(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년08월16일
(11) 등록번호 10-1648521
(24) 등록일자 2016년08월09일

(51) 국제특허분류(Int. Cl.)
G06F 21/34 (2013.01) *G06F 21/77* (2013.01)
H04L 29/06 (2006.01) *H04L 9/00* (2006.01)
(21) 출원번호 10-2011-7023435
(22) 출원일자(국제) 2010년03월05일
심사청구일자 2015년02월17일
(85) 번역문제출일자 2011년10월05일
(65) 공개번호 10-2011-0134455
(43) 공개일자 2011년12월14일
(86) 국제출원번호 PCT/EP2010/052843
(87) 국제공개번호 WO 2010/100262
국제공개일자 2010년09월10일
(30) 우선권주장
61/158,192 2009년03월06일 미국(US)
(56) 선행기술조사문헌
US20090064301 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
제말토 에스에이
프랑스, 92190 므동, 루 드 라 브레리 6
(72) 발명자
크리슈나 크쉐에랍디
프랑스 에프-92197 뭬동 뤼 드 라 베레리 6 제말토 에스에이 인텔렉츄얼 프로퍼티 디파트먼트
사치데바 카필
프랑스 에프-92197 뭬동 뤼 드 라 베레리 6 제말토 에스에이 인텔렉츄얼 프로퍼티 디파트먼트
루 카렌 홍쿠이안
프랑스 에프-92197 뭬동 뤼 드 라 베레리 6 제말토 에스에이 인텔렉츄얼 프로퍼티 디파트먼트
(74) 대리인
리앤목특허법인

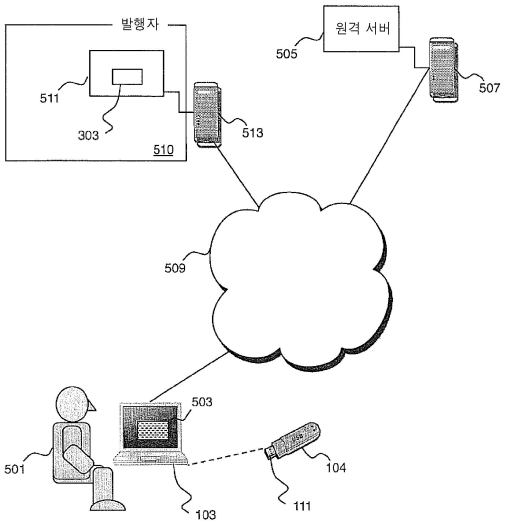
전체 청구항 수 : 총 15 항 심사관 : 문남두

(54) 발명의 명칭 **스마트 카드들로의 브라우저-기반의 액세스에 보안을 제공하는 시스템 및 방법**

(57) 요 약

인터넷에 접속되어 있는 것과 연관된 보안 위협들로부터 스마트 카드를 보호하기 위해서 스마트 카드로 웹 애플리케이션 액세스를 제공하기 위한 적어도 하나의 웹-브라우저 애드-온을 실행시키는 능력을 갖춘 웹-브라우저를 구비한 호스트 컴퓨터를 운영하는 방법이 제공된다. 웹 브라우저 내에서 실행하는 웹 애프리케이션 사이의 접속을 설립하기 이전에, 웹 애플리케이션이 스마트 카드에 웹 애플리케이션 액세스를 제공하기 위해서 웹-브라우저 애드-온을 이용하여 스마트 카드에 접속하는 것을 승인받았는가를 확인한다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

웹 사이트 도메인 이름을 구비한 웹 서버 상에서 시작된 웹 서버 애플리케이션 그리고 호스트 컴퓨터를 경유하여 네트워크를 통해서 웹 서버에 접속된 보안 기기 사이에서 보안 접속을 제공하는 방법으로서,

컴퓨터 네트워크를 통해 웹 서버로의 접속을 설립하는 단계;

웹 서버로부터 브라우저로 웹 서버 애플리케이션을 로딩하는 단계;

상기 웹 서버 애플리케이션이 상기 보안 기기에 액세스한다는 것을 확인할 것을 필요로 하는 상기 보안 기기로 웹 서버 애플리케이션 액세스를 제공하기 위해서 브라우저 확장을 실행하는 단계를 포함하며,

상기 웹 서버 애플리케이션이 보안 기기에 액세스하는 것을 확인하는 것은:

상기 접속이 신뢰받는 루트 인증 기관에 의해 발행된 디지털 인증을 이용하여 설립된 보안 접속이라는 것을 검증함으로써 상기 웹 서버를 인증하는 단계;

승인 조직에 의해서 발행된 접속 키를 상기 웹 서버로부터 수신하는 단계로서, 상기 접속 키는 상기 승인 조직과 암호로 링크되며, 상기 웹 서버의 디지털 인증과 암호로 링크된, 수신 단계;

상기 웹 서버에 의해 제시된 상기 접속 키가 유효한가의 여부를 그리고 상기 웹 서버 애플리케이션이 상기 보안 기기에 액세스하는 것이 상기 승인 조직에 의해서 정당하게 승인되었다는 것을 상기 접속 키가 표시하는가를 판별하는 단계;

상기 접속 키가 유효하고 그리고 상기 웹 서버 애플리케이션이 상기 보안 기기에 액세스하는 것이 상기 승인 조직에 의해서 정당하게 승인되었다는 것을 표시한다면, 상기 웹 서버 애플리케이션이 상기 보안 기기에 접속하는 것을 허용하는 단계; 그리고

접속 키가 유효하지 않거나 또는 상기 웹 서버 애플리케이션이 상기 보안 기기에 액세스하는 것이 상기 승인 조직에 의해서 정당하게 승인되었다는 것을 표시하지 않는다면, 상기 웹 서버 애플리케이션이 상기 보안 기기에 접속할 기회를 거부하는 단계를 포함하는, 보안 접속 제공 방법.

청구항 2

제1항에 있어서,

보안 기기는 스마트 카드인, 보안 접속 제공 방법.

청구항 3

제2항에 있어서,

보안 기기는 SIM 카드인, 보안 접속 제공 방법.

청구항 4

제1항에 있어서,

보안 기기는 보안 토큰, 생물학적 (biometric) 기기, 모바일 전화기 중에서 선택되는, 보안 접속 제공 방법.

청구항 5

제1항에 있어서,

접속 키는 자신과 연관된 공통 이름 (common name)을 구비하며 그리고

접속 키가 유효한가의 여부를 판별하는 것은 공통 이름을 웹사이트 도메인 이름과 비교하는 것을 포함하는, 보

안 접속 제공 방법.

청구항 6

제1항에 있어서,

접속 키는 자신과 연관된 기간 만료 (expiration) 데이터를 구비하며 그리고

접속 키가 유효한가의 여부를 판별하는 것은 기간 만료 데이터가 현재의 달력 날짜보다 이전인가의 여부를 판별하는 것을 포함하는, 보안 접속 제공 방법.

청구항 7

제1항에 있어서,

접속 키는 발행 조직에 의해서 발행되며 그리고 디지털 서명을 구비하며 그리고

접속 키가 유효한가의 여부를 판별하는 것은 발행 조직의 공개키 (public key)를 이용하여 디지털 서명을 확인하는 것을 포함하는, 보안 접속 제공 방법.

청구항 8

제1항에 있어서,

접속 키는 원격 서버 웹사이트의 SSL (secure socket layer) 인증의 지문을 포함하며 그리고

접속 키가 유효한가의 여부를 판별하는 것은 상기 지문을 검증하는 것을 포함하는, 보안 접속 제공 방법.

청구항 9

제1항에 있어서,

허용된 웹사이트들의 목록을 구비한 허가 데이터베이스를 생성하는 단계;

웹사이트 도메인 이름이 허용된 웹사이트들의 목록에 있으면, 웹 서버 애플리케이션이 보안 기기에 접속하도록 허용하는 단계; 및

웹사이트 도메인 이름이 허용된 웹사이트들의 목록에 있지 않으면, 웹 서버 애플리케이션이 스마트 카드에 접속할 것을 사용자가 허가했는지의 여부에 관해서 사용자에게 질의하고 그리고 사용자가 웹 서버 애플리케이션에게 보안 기기에 액세스하는 것을 허용하는 사용자 허가를 표시하면 웹 서버 애플리케이션이 스마트 카드에 접속할 것을 허용하는 단계를 더 포함하는, 보안 접속 제공 방법.

청구항 10

제1항에 있어서,

호스트 컴퓨터 상에서 실행하는 브라우저를 이용하여 웹 서버에 접속하는 단계는 사용자 브라우저와 원격 웹사이트 사이에서의 보안 통신 채널을 설립하는 것을 포함하며,

상기 방법은,

보안 통신 채널이 보안 통신 채널들을 설립하는 용도의 유효한 인증을 이용하여 설립되었는가의 여부를 판별하는 단계; 그리고

보안 통신 채널을 설립하기 위해서 사용된 인증이 유효하지 않다면 웹 서버 애플리케이션으로부터 보안 기기로의 접속을 거부하는 단계를 더 포함하는, 보안 접속 제공 방법.

