(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년01월06일
(11) 등록번호 10-1005910
(24) 등록일자 2010년12월28일

(51) Int. Cl.
H04L 29/06 (2006.01) *H04L 9/32* (2006.01)
G06F 21/00 (2006.01)
(21) 출원번호 10-2009-7005843
(22) 출원일자(국제출원일자) 2007년08월22일
심사청구일자 2009년03월23일
(85) 번역문제출일자 2009년03월20일
(65) 공개번호 10-2009-0042864
(43) 공개일자 2009년04월30일
(86) 국제출원번호 PCT/US2007/018679
(87) 국제공개번호 WO 2008/024454
국제공개일자 2008년02월28일
(30) 우선권주장
60/839,171 2006년08월22일 미국(US)
(뒷면에 계속)
(56) 선행기술조사문헌
LNCS 2437, pp. 40-58, 2002, Jan De Clercq, Single Sign-On Architectures
전체 청구항 수 : 총 13 항

(73) 특허권자
인터디지탈 테크날러지 코포레이션
미국 델라웨어 19810 윌밍턴 실버사이드 로드 3411 콩코드 플라자 스위트 105 해글리 빌딩
(72) 발명자
샤 요겐드라 씨
미국 펜실베이니아주 19341 엑스톤 레전시 코트 10
차 인혁
미국 펜실베이니아주 19067 야들레이 사우스리지 서클 510
(뒷면에 계속)
(74) 대리인
신정건, 김태홍

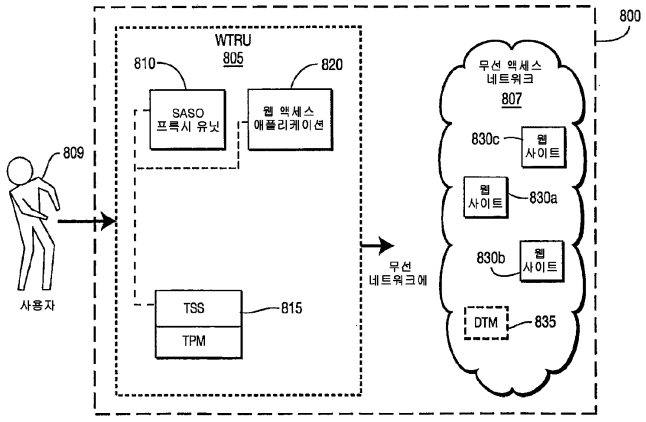
심사관 : 이성영

(54) 애플리케이션 및 인터넷 기반 서비스들에 신뢰성있는 싱글 사인온 액세스를 제공하는 방법 및 장치

(57) 요 약

트러스티드 컴퓨팅(TC) 기술에 기초한 패스워드 관리 및 싱글 사인 온(SSO) 액세스를 위한 방법 및 장치가 개시되어 있다. 이 방법은 패스워드들과 SSO 크리덴셜들을 발생, 저장 및 검색하기 위해 안전하고 신뢰성있는 메카니즘을 제공하도록, SSO 프록시 유닛과 웹 액세스 애플리케이션 양쪽 모두와 상호작용하는 트러스티드 컴퓨팅 그룹(TCG)의 트러스티드 플랫폼 모듈(TPM)을 구현한다. 본 발명의 여러 실시예들이 사용자로 하여금 사용자의 장치에 상주하는 안전한 프록시에 단지 한번 사인온한 후에 미리 식별된 사이트 그룹에 속하는 한 사이트에서 다른 사이트로 안전하고 투과적으로 호핑할 수 있게 한다.

대 표 도



(72) 발명자

레즈닉 알렉산더

미국 뉴저지주 08560 터터스빌 리버 로드 1212

로페즈 토레스 오스카

미국 펜실베이니아주 19406 킹 오브 프러시아 이-305 웨스트 데칼브 파이크 251

(30) 우선권주장

60/887,042 2007년01월29일 미국(US)

60/912,025 2007년04월16일 미국(US)

특허청구의 범위

청구항 1

싱글 사인 온(SSO; single sign-on) 기술을 이용하여 안전한 로그인 ID 및 패스워드 관리를 수행하는 무선 송수신 유닛(WTRU; wireless transmit/receive unit)으로서,

사용자를 인증하고 SSO 동작을 관리하도록 구성된 SSO 프록시 소프트웨어와;

웹사이트에의 사용자 액세스를 제공하도록 구성된 웹 액세스 애플리케이션(WAA; web accessing application)과;

상기 SSO 동작을 위해 플랫폼 소프트웨어, SSO 프록시 소프트웨어 및 웹 액세스 애플리케이션(WAA)의 무결성 검증을 수행하도록 구성된 트러스티드 플랫폼 모듈(TPM; trusted platform module)

을 포함하며,

상기 TPM, 상기 SSO 프록시 소프트웨어 및 상기 WAA는 웹사이트들의 그룹 중 적어도 하나의 웹사이트와 상호작용하여, 상기 적어도 하나의 웹사이트에 대한 사용자 액세스를 승인하기 위하여, 상기 웹사이트들의 그룹 중 상기 적어도 하나의 웹사이트에 액세스하기 위한 로그인 ID 및 패스워드를 안전하게 생성하고 저장하며 제공하는 것인 무선 송수신 유닛.

청구항 2

제1항에 있어서, 상기 TPM은 또한, 랜덤하고 높은 엔트로피의 패스워드를 발생시키도록 구성되는 것인 무선 송수신 유닛.

청구항 3

제1항에 있어서, 상기 TPM은 또한, 랜덤하고 높은 엔트로피의 로그인 ID들을 발생시키도록 구성되는 것인 무선 송수신 유닛.

청구항 4

제1항에 있어서, 상기 SSO 프록시 소프트웨어는 또한, 적어도 생체 팩터를 포함한 인증 팩터들에 기초하여 사용자를 인증하도록 구성되는 것인 무선 송수신 유닛.

청구항 5

제1항에 있어서, 상기 WAA는 또한, 사용자를 인증하였다면, 웹사이트 그룹에서의 모든 웹사이트에의 액세스를 제공하도록 구성되는 것인 무선 송수신 유닛.

청구항 6

제2항에 있어서, 상기 패스워드는 웹사이트 특유의 패스워드인 것인 무선 송수신 유닛.

청구항 7

제3항에 있어서, 상기 로그인 ID는 웹사이트 특유의 로그인 ID인 것인 무선 송수신 유닛.

청구항 8

제1항에 있어서, 상기 TPM은 또한, 웹사이트의 정책 요건들을 만족시키는 로그인 ID 및 패스워드를 발생시키도록 구성되는 것인 무선 송수신 유닛.

청구항 9

제1항에 있어서, 상기 SSO 프록시 소프트웨어는 웹사이트에 의해 프롬프트될 때 또는 만료 시간이 도달할 때 패스워드를 자동으로 업데이트하기 위해 웹사이트와 상호작용하도록 구성된 정책 매니저를 포함하는 것인 무선 송수신 유닛.

청구항 10

제1항에 있어서, 상기 TPM은 또한, 안전한 실행 환경을 형성하고 안전한 저장을 제공하기 위해 부트 코드, 오퍼레이팅 시스템, 드라이버, 소프트웨어 및 파라미터의 검증을 수행함으로써 플랫폼 소프트웨어의 무결성 검증을 수행하도록 구성되는 것인 무선 송수신 유닛.

청구항 11

제1항에 있어서, 상기 WTRU는 장치 트러스트 미러(DTM; device trusted mirror)와의 신뢰성있는 관계를 성립하기 위하여 DTM과의 상호 인증을 수행하도록 구성되는 것인 무선 송수신 유닛.

청구항 12

제11항에 있어서, 상기 WTRU는 또한, 신뢰성에 대한 정보와 크리덴셜들을 상기 DTM을 통하여 외부 요청자들에 제공하고 무선 액세스 네트워크와 웹사이트와의 보안 링크를 성립하도록 구성되는 것인 무선 송수신 유닛.

청구항 13

제1항에 있어서, 상기 TPM은 또한, 통신 링크를 성립시키기 전에 무결성 검증을 수행하도록 구성되는 것인 무선 송수신 유닛.

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 무선 통신에 관한 것이다. 보다 자세하게는, 애플리케이션 및 인터넷 기반 서비스들에 신뢰성있는 싱글 사인온(SSO) 액세스와 신뢰성있는 식별정보(ID) 관리를 제공하는 방법 및 장치가 개시된다.

배 경 기 술

[0002] 무선 통신 장치의 수가 증가함에 따라, 제3자 인터넷 컨텐츠 공급자에 의해 제공된 독립적이고 안전한 웹사이트에 로깅하는 사용자 인증 프로세스를 강화하고 간략화시킬 필요가 있다. 이들 웹사이트들 내의 액세스를 얻기 위하여, 사용자들은 각각의 서비스에 대해 고유한 사용자 ID들과 패스워드들을 세트업할 필요가 있다. 그러나, 서로 다른 패스워드 정책들의 지배를 받는 복수의 사용자 ID들과 패스워드를 이용하는 것은 번거로우며, 보안 침해를 받기 쉽다. 따라서, 무선 통신 장치 사용자에 대한 사용자 인증 프로세스를 간략화하면서 패스워드 관리의 보안 레벨을 강화시키는 방법이 매우 요구된다.

[0003] 제3자 웹서비스 공급자는 무선 네트워크 오퍼레이터와 별도의 협약을 유지하기 때문에, 무선 액세스 네트워크(RAN), 고정 또는 낮은 이동성 무선 네트워크(예를 들어, IEEE 802.16-타입 네트워크)와 같은 무선 네트워크, 또는 고정 유선 네트워크인 액세스 네트워크 상에서의 제3자 서비스에 대한 기본 사용자 인증 프로세스에 대해서는 비실용적이다. 서비스 공급자들과 사용자들은 종종 단일의 아이덴티티들을 이용하여 복수의 RAN들, 무선 네트워크들 또는 고정 네트워크들을 통해 서비스들을 액세스하기 때문에, 사용자들 및 제3자 서비스 공급자들은 서로 다른 네트워크들에 걸쳐 SSO 동작을 실시하기 쉬우며, 여기서, 네트워크 오퍼레이터들은 사용자 허가 승인을 통한 제어를 관리할 수 있다.

[0004] 한 시나리오에서, 무선 네트워크 오퍼레이터들과 제3자 ID 서비스 공급자들은 서로 다른 유형의 네트워크들, 오퍼레이터들 및 서비스 공급자들에 걸쳐 끊김없는 서비스 연속성을 용이하게 하도록 사용자들에 균일한 사용자 ID들을 제공할 수 있다. 균일한 사용자 ID들은 서로 다른 네트워크 유형 및 엔티티들과, 서비스 공급자 바운더

리들의 서비스들에 걸쳐 빈번하고 높은 볼륨의 변화로부터 야기되는 과도적인 문제들을 해결할 수 있다.

[0005] 패스워드들 또는 인증 크리덴셜들의 허술한 관리는 보안에 충격적인 영향을 줄 수 있다. 침입자들(Attacker)은 약한 패스워드 또는 훔친 패스워드를 통하여 민감한 데이터에 대한 액세스를 얻을 수 있다. 허술한 패스워드 관리는 또한 동작 비용에서의 증가를 초래할 수 있다. 예를 들어, 헬프 데스크 콜 볼륨(Help Desk call volume)은 사용자 자신의 손실되거나 또는 잊어버린 패스워드들을 검색하거나 또는 리세트하기 위해 호출하는 사용자 수의 증가에 따라 급격하게 증가할 수 있다.

[0006] 다음은 이하에 보다 자세히 설명될 바와 같이 패스워드 관리를 향상시키는 종래 기술의 솔루션들로서, 고유 패스워드 정책(specific password policy), 패스워드 없이 인증(password-less authentication), 생체 팩터(biometric factor), 패스워드 동기화(password synchronization), 크리덴셜 매핑(credential mapping), 엔터프라이즈 싱글 사이온(enterprise single sign-on; E-SSO), E-SSO와 패스워드 동기화의 결합형(combining E-SSO with password synchronization), 웹 싱글 사이온(web single sign-on; web-SSO) 및 SAML(Security Assertion Markup Language)이 있다.

[0007] 사용자 패스워드 보안 레벨을 강화하기 위하여, 조직(organization)은 고유 패스워드 정책을 실시할 수 있다. 공통 패스워드 정책은 사용자가 하드 투 게스 패스워드(hard-to-guess passwords; 추정이 어려운 패스워드)를 세트업하거나 또는 패스워드들을 자주 변경하는 것을 필요로 할 수 있다. 패스워드 정책은 또한 즉각적인 패스워드 재사용을 방지하기 위해 사용자 패스워드 이력을 로깅할 수 있거나, 또는 특정 횟수의 시도들 후에 로그인에 실패한 누군가를 로크아웃하기 위해 로크아웃 정책들을 실시할 수 있다. 양호한 패스워드 정책들을 실시하는 것은 패스워드 보안성을 강화할 수 있지만, 이것은 또한 사용자로 하여금 기억하고 관리하기에 쉬운 패터닝된 패스워드들을 세트업하도록 하는 것을 조장할 수 있다. 예를 들어, 사용자는 패스워드 정책들의 복잡성 요건들을 충족하기 위해 @#$%9876과 같이 문자와 숫자의 조합을 이용하여 패스워드를 생성할 수 있다. 그러나, 사용자는 패스워드를 변경하도록 시스템에 의해 프롬프트받는 경우, @#$%8765 또는 @#$%7654와 같이 구 패스워드의 변형을 이용하여 새로운 패스워드를 생성할 수 있다. 사용자의 패스워드 이력의 인식(knowledge)은 구 패스워드의 변형에 대한 침입 시도(break-in attempt) 횟수를 매우 좁히기 때문에 패터닝된 패스워드들의 이용은 패스워드 보안 레벨을 약화시킨다. 복잡한 패스워드들은 기억하기가 어렵고, 엄격한 패스워드 정책들은 사용자로 하여금 다른 서비스들에 대하여 동일한 패스워드들을 사용하게끔 할 수 있다. 패스워드들이 다른 서비스들에 걸쳐 공유되는 경우, 임의의 서비스들에서 손상된 단일의 패스워드는 다른 모든 서비스들에서의 패스워드들의 손상을 야기할 것이다.

[0008] 패스워드없는 인증은 인증 프로세스의 보안성을 향상시키는데 이용되는 다른 기술이다. 개인과 조직은 스마트 카드 및 인증 토큰과 같이 사용자 ID들과 패스워드들에 의존하지 않는 인증 방법을 채용한다. 스마트 카드는 사용자 인증 목적을 위하여 카드 상에 저장된 복잡한 패스워드를 언로크시키기 위해 내장형 패스워드 - 개인 식별 번호(PIN)-를 이용한다. 세트업(set-up)은 사용자가 패스워드를 입력할 필요를 제거하며, 멀티팩터 인증(multifactor authentication), 물리적 스마트 카드 및 내부에 저장된 PIN을 이용하여 사용자를 인증한다. 그러나, 스마트 카드는 잃어버리거나 도난당하거나 또는 달리 손상된 카드에 대한 헬프 데스크 지원을 유지하기 위한 높은 지속적인 비용들과 시스템을 설정하기 위한 높은 선행 투자 비용과 같은 결함을 갖고 있다.

[0009] 사용자를 인증하기 위해 생체 팩터를 이용하는 것도 또한 인기를 끌고 있다. 일반적인 생체 인증 장치는 망막 스캐너, 지문 스캐너 및 손 스캐너를 포함한다. 이들 장치는 사용자의 물리적 속성으로부터 유도된 데이터에 의해 사용자를 인증한다. 이들 장치의 결함은 이들이 실시 및 유지를 위해 비용이 든다는 것이다.

[0010] 패스워드 동기화는 사용자로 하여금 복수의 시스템에 걸쳐 단일 패스워드를 이용할 수 있게 하는 기술이다. 패스워드 동기화에서, 패스워드는 패스워드 리세트와 패스워드 변경 양쪽 모두에 대하여 단일의 보안 정책에 지배를 받는다. 이 기술에서, 패스워드의 평문(plaintext) 복사본이 하나의 위치로부터 추출되어, 하나 이상의 외부 서비스 위치들에 설치된다. 이를 실현하기 위해, 모든 사용자 마다의 사용자 프로파일의 복사본이 배치 프로젝트(deployment project)의 처음에 모든 시스템에 존재해야 하고 시스템 수명 전반에 걸쳐 유지되어야 한다. 패스워드 동기화에서의 패스워드 변경은 단방향 푸시 또는 양방향 푸시로 발생할 수 있다. 단방향 패스워드 푸시에서, 중앙 시스템에서의 패스워드 변경이 인터셉트되고 네트워크 내의 다른 위치들에 푸시된다. 양방향 패스워드 푸시에서, 패스워드 변경은 임의의 시스템에서 이루어질 수 있으며, 전체 패스워드 아키텍처에 걸쳐 전파된다.

[0011] 단방향 패스워드 푸시에서의 주요 문제가 패스워드들을 저장하는 시스템들의 보안 측정 내에 존재한다. 동기화된 패스워드가 시스템에 걸쳐 이용되기 때문에, 임의의 시스템에서의 보안 침해는 모든 시스템에서의 막심한 보

안 침해를 가져올 것이다. 양방향 패스워드 동기화는 보다 큰 사용자 유연성을 제공하지만, 이는 패스워드 변경의 무한 루프를 생성하는 것과 같이 추가적인 문제를 야기할 수 있다. 시스템은 나머지 시스템에 새로운 데이터를 전파하도록 프로그래밍되기 때문에, 시스템이 단일의 패스워드 상에서 복수의 패스워드 변경들을 전파하는 끝없는 패스워드 업데이트 프로세스에 잡힐 수 있다.

[0012] 따라서, 패스워드 동기화는 네트워크 내의 복수의 패스워드들을 기억하고 관리해야 하는 것으로부터 사용자를 해방시키지만, 패스워드 동기화도 또한 복수의 서비스들을 액세스하기 위해 사용자가 하나의 패스워드를 이용할 수 있게 함으로써 패스워드 보안성을 약화시킨다.

[0013] E-SSO으로서 일반적으로 언급되는 크리덴셜 매핑은 사용자를 대신하여 사용자 ID들과 패스워드들을 저장하고 검색하고 "타이프-입력(type-in)"하는 기술이다. E-SSO를 실시하기 위해, E-SSO 소프트웨어의 복사본이 각각의 WTRU 상에 설치되어야 한다. 모든 시스템과 애플리케이션에 대한 사용자 ID와 패스워드는 로컬 파일, 네트워크 접속 데이터베이스 또는 사용자 디렉토리에 저장된다. 초기 세트업 후, 사용자들은 자신들이 이전에 행했던 대로 또는 새로운 E-SSO 소프트웨어 인터페이스를 통하여 자신들의 워크스테이션 내에 서명(sign)할 수 있다. 사용자들이 자신들의 워크스테이션을 이용하여 애플리케이션에 접속하는 것을 요청할 때, E-SSO 소프트웨어는 애플리케이션들의 로그인 페이지들의 사용자 ID와 패스워드 필드들을 자동으로 상주시킨다(populate).

[0014] E-SSO 시스템에서, 1) 사용자가 자신들의 워크스테이션들이 아닌 E-SSO 소프트웨어에만 로깅할 필요가 있을 때, 및 2) 사용자가 워크스테이션들과 E-SSO 소프트웨어 양쪽 모두에 로깅해야 할 때, 사용자들은 하나 또는 두개의 사용자 크리덴셜 세트(예를 들어, 사용자 ID들과 패스워드들)에 의해 자신들의 워크스테이션 내에 서명한다.

[0015] 일부 E-SSO 시스템들은 워크스테이션 내에 서명하고 스마트 카드, 인증 토큰 또는 생체 샘플들을 포함한 사용자의 크리덴셜 프로파일을 액세스하기 위해 패스워드 외의 다른 인증 기술들의 이용을 지원한다. 또한, 일부 E-SSO 기술들은 각각의 목표 수신지에 대한 패스워드 관리를 완전하게 제어하도록 구성된다. 이 접근 방식은 사용자들이 임의의 목표 시스템에 대한 자신들의 패스워드들을 기억하는 필요성을 제거한다. E-SSO 소프트웨어는 사용자를 대신하여 사용자에 대하여 자동으로 서명한다.

