(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년10월22일
(11) 등록번호 10-0989487
(24) 등록일자 2010년10월15일

(51) Int. Cl.
G06F 15/00 (2006.01) *G06F 1/00* (2006.01)
H04L 29/06 (2006.01)
(21) 출원번호 10-2004-7018941
(22) 출원일자(국제출원일자) 2003년05월23일
심사청구일자 2008년05월23일
(85) 번역문제출일자 2004년11월23일
(65) 공개번호 10-2004-0105259
(43) 공개일자 2004년12월14일
(86) 국제출원번호 PCT/EP2003/005421
(87) 국제공개번호 WO 2003/100544
국제공개일자 2003년12월04일
(30) 우선권주장
02011440.1 2002년05월24일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
WO2001011450 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
텔레폰악티에볼라겟엘엠에릭슨(펍)
스웨덴왕국 스톡홀름 에스-164 83
(72) 발명자
버스봄액셀
독일 91364 운테르레인레이테르 스톤호퍼 베르그 3
퀸네트라프하엘
벨기에 비-4000 리에지 비세-보이에 66
(뒷면에 계속)
(74) 대리인
서장찬, 최재철, 박병석

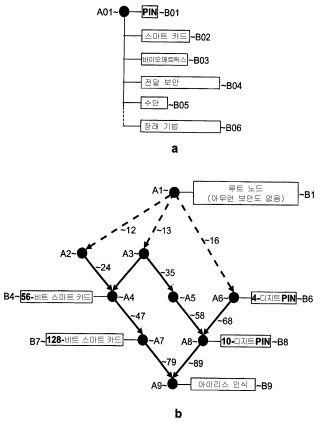
전체 청구항 수 : 총 34 항 심사관 : 임영희

(54) 서비스 제공자의 서비스에 대한 사용자를 인증하는 방법

(57) 요 약

서비스 제공자(SP)의 서비스에 대한 사용자의 인증을 위한 방법, 장치 및 컴퓨터 프로그램이 개시된다. 서비스 제공자(SP)의 서비스에 대한 사용자의 접근이 요구된다. 하나 이상의 인증 보안 프로파일은 상기 서비스 제공자(SP)에 의해 서비스에 대한 사용자의 인증을 위한 서비스 제공자(SP)의 인증 보안 요구 사항을 지정하기 위해 선택된다. 하나 이상의 선택된 인증 보안 프로파일의 지시 및 아이덴티티 제공자(IdP1)에 대해 사용자를 식별하는 사용자 아이덴티티는 서비스 제공자(SP)로부터 아이덴티티 제공자(IdP1)로 전송되어, 아이덴티티 제공자(IdP1)에 의해 사용자의 인증을 요구한다. 사용자는 사용자 아이덴티티 및 하나 이상의 선택된 인증 보안 프로파일 중 하나에 따라 인증된다. 서비스 제공자(SP)에 대한 사용자의 인증을 지시하는 어서션은 서비스 제공자(SP)에게 전송된다.

대 표 도 - 도1



(72) 발명자

슈바마코

독일 52457 알덴호벤 암 쉬와넨캄프 68

홀트만스실케

독일 52499 바에스베일러 울프스가쎄 26아

특허청구의 범위

청구항 1

서비스 제공자(SP)의 서비스에 대한 사용자의 인증 방법에 있어서,

상기 사용자에 대해 상기 서비스 제공자(SP)의 서비스로의 접근을 요구하는 단계,

상기 서비스 제공자(SP)에 의해 서비스에 대한 사용자의 인증을 위한 인증 보안 요구 사항을 특정하는 하나 이상의 보안 속성을 포함하는 하나 이상의 인증 보안 프로파일을 선택하는 단계,

아이덴티티 제공자(IdP1)에 의한 사용자의 인증을 요구하기 위해 하나 이상의 선택된 인증 보안 프로파일의 지시(indication) 및 사용자를 식별하는 사용자 아이덴티티를 상기 아이덴티티 제공자(IdP1)로 전송하는 단계,

사용자 아이덴티티 및, 하나 이상의 선택된 인증 보안 프로파일 중 하나를 기반으로 하여 사용자를 인증하는 단계 및,

사용자의 인증을 지시하는 어서션(assertion)을 서비스 제공자(SP)로 전송하는 단계를 포함하는 것을 특징으로 하는 사용자의 인증 방법.

청구항 2

제 1 항에 있어서,

상기 서비스 제공자(SP)는 인증을 위해 상기 아이덴티티 제공자(IdP1)에 의해 지원되도록 지시되는 하나 이상의 보안 프로파일의 그룹으로부터 하나 이상의 인증 보안 프로파일을 선택하는 것을 특징으로 하는 사용자의 인증 방법.

청구항 3

제 2 항에 있어서,

상기 서비스 제공자(SP)는 상기 아이덴티티 제공자(IdP1)로부터 하나 이상의 지원된 보안 프로파일의 그룹에 대한 지시를 수신하는 것을 특징으로 하는 사용자의 인증 방법.

청구항 4

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 인증이 실행됨에 기반으로 하는 상기 하나 이상의 선택된 인증 보안 프로파일 중 하나는 선택된 인증 보안 프로파일로부터 상기 아이덴티티 제공자(IdP1)에 의해 선택되는 것을 특징으로 하는 사용자의 인증 방법.

청구항 5

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 하나 이상의 선택된 인증 보안 프로파일은 하나 이상의 관계(relations)에 의해 하나 이상의 다른 인증 보안 프로파일에 관계되며, 각 관계는 인증 보안 강도에 관해 상기 하나 이상의 다른 인증 보안 프로파일에 대한 상기 하나 이상의 선택된 인증 보안 프로파일의 순서를 나타내며, 상기 사용자를 인증하는 단계는,

상기 아이덴티티 제공자(IdP1)에 의해, 상기 인증 보안 강도에 관해, 상기 하나 이상의 선택된 인증 보안 프로파일과 비교해 동등하거나 보다 강하게 관계되는 상기 하나 이상의 다른 인증 보안 프로파일 중 하나를 선택하고,

선택된 상기 하나 이상의 다른 인증 보안 프로파일 중 하나를 기반으로 하여 사용자를 인증함으로써 실행되는 것을 특징으로 하는 사용자의 인증 방법.

청구항 6

제 5 항에 있어서,

상기 서비스 제공자(SP)는 하나 이상의 다른 인증 보안 프로파일에 대한 하나 이상의 관계를 특정하고, 상기 서

비스 제공자(SP)는 하나 이상의 다른 인증 보안 프로파일에 대한 하나 이상의 관계의 지시를 상기 아이덴티티 제공자(IdP1)로 전송하는 것을 특징으로 하는 사용자의 인증 방법.

청구항 7

제 1 항에 있어서,

상기 어서션은 인증이 실행됨에 기반으로 하는 인증 보안 프로파일의 지시로 보강되고, 지시된 인증 보안 프로파일은 수락을 위해 서비스 제공자(SP)에 의해 검사되는 것을 특징으로 하는 사용자의 인증 방법.

청구항 8

서비스 제공자(SP)의 서비스에 대한 사용자의 인증 방법에 있어서,

상기 사용자에 대해 상기 서비스 제공자(SP)의 서비스로의 접근을 요구하는 단계,

아이덴티티 제공자(IdP1)에 의해 사용자의 인증을 요구하기 위해 사용자를 식별하는 사용자 아이덴티티를 아이덴티티 제공자(IdP1)로 전송하는 단계,

사용자 아이덴티티 및, 하나 이상의 보안 속성을 포함하는 인증 보안 프로파일을 기반으로 하여 사용자를 인증하는 단계,

사용자의 인증을 지시하는 어서션을 서비스 제공자(SP)로 전송하는 단계로서, 상기 어서션은 인증 보안 프로파일의 지시로 보강되는 단계, 및

서비스 제공자(SP)에 의해 수락을 위해 지시된 인증 보안 프로파일을 검사하는 단계를 포함하는 것을 특징으로 하는 사용자의 인증 방법.

청구항 9

제 1 항 또는 제 8 항에 있어서,

상기 서비스 제공자(SP)로부터 사용자 장치로 전송된 인증 요구에 응답하여, 서비스 제공자(SP)에서, 사용자 장치로부터 사용자 아이덴티티 및 아이덴티티 제공자(IdP1)의 레퍼런스(reference)를 수신하는 단계를 더 포함하는 것을 특징으로 하는 사용자의 인증 방법.

청구항 10

제 1 항 또는 제 8 항에 있어서,

상기 어서션을 기반으로 하여 서비스로의 접근을 승인하는 단계를 더 포함하는 것을 특징으로 하는 사용자의 인증 방법.

청구항 11

제 1 항 또는 제 8 항에 있어서,

상기 어서션 및 수락을 위한 검사를 기반으로 하여 서비스로의 접근을 승인하는 단계를 더 포함하는 것을 특징으로 하는 사용자의 인증 방법.

청구항 12

제 1 항 또는 제 8 항에 있어서,

인증 업그레이드 단계를 더 포함하는데, 상기 인증 업그레이드는 하나 이상의 다른 인증 보안 프로파일을 기반으로 하여 추가적 인증을 수행함으로써 실행되는 것을 특징으로 하는 사용자의 인증 방법.

청구항 13

제 12 항에 있어서,

상기 인증 업그레이드는 상기 다른 인증 보안 프로파일을 기반으로 하여 사용자의 추가적 인증을 실행하기 위한 다른 아이덴티티 제공자(IdP2)의 변경을 포함하는 것을 특징으로 하는 사용자의 인증 방법.

청구항 14

서비스 제공자(SP)에 관련된 장치로서, 메시지를 수신하는 수신 유닛, 메시지를 전송하는 송신 유닛 및, 메시지 및 정보를 처리하는 처리 유닛을 포함하는 서비스 제공자에 관련된 장치에 있어서,

상기 서비스 제공자(SP)의 서비스에 대한 사용자의 접근 요구를 수신하고,

상기 서비스에 대한 사용자의 인증을 위한 인증 보안 요구 사항을 특정하는 하나 이상의 보안 속성을 포함하는 하나 이상의 인증 보안 프로파일을 선택하며,

아이덴티티 제공자(IdP1)에 의해 사용자의 인증을 요구하기 위해 하나 이상의 선택된 인증 보안 프로파일의 지시 및 사용자를 식별하는 사용자 아이덴티티를 상기 아이덴티티 제공자(IdP1)에 전송하고,

상기 아이덴티티 제공자(IdP1)에 의해 사용자의 인증을 지시하는 어서션을 수신하도록 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장치.

청구항 15

제 14 항에 있어서,

인증을 위해 아이덴티티 제공자(IdP1)에 의해 지원되도록 지시되는 보안 프로파일의 그룹으로부터 하나 이상의 인증 보안 프로파일을 선택하도록 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장치.

청구항 16

제 15 항에 있어서,

상기 아이덴티티 제공자(IdP1)로부터 하나 이상의 지원된 보안 프로파일의 그룹의 지시를 수신하도록 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장치.

청구항 17

제 14 항 내지 제 16 항 중 어느 한 항에 있어서,

상기 장치는 하나 이상의 선택된 인증 보안 프로파일을 하나 이상의 다른 인증 보안 프로파일에 관계시키도록 구성되는데, 각 관계는 인증 보안 강도에 관해 상기 하나 이상의 다른 인증 보안 프로파일에 대한 상기 하나 이상의 선택된 인증 보안 프로파일의 순서를 나타내며, 상기 장치는 상기 인증 강도에 관해 동등하거나 보다 강하게 관계되는 하나 이상의 다른 인증 보안 프로파일에 대한 하나 이상의 관계를 인증을 위한 아이덴티티 제공자(IdP1)에 전송하도록 더 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장치.

청구항 18

제 14 항 내지 제 16 항 중 어느 한 항에 있어서,

상기 아이덴티티 제공자(IdP1)에 의해 사용자의 인증이 실행됨에 기반으로 하여 인증 보안 프로파일의 지시를 수신하도록 구성되고, 수락을 위해 지시된 인증 보안 프로파일을 검사하도록 더 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장치.

청구항 19

서비스 제공자(SP)에 관련된 장치로서, 메시지를 수신하는 수신 유닛, 메시지를 전송하는 송신 유닛 및, 메시지 및 정보를 처리하는 처리 유닛을 포함하는 서비스 제공자에 관련된 장치에 있어서,

상기 서비스 제공자(SP)의 서비스에 대한 사용자의 접근 요구를 수신하고,

사용자를 식별하는 사용자 아이덴티티를 아이덴티티 제공자(IdP1)에 의해 사용자의 인증을 요구하는 아이덴티티 제공자(IdP1)에 전송하며,

상기 아이덴티티 제공자(IdP1)로부터 사용자의 인증을 지시하는 어서션을 수신하는데, 상기 어서션은 하나 이상의 보안 속성을 포함하는 인증 보안 프로파일의 지시로 보강되며,

수락을 위해 지시된 인증 보안 프로파일을 검사하도록 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장

치.

청구항 20

제 14 항 또는 제 19 항에 있어서,

상기 서비스 제공자(SP)에 관련된 장치로부터 사용자 장치로 전송된 인증 요구에 응답하여, 사용자 장치로부터 사용자 아이덴티티 및 아이덴티티 제공자(IdP1)의 레퍼런스를 수신하도록 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장치.

청구항 21

제 14 항 또는 제 19 항에 있어서,

상기 어서션을 기반으로 하여 서비스로의 접근을 승인하도록 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장치.

청구항 22

제 14 항 또는 제 19 항에 있어서,

상기 어서션 및 수락을 위한 검사를 기반으로 하여 서비스로의 접근을 승인하도록 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장치.

청구항 23

제 14 항 또는 제 19 항에 있어서,

다른 인증 보안 프로파일을 기반으로 하는 추가적 인증을 기반으로 하여 인증 업그레이드를 실행하도록 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장치.

청구항 24

제 14 항 또는 제 19 항에 있어서,

추가적 인증을 실행하기 위해 다른 아이덴티티 제공자(IdP2)에 대한 인증 업그레이드를 위해 변화하도록 구성되는 것을 특징으로 하는 서비스 제공자에 관련된 장치.

청구항 25

아이덴티티 제공자(IdP1)에 관련된 장치로서, 메시지를 수신하는 수신 유닛, 메시지를 전송하는 송신 유닛 및, 메시지 및 정보를 처리하는 처리 유닛을 포함하는 아이덴티티 제공자에 관련된 장치에 있어서,

아이덴티티 제공자(IdP1)에 대해 사용자를 식별하는 사용자 아이덴티티 및, 서비스 제공자(SP)의 서비스에 대한 사용자의 인증을 위한 서비스 제공자(SP)의 인증 보안 요구 사항을 특정하는 하나 이상의 보안 속성을 포함하는 하나 이상의 인증 보안 프로파일의 지시를 포함하는 사용자의 인증 요구를 수신하고,

사용자 아이덴티티 및, 하나 이상의 인증 보안 프로파일 중 하나를 기반으로 하여 사용자를 인증하며,

서비스 제공자(SP)에 사용자의 인증을 지시하는 어서션을 전송하도록 구성되는 것을 특징으로 하는 아이덴티티 제공자에 관련된 장치.

청구항 26

제 25 항에 있어서,

상기 아이덴티티 제공자(IdP1)에 의해 인증을 위해 지원되는 하나 이상의 보안 프로파일의 그룹의 지시를 상기 서비스 제공자(SP)에 전송하도록 구성되는 것을 특징으로 하는 아이덴티티 제공자에 관련된 장치.

청구항 27

제 25 항 또는 제 26 항에 있어서,

상기 인증 보안 프로파일로부터 상기 인증이 실행됨에 기반으로 하는 상기 하나 이상의 인증 보안 프로파일 중

하나를 선택하도록 구성되는 것을 특징으로 하는 아이덴티티 제공자에 관련된 장치.

청구항 28

제 25 항에 있어서,

상기 하나 이상의 인증 보안 프로파일은 하나 이상의 관계에 의해 하나 이상의 다른 인증 보안 프로파일에 관계되며, 각 관계는 인증 보안 강도에 관해 상기 하나 이상의 다른 인증 보안 프로파일에 대한 상기 하나 이상의 인증 보안 프로파일의 순서를 나타내며, 상기 장치는 인증 보안 강도에 관해 상기 하나 이상의 인증 보안 프로파일과 비교해 동등하거나 보다 강하게 관계되는 상기 하나 이상의 다른 인증 보안 프로파일 중 하나를 선택하고, 선택된 상기 하나 이상의 다른 인증 보안 프로파일 중 하나를 기반으로 하여 사용자를 인증함으로써 사용자의 인증을 실행하도록 구성되는 것을 특징으로 하는 아이덴티티 제공자에 관련된 장치.

청구항 29

제 28 항에 있어서,

하나 이상의 다른 인증 보안 프로파일에 대한 하나 이상의 관계의 지시를 상기 서비스 제공자(SP)로부터 수신하도록 구성되는 것을 특징으로 하는 아이덴티티 제공자에 관련된 장치.

청구항 30

제 25 항에 있어서,

인증이 실행됨에 기반으로 하는 인증 보안 프로파일의 지시로 상기 어서션을 보강하도록 구성되는 것을 특징으로 하는 아이덴티티 제공자에 관련된 장치.

