200
웹 서비스 클라이언트
보안 토큰 서비스
201
인증 요청을 송신한다
205
인증 요청을 수신한다
206
인증 데이터를 유효화한다
202
대칭적 세션 키를 포함하는 인증 응답을 수신한다
207
대칭적 세션 키를 포함하는 인증 응답을 송신한다
203
웹 서비스로 액세스를 위한 액세스 요청을 송신한다
208
웹 서비스로의 액세스를 위한 액세스 요청을 수신한다
209
인증 세션을 확인한다
204
액세스 응답을 수신한다
210
액세스 응답을 송신한다

도면3


300
웹 서비스 클라이언트
웹 서비스
301
보안 토큰 요청을 송신한다
304
보안 토큰 요청을 수신한다
305
개인 키를 사용하여 암호화된 세션 키를 해독한다
306
웹 서비스를 액세스하기 위해 웹 서비스 컴포넌트를 승인한다
307
마스터 대칭적 세션 키를 생성한다
308
마스터 대칭적 세션 키를 암호화한다
302
보안 토큰 응답을 수신한다
309
보안 토큰 응답을 송신한다
303
유도된 키들을 사용하여 데이터를 교환한다
310
유도된 키들을 사용하여 데이터를 교환한다

도면4


시스템 메모리
(ROM) 424
Bios 426
(RAM) 425
운영 시스템 435
에플리케이션 프로그램들 436
기타 프로그램 모듈들 437
프로그램 데이터 438
422
420
프로세싱 유닛 421
비디오 어댑터 448
시스템 버스 423
하드 디스크 드라이브 인터페이스 427
자기 디스크 드라이브 인터페이스 428
광 드라이브 인터페이스 430
직렬 포트 인터페이스 434
네트워크 인터페이스 453
432
433
446
439
429
431
442
키보드
모뎀
354
493
440
452
451
483
WAN
LAN
원격 컴퓨터
원격 컴퓨터
모니터
447
운영 시스템 435
에플리케이션 프로그램들 436
기타 프로그램 모듈들 437
프로그램 데이터 438