[0016] E-SSO 하에서, 사용자들은 또한 목표 시스템 상에서 패스워드들을 변경할 필요가 없다. 소프트웨어는 패스워드 변경 요청들을 인식 또는 예상하며, 그에 따라 사용자를 대신하여 패스워드를 변경한다. 크리덴셜 매핑 패스워드 관리 특성부들은 목표 시스템들이 크리덴셜 관리 소프트웨어를 통해서만 액세스하는 경우 최상으로 동작한다.

[0017] E-SSO 시스템이 세이프가드 사용자 패스워드에 대한 기능들을 제공하지만, 이 시스템은 세트업을 위해 비용이 들고 번거롭다는 결함을 갖는다. E-SSO 시스템을 구현하는 것은 각각의 사용자에 대한 로그인 ID 프로파일을 생성하는 것 뿐만 아니라 각각의 사용자와 각각의 목표 애플리케이션에 대한 현재 패스워드들을 저장하는 것을 필요로 한다. E-SSO 시스템을 세트업하는 것은 클라이언트 소프트웨어를 설치하고, 사용자 ID들과 패스워드들을 저장하기 위하여 크리덴셜 데이터베이스를 배치하는 것을 추가로 필요로 한다. 데이터베이스는 전용 네트워크 서비스를 통하여, 또는 기존 디렉토리(예를 들어, 활성 디렉토리, LDAP, NDS)의 방식을 확장함으로써 얻어질 수 있다. 크리덴셜 데이터베이스는 데이터베이스 자체의 수개 요건들을 갖는다. 자신의 목적을 수행하기 위해서는, 데이터베이스에서의 장애로 인해 많은 수의 사용자들이 임의의 시스템 내에 서명하는 것이 못하게 되기 때문에, 데이터베이스는 고속이며 이용가능해야 한다. 추가적으로, 데이터베이스에서의 손상이 모든 시스템들에서의 모든 사용자 크리덴셜의 손상을 야기할 수 있기 때문에 데이터베이스가 안전해야 한다.

[0018] 중앙 패스워드 제어 시스템으로서, E-SSO는 SPOF(single point-of-failure; 싱글 포인트 오브)를 도입한다. 사용자는 E-SSO 시스템 또는 크리덴셜 데이터베이스가 다운된 경우 임의의 시스템 내에 로깅할 수 없다. 또한, E-SSO 기술은 복수의 사용자 인터페이스(예를 들어, 클라이언트, 웹, 폰 등)를 지원하는 애플리케이션에 의해 인증 프로세스를 지원하지 않는다. 또한, E-SSO는 윈도우 "스크린 스크랩" 기술에 의존하기 때문에, E-SSO 시스템의 배치 및 관리는 특히 복수의 유형의 워크스테이션에 걸쳐 비용이 많이 들 수 있다. 따라서, E-SSO 시스템은 세트업 및 등록을 위해 지루하고 시간 소모적이며 비용이 많이 들 뿐 만 아니라 SPOF에 민감하다.

[0019] E-SSO와 패스워드 동기화를 결합한 것은 E-SSO 시스템 단독으로 구현하는 단점들 중 일부를 해결할 수 있다. 예를 들어, 패스워드 동기화 기술 없이는, 사용자들은 대안의 사용자 인터페이스를 이용하여 애플리케이션들 내에 로깅하기 위해 자신들의 E-SSO 패스워드들을 이용할 수 없을 것이다. 사용자들이 자기 자신들의 패스워드를 반드시 알 필요가 있는 것은 아니기 때문에, Microsoft Outlook(마이크로소프트 아웃룩)과 같은 독점 클라이언트들을 통상적으로 이용하는 사용자는 웹 포탈들을 통하여 이메일 계정을 액세스할 수 없다. 패스워드 동기화와

E-SSO를 결합함으로써, 사용자들은 웹 포탈들과 같은 대안의 인터페이스들을 통하여 다른 애플리케이션들에 로그인하기 위해 자신들의 1차 E-SSO 패스워드들을 이용할 수 있다. 추가로, E-SSO 시스템을 배치하기 전에 패스워드 동기화 시스템을 배치하는 것은 각각의 사용자에 대한 사용자 ID 프로파일을 획득하는데 있어 시간과 수고를 감소시킨다.

[0020] E-SSO 시스템에서, 사용자 크리덴셜들은 1차 E-SSO 패스워드로부터 유도된 키에 의해 통상적으로 암호화된다. 이러한 구성 하에서 1차 E-SSO 패스워드의 손실은 모든 시스템에 대한 사용자 크리덴셜의 손실을 가져온다. 심지어 손실된 E-SSO 패스워드가 리세트된 후에도, 크리덴셜들이 손실된 패스워드로부터 유도된 키에 의해 암호화되기 때문에 암호화된 크리덴셜들이 액세스불가능하게 된다. 즉, 사용자의 E-SSO 1차 패스워드를 리세트하는 것은 사용자의 크리덴셜들을 검색하지 않으며, 사용자는 E-SSO 시스템에 재등록해야 한다.

[0021] 이러한 문제를 해결하기 위해, E-SSO 시스템은 E-SSO 패스워드 리세트 후에 사용자 크리덴셜들을 복구하기 위해 "백 도어(back door)"를 제공해야 한다. 패스워드 리세트 시스템은 이 백 도어 시스템과 통합해야 하거나 또는 자기 자신의 백 도어를 제공해야 한다. 사용자의 1차 E-SSO 패스워드를 리세트한 후, 패스워드 리세트 시스템은, E-SSO 클라이언트 소프트웨어가 다시 액세스가능하도록, 안전한 스토리지로부터 사용자의 이전의 패스워드를 복구하고 사용자의 구 크리덴셜들을 복호화하고 이들을 새로운 패스워드와 키에 의해 재암호화해야 한다.

[0022] 패스워드 리세트, 패스워드 동기화 및 E-SSO 시스템을 통합하는 것은 이러한 문제를 해결하여 조직이 신속한 배치, 자동화된 사인온 및 셀프서비스 문제 해결의 이점들을 누릴 수 있게 한다. 그러나, 기술들의 결합은 패스워드들과 로그인 크리덴셜들을 안전하게 하는 문제를 해결하지 못한다. 추가로, 클라이언트 또는 서버 소프트웨어 또는 데이터베이스에서의 손상은 사용자 프로파일을 손상시킨다. 마지막으로, 이 결합은 여전히 패스워드 동기화 및 E-SSO에 참여하는 시스템들의 "헬쓰(health)" 상태를 검증하는 방식을 제공하는 것을 실패한다. 이러한 검증이 없이, 사용자가 시스템에 의해 권한을 받으면, 사용자는 시스템이 손상될 때에도, 시스템을 액세스할 수 있다.

[0023] 웹-SSO는 웹 브라우저를 통하여 액세스되는 애플리케이션 및 자원들을 다룬다. 웹-SSO에서, 웹 자원에 대한 액세스는 목표의 웹 서버 상의 구성요소 또는 웹 프록시 서버에 의해 인터셉트되며, 웹 자원을 액세스하는 것을 시도하는 인증되지 않은 사용자는 인증 프롬프트로 전환되어, 성공적인 사인온 후에만 원래 사이트에 재연결(redirect)된다. 사용자의 인증 상태를 추적하기 위해 쿠키들이 가장 종종 이용되며, 웹-SSO 인프라스트럭쳐는 쿠키들로부터 사용자 식별 정보를 추출하고 이것을 웹 자원 상에 전달한다.

[0024] 스크린 스크랩과 연계(federation)는 웹-SSO에 이용된 2개의 가장 중요한 종래 기술의 기술들이다. 스크린 스크랩의 일반 유형은 웹 스크랩이다. HTML 스크랩 또는 페이지 스크랩이라 또한 불리는 웹 스크랩은 컴퓨터 프로그램, 웹 스크랩퍼가 웹 페이지로부터 데이터를 추출하는 기술이다. 웹 스크랩은 E-SSO 또는 웹-SSO에 이용될 수 있다.

[0025] 스크린 스크랩 기술들은 웹 페이지가, 종종 텍스트 형태로 정보를 포함하는 텍스트 기반 마크업 언어(예를 들어, HTML)를 이용하여 구축되기 때문에 유용하다. 이와 대조적으로, 프로그램들 간의 데이터 교환은 인간에 의해 쉽게 이해할 수 없는 머신용으로 설계된 데이터 구조를 이용하여 통상 실현된다. 이와 유사하게, 사용자에 대해 의도된 데이터 출력은 종종 머신 해석에 적합하지 않다. 따라서, 스크린 스크랩은, 첫번째로 HTML과 다른 마크업 머신 언어들로부터 머신 친화적인 데이터(machine-friendly data)를 추출한 다음, 추출된 머신 친화적인 데이터를 프로그램들 사이에서 교환함으로써 프로그램들 사이에서의 데이터의 전달을 실현하는 것을 필요로 한다.

[0026] 스크린 스크랩을 수행하는 경우, 컴퓨터 텍스트 디스플레이로부터 데이터를 판독하는 것은 단말의 보조 포트를 통하여 단말의 메모리를 판독하거나 또는 단말의 출력 포트와 다른 시스템의 입력 포트를 접속시킴으로써 일반적으로 행해진다. 이들 경우에, 스크린 스크랩은 또한 웹 페이지들의 컴퓨터화된 구문 분석이라 부를 수 있다.

[0027] 스크린 스크랩은 1) 현재의 하드웨어와 호환가능한 대안의 메카니즘을 제공할 수 없는 레가시 시스템을 인터페이싱하거나, 또는 2) 덜 정교한 애플리케이션 프로그램 인터페이스(API)를 제공하는 제3자 시스템을 인터페이싱하기 위해 가장 종종 행해진다. 후자의 경우에, 제3자 시스템은 증가된 시스템 부하, 광고 수익의 손실, 또는 정보 컨텐츠의 제어 손실과 같은 이유로 스크린 스크랩을 원치않는 것으로서 간주할 수 있다.

[0028] 도 1은 웹 스크랩과 함께 웹-SSO를 이용하는 종래 기술의 WTRU에서의 예시적인 절차를 나타낸다. 이 도면에서, WTRU에는 프록시 소프트웨어가 설치되고, 프록시가 웹 서비스 내에 SSO들을 위한 절차를 설정하고 제어할 수 있

도록 WTRU 상의 웹 액세스 애플리케이션이 SSO 프록시 소프트웨어와 협력하여 상호작용하는 것으로 추정된다. 예를 들어, 브라우저가 URL을 액세스하라는 요청을 수신하는 경우, 브라우저는 웹-SSO가 특정 웹사이트를 액세스하는데 이용될 수 있는지를 검증하기 위해 SSO 프록시 소프트웨어에 URL을 전송한다.

[0029] 연계는 표준 기반 프로토콜을 이용하여 한 애플리케이션이 사용자의 아이덴티티를 제2 엔티티에 표명할 수 있도록 함으로써 이에 의해 리더던트 인증에 대한 필요성을 제거할 수 있게 하는 웹-SSO에 이용된 두 번째로 임포트 기술이다. 연계를 지원하는 사양 표준은 리버티 얼라이언스 ID-FF(Liberty Alliance ID-FF), OASIS, SAML 및 Shibboleth(인터넷2를 위해 개발되고 있음)를 포함한다. 리버티 얼라이언스는 아이덴티티 연계 프레임워크(ID-FF)와 아이덴티티 웹 서비스 프레임워크(ID-WSF)에 대한 사양을 개발하고 있는 중앙 조직이다. 리버티 얼라이언스는 연계된 아이덴티티 관리 및 웹 서비스 통신 프로토콜을 정의하는 사양들을 포함한 한 세트의 브로드 기반 산업 컨소시엄 개발 스위트(broad-based industry consortium developing suite)를 제공한다. 이 프로토콜은 인트라엔터프라이즈와 인터엔터프라이즈 배치 양쪽 모두를 위해 설계된다.

[0030] OASIS는 e-비지니스에 대한 솔루션을 개발하는 비영리 조직이다. 현재 버전 2.0인 SAML은 SSO 인증을 가능하게 하는 사용자 식별 정보를 포함한 보안 표명을 위한 마크업 언어이다. Shibboleth는 연계된 아이덴티티와 SAML에 기초하여 인증 및 인가 인프라스트럭쳐에 대한 아키텍쳐 및 오픈소스 구현을 형성한 인터넷2 미들웨어 이니시에이티브(NMI) 프로젝트이다.

[0031] 도 2는 리버티 얼라이언스 ID-FF를 이용한 WTRU 사용자에 의한 웹-SSO에 대한 절차들을 나타낸다. 웹-SSO의 환경에서, 리버티 얼라이언스는 사용자가 단일의 계정 내에 로깅하도록 하고, 네트워크에서의 ID 관리 엔티티에 의해 관리되는 "circle of trust(트러스트 서클)" 내에서의 수개의 서비스 공급자들로부터 서비스들을 요청하도록 한다. 리버티 얼라이언스의 구별되는 특징은 "연계" 프로세스이다. 각각의 사용자가 진행중인 재인증(undergoing re-authentication) 없이 서비스 공급자(SP)를 액세스하기 위해 어떤 종류의 권한을 갖는지를 결정하는 대신에, 리버티 얼라이언스는 사용자들이 재인증 없이 SP를 액세스하기를 원하는지를 사용자들이 결정할 수 있게 한다. 이러한 권한을 얻기 위하여, 사용자는 첫 번째로 SP에 의해 인식된 아이덴티티 공급자(IDP)에 의해 인증받아야 한다. 이것은 확장된 엔터프라이즈 애플리케이션의 환경에서 아이덴티티 관리를 위한 실제적인 프레임워크를_리버티 얼라이언스에 만들며, 여기서, 사용자들은 엔터프라이즈에 대한 개인 데이터의 관리를 통상적으로 신뢰한다.

[0032] SAML은 보안 도메인들 사이에서, 즉, IDP와 SP 사이에서 인증 및 인가 데이터를 교환하기 위하여 OASIS 조직에 의해 형성된 XML 표준이다. 도 3은 SAML 구성요소들 간의 관계들을 나타낸다. SAML은 네트워크 엔티티들 사이에서 인증 절차와 보안 표명 정보의 끊김없고 신뢰성있는 교환을 용이하게 함으로써 웹-SSO 문제를 해결하려 시도한다. SAML 표준은 다음의 구성요소들을 이용하는데, 이 구성요소는 1) 표명 구성요소(assertions component); 2) 프로토콜 구성요소(protocols component); 3) 바인딩 구성요소(bindings component); 및 4) 프로파일 구성요소(profiles component)이다. 표명 구성요소는 하나의 엔티티가 사용자 이름, 지위, 이메일 주소, 그룹에서의 멤버십 등과 같은 다른 엔티티의 특징들 및 속성들을 표명할 수 있게 한다. 프로토콜 구성요소는 XML 스키마로 인코딩되며, 요청 응답 관련 프로토콜의 리스트들을 정의한다.

[0033] 바인딩 성분은 SAML 프로토콜 메시지들이 SOAP 메시지들 내에서 어떻게 전달되고 SOAP 메시지들이 HTTP를 통하여 어떻게 전달되는지를 정의한다. SOAP 메시지들은 W3C 조직 SOAP 버전 1.2 엔벨로프(envelope) 및 인코딩 규칙에 따라 구성된 잘 형성된 XML 메시지들이다. 도 4는 통상의 바인딩 경우에 SAML 구성요소들 사이에서의 교환의 일례를 나타낸다. 프로파일 구성요소는 SAML 사양의 핵심으로, 이것은 SAML 요청들 및 응답들이 어떻게 전달되는지를 정의한다.

[0034] 리버티 ID-FF와 SAML 양쪽 모두가 패스워드 보안 레벨들을 강화하는데 중요한 역할을 하고 있지만, 사용자 장치 내에서 또는 IDP와 SP 상에서 웹-SSO를 위해 필요한 민감한 정보를 어떻게 안전하게 하는지에 대해서는 어느 것도 해결하지 못한다. 또한, 리버티 ID-FF와 SAML 양쪽 모두가 IDP들과 SP들에 대한 사용자 인증 프로세스의 제어를 궁극적으로 포기하고 이에 의해 사용자의 개인 정보의 공개를 필요로 하기 때문에, 사용자 프로파일이 프로세스에서 손상될 수 있다.

[0035] 트러스티드 컴퓨팅 기술들이 TCG(Trusted Computing Group; 트러스티드 컴퓨팅 그룹)의 기술적 보호(umbrella) 하에서 대부분 문헌 및 제품에 나타난다. 트러스티드 컴퓨팅은 암호 기능과 보호된 저장을 제공하는 전용이고 물리적으로 분리된 하드웨어 모듈의 물리적 보안에 기초한다.

[0036] TCG는 컴퓨팅 엔티티들이 시스템들의 무결성을 표명하고 적합한 신뢰 레벨이 성립된 경우 인증 프로세스를 검증

하며 이러한 목표 장치들의 표명된 신뢰 레벨들에 기초하여 다른 장치들과의 정보와 처리의 교환시 평가와 결정을 수행하는 방법들을 제공하는 여러 기술들을 개발하였다.

[0037] TCG는 트러스티드 플랫폼 모듈(TPM)이라 부르는 코어 플랫폼 모듈을 정의한다. 도 5는 TPM의 구성을 나타내며 이 구성은 TPM 모듈과 그 인터페이스의 물리적 보호를 제공한다. 이 모듈은 또한 휘발성 및 비휘발성 메모리 공간에 대한 보호와, 암호화 및 디지털 서명을 수행하는 암호 기능들을 제공한다. TPM은 공개 키 인프라스트럭처(PKI)에 기초하여 HASH 확장 및 사용자 장치 고유 및 안전 EK(endorsement key)에 의해, 플랫폼과 플랫폼의 소프트웨어 구성요소의 "상태"를 포착하는데 플랫폼 구성 레지스터(PCR)를 이용한다. EK는 외부에 결코 노출되지 않지만, 그 에일리어스인 입증 아이덴티티 키(AIK)가 플랫폼의 무결성 값을 검증하는데 이용된다. 또한, TPM은 메모리에서 AIK들에 의해 서명된 PCR 값들과 결합하여 데이터를 "봉인"하는 프로세스를 이용하며, 이에 의해 TPM으로부터 그리고 봉인된 메모리로부터의 매칭하는 PCR 값들에 의해 측정되고 검증된 플랫폼 또는 소프트웨어 무결성이 검증될 때에만 데이터가 액세스되거나 또는 추출될 수 있다.

[0038] 도 6은 외부의 엔티티(챌린저 또는 검증자(verifier))가 TPM, AIK들 및 PCA(private certification authority)를 이용하여 플랫폼 입증에 대한 요청을 어떻게 행할 수 있는지를 나타낸다. 이러한 입증 메카니즘은 SSO 기술들의 신뢰성 및 보안 형태를 향상시키는데 유용할 수 있다.

[0039] TCG는 또한 TPM을 포함한 컴퓨팅 플랫폼에 의한 이용을 위하여 상세화된 TPM 소프트웨어 스택(TSS)을 특정하였다. 각각의 TSS 모듈은 특수화된 기능을 제공하는 구성요소들을 포함한다. 이들 구성요소의 1차 설계 목표는 애플리케이션들로부터의 적합한 바이트 순서화(order) 및 정렬에 의해 구축한 코맨드 스트림을 감추고 TPM 자원을 관리하도록, 단일의 동기화된 진입 포인트(single, synchronized entry point into)를 TPM에 제공하는 것이다.

[0040] 도 7은 TPM 및 TSS 계층들의 아키텍처를 나타낸다. TSS 모듈은 다음의 구성요소들, 1) 표준화된 TPM 장치 드라이버 라이브러리(TDDL)에 인터페이싱하는 TSS 장치 드라이버 라이브러리 인터페이스(TDDLI); 2) TPM의 TCS 커맨드들(도시 생략)에 인터페이싱하는 TSS 코어 서비스 인터페이스(TCSI); 및 3) TCG의 TSP 커맨드들(도시 생략)와 인터페이싱하고 애플리케이션 바로 아래에 위치하는 TCG 서비스 공급자 인터페이스(TSPI)를 포함한다. TPM 측에서는, TDDL가 TPM과 통신하는 벤더 특정 TPM 장치 드라이버의 상단에 위치한다.