청구항 31

아이덴티티 제공자(IdP1)에 관련된 장치로서, 메시지를 수신하는 수신 유닛, 메시지를 전송하는 송신 유닛 및, 메시지 및 정보를 처리하는 처리 유닛을 포함하는 아이덴티티 제공자에 관련된 장치에 있어서,

아이덴티티 제공자(IdP1)에 대해 사용자를 식별하는 사용자 아이덴티티를 포함하는 사용자의 인증 요구를 수신하고,

상기 사용자 아이덴티티 및, 하나 이상의 보안 속성을 포함하는 인증 보안 프로파일을 기반으로 하여 사용자를 인증하며,

서비스 제공자(SP)에 사용자의 인증을 지시하는 어서션을 전송하는데, 상기 어서션은 상기 사용자의 인증이 실행됨에 기반으로 하는 인증 보안 프로파일의 지시로 보강되도록 구성되는 것을 특징으로 하는 아이덴티티 제공자에 관련된 장치.

청구항 32

제 25 항 또는 제 31 항에 있어서,

다른 인증 보안 프로파일을 기반으로 하는 추가적 인증을 기반으로 하여 인증 업그레이드를 실행하도록 구성되는 것을 특징으로 하는 아이덴티티 제공자에 관련된 장치.

청구항 33

서비스 제공자(SP)에 관련된 장치내에 적재 가능한 컴퓨터 프로그램을 저장한 기록 매체로서, 상기 서비스 제공자(SP)에 관계되는 한 제 1 항 또는 제 8 항에 따른 방법의 어느 단계를 실행하도록 구성되는 코드를 포함하는 컴퓨터 프로그램을 저장한 기록 매체.

청구항 34

아이덴티티 제공자(IdP1)에 관련된 장치내에 적재 가능한 컴퓨터 프로그램을 저장한 기록 매체로서, 상기 아이덴티티 제공자(IdP1)에 관계되는 한 제 1 항 또는 제 8 항에 따른 방법의 어느 단계를 실행하도록 구성되는 코드를 포함하는 컴퓨터 프로그램을 저장한 기록 매체.

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 인증 분야에 관한 것으로써, 특히 서비스 제공자의 서비스에 대한 사용자를 인증하는 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷 또는 전자 상거래에서 웹 사이트와 같이 전자식으로 이용 가능한 많은 서비스는, 기밀 정보 또는 서비스 또는 자원으로의 접근, 예컨대, 웹 기반 이메일 접근 또는 온라인 뱅킹을 제공하고, 사용자 프로파일에 적합한 개인용 서비스를 제공하며, 데이터 마이닝(mining)하며, 즉, 예컨대, 소비자로서의 사용자의 행동의 프로파일을 작성하는 서비스와 다수의 사용자의 상호 작용으로부터의 결론을 도출하거나, 예컨대, 사용자가 항상 계산서를 확실히 지불하게 함으로써 전자 상거래 시에 사용자의 신용도를 검증하는 것처럼 다수의 목적을 위한 사용자의 식별 및 인증을 필요로 한다. 사용자의 식별 및 인증은 또한 차량 또는 회사 빌딩 또는 운전대의 문과 같은 물리적 장치로의 접근하는 것처럼 다른 서비스 형식으로의 접근을 승인하는데 필요할 수도 있다.

[0003] 식별은 어떤 사용자 또는 사용자 그룹을 명백하게 식별하는 아이덴티티(identity)의 명세서(specification)를 의미한다. 지정된 아이덴티티는 특정인 또는 특정인 그룹을 추적할 수 있거나 추적할 수 없을 있다. 즉, 이 아이덴티티는 명백한 텍스트내에서 사용자의 이름일 수 있지만, 또한 랜덤하게 선택된 로그인 이름일 수도 있다. 유일한 요건은, 그룹 로그인의 경우에, 특정인 그룹으로부터 한 사람만이 등록하여, 특정 사용자 아이덴티티 하에 등록된 사용자의 식별이 가능하다는 것이다. 일례로서, 예컨대, 서비스 제공자의 서비스로 접근하기 위한 사용자의 로그인명이 있다. 인증은 아이덴티티의 검증, 예컨대, 어떤 아이덴티티를 제공하는 사용자가 실제로 초기에 동일한 아이덴티티로 등록한 사용자와 동일한 검증으로서 정의된다.

[0004] 인증은 사용자의 자격(credential)을 검증함으로써 행해진다. 본래, 사용자의 자격에는 3가지 타입이 있다. 첫째로, 사용자가 소유한 어떤 것, 예컨대, 키, 스마트 카드, 패스포트, 회사 아이덴티티 카드 등이고, 둘째로, 사용자가 알고 있는 어떤 것, 예컨대, 패스워드, 개인 식별 번호(PIN), 어머니의 처녀 이름 등이며, 셋째로, 사용자의 신체 상의 특징, 예컨대, 홍채 패턴, 음성, 지문, 안면 특징, 필적 등이다.

[0005] 사용자 인증은, 단일 또는 다수 타입의 자격, 예컨대, 단지 패스워드 대 PIN 코드의 지식과 조합한 회사 ID의 소유의 검증으로 이루어질 수 있다. 사용자 아이덴티티는, 예컨대, 사용자의 이름은, 식별 단계에서, 인증 시에 사용자로부터 수집된 사용자 자격을 등록된 사용자 아이덴티티와 관련된 사용자 자격과 관계시키는데 사용된다. 수집된 사용자 자격 및 등록된 사용자 자격이 일치함을 검증함으로써, 사용자 아이덴티티의 검증 및 인증은 달성될 수 있다. 따라서, 인증은 통상적으로 사용자의 전제 조건 및 등록이 통상적으로 인증에 필요할 시에 인증을 요구하는 엔티티(entity)의 식별을 포함한다.

[0006] 과거에는, 각 서비스 제공자는 통상적으로, 보안 전송 프로토콜을 이용하여, 예컨대, 가장 일반적으로 사용자명 및 패스워드를 통해 자신의 사용자 식별 및 인증을 실행하여, 자신의 사용자 프로파일 데이터베이스를 추적하였다. 사용자에 대한 결점으로서, 불편하고, 대부분의 경우에, 사용자가 그의 상이한 사용자 아이덴티티 및 대응하는 각각의 패스워드(자격)을 주목할 시에 상당히 안전하지 않은 상이한 서비스 제공자에 대해, 사용자는 통상적으로 사용자 아이덴티티 및 패스워드의 상이한 조합, 또는 사용자 아이덴티티 및 자격의 보다 일반적 상이한 조합을 기억해야 한다는 것이다. 사용자가 상이한 서비스 제공자에 대해 동일하거나 유사한 조합을 사용할 경우에는 보안이 절충(compromise)된다. 서비스 제공자에 대한 결점은, 서비스 제공자 자신의 데이터베이스를 유지하여, 자신에 의해 인증을 위한 모든 단계를 실행해야 하는 것이다. 게다가, 서비스 제공자 자신의 인증은 통상

적으로 기술적 및 경제적 이유로 인해 단일 또는 매우 제한된 수의 사용자 자격 타입에 기초로 하는데, 그 이유는 상이한 타입의 사용자 자격의 수집 및 처리를 위한 적절한 기반 구조(infrastructure)를 설정하는데에 비용이 많이 들어, 이동 전화에서 가입자 아이덴티티 모듈(SIM) 카드와 같은 스마트 카드 또는 바이오메트릭스에 기초한 방법과 같은 현대의 인증 방법을 소개하는데 상당한 장벽이 된다.

[0007] 최근에는, 많은 기술, 예컨대, Microsoft®Passport가 출시되었다. 예컨대, 2001년 3월, http://www.passport.com에 의해 발표된 Microsoft Passport Technical White Paper를 참조하며, 이는 실제 서비스로부터의 인증을 분리하는데 도움을 준다. 이 경우에, "Identity Provider"("IdP")는 사용자를 등록할 책임이 있고, 사용자가 서비스에 접근하기를 원할 때마다, 사용자를 인증할 책임이 있다. 사용자 등록 및 사용자 인증은 단일 엔티티에서 실시될 수 있거나 분리될 수 있다. 실제 서비스의 제공자("Service Provider", "SP")는 아이덴티티 제공자와 동일하거나 동일하지 않을 수 있다. 아이덴티티 제공자는 그 자체가 어떤 서비스의 제공자 역할을 하고, 또한 외부 서비스 제공자에게로 아이덴티티 서비스를 제공할 수 있다. Microsoft®Passport에서, Microsoft®Passport에 등록된 어떤 종류의 서비스에 접근하기 위해 패스워드 변경 구간에 어떠한 제한을 주지 않고, 사용자 인증은 항상 사용자명/패스워드 메카니즘을 통해 행해지고, SSL을 통해 전송된다.

[0008] 아이덴티티 제공자 및 서비스 제공자의 기능성을 분리함으로써, 많은 이점을 갖게 된다. 즉, 서비스 제공자는 반듯이 자신의 사용자 등록 및 인증을 처리할 필요가 없지만, 이들을 아이덴티티 제공자에게 "아웃소스(outsource)"할 수 있다. 그러나, 특히, 사용자는 상이한 서비스에 걸친 단일의 일관된 로그인 절차를 이용할 수 있다. 상술한 바와 같이, 오늘날 사용자는, 각 서비스 제공자에 대한 분리 인증 자격을 기억 및/또는 소유할 필요가 있거나, 물론, 보안성을 절충하는 패스워드와 같은 자격을 재사용할 필요가 있다. 예컨대, 침입자(attacker)는, 사용자가 웹 포탈에 입력하는 암호화되지 않은 패스워드를 엿들어, 그것을 사용하여 동일한 패스워드를 가진 사용자의 온라인 은행 구좌로 접근할려고 할 수 있다.

[0009] 그러나, 공지된 아이덴티티 제공자 솔루션 Microsoft®Passport는 상이한 서비스 또는 서비스 제공자에 대한 상이한 보안 요구 사항을 구별하지 않는다. 서비스 제공자에 의한 보안 요구 사항은 인증을 필요로 하는 목적에 상당히 의존할 수 있다. 개인용 웹 포탈을 간단히 제공하기 위해, 통상적으로, 은행 구좌로의 온라인 접근 또는 주요 금전 거래를 인증하기 위한 것보다 저 레벨로도 보안은 충분하다. 오히려, Microsoft®Passport는, 인증되거나 인증되지 않은 것과 같은 2진 결정이 단일 자격 타입에 기초한 인증을 고려하고, 사용자명-패스워드 조합에 따른 정적 인증 메카니즘이 아이덴티티 제공자 및 서비스 제공자의 양자 모두에 알려져 있고, 이전에 명백하거나 암시적으로 동의된 것을 추정한다. 이것은, 명백하게도, 무엇보다도 상이한 서비스/자원에 대한 상이한 타입의 보안 요구 사항에 대처할 수 없고, 시간외 보안 요구 사항의 변화에 대처할 수 없는 많은 결점을 가지고 있다. Passport형 아이덴티티 제공자는 인증 처리를 변경하기로 결정하면, 이것은 대역외 수단을 이용하여 각 서비스 제공자에 개별적으로 통신될 필요가 있거나, 서비스 제공자는 아이덴티티 제공자가 사용한 어떠한 변경이 "타당성"이 있기를 바란다.

[0010] WO 01/11450에는 다수의 정보 자원에 대한 인증에 관한 단일 부호를 위한 시스템 구조 및 방법이 개시되어 있다. 보안 구조는 트러스트 레벨(trust-level) 요구 사항을 정보 자원과 관련시키고, 패스워드, 인증서, 바이오메트릭스 기술 및 스마트 카드에 기초한 인증 방식은 이 트러스트 레벨과 관련된다. 충분한 트러스트 레벨로 사전(prior) 인증없이, 정보 자원으로 접근하기 위한 요구를 수신함과 동시에, 클라이언트 엔티티와 정보 자원 사이에 개입된 게이트키퍼(gatekeeper)는, 충분한 트러스트 레벨과 적당한 자격 타입의 세트 간에 대응(correspondence)을 확립하는 맵핑 규칙에 따라, 클라이언트 엔티티에 대한 로그인 자격을 획득하기 위한 자격 수집(gathering) 서비스를 이용한다.

[0011] WO 01/11450 A1에 기재된 시스템은 다수의 제한을 갖는다. 우선 첫째로, 그것은, 정보 자원과 트러스트 레벨 간의 연관(associations) 및, 트러스트 레벨과 인증에 이용된 자격 타입 간의 맵핑 규칙에 의존하며, 이들 양자 모두 아이덴티티 제공자 기능성을 제공하는 엔티티와 정보 자원 간의 연관 및 맵핑 규칙에 관한 사전 지식 및 사전 동의를 필요로 한다. 더욱이, 동일한 트러스트 레벨과 관련되는 모든 정보 자원은 동일한 방식으로 처리된다. 이것은, 특히 아이덴티티 제공자가 연관 및/또는 맵핑 규칙을 변경하기로 결정할 때마다 문제가 되는데, 그 이유는, 이런 변경에 의해 영향을 받는 모든 정보 자원(또는 각각의 정보 자원의 제공자)이, 예컨대, 보안, 기술적 또는 비지니스 관련 이유로 인해 이런 변경을 수락할 수 없기 때문이다. 따라서, 결국은, 정보 자원의 제공자 또는 정보 자원 자체가 아니라 아이덴티티 제공자가 인증 처리를 결정한다. 즉, 특정 자격이 특정 인증에 이용될 수 있음을 결정한다.

[0012] 그러나, 아이덴티티 제공자에 의해 취해진 이런 종류의 정책 결정은 많은 서비스 제공자를 위해 수락할 수 없다. 따라서, 연관 또는 맵핑 규칙의 갱신에 의해, 결과적으로 서비스 제공자와 충돌될 수 있다. 정적 또는 미리 규정된 연관 또는 맵핑 규칙은 수반된 엔티티의 요구 사항을 제공할만큼 유연하지 않다. 게다가, 그것은, 특히, 증가하는 다양한 인증 방법 및 때때로 급속히 변화하는 서비스 제공자의 요구 사항을 고려하여 모든 서비스 제공자 및 서비스의 타입에 대한 각종 보안 요구 사항을 충족하는 규정된 연관 또는 맵핑 규칙에 의해 인증 방식 및 자격 타입의 모든 가능 조합을 표현하는데 오히려 복잡하게 된다. 이와 같은 상당히 다양한 가능성에 대한 규정된 연관 또는 맵핑 규칙의 고유 불요성(inflexibility)으로 인해, 가능하다면, 동작을 갱신하는 성가신 연관 또는 맵핑 규칙은, 새로운 보안 요구 사항에 따른 인증이 행해질 수 있기 전에 실행되어야 한다. 이런 불요성에 의해, 특히, 특별한 상황, 예컨대, 어떠한 또는 유효 트러스트 레벨과 관련되지 않은 도입된 서비스로의 접근이 요구될 시에 결점이 있다. 다른 제한은, 접근된 클라이언트와 정보 자원 간의 세션(session) 중에 요구 및 응답을 포함하는 모든 정보 흐름이 경로내(in-path) 구성 요소로서 게이트키퍼를 통과한다는 것이다. 그러나, 사용자 클라이언트와 서비스 제공자 간의 완전한 정보 흐름을 위한 경로내 구성 요소로서 아이덴티티 제공자를 이용한다는 것은 아이덴티티 제공자에 대한 부하를 불필요하게 증가시킨다.

[0013] Microsoft®Passport 및 WO 01/11450 A1에 공통인 다른 제한은 단일 아이덴티티 제공자가 인증 목적을 위해 사용된다는 것이다. 이런 제한은 사용자 및 서비스 제공자로 하여금 단일 아이덴티티 제공자를 강제로 트러스트시킨다. 그러나, 중앙 집중식 인증 사례(instance)는 종종 프라이버시, 트러스트, 비지니스 또는 비용 이유 때문에 사용자 및 서비스 제공자에 수락될 수 없다. 예컨대, 사용자는, 불필요한 데이터 수집 또는 도용(fraud) 조차 방지하기 위해 단일 아이덴티티 제공자에 수집되는 상이한 타입의 자격과 같은 사용자 관련 정보를 원하지 않을 수 있다.

발명의 상세한 설명

[0014] 본 발명의 목적은 서비스 제공자의 서비스에 대한 사용자의 인증을 보다 안전하고 유연한 방식으로 제공하는 방법, 장치 및 컴퓨터 프로그램을 제공하기 위한 것이다.

[0015] 이 목적은 청구항 1 및 9에 기재된 바와 같은 방법에 의해 달성된다. 더욱이, 본 발명은 청구항 15, 21, 27 및 34에 기재된 장치 및, 청구항 36 및 37에 기재된 컴퓨터 프로그램에서 실시된다. 바람직한 실시예는 다른 청구항에 기재되어 있다.

[0016] 서비스 제공자의 서비스에 대한 사용자의 인증을 위한 방법이 개시된다.

[0017] 이 방법은 사용자가 서비스 제공자의 서비스로의 접근을 요구함으로써 개시할 수 있다. 이런 요구는 사용자의 장치로부터 서비스 제공자를 트리거하는 서비스 제공자로 전송되어, 다음의 단계에 따라 진행할 수 있다. 선택적으로, 이 요구는 미리 구성되어, 서비스 제공자, 예컨대, 미리 규정된 시간 또는 구간에 도달할 수 있다.

[0018] 접근 요구에 의해 트리거되면, 서비스 제공자는 서비스에 대한 사용자의 인증을 위한 인증 보안 요구 사항을 지정하는 하나 이상의 인증 보안 프로파일을 선택한다.