청구항 11

제1항에 있어서,

보안 접속은 SSL 접속이며 그리고

접속 인증은 SSL 인증인, 보안 접속 제공 방법.

청구항 12

제10항에 있어서,

보안 통신 채널들을 설립하기 위해 유효한 인증이 이용되었는가의 여부를 판별하는 것은 인증 내의 공통 이름이 웹 서버의 도메인 이름에 부합하는가의 여부, 보안 통신 채널을 설립하기 위해서 사용된 인증이 기간 만료되지 않았는가의 여부 그리고 보안 통신 채널을 설립하기 위한 인증이 신뢰받는 인증기관에 의해서 발행된 것인가의 여부를 판별하는 것을 포함하는, 보안 접속 제공 방법.

청구항 13

제1항에 있어서,

웹 서버 애플리케이션이 보안 기기에 접속할 것을 허용하기 이전에 웹 브라우저와 원격 서버 사이에서의 접속이 유효한 인증에 의해서 안전한가를 판별하는 단계를 더 포함하는, 보안 접속 제공 방법.

청구항 14

중앙 프로세싱 유닛,

메모리 그리고

메모리로 로딩 가능하며 그리고 중앙 프로세싱 유닛에 의해 실행 가능한 명령어들을 저장하기 위한 저장 매체를 갖춘 호스트 컴퓨터를 구비한 컴퓨터 시스템으로서,

저장 매체는 중앙 프로세싱 유닛으로 하여금, 웹 사이트 도메인 이름을 구비한 웹 서버 상에서 시작된 웹 서버 애플리케이션 그리고 호스트 컴퓨터를 경유하여 네트워크를 통해서 웹 서버에 접속된 보안 기기 사이에서 보안 접속을 제공하도록 하는 명령어들을 포함하며,

상기 컴퓨터 시스템은 제1항 내지 제12항 중의 어느 한 항의 방법을 수행하는 명령어들을 포함하는, 컴퓨터 시스템.

청구항 15

중앙 프로세싱 유닛, 메모리 그리고 메모리로 로딩 가능하며 그리고 중앙 프로세싱 유닛에 의해 실행 가능한 명령어들을 저장하기 위한 저장 매체를 갖춘 호스트 컴퓨터용의, 컴퓨터로 실행 가능한 명령어들을 포함하는 컴퓨터 독출가능 저장 매체로서,

저장 매체는 중앙 프로세싱 유닛으로 하여금, 웹 사이트 도메인 이름을 구비한 웹 서버 상에서 시작된 웹 서버 애플리케이션 그리고 호스트 컴퓨터를 경유하여 네트워크를 통해서 웹 서버에 접속된 보안 기기 사이에서 보안 접속을 제공하도록 하는 명령어들을 포함하며,

저장 매체는 제1항 내지 제12항 중의 어느 한 항의 방법을 수행하는 명령어들을 포함하는, 컴퓨터 독출가능 저장 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 스마트 카드들로의 애플리케이션 프로그램 액세스에 관련된 것이며, 더욱 상세하게는, 웹-브라우저에서 실행되는 애플리케이션들이 스마트 카드 상에 저장된 데이터와 기능들을 액세스할 것을 허용할 때에 정보 보안을 보장하기 위한 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 스마트 카드는 입력 디바이스와 출력 디바이스가 없는 크기가 작은 보안 개인용 컴퓨터이다. 스마트 카드들용의 전형적인 애플리케이션들은 사용자 인증, 개인적인 데이터, 그리고 전자 지갑으로서 사용되는 것을 포함한다. 다른 것들은 물론이며, 이런 애플리케이션들을 위해서, 스마트 카드와의 상호작용 (interact)하기 위한 통상의 모드는 스마트 카드가 접속된 호스트 컴퓨터 상에서 실행되고 있는 호스트 애플리케이션으로부터 온 것이다.

[0003] 2007년 8월 31일에 출원된 미국 특허 출원 번호 11/849,117 Kapil Sachdeva 그리고 Ksheerabdhi Krishna의

"System and Method for Browser Based Access to Smart Cards"은 스마트 카드들에 액세스하는 웹-애플리케이션들을 생성하는데 있어서 프로그래머에 가해지는 많은 부담들을 제거해주는 메커니즘을 설명한다. 하나의 시나리오에서, 사용자가 원격 웹 서비스에 액세스할 때에, 예를 들면, 미국 텍사스, 오스틴에 있는 Gemalto, Inc.로부터의 SConnect 기술을 이용하여, 웹-애플리케이션은 호스트 컴퓨터에 다운로드될 수 있을 것이다. 상기 웹-애플리케이션은 브라우저들과 플랫폼들에 걸쳐서 공통인 애플리케이션 프로그램 인터페이스로 쓰여질 수 있을 것이다. 웹-애플리케이션 개발자를 특정 플랫폼들 그리고 브라우저들의 복잡함으로부터 격리하기 위해서, 브라우저 확장 (browser extension) (여기에서는 스마트 카드 액세스 브라우저 확장으로 언급된다)이 브라우저로 로딩된다. 그 브라우저 확장은 상기 웹-애플리케이션과 상기 스마트 카드 사이에서의 상호작용 (interaction)을 열거한다. 그래서, 상기 브라우저 확장은 상기 웹-애플리케이션을 경유하여 상기 원격 웹-서비스로부터 상기 스마트 카드로의 데이터 파이프를 제공한다. 텍사스, 오스틴에 있는 Gemalto, Inc.로부터의 SConnect 기술은 스마트 카드 액세스 브라우저 확장의 일 예이다.

[0004] 스마트 카드들은 고도로 민감한 정보를 저장하기 위해서 종종 사용된다. 예를 들면, 스마트 카드들은 암호화 연산을 위해서 사용될 수 있을 것이며, 그러면 사용자의 비밀 키를 보유할 것이다. 스마트 카드들은 다양한 유형의 계정들에 액세스하기 위해, 예를 들면, 특정 컴퓨터들이나 네트워크들, 금융 계정들, 건강 정보 계정들로의 액세스를 제공하기 위해서 증명서들을 보유하기 위해 또한 사용될 수 있을 것이다. 자연스럽게, 그런 스마트 카드들에 의해서 제공되는 그런 정보와 서비스들을 제3자에게 부주의하게 드러나게 하는 것으로부터, 제3자에 의한 고의적인 절도로부터, 그리고 부주의한 또는 고의적인 손상으로부터 보호하는 것이 매우 중요하다. 그런 보호들을 제공하는 것에 실패한다면 스마트 카드의 보유자의 정보에 대한 승인되지 않은 액세스, 사용자의 온라인 계정들에 대한 승인되지 않은 액세스, 데이터 파괴 그리고 다른 유형들의 신원 (identity) 절도의 결과로 이끌 수 있을 것이다.

[0005] 스마트 카드 액세스 브라우저 확장은 원격 웹-서비스가 로컬 컴퓨터를 경유하여 인터넷을 통해서 스마트 카드에 접속되는 메커니즘을 제공한다. 그러므로, 인터넷에 접속될 때에 스마트 카드가 노출되는 잠재적인 보안 위협들에 맞서기 위해서 스마트 카드 액세스 브라우저 확장을 이용하는 것이 바람직하다.

[0006] 스마트 카드에 대한 가능한 공격들의 몇 가지 예들은 피싱 (Phishing) 공격, DNS 캐시 포이즌 (DNS Cache Poisoning) 공격, 악의적인 웹사이트들 (Malicious Websites) 공격, 그리고 중간자 (Man-in-the-Middle) 공격을 포함한다.

[0007] *피싱* 공격들은, 예를 들면, 사용자가 계정을 가지고 있을 사용자의 은행이나 다른 온라인 상인인 것처럼 가장하여 사용자들을 속여서 사용자가 액세스하기를 원할 수 있을 정당한 웹사이트들을 닮은 악의적인 웹사이트들에 사용자들의 로그인 증명들을 누설하도록 한다. 피싱을 방지하기 위한 해결책은 사용자가 조심하는 것이다.

[0008] *DNS 캐시 포이즌* 공격은 DNS 서버의 약점들을 찾아서 서버들을 속여서 그 서버가 사기의 정보를 받아들이게 하여 악의적인 웹사이트들로 트래픽을 향하게 한다. 피싱이 개별적인 희생자들을 유인하는데 반하여, DNS 캐시 포이즌은 목적지 웹사이트에 도달하려고 시도하는 모든 사용자들이 사기의 웹사이트로 방향을 돌리도록 할 수 있다.

