(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년10월11일
(11) 등록번호 10-1071790
(24) 등록일자 2011년10월04일

(51) Int. Cl.
H04L 9/32 (2006.01) *G06F 21/20* (2006.01)
(21) 출원번호 10-2008-7028876
(22) 출원일자(국제출원일자) 2007년04월26일
심사청구일자 2009년03월19일
(85) 번역문제출일자 2008년11월26일
(65) 공개번호 10-2009-0017538
(43) 공개일자 2009년02월18일
(86) 국제출원번호 PCT/IB2007/051546
(87) 국제공개번호 WO 2007/135580
국제공개일자 2007년11월29일
(30) 우선권주장
06010468.4 2006년05월21일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
KR1020040080922 A
WO1995030292 A1
전체 청구항 수 : 총 10 항

(73) 특허권자
인터내셔널 비지네스 머신즈 코포레이션
미국 10504 뉴욕주 아몬크 뉴오차드 로드
(72) 발명자
그로스 토마스 알
스위스 씨에이치-8003 취리히 젠트랄스트라쎄 150
솜머 디터 엠
스위스 씨에이치-8038 취리히 엣첼스테이그 1
카메니쉬 장
스위스 씨에이치-8800 탈빌 인 루벤 7
(74) 대리인
신정건, 김태홍

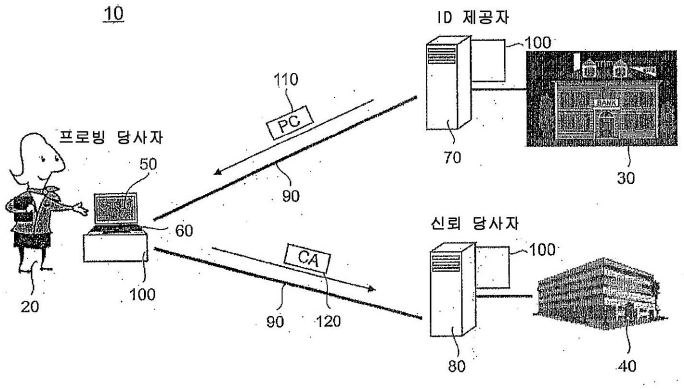
심사관 : 이형일

(54) 어써션 메세지 시그너처

(57) 요 약

본 발명은 프로빙 당사자(20)로부터 신뢰 당사자(40)로 어써션 메세지(200)를 제공하는 방법에 관한 것으로서, 상기 방법은: - 하나 이상의 스테이트먼트를 포함하는 어써션(A)을 생성하는 단계, - 어써션 증명(p_A)을 생성하는 단계, - 상기 어써션(A) 및 상기 어써션 증명(p_A)으로부터 임시 개인키 및 대응하는 임시 공개키(K)를 생성하는 단계, - 상기 임시 공개키(K)에 대한 키 증명(p_K)을 생성하는 단계, - 상기 임시 개인키에 의해 어써션 메세지 시그너처(S)를 생성하는 단계, - 상기 임시 공개키(K), 상기 어써션 증명(p_A), 상기 키 증명(p_K), 상기 어써션(A), 메세지 몸체(220) 및 상기 어써션 메세지 시그너처(S)를 포함하는 어써션 메세지(200)를 신뢰 당사자(40)에 생성하는 단계를 포함한다.

대 표 도



특허청구의 범위

청구항 1

프로빙 당사자(20)로부터 신뢰 당사자(40)로 어써션 메세지(200)를 제공하는 방법으로서,

- 하나 이상의 스테이트먼트(statement)를 포함하는 어써션(assertion; A)을 생성하는 단계,

- 어써션 증명(p_A)을 생성하는 단계,

- 상기 어써션(A) 및 상기 어써션 증명(p_A)으로부터 임시 개인키 및 대응하는 임시 공개키(K)를 생성하는 단계,

- 상기 임시 공개키(K)에 대한 키 증명(p_K)을 생성하는 단계,

- 상기 임시 개인키에 의해 어써션 메세지 시그너처(S)를 생성하는 단계,

- 상기 임시 공개키(K), 상기 어써션 증명(p_A), 상기 키 증명(p_K), 상기 어써션(A), 메세지 몸체(220) 및 상기 어써션 메세지 시그너처(S)를 포함하는 어써션 메세지(200)를 생성하는 단계

를 포함하는 어써션 메세지를 제공하는 방법.

청구항 2

제 1 항에 있어서, 상기 임시 개인키, 상기 임시 공개키(K) 및 상기 키 증명(p_K)은 보안 결합 함수에 의해 생성이 되는 것인 어써션 메세지를 제공하는 방법.

청구항 3

제 2 항에 있어서, 상기 보안 결합 함수는 입증가능 랜덤 함수(verifiable random function)인 것인 어써션 메세지를 제공하는 방법.

청구항 4

제 1 항에 있어서, 상기 어써션 메세지 시그너처(S)를 생성하는 단계는,

상기 어써션 메세지의 하나 이상의 부분들의 어써션 메세지 다이제스트를 생성하는 단계, 및

상기 임시 개인키에 의해 상기 어써션 메세지 다이제스트로부터 상기 어써션 메세지 시그너처(S)를 생성하는 단계를 포함하는 것인 어써션 메세지를 제공하는 방법.

청구항 5

제 1 항에 있어서, 상기 어써션 메세지 시그너처(S)는 엔벨로프(enveloped) 시그너처인 것인 어써션 메세지를 제공하는 방법.

청구항 6

제 1 항에 있어서, 상기 어써션 증명(p_A) 및 상기 키 증명(p_K) 중 적어도 하나는 무정보 증명(zero knowledge proof) 및 최소 공개 증명(minimum disclosure proof) 중 적어도 하나인 것인 어써션 메세지를 제공하는 방법.

청구항 7

하나 이상의 스테이트먼트를 갖는 어써션(A), 상기 어써션(A)에 대한 어써션 증명(p_A), 상기 어써션(A)과 상기 어써션 증명(p_A)으로부터 생성된 임시 공개키(K), 상기 임시 공개키(K)에 대한 키 증명(p_K), 메세지 몸체(220) 및 어써션 메세지 시그너처(S)를 포함하는 어써션 메세지(200)를 평가하기 위한 방법에 있어서,

- 상기 키 증명(p_K)에 의해 상기 임시 공개키(K)를 검사하는 단계,

- 상기 어써션 증명(p_A)에 의해 상기 어써션(A)을 검사하는 단계,

- 상기 임시 공개키(K)에 의해 상기 어써션 메세지 시그너처(S)를 검사하는 단계,

- 상기 어써션 메세지 시그너처(S), 상기 임시 공개키(K) 및 상기 어써션(A)의 검사 결과 유효한 경우 상기 어써션 메세지(200)를 유효한 것으로서 평가하는 단계

를 포함하는 어써션 메세지 평가 방법.

청구항 8

프로빙 당사자(20)로부터 신뢰 당사자(40)로 어써션 메세지(200)를 송신하는 송신 장치(60)에 있어서,

하나 이상의 스테이트먼트를 포함하는 어써션(A)을 생성하고, 어써션 증명(p_A)을 생성하고, 상기 어써션(A)과 상기 어써션 증명(p_A)으로부터 임시 개인키와 대응 임시 공개키(K)를 생성하고, 상기 임시 공개키(K)에 대한 키 증명(p_K)을 생성하며, 상기 임시 개인키에 의해 어써션 메세지 시그너처(S)를 생성하는 프로세서; 및

상기 임시 공개키(K), 상기 어써션 증명(p_A), 상기 키 증명(p_K), 상기 어써션, 메세지 몸체(220) 및 상기 어써션 메세지 시그너처(S)를 포함하는 상기 어써션 메세지(200)를 상기 신뢰 당사자(40)에 보내는 송신 컴포넌트

를 포함하는 송신 장치.

청구항 9

하나 이상의 스테이트먼트를 갖는 어써션(A), 상기 어써션(A)에 대한 어써션 증명(p_A), 상기 어써션(A)과 상기 어써션 증명(p_A)으로부터 생성된 임시 공개키(K), 상기 임시 공개키(K)에 대한 키 증명(p_K), 메세지 몸체(220) 및 어써션 메세지 시그너처(S)를 포함하는 어써션 메세지(200)를 프로빙 당사자로부터 수신하는 수신 장치(80)에 있어서,

상기 어써션 메세지를 수신하고, 상기 어써션 메세지를 처리를 위해 프로세서에 제공하는 수신 컴포넌트; 및

상기 키 증명(p_K)에 의해 상기 임시 공개키(K)를 검사하고, 상기 어써션 증명(p_A)에 의해 상기 어써션(A)을 검사하고, 상기 임시 공개키(K)에 의해 상기 어써션 메세지 시그너처(S)를 검사하며, 상기 어써션 메세지 시그너처(S), 상기 임시 공개키(K) 및 상기 어써션(A)의 검사 결과 유효한 경우 상기 어써션 메세지(200)를 유효한 것으로서 평가하는 프로세서

를 포함하는 수신 장치.

청구항 10

시스템에 있어서,

프로빙 당사자(20)로부터 신뢰 당사자(40)로 어써션 메세지(200)를 송신하는 송신 장치(60), 및

상기 프로빙 당사자로부터 상기 어써션 메세지를 수신하는 수신 장치(80)를 포함하고,

상기 송신 장치는,

하나 이상의 스테이트먼트를 포함하는 어써션(A)을 생성하고, 어써션 증명(p_A)을 생성하고, 상기 어써션(A)과 상기 어써션 증명(p_A)으로부터 임시 개인키와 대응 임시 공개키(K)를 생성하고, 상기 임시 공개키(K)에 대한 키 증명(p_K)을 생성하며, 상기 임시 개인키에 의해 어써션 메세지 시그너처(S)를 생성하는 프로세서; 및

상기 임시 공개키(K), 상기 어써션 증명(p_A), 상기 키 증명(p_K), 상기 어써션, 메세지 몸체(220) 및 상기 어써션 메세지 시그너처(S)를 포함하는 상기 어써션 메세지(200)를 상기 신뢰 당사자(40)에 보내는 송신 컴포넌트를 포함하고,

상기 수신 장치는,

상기 어써션 메세지를 수신하고, 상기 어써션 메세지를 처리를 위해 프로세서에 제공하는 수신 컴포넌트; 및

상기 키 증명(p_K)에 의해 상기 임시 공개키(K)를 검사하고, 상기 어써션 증명(p_A)에 의해 상기 어써션(A)을 검사하고, 상기 임시 공개키(K)에 의해 상기 어써션 메세지 시그너처(S)를 검사하며, 상기 어써션 메세지 시그너처(S), 상기 임시 공개키(K) 및 상기 어써션(A)의 검사 결과 유효한 경우 상기 어써션 메세지(200)를 유효한 것으로서 평가하는 프로세서를 포함하는 것인, 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 어써션 메세지를 프로빙 당사자로부터 신뢰 당사자에게 제공하기 위한 방법, 시스템, 송신 엔티티, 수신 엔티티, 컴퓨터 프로그램, 신호 및 어써션 메세지 포맷에 관한 것이다.