[0041] TDDLI는 TSS의 서로 다른 구현이 임의의 TPM과 적절하게 통신하고, TPM 애플리케이션들에 OS-독립 인터페이스를 제공하며, TPM 벤더로 하여금 사용자 모드 구성요소로서 소프트웨어 TPM 시뮬레이터를 제공할 수 있게 하는 것을 보장한다. TDDL은 플랫폼 상에서 사용자 모드와 커넬 모드 사이에 트랜지션을 제공한다. TCG 코어 서비스들(TCS)은 공통 세트의 플랫폼 서비스들에 인터페이스를 제공한다. TCS는 다음의 4개의 코어 서비스를 제공하는데, 이는 1) TPM에 대한 스레디드 액세스를 실시하는 콘텍스트 관리; 2) 플랫폼과 연관된 크리덴셜과 키들을 저장하는 크리덴셜 및 키 관리; 3) 연관된 PCR들에 대한 이벤트 로그 입력 및 액세스를 관리하는 측정 이벤트 관리; 및 4) TPM 코맨드들을 시리얼화하고 동기시키고 처리하는 파라미터 블록 생성이다.

[0042] TCG 서비스 공급자(TSP)는 객체 지향 아키텍처에 기초한 TPM에 대한 C 인터페이스이다. TSP는 애플리케이션과 동일한 프로세스 어드레스 위치 내에 상주한다. 이 계층에서 인가는 이 계층에 코딩된 사용자 인터페이스의 이용을 통해 또는 TCS 계층에서의 콜백 메카니즘을 통해 발생한다. 말단 사용자들에 대한 표준화된 인가 인터페이스를 제공하기 위하여, 인증 서비스들은 로컬 애플리케이션에 의해서가 아니라 오히려 플랫폼에 의해 제공된다.

[0043] TSP는 2개의 서비스, 1) 콘텍스트 관리; 및 2) 암호화를 제공한다. 콘텍스트 매니저는 애플리케이션과 TSP 자원의 효과적인 이용을 가능하게 동적 핸들들을 제공한다. 각각의 핸들은 한 세트의 상호관련된 TCG 동작들에 대한 컨텍스트를 제공한다. 애플리케이션 내의 서로 다른 스레드들은 동일한 콘텍스트를 공유할 수 있거나 또는 별도의 콘텍스트를 획득할 수 있다.

[0044] TPM 보호 기능들의 전체 이용을 행하기 위해, 암호화 기능들을 지원하는 것이 제공되어야 한다. TSP는 TPM 사양에 의해 요구된 동작들을 수행하는데 필요한 것을 제외하고는 이러한 지원을 제공하지 않는다. 특히, 벌크 데이터 암호화는 인터페이스에 의해 노출되지 않는다. TPM 특정 암호화 기능들의 예들은 (1024 바이트 미만인) 작은 양의 데이터의 암호화와 메시지 다이제스팅을 포함한다.

발명의 상세한 설명

[0045] 트러스티드 컴퓨팅 기술에 기초한 패스워드 관리 및 SSO 액세스를 위한 방법 및 장치가 개시되어 있다. 이 방법은 패스워드들과 SSO 크리덴셜들을 발생, 저장 및 검색하기 위해 안전하고 신뢰성있는 메카니즘을 제공하도록, 프록시 SSO 유닛과 웹 액세스 애플리케이션 양쪽 모두와 상호작용하는 TCG의 TPM을 구현한다. 여러 실시예들이

사용자로 하여금 사용자의 장치 상에 상주하는 안전한 프록시에 단지 한번 서명한 후에 미리 식별된 사이트 그룹에 속하는 한 사이트에서 다른 사이트로 안전하고 투과적으로 호핑할 수 있게 한다.

[0046] 사용자가 모바일 장치 상에 서명한 후, 장치 상에 상주하는 프록시 SSO 유닛은 등록된 그룹에 속하는 안전한 사이트들을 액세스하는 것을 시도하는 애플리케이션들을 인터셉트하며, 그룹 내의 개개의 사이트들에 사인온하도록 TPM에 의해 발생되어 보호 유지되는 사이트별 보안 패스워드를 이용한다. 하드웨어 또는 소프트웨어에서 구현될 수 있는 프록시 SSO 유닛은 자신의 무결성을 위하여 TPM에 의해 또한 보호받는다. 이는 사용자가 개별적으로 기억하거나 또는 저장할 필요가 없는 TPM-발생 랜덤화된 패스워드를 통하여, 다른 사이트들에 대해 SSO를 이용하는 프로세스에 높은 레벨의 신뢰도를 제공한다.

[0047] SSO 특성은 임의의 수의 안전 사이트들에 적용될 수 있고, 사용자가 인터넷을 통해 네비게이트하고 새로운 웹 서버들을 액세스함에 따라 리스트가 커질 수 있다. 각각의 웹 서버는 초기에 웹 서버 상의 등록에서부터 후속하는 로그온 및 인증 세션들까지 SSO 절차의 자율 동작을 실행하는 TCG 발생 사용자 크리덴셜과 연관된 안전한 사인온 인증서와 서버 자신을 연관시킨다. 선택으로서, 사용자는 SSO 웹 액세스가 실행될 웹 사이트 그룹의 프록시 소프트웨어에 의해 프롬프트를 제공받을 수 있다. 사용자는 프록시 소프트웨어에 의해 표시되는 웹사이트들의 그룹에 대해 또는 서브세트에 대해 SSO 동작을 허용할 것인지를 선택할 수 있다.

[0048] 추가적인 실시예들은 연계된 아이덴티티 관리와 함께 E-SSO와 웹-SSO의 TPM 증대를 위한 메카니즘들을 포함한다.

실 시 예

[0063] 이하 언급될 때, 용어, "무선 송수신 유닛(WTRU)"은 이들로 한정되는 것은 아니지만, 사용자 기기(UE), 이동국, 고정 또는 이동 가입자 유닛, 페이저, 셀룰라 전화기, 개인 휴대 정보 단말기(PDA), 컴퓨터 또는 무선 환경 또는 무선/유선 조합의 환경에서 동작가능한 임의의 다른 유형의 사용자 장치를 포함한다. 이하에 언급될 때, 용어, "기지국"은 이들로 한정되는 것은 아니지만, 노드-B, 사이트 컨트롤러, 액세스 포인트(AP) 또는 무선 환경에서 동작가능한 임의의 다른 유형의 인터페이싱 장치를 포함한다.

[0064] 도 8은 적어도 하나의 WTRU(805)와 무선 액세스 네트워크(RAN; 807)를 포함한무선 통신 시스템(800)의 예시적인 블록도이다. WTRU(805)는 사용자(809)와 상호작용하고 싱글 자동 사인온(SASO) 프록시 유닛(810), TPM/TSS(815), 웹 액세스 애플리케이션(WAA)(820)을 포함한다. TPM/TSS(815)는 SASO 프록시 유닛(810) 및 WAA(820) 양쪽 모두와 상호작용하여, 패스워드들과 SSO 크리덴셜들을 생성, 저장 및 검색하기 위해 안전하고 신뢰성있는 메카니즘을 제공한다. SASO 프록시 유닛(810)은 자신의 무결성을 위하여 TPM/TSS(815)에 의해 보호받으며, 따라서, 다른 웹사이트에 대한 SSO을 이용하면서 높은 레벨의 신뢰도를 부여한다. TPM/TSS(815)은 사용자가 개별적으로 기억할 필요가 없는 랜덤화된 패스워드들을 저장 및 발생시킴으로써 높은 레벨의 신뢰도를 제공한다. RAN(807)은 적어도 하나의 웹사이트(830a-c)에 대한 액세스를 통상적으로 포함한다. 선택적으로, RAN(807)은 장치 트러스트 미러(DTM; 835)를 또한 포함할 수 있다.

[0065] 사용자(809)가 기억해야 하는 패스워드의 수를 최소화하기 위하여, 메카니즘이 제공되며, 이에 의해, 사용자(809)는 첫 번째로 사이트 또는 애플리케이션의 리스트를 생성한 다음, SASO 프록시 유닛(810)이 자기 자신의 로그와, 저장 키 바인딩을 이용하여 또는 내부 저장에 의해 TPM/TSS(815)에 의해 안전하게 이후 유지되는 로그 양쪽 모두에 대한 정보를 기록한다. SASO 프록시 유닛(810)은 애플리케이션 또는 웹 사이트(830)에 대한 액세스의 사용자 요청과, 애플리케이션 또는 웹 사이트(830)으로부터의 로그인 및/또는 패스워드 타이프 입력에 대한 프롬프트 양쪽 모두를 인터셉트하도록 웹 스크랩하는 것과 같은 인터셉트 기술 또는 공동 바인딩을 이용한다.

[0066] 사용자(809)의 크리덴셜(또한 루트 아이덴티티라고도 함)은 TPM/TSS(815) 자체에 안전하게 저장될 수 있거나 또는 USIM과 같은 다른 안전한 저장 장치에 안전하게 저장될 수 있다. 추가적으로, 키 계층 구성(hierarchy)이 이 루트 아이덴티티로부터 생성될 수 있다. 루트 아이덴티티는 장치 내에 안전하게 유지되며, 안전하거나 또는 신뢰성있는 도메인의 외부로 절대 누설되지 않는다.

[0067] 사용자(809)가 안전한 웹 사이트(830)에 처음으로 사인온하면 WAA(820)는 SASO 프록시 유닛(810) 및 TPM/TSS(815)와 상호작용하여, 웹 사이트(830)에 대한 인증서 정보와 연관된 높은 엔트로피의 패스워드와 높은 엔트로피의 고유 사용자 ID를 생성한다. 이 후, 사용자(809)가 웹 사이트(830)에 액세스하기를 원할 때마다, 사용자의 크리덴셜들은 WAA(820), SASO 프록시 유닛(810) 및 TPM/TSS(815) 사이에 상호작용을 통하여 통신 링크를 통해 전송된 정보 내에 자동으로 입력된다.

[0068] 선택적으로, 사용자(809)가 RAN(807)를 액세스할 때마다 WTRU(805)는 서비스 공급자(SP) 또는 아이덴티티 공급자(IDP)(도시 생략)와 같은 RAN(807)에서의 관련 네트워크 요소들과의 신뢰 관계를 성립시키는 것과 동일한 방식으로 SASO 프록시 유닛(810)과 TPM/TSS(815)를 이용한다. 다른 방법으로, RAN(807)은 DTM(835)과 같은 신뢰성있는 제3자 엔티티에 대한 특수 시스템 구성요소 또는 관계를 유지시킨다. WTRU(805)가 RAN(807)과의 성립된 신뢰 관계와 보안 링크를 갖고 있다면, DTM(835)은 모바일의 트러스트 서비스에 대한 프록시로서, 그리고 각각의 안전한 웹 사이트에 대하여 생성된 패스워드들에 대한 데이터베이스로서 기능한다.

[0069] 사용자(809)는 WTRU 로크 메카니즘을 액세스하기 위해 싱글 로그인 ID와 패스워드를 이용함으로써 WTRU(805) 기능 및 따라서 인터넷에 대한 액세스를 얻을 수 있다. 일단 로그인되면, 다른 모든 서비스들이 WTRU(805)에 의해 투과적으로 처리된다. 추가적으로, 키 포브(fob)들, 스마트 카드들 및/또는 생체 부분(biometric)이 폰 특성부를 액세스하기 위해 안전한 2 또는 3개 팩터의 인증을 제공하는데 이용될 수 있다. 선택적으로, 인증 크리덴셜들이 인증을 위하여 그리고 사용자가 장치를 액세스하도록 하기 위하여 RAN(807)에 전송될 수 있다.

[0070] TPM/TSS(815)는 물리적으로 보호된 바운더리를 제공함으로써 TPM/TSS가 암호적으로 보호하고 저장하는 데이터 - 패스워드를 포함함 - 에 대한 고유 보안성을 제공한다. 그러나, 데이터 보호의 강도는 또한 이러한 데이터를 보호하는데 이용된 패스워드들 또는 암호 키들의 경우에 데이터 자체의 강도와 선도(freshness)에 부분적으로 의존한다. 침입자의 처리시 암호화된 데이터의 충분한 샘플들과 충분한 컴퓨팅 능력 및 시간이 제공되면, 매우 강력하게 보호된 데이터도 파괴될 수 있다. 따라서, 키를 업데이트하고 필요에 따라 새로운 키로 데이터를 재암호화하는 것은 암호화된 아이덴티티와 인증 데이터를 복호화하려는 도용자의 시도에 대해 추가의 보안 장벽을 제공할 수 있다. 범용 인증에 이용된 키들과 패스워드들은 TPM/TSS(815)에 의해 자주 업데이트되어야 한다. 이러한 업데이트는 어느 프로토콜이 데이터 및/또는 키 업데이트들에 관련된 필요한 절차를 개시하고 확인응답하고 실행할지를 필요로 한다.

[0071] 대안의 실시예에서, WTRU(805)는 자신의 내부에 유니버셜 가입자 식별 모듈(USIM)(도시 생략)을 갖고 있다. 분리되고 보호된 엔티티로서 USIM은 패스워드들과 같은 데이터에 대한 안전한 저장 위치 뿐만 아니라 소프트웨어에 대한 제2 안전 실행 환경을 제공한다. 따라서, SASO 프록시 유닛(810)은 USIM에 상주할 수 있다. WAA(820)는 또한 USIM에 상주할 수 있다.

[0072] WTRU(805)의 다른 대안의 실시예에서, USIM은 단독의 "안전한" 실행 환경으로서 TPM/TSS(815)를 대체할 수 있다. 이 경우, WTRU(815)는 플랫폼 및/또는 애플리케이션 무결성 측정, 검증을 실행하는 기능과, TPM/TSS(815)에 의해 통상적으로 제공되는 입증 기능을 갖지 않을 수 있다. 그러나, USIM은 분리되고, 보호되고 안전한 실행 환경이기 때문에, 이는 SASO 프록시 유닛(810) 및 심지어 가능하다면 WAA(820)의 안전한 실행을 가능하게 한다. USIM은 높은 엔트로피의 사이트 고유 패스워드들을 발생 및 저장하도록 그리고 또한 SSO 패스워드 및 SSO 크리덴셜들을 저장하도록 구성될 수 있다.

[0073] WTRU(805)의 또 다른 대안의 실시예에서, 2007년 5월 8일에 출원된 미국 특허 출원 번호 제11/745,697호(여기에서 전체적으로 설명된 것처럼 참조로서 포함함)에 개시된 바와 같은 "확장된" USIM은 WTRU(805)에 상주하며, SASO 프록시(810)와, WAA(820)와 TPM/TSS(815) 모두에 대해 안전한 실행 환경을 제공한다.

[0074] 도 9는 대안의 실시예에 따라 도 8의 시스템(800)의 구성요소들 간에 시그널링을 나타낸다. 구체적으로, 도 9는 TPM/TSS(815)를 이용한 웹 액세스를 위한 SASO에 대한 예시적인 절차를 나타낸다.

[0075] 이 절차는 단계 1005에서, 사용자(809)가 안전한 1개의 팩터, 또는 바람직하게는 2개 또는 3개의 팩터의 인증을 통하여 WTRU(805)에의 액세스를 얻을 때 개시된다. 이들 인증 팩터는 SASO 프록시 유닛(810)으로 하여금 TPM/TSS(815) 내에 유지된 보안 정보를 액세스하도록 하는 메카니즘이다. 생체 2차 또는 3차 팩터 인증이 이용되는 경우, 단계 910에서 SASO 프록시 유닛(810)은 인증을 위해 생체 인증 데이터를 검색하라는 요청을 TPM/TSS(815)에 전송한다. 단계 915에서 TPM(815)은 SASO 프록시 유닛(810)에 생체 인증 데이터를 제공한다. 그 후, 단계 920에서 사용자(809)는 안전한 웹 사이트에의 등록하라는 요청을 WAA(820)에 전송한다.

[0076] 단계 925에서 WAA(820)는 사용자(809)가 웹 사이트 A(830a)를 접속하기를 원하고 있음을 웹 사이트 A(830a)에 전달한다. 단계 930에서 WAA(820)는 웹 사이트 A(830a)의 로그인이 프롬프트함을 수신 및 표시하거나 또는 달리 나타낸다. 단계 935에서 SASO 프록시 유닛(810)은 웹스크랩에 의해 또는 API 또는 다른 구문 분석 기술을 통한 협력에 의해 WAA(820)로부터의 웹 사이트 A(830a)의 인증 프롬프트를 인터셉트한다. 단계 940에서 SASO 프록시 유닛(810)은 사용자 ID 정보(이 정보는 멀티팩터 인증으로부터의 장치 로그인 정보일 수 있음)를 TPM/TSS(815)에 전달한다. 단계 945에서 웹사이트 고유 보안 패스워드가 TPM/TSS(815)에 의해 발생되어 (TPM NV 메모리에 직

접 또는 통상의 메모리이지만 TPM-보호 바인딩 저장 키에 의해 암호화되어) 안전하게 저장된다. 그 후, 단계 950에서, SASO 프록시 유닛(810)은 WAA(820)를 인터셉트하고, 스크랩 또는 API의 이용 또는 다른 구문 분석 기술과 같은 방법들에 의해 웹 사이트 A(830a)에 대한 WAA(820)의 패스워드 프롬프트에 대해 웹사이트 고유 보안 패스워드를 채워넣는다. WAA(820)는 단계 955에서, 웹사이트 고유 패스워드를 웹 사이트 A(830a)에 전달한다. 웹 사이트 A(830a)는 단계 960에서 웹사이트 고유 패스워드를 등록하고 액세스 허가를 WAA(820)에 전송한다. 일단 등록이 성립되었다면, URL, 디지털 인증서, 사용자 ID 및 패스워드 등과 같은 웹사이트 정보가 TPM/TSS(815) 바인딩 저장 키에 의해 보호된 데이터 블랍(blob)과 TPM/TSS(815)에서의 데이터베이스 기록으로서 공동으로 안전하게 저장된다. 웹사이트 고유 패스워드는 각각의 사이트에 대한 이후의 로그인을 위하여 SASO 프록시 유닛(810)에 의해 재이용될 수 있다. 단계 965에서 웹사이트 A(830a)는 WAA(820)에의 액세스를 승인하고, WAA는 등록 오케이(Okay) 및 액세스 허가 메시지를 SASO 프록시 유닛(810)에 전송한다. 단계 970에서, 통상의 웹기초 통신이 후속할 수 있다.

[0077] 도 9에서의 단계 905 내지 단계 965는 WTRU(805)에 의해 웹사이트에서 관리되는, 사용자의 사이트 고유 패스워드의 초기 등록에 대하여 나타낸 것임을 주목해야 한다. 이러한 초기 등록 이후, 사용자(809)는 (단계 920에서와 유사하게) 웹사이트 A(830a)에의 액세스를 요청하기 위해 WAA(820)를 이용할 수 있다. 그 후, SASO 프록시 유닛(810)은 (단계 935에서와 유사하게) WAA(820)로부터의 로그인 프롬프트를 인터셉트하여 (단계 945에서와 유사하게) TPM/TSS(815)에 저장된 사이트 고유 패스워드를 획득하고, (단계 950에서와 유사하게) 스크랩, API들 또는 구문분석에 의해 WAA(820) 상에서 웹사이트 A(830a)에 대해 특정된 로그인 정보를 채워넣는다. 그 후, WAA(820)는 (단계 955에서와 유사하게) 사이트 고유 로그인 정보를 웹 사이트 A(830a)에 전송하고 웹사이트 A(830a)는 제공된 사이트 고유 로그인 정보를 검증한 후 (단계 960에서와 유사하게) WAA(820)에 요청된 서비스에 대한 액세스를 승인하고, SASO 프록시 유닛(810)은 WAA(820)로부터 이 액세스 허가 메시지를 구한 다음 서비스가 승인되었음을 사용자(809)에게 알릴 수 있다. (단계 970에서와 유사하게) 통상의 웹기반 통신이 후속할 수 있다.

[0078] 패스워드가 TPM(815) 내에 유지되어 있는 이미 성립된 웹사이트를 액세스할 경우, 유사한 세트의 절차가 실행된다. 예를 들어, 단계 975에서, SASO 프록시 유닛(810)에 의해 다른 사이트들에 대하여, 예를 들어, 웹사이트 B(830b)와 같은 다른 웹사이트들에 대하여 단계 905 내지 단계 970에서의 단계들을 반복할 수 있다. TPM/TSS(815)에 의해 실행된 코드 무결성 검증 절차는 안전한 거래들이 발생하는 것을 보장하기 위한 다른 소프트웨어 구성요소들과 SASO 프록시 유닛(810)의 무결성을 보호하는데 이용된다. 예를 들어, 패스워드 업데이트 절차를 관리하도록 정책 또는 프로파일이 성립되면, TPM/TSS(815)는 또한 TPM 바인딩 저장 키에 의해 보호되는 메모리에 정책 및 프로파일 정보를 저장함으로써 정책 및 프로파일 정보를 보호한다. 사용자(809)가 웹이 아닌 제3자 서비스 또는 안전한 서버를 액세스하려 시도할 경우, DTM(835)에 의해 관리될 수 있는 트러스트 미러링 절차를 이용하는 것에 의해 상술한 것과 매우 유사한 절차가 이용될 수 있다.