[0009] *악의적인 웹사이트들* (*Malicious Websites*). 전통적인 스마트 카드들은 호스트 컴퓨터가 안전하다는 것을 가정하여 동작한다. 사용자가 유효한 PIN을 입력하면, 호스트 컴퓨터 상의 클라이언트 프로그램은 그 스마트 카드에 액세스할 수 있다. 실제로, 그 컴퓨터 상의 어떤 프로그램들은 그 사용자가 로그인한 후에 그 카드에 액세스할 수 있다. 글로벌 플랫폼의 안전한 채널 프로토콜 (Global Platform's Secure Channel Protocols (SCP)) 그리고 ISO 7816-4의 시큐어 메시징 (Secure Messaging)은 인증된 보안 통신 채널을 상기 호스트 컴퓨터 상의 하나의 클라이언트 애플리케이션 그리고 상기 스마트 카드 내의 하나의 서버 애플리케이션 사이에 설립함으로써 이 문제를 방지한다. 불행하게도, 이 분야에서의 많은 스마트 카드들은 이런 보안 표준들이 자리를 잡기 이전에 발행되었거나 또는 그런 표준들을 구현하지 않았다는 것 중의 어느 하나이다. 이런 카드들은 컴퓨터들 상의 악의적인 소프트웨어에 의한 공격들에 취약하다.

[0010] *중간자* (Man-In-The-Middle (MITM, middleperson)) 공격은 악명이 높은 네트워크 공격이다. 그 공격자는 클라이언트에 대해서는 서버인 것으로 가장하고, 그리고 서버에게는 클라이언트인 것으로 가장하여, 그들 사이의 메시지들을 가로챈다. 예를 들면, 사용자가 클라이언트 애플리케이션 (예를 들면, 브라우저)을 이용하여 원격 서버에 액세스하기를 원한다고 가정한다. 상기 중간자는 상기 클라이언트와 상기 서버 사이에 위치하여, 사용자의 개인적인 데이터를 가로채고, 트랜잭션을 수정하며 그리고/또는 인증된 채널을 강탈한다.

[0011] 보안 소켓 레이어 (secure socket layer (SSL)), 또는 그것의 더 나중의 버전인 전송 레이어 보안 (transport layer security (TLS)) 프로토콜은 MITM이 두 개의 접속하는 인터넷 파티들 (예를 들면, 클라이언트와 서버) 사이에서 송신되는 메시지들을 도청하거나 수정하는 것을 방지하면서 상기 두 파티들이 안전하게 통신하는 것을 가능하게 한다. MITM 공격들을 완전하게 방지하기 위해서, 상기 두 통신 파티들은 서로를 알고 그리고 인증해야만 한다. 그러나, 대개의 경우 이는 흔히 있는 일은 아니다; 클라이언트 인증은 대개는 사용되지 않는다.

[0012] HTTPS는 TCP에 의해서 직접 운반된 것이 아니라 SSL/TLS에 의해서 운반된 HTTP이다. 그것은 웹 애플리케이션들 사이에서의 통신이 안전하게 하는 것을 가능케 한다.

[0013] 인터넷 기반의 공격들에 추가로, 스마트 카드는 호스트 컴퓨터로부터 시작된 공격들에는 취약할 수 있다. 그런 공격 매카니즘의 하나는 *키스트로크 로거* (Keystroke Logger)이다. 키스트로크 로거는 사용자 이름과 패스워드와 같은 사용자의 로그인 정보들을 훔치기 위한 동기를 가지고 사용자의 키스토로크들을 캡쳐하는 악의적인 소프트웨어 프로그램이다. 그러면 상기 로거는 정보를 추출하고 그리고 사기의 행동들을 위해서 그 정보를 사용하기 위해서 상기 캡쳐된 키스트로크들을 원격 서버로 송신할 수 있다. 캡쳐된 PIN은 대응하는 스마트 카드들이 없이는 아무 소용이 없기 때문에, 단순한 키스트로크 로거들은 스마트 카드들에는 덜 효과적이다. 복잡한 키스트로크 로거는 그러나 사용자 PIN을 캡쳐하고, 다음에 스마트 카드가 삽입되는 것을 기다리고 그리고 그 카드 소지자가 알지 못하게 그 카드에 액세스할 수 있다.

[0014] 스마트 카드 데이터 보안에 대한 다른 취약성들은 사용자의 행동으로부터 시작한다. 사용자들에게로의 여러 소프트웨어 프로그램들의 현존 경고 메시지들이 있지만, 사용자들이 그런 경고들을 무시하는 것은 보기 드물지 않다.

[0015] 유사하게, 클라이언트 웹 브라우저 그리고 원격 웹 서버 사이의 많은 상호작용들이 SSL 또는 TLS를 이용하여 보안이 되지만, 클라언트와 서버 사이의 그런 보안 통신은 상기 서버가 유효하고 그리고 신뢰할 수 있는 SSL 인증을 소유하고 있을 것을 필요로 한다. 유효하고 그리고 신뢰할 수 있기 위해서, SSL 인증에는 신뢰받는 루트 인증 기관 (certificate authority (CA))에 의해서 서명이 되어야만 하며 그리고 상기 인증의 공통 이름 (Common Name (CN)) 그리고 액세스되고 있는 웹 페이지의 URL 사이는 서로 부합되어야만 한다. 상기 SSL 인증이 이런 요구 사항들을 충족하지 않으면, 웹 브라우저는 사용자에게 경고한다. 사용자들이 그런 경고들을 단순하게 무시하고 그리고 SSL 인증이 유효하지 않음에도 불구하고 원격 서버와의 세션을 설립하는 것을 진행하는 것은 매우 흔하다. 그것은 악의적인 웹 사이트가 액세스되고 있으며, 이는 그 사용자의 스마트 카드의 내용물들에 부적절하게 액세스하거나 또는 그 내용물들을 조작하도록 할 수 있을 것이라는 위험을 상기 사용자에게 제기한다.

[0016] 그러므로, 스마트 카드 액세스 브라우저 확장을 경유한 원격 웹-서비스들에 의한 스마트 카드로의 상호작용이 악의적인 공격들 그리고 의도하지 않은 손상들에 대해서 보호되는 보안 메커니즘을 제공하는 것이 필요하다.

[0017] 전술한 내용으로부터, 스마트 카드들로의 웹 애플리케이션 액세스를 제공하기 위한 개선된 방법에 대한 필요성이 존재한다는 것이 명백하다.

선행기술문헌

특허문헌

[0018] (특허문헌 0001) 미국 특허 출원 번호 11/849,117 Kapil Sachdeva 그리고 Ksheerabdhi Krishna의 "System and Method for Browser Based Access to Smart Cards" (2007년 8월 31일에 출원)

비특허문헌

[0019] (비특허문헌 0001) ISO 7816-4의 시큐어 메시징 (Secure Messaging)

발명의 내용

해결하려는 과제

[0020] 본 발명은, 스마트 카드 액세스 브라우저 확장을 경유한 원격 웹-서비스들에 의한 스마트 카드로의 상호작용이

악의적인 공격들 그리고 의도하지 않은 손상들에 대해서 보호되는 보안 메커니즘을 제공하는 것이며, 전술한 내용으로부터, 스마트 카드들로의 웹 애플리케이션 액세스를 제공하기 위한 개선된 방법을 제공하려고 한다.

과제의 해결 수단

[0021] 상기의 과제를 위해서, 본 발명은 웹 사이트 도메인 이름을 구비한 웹 서버 상에서 시작된 웹 서버 애플리케이션 그리고 호스트 컴퓨터를 경유하여 네트워크를 통해서 웹 서버에 접속된 보안 기기 사이에서 보안 접속을 제공하는 방법을 제공한다. 상기 방법은, 컴퓨터 네트워크를 통해서 호스트 컴퓨터 상에서 실행하는 브라우저를 이용하여 웹 서버에 접속하는 단계; 웹 서버로부터 브라우저로 웹 서버 애플리케이션을 로딩하는 단계; 웹 서버 애플리케이션이 모바일 기기에 액세스한다는 것을 확인할 것을 필요로 하는 모바일 기기로 웹 서버 애플리케이션 액세스를 제공하기 위해서 브라우저 확장을 실행하는 단계로서, 웹 서버 애플리케이션이 모바일 기기에 액세스하는 것을 확인하는 것은: 웹 서버와 연관된 접속 키가 유효한가의 여부를 판별하는 단계로서, 이 경우 접속 키는 웹 서버 애플리케이션이 모바일 기기에 액세스하는 것이 승인 조직에 의해서 정당하게 승인되었는가를 검증할 수 있는 메커니즘을 제공하고 그리고 브라우저 확장이 접속 키의 유효성 그리고 진정함을 검증할 수 있는 메커니즘을 제공하는, 판별 단계; 접속 키가 유효하면, 웹 서버 애플리케이션이 모바일 기기에 접속하는 것을 허용하는 단계; 그리고 접속 키가 유효하지 않으면, 웹 서버 애플리케이션이 모바일 기기에 접속할 기회를 거부하는 단계를 포함한다.