[0019] 이 방법은, 하나 이상의 선택된 인증 보안 프로파일 및 사용자를 식별하는 사용자 아이덴티티의 지시를 아이덴티티 제공자에 의해 사용자의 인증을 요구하는 아이덴티티 제공자에게 전송함으로써 진행한다. 즉, 서비스 제공자는, 관련 장치 또는, 예컨대, 서비스 제공자에 의해 원격적으로 수락 가능한 장치로부터, 하나 이상의 선택된 인증 보안 프로파일을, 인증이 실행될 수 있는 상기 프로파일 중 하나에 따른 하나 이상의 인증 보안 프로파일의 형식의 인증 보안 요구 사항을 아이덴티티 제공자에게 지시하기 위한 지시의 한 형식으로서 전송한다. 게다가, 사용자 아이덴티티는 인증 단계 동안에 사용자의 식별을 위한 아이덴티티 제공자에게 전송된다.

[0020] 그 다음, 사용자 아이덴티티 및 하나 이상의 선택된 인증 보안 프로파일 중 하나에 따라, 사용자는 아이덴티티 제공자에 의해 인증된다. 예컨대, 아이덴티티 제공자에게 사전에 등록된 바와 같은 사용자를 식별하여, 한 인증 보안 프로파일에 따라 사용자 아이덴티티에 기초하여 사용자를 검증함으로써 인증이 달성될 수 있다.

[0021] 최종으로, 아이덴티티 제공자에 의한 인증의 결과에 관한 정보는 서비스 제공자에게 전송될 수 있다. 특히, 사용자의 인증을 지시하는 어서션(assertion)은 서비스 제공자에게 전송되어, 예컨대, 사용자의 인증이 서비스 제공자에 의해 인증 보안 프로파일로 지정된 바와 같은 인증 보안 요구 사항에 따라 달성되었음을 지시한다. 실시 또는 사용 케이스에 따라, 어서션은, 예컨대, 인증에 사용된 한 인증 프로파일을 지정하거나, "인증 성공"을 간단히 지시할 수 있다. 어서션을 위한 다른 실시도 가능하다.

[0022] 본 발명의 방법은 서비스 제공자의 서비스에 대한 사용자의 인증을 개선하여, 특히 서비스 제공자에게 매우 안전하게 하는데, 그 이유는, 서비스 제공자 및 아이덴티티 제공자가 결국에는 서비스 제공자에 의해 선택되는 바와 같은 인증 보안 프로파일 중 하나에 따라 사용자의 인증을 위해 아이덴티티 제공자에 의해 충족되는 보안 요구 사항을 결정하기 때문이다. 이 방법은 또한 아이덴티티 제공자에 보다 안전한데, 그 이유는 서비스 제공자의 인증 요구 사항이 현재 적용하고, 사용자의 현재 인증에 충족되어야 하는 방법이 명백하고 활동 중에 구성될 수 있기 때문이다. 서비스 제공자의 인증 보안 요구 사항은 변경될 수 있다. 이 경우에, 서비스 제공자는 상기 방법을 보다 안전하게 할 뿐만 아니라, 서비스 제공자에 매우 유연하게도 하는 다른 인증 보안 프로파일을 선택함으로써 변경된 보안 요구 사항에 바로 적응할 수 있다. 따라서, 특히, 특별한 시나리오에서 뿐만 아니라, 서비스 제공자에 대한 인증 보안 요구 사항 변경에 따른 다른 상황 및 환경에서도, 서비스 제공자는 유연하게 동작할 수 있고, 아이덴티티 제공자로부터 인증을 요구할 시에 하나 이상의 선택된 인증 프로파일에 의해 변경된 인증 요구 사항을 아이덴티티 제공자에 바로 지정하여 통신될 수 있다. 더욱이, 상기 방법은 특정 단일 아이덴티티 제공자를 이용하는 서비스 제공자를 필요로 하지 않는다. 대신에, 임의의 아이덴티티 제공자는 인증을 위해 이용될 수 있다. 게다가, 그것은, 서비스 제공자와 클라이언트 사이에 개입되는 경로내 구성 요소로 아이덴티티 제공자를 가질 필요가 없다.

[0023] 양호한 실시예에 따르면, 하나 이상의 인증 보안 프로파일은, 예컨대, 인증 보안 요구 사항을 보다 정확히 지정하기 위한 적어도 하나의 보안 속성(attribute)을 포함한다. 서비스 제공자는 보안 속성을 지정함으로써 하나 이상의 인증 보안 프로파일을 어셈블(assemble)할 수 있다. 자신의 명세(specification)를 행함으로써, 서비스 제공자는 인증 보안 프로파일을 그의 보안 요구 사항에 정확히 맞출 수 있다. 서비스 제공자는, 선택적으로 또는 부가적으로, 미리 규정된 방식으로 배치된 하나 이상의 보안 속성을 포함하는 미리 규정된 인증 보안 프로파일을 선택할 수 있다. 아이덴티티 제공자 및/또는 사용자의 인증 기능(capabilities)은 하나 이상의 보안 속성에 따라 인증 보안 프로파일을 지정 및/또는 선택할 시에 고려될 수 있다. 보안 속성의 예는, 한 그룹의 자격, 트랜스포트 계층(transport layer) 보안, 네트워크 보안, 링크 계층 보안, 타이밍 정보, 정책, 도용 검출 측정, 책임(liability) 및/또는 보증 및 다른 보안 특성으로부터 항목을 나타낸 명세이다. 보안 속성은, 한 타입, 예컨대, 패스워드 또는 바이오메트릭스와 같은 자격 타입의 명세 및, 특정 타입에 관련된 값(value), 예컨대, 패스워드에 관련된 패스워드 길이, 또는 바이오메트릭스에 관련된 어떤 해상도의 지문의 명세를 포함할 수 있다. 보안 속성을 이용하여, 아이덴티티 제공자는, 서비스 제공자의 요구 사항에 따라, 사용자의 인증이 아이덴티티 제공자에 의해 실행되어야 하는 어느 보안 특성에 기초하여 서비스 제공자에 의해 정확히 구성될 수 있다.

[0024] 다른 양호한 실시예에 따르면, 서비스 제공자는, 인증을 위해 아이덴티티 제공자에 의해 지원되도록 지시되는 하나 이상의 보안 프로파일의 그룹으로부터 하나 이상의 인증 보안 프로파일을 선택한다. 하나 이상의 지원된 인증 보안 프로파일의 그룹으로부터 하나 이상의 인증 보안 프로파일을 선택함으로써, 성공적인 인증의 가능성이 증가된다.

[0025] 다른 양호한 실시예에 따르면, 서비스 제공자는, 예컨대, 지원된 인증 보안 프로파일의 리스트를 전송함으로써, 아이덴티티 제공자로부터 하나 이상의 지원된 보안 프로파일의 그룹에 대한 지시를 수신한다. 이 지시는 또한 이 그룹이 서비스 제공자에 의해 획득될 수 있는, 예컨대, 다운로드될 수 있는 서버에 지시한 URI일 수 있다. 다른 방식의 지시도 가능하다. 바람직하게는, 아이덴티티 제공자의 인증 기능의 변경이 일어날 시에, 예컨대, 아이덴티티 제공자가 자격 타입 및/또는 자격 값과 같은 어떤 보안 속성이 지원되지 않게 버릴 시에, 예컨대, 4개의 문자 보다 짧은 패스워드 길이가 더 이상 지원되지 않을 시에, 또는 아이덴티티 제공자가 신규 도입된 자격 타입 또는 값을 제공할 경우, 예컨대, 지문이 오늘부터 지원될 경우에는, 지시의 한 형식으로서 그룹 또는 그룹 자체에 대한 지시가 발생한다.

[0026] 다른 양호한 실시예에 따르면, 인증을 실행하는데에 따른 상기 하나의 인증 보안 프로파일은 하나 이상의 선택된 인증 보안 프로파일로부터 아이덴티티 제공자에 의해 선택된다. 그렇게 행함으로써, 아이덴티티 제공자는, 인증을 실행할 수 있는 선택된 인증 보안 프로파일 중 어느 하나에 따른 서비스 제공자에게 질의하는 것을 방지할 수 있다. 대신에, 아이덴티티 제공자는, 선택 및 지시된 인증 보안 프로파일의 모두가 서비스 제공자의 인증 보안 요구 사항을 충족하는 것으로 추정하여, 예컨대, 인증되어야 하는 아이덴티티 제공자 및/또는 사용자의 요구 또는 자격에 가장 잘 맞는 것을 선택할 수 있다. 더욱이, 사용자이 인증이 실제로 실행하는 것에 기초한 인증 보안 프로파일을 절충하기 위한 서비스 제공자와 아이덴티티 제공자 간의 상호 동작은 최소화되어, 성공적인 인증의 속도 및 가능성이 높아진다.

[0027] 다른 양호한 실시예에 따르면, 하나 이상의 선택된 인증 보안 프로파일은 하나 이상의 관계에 의해 하나 이상의 다른 인증 보안 프로파일과 관계될 수 있다. 이들 관계의 각각은, 인증 보안 강도에 관한 하나 이상의 인증 보

안 프로파일에 대한 하나 이상의 선택된 인증 보안 프로파일의 순서를 나타낸다. 이들 관계에 대한 예는, 예컨대, 2개의 인증 보안 프로파일 간의 관계 보다 더 우세하거나 동일하게 우세함을 나타내는 가장자리(edge)에 있다. 선택된 인증 보안 프로파일은 또한 서로와 관계될 수 있다. 하나 이상의 선택된 인증 보안 프로파일과 하나 이상의 다른 인증 보안 프로파일과의 관계, 즉, 선택된 및 다른 인증 프로파일과 각각의 관계의 전체에 관한 정보에 따라, 하나 이상의 선택된 인증 보안 프로파일 중 하나에 따라 사용자를 인증하는 단계는, 하나 이상의 선택된 인증 보안 프로파일에 비해 인증 보안 강도(strength)에 관해 동일하거나 보다 우세하게 관계되는 하나 이상의 다른 인증 보안 프로파일 중 하나를 아이덴티티 제공자에 의해 선택하여, 아이덴티티 제공자에 의해 선택된 바와 같은 다른 인증 보안 프로파일에 따라 사용자를 인증함으로써 실행될 수 있다. 따라서, 서비스 제공자의 인증 보안 요구 사항을 충족하는 인증 보안 프로파일의 종류 및 수가 확대된다. 확대된 인증 보안 프로파일의 종류 및 수로부터, 아이덴티티 제공자는 인증을 위한 한 인증 프로파일, 예컨대, 상술한 바와 같은 어떤 자격에 가장 잘 맞는 인증 프로파일을 유연하게 선택하여, 성공적인 인증 가능성 및 인증 속도를 증가시킬 수 있다.

[0028] 다른 양호한 실시예에 따르면, 서비스 제공자는 하나 이상의 다른 인증 보안 프로파일과의 하나 이상의 관계를 지정할 수 있고, 서비스 제공자는 하나 이상의 다른 인증 보안 프로파일과의 하나 이상의 관계의 지시를 아이덴티티 제공자로 전송할 수 있다. 그렇게 행함으로써, 하나 이상의 선택된 및 하나 이상의 다른 인증 보안 프로파일 간의 관계는 서비스 제공자의 인증 보안 요구 사항을 보다 정확히 반영하는데, 이 요구 사항은 인증을 위해 실제로 사용되도록 인증 보안 프로파일의 절충을 위한 보다 적은 상호 동작에 의해 인증을 보다 고속으로 달성할 수 있게 할 수 있다.

[0029] 다른 양호한 실시예에 따르면, 인증이 실행되는 것에 따른 인증 보안 프로파일의 지시로 어서션이 보강(supplement)되고, 지시된 인증 보안 프로파일은 수락(acceptance)을 위해 서비스 제공자에 의해 검사된다. 인증을 실행함에 따른 인증 보안 프로파일에 관한 정보를 서비스 제공자에게 제공함으로써, 서비스 제공자에 대한 보안성이 더욱 증가되고, 예컨대, 인증을 위해 실제로 이용된 인증 보안 프로파일이 현재 인증 보안 요구 사항을 충족하는 지를 검사할 가능성이 서비스 제공자에 제공된다.

[0030] 서비스 제공자의 서비스에 대한 사용자의 인증을 위한 방법이 개시된다. 이 방법은, 서비스 제공자의 서비스에 대한 사용자에 접근을 요구하는 단계, 아이덴티티 제공자에 의해 사용자의 인증을 요구하기 위해 사용자를 식별하는 사용자 아이덴티티를 아이덴티티 제공자로 전송하는 단계, 사용자 아이덴티티 및 인증 보안 프로파일에 따라 사용자를 인증하는 단계, 사용자의 인증을 지시하는 어서션을 서비스 제공자에 전송하는 단계로서, 상기 어서션은 인증 보안 프로파일의 지시로 보강(supplement)되는 단계 및, 서비스 제공자에 의해 수락을 위해 지시된 인증 보안 프로파일을 검사하는 단계를 포함한다.

[0031] 여기서, 서비스 제공자는 아이덴티티 제공자에게 인증 전에 보안 인증 요구 사항을 제공하지 않는데, 이는 어떤 실시에 바람직할 수 있다. 그러나, 서비스 제공자의 보안 요구 사항과 비교하여 사용자의 인증을 실행함에 따른 지시된 인증 보안 프로파일을 검사함으로써, 서비스 제공자는 서비스에 대한 사용자의 인증이 서비스 제공자의 인증 보안 요구 사항과 일치함을 검증할 수 있다. 더욱이, 아이덴티티 제공자에 의해 지원된 임의의 인증 보안 프로파일에 따른 인증이, 자격 검증이 필요하다면, 바람직하게는 사용자의 인증 기능과 일치된 인증에 이용될 수 있다는 사실로 인해 아이덴티티 제공자의 유연성은 증가될 수 있다. 결국, 서비스 제공자는 사용자가 인증되든지 충분히 인증되지 않는 지를 판단할 수 있다.

[0032] 양방의 방법은, 서비스 제공자로부터 사용자 장치로 전송된 인증 요구에 응답하여 사용자 장치로부터의 서비스 제공자에서 사용자 아이덴티티 및 아이덴티티 제공자에 대한 레퍼런스(reference)를 수신하는 단계를 더 포함한다. 사용자 장치와의 상호 동작은 매우 일반적이고, 실시를 쉽게 할 수 있다.

[0033] 수신 어서션에 따라, 이 어서션에 따른 서비스로의 접근이 승인될 수 있다. 선택적으로, 예컨대, 지시된 인증 보안 프로파일이 서비스 제공자의 인증 보안 요구 사항과 일치하는 지를 검사하여, 특히, 서비스 제공자에 대한 인증 보안성을 증가시킴으로써, 서비스로의 접근은 어서션 및 수락을 위한 검사에 따라 승인될 수 있다.

[0034] 다른 양호한 실시예에 따르면, 상기 방법은 인증 업그레이드 단계를 포함할 수 있다. 인증 업그레이드는 다른 인증 보안 프로파일에 따른 추가적인 인증을 수행함으로써 실행될 수 있다. 선택 및 추가적인 인증은, 상술한 바와 같이, 서비스 제공자의 서비스에 대한 사용자를 인증하는 방법의 선택 및 인증에 관한 어느 단계에 따라 실행될 수 있다. 예컨대, 서비스 제공자는 하나 이상의 인증 보안 프로파일을 선택하여, 이들을 사용자의 인증을 위해 이들 중 하나를 선택하는 아이덴티티 제공자로 전송할 수 있다. 아이덴티티 제공자는 관계에 따른 한 인증 보안 프로파일을 선택하여, 서비스 제공자에게 인증을 실행함에 따라 선택된 인증 보안 프로파일을 지시할

수 있으며, 이 서비스 제공자는, 예컨대, 인증을 위한 인증 보안 프로파일과 일치할 경우에 지시된 인증 보안 프로파일을 검사할 수 있다. 업그레이드 기능이 사용자 및 서비스 제공자에 제공하여, 보다 강력한 인증 보안 요구 사항을 가진 서비스에 접근할 경우에 세션(session)을 계속한다.

[0035] 다른 양호한 실시예에 따르면, 인증 업그레이드는, 추가적인 인증 보안 프로파일에 따른 사용자의 추가적인 인증을 실행하여, 이전의 아이덴티티 제공자가 서비스 제공자의 강력한 인증 보안 요구 사항에 따라 추가적인 인증 프로파일을 지원할 수 없을 경우에 서비스 세션을 계속하기 위한 추가적인 아이덴티티 제공자의 변경을 포함할 수 있다.

[0036] 본 발명은 또한 이들 장치에서 실시된다. 다음에는, 서비스 제공자에 관련된 장치 및 아이덴티티 제공자에 관련된 장치가 기술된다.

[0037] 서비스 제공자에 관련된 장치가 개시된다. 서비스 제공자에 관련된 장치는 메시지를 수신하는 수신 유닛, 메시지를 전송하는 송신 유닛 및, 메시지 및 정보를 처리하는 처리 유닛을 포함한다. 서비스 제공자에 관련된 장치는 서비스 제공자의 서비스에 대한 사용자의 접근을 위한 요구를 수신하고, 이 서비스에 대한 사용자의 인증을 위한 인증 보안 요구 사항을 지정하는 하나 이상의 인증 보안 프로파일을 선택하며, 하나 이상의 선택된 인증 보안 프로파일 및 사용자를 식별하는 사용자 아이덴티티의 지시를 아이덴티티 제공자에 의해 사용자의 인증을 요구하는 아이덴티티 제공자에 전송하고, 아이덴티티 제공자에 의해 사용자의 인증을 지시하는 어서션을 수신하도록 구성될 수 있다.