[0079] 도 10은 다른 실시예에 따라 도 8에 도시된 구성요소들 간에 시그널링을 나타낸다. 구체적으로, 도 10은 WTRU(805)에서 그리고 이후 DTM(835)에서의 사용자 인증 정보의 등록을 위해 TPM/TSS(815)와 DTM(835)을 이용하여 웹 액세스하기 위한 SASO에 대한 예시적인 절차(1000)를 나타낸다. RAN(807)에 통상적으로 상주하지만 RAN의 외부에도 위치될 수 있는 DTM(835)은 WTRU(805)의 신뢰성있는 서비스를 '미러링'하는 서비스를 제공하고 이 정보의 외부 요청자들에 대해 이를 입증할 수 있다. 예를 들어, DTM(835)은 도 9에서의 TPM/TSS(815)에 대하여 설명된 바와 같이, 아이덴티티 정보를 관리하는 작업을 운영할 수 있다.

[0080] 사용자(809)는 단계 1005에서 SASO 프록시 유닛(810)에 자신들의 인증 정보를 등록함으로서 절차(1000)를 개시한다. 이러한 등록은 한개의 안전한 팩터 또는 바람직하게는 2개의 팩터의 인증을 이용하여 발생할 수 있다. 추가로, 제3 팩터가 TPM/TSS(815)에 의해 안전하게 유지된 생체 정보를 통한 것일 수 있다. 또한, 단계 1005에서, 또는 별도의 단계에서, 사용자(809)는 원하는 서비스의 리스트를 선택적으로 제공할 수 있다.

[0081] 그 후, 단계 1010에서, SASO 프록시 유닛(810)은 인증 데이터와 원하는 서비스의 리스트를 TPM/TSS(815)에 전송한다. 단계 1015에서, TPM/TSS(815)는 SASO 프록시 유닛(810)과 WAA(820)의 무결성에 대해 인증 데이터와 원하는 서비스의 리스트를 봉인한다. 단계 1020에서, SASO 프록시 유닛(810)은 인증 데이터 및 애플리케이션과 서비스의 원하는 리스트와 함께 WTRU(805)에 대한 무결성 정보(또는 등가적으로 입증 정보)를 DTM(835)에 전송한다.

[0082] 단계 1025에서 DTM(835)은 사용자의 인증 크리덴셜을 웹사이트 A(830a)에 등록한다. 이 처리 동안에, DTM(835)과 웹 사이트 A(830a)는 웹사이트 A(830a)로부터 서비스를 획득하는데 특히 이용되는 패스워드를 사용자(809)와 WTRU(805)에 대하여 상호간에 성립시킨다. 단계 1030에서 DTM(835)은 웹 사이트 A(830a)에의 등록이 완료됨을

나타내는 메시지를 SASO 프록시 유닛(810)에 전송한다. 단계 1035에서, SASO 프록시 유닛(810)은 등록이 완료됨을 사용자(809)에 표시한다.

[0083] 등록이 완료된 후, 사용자는 신뢰성있는 DTM 유닛(835)을 이용하여 중개되는 SASO 프로세스(단계 1040 내지 단계 1095)에서 웹사이트 A(830a)를 액세스할 수 있다. 단계 1040에서, 사용자(809)는 사용자(809)가 웹사이트 A(830a)를 액세스하려 함을 SASO 프록시 유닛(810)에 (또는, SASO 프록시 유닛(810)이 스크랩 또는 유사한 기술들에 의해 이 메시지를 인터셉트할 수 있는 경우에는 WAA(820)에) 표시한다. 단계 1045에서, SASO 프록시 유닛(810)은 사용자(809)가 웹사이트 A(830a)를 액세스하려 함을 WAA(820)에 표시한다. 다른 방법으로, 사용자가 웹사이트 A(830a)를 액세스하려는 자신의 의도를 WAA(820)에 직접 표시하고, SASO 프록시 유닛(810)이 동일한 정보를 획득하기 위해 스크랩을 이용하는 경우, 단계 1045는 요구되지 않는다.

[0084] 그 후, 단계 1050에서 WAA(820)는 웹사이트 A(830a)에의 액세스에 대한 요청을 DTM(835)에 전송한다. 그 후, 단계 1055에서 DTM(835)은 웹사이트 A(830a)에의 액세스에 대한 요청을 전달한다. 단계 1060에서, 웹사이트 A(830a)는 서비스 고유 패스워드에 대한 요청을 DTM 유닛(835)에 전송한다. 단계 1065에서 DTM 유닛(835)은 웹사이트 고유 패스워드를 웹사이트 A(830a)에 전송한다. 단계 1070에서, 웹사이트 A(830a)는 서비스 액세스 허가 메시지를 DTM 유닛(835)에 전송한다. 단계 1075에서, DTM 유닛(835)은 서비스 액세스 허가 메시지를 WAA(820)에 전송한다. 단계 1080에서 WAA(820)는 액세스가 웹사이트 A(830a)에 대해 승인됨을 사용자(809)에 표시한다. 단계 1085에서, 사용자는 WAA(820)를 이용하여, 웹사이트 A(830a)로부터의 서비스를 수신하는 것을 시작할 수 있다.

[0085] DTM(835)은 단계 1088, 1090 및 1093에서 WTRU(805)와 WAA(820) 무결성, 및 사용자 인증 데이터 및 (애플리케이션과 원하는 서비스의 리스트와 같은) 서비스 고유 데이터의 무결성의 입증을 검증하기 위해 정보를 요청하여 수신할 수 있다. 이러한 원격 입증 절차는 WTRU(805) 상의 TPM/TSS(815) 원격 입증 능력을 이용하여 행해질 수 있다. 단계 1088, 1090 및 1093의 절차는 또한 예를 들어, WTRU(805)가 부트업될 때의 시간에 수행될 수 있다. 이들 단계는 또한 단계 1050의 일부로서, DTM(835)으로부터 웹사이트에의 서비스 요청 메시지에 통합될 수 있다. 웹사이트 B(830b) 또는 등록된 리스트 상의 임의의 다른 웹사이트와 같은 다른 웹사이트들에 대하여 단계 1040 내지 단계 1085에 유사한 단계들을 반복할 수 있다.

[0086] 도 10의 일부 대안의 실시예들에서, WTRU(805)는 TPM/TSS(815)를 결여할 수 있다. 이러한 경우에, DTM(835)이 여전히 이용될 수 있다. 도 10으로 되돌아가면, WTRU가 TPM/TSS(815)를 결여한 경우, SASO 프록시 유닛(810)은 사용자 및 장치 인증 데이터, 원하는 서비스들의 리스트를 DTM 유닛(835)에 직접 등록한다. 정보의 수신 후에, DTM(835)은 (도 10의 단계 1125에서와 유사하게) 높은 엔트로피 사이트(또는 서비스) 고유 패스워드들을 발생시켜 유지시킨다. 초기 등록 후에 사용자(809)가 웹사이트 A(830a)를 액세스하려 할 경우, SASO 프록시 유닛(810)는 (도 10에서의 단계 1145 및 단계 1150와 유사하게) DTM(835)을 액세스하도록 WAA(820)를 프롬프트한다. DTM(835)은 (단계 1155와 유사하게)웹사이트 A(830a)에 대한 액세스를 요청한다. 웹사이트 A(830a)는 (단계 1160과 유사하게) 고유 서비스 패스워드에 대한 요청을 DTM(835)에 전송한다. DTM(835)은 (단계 1165와 유사하게) 웹사이트 고유 패스워드를 웹사이트 A(830a)에 전송한다. 웹사이트 A(830a)는 (단계 1170와 유사하게) 서비스 액세스 허가 메시지를 DTM(835)에 전송한다. DTM(835)은 (단계 1175와 유사하게) 액세스 허가 메시지를 WAA(820)에 전송한다. WAA(820)는 (단계 1180과 유사하게) 웹사이트 A(830a)에 대해 액세스가 허가됨을 사용자(809)에 표시한다. 사용자는 WAA(820)를 이용하여 (단계 1185와 유사하게) 웹사이트 A(830a)로부터 서비스를 수신하는 것을 시작할 수 있다.

[0087] 도 11은 다른 실시예에 따라 도 8의 시스템(800)의 구성요소들 간에 시그널링을 나타낸다. 구체적으로, 도 11은 종래 기술의 방법 보다 더 안전한 방식으로 TPM/TSS(815)를 이용하여 웹 액세스하기 위한 SSO에 대한 예시적인 절차(1100)를 나타낸다.

[0088] 이 방법에서, 사용자(809)는 사이트들의 그룹을 구성하고, 그룹 각각에 대한 액세스는 SASO 프록시 유닛(810)에 의해 제어되며, 공통적으로, 그룹 고유 로그인/패스워드가 사용자(809)에 의해 제공된다. 이러한 절차를 이용함으로써, 사용자(809)는 그룹 고유 패스워드들을 이용하여 특정 웹사이트 그룹들에 대한 액세스를 제어할 수 있고 이에 의해, 특정 웹사이트 그룹에만 액세스하려는 사용자(809)의 의도에 따라 심지어 SASO 프록시 유닛(810)의 액세스 권한을 설정한다. 예를 들어, 사용자(809)가 금융 웹사이트 그룹에 대해서만 공통 패스워드를 제공하고 개인 웹사이트 그룹에 대해서는 또 하나의 다른 패스워드를 제공하지 않는 경우, SASO 프록시 유닛(810)은 금융 웹사이트 그룹에 속하는 사이트들에 대한 SSO 동작을 관리하기 위해서만 권한부여된다. 도 11에 나타낸 바와 같이, 이 실시예는 예를 들어, 다음의 바람직한 시그널링 단계들을 포함한다. 시퀀스 및/또는 컨텐츠에서의

다른 변경들이 가능하며 또한 본 실시예의 범위 내에 있다.

[0089] 사용자(809)는 단계 1105에서 웹사이트 그룹의 성립을 위한 요청을 SASO 프록시 유닛(810)에 전송함으로써 SASO 프록시 유닛(810)에 의한 프롬프트시 가능하게 절차(1100)를 개시한다. 요청은 웹사이트 A(830a) 및 웹사이트 B(830b)와, 또한 사용자가 웹사이트 그룹에 대하여 만든 SSO 패스워드와, 그룹에 속하는 웹사이트의 URL들을 포함할 수 있다. 이 단계는 증분 방식(incremental manner)으로 행해질 수 있으며, 이에 의해, 사용자(809)는 웹사이트 A(830a)만을 갖고 그 후, 다른 웹사이트들을 추가 또는 삭제함으로써 그룹을 시작시킨다. 이러한 웹 사이트 리스트 업데이트가 임의의 시점에서 수행되는 경우, SASO 프록시 유닛(810)은 TPM/TSS(815)에 의해 유지되는 특정 데이터(그리고 SASO 프록시 유닛(810)에 의해 또한 이들 일부가 유지됨)를 추가, 삭제, 또는 심지어 바인딩해제 및 재바인딩을 위한 절차를 요청하는 것이 필요할 것이다.

[0090] 그 후, SASO 프록시 유닛(810)은 단계 1110에서 웹사이트 그룹에서의 각각의 웹사이트에 대해 웹사이트 URL들과 단일 SSO 패스워드를 등록한다. 그 후, SASO 프록시 유닛(810)은 단계 1115에서, SSO 패스워드, 그룹에 속하는 모든 웹사이트들에 대한 URL들 및 웹사이트 크리덴셜, WAA(820)와 SSO 프록시 유닛(810)의 어드레스 핸들과, 또한 TPM/TSS(815)에 대한 데이터 바인딩 및 웹사이트 고유 패스워드 발생을 위한 요청을 TPM/TSS(815)에 전송한다. 웹사이트 리스트에서의 각각의 URL에 대하여, TPM/TSS(815)는 단계 1120에서 TPM 난수 발생기(RNG)를 이용하여 암호적으로 강력한(cryptographically strong) 패스워드를 발생시킨다. 그 후, 단계 1125에서, TPM/TSS(815)은 TPM 저장 키에 의해 암호화된 데이터 블랍에서 웹사이트 고유 URL, (사이트 인증서를 포함한) 임의의 크리덴셜, SSO 패스워드 및 TPM/TSS가 발생시켰던 사이트 고유 패스워드를 바인딩시킨다. 이러한 키는 TPM을 하우징하는 플랫폼(예를 들어, WTRU 또는 컴퓨터)에 '바인딩'된다. 단계 1105에서, 사용자(809)가 웹사이트 그룹의 리스트의 업데이트(추가, 삭제, 또는 변경)를 자신의 연관 정보(URL들, 크리덴셜들 등)에 의해 표시했을 경우, 영향을 받는 웹사이트들에 대한 웹사이트 고유 기록들을 추가 또는 삭제하기 위해 SASO 프록시 유닛(810) 및 TPM/TSS(815)로부터의 표시가 있어야 한다.

[0091] 그 후, 단계 1130에서 사용자(809)는 웹사이트 A(830a)에 대한 URL을 WAA(820)에 제공한다. 단계 1135에서, SASO 프록시 유닛(810)은 웹스크랩에 의해 또는 API 또는 다른 구문분석 기술들을 통한 협력에 의해 웹사이트 A(830a)로부터의 패스워드 프롬프트를 인터셉트한다. 그 후, 단계 1140에서 SASO 프록시 유닛(810)은 웹사이트 A(830a)가 등록된 웹사이트 그룹의 멤버인지를 검증하고 이 판정이 긍정적이라면 이러한 그룹을 식별한다. 단계 1145에서, SASO 프록시 유닛(810)은 웹사이트 A(830a)가 속하는 웹사이트 그룹에 대한 SSO 패스워드를 제공하도록 휴먼 사용자(809)에 요청한다. 단계 1150에서, 휴먼 사용자(809)는 (예를 들어, USIM, 생체 또는 타이핑에 의해) 웹사이트 A(830a)에 대한 SSO 패스워드 및 웹사이트 URL을 제공한다. 다른 방법으로, 단계 1145 및 1150은 투과적으로 이루어질 수 있으며, SASO 프록시 유닛(810)에 의해 자동으로 제공될 수 있다.

[0092] 그 후, 단계 1155에서, SASO 프록시 유닛(810)은 사용자(809)가 제공한 SSO 패스워드를 검사한다. 단계 1160에서, SASO 프록시 유닛(810)은 웹사이트 A(830a)에 대한 패스워드를 바인딩해제하고 검색하라는 요청을 TPM/TSS(815)에 전송한다. 이 요청에서, SASO 프록시 유닛(810)은 웹사이트 A(830a)에 대한 SSO 패스워드와 사이트 URL을 포함한다. 단계 1165에서, TPM/TSS(815)는 이전에 저장된 데이터 블랍으로부터 웹사이트 A(830a)에 대한 사이트 고유 패스워드 및 크리덴셜들을 바인딩해제하기 위해 데이터 핸들로서 웹사이트 A(830a)에 대한 SSO 패스워드와 URL을 이용한다. 이전에 저장된 웹사이트 고유 패스워드, URL 리스트 및 웹사이트 고유 크리덴셜들을 바인딩해제하고 검색한 후, TPM/TSS(815)는 TPM/TSS(815)이 바인딩 저장으로부터 방금 복구했던 데이터의 값들에 대하여, TPM/TSS(815)이 SASO 프록시 유닛(810)으로부터 수신했던 SSO 패스워드 및 웹사이트 URL을 검증한다. 위의 단계 1165에서 검증이 이루어지면, 단계 1170에서 TPM/TSS(815)는 웹사이트 A(830a)에 대한 웹사이트 고유 패스워드와 크리덴셜들을 SASO 프록시 유닛(810)에 제공한다.

[0093] 그 후, 단계 1173에서, SASO 프록시 유닛(810)은 웹 스크래핑, API들 또는 다른 구문 분석 기술들과 같은 기술들을 이용하여 웹사이트 A(830a)에 대한 패스워드 및 크리덴셜 필드를 WAA(820) 상에 상주시킨다. 그 후, 단계 1175에서 WAA(820)는 채워지고 웹사이트 고유 패스워드와 크리덴셜을 웹사이트 A(830a)에 전송한다. 그 후, 단계 1180에서 패스워드와 크리덴셜은 웹사이트 A(830a)에 등록된다. 단계 1185에서, 웹사이트 등록에 대한 성공이 WAA(820)에 표시된다. 단계 1190에서, 웹사이트 등록의 성공은 SASO 프록시 유닛(810)에 표시되고 SASO 프록시 유닛의 데이터베이스에 기록된다. 또한 단계 1190에서, 웹사이트 등록의 성공 기록은 또한 TPM 키에 의해 보호되는 안전 메모리에 저장된 측정 로그(SML; stored measurement log)로서 기록된다. 단계 1195에서 TPM/TSS(815)에 의해 유지되는 사이트 고유 패스워드 및 크리덴셜들을 포함한 신뢰성있는 SSO의 성립이 완료된다.

[0094] 웹사이트 등록이 성립된 후, 사용자(809)가 나중 시간에 웹사이트의 서비스들을 이용하기 위해 사이온을 위하여 웹사이트 A(830a)를 액세스하기를 원하는 경우, 최종 결과가 초기 사이트 등록이 아니라 웹사이트 A(830a)에 대한 SSO 사인온인 경우에만, 단계 1130 내지 단계 1185와 동일한 단계들이 본질적으로 발생한다. 또한, 사용자(809)가 웹사이트 A(830a) 대신에 웹사이트 B(830b)에 등록하려 하는 경우, 이전에 웹사이트 A(830a)에 이용된 동일 단계들이 웹사이트 B(830b)의 SSO 등록 또는 인증에 이용될 수 있다. 그러나, 웹사이트 B의 URL, 크리덴셜, 사이트 고유 패스워드 및 토큰과 같은 웹사이트 B(830b)에 대한 웹사이트 고유 정보가 웹사이트 A(830a)에 대한 웹사이트 고유 정보 대신에 이용될 것이다.

[0095] 대안의 실시예에서, 그룹 방식의 액세스 제어(group-wise access control)가 사용자(809)에 의한 명시적 구성 없이 수행될 수 있다. 대신에, SASO 프록시 유닛(810)이 서로 다른 유형의 웹사이트 그룹들에 대한 액세스를 관리하는 (TPM에 의해 자체적으로 보호될 수 있는) 정책 또는 프로파일 데이터에 의해 제공될 수 있다. 이 실시예에서, 그룹 방식 액세스 제어는 설치 시간에 SASO 프록시 유닛(810)에 의해 구성될 것이다. 추가적으로, 정책 업데이트가 또한 설치 시간 이후에 가능할 수 있다.

[0096] 도 12는 대안의 실시예에 따라 구성된 무선 통신 시스템(1200)의 예시적인 블록도이다. 시스템(1200)은 적어도 하나의 WTRU(1215)와 무선 액세스 네트워크(RAN; 1203)를 포함한 리버티 얼라이언스 순응형 무선 통신 시스템이다. WTRU는 사용자(1205)와 상호작용하도록 구성되며 웹-SSO 유닛(1212), 플랫폼 처리 유닛(1210) 및 TPM/TSS(1217)를 포함한다. 플랫폼 처리 유닛(1210)은 소프트웨어(SW) 또는 하드웨어로서 구현될 수 있다. RAN(1203)은 ID 공급자(1220)와 서비스 공급자(1225)를 포함한다. 다른 방법으로, ID 공급자(1220)는 공용 인터넷 상에 위치되는 바와 같이, RAN(1203)의 외부에 위치될 수 있다.

[0097] 도 13은 다른 실시예에 따라 도 12의 시스템(1200)의 구성요소들 간에 시그널링을 나타낸다. 구체적으로, 도 13에서, ID-FF/SAML 기반 웹-SSO 기술은 또한 TPM/TSS(1217)에 의해 제공된 무결성 검사 메카니즘들과 결합된다. 시퀀스 및/또는 컨텐츠에서의 다른 변형들이 가능하며, 또한 본 실시예의 범위 내에 있다. 단계 1303에서 사용자(1205)는 웹-SSO 유닛(1212)을 실행시키려는 의도를 표시함으로써(예를 들어, 웹-SSO 유닛(1212) 상에서 클릭함으로써 또는 시스템 부팅에 의한 디폴트에 의해서 등) 절차(1300)를 개시한다. 단계 1308에서 플랫폼 처리 유닛(1210)은 웹-SSO 유닛(1212)의 코드 무결성 검사를 수행하도록 TPM/TSS(1217)에 요청한다. 단계 1312에서 TPM(1217)은 코드 무결성 검사를 실행하고 그 결과를 플랫폼 처리 유닛(1210)에 전달한다.