[0022] 본 발명에 따른 컴퓨터 시스템은, 중앙 프로세싱 유닛, 메모리 그리고 메모리로 로딩 가능하며 그리고 중앙 프로세싱 유닛에 의해 실행 가능한 명령어들을 저장하기 위한 저장 매체를 갖춘 호스트 컴퓨터를 구비하며, 저장 매체는 중앙 프로세싱 유닛으로 하여금, 웹 사이트 도메인 이름을 구비한 웹 서버 상에서 시작된 웹 서버 애플리케이션 그리고 호스트 컴퓨터를 경유하여 네트워크를 통해서 웹 서버에 접속된 보안 모바일 기기 사이에서 보안 접속을 제공하도록 하는 명령어들을 포함하며, 상기 컴퓨터 시스템은 상기의 방법을 수행하는 명령어들을 포함한다.

[0023] 본 발명은, 중앙 프로세싱 유닛, 메모리 그리고 메모리로 로딩 가능하며 그리고 중앙 프로세싱 유닛에 의해 실행 가능한 명령어들을 저장하기 위한 저장 매체를 갖춘 호스트 컴퓨터용의 컴퓨터로 실행 가능한 명령어들을 포함하는 컴퓨터 독출가능 저장 매체를 제공한다. 상기 저장 매체는 중앙 프로세싱 유닛으로 하여금, 웹 사이트 도메인 이름을 구비한 웹 서버 상에서 시작된 웹 서버 애플리케이션 그리고 호스트 컴퓨터를 경유하여 네트워크를 통해서 웹 서버에 접속된 보안 모바일 기기 사이에서 보안 접속을 제공하도록 하는 명령어들을 포함하며, 상기 컴퓨터 시스템은 상기 방법을 수행하는 명령어들을 포함한다.

발명의 효과

[0024] 본 발명의 효과는 본원 명세서의 해당되는 부분에 개별적으로 명시되어 있다.

도면의 간단한 설명

[0025] 도 1은 사용자가 원격 웹 서비스에 액세스할 것을 시도할 수 있을 네트워크의 개략적인 표현이다.

도 2는 웹-브라우저 애플리케이션들이 스마트 카드와 상호작용하며 그리고 상기 웹 브라우저 애플리케이션과 상기 스마트 카드 사이의 상호작용이 스마트 카드 액세스 브라우저 확장을 경유하는 일 실시예를 도시하는 블록도이다.

도 3은 스마트 카드 상에 저장된 데이터에 대한 보안을 유지하면서, 웹 서버로부터 로딩된 웹 애플리케이션이 브라우저가 위치한 호스트 컴퓨터에 접속된 스마트 카드에 액세스하는 것을 허용하기 위한 원격 웹 서버와 브라우저 사이의 메시지 흐름을 도시하는 타이밍 시퀀스 도면이다.

도 4는 스마트 카드 브라우저 확장을 안전하게 다운로드하고 설치하기 위한 브라우저의 동작을 도시한 흐름도이다.

도 5는 브라우저가 실행되고 있는 호스트 컴퓨터에 접속된 스마트 카드로의 웹 애플리케이션들의 액세스를 안전하게 하기 위한 스마트 카드 액세스 브라우저 확장의 동작을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 다음의 상세한 설명에서, 첨부된 도면들을 참조하며, 그 도면들은 본 발명이 실행될 수 있을 특정 실시예들을

예시로 보여준다. 이런 실시예들은 본 발명이 속한 기술 분야에서의 통상의 지식을 가진 자들이 본 발명을 실행하는 것이 가능하도록 충분히 상세하게 설명된다. 본 발명의 다양한 실시예들이 비록 상이하지만 항상 상호 배타적인지는 않다는 것이 이해될 것이다. 예를 들면, 일 실시예와 연결하여 여기에서 설명된 특정한 특징, 구조 또는 특징은 본 발명의 사상과 범위로부터 벗어나지 않으면서 다른 실시예들 내에서 구현될 수 있을 것이다. 추가로, 각 개시된 실시예 내에서의 개별 엘리먼트들의 위치나 배치는 본 발명의 사상과 범위를 벗어나지 않으면서 수정될 수 있을 것이다. 그러므로, 다음의 상세한 설명은 제한하는 의미로 받아들여서는 안되며, 본 발명의 범위는 적절하게 해석된 첨부된 청구 범위에 의해서만 제한되며, 그 청구 범위는 청구 범위에게 부여된 등가물들의 전체 범위를 구비한다. 도면들에서, 유사한 참조번호들은 여러 모습들을 통해 동일하거나 유사한 기능들을 언급한다.

[0027] 본 발명의 일 실시예에서, 웹-브라우저 확장은 대부분의 컴퓨터들에서 발견되는 스마트 카드 자원 관리자(smart card resource manager (PC/SC)) 그리고 웹-브라우저 애플리케이션들 사이에 인터페이스를 제공한다. 상기 웹-브라우저 확장은 상기 웹-브라우저 애플리케이션들을 상기 스마트 카드 자원 관리자로부터 격리한다. 게다가, 상기 스마트 카드 액세스 웹-브라우저 확장은 상기 웹-브라우저 확장을 포함하여 웹 애플리케이션들이 상기 스마트 카드들로 액세스하도록 하는 상기 웹-브라우저가 실행되고 있는 상기 호스트 컴퓨터에 접속된 스마트 카드 그리고 상기 웹-브라우저 애플리케이션 사이에 상기 스마트 카드 자원 관리자를 경유하여 통신 파이프를 제공한다. 상기 웹-브라우저 애플리케이션들과 상기 스마트 카드 사이의 상호 작용은, 승인된 웹 애플리케이션들만이 상기 스마트 카드 액세스 웹-브라우저 확장을 경유하여 상기 스마트 카드의 내용물들에 액세스하는 것을 보장하기 위한 메커니즘들을 이용하여 안전하게 된다.

[0028] 도 1은 사용자 (501)가 웹 서버에 액세스할 것을 시도하고 있을 네트워크의 개략적인 모습이다. 상기 사용자 (501)는 호스트 컴퓨터 (103) 상에 윈도우 (503)를 디스플레이하는 웹-브라우저를 운용하고 있다. 사용자는 네트워크 (509)를 통해 온라인 트랜잭션의 몇몇 모습을 수행하기 위해서 원격 컴퓨터 시스템 (507) 상에서 실행되는 원격 웹 서버 (505)와 상호 대화하기를 원한다. 그 트랜잭션을 안전하게 하기 위해서, 상기 사용자 (501)는 인터페이스 기기 (111)를 경유하여 상기 호스트 컴퓨터 (103)에 연결된 스마트 카드 (104)를 사용한다. 상기 스마트 카드 (104)는 계정 정보 또는 그 사용자 (501)에 관련된 개인 정보와 같은 다른 사용자 데이터를 또한 포함할 수 있을 것이다. 많은 경우들에 있어서, 상기 스마트 카드 (104)는 암호화 기능들을 수행하도록 요청받을 수 있을 것이다.

[0029] 도 2는 웹 브라우저 애플리케이션 A (300a) 및 웹 브라우저 애플리케이션 B (300b)가 스마트 카드 액세스 브라우저 확장 (303)을 통해서 스마트카드 (104)와 상호 작용하는 본 발명의 일 실시예를 도시하는 블록도이다. 공동으로 계속중인 미국 특허 출원 112/849,117에서 설명되는 것처럼, 상기 스마트 카드 액세스 브라우저 확장 (303)은, 예를 들면, 공통 애플리케이션 프로그램 인터페이스 모습들로부터 브라우저 그리고 플랫폼 특정의 모습들을 나누기 위해서 여러 컴포넌트들로 분할될 수 있을 것이다. 그러나, 여기에서는, 설명을 간략하게 하기 위해서, 상기 스마트 카드 액세스 브라우저 확장 (303)은 하나의 모듈로서 설명된다.

[0030] 상기 스마트 카드 액세스 브라우저 확장 (303)은 스마트 카드 자원 관리자 (107)를 경유하여 상기 스마트 카드 (104)와 통신한다.

[0031] 상기 스마트 카드 액세스 브라우저 확장 (303)은 상기 브라우저(203) 내에 미리 설치될 수 있을 것이다. 그렇지 않다면, 상기 스마트 카드 액세스 브라우저 확장 (303)은 원격 서버 시스템 (513) 상에서 동작하는 서버 (511)로부터의 발행자 (510)로부터 다운로드될 것이다.