배 경 기 술

[0002] 사용자는 인터넷을 브라우징하거나 기타 유형의 전자거래를 수행할 시에 자신의 프라이버시에 대해 더욱 더 염려하게 된다. 이에 따라, 사용자의 ID(identity)의 안전하고 개선된 관리에 대한 요구가 커져만 가고 있다. 최광의의 ID 관리란 적어도 개인의 모든 디지털 관련사항을 포함하여, 개인에 관한 모든 개인 정보의 관리를 의미한다. 영업의 측면에서 보면, 예컨대, 사용자 관리 비용의 감축 및 전자 영업의 총체적 생산 증대가 있다. ID 관리는 인터넷과 웹 표준과 같은 표준이 거의 모든 당사자들에게 이익을 줄 수 있는 인프라구조 문제이다. 오늘날의 대부분의 중요 온라인 거래는 사용자로 하여금 자신의 ID 또는 일정한 속성을 서비스 제공자에게 제공할 것을 요구한다. 보급된 접근법으로서 사용자가 비인증된 속성을 웹 형식내에 기입하는 경우, 이것은 서비스 제공자가 영업 프로세스 자체에서 필요로 하는 것 보다 많은 속성들을 요청할 것임을 암시해준다. 서비스 제공자는 제공된 속성의 일치성을 검사하기 위해 추가적인 정보를 이용한다.

[0003] 연합 ID 관리(Federated identity management; FIM) 프로토콜은 이러한 접근법에 비해 다수의 장점을 갖는다. 서비스 제공자는 필요로 하는 속성을 정확하게 획득하고 이러한 속성을 신뢰된 ID 제공자에 의해 인증받는다. FIM 프로토콜은 사용자를 대리하여 동작하는 요청자를 ID 제공자에게 보내어 서비스 제공자에 의해 요청된 속성에 관한 크레덴셜(credential)을 사용자가 확증하고 획득하는 방식을 따른다. FIM 접근법은 데이터 최소화 원리, 즉 오로지 서비스에서 필요로 하는 사용자 데이터만을 전송하는 원리를 따름으로써 사용자의 프라이버시를 향상시킬 수 있다. FIM 접근법은 사용자의 속성과 프라이버시의 보호라는 측면에서 장점을 갖는 폭넓게 배치된 표준화된 프로토콜이다.

[0004] 익명 크레덴셜 시스템은 ID 관리 및 속성 교환에 대한 훨씬 강력한 방법을 제공한다. 이러한 개념은 "Security without identification: Transaction systems to make big brother obsolete. Communications of theACM, 28(10):1030.1044, Oct. 1985."에서 D. Chaum에 의해 소개되었다. 익명 크레덴셜 시스템의 중요 특성은 익명 크레덴셜에 관한 발행 거래는 자체적인 표시 거래와 링크되지 않는다라는 점이다. 이것은 사용자로 하여금 익명 크레덴셜을 비밀로 유지할 수 있게 해주고 신뢰 당사자측에게 인증된 속성 데이터를 제공하기 위해 이 익명 크레덴셜을 여러번 사용할 수 있도록 해준다. 개선된 익명 크레덴셜 시스템은 "J. Camenisch and A. Lysyanskaya, Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation, in B. Pfitzmann, editor, Advances in Cryptology, EUROCRYPT 2001, volume 2045 of LNCS, pages 93.118. Springer Verlag, 2001."에서 개시되고 있다. 이 개선된 익명 크레덴셜 시스템은 심지어 동일 크레덴셜의 다수의 표시들도 서로 링크되지 않도록 해준다. 이 시스템은 사용자로 하여금 단일 크레덴셜내에 저장된 ID 속성에 관련된 스테이트먼트를 선택적으로 표시할 수 있게 해주고, 보다 차별화된 속성들과, 이러한 속성들에 대한 임의적 논리 공식의 표시와, 그리고 입증가능한 암호화된 속성과 속성의 암호 서약의 통합을 지원할 수 있도록 해주는 소위 말하는 개인 인증서 시스템으로 한층 일반화되었다. 속성을 이러한 시스템으로 어서팅하는 경우, ID 제공자는 거래에 관여할 필요가 없다. 사용자는 자신의 개인 인증서들을 사전에 획득하고 이들을 국지적으로 저장한다. 사용자가 인증된 속성을 서비스 제공자에게 제공하기를 원할 때마다 사용자는 하나 이상의 개인 인증서들을 사용하여 자신의 개인 인증서내의 속성에 대한 논리 공식을 표시하기 위한 새로운 증명을 생성시킨다.

[0005] 상술한 일반화된 시스템은 정보의 무정보 증명(zero-knowledge proofs)에 기초된 것이다. 현재의 시그너처 표준, 특히 안정적으로 잘 구축된 XML 시그너처를 위한 표준(Donald Eastlake, Joseph Reagle, David Solo (eds.): XML-Signature Syntax and Processing, W3C Recommendation, 2002, http://www.w3.org/TR/xmldsig-core/ 로부터 입수가능)과 같은 공개키 시그너처 표준은 무정보 증명과 호환되지 않는다. 하지만, XML-시그너처는 대부분의 FIM과 웹 서비스(WS)-보안 프레임워크의 기초가 된다.

[0006] 본 발명의 목적은 ID 관리를 위한 개선된 해결책을 제공하는 것이다.

발명의 상세한 설명

[0007] 본 발명은 독립 청구항들에서 정의된 바와 같은 방법, 시스템, 송신 엔티티, 수신 엔티티, 컴퓨터 프로그램, 신호 및 어써션 메세지 포맷에 관한 것이다. 본 발명의 추가적인 실시예들은 부가된 종속 청구항들에서 제공된다.

[0008] 본 발명의 하나의 실시모습에 따르면, 프로빙 당사자로부터 신뢰 당사자에 어써션 메세지를 제공하는 방법으로서:

[0009] - 하나 이상의 스테이트먼트(statement)를 포함하는 어써션(assertion)을 생성하는 단계,

[0010] - 어써션 증명을 생성하는 단계,

[0011] - 어써션 및 어써션 증명으로부터 임시 개인키 및 대응하는 임시 공개키를 생성하는 단계,

[0012] - 임시 공개키에 대한 키 증명을 생성하는 단계,

[0013] - 임시 개인키에 의해 어써션 메세지 시그너처를 생성하는 단계,

[0014] - 임시 공개키, 어써션 증명, 키 증명, 어써션, 메세지 몸체 및 어써션 메세지 시그너처를 포함하는 어써션 메세지를 생성하는 단계

[0015] 를 포함하는 어써션 메세지를 제공하는 방법이 제시된다.

[0016] 이러한 본 발명의 실시모습에 따른 방법에서, 임시 개인키와 임시 공개키의 키 쌍이 어써션과 어써션 증명으로부터 생성된다. 이것은 어써션과 어써션 증명을 메세지 몸체와 결합시킨다.

[0017] 어써션의 스테이트먼트는 프로빙 당사자의 임의의 속성과 관련이 있을 수 있다. 예를 들어, 스테이트먼트는 프로빙 당사자의 나이, 소재지, 국적 또는 신용 카드에 관한 정보와 같은 프로빙 당사자의 ID에 관한 정보를 포함할 수 있다. 프로빙 당사자의 속성에 관한 스테이트먼트는 논리 공식으로서 규정될 수 있다.

[0018] 전통적인 공개키 시그너처는 공개키 인증서를 시그너처와 함께 보내는 것을 필요로 한다. 이와 유사하게, 본 발명의 이러한 실시모습에 따라 어써션, 어써션 증명 및 임시 공개키는 전통적인 공개키 시그너처 방식의 공개키 인증서에 대응하는 것으로 간주될 수 있다.

[0019] 프로빙 당사자는 신뢰 당사자에게 자신의 속성에 관한 스테이트먼트를 제공할 것을 원하는 임의의 엔티티일 수 있다. 예를 들어, 프로빙 당사자는 인터넷과 같은 네트워크의 사용자일 수 있다. 이와 다른 경우에서, 프로빙 당사자는 자신에 관한 특성을 입증하는 하드웨어 장치이거나 또는 특성 증명에 의해 통신을 강화시키는 중간 당사자일 수 있다.

[0020] 어써션 증명은 어써션내에서 만들어진 스테이트먼트의 암호 증명을 제공한다. 어써션 증명에 의해, 어써션내에서 만들어진 스테이트먼트는 신뢰 당사자에 의해 검증될 수 있다.

[0021] 어써션은 명시적으로 표명하는 것 없이 어써션 증명에 의해 암시될 수 있다.

[0022] 신뢰 당사자는 프로빙 당사자에 관한 정보를 요청하는 임의의 엔티티일 수 있다. 예를 들어, 신뢰 당사자는 인터넷을 통해 서비스를 제공하는 서비스 제공자일 수 있다.

[0023] 어써션 메세지 시그너처는 임시 개인키에 의해 생성된다. 어써션 메세지 시그너처에 의해, 어써션과 어써션 증명은 메시지의 메세지 몸체에 안전하게 결합될 수 있다.

[0024] 최종적으로, 어써션 메세지는 어써션, 어써션 증명, 임시 공개키, 키 증명, 주 메세지 몸체 및 어써션 메세지 시그너처를 포함하면서 생성된다. 그 후, 어써션 메세지는 신뢰 당사자에게 보내질 수 있다.

[0025] 이러한 방법은 개인키/공개키 시그너처를 필요로 하는 방법 및 프로토콜에 의해 어써션과 대응 어써션 증명의 교환이 가능할 수 있도록 해주는 장점을 갖는다.

[0026] 본 발명의 실시예에 따르면, 임시 개인키, 임시 공개키 및 키 증명이 보안 결합 함수에 의해 생성된다.

[0027] 보안 결합 함수는 임시 개인키와 임시 공개키를 포함하는 임시 키 쌍이 어써션 증명과 어써션으로부터 의사적 랜덤방식으로, 랜덤방식으로, 또는 예측불가능 방식으로 생성되었다라는 검증을 가능하게 해주는 함수로서 이해된다. 다시 말하면, 보안 결합 함수는 임시 키 쌍 및 임시 키 쌍에 의해 생성된 어써션 메세지 시그너처를 각각

어써션과 어써션 증명에 결합시킨다. 다시 말하면, 보안 결합 함수는 임시 개인키를 생성하는데에 사용되고, 임시 개인키의 암호 규약으로서 사용되는 대응 임시 공개키에 대한 정확성 증명을 하는데에 사용된다.