[0038] 바람직한 실시예에 따르면, 서비스 제공자에 관련된 장치는 인증 보안 요구 사항을 지정하기 위해 적어도 하나의 보안 속성을 포함하는 하나 이상의 인증 보안 프로파일을 선택하도록 구성될 수 있다.

[0039] 다른 바람직한 실시예에 따르면, 서비스 제공자에 관련된 장치는 인증을 위해 아이덴티티 제공자에 의해 지원되도록 지시되는 보안 프로파일의 그룹으로부터 하나 이상의 인증 보안 프로파일을 선택하도록 구성될 수 있다.

[0040] 다른 바람직한 실시예에 따르면, 서비스 제공자에 관련된 장치는 아이덴티티 제공자로부터 하나 이상의 지원된 보안 프로파일의 그룹에 대한 지시를 수신하도록 구성될 수 있다.

[0041] 다른 바람직한 실시예에 따르면, 서비스 제공자에 관련된 장치는 하나 이상의 선택된 인증 보안 프로파일을 하나 이상의 다른 인증 보안 프로파일에 관계시키도록 구성될 수 있는데, 각 관계는, 인증 보안 강도에 관한 하나 이상의 다른 인증 보안 프로파일에 대한 하나 이상의 선택된 인증 보안 프로파일의 순서를 나타내며, 상기 장치는, 상기 인증 강도에 관해 동일하거나 보다 강력하게 관계되는 하나 이상의 다른 인증 보안 프로파일에 대한 하나 이상의 관계를 인증을 위한 아이덴티티 제공자에 전송하도록 구성될 수 있다.

[0042] 다른 바람직한 실시예에 따르면, 서비스 제공자에 관련된 장치는 아이덴티티 제공자가 사용자의 인증을 실행함에 따른 인증 보안 프로파일의 지시를 수신하도록 구성될 수 있고, 상기 장치는 또한 수락을 위한 지시된 인증 보안 프로파일을 검사하도록 구성된다.

[0043] 선택적으로 또는 부가적으로, 서비스 제공자에 관련된 장치는, 서비스 제공자의 서비스에 대한 사용자의 접근을 위한 요구를 수신하고, 사용자를 식별하는 사용자 아이덴티티를 아이덴티티 제공자에 의해 사용자의 인증을 요구하는 아이덴티티 제공자에 전송하며, 아이덴티티 제공자로부터 사용자의 인증을 지시하는 어서션을 수신하도록 구성될 수 있으며, 상기 어서션은 수락을 위해 지시된 인증 보안 프로파일을 검사하기 위해 인증 보안 프로파일의 지시로 보강된다.

[0044] 다른 바람직한 실시예에 따르면, 서비스 제공자에 관련된 장치는, 서비스 제공자에 관련된 장치로부터 사용자 장치로 전송된 인증 요구에 응답하여, 사용자 장치로부터 사용자 아이덴티티 및 아이덴티티 제공자에 대한 레퍼런스를 수신하도록 구성될 수 있다.

[0045] 다른 바람직한 실시예에 따르면, 서비스 제공자에 관련된 장치는 상기 어서션에 따라 서비스로의 접근을 승인하도록 구성될 수 있다.

[0046] 다른 바람직한 실시예에 따르면, 서비스 제공자에 관련된 장치는 상기 어서션 및 수락을 위한 검사에 따라 서비스로의 접근을 승인하도록 구성될 수 있다.

[0047] 다른 바람직한 실시예에 따르면, 서비스 제공자에 관련된 장치는 다른 인증 보안 프로파일에 따른 추가적인 인증에 따라 인증 업그레이드를 실행하도록 구성될 수 있다.

[0048] 다른 바람직한 실시예에 따르면, 서비스 제공자에 관련된 장치는 추가적인 인증을 실행하기 위해 다른 아이덴티

티 제공자에 대한 인증 업그레이드를 변경하도록 구성될 수 있다.

[0049] 아이덴티티 제공자에 관련된 장치가 개시된다. 아이덴티티 제공자에 관련된 장치는 메시지를 수신하는 수신 유닛, 메시지를 전송하는 송신 유닛 및, 메시지 및 정보를 처리하는 처리 유닛을 포함한다. 아이덴티티 제공자에 관련된 장치는 사용자의 인증을 위한 요구를 수신하도록 구성될 수 있다. 이 요구는, 아이덴티티 제공자, 예컨대, 아이덴티티 제공자에 관련된 장치에 대한 사용자를 식별하는 사용자 아이덴티티 및, 서비스 제공자의 서비스에 대한 사용자의 인증을 위한 서비스 제공자의 인증 보안 요구 사항을 지정하는 하나 이상의 인증 보안 프로파일에 대한 지시를 포함한다. 아이덴티티 제공자에 관련된 장치는 또한, 사용자 아이덴티티에 따른 사용자 및 하나 이상의 인증 보안 프로파일 중 하나를 인증하여, 사용자의 인증을 서비스 제공자에게 지시하는 어서션을 전송하도록 구성될 수 있다.

[0050] 바람직한 실시예에 따르면, 아이덴티티 제공자에 관련된 장치는 인증을 실행함에 따른 한 인증 보안 프로파일내에 포함된 적어도 하나의 보안 속성에 따라 사용자를 인증하도록 구성될 수 있다.

[0051] 다른 바람직한 실시예에 따르면, 아이덴티티 제공자에 관련된 장치는 인증을 위해 아이덴티티 제공자에 의해 지원되는 하나 이상의 보안 프로파일의 그룹에 대한 지시를 서비스 제공자로 전송하도록 구성될 수 있다.

[0052] 다른 바람직한 실시예에 따르면, 아이덴티티 제공자에 관련된 장치는 하나 이상의 인증 보안 프로파일로부터 인증을 실행함에 따른 상기 하나의 인증 보안 프로파일을 선택하도록 구성될 수 있다.

[0053] 하나 이상의 인증 보안 프로파일은 하나 이상의 관계에 의해 하나 이상의 다른 인증 보안 프로파일에 관계될 수 있다. 하나 이상의 관계의 각각은, 인증 강도에 관한 하나 이상의 다른 인증 보안 프로파일에 대한 하나 이상의 인증 보안 프로파일의 순서를 나타낸다. 아이덴티티 제공자에 관련된 장치는, 하나 이상의 인증 보안 프로파일에 비해 상기 인증 보안 강도에 관해 동일하거나 보다 강력하게 관계되는 하나 이상의 다른 인증 프로파일 중 하나를 선택하여, 선택된 다른 인증 보안 프로파일에 따라 사용자를 인증함으로써, 사용자의 인증을 실행하도록 구성될 수 있다.

[0054] 다른 바람직한 실시예에 따르면, 아이덴티티 제공자에 관련된 장치는 하나 이상의 다른 인증 보안 프로파일에 대한 하나 이상의 관계에 대한 지시를 서비스 제공자로부터 수신하도록 구성될 수 있다.

[0055] 다른 바람직한 실시예에 따르면, 아이덴티티 제공자에 관련된 장치는 인증을 실행함에 따른 인증 보안 프로파일의 지시에 따른 어서션을 보강하도록 구성될 수 있다.

[0056] 선택적으로 또는 부가적으로, 아이덴티티 제공자에 관련된 장치는 사용자의 인증을 위한 요구를 수신하도록 구성될 수 있다. 이 요구는 아이덴티티 제공자, 예컨대, 아이덴티티 제공자의 장치에 대한 사용자를 식별하는 사용자 아이덴티티를 포함한다. 아이덴티티 제공자에 관련된 장치는, 사용자 아이덴티티 및 인증 보안 프로파일에 따라 사용자를 인증하여, 사용자의 인증을 서비스 제공자에 지시하는 어서션으로 전송하도록 구성될 수 있다. 상기 어서션은 사용자의 인증을 실행함에 따른 인증 보안 프로파일의 지시로 보강된다.

[0057] 다른 바람직한 실시예에 따르면, 아이덴티티 제공자에 관련된 장치는 다른 인증 보안 프로파일에 따른 추가적인 인증에 따라 인증 업그레이드를 실행하도록 구성될 수 있다.

[0058] 본 발명은 또한 하나 이상의 컴퓨터 프로그램에서 실시된다. 하나 이상의 컴퓨터 프로그램은 인증 방법의 어떠한 단계를 실행하기 위한 장치내에 적재 가능한 소프트웨어 코드 부분을 포함한다. 하나 이상의 컴퓨터 프로그램은 컴퓨터 판독 가능 매체 상에 저장될 수 있다. 컴퓨터 판독 가능 매체는 장치내나 외부에 배치되는 영구 또는 재기록 가능 메모리일 수 있다. 컴퓨터 프로그램은 또한, 예컨대, 신호의 시퀀스로서 케이블 또는 무선 링크를 통해 장치로 전송될 수 있다.

[0059] 특히, 서비스 제공자와 관련된 장치내에 적재 가능한 컴퓨터 프로그램이 개시된다. 이 컴퓨터 프로그램은, 서비스 제공자의 서비스에 대한 사용자의 접근을 위한 요구를 처리하고, 서비스에 대한 사용자의 인증을 위한 인증 보안 요구 사항을 지정하는 하나 이상의 인증 보안 프로파일을 선택하며, 하나 이상의 선택된 인증 보안 프로파일 및 사용자를 식별하는 사용자 아이덴티티의 지시를 아이덴티티 제공자에 의해 사용자의 인증을 요구하는 아이덴티티 제공자로의 전송을 초기화하며, 아이덴티티 제공자에 의해 사용자의 인증을 지시하는 어서션을 처리하도록 하는 코드를 포함한다.

[0060] 선택적으로, 컴퓨터 프로그램은, 하나 이상의 인증 보안 프로파일의 선택 및, 하나 이상의 인증 보안 프로파일의 지시를 아이덴티티 제공자로의 전송에 관한 소프트웨어 부분이 포함되지 않거나 스킵(skip)되는 포맷일 수 있고, 대신에 또는 부가적으로, 컴퓨터 프로그램은, 수락을 위해 사용자의 인증을 실행함에 따른 지시된 인증

보안 프로파일을 검사하도록 하는 코드를 포함하며, 지시된 인증 프로파일은 어서션과 관련하여 컴퓨터 프로그램내에 입력된다.

[0061] 더욱이, 아이덴티티 제공자에 관련된 장치내에 적재 가능한 컴퓨터 프로그램이 개시된다. 이 컴퓨터 프로그램은 사용자의 인증을 위한 요구를 처리하도록 구성된 코드를 포함하며, 이 요구는, 아이덴티티 제공자에 대한 사용자를 식별하는 사용자 아이덴티티 및, 서비스 제공자의 서비스에 대한 사용자의 인증을 위한 서비스 제공자의 인증 보안 요구 사항을 지정하는 하나 이상의 인증 보안 프로파일의 지시를 포함하여, 서비스 제공자로부터 수신된 하나 이상의 인증 보안 프로파일 중 하나 및 사용자 아이덴티티에 기초한 사용자의 인증을 실행하고, 사용자의 인증을 서비스 제공자에게 지시하는 어서션의 전송을 초기화한다.

[0062] 본 발명에 따른 방법을 컴퓨터 프로그램에 의해 실시하는 다른 방식도 가능하다. 특히, 컴퓨터 프로그램은 상술한 바와 같은 방법의 어떠한 실시예를 실시할 수 있다.

[0063] 다음에는, 본 발명의 상세한 실시예가 도면을 참조로 기술된다.

실 시 예

[0080] 인증 방법은 다음의 3개의 구성 요소로 이루어질 수 있다. 첫째로는, 구조적 확장 가능 및 기계 판독 가능 세트로서 하나 이상의 인증 보안 프로파일(ASProfs) 및 가능한 관계를 기술하는 데이터 구조가 있다. 이 데이터 구조를 기술하기 위해, 상이한 ASProfs 간의 관계, 예컨대 "보다 강하거나 동일한(is stronger than or equally strong as)"(≥)을 표현하기 위한 방향성(directed) 그래프가 이용될 수 있다. 이 그래프에서, 각 노드는 ASProf이고, 각 방향성 에지(edge)는 2개의 ASProfs 간의 관계를 표현한다. 둘째로는, 서비스 제공자의 서비스에 대한 사용자의 인증을 위해 이용되도록 ASProf에 일치시키는 방법이 있다. 서비스 제공자는 "wish list"를 감지하여 하나 이상의 요구된 ASProfs를 아이덴티티 제공자로 전송하여, 이에 응하여 이용되는 하나 이상의 ASProfs에 대한 제시를 선택적으로 행할 수 있는 지의 여부를 판단한다. 전(full) ASProfs를 전후로 전송하는 것과는 대조적으로, 레퍼런스 및 갱신을 이용함으로써, 교환 데이터가 감소될 수 있다. 다른 아이덴티티 제공자는 제 1 아이덴티티 제공자가 서비스 제공자에 대한 요구 사항을 충족할 수 없을 경우에 인증을 위해 접촉될 수 있다. 셋째로는, 세션(session) 동안 ASProf를 업그레이드하는 방법이 있는데, 세션 동안 ASProf를 업그레이드함으로써, ASProf의 재절충(re-negotiating)이 수반되고, 또한, 사용자 자격의 새로운 타당성 검사가 요구될 수 있다. 아이덴티티 제공자가 업그레이드된 ASProf를 충족할 수 없을 경우, 서비스 제공자는 업그레이드를 위해 선택적인 아이덴티티 제공자와 접촉할 수 있다.

[0081] 아이덴티티 X를 가진 것으로 주장하는 사용자가 실제로 이 아이덴티티와 관련된 사용자인 확실성의 레벨은 연속적으로 크기 조정(scale)될 수 있고, 다음의 것을 포함하지만, 이에 제한되지 않는 많은 요소에 의존할 수 있다:

[0082] - 인증을 우해 검증된 하나 이상의 타입의 사용자 자격, 예컨대, 패스워드는 PIN 코드와 조합하여 회사 ID보다 덜 안전한 것으로 고려될 수 있고;

[0083] - 클라이언트와 서버 간에 인증 정보(예컨대, 패스워드)를 통신할 시에 이용되는 전달, 네트워크 및 링크층 보안 특성, 예컨대, TLS, IPsec;

[0084] - 10 초 전에 입력된 최근 인증의 시간, 예컨대, PIN은 통상적으로 3일 전에 입력된 PIN 보다 더 안전한데, 그 이유는 침입자가 그 사이에 클라이언트 장치로의 허가되지 않은 접근을 획득할 수 있기 때문이며;

[0085] - 사용자 자격의 길이 및 복잡성, 예컨대, 패스워드 또는 PIN의 길이, 문자만을 포함한 패스워드 대 적어도 2개의 숫자 및 적어도 2개의 특정 문자를 포함하는 패스워드, 비밀 키의 길이 등;

[0086] - 비밀 사용자 자격의 취급, 예컨대, 얼마나 자주 패스워드를 변경해야 하는지, 그 후 얼마나 많은 변경이 구 패스워드를 재사용할 수 있는지, 아이덴티티 제공자가 비밀 사용자 자격 데이터의 신뢰성 및 무결성을 어느 정도 보호하는지에 관한 수단;

[0087] - 공중 키 기반 구조(PKI)가 이용되는지, 예컨대, 인증서 파기를 어떻게 처리되는지, 루트(root) 인증서가 신뢰되는 지 등을 처리하는 키에 관한 수단;

[0088] - 도용(fraud) 검출의 경우에 파기에 필요한 시간 및 자격의 파기를 위한 절차 뿐만 아니라 도용을 검출하기 위해 취해진 측정;

[0089] - 아이덴티티 제공자에 의해 도용의 경우에 서비스 제공자에 제공된 책임/보증;

[0090] - 아이덴티티 제공자에 등록할 시에 사용자의 "실" 아이덴티티를 검증하는 것, 예컨대, 웹 페이지 상에 이름 및 개인 데이터를 입력하는 것에 관한 수단이 허가증의 검증 보다 덜 안전한 것으로 고려될 수 있다.

[0091] 이 서류에서, 사용자 인증의 확실성 레벨에 영향을 주는 이들 및 다른 속성의 수집(aggregation)은 "인증 보안 프로파일"(ASProf)로서 지칭된다.

[0092] ASProf은 한 세트의 속성, 예컨대, 속성값을 가지거나 가지지 않고 상기에 주어진 이들 속성으로 기술된다. 예컨대, 공백 또는 디폴트 ASProf는 이 속성에 지정된 속성값을 가지지 않고 속성을 가질 수 있다. ASProf는 인증 자격을 다루고, 갱신하며, 파기하는 처리를 기술하는 수단을 포함하는 것을 알 수 있다. ASProf 기술은 바람직하게는 변경 가능하고, 확장 가능하며, 기계 판독 가능하다. 바람직하게는, eXtensible Markup Language(XML)은 언더라잉 메타 언어(underlying meta-language)로서 이용된다. ASProf가 통상적으로 폐쇄된 세트의 데이터가 아니지만, 바이오메트릭스(biometrics)와 같은 인증 기술 및 신규 보안 기술, 예컨대, 암호화 기술에 적합하도록 할 필요가 있을 수 있기 때문에 확장 가능성은 중요하다. 확장 가능성은 장래 속성이 ASProf내에 포함될 수 있고, 또한 소정의 ASProf의 속성을 대신하기 위한 요구 사항으로서 교환 가능성을 포함할 수 있도록 한다.