[0032] 도 3은 스마트 카드 (104) 상에 저장된 데이터를 위해서 그리고 원격 웹 서버 상의 사용자 계정을 위해 안전을 유지하면서 브라우저 (203)가 위치하고 있는 호스트 컴퓨터 (103)에 연결된 스마트 카드 (104)에 액세스하기 위해서 웹 서버 (505)로부터 로딩된 웹 애플리케이션 (300)을 허용하기 위한 원격 웹 서버 (505)와 브라우저 (203) 사이의 메시지 흐름을 예시한 타이밍 시퀀스 도면이다. 도 3의 예에서, 상기 스마트 카드 액세스 브라우저 확장 (303)은 상기 브라우저 (203)으로 이미 설치되어 있다는 것으로 추정된다.

[0033] 도 4는 상기 스마트 카드 액세스 브라우저 확장 (303)을 설치하는 것을 보여주는 흐름도이다.

[0034] 사용자 (501)는 자신이 웹 페이지에 액세스하는 것을 또는 원격 서버 (505) 상의 웹페이지와 어떤 방식으로 상호작용하는 것을 원하는가를 브라우저 (203)에게 지시함으로써 상호작용을 시작한다 (단계 351). 사용자의 요청에 응답하여, 상기 브라우저 (203)는 상기 원격 웹 서버 (505)로 http 요청 메시지를 발행한다 (단계 353). 여기에서 예측되는 시나리오를 위해서, 웹 애플리케이션이 상기 브라우저 (203)로 로딩된다. 그래서, 상기 웹 서

버 (505)는 상기 http 요청 (353)에 웹 애플리케이션 (300)을 포함하는 메시지 (355)로 응답한다 (단계 355). 상기 웹 애플리케이션이 이미 상기 브라우저 (203)로 로딩되었다면, 원격 웹 서버 (505)로부터 그것을 다운로딩하여 브라우저 (203)에 설치하는 단계는 필요하지 않다.

[0035] 다음에, 상기 웹 애플리케이션 (300)은 상기 스마트 카드 (104)에 액세스할 것을 시도한다 (단계 361). 상기 스마트 카드 (104)와의 상호작용들은 상기 스마트 카드 액세스 브라우저 확장 (303)에 의해서 열거된다. 상기 스마트 카드 액세스 브라우저 확장 (303)이 존재하지 않으면, 그것은 발행자 (510)로부터 다운로드된다. 스마트 카드 액세스 브라우저 확장 (303)을 다운로드하고 설치하는 것은 도 4와 함께 아래에서 더욱 상세하게 설명된다.

[0036] 보안 예방책으로서, 상기 웹 애플리케이션 (300)이 스마트 카드에 액세스하는 것을 허용하기 이전에, 상기 스마트 카드 액세스 브라우저 확장 (303)은 상기 웹 애플리케이션 (300)이 상기 스마트 카드 액세스 브라우저 확장 (303)을 통해서 스마트 카드들에 액세스하는 것을 승인받았는가의 여부를 판별한다 (단계 363). 웹 애플리케이션 (300)이 상기 스마트 카드 액세스 브라우저 확장 (303)을 통해서 스마트 카드들에 액세스하는 것을 승인받았는가의 여부를 판별하는 것은 도 5와 함께 더욱 상세하게 설명된다.

[0037] 상기 웹 애플리케이션 (300)이 (도 5의 프로세스에 의해서 판별된 것처럼) 승인받았다면 (참조번호 365의 판단 박스), 스마트 카드 액세스 브라우저 확장 (303)을 경유한 상기 스마트 카드 (104)와 웹 애플리케이션 (300) 사이의 접속이 설립된다 (단계 367). 승인받지 않았다면, 상기 스마트 카드 액세스 브라우저 확장 (303) 그리고 상기 스마트 카드 (104) 사이의 접속은 거절된다.

[0038] 상기 스마트 카드 액세스 브라우저 확장을 안전하게 다운로드하고 설치하기 위한 상기 브라우저의 동작들을 도시하는 흐름도인 도 4를 이제 참조한다. 스마트 카드 액세스 브라우저 확장 (303)의 설치는 두 가지의 주요한 부분들을 구비한다: https 프로토콜을 이용하여 웹 페이지들에 액세스할 때에 브라우저들에 의한 표준의 운용 절차로서 수행된 표준 브라우저 보안 검사 (401), 그리고 스마트 카드 액세스 브라우저 확장 (303)을 설치하기 위한 프로세스 (403). 상기 표준 브라우저 보안 검사 (401)는 상기 원격 서버 (505)로의 접속이 안전한 통신 프로토콜, 예를 들면, https를 통해서 존재하는 것인가를 판별함으로써 시작한다 (단계 405). 안전한 통신 프로토콜이 존재하지 않는다면, 상기 프로세스는 스마트 카드 액세스 브라우저 확장 프로세스 (403)를 검사하고 설치하는 것으로 진행한다.

[0039] 안전한 통신 프로토콜이 존재하면, SSL 인증의 유효성이 판별된다 (단계 407). SSL 인증의 유효성은 SSL 인증 내에 목록화된 공통 이름 (common name) 그리고 액세스되는 웹 페이지의 URL 사이에서의 부합 (match)을 필요로 하며, 상기 인증은 신뢰받는 루트 인증 기관에 의해서 서명되었다는 것 그리고 그 인증이 기간만료 되지 않았다는 것을 필요로 한다. 상기 SSL 인증이 유효하면, 상기 프로세스는 스마트 카드 액세스 브라우저 확장 설치 프로세스 (403)로 진행한다. 인증이 유효하지 않으면, 사용자는 설치를 진행할 것인가 아닌가를 결정할 것을 질문받으며 (단계 409), 설치를 진행한다면 (예), 프로세스는 스마트 카드 액세스 브라우저 확장 설치 프로세스 (403)로 진행한다. 설치를 진행하지 않는다면, 프로세스는 중단되며 (단계 415), 그리고 상기 스마트 카드 액세스 브라우저 확장 (303)은 설치되지 않으며 그래서 스마트 카드 (104)로의 어떤 액세스도 방지된다.

[0040] 스마트 카드 액세스 브라우저 확장 설치 프로세스 (403)는 상기 스마트 카드 액세스 브라우저 확장 (303)이 이미 설치되었는가의 여부를 검사하는 것으로 시작한다 (단계 411). 설치되었다면, 상기 스마트 카드 액세스 브라우저 확장 (303)은 승인된 웹 애플리케이션들 (300)이 스마트 카드 (104)로 액세스하는 것을 허용하기 위해서 사용될 수 있을 것이다 (그 프로세스는 도 5에서 도시되고 그리고 도 5와 함께 설명된다). 설치되지 않았다면, 상기 프로세스는 사용자에게 상기 스마트 카드 액세스 브라우저 확장 (303)을 설치하는가의 여부, 예를 들면, 호스트 컴퓨터 (103)로 접속된 스마트 카드들로의 액세스를 웹 애플리케이션들 (300)에게 제공하는 기능성을 상기 브라우저 (203)가 제공하는 것을 가능하게 하는 것을 상기 사용자가 원하는가의 여부를 사용자에게 물어보는 것으로서 진행한다. 원하지 않는다면, 프로세스는 중단된다. 원한다면, 상기 스마트 카드 액세스 브라우저 확장 (303)은 발행자 (510)로부터 다운로드된다 (단계 417).

[0041] 상기 스마트 카드 액세스 브라우저 확장 (303)이 다운로드되었을 때에, 스마트 카드 액세스 브라우저 확장 (303)의 유효성이 검증된다 (단계 419). 상기 스마트 카드 액세스 브라우저 확장 (303)이 유효하면, 스마트 카드 액세스 브라우저 확장 (303)은 그 발행자의 비밀 키를 이용하여 발행자에 의해서 서명이 되어야만 한다. 대응하는 공개 키 (public key)를 포함하는 SSL 인증은 신뢰받은 루트 인증기관, 예를 들면, Versign에 의해서 서명이 된다. 그래서, 상기 브라우저 (203)는 상기 스마트 카드 액세스 브라우저 확장 (303)이 상기 발행자 (510)에 의해서 서명되었으며 그리고 상기 스마트 카드 액세스 브라우저 확장 (303)에 대한 SSL 인증이 신뢰받는

루트 인증기관에 의해서 서명되었다는 것을 확인함으로써 상기 스마트 카드 액세스 확장 브라우저 (303)를 검증할 수 있을 것이다. 상기 스마트 카드 액세스 브라우저 확장 (303)의 유효성이 확인되면 (예), 스마트 카드 액세스 브라우저 확장 (303)은 상기 브라우저 (203)로 설치된다 (단계 421).