[0028] 본 발명의 실시예에 따르면, 보안 결합 함수는 입증가능 랜덤 함수(verifiable random function)이다.

[0029] 입증가능 랜덤 함수는 모두에게 알려진 값에 입증가능 랜덤 함수를 적용함으로써 당사자로 하여금 보안값을 생성할 수 있도록 해준다. 입증가능 랜덤 함수의 수학적 구조는 보안값이 이에 따라 생성되었다라는 증명을 당사자가 생성할 수 있도록 해준다. 입증가능 랜덤 함수에 의해, 임시 개인키와 임시 공개키는 각각의 어써션 및 어써션 증명에 대해 의사적 랜덤방식으로 그리고 새롭게 생성된다.

[0030] 이러한 실시예에 따르면, 키 증명은 임시 키 쌍이 보안 결합 함수, 특히 입증가능 랜덤 함수를 어써션, 어써션 증명 및 (택일적 사항으로) 시간 스탬프와 같은 기타 입력 파라미터에 적용함으로써 생성되었음을 입증한다.

[0031] 본 발명의 이러한 실시모습의 실시예에 따르면, 어써션 메세지 시그너처는,

[0032] - 어써션 메세지의 하나 이상의 부분들의 어써션 메세지 다이제스트를 생성하는 단계,

[0033] - 임시 개인키에 의해 어써션 메세지 다이제스트로부터 어써션 메세지 시그너처를 생성하는 단계

[0034] 의 서브단계를 포함한다.

[0035] 이것은 특히 대량의 정보의 시그너처에 대하여 시그너처 생성의 효율성을 향상시킨다. 어써션 메세지 다이제스트는 서명되어야하는 어써션 메세지의 모든 부분들로부터 생성되어야 한다. 본 발명의 추가적인 실시예에 따르면, 어써션 메세지 다이제스트는 해시 함수에 의해 계산된다.

[0036] 본 발명의 이러한 실시모습의 추가적인 실시예에 따르면, 어써션 메세지 시그너처는 엔벨로프(enveloped) 시그너처이다. 이와 같은 엔벨로프 시그너처는 전체 어써션 메세지로부터 다이제스트를 생성한다. 이것은 메세지의 모든 부분들이 엔벨로프 시그너처에 의해 서명되는 장점을 갖는다.

[0037] 본 발명의 이러한 실시모습의 추가적인 실시예에 따르면, 어써션 증명 및/또는 키 증명은 무 정보 증명이다. 이것은 프로빙 당사자가 신뢰 당사자에게 자신의 ID를 공개할 필요가 없는 장점을 갖는다. 이것은 완전하게 익명으로 유지될 수 있다. 이것은 프로빙 당사자로 하여금 다수의 거래들에 대하여 완전하게 비링크된 채로 유지하면서 자신에 관한 스테이트먼트를 선택적으로 제공할 수 있게 해준다.

[0038] 본 발명의 추가적인 실시예에 따르면, 어써션 증명 및/또는 키 증명은 최소 공개 증명(minimum disclosure proof)이다. 이것은 사용가능한 알고리즘의 갯수를 확대시키고 단순한 구현 솔루션을 제공하는 장점을 갖는다.

[0039] 본 발명의 추가적인 실시예에 따르면, 어써션 증명 및/또는 키 증명은 비상호작용 증명(non-interactive proof)이다. 비상호작용 증명은 예컨대 피아트-샤미르 휴리스틱(Fiat-Shamir heuristics)을 상호작용 무정보 증명에 적용시킴으로써 구축될 수 있다. 이러한 비상호작용 프로토콜은 어떠한 상호작용도 필요로 하지 않기 때문에, 비상호작용 증명은 단일 어써션 메세지에 적합하다.

[0040] 본 발명의 추가적인 실시예에 따르면, 임시 공개키 및 임시 개인키는 디지털 시그너처 알고리즘(DSA) 키 쌍이다.

[0041] DSA는 널리 사용되고 있는 시그너처 알고리즘이다. 본 발명에 따른 방법은 무정보 프로토콜 또는 최소 공개 프로토콜과 이와 같은 DSA 시그너처의 조합을 가능케 해준다.

[0042] 본 발명의 추가적인 실시예에 따르면, 어써션 메세지 시그너처는 확장 마크업 언어 디지털 시그너처(XML-DSIG) 표준에 따른 시그너처이다. XML-DSIG 시그너처 표준은 수 많은 웹 서비스 표준, 예컨대, WS-보안 표준의 시그너처 표준이다.

[0043] 본 발명의 추가적인 실시예에 따르면, 입증가능 랜덤 함수는 도디스(Dodis)와 얌폴스키(Yampolsky)가 제안한 함수이다.

[0044] 이러한 입증가능 랜덤 함수의 사용은 매우 효율적인 솔루션이다.

[0045] 이러한 입증가능 랜덤 함수의 상세한 설명은 "Y. Dodis and A. Yampolsky. A Verifiable Random Function with Short Proofs and Keys. In Public Key Cryptography, volume 3386 of LNCS, pages 416.431, 2005."에서 주어진다.

[0046] 이 함수는 쌍선형 맵에 기초된 키 증명을 이미 포함한다.

[0047] 이러한 쌍선형 맵에 기초된 키 증명 대신에, 이산 대수 정보의 비상호작용 무정보 증명이 사용될 수 있다.

[0048] 본 발명의 추가적인 실시예에 따르면, 어써션 증명은 프로빙 당사자의 하나 이상의 개인 인증서로부터 얻어진다. 개인 인증서 시스템은 복잡한 속성 스테이트먼트가 지원된다는 점에서 익명 크레덴셜 시스템의 일반화된 형태이다. 개인 인증서 시스템은 ID 제공자로부터 개인 인증서들을 획득하게 해주며 이 개인 인증서들을 이용하여 인증된 스테이트먼트를 만들도록 해줌과 동시에, 이러한 발행 및 사용 모두가 프라이버시를 개선시키는 방법으로 가능할 수 있도록 해준다. 사용자 또는 프로빙 당사자는 ID 제공자로부터 개인 인증서를 획득하고 이 인증서를 국지적으로 보존한다. 인증서들은 예컨대 수 년의 장기간 수명을 가질 수 있다. 일단 획득된 인증서는 신뢰 당사자에게 절대로 보내지지 않는다. 사용자가 속성에 관한 스테이트먼트를 갖는 어써션을 신뢰 당사자에게 제공할 필요가 있을 때 마다, 사용자는 자신의 하나 또는 다수의 개인 인증서를 이용하여 자신의 제3 당사자 서명된 속성에 관한 부분적 정보를 제어된 방법으로 공개한다. 이러한 공개는 ID 제공자를 관여시키는 것 없이 수행될 수 있다.

[0049] 본 발명의 추가적인 실시예에 따르면, 본 방법은 연합 ID 관리(FIM) 시스템내에서 수행된다. 연합 ID 관리(FIM) 프로토콜은 세 가지 유형의 플레이어들, 즉 자신의 ID가 연합화되는 사용자(프로빙 당사자), ID를 인증하여 발급해주는 ID 제공자 및 사용자의 ID의 수령자인 신뢰 당사자간의 프로토콜이다. 오늘날에 표준화되어 구축된 FIM 프로토콜은 일반적으로 ID 제공자로부터 사용자에게 그리고 사용자로부터 신뢰 당사자에게 전송되는 서명된 어써션 토큰을 이용한다. 이와 같은 프로토콜의 주요 예시는 "C. Kaler and A. Nadalin. (eds.). WS-Federation: Active Requestor Profile, Version 1.0, JuI 2003. http://www-128.ibm.com/developerworks/library/"에서 규정된 WS-연합 능동 요청자 프로파일이다. 후자는 WS-보안 메세지 내에 포함된 보안 어써션에 기초된 것이다. 사용자의 ID가 필요할 때마다, 보안 어써션은 ID 제공자로부터 요청자(프로빙 당사자)에 의해 획득되고, 그 후 신뢰 당사자에게 전달된다. 이것은 i) 속성이 ID 제공자에 의해 인증되고, ii) 필요로 하는 속성이 정확하게 신뢰 당사자에게 전송되는 특성들이 가능하도록 해준다. 제1 특성은 신뢰 당사자를 위한 보안성을 제공하고, 제2 특성은 사용자(프로빙 당사자)를 위한 프라이버시를 제공한다.

[0050] 본 발명의 제2 실시모습에 따르면, 하나 이상의 스테이트먼트를 갖는 어써션, 어써션에 대한 어써션 증명, 어써션 및 어써션 증명으로부터 생성된 임시 공개키, 임시 공개키에 대한 키 증명, 메세지 몸체 및 어써션 메세지 시그너처를 포함하는 어써션 메세지를 평가하는 방법으로서:

[0051] - 키 증명에 의해 임시 공개키를 검사하는 단계,

[0052] - 어써션 증명에 의해 어써션을 검사하는 단계,

[0053] - 임시 공개키에 의해 어써션 메세지 시그너처를 검사하는 단계,

[0054] - 어써션 메세지 시그너처, 임시 공개키 및 어써션의 검사의 결과가 긍정적인 경우 어써션 메세지를 유효한 것으로서 평가하는 단계

[0055] 를 포함하는 어써션 메세지 평가 방법이 제공된다.

[0056] 어써션 메세지를 수신하는 신뢰 당사자는 어써션 메세지의 유효성을 평가하기 위하여 임시 공개키의 유효성, 어써션의 유효성 및 어써션 메세지 시그너처의 유효성을 검사해야한다.

[0057] 바람직하게, 어써션 메세지 시그너처는 임시 공개키에 대한 참조를 포함하며, 임시 공개키는 대응하는 키 증명에 대한 참조를, 키 증명은 어써션과 어써션 증명에 대한 참조를 포함한다. 그러면, 임시 공개키에 대한 참조는 어써션 메세지 시그너처로부터 추출될 수 있고, 키 증명에 대한 참조는 임시 공개키로부터 추출될 수 있다. 임시 공개키는 키 증명에 의해 검증될 수 있다. 어써션과 대응 어써션 증명에 대한 참조를 따라, 어써션내에서 만들어진 스테이트먼트는 어써션 증명에 의해 검증될 수 있다. 그 후, 어써션 메세지 시그너처는 임시 공개키에 의해 검증될 수 있다.

[0058] 본 발명의 여러 실시모습들의 단계들은 여러 순서들로 수행될 수 있음을 유념해야 한다. 이에 더하여, 단계들은 또한 결합될 수 있는데, 즉, 예컨대 두 개 이상의 단계들이 함께 수행될 수도 있다.

[0059] 본 발명의 다른 실시모습은 컴퓨터 프로그램이 컴퓨터 시스템상에서 수행되는 경우, 청구항 제1 내지 제4항 중 임의의 한 항에 따른 방법의 단계들을 수행하는 명령어를 포함하는 컴퓨터 프로그램과 관련이 있다.