[0098] 단계 1312에서의 검사가 긍정적인 경우, 단계 1316에서, 로그인 또는 인증 정보가 플랫폼 처리 유닛(1210)에 제공되며, 웹-SSO 유닛(1212)에 전달된다. 단계 1320에서 웹-SSO 유닛(1212)은 TPM 키를 이용하여 이전에 저장되었던 로그인 크리덴셜을 검색하도록 TPM(1217)에 요청한다. 단계 1324에서 TPM(1217)은 로그인 크리덴셜 데이터를 검색하여 이를 웹-SSO 소프트웨어(1212)에 전달한다. 단계 1328에서 웹-SSO 유닛(1212)은 IDP(1220)에 로그인하기 위해 검색된 로그인 크리덴셜 데이터를 이용한다. 단계 1332에서 IDP(1220)는 웹-SSO 유닛(1212)에 도입 쿠키를 전송한다.

[0099] 그후, 단계 1336에서, 웹-SSO 유닛(1212)은 SP(1225)에 대해 인증한다. 단계1340에서, SP(1225)는 1) 웹-SSO 유닛(1212)이 IDP(1220)로부터의 쿠키를 갖는지, 2) 웹-SSO 유닛(1212)이 IDP(1220)에 의해 지원되는 웹-SSO 유닛의 연계된 ID를 이용하려 하는지, 및 3) 웹-SSO 유닛(1212)이 플랫폼 바인딩된 TPM 개인 키 - 공개 키는 SP에 이미 저장되어 있거나 또는 PCA에 의해 획득될 수 있음 - 에 의해 서명된 자신의 플랫폼 보안 상태의 스테이터스를 기술하는 인증서를 제공할 수 있는지를 웹-SSO 유닛(1212)에 문의한다. 선택적으로, PCA는 IPD(1220)일 수 있다.

[0100] 그 후, 단계 1344에서 웹 SSO 유닛(1212)은 플랫폼 신뢰 상태를 TPM/TSS(1217)에 전송한다. 단계 1348에서 TPM/TSS(1217)는 플랫폼의 신뢰 상태를 입증하는 TPM-유지 개인 서명 키에 의해 서명된 인증서를 생성하여 웹-SSO 소프트웨어(1212)에 전달한다. 단계 1352에서, 웹-SSO 유닛(1212)은 1) 웹-SSO 유닛이 IDP(1220)으로부터의 쿠키들을 갖고 있음을 긍정하고, 2) 웹-SSO 유닛이 IDP(1220)에 의해 유지되는 웹-SSO 유닛의 연계된 계정을 이용하려 함을 긍정함을 SP(1225)에 표시하며, 또한 3) SP(1225)에 플랫폼 보안 상태 인증서를 전송한다. 단계 1356에서, SP(1225)는 PCA로부터의 도움으로 웹-SSO 유닛(1212)에 의해 전송된 신뢰 인증서를 평가한다. 그 후, 단계 1358에서, SP(1212)는 다시 재연결하고 인증하도록 웹-SSO 유닛(1212)에 요청하며, 이번에는 연계 인증 요청을 이용한다.

[0101] 그 후, 단계 1362에서, 웹-SSO 유닛(1212)은 IDP(1220)에 연계된 인증 요청을 전송한다. 단계 1364에서, IDP(1220)는 연계된 NameID와 연관된 인증문을 발생시킨다. 단계 1368에서, IDP(1220)는 SP(1225)에 재연결하도록 웹-SSO 유닛(1212)에 요청한다. 단계 1372에서, 웹-SSO 유닛(1212)은 TPM/TSS(1217)에 의해 보호된 키를

이용하여 저장되었던 연계 <Assertion>의 연계 아티팩트(artifact)를 검색하도록 TPM/TSS(1217)에 요청한다. 단계 1372에서, TPM/TSS(1217)는 아티팩트 데이터를 검색하여 이를 웹-SSO 유닛(1212)에 전달한다. 단계 1380에서 웹-SSO 유닛(1212)은 IDP(1220)에 의해 유지된 검색된 연계 <Assertion> 아티팩트를 SP(1225)에 전송한다.

[0102] 그 후, 단계 1384에서 SP(1225)는 IDP(1220)에 의해 검증 프로세스를 개시하여, SOAP 프로토콜을 이용해 휴먼 사용자(1205)에 대한 <Assertion>를 검증한다. 단계 1388에서 IDP(1220)는 SOAP 프로토콜을 이용하여 검증 프로세스를 응답(reciprocate)한다. 단계 1392에서 SP(1225)는 휴먼 사용자(1205)에 대한 <Assertion>와 연계된 계정을 평가한다. 마지막으로, 단계 1396에서, SP(1225)는 승인된 서비스 시작을 웹-SSO 유닛(1212)에 표시하며, 이 표시는 휴먼 사용자(1205)에 의해 (예를들어, 디스플레이 등에 의해) 제공된다.

[0103] 도 13의 대안의 실시예에서, 장치의 신뢰 상태가 IDP(1220)에 의해 한번 평가될 수 있고 그 후, IDP의 이용을 위하여 필요에 따라 각각의 SP(1225)에 통신될 수 있다. 이러한 정보의 전달은 SAML 또는 SOAP 절차와 같은 연계된 방식 내에서 쿠키들 또는 다른 기존의 또는 변경된 메시지/프로토콜들과 같은 수단에 의해 행해질 수 있다.

[0104] 특성 및 요소들이 바람직한 실시예에서 특정 조합으로 설명되어 있지만, 각각의 특성 또는 요소들은 바람직한 실시예의 다른 특성들 및 다른 요소들 없이 단독으로 또는 개시된 다른 특성 및 요소들과 함께 또는 이들 없이 여러 조합으로 이용될 수 있다. 본 발명에 제공되는 방법들 또는 흐름도는 범용 컴퓨터 또는 프로세서에 의한 실행을 위하여 컴퓨터 판독가능 저장 매체에 실체적으로 구체화되어 있는 컴퓨터 프로그램, 소프트웨어, 또는 펌웨어로 구현될 수 있다. 컴퓨터 판독가능 저장 매체의 예들은 판독 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 레지스터, 캐시 메모리, 반도체 메모리 장치, 내부 하드 디스크 및 착탈가능 디스크들과 같은 자기 매체, 자기 광학 매체, 및 CD-ROM 디스크 및 디지털 다기능 디스크(DVD)와 같은 광학 매체를 포함한다.

[0105] 적합한 프로세서들은 예를 들어, 범용 프로세서와, 특수 목적 프로세서와, 통상의 프로세서와, 디지털 신호 프로세서(DSP)와, 복수의 마이크로프로세서와, DSP 코어와 관련된 하나 이상의 마이크로프로세서, 컨트롤러, 마이크로컨트롤러, 응용 주문형 집적 회로(ASIC), 필드 프로그래밍가능 게이트 어레이(FPGA) 회로, 어떤 다른 유형의 집적 회로(IC) 및/또는 상태 머신을 포함한다.

[0106] 소프트웨어와 관련된 프로세서는 무선 송수신 유닛(WTRU), 사용자 기기(UE), 단말기, 기지국, 무선 네트워크 컨트롤러(RNC) 또는 어떤 호스트 컴퓨터에서의 이용을 위한 무선 주파수 트랜시버를 구현하는데 이용될 수 있다. WTRU는 카메라, 비디오 카메라 모듈, 비디오 폰, 스피커 폰, 바이블레이션 장치, 스피커, 마이크로폰, 텔레비젼 트랜시버, 핸드 프리 헤드셋, 키보드, 블루투스®

모듈, 주파수 변조(FM) 무선 유닛, 액정 디스플레이(LCD) 디스플레이 유닛, 유기 발광 다이오드(OLED) 디스플레이 유닛, 디지털 뮤직 플레이어, 미디어 플레이어, 비디오 게임 플레이어 모듈, 인터넷 브라우저, 및/또는 임의의 무선 근거리 통신망(WLAN) 모듈과 같이, 하드웨어 및/또는 소프트웨어로 구현되는 모듈들과 결합하여 이용될 수 있다.

[0107] 실시예들

[0108] 1. 트러스티드 플랫폼 모듈(TPM)을 갖는 무선 송수신 유닛(WTRU)에 의한 웹사이트 액세스를 위한 안전 싱글 사인온(SSO)을 제공하는 방법으로서,

[0109] WTRU에서, 목표 웹사이트 그룹을 결정하는 단계와; 목표 웹사이트 그룹으로부터 선택된 한 웹사이트에 대해 안전하게 사인온하는 단계와; WTRU의 TPM에 발생되어 저장된 보안 패스워드를 이용하여 웹사이트 그룹으로부터 선택된 다른 웹사이트에 대해 사인온하는 단계를 포함한다.

[0110] 2. 실시예 1의 방법에서, TPM은 목표 웹사이트 그룹에 대한 액세스가 요청될 때를 결정하는 SSO 프록시 유닛을 포함한다.

[0111] 3. 실시예 2의 방법에서, SSO 프록시 유닛은 TPM에 의해 안전하게 보호된다.

[0112] 4. 임의의 선행하는 실시예의 방법에서, TPM은 목표 웹사이트 그룹으로부터 선택된 웹사이트들을 액세스하기 위해 랜덤 패스워드를 발생시킨다.

[0113] 5. 실시예 4의 방법에서, TPM은 목표 웹사이트 그룹으로부터 선택된 웹사이트들을 액세스하기 위해 발생된 랜덤

패스워드를 저장한다.

[0114] 6. 임의의 선행하는 실시예의 방법에서, 결정하는 단계는 WTRU의 사용자가 목표 웹사이트 그룹을 선택하는 단계를 더 포함한다.

[0115] 7. 임의의 선행하는 실시예의 방법에서, SSO 프록시 유닛은 패스워드 정보를 안전하게 기록한다.

[0116] 8. 실시예 7의 방법에서, 기록된 패스워드 정보는 키 바인딩 기술을 이용하여 저장된다.

[0117] 9. 실시예 7 또는 실시예 8의 방법에서, 기록된 패스워드 정보는 TPM 내에 내부적으로 저장된다.

[0118] 10. 임의의 선행하는 실시예의 방법에서, WTRU는 TPM에 저장된 고유 아이덴티티를 포함한다.

[0119] 11. 임의의 선행하는 실시예의 방법에서, WTRU는 유니버셜 가입자 식별 모듈(USIM)에 저장된 고유 아이덴티티를 포함한다.

[0120] 12. 실시예 10 또는 실시예 11의 방법은 고유 아이덴티티에 기초하여 암호 키 계층 구성(hierarchy)을 생성하는 단계를 더 포함한다.

[0121] 13. 임의의 선행하는 실시예의 방법에서, 웹사이트 그룹으로부터 선택된 웹사이트에 대한 안전한 사인온 단계는 웹사이트의 인증서 정보와 연관된 고유 사용자 식별정보와 패스워드를 생성하는 단계를 더 포함한다.

[0122] 14. 임의의 선행하는 실시예의 방법에서, 웹사이트 그룹으로부터 선택된 다른 웹사이트에 대한 사인온 단계는 웹사이트에 사용자 크리덴셜을 자동으로 전송하는 단계를 더 포함한다.

[0123] 15. 실시예 14의 방법에서, 사용자 크리덴셜은 데이터와 함께 전송된다.

[0124] 16. 임의의 선행하는 실시예의 방법에서, 사용자의 생체 정보를 감지하는 단계를 더 포함한다.

[0125] 17. 실시예 16의 방법에서, 감지된 생체 정보는 보안 목적으로 이용된다.

[0126] 18. 임의의 선행하는 실시예의 방법은 사용자가 웹사이트 A와 웹사이트 B를 포함한 웹사이트 그룹에의 등록을 요청하는 단계를 더 포함한다.

[0127] 19. 실시예 18의 방법에서, 등록은 웹사이트 A와 웹사이트 B를 포함한 웹사이트 그룹에 대한 SSO 패스워드 및 그룹에 속하는 웹사이트들의 URL을 더 포함한다.

[0128] 20. 실시예 18 또는 실시예 19의 방법에서, 등록은 증분적으로 수행된다.

[0129] 21. 실시예 18 내지 실시예 20 중 어느 한 실시예의 방법은 SSO 프록시 유닛이 웹사이트 그룹에 대한 웹사이트 URL들 및 싱글 SSO 패스워드를 등록하는 단계를 더 포함한다.

[0130] 22. 실시예 21의 방법은, SSO 프록시 유닛이 웹사이트 그룹에 속하는 모든 웹사이트들에 대한 SSO 패스워드, URL들 및 웹사이트 크리덴셜, 웹 액세스 애플리케이션(WAA) 및 프록시의 어드레스 핸들을 TPM 및 TPM 소프트웨어 스택(TSS)(TPM/TSS)에 전송하는 단계와, SSO 프록시가 데이터 바인딩 뿐만 아니라 웹사이트 고유 패스워드 발생을 TPM/TSS에 요청하는 단계를 더 포함한다.

[0131] 23. 실시예 22의 방법은 TPM/TSS가 미리 결정된 레퍼런스에 대하여 프록시 및 WAA의 코드 무결성을 검증하는 단계를 더 포함한다.

[0132] 24. 실시예 23의 방법은 TPM/TSS가 TPM 난수 발생기를 이용하여 웹사이트 그룹의 각각의 URL에 대하여 암호적으로 강력한 패스워드를 발생시키는 단계를 포함한다.

[0133] 25. 실시예 24의 방법은 TPM이 TPM/TSS에 의해 발생된 다음 보호되는 저장 키를 이용하여 웹사이트 고유 URL, 크리덴셜, SSO 패스워드 해시 및 발생된 웹사이트 고유 패스워드를 결합 코드 무결성 값으로 봉인하는 단계를 더 포함한다.

[0134] 26. 실시예 24의 방법은 TPM이 TPM/TSS에 의해 발생된 다음 보호되는 저장 키를 이용하여 웹사이트 고유 URL, 크리덴셜, SSO 패스워드 해시 및 발생된 웹사이트 고유 패스워드를 결합된 코드 무결성 값에 바인딩시키는 단계를 더 포함한다.

[0135] 27. 실시예 25 또는 실시예 26의 방법은 TPM/TSS가 웹사이트 그룹의 각각의 웹사이트에 대응하는 추가의 액션들 및 요청들의 표시를 위해 TPM과 SSO 프록시 유닛 사이의 토큰으로서 이용하기 위한 암호적으로 강력한 난수를

발생시키는 단계를 더 포함한다.

[0136] 28. 실시예 27의 방법은, TPM/TSS가 웹사이트 그룹에서의 각각의 웹사이트에 대한 데이터 핸들로서 토큰을 이용하는 단계를 더 포함한다.

[0137] 29. 실시예 28의 방법은, TPM/TSS가 SSO 패스워드를 해싱하고, 그 패스워드와 해시를 안전하게 저장하는 단계를 더 포함한다.

[0138] 30. 실시예 29의 방법은, TPM/TSS가 SSO 프록시 유닛에 모든 토큰을 전송하는 단계와, TPM/TSS가 토큰들 사이의 매핑을 나타내는 매핑 데이터를 웹사이트 URL들에 전송하는 단계를 더 포함한다.

[0139] 31. 실시예 30의 방법은 WTRU의 사용자가 URL을 선택하는 단계를 더 포함한다.

[0140] 32. 실시예 31의 방법은, 프록시가 웹사이트 A로부터의 패스워드 프롬프트를 인터셉트하는 단계를 더 포함한다.

[0141] 33. 실시예 32의 방법에서, SSO 프록시 유닛은 웹사이트 A로부터 패스워드를 인터셉트하기 위하여 웹 스크랩 또는 애플리케이션 프로그래밍 인터페이스(API)와의 협력을 이용한다.

[0142] 34. 실시예 32 또는 실시예 33의 방법은, SSO 프록시 유닛이 웹사이트 A가 웹사이트 그룹의 멤버인지를 검증하는 단계를 더 포함한다.

[0143] 35. 실시예 34의 방법은, 프록시가 웹사이트 A를 포함한 웹사이트 그룹에 대한 SSO 패스워드를 제공하도록 WTRU의 사용자에 요청하는 단계를 더 포함한다.

[0144] 36. 실시예 35의 방법은 WTRU의 사용자가 SSO 패스워드를 제공하는 단계를 더 포함한다.

[0145] 37. 실시예 36의 방법은 프록시가 WTRU의 사용자에 의해 제공된 SSO 패스워드를 검증하는 단계를 더 포함한다.

[0146] 38. 실시예 37의 방법은 프록시가 웹사이트 A에 대한 패스워드를 봉인해제하라는 요청을 TPM/TSS에 전송하는 단계를 더 포함한다.

[0147] 39. 실시예 38의 방법에서, 웹사이트 A에 대한 패스워드를 봉인해제하라는 요청은 SSO 프록시 유닛이 데이터베이스에 저장한 웹사이트 A에 대한 SSO 패스워드 및 임의의 웹사이트 고유 크리덴셜을 포함한다.

[0148] 40. 실시예 38 또는 실시예 39의 방법에서, 웹사이트 A에 대한 패스워드를 봉인해제하라는 요청은 SSO 프록시 유닛과 WAA에 대한 코드 핸들을 포함한다.

[0149] 41. 실시예 39 또는 실시예 40의 방법은 TPM/TSS가 웹사이트 A에 속하는 토큰을 검증하고 웹사이트 A에 대한 웹사이트 고유 패스워드와 크리덴셜을 봉인해제하는 단계를 더 포함한다.

[0150] 42. 실시예 41의 방법은 TPM/TSS가 웹사이트 A에 대한 웹사이트 고유 패스워드 및 크리덴셜을 SSO 프록시 유닛에 제공하는 단계를 더 포함한다.

[0151] 43. 실시예 42의 방법은 SSO 프록시 유닛이 WAA 상에 웹사이트 A에 대한 패스워드 및 크리덴셜 필드를 상주시키는 단계를 더 포함한다.

[0152] 44. 실시예 43의 방법은 웹사이트 고유 패스워드 및 크리덴셜을 웹사이트 A에 전송하는 단계와, 웹사이트 A에서의 성공적인 등록을 확인하는 단계를 더 포함한다.

[0153] 45. 실시예 44의 방법은 SSO 프록시 유닛에 성공적인 웹사이트 등록을 표시하는 단계와, SSO 프록시 유닛 데이터베이스에 성공적인 등록을 기록하는 단계를 더 포함한다.

[0154] 46. 임의의 선행하는 실시예의 방법에서, WTRU의 인증 및 ID에 관련된 데이터가 WTRU의 TPM에 의해 암호적으로 보호된다.

[0155] 47. 임의의 선행하는 실시예의 방법은 새로운 암호 키를 이용하여 저장된 암호화된 데이터를 주기적으로 업데이트하는 단계를 더 포함한다.

[0156] 48. 트러스티드 플랫폼 모듈(TPM)을 이용하는 장치 상에서 애플리케이션 또는 인터넷 기반 서비스들에 대한 액세스를 위한, 사용자에 의한 안전 자동화된 사인온(SASO)에 대한 방법은, 사용자가 싱글 로그인 ID와 패스워드에 의해 애플리케이션 또는 인터넷 기반 서비스들을 액세스하는 단계를 포함한다.

[0157] 49. 실시예 48의 방법에서, TPM은 TPM 소프트웨어 스택(TSS)을 포함한다.

[0158] 50. 실시예 48 또는 실시예 49의 방법은 사용자가 장치에 대해 인증하고 안전한 한 팩터 인증을 통하여 장치에 대한 액세스를 구하는 단계를 더 포함한다.

[0159] 51. 실시예 48 또는 실시예 49의 방법은 사용자가 장치를 인증하고 안전한 2개의 팩터 인증을 통하여 장치에 대한 액세스를 구하는 단계를 더 포함하며, 2개의 팩터는 TPM에 의해 안전하게 유지된 생체(biometrics)를 통한다.

[0160] 52. 실시예 48 내지 실시예 51 중 어느 한 실시예의 방법에서, SASO 프록시 유닛은 TPM 내에 유지된 보안 정보를 액세스한다.

[0161] 53. 실시예 51 또는 실시예 52의 방법에서, 생체 2차 팩터 인증이 이용되고, SASO 프록시 유닛은 인증을 위해 TPM을 검색하도록 TPM에 요청을 전송한다.