[0042] 검증 실패에 대한 두 가지의 대안의 실시예들이 존재한다. 먼저, 설치가 단순하게 거절될 수 있을 것이며 (아니오 [1]) 그러면 상기 설치 프로세스 (403)는 종결된다 (415). 두 번째 대안에서 (아니오 [2]), 사용자는 상기 설치를 진행할 것인가의 여부에 관해서 질문받는다 (단계 423). 그 대안에서, 사용자가 검증 실패에도 불구하고 설치를 수락하면, 그 설치는 진행된다 (단계 421). 수락하지 않는다면, 그 프로세스는 스마트 카드 액세스 브라우저 확장 (303)을 설치하지 않고 종결된다 (단계 415).

[0043] 일단 상기 스마트 카드 액세스 브라우저 확장 (303)이 설치되면, 스마트 카드 액세스 브라우저 확장 (303)은 스마트 카드들 (104)에 액세스하기 위해서, 승인된 웹 애플리케이션들에 의해서 사용될 수 있을 것이다 (단계 425). 스마트 카드들에 액세스하기 위해서 웹 애플리케이션이 스마트 카드 액세스 브라우저 확장 (303)을 이용하는 것을 승인받았다는 것을 검증하는 프로세스는 도 5와 함께 더욱 상세하게 설명된다.

[0044] 도 5는 브라우저 (300)가 실행되고 있는 호스트 컴퓨터 (104)에 연결된 스마트 카드 (104)에 웹 애플리케이션들 (300)이 안전하게 액세스하기 위한 스마트 카드 액세스 브라우저 확장 (303)의 동작들을 예시하는 흐름도이다.

[0045] 원격 웹 서버 (505)와의 안전한 통신을 보장하기 위해 그리고 MITM 공격들이 성취되는 것을 더욱 어렵게 만들기 위해서, 상기 스마트 카드 액세스 브라우저 확장 (303)은 보안 접속들, 예를 들면, 웹 브라우저와 원격 웹 서버 사이의 https 접속들로서, 상기 https 접속이 유효한 인증을 이용하여 보안이 되는 보안 접속들만을 허용한다. 사용자가 인증이 유효하지 않음에도 불구하고 계속하기 위해서 경보 메시지를 무시하면, 도 5의 프로세스는 상기 사용자에 의한 그 결정을 무효로 하고 그리고 비록 상기 사용자가 무효의 인증을 이용하여 상기 브라우저 (203)와 상기 원격 서버 (505) 사이의 접속을 이전에 허용했다고 하더라도 상기 웹 애플리케이션 (300)과 상기 스마트 카드 (1040 사이의 접속을 허용하지 않는다. 상기 SSL-특정 실시예에서, 이런 방식으로, MITM을 달성하기 위해서, 악의적인 웹사이트는 유효한 SSL 인증을 가지고 있어야만 한다. 악의적인 웹사이트가 SSL 인증을 획득하는 것이 가능할 수 있을 것이지만, 스마트 카드 (104)의 내용물들 그리고 원격 서버에서의 사용자의 계정을 MITM 공격으로부터 또한 보호하기 위해서, 상기 스마트 카드 액세스 브라우저 확장 (303)은 접속 키 (connection key) 그리고 서버 검증 (server validation)이라는 두 가지 다른 매커니즘들을 채택하며, 이는 아래에서 더욱 상세하게 설명된다. 그러나, 원격 웹 서버 (505)로의 접속이 안전한 프로토콜, 예를 들면, https를 이용하여 보안이 되는가의 여부가 초기 단계에서 판별된다 (단계 551). 상기 접속이 https가 아니면 (판단 박스 553), 상기 웹 애플리케이션 (300)은 스마트 카드 (104)로 액세스하는 것이 허용되지 않으며, 그리고 상기 프로세스는 종결된다 (단계 555). 상기 접속이 https이면, 상기 스마트 카드 액세스 브라우저 확장 (303)은 상기 원격 서버 (505)의 SSL 인증을 확인하는 것으로 진행한다 (단계 557).

[0046] 원격 서버로부터 통신 채널을 안전하게 지키는 인증이 유효하지 않으면, 예를 들면, 상기 https-특정 실시예에서 상기 SSL 인증이 유효하지 않으면 (판단 박스 559), 상기 웹 애플리케이션 (300)은 상기 스마트 카드 (104)에 액세스하는 것이 허용되지 않으며, 그리고 프로세스는 종결된다 (단계 555). 그렇지 않다면 (예), 상기 웹 애플리케이션 (300)이 상기 스마트 카드 액세스 브라우저 확장 (303)을 경유하여 스마트 카드들 (104)에 액세스하는 것이 상기 발행자 (510)에 의해서 승인되었는가의 여부를 판별하기 위해서 접속 키가 검사된다 (단계 561).

[0047] 정당한 웹사이트들만이, 예를 들면, 해로운 오퍼레이터인 것 같지 않은 것으로서 상기 발행자 (510)에 의해서 상세하게 조사되었던 웹 사이트들만이 스마트 카드들 (104)에 액세스하기 위해서 상기 스마트 카드 액세스 브라우저 확장 (303)을 이용할 수 있다는 것을 보장하기 위해서, 상기 발행자는 상기 발행자가 정당한 것으로 믿고 있는 웹사이트들로 접속 키들을 발행한다. 예를 들면, 상기 스마트 카드 액세스 브라우저 확장 (303)이, 미국 텍사스, 오스틴에 있는 Gemalto, Inc.로부터의 SConnect 기술이면, Gemalto에 의해 승인된 웹사이트들만이 SConnect를 경유하여 스마트 카드들에 액세스하는 것이 허용된다. 상기 접속 키는 발행자의 비밀 키 K_{priv} 에 의해서 서명된다. 상기 발행자의 대응 공개 키 K_{pub} 는 상기 스마트 카드 액세스 브라우저 확장 (303)으로 인코딩된다. 상기 접속 키는 어떤 비밀도 포함하지 않는다. 상기 접속 키는 다음의 항목들을 포함한다:

[0048] 1. 조직 이름;

[0049] 2. 공통 이름, 이는 웹사이트의 도메인 이름이다;

[0050] 3. 발행자 이름, 예를 들면, Gemalto;

[0051] 4. 상기 접속 키의 발행 날짜 그리고 기간 만료 날짜;

[0052] 5. 서명, 이는 발행자에 의해서 서명된 상기 요소의 디지털 서명이다;

[0053] 6. 웹사이트 SSL 인증의 지문.

[0054] 웹 애플리케이션 (300)이 스마트 카드 (104)에 접속하려고 하는 세션을 설립할 때에, 웹사이트는 그 웹사이트의 접속 키를 상기 스마트 카드 액세스 브라우저 확장 (303)에게 제출해야만 한다. 상기 스마트 카드 액세스 브라우저 확장 (303)은 상기 접속 키 내의 다음의 항목들을 검사함으로써 상기 접속 키를 검증한다 (단계 561):

[0055] 1. 공통 이름이 상기 웹사이트의 도메인 이름 (요청자의 도메인 이름의 근원 (origin))과 부합해야만 한다;

[0056] 2. 상기 기간만료 날짜는 현재의 날짜이거나 또는 현재의 날짜를 지나야만 한다;

[0057] 3. 상기 서명은 상기 Gemalto 공개 키 (K_{pub})를 이용하여 검증을 통과해야만 한다;

[0058] 4. 상기 지문은 상기 웹사이트 SSL 인증의 지문과 부합해야만 한다.

[0059] 상기 스마트 카드 액세스 브라우저 확장 (303)은 상기 접속 키를 검증하는 것이 성공적이어야만 (판단 박스 563) 상기 웹사이트로부터 상기 스마트 카드로의 접속을 허용한다. 성공적이지 않다면, 상기 접속 요청은 거부된다.

[0060] 일 실시예에서, 오퍼레이터에게 승인된 접속 키를 철회하기 위해서 철회 매커니즘이 구현된다. 그것은 OCSP (Online Certificate Status Protocol)를 이용하여 달성될 수 있을 것이다. 대안의 실시예에서, 상기 접속 키는 규정된 기간 이후에 기간 만료로 설정된다. 웹사이트 (505)는 자신의 접속 키가 기간 만료되면 그 접속 키를 갱신해야만 한다.

[0061] 접속 키가 유효하지 않은 것으로 판별되면 (판단 박스 563), 상기 프로세스는 상기 스마트 카드 액세스 브라우저 확장 (303)을 경유한 웹 애플리케이션 (300)과 스마트 카드 (104) 사이의 접속을 생성하지 않고 종결된다 (단계 555).

[0062] 대안의 일 실시예에서, 상기 접속 키는 그 자체적으로는 원격 서버를 인증하기에 충분한 것으로 간주되지 않는다. 웹사이트가 스마트 카드 액세스 브라우저 확장 (303)을 사용하는 것에 대한 승인을 주는 것은 주로 승인 툴이다. 웹 서버와 웹 브라우저 사이에서 수행되는 SSL 핸드세이킹, 스마트 카드 액세스 브라우저 확장 (303)에 의해서 수행되는 서버 검증 (여기에서는 아래에서 설명된다), 그리고 접속 키 확인은 함께 서버 승인 및 인증을 제공한다.