[0060] 본 발명의 다른 실시모습은 프로빙 당사자로부터 신뢰 당사자에 어써션 메세지를 송신하는 송신 엔티티에 관한 것으로서, 상기 송신 엔티티는,

[0061] - 하나 이상의 스테이트먼트들을 포함하는 어써션을 생성하고,

[0062] - 어써션 증명을 생성하고,

[0063] - 어써션과 어써션 증명으로부터 임시 개인키와 대응하는 임시 공개키를 생성하고,

[0064] - 임시 공개키에 대한 키 증명을 생성하고,

[0065] - 임시 개인키에 의해 어써션 메세지 시그너처를 생성하고,

[0066] - 임시 공개키, 어써션 증명, 키 증명, 어써션, 주 메세지 몸체 및 어써션 메세지 시그너처를 포함하는 어써션 메세지를 신뢰 당사자에 보내는 동작을 하도록 제공된다.

[0067] 이와 같은 송신 엔티티는 예컨대, 프로빙 당사자의 컴퓨터일 수 있다.

[0068] 본 발명의 다른 실시모습은 프로빙 당사자로부터 어써션 메세지를 수신하는 수신 엔티티에 관한 것으로서, 상기 어써션 메세지는, 하나 이상의 스테이트먼트들을 갖는 어써션, 어써션에 대한 어써션 증명, 어써션과 어써션 증명으로부터 생성된 임시 공개키, 임시 공개키에 대한 키 증명, 메세지 몸체 및 어써션 메세지 시그너처를 포함하며, 상기 수신 엔티티는:

[0069] - 키 증명에 의해 임시 공개키를 검사하고,

[0070] - 어써션 증명에 의해 어써션을 검사하고,

[0071] - 임시 공개키에 의해 어써션 메세지 시그너처를 검사하고,

[0072] - 어써션 메세지 시그너처, 임시 공개키 및 어써션의 검사의 결과가 긍정적인 경우 어써션 메시지를 유효한 것으로서 평가하는 동작을 하도록 제공된다.

[0073] 이와 같은 수신 엔티티는 예컨대, 신뢰 당사자의 서버일 수 있다.

[0074] 본 발명의 다른 실시모습은 어써션 메세지를 포함하는 신호에 관한 것으로서, 상기 어써션 메세지는 메세지 헤더와 메세지 몸체를 포함하며, 메세지 헤더는 하나 이상의 스테이트먼트들을 갖는 어써션, 어써션 증명, 어써션과 어써션 증명으로부터 생성된 임시 공개키, 임시 공개키에 대한 키 증명 및 임시 공개키에 대응하는 임시 개인키에 의해 생성된 어써션 메세지 시그너처를 포함한다.

[0075] 본 발명의 다른 실시모습은 어써션 메세지의 포맷을 규정하는 어써션 메세지 포맷에 관한 것으로서, 상기 포맷에 따른 어써션 메세지는 메세지 헤더와 메세지 몸체를 포함하며, 메세지 헤더는 하나 이상의 스테이트먼트들을 갖는 어써션, 어써션 증명, 어써션과 어써션 증명으로부터 생성된 임시 공개키, 임시 공개키에 대한 키 증명 및 임시 공개키에 대응하는 임시 개인키에 의해 생성된 어써션 메세지 시그너처를 포함한다.

[0076] 본 발명의 다른 실시모습은 청구항 제6항에 따른 송신 엔티티와 청구항 제7항에 따른 수신 엔티티를 포함하는 시스템에 관한 것이다.

[0077] 위에서 제시된 본 발명의 여러 실시모습들은 개인 인증서 시스템과 같은 무정보 증명 기반의 프로토콜의 시맨틱(semantic)을 XML-DSIG 키 및 시그너처와 같은 공개키 시그너처 시스템으로 변경가능하게 해주는 일반적 구성을 제공한다. 공개키- 시그너처 시스템은 널리 사용되고 있고 수 많은 산업 표준, 특히 웹 서비스(WS)-보안 표준에 따른 강제적 사항이기 때문에, 본 발명은 폭넓게 적용가능하다.

[0078] 본 발명의 여러 실시모습들은 개인 인증서 시스템과 WS-보안의 통합을 가능하게 해주고 이에 따라 향상된 프라이버시 특성을 갖는 새로운 WS-연합 능동 요청자 프로파일을 가능케 해준다.

[0079] 특히, 위에서 제시된 본 발명의 여러 실시모습들은 다음의 요구조건들을 충족시켜주는 시스템의 제공을 가능케 해준다:

[0080] (a) XML-DSIG 표준은 이미 안정화되어 있고, 무정보 증명으로의 변경은 XML-DSIG 시맨틱을 처리가능 한도를 넘어 복잡하게 만들 수 있으므로 XML-DSIG 표준을 변경시키지 않는다.

[0081] (b) 표준부들의 원래 의도를 넘어, 심지어는 의도되었던 시맨틱을 위반할 정도의 표준부들의 극도로 넓은 해석에 의존하지 않는다.

[0082] 이것은 개인 인증서 시스템과 WS-보안 환경내의 현존하는 표준 시맨틱의 끊김없는 통합의 가능성을 제공한다.

실 시 예

[0097] 도 1을 참조하면, 본 발명의 예시적인 실시예에 따른 시스템(10)의 개략적 레이아웃이 도시된다. 본 도면들에서, 동일한 참조부호들은 동일하거나 유사한 부분들을 표기하는데에 사용된다. 시스템은 프로빙 당사자(20), ID 제공자(30) 및 신뢰 당사자(40)를 포함한다. 본 예시에서, 프로빙 당사자(20)는 신뢰 당사자(40)와 예컨대 구입 거래와 같은 거래를 수행하기를 원하는 사용자이다. 프로빙 당사자(20)는 컴퓨터(60)상에서 예컨대, 웹 브라우저와 같은 클라이언트 애플리케이션(50)을 실행한다. ID 제공자(30)는 서버(70)를 운영하고 신뢰 당사자(40)는 서버(80)를 운영한다. 컴퓨터(60)는 통신라인(90)을 통해 ID 제공자(30)의 서버(70)에 연결가능할 뿐만이 아니라 신뢰 당사자(40)의 서버(80)에 연결가능하다. 통신 라인(90)은 통상적으로 네트워크, 예컨대 인터넷을 통해 제공된다. ID 제공자(30)는 예를 들어, 은행이나 또는 ID 관리 서비스를 제공하는 다른 전문 조직체일 수 있다. ID 제공자(30)는 일반적으로 ID 관련 정보(IRI)를 발행하기 위해 제공된다. ID 관련 정보(IRI)의 용어는 개인 또는 사용자와 관련된 임의의 정보를 포함하는 것으로 이해된다. ID 관련 정보(IRI)는 성명, 주소, 그룹 멤버쉽, 인가 크레덴셜, 인구 통계학적 데이터, 개인 선호사항, 칼렌더 엔트리, 의료 및 재정 정보, 및 개인에 관련되거나 또는 사용자 성명으로 디지털방식으로 저장될 수 있는 기타 모든 것을 포함한다. 프로빙 당사자(20)는 예컨대, 액세스 제어 문제, 인가 문제, 개인적 문제, 인증 문제, 로그인 문제, 영업 문제, 의료 문제, 정부행정 문제 또는 기타 문제들을 위해 이와 같은 IRI를 희망할 수 있다. ID 제공자(30)는 특히 개인 인증서 또는 사용자 인증서로도 표기되는 속성 크레덴셜의 발행을 위해 제공된다. ID 제공자(30)의 서버(70), 프로빙 당사자(20)의 컴퓨터(60) 및 신뢰 당사자(40)의 서버(80)는 개인 인증서 시스템 플러그인(100)을 포함한다. 이 개인 인증서 시스템 플러그인(100)은 시스템(10)이 개인 인증서 시스템으로서 동작하도록 촉진시킨다. 개인 인증서 시스템은 속성 스테이트먼트에 관련된 복잡한 어써션이 지원된다는 점에서 익명 크레덴셜 시스템의 일반화된 형태이다. 프로빙 당사자(20)는 ID 제공자(30)로부터 하나 이상의 개인 인증서(110)를 획득할 수 있다. 개인 인증서(110)는 프로빙 당사자(20)의 컴퓨터(60)상에서 국지적으로 저장될 수 있다. 프로빙 당사자(20)는 개인 인증서(110)를 이용하여 인증된 어써션(120)을 생성한다. 인증된 어써션(120)은 프로빙 당사자(20)의 속성에 관한 스테이트먼트를 갖는 어써션과 대응하는 어써션 증명을 포함한다. 이러한 인증된 어써션(120)을 신뢰 당사자(40)에게 보냄으로써, 프로빙 당사자(20)는 완전히 익명의 비링크 상태를 유지하면서 신뢰 당사자(40)에게 이러한 어써션을 입증할 수 있다. 어써션에 대한 증명은 예컨대, 비상호작용 무 정보 증명 또는 비상호작용 최소 공개 증명에 의해 구축될 수 있다.

[0098] 도 2는 본 발명의 예시적인 실시예에 따른 어써션 메세지(200)의 포맷의 개략적 도해를 도시한다. 어써션 메세지(200)는 도 1을 참조하여 설명된 인증된 어써션(120)의 바람직한 실시예이다. 어써션 메세지(200)는 메세지 헤더(210)와 메세지 몸체(220)를 포함한다. 메세지 헤더(210)는 어써션(A)을 갖는 어써션 토큰(230), 증명 토큰(240), 임시 공개키(K)를 갖는 임시 공개키 토큰(250) 및 시그너처(S)를 갖는 엔벨로프 시그너처 토큰(260)을 포함한다. 증명 토큰(240)은 어써션에 대한 어써션 증명(p_A)을 갖는 어써션 증명 토큰(241)과 임시 공개키(K)에 대한 키 증명(p_K)을 갖는 키 증명 토큰(242)을 포함한다. 엔벨로프 시그너처 토큰(260)은 임시 공개키 토큰(250)에 대한 참조(270)를 포함한다. 임시 공개키 토큰(250)은 증명 토큰(240)에 대한 참조(280)를 포함하며, 증명 토큰(240)은 어써션 토큰(230)에 대한 참조(290)를 포함한다. 메세지 헤더(210)는 추가적인 요소들 또는 토큰들을 포함할 수 있다. 메세지 몸체(220)는 모든 종류의 메세지들, 예컨대 도 1의 신뢰 당사자(40)의 서비스에 액세스하기 위한 요청을 포함할 수 있다.

[0099] 컴퓨터(60)는 프로빙 당사자(20)로부터 신뢰 당사자(40)에 어써션 메세지(200)를 송신하는 송신 엔티티로서 동작할 수 있다.

[0100] 서버(80)는 어써션 메세지(200)를 송신하고 검증하는 수신 엔티티로서 동작할 수 있다.