[0093] 도 1a는 PIN B01, Smart Card B02, Biometrics B03, Transport Security B04, 및 Policy B05와 같은 상이한 속성을 가진 ASProf A01의 일례를 도시한 것이다.

[0094] ASProf은 장래 속성에 의해, 예컨대, 인증을 위한 Future Technologies B06을 커버하기 위해 확장될 수 있다.

[0095] 속성 값은 ASProf의 속성에 지정될 수 있다. 예컨대, 속성 세트는, 수치적, 즉, "키 길이" = "128", 최소 패스워드 길이" = "10", 또는 기술적, 예컨대, "Transport Security" = "TLS Tunnelling" 또는 "Transport Security" = "WTLS"일 수 있는데, TLS는 Transport Layer Security로 지칭하고, WTLS는 Wireless TLS로 지칭한다. 도 1a를 참조하면, 속성 값은 다음과 같이 지정될 수 있다.

[0096] 속성	속성 값
[0097] PIN	10 문자
[0098] Smart Card	없음
[0099] Biometrics (예컨대, Fingerprint)	고 해상도 (200 kByte)
[0100] Transport Security	WTLS
[0101] Policy	없음

[0102] XML 내에 코드화된 속성을 가진 ASProf의 다른 예는 아래의 텍스트에 주어진 주석과 함께 아래의 테이블 A에 도시되어 있다. 어떤 속성 간의 관계는 아래 예에 존재한다.

AA1

```
<?xml version="1.0"?>
<ASProf>
  <user_credentials>
    <password>
      <min_length>5</min_length>
      <max_length>10</max_length>
      <max_session_duration>
        <unit>hours</unit>
        <value>8</value>
      </max_session_duration>
      <case_sensitive>yes</case_sensitive>
      <special_chars_required>
        none
      </special_chars_required>
      <digits_required>1</digits_required>
    </password>
```

[0103]

```
</user_credentials>

<transport_layer_security>                                    AA2
  <protocol>
    <type>TLS</type>
    <MAC>MD5</MAC>
    <MAC>SHA</MAC>
    <cipher>DES</cipher>
    <cipher>3DES</cipher>
  </protocol>
  <protocol>
    <type>SSL>/type>
  </protocol>
</transport_layer_security>

<security_policies>
  <password>                                                  AA3
    <max_validity>
      <unit>months</unit>
      <value>6</value>
    </max_validity>
    <first_reuse>10</first_reuse>
    <privacy_policy>
      http://www.idprovider.com/w3c/p3p.xml
    <privacy_policy>
  </password>
  <PKI>
    <trusted_CA>Verisign</trusted_CA>                         AA4
    <trusted_CA>RSA</trusted_CA>
    <trusted_CA>Thawte</trusted_CA>
  </PKI>
  <liability>                                                 AA5
    <max_liability>
      <unit>USD</unit>
      <value>0.00</value>
    </max_liability>
</security_policies>

<user_registration>
  <ID_verification>                                           AA6
    <type>email_confirmation</type>
  </ID_verification>
  <expiration>
    <time>
      <unit>months</unit>
      <value>6</value>
    </time>
  </expriation>
  <renewal>
```

[0104]

```
    <time>never</time>
  </renewal>
  <revocation>                                                AA7
    <guaranteed_revocation_time>
      <unit>minutes</unit>
      <value>30</value>
    </guaranteed_revocation_time>
  </revocation>
</user_registration>
</ASProf>
```

[0105]

[0106] 테이블 A: XML 내에 코드화된 ASProf의 예

[0107] 테이블 A에 대한 주석;

[0108] AA1: 패스워드가 최소 5 및 최대 10 문자를 가지고, 사용자 인증을 위해 사용된다. 재인증이 요구될 때까지의 최대 세션 기간은 8 시간이다. 패스워드는 케이스 감지 가능하고(case sensitive), 특정 문자를 포함하지 않지만, 적어도 하나의 수치적 문자를 포함해야 한다.

[0109] AA2: TLS는 전달 층의 허용 가능한 메시지를 안전하게 하는데 이용된다. 인증 알고리즘은 Message Digest Algorithm No. 5 (MD5) 및 Security Hash Algorithm (SHA)이고, 허용 가능한 암호화 알고리즘은 Data Encryption Standard (DES) 및 3배의 DES이다. SSL은 또한 TLS 대신에 전달 층의 보안 프로토콜로서 허용된다.

[0110] AA3: 패스워드는 적어도 6 달 마다 변경되어야 하고, 구 패스워드는 적어도 10개의 다른 패스워드가 사용될 때까지 재사용될 수 없다. 사용자 데이터를 처리하기 위한 상세 비밀 수단은 주어진 URL에서 발견될 수 있다.

[0111] AA4: Versign, RSA 및 Thawte는 루트 증명 인증으로서 신뢰된다.

[0112] AA5: 아이덴티티 제공자는 도용 또는 아이덴티티 절도에 대한 책임($0.00)을 지지않는다.

[0113] AA6: 등록 시에, 사용자 아이덴티티는 이메일 주소로 전송된 확인 이메일을 이용하여 확인된다. 등록은 6 달 동안에 계정(account)이 사용되지 않을 시에 만료된다. 이 등록의 정규 갱신은 요구되지 않는다.

[0114] AA7: 자격의 검출된 도용 또는 누출의 경우에 계정은 30 분내에 차단(취소)되어야 한다.

[0115] 다수의 ASProfs은 바람직하게는 인증 보안 강도에 대해 관계된다. ASProfs의 순위 및 순서를 나타내는 관계는 방향성 그래프에 의해 기술될 수 있다. 이 그래프에서, 각 노드는 ASProf이다. 이 그래프는 공백 ASProf, 즉, 아무런 보안도 없음(no security whatsoever)일수 있는 "루트 노드"를 가질 수 있다. 각 방향성 에지는 2개의 ASProfs 간의 관계, 예컨대, a "≥" relation을 특정한다. ASProfs의 세트 및 ASProfs 간의 관계의 기술은 바람직하게는 변경 가능하고, 확장 가능하며, 기계 판독 가능하다. 바람직하게는, XML은 언더라잉 메타 언어로서 이용된다.

[0116] 특정 케이스, 예컨대, 그래프가 n 차원 그리드가 되는 케이스(n 속성의 케이스)가 생각할 수 있다. 이 경우에, 각 속성에 대한 독립 관계가 있고, 2개의 ASProfs의 비교는 각 속성의 개별 비교에 대응한다. a ≥ relation을 가진 2개의 ASProfs 간의 비교를 위한 일례로서:

[0117] key length 1 ≥ key length 2 AND password length 1 ≥ password length 2인 경우,

[0118] ASProf1 ≥ ASProf2이다.

[0119] 그러나, 보다 많은 일반적 그래프 표기는 보다 많은 복잡한 명세를 허용한다. 예컨대, 키 길이 64를 가진 지문 인식은 키 길이 256를 가진 패스워드 보다 더 안전하다. "사과와 오렌지의 비교"의 케이스는 완전히 상이한 인증 메카니즘이 단일 시스템에 이용될 시에 중요하게 된다. 이 그래프 표기는 개별 속성이 독립적으로 처리되는 다른 개념보다 더 일반적이고, 다른 인증 방법 및 기법 간의 우선 순위를 나타낸다.

[0120] 이 그래프는 원칙적으로 각 서비스 제공자에 의해 작성될 수 있고, 상이한 서비스 제공자는 상이한 그래프를 사용할 수 있다. 서비스 제공자는 예컨대, 상이한 사용자 또는 아이덴티티 제공자 또는 서비스에 대한 다수의 그래프를 가질 수 있다. 이것은, 각 서비스 제공자가 바람직하게는 인증 보안 특성에 관한 자신의 선택 및 우선 순위를 정할 수 있는 요구 사항을 반영한다. 제 1 서비스 제공자는 키워드보다 더 안전한 아이리스 스캔(iris scan)을 고려할 수 있다. 제 2 서비스 제공자는 보다 안전한 키워드를 고려할 수 있다. 물론, 이것은, 서비스 제공자가 그렇게 행하기를 바랄 경우에, "디폴트" 그래프의 재사용을 배제하지 않는다.

[0121] 도 1b에서는, ASProfs 그래프의 일례가 도시된다. 이 그래프는 포인트로 표시되고, 2개의 ASProfs 간의 a ≥ relation를 나타내는 화살표로 접속되는 ASProfs A1, A2, A3, A4, A5, A6, A7, A8, A9를 포함한다. 도 1b의 그래프 표시에 이용된 화살표 표기는, 화살촉(arrowhead)에 의해 2개의 ASProfs을 접속하는 화살표가 2개의 ASProfs의 다른 ASProf과 비교되는 ≥인 2개의 ASProfs 중 하나를 나타내는 것을 의미한다. 즉, ASProf1 → ASProf2는 ASProf2 ≥ ASProf1임을 의미한다. ASProfs 간의 ≥ 관계를 나타내는 화살표 12, 13, 16, 24, 35, 47, 58, 68, 79, 89는 그래프에서 발견될 수 있다.

[0122] 스마트 카드, PIN 및 바이오메트릭스의 속성 및 속성 값은 ASProfs에 관계된다. 특히, ASProf A4는 56 비트 스마트 카드 속성 B4를 포함하고, ASProf A7은 128 비트 스마트 카드 속성 B7을 포함하며, ASProf A6은 4 디지트 PIN 속성 B6을 포함하고, ASProf A8은 10 디지트 PIN 속성 B8을 포함하며, ASProf A9는 아이리스 인식 속성 B9를 포함한다. 다른 속성 또는 속성의 조합은 도 1에서 ASProfs에 관계될 수 있다. 게다가, "아무런 보안도 없음"을 나타내는 루트 노드 ASProf A1은 도 1b에서 관계 12, 13 및 16를 통해 설정되어, ASProfs, 예컨대,

ASProfs A2, A3, A6에 관계될 수 있다. 다른 ASProfs 또는 관계는 그래프내에 포함될 수 있고, 현행 ASProfs 또는 관계는 변경되거나 삭제될 수 있다.

[0123] 10 디지트를 가진 PIN의 지식은 4 디지트를 가진 PIN의 지식 보다 ≥인 것으로 설정된다. 이 ≥ 관계는, 4 디지트 PIN 속성 B6을 포함하는 ASProf A6에서 개시하고, 10 디지트 PIN 속성 B8을 포함하는 ASProf A8을 가르키는 화살표 68에 의해 표시된다. 128 비트 비밀 키를 가진 스마트 카드의 소유는 56 비트 비밀 키를 가진 스마트 카드의 소유 보다 ≥인 것으로 설정된다. 이에 대응하여, ASProf B7과 ASProf B4 간의 ≥ 관계는 56 비트 스마트 카드에서 128 비트 스마트 카드로 지적하는 화살표 47에 의해 표시된다. 또한, 아이리스 인식 방법은 제각기 화살표 89 및 79를 가진 스마트 카드 상에서 10 디지트 패스워드 보다 ≥이고, 128 비트 비밀 키 보다 ≥인 것으로 설정되며, 각각 ≥ 관계를 표시할 수 있다. 그러나, 10 디지트 패스워드가 스마트 카드 상에서 128 비트 비밀 키 보다 ≥인 지의 여부를 판단할려는 많은 감지를 할 수 없다. 2개의 ASProfs 간의 ≥ 관계가 실행할 수 없거나 원하지 않는 경우에, 대응하는 화살표는 그래프에서 없어진다.

[0124] 도 1b에 도시된 그래프의 XML 표시의 일례는 아래에 주어진다. 일반적으로 방향성 그래프를 표시하는데 이용되는 2개의 데이터 구조가 있다. 즉, (1) 각 쌍이 (때때로 또한 화살표 또는 관계로 지칭되는) 방향성 에지를 표시하고, 이 쌍의 제 1 요소는 발신 ASProf를 지정하고, 제 2 요소는 각각의 방향성 에지의 종료 ASProf를 지정하는 쌍의 리스트인 인접한 리스트를 이용하는 데이터 구조가 있고, (2) 각 발신 노드가 그래프에서 에지가 존재하는 종료 노드의 리스트를 포함하는 근접 행렬을 이용하는 데이터 구조가 있다. 아래의 테이블 B에 주어진 예에서, 근접 행렬 표시가 이용된다. 다른 표시도 가능하다.

```
<?xml version="1.0"?>
<ASProf_graph>
  <ASProf>
    <name>A1</name>                                    BB1
    <successor>A2<successor>
    <successor>A3<successor>
    <successor>A6<successor>
  </ASProf>

  <ASProf>                                             BB2
    <name>A2</name>
    ...
    <successor>A4<successor>
  </ASProf>
```

[0125]

```
<ASProf>
  <name>A3</name>
  ...
  <successor>A4<successor>
</ASProf>

<ASProf>
  <name>A4</name>
  <user_credentials>                                    BB3
    <smart_card>
       <key_length>56</key_length>
    </smart_card>
  </user_credentials>
  <successor>A7<successor>
</ASProf>

<ASProf>
  <name>A5</name>
  ...
  <successor>A8<successor>
</ASProf>

<ASProf>
  <name>A6</name>
  <user_credentials>                                    BB4
    <PIN>
       <digits>4</digits>
    </PIN>
  </user_credentials>
  <successor>A8<successor>
</ASProf>

<ASProf>
  <name>A7</name>
  <user_credentials>                                    BB5
    <smart_card>
       <key_length>128</key_length>
    </smart_card>
  </user_credentials>
  <successor>A9<successor>
</ASProf>

<ASProf>
  <name>A8</name>
  <user_credentials>
    <PIN>                                               BB6
       <digits>10</digits>
    </PIN>
  </user_credentials>
```

[0126]

```
    <successor>A9<successor>
  </ASProf>

  <ASProf>
    <name>A9</name>
    <user_credentials>
      <biometrics>                                      BB7
         <type>iris_scan</type>
      </biometrics>
    </user_credentials>
  </ASProf>
</ASProf_graph>
```

[0127]

[0128] 테이블 B: XML 내에 인코드화된 도 1b에 따른 관계를 가진 ASProf의 예.

[0129] 테이블 B에 대한 주석;

[0130] BB1: A1는 그래프의 루트 노드이고, 공백 ASProf, 즉, 보안 특성을 전혀 갖지 않음을 나타낸다.

[0131] BB2: 루트 노드 A1에서 노드 A2, A3 및 A6까지 그래프에 방향성 에지가 있다. 노드의 "후속자(successor)"는 발신 노드보다 "강하거나 동일한"것으로 설정된다.

[0132] BB3: 도 1b에 따라, 속성 값 "56 비트"를 가진 속성 B4의 "스마트 카드"는 ASProf A4에 관련된다.

[0133] BB4: 도 1b에 따라, 속성 값 "4 디지트"를 가진 속성 B6의 "PIN"은 ASProf A6에 관련된다.

[0134] BB5: 도 1b에 따라, 속성 값 "128 비트"를 가진 속성 B7의 "스마트 카드"는 ASProf A7에 관련된다.

[0135] BB6: 도 1b에 따라, 속성 값 "10 디지트"를 가진 속성 B8의 "PIN"은 ASProf A8에 관련된다.

[0136] BB7: 도 1b에 따라, 속성 값 "아이리스 인식"을 가진 속성 B9의 "바이오메트릭스"는 ASProf A9에 관련된다.

[0137] 또한, ASProf의 속성은 계층 구조를 가질 수 있다. 예컨대, "키 길이" 속성은, 다음의 보다 고 레벨 속성이 "TLS Tunnelling" 또는 "WTLS"를 지정하는 지에 따라 상이한 해석을 가질 수 있다. 그래서, "키 길이" 속성의 수치적 값은, 먼저 다음의 보다 고 레벨 속성을 비교하지 않고, 항상 서로 직접 비교될 수 없다.

[0138] 수치적 속성 값의 경우에, 예컨대, 보다 큰 키 길이가 항상 보다 고 인증 보안 강도를 의미한다는 점에서, 속성 값과 인증 보안 강도 간에 단조(monotonous) 관계일 필요가 없다. 도 2는 비단조 관계의 일례를 도시한 것으로, 이 예에서, around 9의 패스워드 길이는 인증 보안 강도에 관해 최적인 것으로 생각된다. 보다 짧은 패스워드는 덜 보안적인 것으로 고려되는데, 그 이유는, 이 패스워드가, 예컨대, 매우 짧은 길이의 경우의 억지 침입(brute-force attack) 및 보다 긴 패스워드의 어휘 침입에 의해 보다 쉽게 브레이크(break)시키기 때문이다. 그러나, 9 보다 훨씬 긴 패스워드는 또한 덜 보안적인 것으로 고려되는데, 그 이유는, 기억하기가 너무 어려워 사용자가 기록해 두어야 할 것 같기 때문이다. 속성 값 "패스워드 길이"와 대응하는 인증 보안 길이 간의 관계는 도 2의 상부에 도시되어 있다. 하부는 이 맵핑이 방향성 그래프로 어떻게 표시될 수 있는 가를 나타내지만, 다른 표시도 생각할 수 있다. 속성 패스워드 길이를 가진 제 1 ASProf와, 속성 패스워드 길이를 가진 제 2 ASProf 간의 관계는 이에 대응하여 하나의 화살표가 보다 강한 (">") 관계를 표시하는 화살표로 표시된다. 즉, 제 1 ASProf는, 제 2 ASProf에서 시작하고, 제 1 ASProf에서의 화살촉으로 끝나는 화살표에 의해, 제 2 ASProf 보다 더 강한 (">") 것으로 지시된다. 제 1 ASProf 및 제 2 ASProf는, 부가적인 화살표가 제 1 ASProf에서 시작하고, 제 2 ASProf에서의 화살촉으로 끝날 경우에 동일한 길이 ("=")인 것으로 지시된다. 예컨대, 2개의 패스워드 길이의 강도가 동일함을 나타내는 "=" 관계는, 제 1 화살표가 제 1 패스워드 길이로부터 제 2 패스워드 길이로 향하고, 제 2 화살표가 제 2 패스워드 길이로부터 제 1 패스워드 길이로 향하는 2개의 화살표로 표시된다. 이 예에서, 11 내지 20 문자를 가진 패스워드는 3 내지 6 문자를 가진 패스워드와 동일한 인증 보안 강도인 것으로 설정된다.