[0063] 그래서, 상기 접속 키가 유효한 것으로 판별되면 (판단 박스 563), 상기 웹 사이트가 스마트 카드 액세스 브라우저 확장 (303)을 경유하여 스마트 카드들 (104)에 액세스하는 것을 사용자가 허용했던 웹 사이트인가의 여부가 다음의 단계에서 판별된다 (단계 565). 허용된 사이트들은 허가 데이터베이스에서 화이트 리스트 내에서 유지되며, 상기 데이터베이스는 스마트 카드 액세스 브라우저 확장 (303)을 경유하여 스마트 카드들에 액세스하는 것이 허용되지 않은 사이트들의 블랙 리스트를 또한 보유한다. 상기 웹 사이트가 (허용된 웹 사이트들을 포함하는) 화이트 리스트 내에 있으면 (판단 박스 (567) (예)), 참조번호 367의 접속 (도 3)이 설립된다 (단계 569).

[0064] 상기 웹 사이트가 화이트 리스트 내에 있지 않다면, 사용자는 그 웹 사이트를 허용하는가의 여부에 대해서 질문을 받으며 (단계 571), 허용한다면 (판단 박스 (573)), 그 대답을 허가 DB 내에 저장하는가의 여부를 질문받는다 (판단 박스 575). 사용자가 웹사이트의 스마트 카드로의 액세스 그리고 허가 데이터베이스로 추가되는 것을 허용하기 원한다면, 상기 웹사이트는 상기 허가 데이터베이스의 화이트 리스트에 추가된다 (단계 577). 반대로, 사용자가 웹 사이트 액세스를 허용하기 원하지 않는다면, 그 웹 사이트는 상기 허가 데이터베이스의 블랙 리스트에 추가될 수 있을 것이다 (도면을 간략하게 하기 위해서 이것은 명시적으로 도시되지는 않는다. 그러나, 그 매커니즘은 허용된 웹 사이트를 화이트 리스트에 추가하는 것과 유사하다).

[0065] 허가 데이터베이스에 대해서 허가되지 않은 것으로 결정된 웹사이트를 허용하기를 사용자가 원하지 않는다면, 상기 프로세스는 웹 애플리케이션 (300)과 스마트 카드 (104) 사이에서의 접속을 설립하지 않고 종결된다 (555).

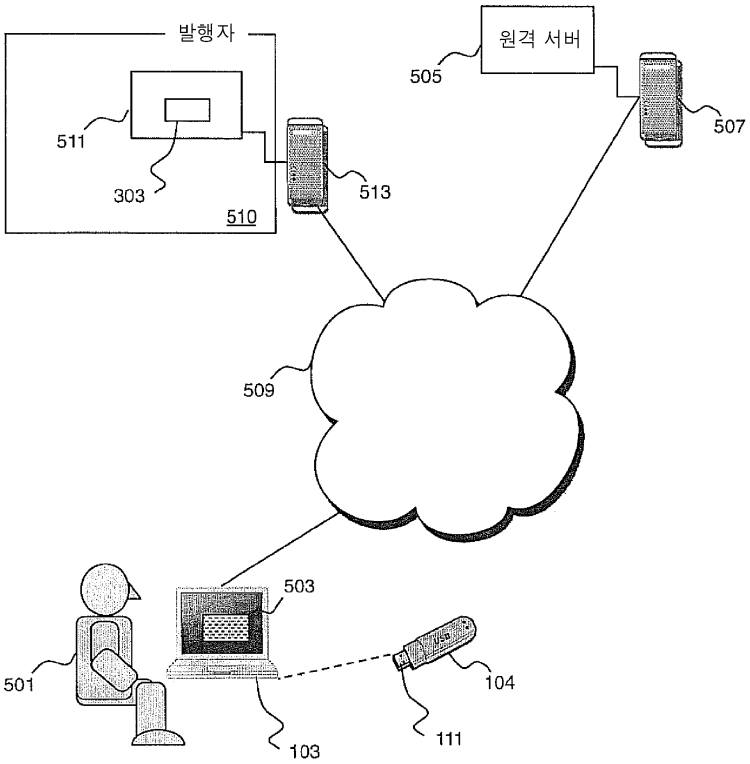
[0066] 앞의 설명으로부터, 여기에서 설명된 기술이 웹 애플리케이션들의 환경에서 한결같이 (seamlessly) 스마트 카드들을 사용하기 위한 효율적인 매커니즘을 제공한다는 것이 명백할 것이다. 이런 매커니즘들은, 확인되었던 승인

된 웹 애플리케이션들만이 호스트 컴퓨터 상에서 웹 애플리케이션들과 스마트 카드들 사이에서의 상호작용을 안내하는 스마트 카드 액세스 브라우저 확장 (303)을 경유하여 스마트 카드들로의 액세스를 할 수 있을 것이라는 것을 보장하기 위해서, 강화된 레벨의 보안을 제공한다. 전술한 메커니즘들을 통해서, 중간자 공격, DNS 캐시 포이즌 공격, 피싱 등과 같은 공격들에 노출되는 위험들이 최소화된다.

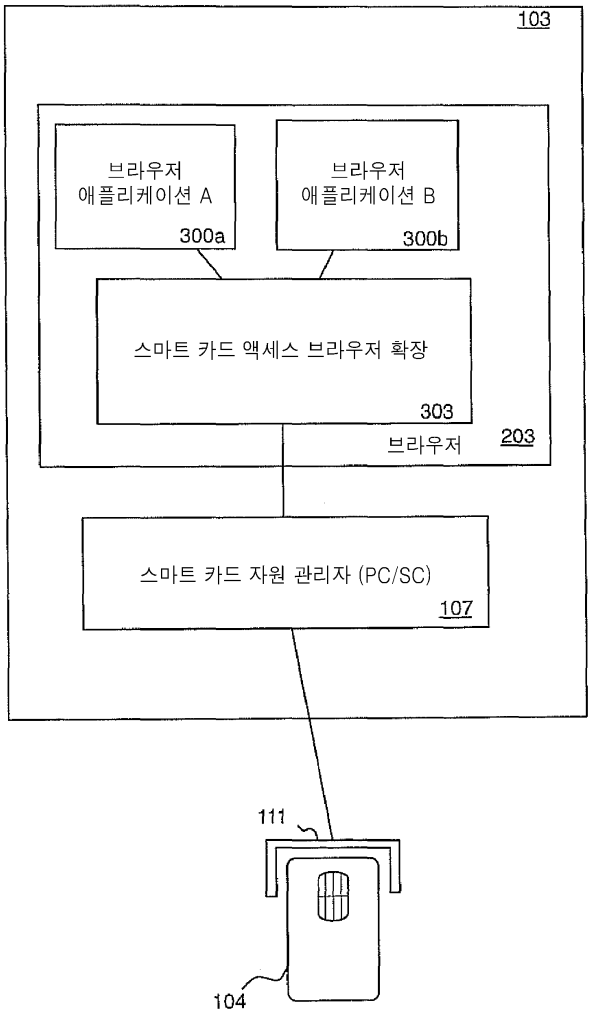
[0067] 비록 본 발명의 특정 실시예들이 설명되고 예시되었지만, 본 발명은 그렇게 설명되고 예시된 부분들의 특정 형상들이나 배치들로 한정되지 않는다. 본 발명은 청구범위에 의해서만 한정된다.