[0101] 도 2에서 도시된 어써션 메세지(200)를 프로빙 당사자(20)로부터 신뢰 당사자(40)에 제공하기 위한 이하의 흐름 설명을 용이하게 하기 위하여 도 1에서의 시나리오가 도시된다.

[0102] 도 3은 본 발명의 예시적인 실시예의 메세지 흐름의 개략적 도해를 도시한다. 여기서는, 프로빙 당사자(20), ID 제공자(30) 및 신뢰 당사자(40)간의 메세지 흐름이 각각의 로마 숫자가 할당되어 붙여진 화살표와 함께 도시된다. 추가적인 단계들 또는 서브 단계들은 원모양의 로마 숫자에 의해 표기된다. 흐름은 커져가는 로마 숫자들에 의해 나타나는 바와 같이 위에서 아래로 순차적으로 수행되는 것으로 이해한다. 하지만, 특정한 순서없이 병렬적으로 구동되는 이 프로토콜의 다수의 예시들이 존재할 수 있음에 유념해야 한다.

[0103] 단계 I에서, 프로빙 당사자(20)는 예컨대, 생년월일, 우편 번호 및 프로빙 당사자(20)의 ID에 관한 추가 정보를

포함하는 개인 인증서를 ID 제공자(30)에게 요청한다. ID 제공자(30)는 요청된 개인 인증서를 발행하고, 단계 II에서 이것을 프로빙 당사자(20)에게 되돌려 보낸다. 단계 III에서, 프로빙 당사자(20)는 개인 인증서를 컴퓨터(60)상에 저장한다. 단계 I와 단계 II는 여러번 반복될 수 있는데, 즉 프로빙 당사자(20)는 컴퓨터(60)상에 여러 개의 개인 인증서들을 저장할 수 있다.

[0104] 만약 프로빙 당사자(20)가 신뢰 당사자(40)의 서비스를 이용하는 것을 원하는 경우에는, 프로빙 당사자(20)는, 단계 IV에서, 희망하는 서비스를 위한 정책을 획득하기 위한 요청을 신뢰 당사자(40)에게 보낸다. 단계 V에서, 신뢰 당사자(40)는 해당 정책을 프로빙 당사자(20)에게 되돌려 보낸다. 본 예시에서, 요청된 서비스를 위한 정책은 21세 보다 나이 많은 사용자의 증명을 필요로 하는 것으로 가정한다. 단계 VI에서, 프로빙 당사자(20)는 수신된 정책을 분석하고, 이것을 컴퓨터(60)상에 저장된 이용가능한 개인 인증서(110)와 비교한다. 만약 하나 이상의 적합한 개인 인증서(110)가 이용가능한 경우, 사용자 또는 프로빙 당사자(20)는 각각 개인 인증서를 선택할 수 있고, 컴퓨터(60)의 개인 인증서 시스템 플러그인(100)에 의해 도 2에서 도시된 어써션 메세지(200)와 같은 어써션 메세지가 생성된다. 본 예시에서, 어써션 메세지는 프로빙 당사자(20)가 21세 보다 나이 많다라는 내용의 어써션을 포함한다. 이 어써션과 대응하는 어써션 증명은 개인 인증서의 생년월일로부터 구해질 수 있다. 단계 VII에서, 어써션 메세지는 프로빙 당사자(20)로부터 신뢰 당사자(40)에 보내진다. 어써션 메세지의 수신 이후, 신뢰 당사자(40)는 단계 VIII에서 어써션 메세지의 유효성을 검사한다. 어써션 메세지가 유효한 것으로서 검증되면, 신뢰 당사자(40)는 단계 IX에서 결과물, 예컨대 요청된 정보를 프로빙 당사자(20)에 보낸다. 요청된 정보는 예컨대 오로지 21세 보다 많은 사람에 대해서만 액세스가능한 웹페이지일 수 있다.

[0105] 만약 프로빙 당사자(20)가 신뢰 당사자(40)의 다른 서비스를 이용하고자 한다면, 프로빙 당사자(20)는 단계 X에서 희망하는 서비스에 대한 정책을 획득하기 위한 추가 요청을 신뢰 당사자(40)에 보낼 수 있다. 단계 XI에서, 신뢰 당사자(40)는 프로빙 당사자(20)에게 해당 정책을 되돌려 보낸다. 본 예시에서는 요청된 서비스에 대한 정책은 프로빙 당사자(20)의 우편 번호의 증명을 필요로 하는 것으로 가정한다. 단계 XII에서, 프로빙 당사자(20)는 수신된 정책을 분석하고, 이것을 컴퓨터(60)상에 저장된 이용가능한 개인 인증서(110)와 비교한다. 만약 적합한 개인 인증서(110)가 이용가능한 경우, 사용자 또는 프로빙 당사자(20)는 각각 개인 인증서를 선택할 수 있고, 인증된 어써션, 즉 어써션과 대응하는 어써션 증명이 컴퓨터(60)의 개인 인증서 시스템 플러그인(100)에 의해 생성된다. 본 예시에서, 인증된 어써션은 프로빙 당사자(20)가 표시된 우편 번호를 갖는 내용의 정보를 포함한다. 또한, 컴퓨터(60)의 개인 인증서 시스템 플러그인(100)은 인증된 어써션을 포함하는 다른 어써션 메세지를 생성한다. 단계 XIII에서, 어써션 메세지는 프로빙 당사자(20)로부터 신뢰 당사자(40)로 보내진다. 어써션 메세지의 수신 이후, 신뢰 당사자(40)는 단계 XIV에서 어써션 메세지의 유효성을 검사한다. 어써션 메세지가 유효한 것으로서 검증되면, 신뢰 당사자(40)는 단계 VX에서 결과물, 예컨대 요청된 정보를 프로빙 당사자(20)에 보낸다.

[0106] 도 2의 어써션 메세지 포맷은 개인 크레덴셜 시스템을 갖는 인증을 XML-DSIG과 같은 표준 공개키 시그너처 방식대로 통합시키는데에 사용될 수 있다. 이것은 개인 크레덴셜을 갖는 인증을 XML-DSIG-시그너처를 생성시킬 수 있는 임시 공개키/개인키 시그너처를 갖는 인증으로 변경시킴으로써 구축될 수 있다. 이러한 인증 변경을 위해 보안 모델은 프로빙 당사자(20)가 신뢰 당사자(40)에 의해 신뢰받지 않는 것을 가정한다. 그러므로, 프로빙 당사자(20)는 프로토콜에 따른 임시 시그너처 키 쌍을 신뢰있게 선택하거나 또는 검증이 중단되는 것을 강제해야 한다. 이것은 프로빙 당사자가 항상 단일 인증된 어써션마다 의사적 랜덤방식의 새로운 임시 시그너처 키 쌍을 선택하는 요구조건을 설정함으로써 이행될 수 있다.

[0107] 이러한 임시 시그너처 키 쌍의 특성은 악의적인 프로빙 당사자(20)가 임시 시그너처 키 쌍을 여러번 이용하거나, 다른 주축 키를 갖는 오결합된 키 쌍을 이용하거나 또는 단일 키 쌍을 다수의 크레덴셜에 결합하려고 시도할 수 있는 것을 방지한다. 본 발명의 이러한 실시예에 따르면, 개인 인증서 시스템으로 만들어진 인증 스테이트먼트(예컨대, 프로빙 당사자(20)는 특성 stt = '21세 보다 나이 많은'을 갖는다)는 다음과 같은 스테이트먼트를 포함하는 어써션으로 변형된다:

[0108] (a) 프로빙 당사자(20)는 속성 att(예컨대, '21세 보다 나이 많은')을 갖는다.

[0109] (b) 프로빙 당사자(20)는 임시 공개키(K)에 대응하는 임시 개인키(K_s)를 보유한다.

[0110] (c) 키 쌍(K_s; K)은 이 어써션에 대해 의사적 랜덤방식으로 새롭게 생성된다.

[0111] 예컨대, 프로빙 당사자(20)에 의해 무정보 증명에 기초된 프로토콜로 만들어진 스테이트먼트마다, 새로운 임시 키 쌍이 새롭게 그리고 의사적 랜덤방식으로 생성되는 것이 보장될 수 있다. 또한, 입증가능 의사난수 함수 및

임시 공개키가 정확하게 계산되었음을 말해주는 대응하는 무정보 증명에 의해, 프로빙 당사자(20)는 임시 키 쌍을 신뢰할 만하게 생성하였음이 보장될 수 있다. 임시 키 쌍의 1회성(one-timeness)은 거래의 비링크성을 가능케 해준다.

[0112] 이 임시 키 쌍은 입증된 어써션에 의해 확장된 시맨틱을 갖는 XML 시그너처를 생성하는데에 사용될 수 있다. 입증된 어써션은 세 개의 토큰 유형: 어써션 토큰(230), 증명 토큰(240) 및 임시 공개키 토큰(250)으로 나타난다. 임시 공개키 토큰(250)은 특성에 관한 스테이트먼트와 임시 키 쌍의 신뢰적인 생성과 연관된다. 어써션 토큰(230)은 임시 키 쌍과 연관된 프로빙 당사자(20)의 속성에 관한 추가적인 스테이트먼트를 제공한다. 최종적으로, 증명 토큰(240)은 이러한 스테이트먼트들에 대해 이중 증명, 즉, 한편으로는 특성과 임시 키 쌍의 신뢰적인 생성이 입증되고, 다른 한편으로는, 프로빙 당사자(20)의 속성에 관한 어써션의 추가적인 스테이트먼트가 입증되는 것을 유지한다.

[0113] 아래에서는 어써션 메세지의 생성과 검증을 보다 자세하게 설명할 것이다.

[0114] 전제조건으로서, G는 제1 차수 q 순환 그룹이며, g는 이것의 생성자이며, g와 그룹 G는 모두 도 1에서 도시된 시스템(10)의 시스템 파라미터인 것으로 가정한다. G와 g는 모든 시스템 참가자들, 즉 ID 제공자(30), 프로빙 당사자(20) 및 신뢰 당사자(40)에 의해 사용된 DSA 시그너처 방식의 공개 파라미터로서 사용될 수 있도록 선택된다. 프로빙 당사자(20)는 프로토콜이 수행되는데에 필요한 모든 개인 인증서를 갖는 것으로 가정한다. 또한 모든 참가자들은 프로토콜에 대한 입력으로서 필요로 하는 인증서 검증 키를 갖는 것으로 가정한다. 전제조건으로서, 입증가능 랜덤 함수가 시스템을 이용하는 모든 플레이어들, 즉 프로빙 당사자(20), ID 제공자(30) 및 신뢰 당사자(40)에 대해 이용가능한 것을 더 가정한다. 입증가능 랜덤 함수는 도 1에서 도시된 개인 인증서 시스템 플러그인(100)내에서 이용가능하도록 만들어질 수 있다. 입증가능 랜덤 함수는 해당 그룹에 대한 1차 계수 p, 1차 차수 q 및 생성자 g를 갖는 순환 그룹 G에 의해 정의된다.