[0162] 54. 실시예 53의 방법은 TPM이 SASO 프록시 유닛에 생체 인증 데이터를 제공하는 단계를 더 포함한다.

[0163] 55. 실시예 48 내지 실시예 54 중 어느 한 실시예의 방법은 사용자가 WAA를 이용하여 안전 웹사이트에 등록하는 것을 시도하는 단계를 더 포함한다.

[0164] 56. 실시예 55의 방법에서, 애플리케이션은 웹-WAA(WAA)이다.

[0165] 57. 실시예 55 또는 실시예 56의 방법에서, WAA는 사용자가 제1 인터넷 기반 서비스 웹사이트를 액세스하기를 원한다는 표시를 제1 인터넷 기반 서비스 웹사이트에 전송하는 단계를 더 포함한다.

[0166] 58. 실시예 57의 방법은 WAA가 제1 인터넷 기반 서비스 웹사이트의 로그인 프롬프트를 수신하여 표시하는 단계를 더 포함한다.

[0167] 59. 실시예 48 내지 실시예 58 중 어느 한 실시예의 방법은 SSO 프록시 유닛이 WAA로부터의 제1 웹사이트의 인증 프롬프트를 인터셉트하는 단계를 더 포함한다.

[0168] 60. 실시예 59의 방법에서, 인터셉트하는 단계는 웹 스크랩에 의해 또는 구문 분석 기술을 통한 협력에 의해 실현된다.

[0169] 61. 실시예 48 내지 실시예 60 중 어느 한 실시예의 방법은 SASO 프록시 유닛이 사용자 ID 정보를 TPM에 전달하는 단계를 더 포함한다.

[0170] 62. 실시예 61의 방법에서, 사용자 ID 정보는 2개의 팩터 인증으로부터의 장치 로그인 정보를 포함한다.

[0171] 63. 실시예 48 내지 실시예 62 중 어느 한 실시예의 방법은 웹사이트 고유 보안 패스워드가 TPM에 의해 발생되어 안전하게 저장되는 단계를 더 포함한다.

[0172] 64. 실시예 63의 방법에서, 패스워드는 TPM NV 메모리에 직접 안전하게 저장되거나 또는 TPM-보호된 바인딩 저장 키에 의해 통상의 메모리에서 암호화된다.

[0173] 65. 실시예 59 내지 실시예 64 중 어느 한 실시예의 방법에서, SASO 프록시 유닛은 WAA 패스워드 프롬프트시 웹사이트 고유 안전 패스워드에 대한 정보를 채워넣으며, 이 정보는 제1 웹사이트에 대하여 웹사이트 고유이다.

[0174] 66. 실시예 65의 방법에서, WAA가 웹사이트 고유 패스워드를 제1 웹사이트에 전달하는 단계와, 제1 웹사이트가 웹사이트 고유 패스워드를 등록하고 액세스 허가를 WAA에 전송하는 단계를 더 포함한다.

[0175] 67. 실시예 48 내지 실시예 66 중 어느 한 실시예의 방법에서, 등록이 성립되었으며, TPM 바인딩 저장 키에 의해 보호되는 TPM 데이터 블랍에서의 데이터베이스 기록으로서 공동으로 웹사이트 고유 정보를 암호적으로 저장하는 단계를 더 포함한다.

[0176] 68. 실시예 67의 방법에서, 웹사이트 고유 정보는 URL, 디지털 인증서, 사용자 ID 및 패스워드 중 적어도 하나를 포함한다.

[0177] 69. 실시예 66 내지 실시예 68 중 어느 한 실시예의 방법에서, 웹사이트 고유 패스워드가 각각의 웹사이트에 대한 이후의 로그인을 위하여 SASO 프록시 유닛에 의해 재이용된다.

[0178] 70. 실시예 48 내지 실시예 69 중 어느 한 실시예의 방법에서, 제1 웹사이트가 WAA에 대한 액세스를 승인하며, 일반적인 웹 기반 통신을 더 포함한다.

[0179] 71. 실시예 48 내지 실시예 70 중 어느 한 실시예의 방법은 패스워드가 TPM 내에 유지되어 있는 이미 성립된 웹

사이트를 액세스하는 단계를 더 포함한다.

[0180] 72. 실시예 48 내지 실시예 71 중 어느 한 실시예의 방법은 추가의 웹사이트를 액세스하기 위해 SASO 프록시 유닛을 이용하는 단계를 더 포함한다.

[0181] 73. 실시예 48 내지 실시예 72 중 어느 한 실시예의 방법에서, TPM에 의해 실시되는 코드 무결성 검증 절차는 안전한 거래가 발생하도록 보장하기 위해 SASO 프록시 유닛의 무결성을 보호하는데 이용된다.

[0182] 74. 실시예 48 내지 실시예 73 중 어느 한 실시예의 방법은, 패스워드 업데이트 절차를 관리하기 위해 정책 또는 프로파일을 설정하는 단계를 더 포함하며, TPM은 TPM 바인딩 저장 키에 의해 보호된 데이터 블랍에 정책 및 프로파일 정보를 저장함으로써 정책 및 프로파일 정보를 보호한다.

[0183] 75. 실시예 48 내지 실시예 74 중 어느 한 실시예의 방법은 관리될 보안 패스워드 업데이트 정책을 제공하기 위해 보안 시간 기능(facility)을 이용하는 단계를 더 포함한다.

[0184] 76. 실시예 48 내지 실시예 75 중 어느 한 실시예의 방법은 싱글 인증 패스워드 하에서 TPM 내에 유지되는 수개의 웹사이트들을 공동으로 풀링하는 단계를 더 포함한다.

[0185] 77. 실시예 48 내지 실시예 76 중 어느 한 실시예의 방법은, TPM이 인증에 이용된 키와 패스워드들의 빈번한 업데이트를 수행하는 단계를 더 포함한다.

[0186] 78. 실시예 77의 방법에서, TPM은 패스워드 업데이트 절차를 트리거링하기 위해, 마지막 패스워드 업데이트가 발생했고 업데이트 시간 간격이 사용자 또는 인터넷 기반 서비스에 의해 제공될 때의 시간의 트랙을 유지시키는 보안 타이머 모듈을 포함한다.

[0187] 79. 싱글 자동화 사인온(SASO) 프록시 유닛과 트러스티드 플랫폼 모듈(TPM)을 갖는 장치 상에서 애플리케이션 또는 인터넷 기반 서비스에 대한 액세스를 위한, 사용자에 의한 SASO에 대한 방법으로, 사용자가 애플리케이션 또는 인터넷 기반 서비스의 그룹을 구성하는 단계로서 이에 의해 각각의 애플리케이션 또는 인터넷 기반 서비스에 대한 액세스가 그룹 고유 패스워드에 의해 제어되는 것인 구성 단계를 포함한다.

[0188] 80. 실시예 79의 방법은, SASO 프록시 유닛이 제1 인터넷 웹사이트와 제2 인터넷 웹사이트를 포함하는 웹사이트 그룹의 등록 또는 성립을 위한 요청을 수신하는 단계와, 웹사이트 그룹에 대한 SSO 패스워드와 웹사이트 그룹에 속하는 인터넷 웹사이트의 URL들을 발생시키는 단계를 더 포함한다.

[0189] 81. 실시예 80의 방법에서, 사용자는 제1 인터넷 웹사이트만을 가진 후 다른 웹사이트들을 추가 또는 삭제함으로써 그룹을 증분적으로 시작한다.

[0190] 82. 실시예 79 내지 실시예 81 중 어느 한 실시예의 방법은 웹사이트 그룹에 대한 업데이트를 수행하는 단계와, SASO 프록시 유닛이 TPM에 의해 유지되는 데이터의 추가, 삭제 또는 심지어 바인딩 해제 및 재바인딩을 위한 절차를 요청하는 단계를 더 포함한다.

[0191] 83. 실시예 79 내지 실시예 82 중 어느 한 실시예의 방법은, SASO 프록시 유닛이 웹사이트 그룹에 대한 웹사이트 URL들과 싱글 SSO 패스워드를 등록하는 단계를 더 포함한다.

[0192] 84. 실시예 79 내지 실시예 83 중 어느 한 실시예의 방법에서, TPM은 TPM 소프트웨어 스택(TSS)을 포함한다.

[0193] 85. 실시예 80 내지 실시예 84 중 어느 한 실시예의 방법은 SASO 프록시 유닛이 그룹에 속하는 모든 웹사이트들에 대한 SSO 패스워드, URL들 및 웹사이트 크리덴셜, 인터넷 WAA 소프트웨어 및 SSO 프록시 유닛 자체의 어드레스 핸들을 TPM에 전송하는 단계와; 데이터 바인딩 및 웹사이트 고유 패스워드 발생을 위한 요청을 TPM에 전송한다.

[0194] 86. 실시예 85의 방법에서, 리스트에서의 각각의 URL에 대하여, TPM은 TPM 난수 발생기(RNG)를 이용하여 암호적으로 강력한 패스워드를 발생시킨다.

[0195] 87. 실시예 86의 방법은, TPM이 TPM 저장 키를 이용하여 암호화된 데이터 블랍에서 웹사이트 고유 URL, 임의의 크리덴셜, SSO 패스워드 및 TPM이 발생시켰던 웹사이트 고유 패스워드를 바인딩하는 단계를 더 포함한다.

[0196] 88. 실시예 87의 방법에서, 키는 TPM을 하우징하는 플랫폼에 바인딩된다.

[0197] 89. 실시예 80 내지 실시예 88 중 어느 한 실시예의 방법에서, 사용자는 자신의 연관 정보에 의해 웹사이트 그룹에 대한 업데이트를 표시하며, 영향을 받은 웹사이트들에 대한 웹사이트 고유 기록들을 추가 또는 삭제하라는

SASO 프록시 유닛과 TPM으로부터의 표시를 더 포함한다.

[0198] 90. 실시예 79 내지 실시예 89 중 어느 한 실시예의 방법은 사용자가 제1 인터넷 웹사이트에 대한 장치 내의 URL을 WAA에 입력하는 단계를 더 포함한다.

[0199] 91. 실시예 90의 방법은 SASO 프록시 유닛이 제1 인터넷 웹사이트로부터의 패스워드 프롬프트를 인터셉트하는 단계를 더 포함한다.

[0200] 92. 실시예 91의 방법에서, 상기 인텁세트하는 단계는 웹스크랩에 의해 또는 API 또는 다른 구문 분석 기술을 통한 협력에 의한다.

[0201] 93. 실시예 91 또는 실시예 92의 방법은 SASO 프록시 유닛이 제1 인터넷 웹사이트가 등록된 웹사이트 그룹의 멤버인지를 검증하고 긍정적인 경우 이러한 그룹을 식별하는 단계를 더 포함한다.

[0202] 94. 실시예 91 내지 실시예 93 중 어느 한 실시예의 방법은, SASO 프록시 유닛이 제1 인터넷 웹사이트가 속하는 웹사이트 그룹에 대한 SSO 패스워드를 제공하도록 사용자에 요청하는 단계를 더 포함한다.

[0203] 95. 실시예 91 내지 실시예 94 중 어느 한 실시예의 방법은, 사용자가 제1 인터넷 웹사이트에 대한 SSO 패스워드 및 웹사이트 URL을 입력하거나 또는 제공하는 단계를 더 포함한다.

[0204] 96. 실시예 95의 방법에서, 제공하는 단계는 생체에 의한 것이다.

[0205] 97. 실시예 94 내지 실시예 96 중 어느 한 실시예의 방법에서, SASO 프록시 유닛은 사용자가 제공했던 SSO 패스워드를 검사한다.

[0206] 98. 실시예 91 내지 실시예 93 중 어느 한 실시예의 방법은 SSO 프록시 유닛이 웹사이트 URL, SSO 프록시 유닛의 인증서 및 패스워드에 대한 프롬프트에 의해 SSO 패스워드를 자동으로 제공하는 단계를 더 포함한다.

[0207] 99. 실시예 79 내지 실시예 98 중 어느 한 실시예의 방법은, SSO 프록시 유닛이 제1 인터넷 웹사이트에 대한 SSO 패스워드 및 웹사이트 URL을 포함한, 제1 인터넷 웹사이트에 대한 패스워드를 바인딩해제하고 검색하라는 요청을 TPM에 전송하는 단계를 더 포함한다.

[0208] 100. 실시예 99의 방법은 TPM이, 이전에 저장된 데이터 블랍으로부터 제1 인터넷 웹사이트에 대한 웹사이트 고유 패스워드와 크리덴셜을 바인딩 해제하도록 데이터 핸들로서 제 1 인터넷 웹사이트에 대한 SSO 패스워드 및 URL을 이용하는 단계와, TPM이 바인딩 저장으로부터 복구했던 데이터의 값에 대하여 TPM이 SASO 프록시 유닛으로부터 수신했던 웹사이트 URL과 SSO 패스워드를 TPM이 검증하는 단계를 더 포함한다.

[0209] 101. 실시예 100의 방법에서, SSO 패스워드에 대한 검증이 이루어지면, TPM은 SSO 프록시 유닛에 제1 인터넷 웹사이트에 대한 웹사이트 고유 패스워드 및 크리덴셜을 제공한다.

[0210] 102. 실시예 79 내지 실시예 101 중 어느 한 실시예의 방법은, SSO 프록시 유닛이 웹사이트 스크랩, API들 또는 다른 구문분석 기술을 이용하여, 제1 인터넷 웹사이트에 대한 패스워드 및 크리덴셜 필드들을 상주시키는 단계를 더 포함한다.

[0211] 103. 실시예 102의 방법은 인터넷 WAA를 채워넣는 단계와, 제1 인터넷 웹사이트에 웹사이트 고유 패스워드 및 크리덴셜을 전송하며, 제1 인터넷 웹사이트에 등록된 패스워드 및 크리덴셜을 등록하는 단계를 더 포함한다.

[0212] 104. 실시예 103의 방법은, 인터넷 WAA에 대한 성공적인 등록을 표시하는 단계와, SASO 프록시 유닛에 대한 등록을 표시하고 SASO 프록시 유닛의 데이터베이스에 등록을 기록하는 단계를 더 포함한다.

[0213] 105. 실시예 104의 방법은, TPM 키에 의해 보호되는 안전 메모리에 저장된 측정 로그(SML)로서 등록을 기록하는 단계를 더 포함한다.

[0214] 106. 실시예 79 내지 실시예 105 중 어느 한 실시예의 방법에서, 사용자는 이후의 시간에 웹사이트 서비스를 이용하도록 사인온하기 위해 제1 인터넷 웹사이트를 액세스하려 하고, 사용자가 SASO에 의해 액세스를 구하는 단계를 더 포함한다.

[0215] 107. 실시예 79 내지 실시예 106 중 어느 한 실시예의 방법에서, 사용자는 제1 인터넷 웹사이트 대신에 제2 인터넷 웹사이트를 등록 또는 이후에 액세스하려 하며, URL, 크리덴셜, 웹사이트 고유 패스워드 및 토큰 중 하나 이상을 포함한, 제2 인터넷 웹사이트에 대한 웹사이트 고유 정보를 이용하여 제2 인터넷 웹사이트의 SASO 등록 또는 인증을 수행하는 단계를 더 포함한다.

[0216] 108. 임의의 선행하는 실시예들의 방법은, 기능하는 TPM이 사용자들의 플랫폼에 의해 바인딩되는 경우, 사용자의 장치 또는 플랫폼에 상주하는 TPM에 의해 TPM의 비밀성(confidentiality), 무결성, 확실성(authenticity)에 대한 사용자 또는 사용자 장치의 인증 및 ID에 관련된 데이터를 암호적으로 보호하는 단계를 더 포함한다.

[0217] 109. 실시예 108의 방법에서, TPM은 물리적으로 보호된 바운더리를 제공함으로써 TPM이 암호적으로 보호하고 저장한 데이터에 대한 고유 보안성(inherent security)을 제공한다.

[0218] 110. 실시예 108 또는 실시예 109의 방법은 애플리케이션 보안 구성요소와 IP 스택 보안 구성요소에, 높은 엔트로피 패스워드들을 포함한 보안 크리덴셜들이 제공되도록 USIM 기능을 확장하는 단계를 더 포함한다.

[0219] 111. 실시예 110의 방법에서, 애플리케이션 보안 구성요소는 DRM 및 PGP 서비스 구성요소를 포함한다.

[0220] 112. 실시예 110 또는 실시예 111의 방법에서, IP 스택 보안 구성요소는 IPSec 또는 TLS 또는 이들 양쪽 모두를 포함한다.

[0221] 113. 실시예 108 내지 실시예 110 중 어느 한 실시예의 방법에서, USIM 내에 통합된 TPM 내에서 리프레쉬되는 패스워드 및/또는 암호 키들의 정책 기초 자동 업데이트하는 단계를 더 포함한다.

[0222] 114. 실시예 108 내지 실시예 110 중 어느 한 실시예의 방법은 TLS 및 애플리케이션 보안에 요구되는 인증 알고리즘을 포함하도록 USIM 기능을 확장하는 단계를 더 포함한다.

도면의 간단한 설명

[0049] 첨부한 도면과 결합하여 이해되고 예를 들어 주어진 바람직한 실시예의 다음 설명으로부터 본 발명의 보다 자세한 이해가 이루어질 것이다.

[0050] 도 1은 종래 기술에 따른 WTRU에 대한 웹-SSO의 예시적인 흐름도이다.

[0051] 도 2는 종래 기술에 따른 리버티 얼라이언스 ID-FF 탑재 WTRU를 웹-SSO 프로세스하기 위한 예시적인 흐름도이다.

[0052] 도 3은 SAML 구성요소 간에 관계들의 블록도를 나타낸다.

[0053] 도 4는 SSO에서의 SP-개시된 포스트-포스트 바인딩의 일례를 나타낸다.

[0054] 도 5는 일반 TPM의 블록도를 나타낸다.

[0055] 도 6은 TPM AIK들을 이용하여 외부 참여자에 의한 AIK 크리덴셜 검증을 위한 예시적인 처리를 나타낸다.

[0056] 도 7은 TPM 및 TSS 내의 서로 다른 계층들의 블록도이다.

[0057] 도 8은 무선 통신 시스템의 예시적인 블록도이다.

[0058] 도 9는 TPM/TSS를 이용한 안전 자동화된 사인온의 일 실시예의 예시적인 흐름도이다.

[0059] 도 10은 TPM/TSS와 장치 트러스트 미러를 이용한 안전 자동화된 사인온의 일 실시예의 다른 예시적인 흐름도이다.

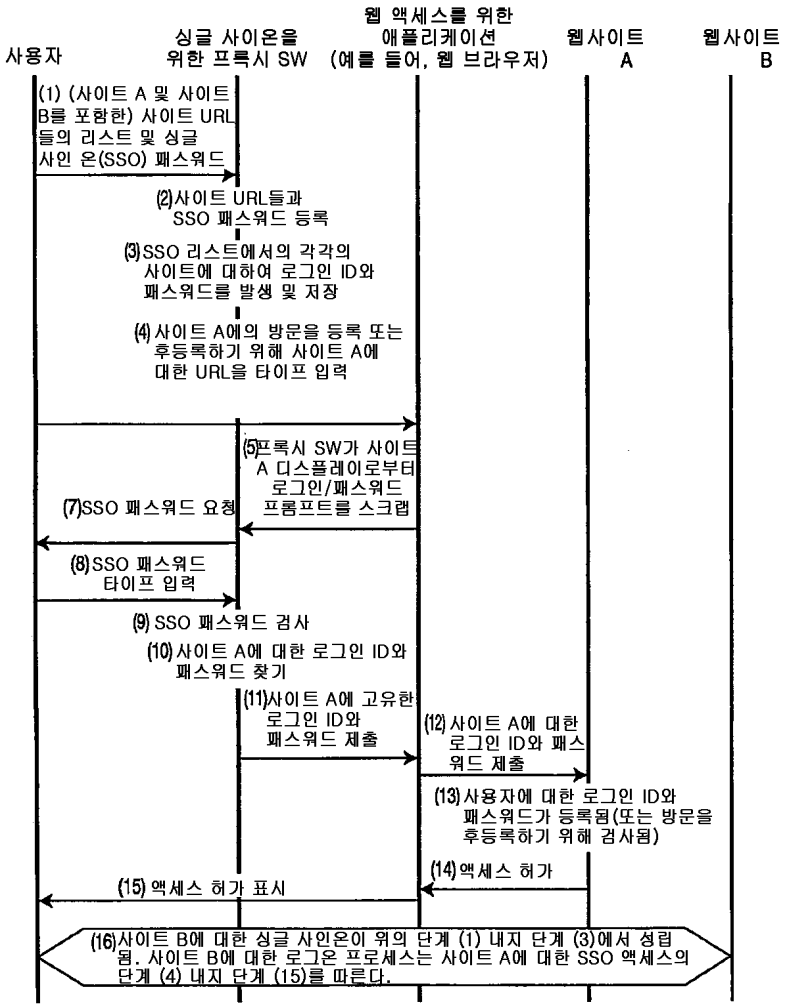
[0060] 도 11은 TPM을 이용한 그룹형태(group-wise) 패스워드에 기초한 TPM/TSS를 이용한 웹 액세스에 대한 SSO의 일 실시예의 예시적인 흐름도이다.