도면

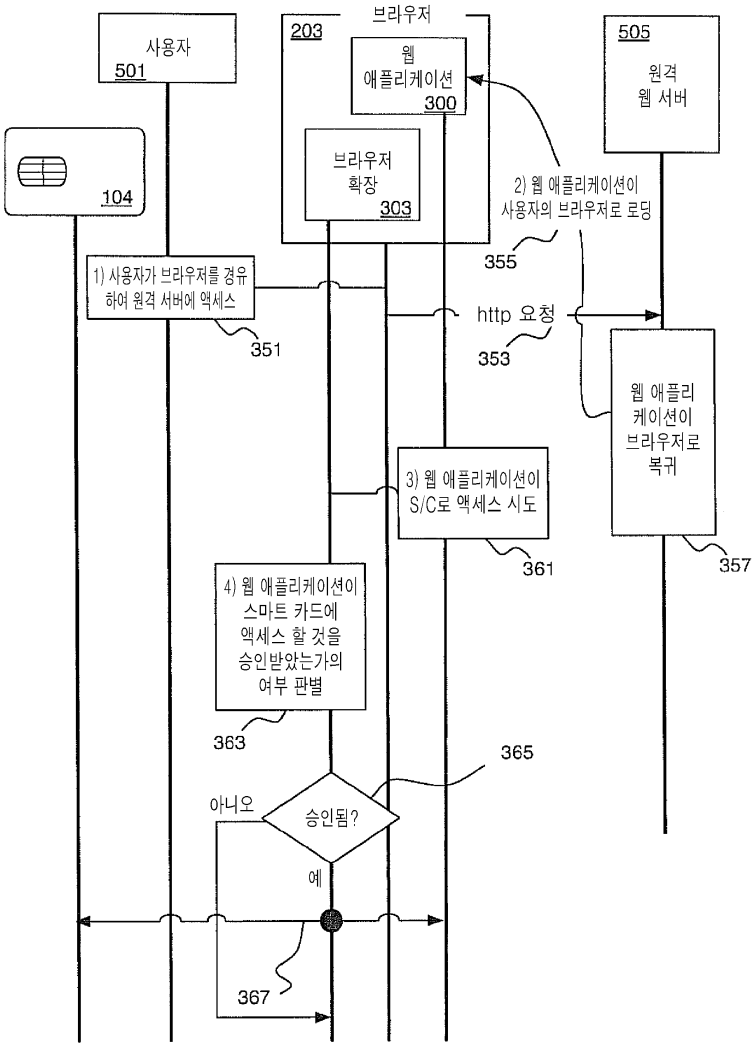
도면1



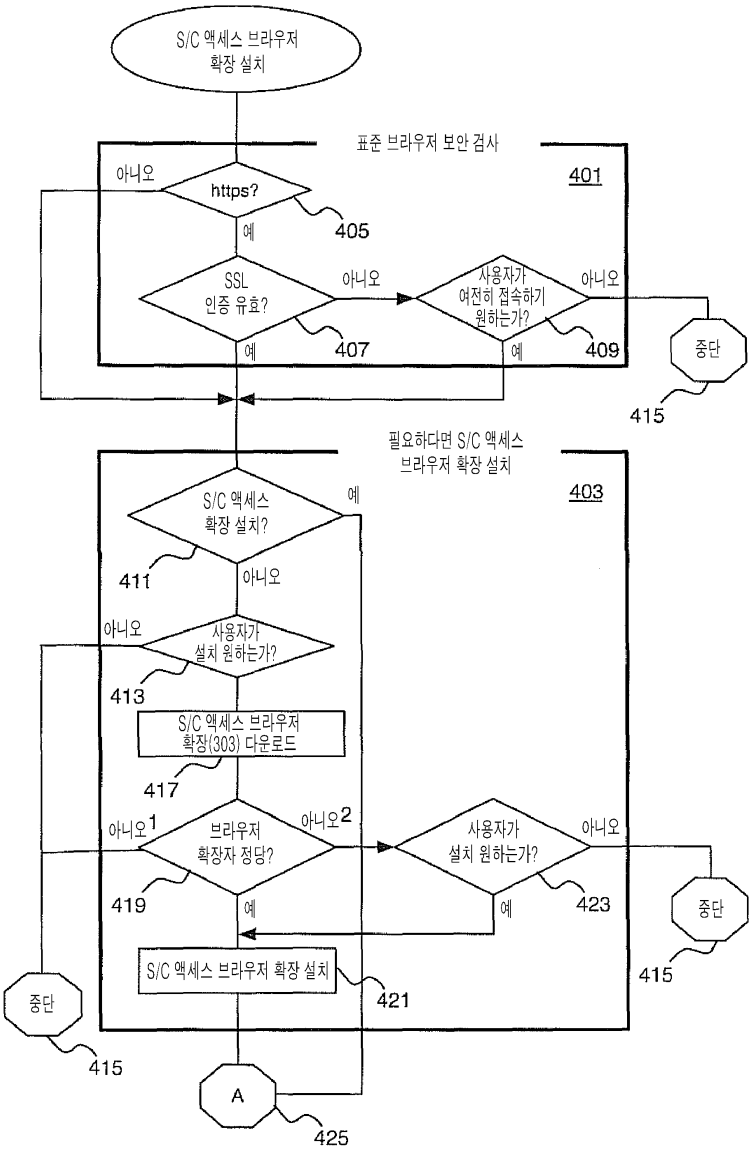
도면2


103
브라우저
애플리케이션 A
300a
브라우저
애플리케이션 B
300b
스마트 카드 액세스 브라우저 확장
303
브라우저
203
스마트 카드 자원 관리자 (PC/SC)
107
111
104

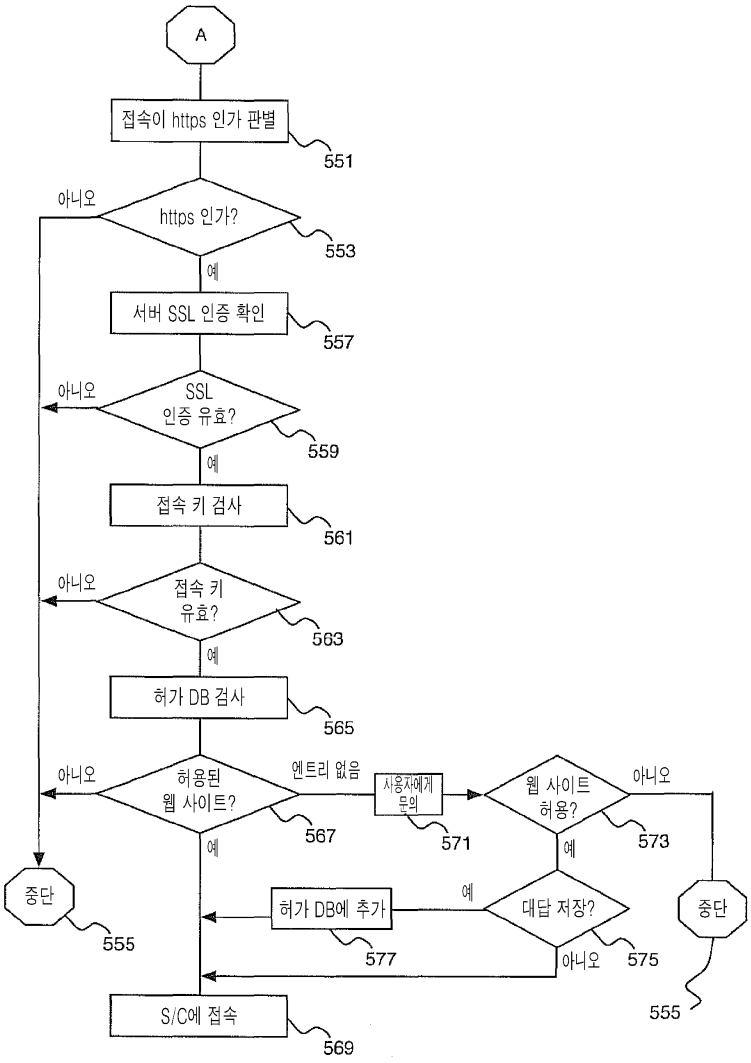
도면3


사용자
501
104
브라우저
203
웹
애플리케이션
300
브라우저
확장
303
505
원격
웹 서버
2) 웹 애플리케이션이
사용자의 브라우저로 로딩
355
1) 사용자가 브라우저를 경유
하여 원격 서버에 액세스
351
http 요청
353
웹 애플리
케이션이
브라우저로
복귀
357
3) 웹 애플리케이션이
S/C로 액세스 시도
361
4) 웹 애플리케이션이
스마트 카드에
액세스 할 것을
승인받았는가의
여부 판별
363
365
아니오
승인됨?
예
367

도면4


S/C 액세스 브라우저
확장 설치
표준 브라우저 보안 검사
401
아니오
https?
405
예
SSL
인증 유효?
아니오
407
예
사용자가
여전히 접속하기
원하는가?
아니오
409
예
중단
415
필요하다면 S/C 액세스
브라우저 확장 설치
403
S/C 액세스
확장 설치?
예
411
아니오
아니오
사용자가
설치 원하는가?
413
S/C 액세스 브라우저
확장(303) 다운로드
417
아니오1
브라우저
확장자 정당?
아니오2
419
예
사용자가
설치 원하는가?
아니오
423
예
중단
415
S/C 액세스 브라우저 확장 설치
421
중단
415
A
425

도면5


A
접속이 https 인가 판별
551
https 인가?
553
아니오
예
서버 SSL 인증 확인
557
SSL 인증 유효?
559
아니오
예
접속 키 검사
561
접속 키 유효?
563
아니오
예
허가 DB 검사
565
허용된 웹 사이트?
567
아니오
엔트리 없음
사용자에게 문의
571
웹 사이트 허용?
573
아니오
예
예
중단
555
허가 DB에 추가
577
대답 저장?
575
예
아니오
중단
555
S/C에 접속
569