[0115] 이어서, 프로빙 당사자(20)(서명자)와 신뢰 당사자(40)(검증자)간의 프로토콜인 방법을 설명한다. 프로토콜은 프로빙 당사자(20)에 의해 수행된 어써션 메세지 생성과 신뢰 당사자(40)에 의해 수행된 어써션 메세지의 검증에 의해 진행된다.

[0116] 도 4는 본 발명의 예시적인 실시예에 따라 도 3에서 도시된 어써션 메세지의 생성의 흐름도를 도시한다.

[0117] 단계 400에서, 프로빙 당사자(20)는 현재의 요청(액세스 제어 정책)에 관한 액세스 정보를 포함하는 신뢰 당사자(40)의 정책을 신뢰 당사자(40)로부터 수신한다. 이 단계 400은 도 2를 참조하여 설명한 단계 V와 단계 XI에 대응한다.

[0118] 다음의 단계 410에서는, 수신된 정책이 프로빙 당사자(20)의 컴퓨터(60)의 개인 인증서 시스템 플러그인(100)내에 저장된 개인 인증서들과 미리정의된 선호사항 및 프로빙 당사자(20)의 입력과 관련하여 분석된다.

[0119] 단계 420에서는 이전 단계 410의 결과로서 어써션이 생성된다. 이와 같은 어써션은 예컨대 프로빙 당사자(20)의 나이가 21 이상인 내용의 스테이트먼트일 수 있다.

[0120] 단계 430에서는 어써션 증명이 생성된다. 이러한 본 발명의 실시예에 따르면, 어써션 증명은 정보의 비상호작용 무정보 증명, 즉 어써션의 유효성에 대한 증명이지만 어써션의 유효성 이외의 임의의 기타 정보를 전달하지 않는 증명이다. 어써션 증명은 프로빙 당사자(20)의 개인 인증서(110)의 서브세트, 어써션(A), 인증서 발행자의 공개키 및 추가적인 공개 파라미터들을 입력으로서 이용함으로써 생성된다.

[0121] 어써션 증명의 예시에 관한 자세한 설명은 "BANGERTER, E., CAMENISCH, J., AND LYSYANSKAYA, A. A cryptographic framework for the controlled release of certified data. Twelfth International Workshop on Security Protocols 2004 (2004), LNCS, Springer Verlag"에서 주어진다. 이것은 참조로서 병합된다.

[0122] 다음의 설명을 위해, 변수 콘텍스트(context)는 상호작용의 보안 콘텍스트, 예컨대 신뢰 당사자(40)로부터의 현재 시각 또는 요청(challenge)인 것으로 가정한다.

[0123] 다음의 단계 440에서, 임시 개인키(K_s)와 임시 공개키(K) 뿐만이 아니라 키 증명(p_K)을 포함하는 임시 DSA 키 쌍이 어써션(A), 어써션 증명(p_A)) 및 보안 콘텍스트를 입력으로서 갖는 도디스 및 얌폴스키의 입증가능 랜덤 함수를 이용하여 생성된다.

[0124] 단계 440는 이하의 서브 단계들을 포함한다:

[0125] a.) 암호 해시 함수 H를 이용하여 A || P_A || 콘텍스트의 해시로서 중간값 m을 계산하는 단계

[0126] b.) {1,...,q} 로부터 무작의로 x를 선택하는 단계

[0127] c.) 중간값 y := g^x를 계산하는 단계

[0128] d.) 임시 개인 키(k_s)를 K_s := 1 / (x+m)(mod q)로서 계산하는 단계

[0129] e.) 임시 공개키(K)를 K := g^{ Ks }(mod p)로서 계산하는 단계

[0130] f.) 키 증명(p_K)을 "J. Camenisch and M. Stadler. Efficient group signature schemes for large groups. In B. Kaliski, editor, Advances in Cryptology. CRYPTO '97, volume 1296 of LNCS, pages 410.424. Springer Verlag, 1997."에서 카메니쉬(Camenisch)와 스테이들러(Stadler)에 의해 도입된 표기를 이용하여 아래와 같이 규정된 비상호작용 증명으로서 계산하는 단계

[0131] 키 증명(p_K)의 계산은 이하의 서브 단계들을 포함한다:

[0132] f1.) Z_q로부터 무작의로 변수 r_1을 선택하는 단계(여기서, Z_q는 0...q-1로부터의 정수 세트이다)

[0133] f2.) Z_q로부터 무작의로 변수 r_2을 선택하는 단계

[0134] f3.) t_1:=g^{r_1}을 계산하는 단계

[0135] f4.) t_2:=g^{r_2}을 계산하는 단계

[0136] f5.) t_3:=y^{r_2}g^{mr_2}을 계산하는 단계

[0137] f6.) c:=H(t_1, t_2, t_3, y, K, g, p, q)을 계산하는 단계

[0138] f7.) s_1:=r_1+cx을 계산하는 단계

[0139] f8.) s_2:=r_2+cK_s을 계산하는 단계

[0140] 결과적인 키 증명(p_K)은 후에 (y, K, g, S_1, S_2, c)의 세트에 의해 구축된다.

[0141] 단계 b와 단계 c는 입증가능 랜덤 함수의 인스턴스를 생성한다. 단계 d, 단계 e, 및 단계 f는 입증가능 랜덤 함수의 인스턴스를 이용하여 임시 키 쌍과 임시 키 상에 대한 키 증명을 생성한다.

[0142] 이와 달리 키 증명은 쌍선형 맵에 기초될 수 있다.

[0143] 단계 450에서는, 어써션 메세지(200)가 메세지 몸체(210), 임시 공개키 토큰(250), 어써션 증명 토큰(241)과 키 증명 토큰(242)으로 구성된 증명 토큰(240), 및 어써션 토큰(230)을 포함하면서 부분적으로 어셈블링된다.

[0144] 단계 460에서는, 엔벨로프 XML 디지털 시그너처가 임시 개인키(K_S)를 이용하여 단계 450의 부분적으로 어셈블링된 메세지에 대해 어써션 메세지 시그너처로서 계산된다. 실시예에 따르면, 단계 460은 해시 함수 H에 의해 단계 450의 부분적으로 어셈블링된 메세지의 어써션 메세지 다이제스트를 생성하는 서브 단계를 포함한다. 이하의 서브 단계에서는 어써션 메세지 시그너처(S)가 임시 개인키(K_s)에 의해 어써션 메세지 다이제스트로부터 계산된다.

[0145] 단계 470에서는, 어써션 메세지 시그너처(S)가 어써션 메세지(200)의 메세지 헤더(210)에 추가된다. 그 결과로, 도 2에서 도시된 어써션 메세지(200)가 얻어진다.

[0146] 엔벨로프 시그너처(S)와 달리, 어써션 메세지 시그너처가 오로지 메세지의 부분만을 서명함으로써 생성될 수 있다. 하지만, 적어도 어써션 증명(p_A)은 서명되어야 한다.

[0147] 그 후, 최종 단계 480에서, 어써션 메세지는 프로빙 당사자(20)로부터 신뢰 당사자(40)에 보내진다.

[0148] 도 5는 본 발명의 예시적인 실시예에 따른 어써션 메세지(200)의 검증의 흐름도이다. 이하의 단계들은 신뢰 당사자(40)에 의해 수행된다.

[0149] 단계 500에서, 신뢰 당사자(40)는 프로빙 당사자(20)로부터 어써션 메세지(200)를 수신한다.

[0150] 단계 510에서, 어써션(A), 어써션 증명(p_A) 및 키 증명(p_K), 임시 공개키(K)와 어써션 메세지 시그너처(S)가 어써션 메세지(200)로부터 추출된다.

[0151] 단계 520에서, 임시 공개키(K)가 입증가능 랜덤 함수에 의해 검증된다. 입증가능 랜덤 함수는 신뢰 당사자(40)의 서버(80)의 개인 인증서 시스템 플러그인(100)내에서 이용가능하다.

[0152] 단계 520의 제1 서브 단계에서는, 중간값 m이 암호 해시 함수 H를 이용하여 A || P_A || 콘텍스트의 해시로서 계산된다.

[0153] 단계 520의 제2 서브 단계에서는, 임시 공개키(K)의 키 정확성을 입증하는 무정보 증명(p_K)이 검증된다.

[0154] 임시 공개키의 검증은 다음의 서브 단계들을 포함한다:

[0155] a1.) u_1:=y^{-c}g^{s_1}을 계산하는 단계

[0156] a2.) u_2:=y^{-c}g^{r_2}을 계산하는 단계

[0157] a3.) u_3:=g^{-c}y^{s_2}g^{ms_2}을 계산하는 단계

[0158] a4.) c':=H(u_1, u_2, u_3, y, K, g, p, q)을 계산하는 단계

[0159] a5.) c와 c'를 비교하고, 오로지 c=c'인 경우에서만 키 증명(p_K)을 검증하는 단계

[0160] 단계 530에서, 어써션 증명(p_A)이 프로빙 당사자(20)의 개인 인증서의 서브세트, 어써션(A), 개인 인증서 발행자, 즉 ID 제공자(30)의 공개키, 및 추가적인 공개 파라미터들을 입력으로서 이용함으로써 검증된다.

[0161] 단계 540에서, 어써션 메세지 시그너처(S)가 임시 공개키(K)에 의해 검증된다.

[0162] 만약 단계 520, 단계 530 및 단계 540에서 수행된 모든 검사들의 결과가 긍정적이면, 어써션 메세지(200)는 유효한 것으로 간주되고 어써션 메세지(200)의 검증이 단계 550에서 수행된다. 만약 단계 520, 단계 530 및 단계 540에서 수행된 검사들 중 하나의 결과가 부정적이면, 어써션 메세지(200)는 무효한 것으로 간주되고 검증 프로세스는 단계 560에서 중단된다.

[0163] 도 6은 WS-보안 표준에 따라 구현된 어써션 메세지의 메세지 헤더(600)의 예시를 도시한다. 본 예시는 웹 서비스 메세지의 WS-보안 헤더의 뼈대이다. 본 예시에서 네임스페이스 wsse는 WS-보안의 것이고, cred 네임스페이스는 본 발명의 확장부에 대한 것임을 유념한다.

[0164] 메세지 헤더(600)는 어써션 증명과 키 증명을 포함하는 증명 섹션(610), 어써션을 포함하는 어써션 섹션(620), 임시 공개키를 포함하는 임시 공개키 섹션(630) 및 엔벨로프 시그너처를 포함하는 엔벨로프 시그너처 섹션(640)을 포함한다.