[0061] 도 12는 리버티 얼라이언스 ID-FF를 이용한 무선 통신 시스템의 예시적인 블록도이다.

[0062] 도 13은 리버티 얼라이언스 ID-FF를 이용한 TPM/TSS 보호 웹-SSO의 일 실시예의 예시적인 흐름도이다.

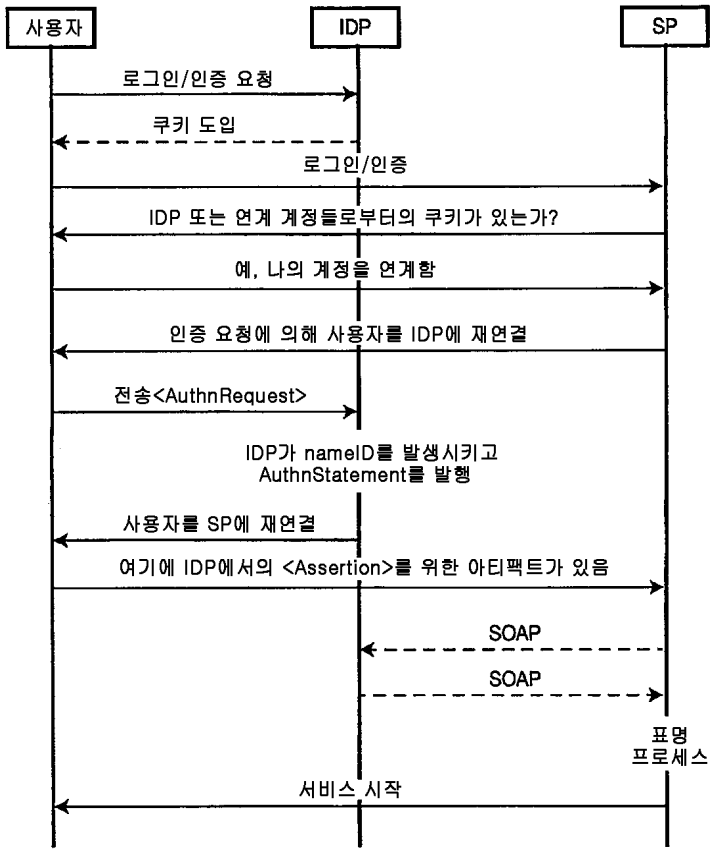
도면

도면1


사용자
싱글 사이온을 위한 프록시 SW
웹 액세스를 위한 애플리케이션 (예를 들어, 웹 브라우저)
웹사이트 A
웹사이트 B
(1) (사이트 A 및 사이트 B를 포함한) 사이트 URL들의 리스트 및 싱글 사인 온(SSO) 패스워드
(2)사이트 URL들과 SSO 패스워드 등록
(3)SSO 리스트에서의 각각의 사이트에 대하여 로그인 ID와 패스워드를 발생 및 저장
(4)사이트 A에의 방문을 등록 또는 후등록하기 위해 사이트 A에 대한 URL을 타이프 입력
(5)프록시 SW가 사이트 A 디스플레이로부터 로그인/패스워드 프롬프트를 스크랩
(7)SSO 패스워드 요청
(8)SSO 패스워드 타이프 입력
(9) SSO 패스워드 검사
(10)사이트 A에 대한 로그인 ID와 패스워드 찾기
(11)사이트 A에 고유한 로그인 ID와 패스워드 제출
(12)사이트 A에 대한 로그인 ID와 패스워드 제출
(13)사용자에 대한 로그인 ID와 패스워드가 등록됨(또는 방문을 후등록하기 위해 검사됨)
(14)액세스 허가
(15) 액세스 허가 표시
(16)사이트 B에 대한 싱글 사인온이 위의 단계 (1) 내지 단계 (3)에서 성립됨. 사이트 B에 대한 로그온 프로세스는 사이트 A에 대한 SSO 액세스의 단계 (4) 내지 단계 (15)를 따른다.

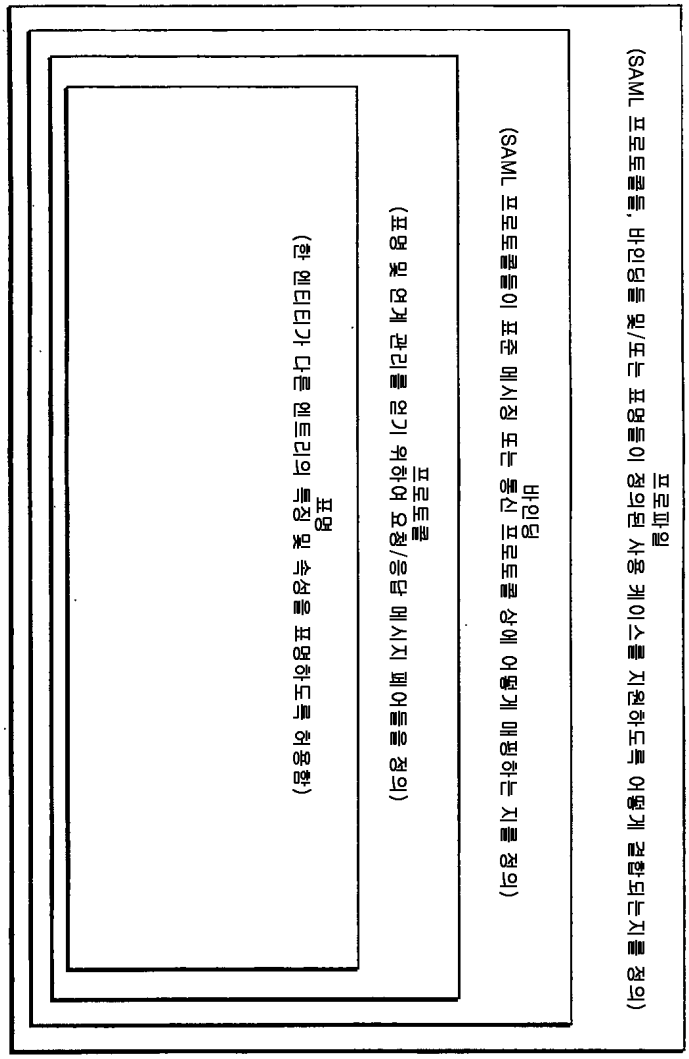
종래기술

도면2

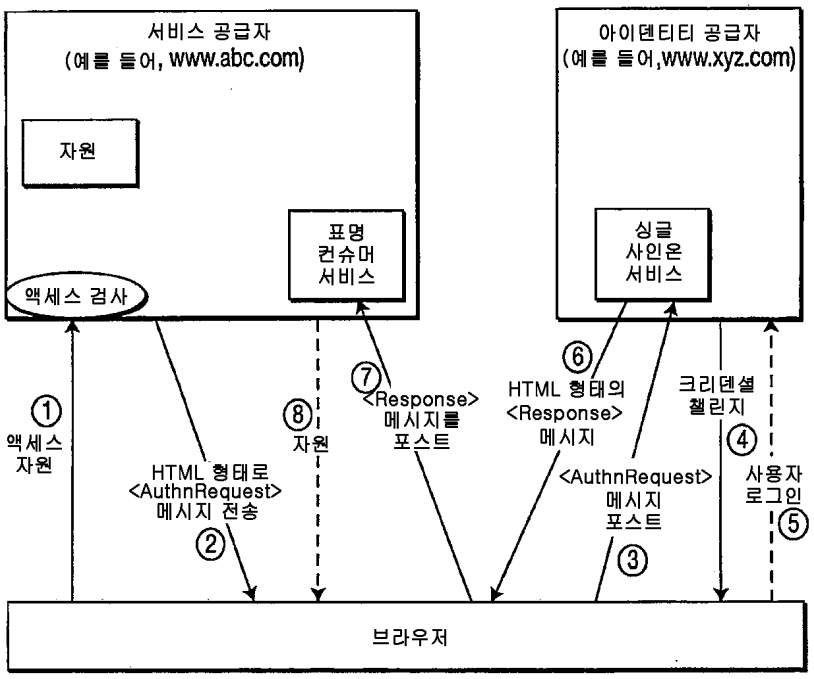

사용자
IDP
SP
로그인/인증 요청
쿠키 도입
로그인/인증
IDP 또는 연계 계정들로부터의 쿠키가 있는가?
예, 나의 계정을 연계함
인증 요청에 의해 사용자를 IDP에 재연결
전송<AuthnRequest>
IDP가 nameID를 발생시키고
AuthnStatement를 발행
사용자를 SP에 재연결
여기에 IDP에서의 <Assertion>를 위한 아티팩트가 있음
SOAP
SOAP
표명
프로세스
서비스 시작

종래기술

도면3

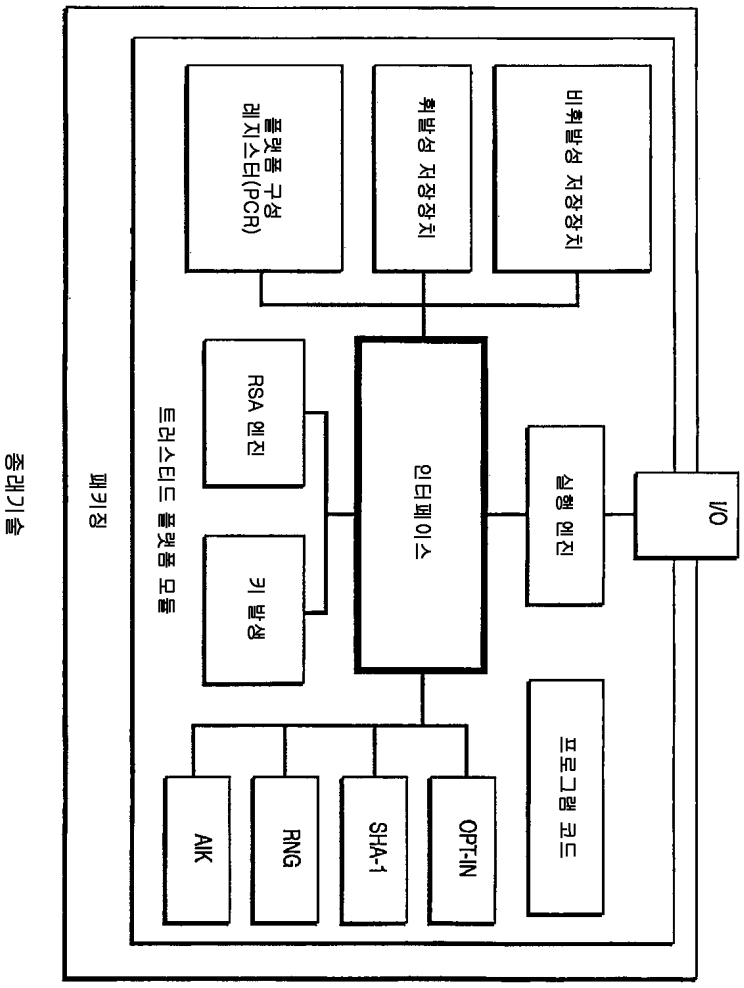

프로파일
(SAML 프로토콜들, 바인딩들 및/또는 표명들이 정의된 사용 케이스를 지원하도록 어떻게 결합되는지를 정의)
바인딩
(SAML 프로토콜들이 표준 메시징 또는 통신 프로토콜 상에 어떻게 매핑하는 지를 정의)
프로토콜
(표명 및 연계 관리를 얻기 위한 요청/응답 메시지 페어들을 정의)
표명
(한 엔티티가 다른 엔트리의 특징 및 속성을 표명하도록 허용함)
종래기술

도면4

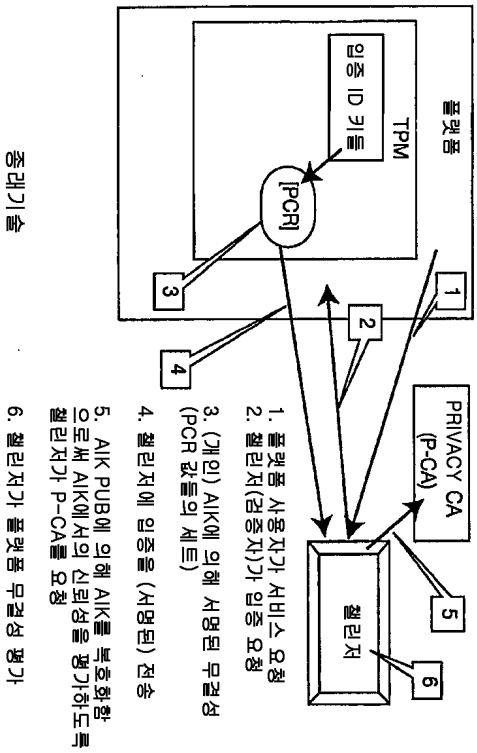

서비스 공급자
(예를 들어, www.abc.com)
자원
표명
컨슈머
서비스
액세스 검사
아이덴티티 공급자
(예를 들어,www.xyz.com)
싱글
사인온
서비스
① 액세스 자원
HTML 형태로 <AuthnRequest> 메시지 전송
②
⑧ 자원
⑦ <Response> 메시지를 포스트
⑥ HTML 형태의 <Response> 메시지
<AuthnRequest> 메시지 포스트
③
크리덴셜 챌린지
④
사용자 로그인
⑤
브라우저

종래기술

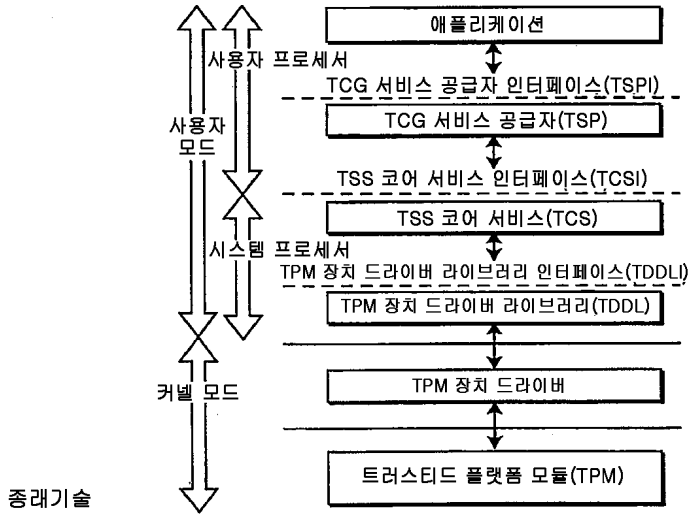
도면5


종래기술
패키징
트러스티드 플랫폼 모듈
플랫폼 구성 레지스터(PCR)
휘발성 저장장치
비휘발성 저장장치
RSA 엔진
키 발생
인터페이스
실행 엔진
I/O
AIK
RNG
SHA-1
OPT-IN
프로그램 코드

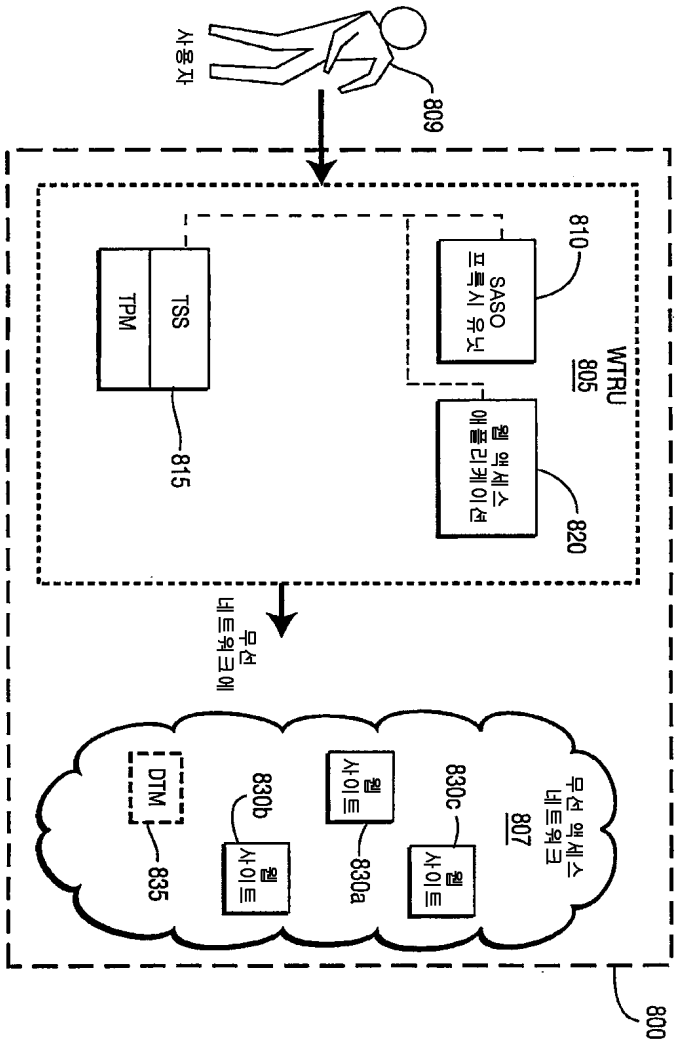
도면6


종래기술
플랫폼
TPM
입증 ID 키들
[PCR]
PRIVACY CA
(P-CA)
챌리저
1
2
3
4
5
6
1. 플랫폼 사용자가 서비스 요청
2. 챌리저(검증자)가 입증 요청
3. (개인) AIK에 의해 서명된 무결성
(PCR 값들의 세트)
4. 챌리저에 입증을 (서명된) 전송
5. AIK PUB에 의해 AIK를 복호화함
으로써 AIK에서의 신뢰성을 평가하도록
챌리저가 P-CA를 요청
6. 챌리저가 플랫폼 무결성 평가

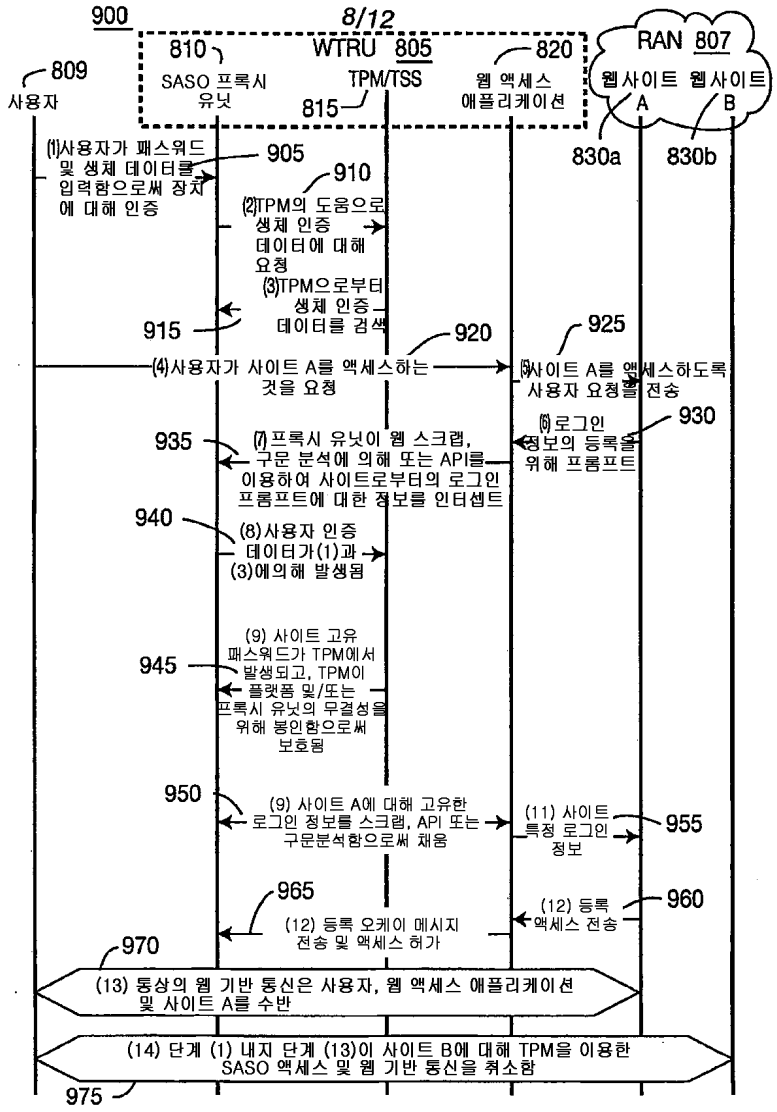
도면7


종래기술
사용자 모드
커널 모드
사용자 프로세서
시스템 프로세서
애플리케이션
TCG 서비스 공급자 인터페이스(TSPI)
TCG 서비스 공급자(TSP)
TSS 코어 서비스 인터페이스(TCSI)
TSS 코어 서비스(TCS)
TPM 장치 드라이버 라이브러리 인터페이스(TDDLI)
TPM 장치 드라이버 라이브러리(TDDL)
TPM 장치 드라이버
트러스티드 플랫폼 모듈(TPM)