[0139] 사실상, 그것은 서비스 제공자가 자신의 선택 및 우선 순위를 결정하도록 서비스 제공자에게 완전히 남겨질 수 있다. 예컨대, 제 1 서비스 제공자는 단조 맵핑을 결정할 수 있고, 다른 서비스 제공자는 도 2에 따라 맵핑을 결정할 수 있으며, 제 3 서비스 제공자는 맵핑의 상세 사항에 관심을 가질 필요없이 아이덴티티 제공자에 의해 디폴트 그래프를 액셉트할 수 있다.

[0140] 도 2의 예는 비단조 관계가 방향성 그래프에 어떻게 표시될 수 있는 지를 나타낸 것이다. 이것은 또한 그래프 표시에서 속성 값의 범위, 예컨대, "7-10 문자"가 단일 노드에 어떻게 축약(collapse)될 수 있는 지를 설명하며, 즉, 각 허용된 수치적 값이 그래프에 별개의 노드를 형성하는 요구 사항이 없음을 나타낸다.

[0141] 다음에는, 하나 이상의 아이덴티티 제공자에 의한 서비스 제공자(SP)의 서비스에 대한 사용자 인증에 대해 기술된다.

[0142] 도 3에 따르면, 메시지(1a)를 통해 서비스 요구를 전송함으로써, 서비스 제공자(SP)에 의해 제공되고, 사용자가 간절히 원하는 서비스에 클라이언트는 접촉한다. 이 서비스는 사용자 인증을 필요로 하고, 서비스 제공자(SP)는 메시지(1b)를 통해 사용자 인증에 대한 요구를 클라이언트로 전송한다. 클라이언트는 메시지(1c)를 통해 사용자 아이덴티티를 사용자 아이덴티티를 검증할 수 있는 서비스 제공자(SP)에게 제공한다. 클라이언트의 인증을 위한 아이덴티티 제공자(IdP1)가 서비스 제공자(SP)에게 알려져 있지 않다면, 클라이언트는 메시지(1c)를 통해 레퍼런스를 아이덴티티 제공자(IdP1)에게로 전송하며, 예컨대, Uniform Resource Identifier(URI)을 SP로 전송한다. 선택적으로, 아이덴티티 제공자(IdP1)로의 레퍼런스는 디폴트에 의해 클라이언트로부터 서비스 제공

자(SP)로 전송된다.

[0143] 서비스 제공자(SP)는, 메시지(2)를 통해 사용자 아이덴티티 및 서비스의 인증 보안 요구 사항을 지정하는 원하는 ASProf를 아이덴티티 제공자(IdP1)로 전송함으로써, 사용자의 인증을 요구한다. 통상적으로, 서비스 제공자(SP) 및 아이덴티티 제공자(IdP1)는, 이들이 교환하는 정보의 신뢰성, 무결성 및 인증성을 제공할 뿐만 아니라, 서비스 제공자(SP)와 아이덴티티 제공자(IdP1) 사이에 일방 또는 상호 인증을 제공하는 보안 세션(예컨대, TLS를 이용하여)을 설정한다. 제안된 보안 방법에 수반된 어떤 종류의 엔티티 간의 어떤 종류의 암호화를 필요로 하는 프로세스 및 메시지는 도 3에 도시되어 있지 않거나, 다음의 도면에도 도시되어 있지 않다.

[0144] 프로세스(3a)에서, 아이덴티티 제공자(IdP1)는, SP로부터 수신되는 ASProf에서 설명된 요구 사항을 충족할 수 있는 지의 여부를 검사한다. 이 요구 사항이 충족할 수 있다면, 프로세스(3a)에서, 아이덴티티 제공자(IdP1)는, 사용자 자격의 검증이 필요한 지 않은 지를 더 검사할 수 있다. 자격 검증이 필요하다면, 사용자 자격에 대한 요구(3b)는 클라이언트로 전송될 수 있고, 클라이언트는, 요구된 사용자 자격을 제공함으로써, 메시지(3c)를 통해 요구(3b)에 응답할 수 있다. 양방의 대역내 및 대역외 통신은 요구(3b) 및 대응하는 응답(3c)에 가능하다. 선택적 자격 검증 및 ASProf의 요구 사항의 검사에 대한 포지티브(positive) 결과에 따라, 아이덴티티 제공자(IdP1)는 메시지(3d)를 통해 사용자 인증의 어서션을 SP로 전송한다. 이 어서션에 따라, 서비스 제공자(SP)는 클라이언트로의 접근을 승인하여, 요구된 서비스 세션에 접근할 수 있다.

[0145] 사용자 자격의 검증의 일례로서, 사용자는 사용자명/패스워드 메카니즘을 이용하여 IdP를 통해 9 am에서 좋아하는 웹 포털에 인증을 받는다. 11 am에서, 사용자는 인터넷 서적 세일을 위한 서비스를 제공하는 서비스 제공자에 사용자의 프로파일을 접근하기를 원하고, 상기 서비스 제공자는 또한 동일한 IdP로부터 인증 어서션을 액셉트한다. 상기 서비스 제공자가 패스워드 엔트리가 1 시간 이상 경과하지 않은 ASProf에서 필요하다면, IdP는 사용자가 상기 서비스 제공자에 인증될 수 있기 전에 패스워드를 재입력하도록 사용자에게 요청할 필요가 있다. 한편, 상기 서비스 제공자가 24 시간까지 경과한 패스워드 엔트리를 액셉트한다면, 패스워드를 재입력할 필요가 없다.

[0146] 도 3 및 도 3의 설명에 의하면, 하나의 ASProf만이 서비스 제공자(SP)로부터 아이덴티티 제공자(IdP1)로 전송된다. 그러나, 제안된 방법은, 다수의 원하는 ASProfs가 서비스 제공자(SP)로부터 아이덴티티 제공자(IdP1)로 전송되는 경우에 쉽게 구성될 수 있다. 이 경우에, 서비스 제공자(SP)는 서비스 제공자(SP)가 클라이언트의 인증에 충분한 것으로 고려하는 ASProfs의 "소망의 리스트(wish list)"를 전송한다. 아이덴티티 제공자(IdP1)는 소망의 리스트를 검사한다. 소망의 리스트의 하나 이상의 ASProfs가 아이덴티티 제공자(IdP1)에 의해 지원되면, 예컨대, 어떤 자격 검증도 필요하지 않거나, 자격 검증이 소망의 리스트의 다른 지원된 ASProfs에 비해 덜 곤란한 경우에, 아이덴티티 제공자(IdP1)는 아이덴티티 제공자(IdP1)에 의해 최상으로 지원되는 ASProfs 중 하나를 선택할 수 있다.

[0147] 도 3과 관련하여 기술된 방법은, 아이덴티티 제공자(IdP1)와 SP 간의 직접 메시지 교환을 수반하는 "백 채널(back channel)" 메시지 흐름을 이용한다. 선택적으로, 이 방법은 "프론트 채널(front channel)" 통신을 이용하여 실시될 수 있다. 즉, 아이덴티티 제공자(IdP1)와 서비스 제공자(SP) 간의 어떠한 통신은 바람직하게는 적절한 보안 경계(precaution)를 이용하여 클라이언트에 의해 중계되어, 클라이언트가 전후로 전달되는 정보를 탬퍼(tamper)할 수 없다. 상이한 메시지에 대한 백 채널 및 프론트 채널의 조합도 가능하다.

[0148] 프론트 채널 통신에 대한 일례는 도 3에 대응하는 인증을 위해 도 4에 도시되어 있다. 프론트 채널 통신 시에, 원하는 ASProf 및 선택적으로 사용자 아이덴티티는 메시지(42a)를 통해 서비스 제공자(SP)로부터 클라이언트로 전송된다. 클라이언트는 메시지(42b)를 통해 원하는 ASProf 및 사용자 아이덴티티를 아이덴티티 제공자(IdP1)로 전송한다. 사용자 아이덴티티가 서비스 제공자(SP)에 의해 제공되지 않으면, 클라이언트는 사용자 아이덴티티를 획득하여, 메시지(42b)를 통해 아이덴티티 제공자(IdP1)로 전송한다. 도 3에서와 같이, 프로세스(3a)에서, 아이덴티티 제공자(IdP1)는 자격 검증이 필요할 경우에 수신된 ASProf를 검사할 수 있다. 그럴 경우, 아이덴티티 제공자(IdP1)는 메시지(3b, 3c)를 이용하여 사용자 자격을 검증할 수 있다. 도 3에서와 같이, 메시지(3b, 3c)는 선택적이고, 대역내 또는 대역외 통신이 이용될 수 있다. 아이덴티티 제공자(IdP1)에 의해 제공된 보안 어서션은 메시지(43d, 43e) 및 클라이언트를 통해 서비스 제공자(SP)로 전송된다. 이 경우에, 보안 어서션은 인증 토큰(token) 또는 티켓으로 고려될 수 있다.

[0149] 이동 클라이언트의 경우에, 백 채널 구현은 클라이언트의 무선 인터페이스를 통해 서비스 제공자(SP)와 아이덴티티 제공자(IdP1) 간의 통신을 회피하는 이점을 갖는다. 프론트 채널 통신의 경우, 여분 대역폭이 이용되고, 여분 대기 시간(latency)이 서비스 제공자(SP)와 아이덴티티 제공자(IdP1) 간에 정보를 전후로 전송하기 위해서

만 무선 인터페이스 상에 생성된다.

[0150] 프론트 채널 접근 방식은 인터넷과 같은 고정 네트워크에는 일반화되어 있고, 구현 노력을 줄이기 위해서는 백 채널 접근 방식에 비해 바람직할 수 있다. 또한, 이것은 세션 방향 변경(redirection)이 일어나는 이점을 가진다. 즉, 도 4의 1c에서의 서비스 제공자(SP)에 대한 요구는 메시지(42a)에서 서비스 제공자(SP)로부터의 응답에 의해 응답되며, 백 채널의 경우에는 아이덴티티 제공자(IdP1)로부터의 응답에 의해 응답되지 않는다. 이것은 인증에 필요한 전체 시간을 백 채널 통신의 경우보다 더 단축시킬 수 있다.

[0151] 예컨대, 프럭시(proxy) 서버를 이용하여, 하이브리드 구현은 또한 서비스 제공자(SP)와 아이덴티티 제공자(IdP1) 간의 통신을 위한 프론트 채널을 에뮬레이트(emulate)하면서, 클라이언트를 통한 트래픽을 회피하기 위해 가능할 수 있다. 그래서, 하이브리드 구현은 이동 클라이언트에 매우 유용할 수 있다.

[0152] 이 경우에, 도 3과 관련하여 기술된 바와 같이, 서비스 제공자(SP)로부터 아이덴티티 제공자(IdP1)로 전송된 원하는 하나 이상의 ASProfs를 지원할 수 없고, 아이덴티티 제공자(IdP1)는 원하는 하나 이상의 ASProfs에 대한 대안(counterproposal)을 서비스 제공자(SP)에게 제공할 수 있다. 도 5에 따르면, 서비스 제공자(SP)는 원하는 ASProf 및 사용자 아이덴티티를 포함하는 인증 요구를 메시지(2)를 통해 아이덴티티 제공자(IdP1)에게 전송한다. 아이덴티티 제공자(IdP1)는 수신된 원하는 ASProf를 검사하여, 원하는 ASProf가 지원되지 않음을 깨닫는다. 하나 이상의 선택적 ASProfs가 판단되어, 제안된 바와 같은 메시지(4)를 통해 선택적 ASProfs를 아이덴티티 제공자(IdP1)로부터 SP로 전송된다. 프로세스(5a)에서, 서비스 제공자(SP)는 하나 이상의 제안된 선택적 ASProfs 중 적어도 하나가 수락 가능한 지를 검사한다. 수신되는 제안된 선택적 ASProfs 중 어떤 것도 수락 가능하지 않을 경우, 서비스 제공자(SP)는 하나 이상의 다른 원하는 ASProfs를 아이덴티티 제공자(IdP1)에게로 전송할 수 있거나, 인증을 위해 다른 아이덴티티 제공자(IdP1)와 접촉할 수 있으며, 또는 인증을 종료할 수 있다. 하나 이상의 제안된 선택적 ASProfs 중 적어도 하나가 수락 가능할 경우, 서비스 제공자(SP)는 하나 이상의 제안된 선택적 ASProfs의 승인을 메시지(5b)를 통해 아이덴티티 제공자(IdP1)에게 전송한다. 다수의 제안된 선택적 ASProfs가 수락 가능할 경우, 서비스 제공자(SP)는, 선택된 ASProfs의 승인을 전송하기 전에 다수의 ASProfs 중 하나를 선택할 수 있다. 예컨대, 서비스 제공자(SP)는 수신된 하나 이상의 제안된 선택적 ASProfs를 검사할 수 있고, 제 1 ASProf가 수락할 수 있는 것으로 검색된 후에 검사를 종료한다. 이 ASProf는 서비스 제공자(SP)에 의해 승인되고, 이 ASProf의 승인의 지시는 아이덴티티 제공자(IdP1)에게 전송된다. 승인된 ASProf의 경우, 아이덴티티 제공자(IdP1)는, 도 3과 관련하여 기술된 바와 같이, 프로세스 및 메시지(3a-3d)에 의해 진행한다.

[0153] 도 3 내지 도 5와 관련하여 기술되는 바와 같이, 원하는 하나 이상의 ASProfs가 아이덴티티 제공자(IdP1)에게 전송된다는 점에서, 서비스 제공자(SP)는 아이덴티티 제공자(IdP1)에 의해 이용될 하나 이상의 ASProfs를 원한다. 그러나, 서비스 제공자(SP)는 반듯이 인증 요구 시에 하나 이상의 원하는 ASProfs를 아이덴티티 제공자(IdP1)에게 전송할 필요는 없다. 대신에, 서비스 제공자(SP)는 아이덴티티 제공자(IdP1)로부터 지원된 ASProfs의 리스트를 요구할 수 있다. 이것은 도 6에 도시되어 있다. 서비스 제공자(SP)는 메시지(62a)를 통해 사용자 아이덴티티를 아이덴티티 제공자(IdP1)에게 전송하여, 인증을 요구한다. 아이덴티티 제공자(IdP1)는 메시지(62b)를 통해 아이덴티티 제공자(IdP1)에 의해 지원된 ASProfs의 리스트에 응답한다. 이 리스트는 프로세스(62c)에서 서비스 제공자(SP)에 의해 검사되고, 이 리스트의 수락 가능한 ASProf는 선택된다. (지시에 대한 일례로서) 선택된 ASProf 또는 선택된 ASProf의 지시는 메시지(62d)를 통해 아이덴티티 제공자(IdP1)에게 전송된다. (지시에 대한 일례로서) 선택된 ASProf 또는 지시를 전송함으로써, 메시지(62a)를 통해 전송된 인증 요구와 선택된 ASProf를 상관시키기 위해 사용자 아이덴티티를 보강할 수 있다. 프로세스(63a)에서, 아이덴티티 제공자(IdP1)는, 자격 검증이 선택된 ASProf를에 필요하고, 도 3과 관련하여 기술된 바와 같이 3b-3d를 따른 프로세스 및 메시지에 의해 진행하는 지를 검사할 수 있다.

[0154] 보안 강도의 레벨을 노출시키는 관계를 가지거나 가지지 않고 개별 ASProfs를 전송함으로써, ASProfs의 전송이 달성될 수 있다. 개별 ASProfs 또는 ASProfs 및, ASProfs 간의 관계에 관한 정보가 전송될 수 있다. 예컨대, 도 1 및 도 2와 관련하여 기술된 바와 같은 그래프 주석에 대해, ASProfs와 같은 그래프의 부분 또는 전체 그래프 및 화살표는 전송될 수 있다. ASProfs의 전송자, 예컨대, 서비스 제공자(SP)는 ASProfs가 수신자, 예컨대, 아이덴티티 제공자(IdP1)에 의해 이용되기를 원하는 지를 지정할 수 있다. 특히, 수신자가 어떤 원하는 ASProfs를 지원하지 않는 경우, 수신자는 원하는 ASProfs에서 시작하는 그래프를 통해 내비게이트(navigate)하여, 그것이 ASProfs 간의 관계에 관한 정보가 수신자에서 이용 가능할 경우에 원하는 ASProf 보다 강하거나 동일한 것으로 인식되는 ASProf를 지원할 수 있는 지를 탐색할 수 있다. 수신자에게 알려진 그래프 또는 그래프의 부분을 통해 내비게이트할 시에, 수신자는 전송자가 원할 시에 ASProf의 강도에 대한 요구 사항을 충족하기 위해 동일하거나

보다 강한 적어도 하나의 ASProf를 선택할 수 있다.