[0165] 개시된 임의의 실시예는 도시되고 및/또는 설명된 하나 또는 여러개의 다른 실시예들과 결합될 수 있다. 또한 실시예들의 하나 이상의 특징들에 대해서도 이와 같이 가능하다.

산업상 이용 가능성

[0166] 추가적인 실시예 설명

[0167] 설명된 기술들은 소프트웨어, 펌웨어, 마이크로-코드, 하드웨어 및/또는 이들의 임의의 조합을 포함하는 방법, 장치 또는 제조 물품으로서 구현될 수 있다. 본 명세서에서 사용된 용어 "제조 물품"은 매체내에서 구현되는 코드 또는 로직을 말하며, 여기서 이와 같은 매체는 자기 저장 매체(예컨대, 하드 디스크 드라이브, 플로피 디스크, 테잎 등), 광학 저장소(CD-ROM, 광 디스크, 등), 휘발성 및 비휘발성 메모리 장치[예컨대, EEPROM(Electrically Erasable Programmable Read Only Memory), ROM(Read Only Memory), PROM(Programmable Read Only Memory), RAM(Random Access Memory), DRAM(Dynamic Random Access Memory), SRAM(Static Random Access Memory), 플래쉬, 펌웨어, 프로그램가능 로직, 등]과 같은, 하드웨어 로직[예컨대, 집적 회로칩, 프로그램가능 게이트 어레이(PGA), 응용 특정 집적 회로(ASIC), 등] 또는 컴퓨터 판독가능 매체를 포함할 수 있다. 컴퓨터 판독가능 매체내의 코드는 프로세서에 의해 액세스되어 실행된다. 코드 또는 로직이 인코딩되어 있는 매체

는 또한 광 섬유, 구리선 등과 같은 공간 또는 전송 매체를 통해 전파되는 전송 신호를 포함할 수도 있다. 코드 또는 로직이 인코딩되어 있는 전송 신호는 무선 신호, 위성 전송, 무선파, 적외선 신호, 블루투스 등을 더 포함한다. 코드 또는 로직이 인코딩되어 있는 전송 신호는 송신 스테이션에 의해 송신가능하고 수신 스테이션에 의해 수신가능하며, 전송 신호내에 인코딩된 코드 또는 로직은 디코딩되어, 수신 스테이션 및 송신 스테이션 또는 장치들에서 하드웨어 또는 컴퓨터 판독가능 매체내에 저장된다. 추가적으로, "제조 물품"은 코드가 내장되고, 처리되고 실행되는 하드웨어 및 소프트웨어 구성부의 조합을 포함할 수 있다. 물론, 본 발명분야의 당업자는 실시예들의 범위를 일탈하는 것 없이 수 많은 변형이 취해질 수 있으며, 제조 물품은 임의의 정보 함유 매체를 포함할 수 있음을 알 것이다. 예를 들어, 제조 물품은 머신에 의해 실행되는 경우 동작들이 수행되는 결과를 가져오는 명령어를 저장한 저장 매체를 포함한다. 어떤 실시예들은 오로지 하드웨어 실시예의 형태만을 취할 수 있거나, 오로지 소프트웨어 실시예의 형태만을 취할 수 있거나, 하드웨어 및 소프트웨어 요소들 모두를 포함하는 실시예의 형태를 취할 수 있다. 바람직한 실시예에서, 본 발명은 비제한적인 예시로서 펌웨어, 상주 소프트웨어, 마이크로코드 등을 포함하는 소프트웨어에서 구현된다. 또한, 어떤 실시예들은 컴퓨터 또는 임의의 명령어 실행 시스템에 의한 사용 또는 이와 관련된 사용을 위한 프로그램 코드를 제공하는 컴퓨터 사용가능 매체 또는 컴퓨터 판독가능 매체로부터 액세스가능한 컴퓨터 프로그램 제품의 형태를 취할 수 있다. 이러한 설명의 목적을 위해, 컴퓨터 사용가능 매체 또는 컴퓨터 판독가능 매체는 명령어 실행 시스템, 장치 또는 장비에 의한 사용 또는 이와 관련된 사용을 위한 프로그램을 포함, 저장, 통신, 전파, 또는 전송할 수 있는 임의의 장치일 수 있다. 매체는 전자 매체, 광학 매체, 전자기 매체, 적외선 매체, 또는 반도체 시스템(또는 장치 또는 장비) 매체 또는 전파 매체일 수 있다. 컴퓨터 판독가능 매체의 예로서는 반도체 또는 고체 상태 메모리, 자기 테이프, 탈착가능 컴퓨터 디스켓, RAM, ROM, 고정 자기 디스크 및 광학 디스크를 포함한다. 오늘날의 광학 디스크의 예로서는 CD-ROM, CD-R/W 및 DVD를 포함한다.

[0168] 용어 "어떤 실시예들", "일 실시예", "실시예", "실시예들", "상기 실시예", "상기 실시예들", "하나 이상의 실시예들", "일부 실시예들", 및 "하나의 실시예"는 이와 달리 특정하여 표현되지 않는 한 하나 이상의 (하지만 모든 실시예들은 아닌) 실시예들을 의미한다. 용어 "포함하는", "구비하는", "갖는" 및 이들의 변형체들은 이와 달리 특정하여 표현되지 않는 한 "포함하지만 이에 한정되지 않는"을 의미한다. 열거된 아이템 리스트들은 이와 달리 특정하여 표현되지 않는 한 임의의 아이템 또는 모든 아이템들이 상호 배타적인 것을 의미하지 않는다. 용어 "일", "하나" 및 "상기"는 이와 달리 특정하여 표현되지 않는 한 "하나 이상"을 의미한다. 서로 통신하는 장치들은 이와 달리 특정하여 표현되지 않는 한 서로 연속적으로 통신할 필요는 없다. 추가로, 서로 통신하는 장치들은 하나 이상의 매개물들을 통해 직접 또는 간접적으로 통신할 수 있다. 추가적으로, 서로 통신하는 여러 구성부들을 갖는 실시예의 설명은 이와 같은 모든 구성부들이 필요로 하는 것을 의미하지는 않는다. 이에 반해, 다양한 택일적 구성부들은 폭넓게 다양한 잠재적인 실시예들을 설명하기 위해 기술된다. 또한, 프로세스 단계, 방법 단계, 알고리즘 등이 순차적 순서로 기술될 수 있지만, 이와 같은 프로세스, 방법 및 알고리즘은 교차적 순서로 동작하도록 구성될 수 있다. 즉, 기술될 수 있는 임의의 단계 시퀀스 또는 순서는 단계들이 이러한 순서로 수행되는 요구조건을 반드시 나타내는 것은 아니다. 본 명세서에서 기술된 프로세스의 단계는 임의의 실제 순서로 수행될 수 있다. 또한 일부 단계들은 동시적으로, 병렬로, 또는 일시에 수행될 수 있다. 본 명세서에서 단일 장치 또는 물품이 기술되는 경우, 단일 장치/물품 대신에 하나 보다 많은 장치/물품(이들이 서로 함께 작용하던지 않던지 간에)이 사용될 수 있음이 자명할 것이다. 마찬가지로, 본 명세서에서 하나 보다 많은 장치 또는 물품(이들이 서로 함께 작용하던지 않던지 간에)이 기술되는 경우, 하나 보다 많은 장치 또는 물품 대신에 단일의 장치/물품이 사용될 수 있음이 자명할 것이다. 장치의 기능성 및/또는 특징은 이와 같은 기능성/특징을 갖는 것으로 명백하게 기술되지 않은 하나 이상의 다른 장치들에 의해 이를 대신하여 구현될 수 있다. 따라서, 다른 실시예들은 해당 장치 자체를 포함할 필요는 없다.

[0169] 본 문맥에서 컴퓨터 프로그램 수단 또는 컴퓨터 프로그램은 정보 처리 기능을 갖는 시스템으로 하여금 특정의 기능을 a) 다른 언어, 코드 또는 노테이션으로의 전환; b) 상이한 물질 형태에서의 재현 중 하나 또는 모두에서 직접 또는 그 후에 수행하도록 하는 명령어들 세트의 코드 또는 노테이션의 임의의 언어로된 임의의 표현을 의미한다.

도면의 간단한 설명

[0083] 본 발명의 바람직한 실시예들이 후속하는 개략적인 도면들을 참조하여 단지 예시를 통해 아래에서 상세하게 설명된다.

[0084] 도 1은 본 발명의 실시예에 따른 시스템의 개략적 도해를 도시한다.

[0085] 도 2는 본 발명에 따른 실시예의 메세지 흐름의 개략적 도해를 도시한다.

[0086] 도 3은 본 발명의 실시예에 따른 어써션 메세지의 개략적 도해를 도시한다.

[0087] 도 4는 본 발명의 실시예에 따른 어써션 메세지의 생성의 흐름도를 도시한다.

[0088] 도 5는 본 발명의 실시예에 따른 어써션 메세지의 검증의 흐름도를 도시한다.

[0089] 도 6은 WS-보안 표준의 포맷을 취하는 본 발명의 실시예에 따른 어써션 메세지 토큰의 개략적 도해를 도시한다.

[0090] 도면들은 오로지 설명을 위한 목적으로 제공된 것이며, 본 발명의 실용적 예시들을 반드시 일정한 실비율로 나타낸 것은 아니다.

[0091] **용어 해설**

[0092] 이하는 본 설명의 이해를 돕기 위한 비공식적인 정의들이다.

[0093] **사용자 또는 프로빙 당사자**: 자신의 ID가 관리되는 엔티티. 일반적으로 사용자 또는 프로빙 당사자는 개인이지만, 적어도 소규모의 기업체들이 예컨대 여행 예약과 정보 수집시에 개인과 꼭 같은 다른 기업체들과 종종 상호작용할 것이다. 다른 경우들에서, 프로빙 당사자는 자신에 관한 특성을 입증하는 하드웨어 장치이거나 또는 특성 증명에 의해 통신을 강화시키는 중간 당사자일 수 있다.