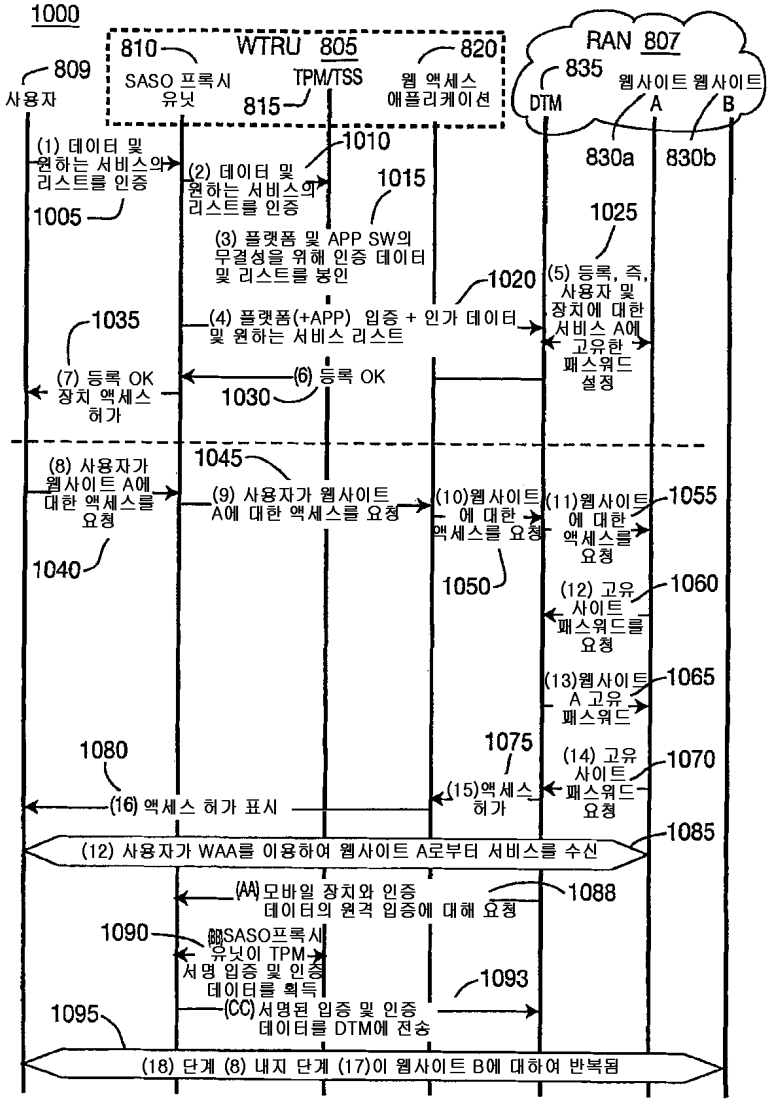
도면8


사용자
809
WTRU
805
SASO
프록시 유닛
810
TSS
TPM
815
웹 액세스
애플리케이션
820
무선
네트워크에
무선 액세스
네트워크
807
DTM
835
웹
사이트
830b
웹
사이트
830a
웹
사이트
830c
800

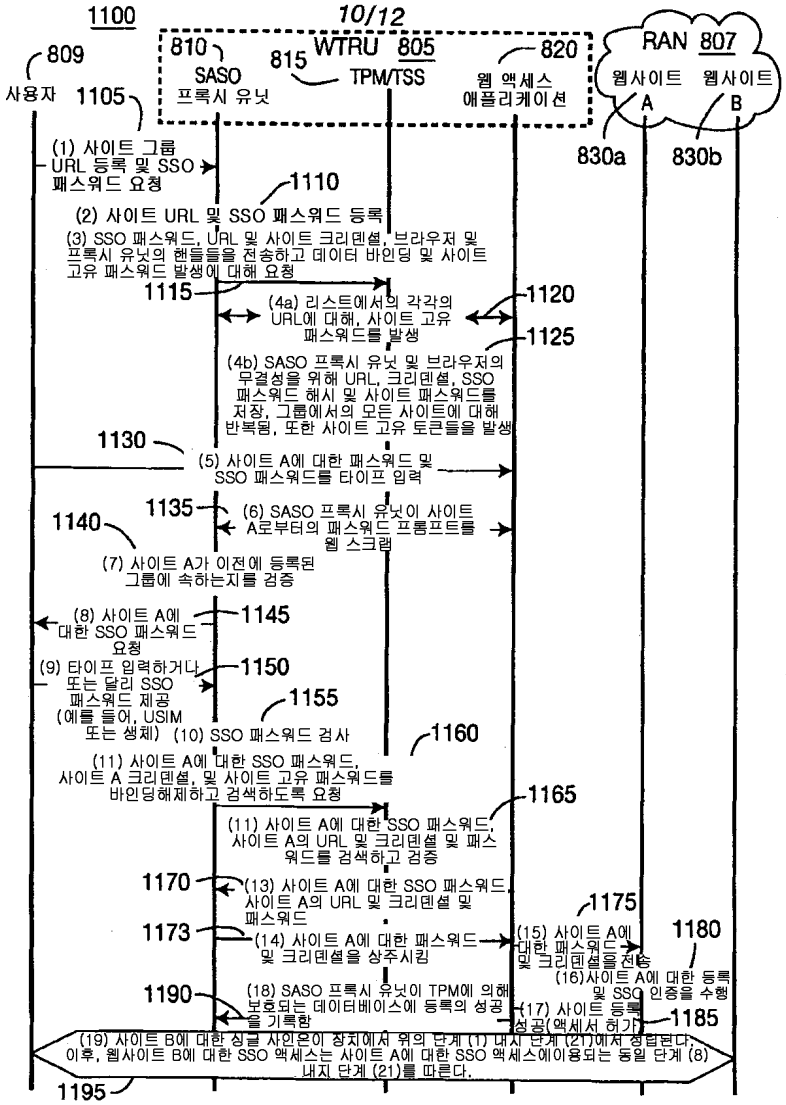
도면9


900
8/12
WTRU 805
810
SASO 프록시 유닛
TPM/TSS
815
820
웹 액세스 애플리케이션
RAN 807
웹사이트 A
웹사이트 B
830a
830b
809
사용자
(1)사용자가 패스워드 및 생체 데이터를 입력함으로써 장치에 대해 인증
905
910
(2)TPM의 도움으로 생체 인증 데이터에 대해 요청
(3)TPM으로부터 생체 인증 데이터를 검색
915
920
925
(4)사용자가 사이트 A를 액세스하는 것을 요청
(5)사이트 A를 액세스하도록 사용자 요청을 전송
(6)로그인 정보의 등록을 위해 프롬프트
930
935
(7)프록시 유닛이 웹 스크랩, 구문 분석에 의해 또는 API를 이용하여 사이트로부터의 로그인 프롬프트에 대한 정보를 인터셉트
940
(8)사용자 인증 데이터가 (1)과 (3)에의해 발생됨
(9) 사이트 고유 패스워드가 TPM에서 발생되고, TPM이 플랫폼 및/또는 프록시 유닛의 무결성을 위해 봉인함으로써 보호됨
945
950
(9) 사이트 A에 대해 고유한 로그인 정보를 스크랩, API 또는 구문분석함으로써 채움
(11) 사이트 특정 로그인 정보
955
960
(12) 등록 액세스 전송
965
(12) 등록 오케이 메시지 전송 및 액세스 허가
970
(13) 통상의 웹 기반 통신은 사용자, 웹 액세스 애플리케이션 및 사이트 A를 수반
(14) 단계 (1) 내지 단계 (13)이 사이트 B에 대해 TPM을 이용한 SASO 액세스 및 웹 기반 통신을 취소함
975

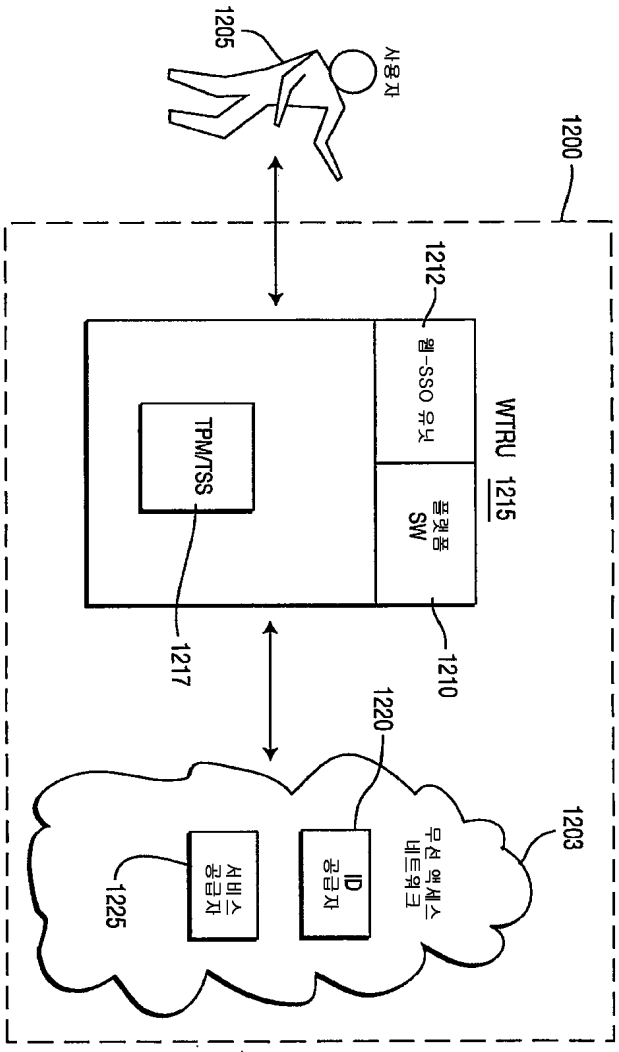
도면10


1000
WTRU 805
810
SASO 프록시 유닛
815
TPM/TSS
820
웹 액세스 애플리케이션
RAN 807
835
DTM
웹사이트 A
웹사이트 B
830a
830b
809
사용자
(1) 데이터 및 원하는 서비스의 리스트를 인증
1005
(2) 데이터 및 원하는 서비스의 리스트를 인증
1010
1015
(3) 플랫폼 및 APP SW의 무결성을 위해 인증 데이터 및 리스트를 봉인
1020
(4) 플랫폼(+APP) 입증 + 인가 데이터 및 원하는 서비스 리스트
1025
(5) 등록, 즉, 사용자 및 장치에 대한 서비스 A에 고유한 패스워드 설정
1030
(6) 등록 OK
1035
(7) 등록 OK 장치 액세스 허가
1040
(8) 사용자가 웹사이트 A에 대한 액세스를 요청
1045
(9) 사용자가 웹사이트 A에 대한 액세스를 요청
1050
(10)웹사이트에 대한 액세스를 요청
1055
(11)웹사이트에 대한 액세스를 요청
1060
(12) 고유 사이트 패스워드를 요청
1065
(13)웹사이트 A 고유 패스워드
1070
(14) 고유 사이트 패스워드 요청
1075
(15)액세스 허가
1080
(16) 액세스 허가 표시
1085
(12) 사용자가 WAA를 이용하여 웹사이트 A로부터 서비스를 수신
1088
(AA) 모바일 장치와 인증 데이터의 원격 입증에 대해 요청
1090
(BB) SASO프록시 유닛이 TPM 서명 입증 및 인증 데이터를 획득
1093
(CC) 서명된 입증 및 인증 데이터를 DTM에 전송
1095
(18) 단계 (8) 내지 단계 (17)이 웹사이트 B에 대하여 반복됨

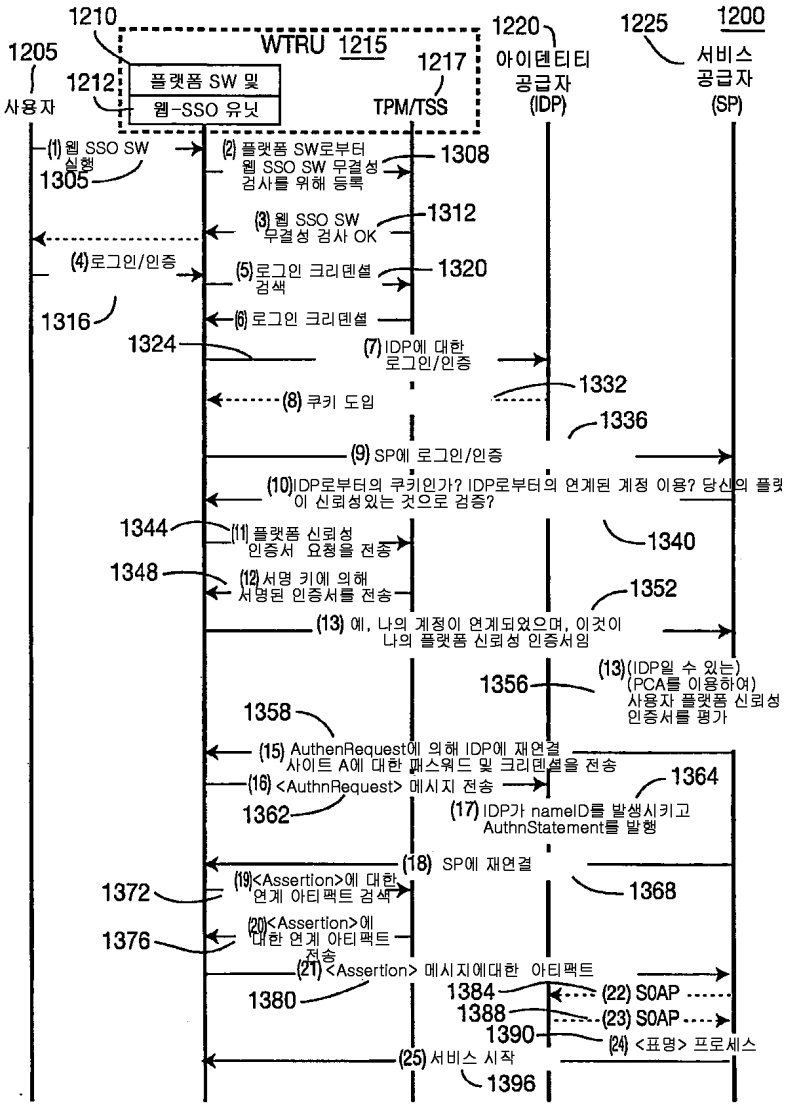
도면11


1100
10/12
809
사용자
1105
810
SASO
프록시 유닛
815
WTRU 805
TPM/TSS
820
웹 액세스
애플리케이션
RAN 807
웹사이트 A
웹사이트 B
830a
830b
(1) 사이트 그룹 URL 등록 및 SSO 패스워드 요청
1110
(2) 사이트 URL 및 SSO 패스워드 등록
(3) SSO 패스워드, URL 및 사이트 크리덴셜, 브라우저 및 프록시 유닛의 핸들들을 전송하고 데이터 바인딩 및 사이트 고유 패스워드 발생에 대해 요청
1115
1120
(4a) 리스트에서의 각각의 URL에 대해, 사이트 고유 패스워드를 발생
1125
(4b) SASO 프록시 유닛 및 브라우저의 무결성을 위해 URL, 크리덴셜, SSO 패스워드 해시 및 사이트 패스워드를 저장, 그룹에서의 모든 사이트에 대해 반복됨, 또한 사이트 고유 토큰들을 발생
1130
(5) 사이트 A에 대한 패스워드 및 SSO 패스워드를 타이프 입력
1135
(6) SASO 프록시 유닛이 사이트 A로부터의 패스워드 프롬프트를 웹 스크랩
1140
(7) 사이트 A가 이전에 등록된 그룹에 속하는지를 검증
(8) 사이트 A에 대한 SSO 패스워드 요청
1145
(9) 타이프 입력하거나 또는 달리 SSO 패스워드 제공 (예를 들어, USIM 또는 생체)
1150
1155
(10) SSO 패스워드 검사
1160
(11) 사이트 A에 대한 SSO 패스워드, 사이트 A 크리덴셜, 및 사이트 고유 패스워드를 바인딩해제하고 검색하도록 요청
1165
(11) 사이트 A에 대한 SSO 패스워드, 사이트 A의 URL 및 크리덴셜 및 패스워드를 검색하고 검증
1170
(13) 사이트 A에 대한 SSO 패스워드, 사이트 A의 URL 및 크리덴셜 및 패스워드
1175
1173
(14) 사이트 A에 대한 패스워드 및 크리덴셜을 상주시킴
(15) 사이트 A에 대한 패스워드 및 크리덴셜을 전송
1180
(16)사이트 A에 대한 등록 및 SSO 인증을 수행
1190
(18) SASO 프록시 유닛이 TPM에 의해 보호되는 데이터베이스에 등록의 성공을 기록함
(17) 사이트 등록 성공(액세서 허가)
1185
(19) 사이트 B에 대한 싱글 사인온이 장치에서 위의 단계 (1) 내지 단계 (21)에서 성립된다. 이후, 웹사이트 B에 대한 SSO 액세스는 사이트 A에 대한 SSO 액세스에이용되는 동일 단계 (8) 내지 단계 (21)를 따른다.
1195

도면12


1205
사용자
1200
1212
웹-SSO 유닛
WTRU 1215
TPM/TSS
플랫폼 SW
1217
1210
1220
1203
무선 액세스 네트워크
ID 공급자
서비스 공급자
1225

도면13


1210
WTRU 1215
1205
사용자
1212
플랫폼 SW 및
웹-SSO 유닛
1217
TPM/TSS
1220
아이덴티티
공급자
(IDP)
1225
서비스
공급자
(SP)
1200
(1) 웹 SSO SW 실행
1305
(2) 플랫폼 SW로부터 웹 SSO SW 무결성 검사를 위해 등록
1308
(3) 웹 SSO SW 무결성 검사 OK
1312
(4) 로그인/인증
(5) 로그인 크리덴셜 검색
1320
1316
(6) 로그인 크리덴셜
1324
(7) IDP에 대한 로그인/인증
1332
(8) 쿠키 도입
1336
(9) SP에 로그인/인증
(10) IDP로부터의 쿠키인가? IDP로부터의 연계된 계정 이용? 당신의 플랫
이 신뢰성있는 것으로 검증?
1344
(11) 플랫폼 신뢰성 인증서 요청을 전송
1340
1348
(12) 서명 키에 의해 서명된 인증서를 전송
1352
(13) 예, 나의 계정이 연계되었으며, 이것이 나의 플랫폼 신뢰성 인증서임
1356
(13) (IDP일 수 있는) (PCA를 이용하여) 사용자 플랫폼 신뢰성 인증서를 평가
1358
(15) AuthenRequest에 의해 IDP에 재연결 사이트 A에 대한 패스워드 및 크리덴셜을 전송
(16) <AuthnRequest> 메시지 전송
1364
1362
(17) IDP가 nameID를 발생시키고 AuthnStatement를 발행
(18) SP에 재연결
1368
1372
(19) <Assertion>에 대한 연계 아티팩트 검색
(20) <Assertion>에 대한 연계 아티팩트 전송
1376
(21) <Assertion> 메시지에대한 아티팩트
1380
1384
(22) SOAP
1388
(23) SOAP
1390
(24) <표명> 프로세스
(25) 서비스 시작
1396