[0155] 내비게이션에 대해 대응하는 일례는 도 7에 도시되어 있으며, 여기서, 서비스 제공자(SP)는 메시지(72)를 통해 ASProf 그래프의 일부 또는 전체, 원하는 ASProf에 대한 지시 및 사용자 아이덴티티를 인증을 위해 아이덴티티 제공자(IdP1)에게 전송한다. 그래프 전체를 전송하는 대신에, 서비스 제공자(SP)는 원하는 ASProf 보다 강하거나 동일한 ASProfs를 포함하는 그래프의 부분만을 전송하여, 송신 노력을 낮추거나, 이런 인증에 유용하지 않은 정보를 아이덴티티 제공자(IdP1)에게 제공하지 않을 수 있다. 프로세스(73a)에서, 아이덴티티 제공자(IdP1)는 원하는 ASProf가 지원되는 지를 검사한다. 지원되지 않으면, 프로세스(73a)에서, 아이덴티티 제공자(IdP1)는, (도 7에 도시된 바와 같이) 보다 강한 ASProf 또는 동일한 강도의 ASProf가 SP로부터 수신되는 바와 같은 그래프를 내비게이트함으로써 지원되는 지를 검사한다. 지원되지 않은 원하는 ASProf와 상이한 보다 강하거나 동일한 강도의 적어도 하나의 ASProf가 아이덴티티 제공자(IdP1)에 의해 지원되면, 프로세스(73a)에서, 아이덴티티 제공자(IdP1)는 사용자 자격의 검증을 위해 검사하여, 도 3과 관련하여 기술된 바와 같이 필요하다면 사용자로부터 사용자 자격을 요구할 수 있다(프로세스 및 메시지(3a-3c). 동일하거나 보다 강한 ASProf가 이용되고, 선택적으로 사용자 자격이 검증되면, 아이덴티티 제공자(IdP1)는, 메시지(73d)를 통해 이용되는 동일하거나 보다 강한 ASProf의 지시에 의해 바람직하게 보강된 사용자 인증의 어서션을 아이덴티티 제공자(IdP1)에게 전송한다. 클라이언트에 대한 서비스 접근을 승인하기 전에, 프로세스(73e)에서, 서비스 제공자(SP)는, 이용된 ASProf가 서비스 제공자(SP)에 수락할 수 있는 지를, 예컨대, 서비스 제공자(SP)의 인증 보안 요구 사항에 응하는 지를 검사할 수 있다.

[0156] 서비스 제공자(SP) 및 아이덴티티 제공자가, 적어도 어느 정도까지, ASProf를 다른 ASProf에 비해 보다 강하거나 동일하게 하는 어떤 유사한 아이디어(idea)를 공유할 경우, 즉, 이들이 인증 보안 강도에 대해 ASProf 간의 관계 및 ASProfs에 관한 정보를 공유할 경우, 상술한 바와 같은 그래프 또는 그래프의 부분의 송신은 메시지 라운드트립(roundtrip)의 수에 의해 제안된 방법을 보다 효율적이게 한다. 게다가, 그래프를 송신함으로써, 서비스 제공자(SP) 및 아이덴티티 제공자 간의 메시지 라운드트립의 수를 최소화하여, 인증 서비스를 보다 고속으로 행하면서, SP의 보안 선택 및 우선 순위가 확실히 관측한다.

[0157] 예컨대, 서비스 제공자(SP)가 128 비트의 키 길이를 요구하고, 아이덴티티 제공자가 64 비트 또는 256 비트 중 어느 하나만을 제공할 수 있다면, 서비스 제공자(SP) 및 아이덴티티 제공자는 서비스 제공자(SP)에 의해 128 비트 키 보다 더 강하도록 수락되는 의견(notion)을 공유한다. 이 의견이 공유되지 않으면, 서비스 제공자(SP) 및 아이덴티티 제공자가 사용될 ASProf에 일치할 수 있을 때까지 부가적인 메시지가 교환될 필요가 있다. 256 비트 키가 128 비트 키 보다 더 강한 관계의 지식없이, 아이덴티티 제공자는 예컨대 어떤 지시를 128 비트 키가 지원되지 않는 서비스 제공자(SP)에게 전송한다. 이 경우에, 서비스 제공자(SP)는 지원되는 256 비트의 선택적 ASProf에 응답할 수 있다.

[0158] 어떤 ASProf가 다른 ASProf 보다 강하거나 동일한 지의 여부의 공유된 의견은 암시적이거나 명백할 수 있다. 암시적 협정(agreement)의 일례는, 256 비트가 일반적으로 128 비트 보다 더 강한 것으로 이해됨을 의미하는 128 비트 대 256 비트 경우이다. 서비스 제공자(SP)가 128 비트를 요구하였을 시에 서비스 제공자(SP)가 256 비트를 수락할 수 있다면, 128 비트를 제공할 수 없는 아이덴티티 제공자는 대신에 256 비트를 사용하고, 이 사실을 ASProf의 서비스 제공자(SP)에게 전달한다. 그러나, 서비스 제공자(SP)는 아이덴티티 제공자와 상이한 ASProf의 강도의 설정을 이용한다면, 아이덴티티 제공자의 잘못된 가정(assumption)에 의해, 부가적인 재절충(renegotiation) 및 부가적인 메시지 또는 인증의 종료가 이루어진다. 서비스 제공자(SP)와 아이덴티티 제공자 간의 명백한 공유 의견이 암시적 공유 의견에 비해 바람직할 수 있는 일례가 도 2에서 제공되며, 여기서, 서비스 제공자(SP)는 비단조를 설정하고, 일반적으로 수치적 속성과 파악된 인증 보안 강도 간의 관계에 일치하지 않는다.

[0159] 도 8은 서비스 제공자(SP)가 메시지(2)를 인증 요구를 전송하는 인증서를 도시한 것으로, 이 인증 요구는 원하는 ASProf 및 사용자 아이덴티티를 포함하지만, SP의 그래프에 관한 다른 정보를 전송하지 않는다. 아이덴티티 제공자(IdP1)는 원하는 ASProf를 지원하지 않고, 아이덴티티 제공자(IdP1)는 프로세스(83a)에 도시된 바와 같이 선택적 ASProf를 선택한다. 아이덴티티 제공자는 자격 검증이 프로세스(83a)에서 필요한 지를 검사한다. 도 3과 관련하여 제공된 설명에 따라 메시지(3b 및 3c)를 이용하여 사용자 자격을 선택적으로 검증한 후에, 사용자 인증 및 사용된 선택적 ASProf의 지시의 어서션은 메시지(83d)를 통해 SP로 전송된다. 프로세스(83e)에서, 서비스 제공자(SP)는, 선택적 ASProf가 수락 가능한 지의 여부를 검사한다. ASProf가 수락 가능하면, 서비스 세션은 시작할 수 있다. 선택적 ASProf를 선택하는 경우, ASProf는, 예컨대, 자신의 그래프를 이용하거나 명백한 의견을 추정함으로써, 자신의 의견을 이용할 수 있다. 그러나, 서비스 제공자(SP)가 선택적 ASProf를 수락할 수 없음을

발견함을 회피하기 위해, 아이덴티티 제공자(IdP1)는 바람직하게는 서비스 제공자(SP)와 아이덴티티 제공자(IdP1) 사이에서 공유되는 의견을 이용한다. 서비스 제공자(SP)에 따른 순서를 반영하는 그래프는, 서비스 제공자(SP)를 아이덴티티 제공자(IdP1)에 의해 제공된 인증 서비스에 등록할 시에 제공될 수 있다. 그러나, 원하는 ASProf 및 사용자 아이덴티티와 상이한 어떤 정보도 아이덴티티 제공자(IdP1)에서 이용할 수 없는 특별 시나리오의 경우, 아이덴티티 제공자(IdP1)는 바람직하게는 자신의 의견, 예컨대, 자신의 그래프를 이용할 수 있거나, 아이덴티티 제공자로부터, 예컨대, 그래프 형태로 하나 이상의 지원된 ASProfs를 요구할 수 있다.

[0160] ASProfs를 관계와 관련시킴으로써, ASProfs의 그룹이 작성될 수 있다. 예컨대, 다수의 ASProfs는, 상기 다수의 ASProfs의 각 쌍을 = 관계로 관계시켜, 예컨대, ASProfs으로 도 2에 나타낸 바와 같이 동일한 인증 보안 강도의 ASProfs의 그룹을 형성하며, 3-6 및 11-20 문자가 동일한 인증 보안 강도의 그룹을 형성함으로써 관계될 수 있다. 서비스 제공자는 아이덴티티 제공자에 지시하여, 사용자의 인증을 위한 어떤 그룹에 속하는 어떠한 ASProfs를 이 그룹에 속하는 ASProfs 중 하나를 선택함으로써 이용하여, 선택된 ASProf의 지시를 사용자의 인증을 위한 아이덴티티 제공자에게 전송할 수 있다. 아이덴티티 제공자가, 예컨대, 그룹의 특징에 관한 정보, 즉, ASProfs 및 이들의 관계가 서비스 제공자(SP)에 의해 IdP에 제공되거나 그 역으로 제공된다는 사실로 인해, 지시된 그룹을 알고 있다면, 아이덴티티 제공자는 지시에 기초한 그룹으로부터 인증을 위한 하나의 ASProf를 선택할 수 있다. 서비스 제공자 및 아이덴티티 제공자가 그룹의 동일한 의견을 공유할 경우에 그룹 식별자는 그룹을 아이덴티티 제공자에 지시하기 위해 이용될 수 있다. 개별 그룹은 계층적으로 순위가 정해질 수 있다. 예컨대, 제 1 수의 ASProfs를 포함하는 제 1 그룹은 ASProfs의 제 2 그룹에 관계될 수 있고, 아이덴티티 제공자는 인증을 위한 한 그룹에서 다른 그룹까지 내비게이트할 수 있다. 인증을 실행함에 따른 ASProf가 서비스 제공자의 인증 보안 요구 사항에 일치하는 지를 검사하기 위해, 상기 인증 보안 프로파일이 관계되는 그룹의 지시는 충분할 수 있다. 그룹 형성은, 비교 가능한 자격 타입 또는 비교 가능한 작성 또는 타당성 주기와 같은 비교 가능한 특징을 가진 인증 보안 프로파일의 양호한 범위성(scalability) 및 관리성(manageability)의 이점을 가질 수 있다.

[0161] 선택적 인증 방법으로서, 서비스 제공자(SP)는 어떤 ASProf를 지정하지 않고 인증을 요청할 수 있다. 대응하는 시나리오는 도 9에 도시되어 있다. 서비스 제공자(SP)는 메시지(62a)를 통해 사용자 아이덴티티를 포함하는 인증 요구를 아이덴티티 제공자(IdP1)에게 전송한다. 프로세스(93a)에서 나타낸 바와 같이, 아이덴티티 제공자(IdP1)는 자신의 선택의 ASProf를 이용하여, 도 3과 관련하여 설명된 바와 같이, 예컨대, 메시지(3b, 3c)를 이용함으로써 선택된 ASProf에 따라 자격 검증을 선택적으로 실행한다. 그 후, 아이덴티티 제공자(IdP1)는, 메시지(93d)를 통해, 이용된 ASProf의 지시, 또는 선택적인 지시 형태로서 이용된 ASProf 자체를 인증 어서션과 함께 서비스 제공자(SP)에게 전송한다. 그 후, 서비스 제공자(SP)는 인증을 수락할 것인 지의 여부를 판단한다. 즉, 프로세스(93e)에서, 이용된 ASProf가 수락 가능한 지의 여부가 검사된다.

[0162] 서비스 세션 동안에 아이덴티티 제공자에 의해 서비스 제공자(SP)에 대한 사용자 인증을 업그레이드하는 방법은 다음의 2개의 도 10 및 도 11에서 기술된다. 도 10에 따르면, 클라이언트는 서비스 세션에 참여한다. 서비스 제공자의 서비스에 대한 사용자의 제 1 인증에 의한 서비스 세션의 확립은 도 3 내지 도 9의 설명에 따라 달성될 수 있다. 서비스 세션 동안, 클라이언트는 확립된 세션 보다 고 보안 레벨을 필요로 하는 서비스에 접근한다. 고 보안 레벨에 대한 일례로서, 사용자는 5 디지트 PIN 코드에 의해 온라인 은행 구좌에 접근할 수 있다는 것이다. 그러나, 부가적으로 사용자가 자신의 은행 구좌에서 금전 거래를 허가하기를 원하면, 부가적인 1회성 패스워드 또는 TIN이 필요하다. 다른 예로서, 사용자는 패스워드에 의해 자신의 개인용 웹 포털에 접근할 수 있다. 이 포털 상의 어떤 서비스는 요금을 지불할 수 있다. 사용자가 이와 같은 서비스에 클릭하면, 사용자의 PC에 부착된 스마트 카드 판독기를 이용한 인증이 필요할 수 있다.

[0163] 서비스 제공자(SP)는, 메시지(102a)를 통해 클라이언트에서 서비스 제공자(SP)로 전송된 서비스 요구를 검출하여, 다음의 수정된 ASProf을 요구하고, 보다 엄격한 요구 사항을 충족하는 ASProf를 선택한다. 즉, 수정된 ASProf는 제 1 인증에 이용된 ASProf 보다 더 강하다. 서비스 제공자(SP)는, 메시지(102b)를 통해, 수정된 ASProf 및 사용자 아이덴티티를 포함하는 인증 요구를 제 1 인증에 이용된 아이덴티티 제공자와 반듯이 동일하지 않은 아이덴티티 제공자에게 전송한다. 프로세스(103a)에서, 아이덴티티 제공자(IdP1)는 보다 강렬한 요구 사항의 ASProf를 충족할 수 있는 지를 검사한다. 충족한다면, 프로세스(103a)에서, 아이덴티티 제공자(IdP1)는 이런 보다 강한 ASProf가 사용자 자격의 새로운 검증을 필요로 하는 지를 검사하여, 메시지(103b, 103c)를 통해, 필요하다면 이런 검증을 실행한다. 도 3에서와 같이, 선택적 메시지(103b, 103c)는 대역내 또는 대역외 통신을 통해 교환될 수 있다. 그 후, 이것은, 메시지(103d)를 통해 아이덴티티 제공자(IdP1)로부터 서비스 제공자(SP)로 전송된 사용자 인증의 어서션에 대해 도 3과 관련하여 기술된 바와 같이 진행된다. 이 어서션에 기초하여, 서비스 제공자(SP)는 업그레이드된 ASProf를 필요로 하는 서비스로의 접근을 승인할 수 있고, 서비스 세

션은 계속될 수 있다. (지시의 한 형태로서) 선택된 ASProf를 전송하는 대신에, 선택된 ASProf에 대한 URI와 같은 지시는, 예컨대, 선택된 ASProf가 아이덴티티 제공자(IdP1)에 알려지거나 접근 가능할 시에 전송될 수 있다. 제 1 인증에 이용된 ASProf가 아이덴티티 제공자(IdP1)에게 알려진다면, 서비스 제공자(SP)는 대신에 어떤 지시를 전송하여, 제 1 인증에 이용된 ASProf 보다 더 강한 ASProf를 이용할 수 있다. 이 경우에, 아이덴티티 제공자(IdP1)는, 예컨대, 그래프를 내비게이트함으로써, 수정된 ASProf의 선택을 실행할 수 있다. 바람직하게는, 업그레이드 인증에 이용되는 이런 수정된 ASProf는 업그레이드 인증을 위해 서비스 제공자(SP)에게 지시되고, 서비스 제공자(SP)의 의해 승인된다.

[0164] 도 11은 인증 및 서비스 세션이 제 1 아이덴티티 제공자(IdP1)에 의해 확립되고, 클라이언트가 확립된 세션 보다 고 보안 레벨을 필요로 하는 서비스로의 서비스 접근을 요구하는 경우를 도시한 것이다. 따라서, 서비스 제공자(SP)는, 보다 고 보안 레벨을 필요로 하는 메시지(102a)를 통해 전송된 서비스 요구를 검출하여, 메시지(102b)를 통해, 수정된 ASProf 및 사용자 아이덴티티를 포함하는 인증 요구를 제 1 IdP로 전송한다. 프로세스(113a1)에서, 제 1 아이덴티티 제공자(IdP1)는 수신되는 수정된 ASProf를 검사하여, 수정된 ASProf가 지원되지 않는 지를 검출한다. 따라서, 제 1 아이덴티티 제공자(IdP1)는 수정된 ASProf 및, 제 1 아이덴티티 제공자(IdP1)에 의해 지원되는 선택적 ASProfs의 메시지(113b)를 통해 거절(refusal)을 전송한다. 프로세스(113c)에서, 서비스 제공자(SP)는 선택적 ASProfs를 검사하여, 이들을 수락할 수 없음을 검색할 수 있다. 이 거절에 대한 응답은 제 1 아이덴티티 제공자(IdP1)에 대해 인증을 종료함을 지시하기 위해 제 1 아이덴티티 제공자(IdP1)에게 전송될 수 있다. 이 점에서, 서비스 제공자(SP)는 인증 업그레이드를 종료하거나, 인증 업그레이드를 위해 제 2 아이덴티티 제공자(IdP2)를 선택할 수 있다. 제 2 아이덴티티 제공자(IdP2)가 이용 가능하다면, 다른 인증 요구는 메시지(112b)를 제 2 아이덴티티 제공자(IdP2)로 전송된다. 다른 요구는 수정된 ASProf 및, 제 1 아이덴티티 제공자(IdP1)에서의 제 1 인증을 위해 이용된 사용자 아이덴티티와 동일하거나 동일하지 않은 사용자 아이덴티티를 포함한다. 프로세스(113a2)에서, 제 2 아이덴티티 제공자(IdP2)는 수정된 ASProf가 지원되는 지를 검사한다. 수정된 ASProf가 지원되면, 사용자 자격의 검증은, 필요하다면, 대역내 또는 대역외 통신을 통해 메시지(113b, 113c)를 이용함으로써 실행될 수 있다. 사용자 인증의 어서션은 메시지(113d)를 통해 SP로 전송된다. 이 어서션에 따라, 서비스 제공자(SP)는 보다 엄격한 보안을 필요로 하는 서비스로의 접근을 승인할 수 있고, 서비스 세션은 계속될 수 있다.