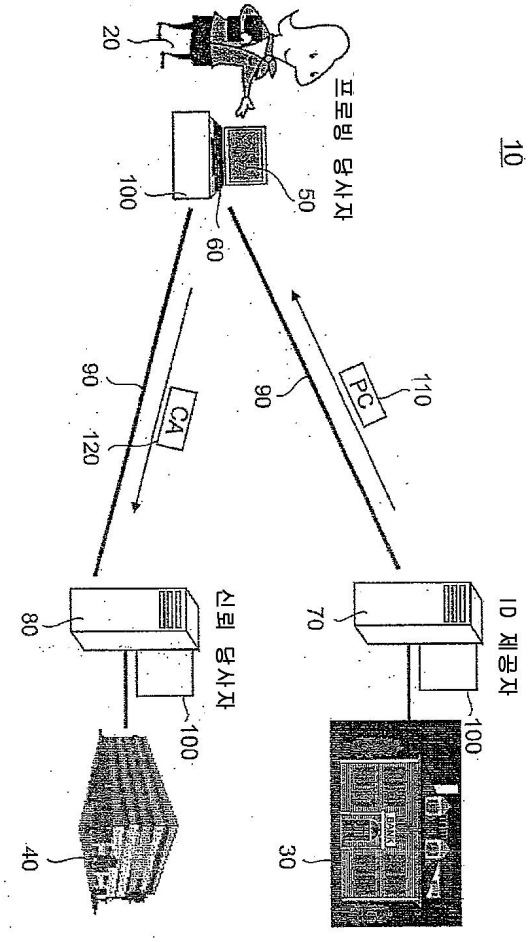
[0094] **신뢰 당사자**: 사용자 또는 프로빙 당사자의 성명 또는 속성을 알고자 하는, 예컨대 서버로 표현되는 엔티티, 예컨대 조직체. 조직체는 은행, 의사, 동료, 인터넷 서비스 제공자 및 가족과 같은 개인의 통신 파트너들 모두를 포함한다.

[0095] **ID 제공자**: 개인의 ID 관련 정보를 저장하는 엔티티. 이 엔티티는 은행, 인증기관(CA), 인터넷 서비스 제공자 등일 수 있다.

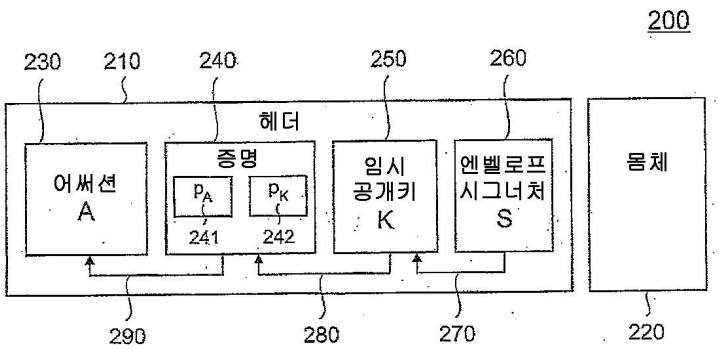
[0096] 용어 **컴퓨터**는 PC와 같은 장치뿐만 아니라, 디지털 보조 단말기, 이동 전화기 및 기타 전자 장치들을 포함한다.

도면

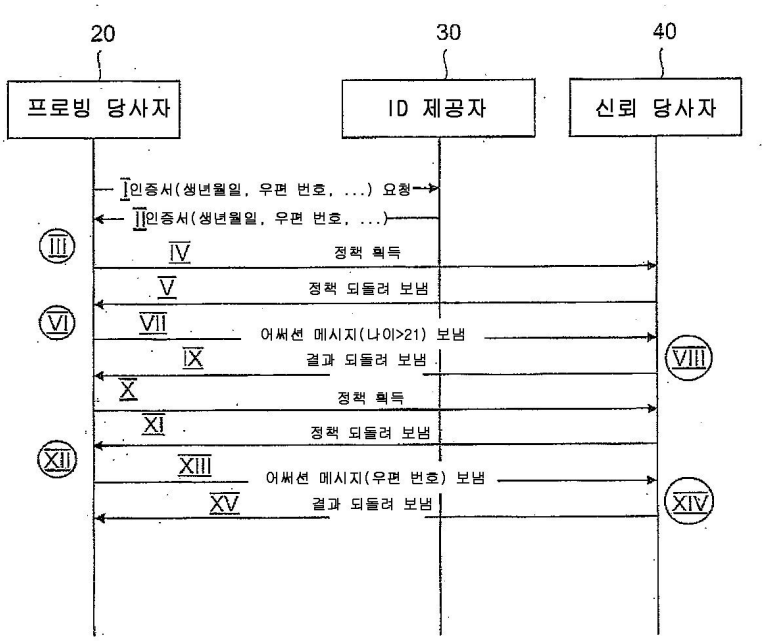
도면1


10
20
프로필 당사자
100
50
60
90
CA
120
90
PC
110
신뢰 당사자
80
100
40
ID 제공자
70
100
30

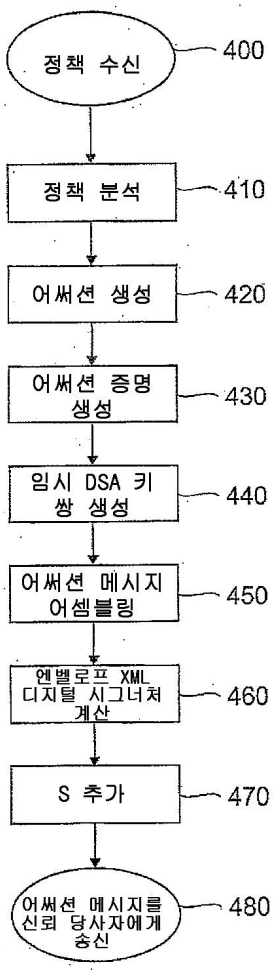
도면2


200
230
210
240
250
260
헤더
어써션
A
증명
P_A
P_K
241
242
임시
공개키
K
엔벨로프
시그너처
S
몸체
290
280
270
220

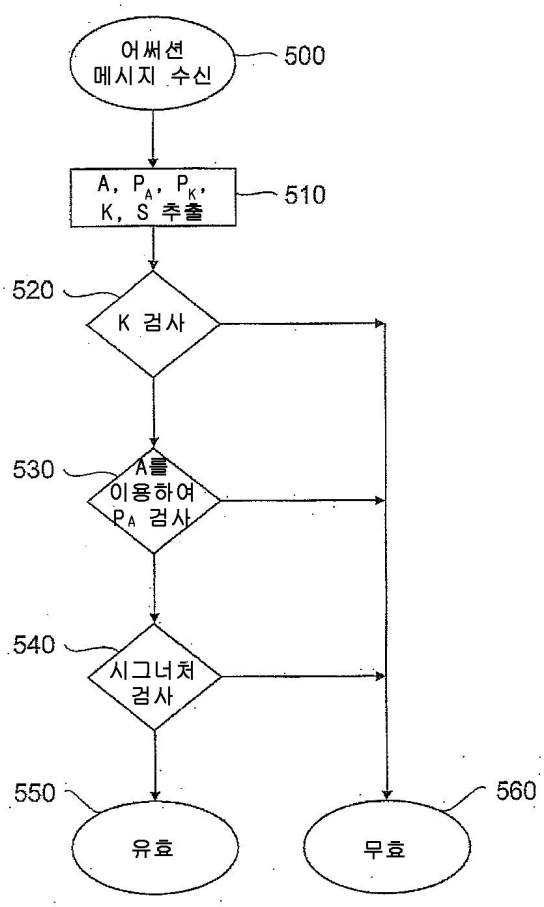
도면3


20
30
40
프로빙 당사자
ID 제공자
신뢰 당사자
I 인증서(생년월일, 우편 번호, ...) 요청
II 인증서(생년월일, 우편 번호, ...)
III
IV 정책 획득
V 정책 되돌려 보냄
VI
VII 어써션 메시지(나이>21) 보냄
IX 결과 되돌려 보냄
VIII
X 정책 획득
XI 정책 되돌려 보냄
XII
XIII 어써션 메시지(우편 번호) 보냄
XV 결과 되돌려 보냄
XIV

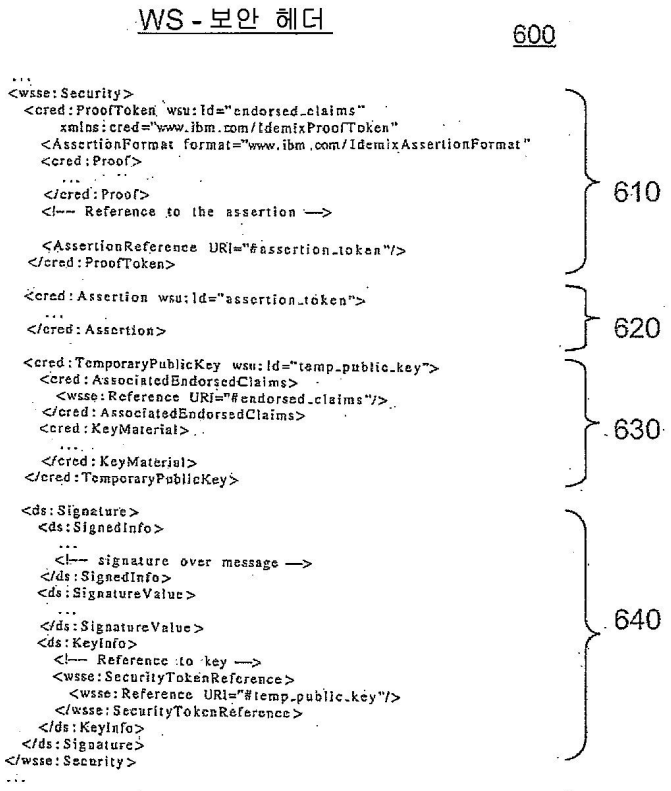
도면4


정책 수신
400
정책 분석
410
어써션 생성
420
어써션 증명 생성
430
임시 DSA 키 쌍 생성
440
어써션 메시지 어셈블링
450
엔벨로프 XML 디지털 시그너쳐 계산
460
S 추가
470
어써션 메시지를 신뢰 당사자에게 송신
480

도면5


어써션
메시지 수신
500
A, P_A, P_K,
K, S 추출
510
520
K 검사
530
A를
이용하여
P_A 검사
540
시그너쳐
검사
550
유효
560
무효

도면6


WS - 보안 헤더
600
610
620
630
640
...
<wsse:Security>
<cred:ProofToken wsu:Id="endorsed_claims"
xmlns:cred="www.ibm.com/IdemixProofToken"
<AssertionFormat format="www.ibm.com/IdemixAssertionFormat"
<cred:Proof>
...
</cred:Proof>
<!-- Reference to the assertion -->
<AssertionReference URI="#assertion_token"/>
</cred:ProofToken>
<cred:Assertion wsu:Id="assertion_token">
...
</cred:Assertion>
<cred:TemporaryPublicKey wsu:Id="temp_public_key">
<cred:AssociatedEndorsedClaims>
<wsse:Reference URI="#endorsed_claims"/>
</cred:AssociatedEndorsedClaims>
<cred:KeyMaterial>
...
</cred:KeyMaterial>
</cred:TemporaryPublicKey>
<ds:Signature>
<ds:SignedInfo>
...
<!-- signature over message -->
</ds:SignedInfo>
<ds:SignatureValue>
...
</ds:SignatureValue>
<ds:KeyInfo>
<!-- Reference to key -->
<wsse:SecurityTokenReference>
<wsse:Reference URI="#temp_public_key"/>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature>
</wsse:Security>
...