[0165] 다른 예시적인 업그레이드 시나리오는 다음과 같다: 사용자는 패스워드를 통해 때때로 또한 인터넷으로 명명하는 자신의 인터넷 서비스 제공자(ISP)에 의해 인증된다. 어떤 시간에, 사용자는 영상 스트리밍(video streaming) 서비스에 접근하기를 원하며, 이 서비스는 요금을 지불하고, 예컨대, 인증 토큰으로서 이동 전화(가입자 아이덴티티 모듈/무선 식별 모듈, SIM/WIM)를 통해 보다 확실한 인증을 필요로 한다. 서비스 제공자, 즉, 비디오 서비스 스트리밍 서비스의 제공자는 먼저 인증 업그레이드를 위해 ISP에 접촉한다. ISP는 통상적으로 SIM 및 이동 전화를 관리하지 않지만, 아마 간단한 패스워드 리스트만은 엄격한 ASProf를 충족시킬 수 없다. 그것은 서비스 제공자에 대한 보다 약한 ASProf를 제안할 수 있지만, 서비스 제공자는 거절한다. 그 후, 서비스 제공자는 초기 서비스 요구 시에 잠재적 아이덴티티 제공자로서 클라이언트에 의해 지정될 수 있는 사용자의 이동 조작원에 접촉한다. 아이덴티티 제공자로서의 이동 조작원은 지정된 ASProf를 충족할 수 있다. 즉, 특정 SIM/WIM의 소유 뿐만 아니라 PIN 코드의 지식을 필요로 할 수 있다. 이것은 보다 확실한 인증의 어서션을 서비스 제공자에게 전송함으로써, 사용자는 스트리밍 서비스를 이용하여 진행할 수 있다.

[0166] ASProf가 아이덴티티 제공자로부터 서비스 제공자로, 또는 그 역으로 전송될 때마다 ASProf의 속성의 완전한 세트를 모두 다 나타낼 필요는 없다. 이에 대응하여, ASProfs 간의 관계 또는 전체 그래프는 모두 다 전송될 필요가 없다. 대신에, 레퍼런스(URI's) 뿐만 아니라 갱신도 아래에 설명되는 바와 같이 교환되는 데이터량을 줄이기 위해 사용될 수 있다.

[0167] ASProf는 각각 하나 이상의 속성을 지정하는 단편(fragments)의 시퀀스로 이루어지며, 예컨대, 테이블 A에 따른 XML 설명과, <user_credentials>, <transport_layer_security>, <security_policies> 및 <user_registration>에 관계한 단편을 비교할 수 있다. 개별 단편으로부터의 속성은 서로 보완적이며, 즉, 이들 속성이 하나의 단편에만 제공되거나 서로 오버라이드(override)될 경우, 즉, 이들 속성이 양방의 단편에 제공될 경우에 보완적이다. 오버라이드의 경우, 단편의 순서에 기초한 우선 순위 규칙이 지정될 필요가 있다. 즉, 후속 단편은 이전의 단편에 오버라이드하거나, 그 역으로 오버라이드한다.

[0168] 레퍼런스, 예컨대, 바람직하게는 URI는 ASProf 또는 단편을 참조하는데 이용될 수 있으며, 이 단편은 바람직하게는 ASProf 또는 단편의 모든 속성을 모두 다 나타내는 대신에 전체 ASProf의 의미 부분 집합(semantic

subset)을 나타낸다. 레퍼런스의 이용에 의해 페칭(fetching) 및 캐싱(caching)이 가능하고, 전후로 전송되는 데이터량이 실질적으로 감소될 수 있다. 예컨대, 서비스 제공자가 어떤 시간 주기 동안에 동일한 ASProf를 이용하는 어떤 아이덴티티 제공자를 자주 이용하면, 새로운 사용자가 상기 어떤 시간 주기 내에서 인증될 때마다 ASProf가 서비스 제공자와 아이덴티티 제공자 사이에서 명백히 교환될 필요가 없다.

[0169] 기존 ASProfs와 새로운 ASProfs 간의 차에 관한 델타 갱신한다는 점에서 ASProfs의 갱신을 이용함으로써, 교환되는 데이터량이 감소될 수 있다. 갱신 ASProf는 새로운 ASProf이며, 이는 기존 ASProf에 보완적이거나 그의 어떤 속성을 오버라이드한다. 또한, 갱신 단편 또는 갱신 속성이 가능하다. 예컨대, 사용자는 패스워드 검증을 이용하여 아이덴티티 제공자에 의해 서비스 제공자에게 인증된다. 어떤 사용자의 상호 작용의 경우, 이전에 이용된 ASProf와의 유일한 차는 패스워드 검증에 대해 보다 짧은 활동 시간(time-to-live)이 지정된다는 것일 경우에는 인증 업그레이드가 요구된다. 이 경우에, 수신 파티(party)가 완전히 페치 및 캐시해야 하는 새로운 ASProf로 레퍼런스를 전송하는 것과는 반대로, 레퍼런스를 이전에 이용된 ASProf, 플러스 벗어난(deviating) 활동 시간 속성을 나타내는 단일 속성으로 전송하는 것이 보다 효율적이다.

[0170] 제안된 방법은 또한 서비스 제공자, 아이덴티티 제공자, 또는 프럭시(proxy), 또는 클라이언트 장치와 관련된 서버와 같은 장치 내에서 실시된다. 이와 같은 장치는, 적어도, 메시지(M2)를 수신하는 수신 유닛(R), 메시지(M1)를 전송하는 송신 유닛(T) 및, 메시지 및 정보를 처리하는 처리 유닛(P) 및, 바람직하게는 정보를 저장하는 데이터베이스(D)를 포함한다. 이와 같은 장치에 대한 일례가 도 12에 도시되어 있으며, 도 12는 유닛(R, T, P, D) 및 메시지(M1, M2) 및, 개별 유닛(R, T, P, D) 간에 정보 및 메시지를 교환하는 상호 접속부(PR, PT, PD)를 도시한다. 장치(DEV)는, 서비스 제공자, 아이덴티티 제공자, 또는 방법을 구현하는 클라이언트 장치로서의 사용자에 의해 사용될 수 있는 장치의 일례이다.

[0171] 인증 방법을 실행하는 장치 간에 메시지 및 정보를 교환하는 장치 및 링크의 예들은, 제각기 백 채널, 프론트 채널 및 하이브리드 백/프론트 채널 통신을 위한 도 13, 도 14 및 도 15에 제공된다. 이들 장치는 도 12와 관련하여 도시되고 기술된 바와 같이 구성될 수 있다.

[0172] 도 13은 클라이언트(D12), 서비스 제공자(D10), 아이덴티티 제공자(D11) 및, 프론트 채널 통신을 통해 서비스 제공자(D10)에 대한 클라이언트(D12)의 인증을 위한 3 파티 간의 링크(CON10, CON11, CON12)를 도시한 것이다. 클라이언트(D12)와 서비스 제공자(D10) 간의 통신은 링크(CON10)를 통해 수행되고, 서비스 제공자(D10)와 아이덴티티 제공자(D11) 간의 통신은 링크(CON11)를 통해 수행되며, 아이덴티티 제공자(D11)와 클라이언트(D12) 간의 통신은 링크(CON12)를 통해 수행된다. 링크(CON10, CON11, CON12)를 통해 3 파티 간에 교환되는 정보 및 메시지에 대한 예들은, 즉, 링크(CON10)를 통하는, 서비스 요구 (메시지(1a)), 인증 요구 (메시지(1b)), 아이덴티티 제공자에 대한 사용자 아이덴티티 및 레퍼런스 (메시지(1c)) 및 서비스 세션, 링크(CON11)를 통하는, 원하는 ASProf 및 사용자 아이덴티티 (메시지(2)) 및 사용자 인증의 어서션 (메시지(3d)) 및, 링크(CON12)를 통하는, 사용자 자격 요구 (메시지(3b)) 및 사용자 자격의 전송 (메시지(3c))은, 예컨대, 도 3에서 발견될 수 있다. 링크(CON10, CON11, CON12)는 고정 접속부일 수 있지만, 고정 접속부일 필요는 없다. 예컨대, 링크(CON12)는 클라이언트(D12)가 이동 전화일 경우에 짧은 메시지 서비스(SMS)를 통해 달성될 수 있다.

[0173] 도 14는 클라이언트(D22), 서비스 제공자(D20), 아이덴티티 제공자(D21) 및, 프론트 채널 통신을 통하는 서비스 제공자(D20)에 대한 클라이언트(D22)의 인증을 위한 3 파티 간의 링크(CON20, CON21)를 도시한 것이다. 도 11과는 대조적으로, 서비스 제공자(D20)와 아이덴티티 제공자(D21) 사이에는 어떤 직접 링크도 존재하지 않는다. 대신에, 서비스 제공자(D20)와 아이덴티티 제공자(D21) 간의 통신은, 서비스 제공자(D20)와 아이덴티티 제공자(D21) 간에 교환되는 정보가 클라이언트(D22)에 의해 중계된다는 점에서 클라이언트(D22)를 통해 달성된다. 링크(CON20 및 CON21)를 통해 3 파티 간에 교환되는 정보 및 메시지에 대한 예들은 도 4에서 발견될 수 있다. 즉, 서비스 요구 (메시지(1a)), 인증 요구 (메시지(1b)), 아이덴티티 제공자에 대한 사용자 아이덴티티 및 레퍼런스 (메시지(1c)) 및 서비스 세션은 링크(CON20)를 통해 전송된다. 이에 대응하여, 사용자 자격 요구(3b) 및 사용자 자격은 링크(CON21)를 통해 전송된다. 그러나, 인증 요구(메시지(42a, 42b)) 시에 구성되는 원하는 ASProf 및 사용자 아이덴티티는 클라이언트(D22)를 통하는 서비스 제공자(D20)로부터 링크(CON20 및 CON21)를 통하는 아이덴티티 제공자(D21)로 전송된다. 이에 대응하는 중계는 클라이언트(D22) 및 링크(CON21 및 CON20)를 통해 아이덴티티 제공자(D21)로부터 서비스 제공자(D20)로 전송되는 사용자 인증(메시지(42d, 42e))의 어서션을 위해 달성된다.

[0174] 도 15는 프론트 채널 구현을 에뮬레이트하기 위해 프럭시(D31)를 이용한 하이브리드 구성을 도시한 것이다. 서비스 제공자(D30)의 서비스에 대한 클라이언트(D33)의 사용자의 인증을 위해, 클라이언트(D33)는 서비스 요구를

링크(CON30)를 통해 서비스 제공자(D30)로 전송한다. 서비스 제공자(D30)는 링크(C30)를 통해 클라이언트에 대한 사용자 인증 요구에 응답하고, 클라이언트(D33)는 링크(CON30)를 통해 사용자 아이덴티티 및 선택적으로는 아이덴티티 제공자(D32)에 대한 레퍼런스를 서비스 제공자(D30)에게 제공한다. 서비스 제공자(D30)와 아이덴티티 제공자(D32) 간의 통신을 위해, 예컨대, 사용자 아이덴티티 및 원하는 ASProf를 전송하거나, 사용자 인증의 어서션을 위해, 프럭시(D31)는 서비스 제공자(D30)와 아이덴티티 제공자(D32) 사이에 개입된다. 서비스 제공자(D30)에서 아이덴티티 제공자(D32)로의 정보 및 그 역으로의 정보는 접속부(CON31 및 CON32)를 이용하여 프럭시(D31)를 통해 전송될 수 있다. 사용자 자격의 요구 및 사용자 자격의 전송을 위해, 링크(CON35)가 이용될 수 있다. 선택적으로, 링크(CON32 및 CON34)는 사용자 자격의 요구 및 전송에 이용될 수 있다. 다른 정보는 링크(C34)를 통해 프럭시(D31)와 클라이언트(D33) 간에 교환될 수 있다.

산업상 이용 가능성

[0175] 본 발명에 따른 방법은, 서비스 제공자, 아이덴티티 제공자, 프럭시 또는 클라이언트에 관련된 장치에 적재 가능한 하나 이상의 컴퓨터 프로그램에서도 실시된다. 하나 이상의 컴퓨터 프로그램은 상술한 바와 같은 방법을 실시하기 위해 소프트웨어 코드부를 포함한다. 하나 이상의 컴퓨터 프로그램은 컴퓨터 판독 가능 매체 상에 저장될 수 있다. 컴퓨터 판독 가능 매체는 서버내나 외부에 배치된 영구 또는 재기록 가능한 메모리일 수 있다. 컴퓨터 프로그램은 또한 신호의 시퀀스로서, 예컨대, 케이블 또는 무선 링크를 통해 서버로 전송될 수 있다.

[0176] 제안된 방법은 제각기 GPRS 및 UMTS와 같은 2G 및 3G 이동 통신 시스템에 이용되도록 구성될 수 있다. 또한, 그것은, 인터넷과 같은 고정망 및, 무선 근거리 통신망(WLAN)을 포함하는 무선망 및 고정망의 조합에서의 서비스에 대한 인증에 사용될 수도 있다. 이동 및 고정 클라이언트 단말기는 사용자에 의해 사용될 수 있다. 서비스 제공자, 아이덴티티 제공자 또는 프럭시에 관련된 서비스는 통상적으로 네트워크에 고정된다. 그러나, 제안된 방법은 비고정 서버를 이동하는데 사용될 수 있다. 이들 서버에 대한 예들은 개인용 컴퓨터(PC) 또는 랩탑 컴퓨터이다.

[0177] 다음에는, 본 발명의 어떤 이점이 요약되어 있다:

[0178] 정적 인증 보안 수단을 가지는 서비스 제공자와 아이덴티티 제공자 간의 고정 관계를 가지기 보다는, 본 발명은 인증 보안 프로파일의 특별 절충 및 업그레이드를 제공할 수 있다. 특별 절충을 위해, 이전에는 ASProf에 관해 서비스 제공자와 아이덴티티 제공자 간의 어떤 일치도 요구되지 않는다.

[0179] 더욱이, 상이한 타입의 서비스 및 거래는 어떤 사용자가 청구하는 사람인 지를 아는 확실성에 관해 매우 상이한 요구 사항을 가질 수 있다. 또한, 상이한 인증 메카니즘 및 보안 기반 구조는 상이한 레벨의 확실성을 제공한다. 제안된 방법은 이들 상이한 레벨의 확실성을 지원하여, 이진 인증 개념과 공통의 제한을 극복하는 것이다.

[0180] 다른 이점은, 본 발명이 서비스 제공자측 및 아이덴티티 제공자측 쌍방에 관한 수단을 연속적으로 변경하는 유연한 모델을 제공한다는 것이다. 수단 및 보안 특성이 변할 경우, 서비스 제공자와 아이덴티티 제공자 간의 대역외 통신은 최소화될 수 있다.

[0181] 더욱이, 인증 방법은 ASProf의 복잡한 명세를 처리하도록 한다. 즉, 지문 인식 및 패스워드와 같은 상이한 타입의 속성은 인증 보안 강도에 관해 비교될 수 있다. 더욱이, 또한, 상이한 속성의 조합은 절충되어 제안된 방법을 매우 범용적이게 할 수 있다.

[0182] 또한, 인증 방법은 제각기 서비스 제공자에게 서비스를 허용하여, 궁극적으로 인증에 관해 결정하는 수단 결정 및 수단 집행 포인트 역할을 한다. 이런 서비스 제공자의 경우, 제안된 방법은, 아이덴티티 제공자가 사용자 자격을 확인하는 서비스를 제공하고, 바람직하게는 세션 확립 시나 인증 갱신을 위해서만 수반되도록 구현될 수 있다. 세션 동안에 어떤 추가적으로 아이덴티티 제공자를 필요로 하지 않아, 결과적으로 아이덴티티 제공자의 부하 및, 세션 관리의 복잡성이 감소되며, 중간 아이덴티티 제공자를 가지는 종래 기술의 인증 방법에 비해 범위성이 개선된다.

도면의 간단한 설명

[0064] 도 1a는 속성을 가진 인증 보안 프로파일의 일례를 도시한 것이다.

[0065] 도 1b는 인증 보안 프로파일 및 인증 보안 강도에 관한 순서의 일례를 도시한 것이다.

[0066] 도 2는 수치적 속성값과 인증 보안 강도 간의 맵핑의 예를 도시한 것이다.

[0067] 도 3은 인증을 위한 제 1 예시적인 메시지 흐름을 도시한 것이다.

[0068] 도 4는은 인증을 위한 제 2 예시적인 메시지 흐름을 도시한 것이다.

[0069] 도 5는은 인증을 위한 제 3 예시적인 메시지 흐름을 도시한 것이다.

[0070] 도 6은 인증을 위한 제 4 예시적인 메시지 흐름을 도시한 것이다.

[0071] 도 7은 인증을 위한 제 5 예시적인 메시지를 도시한 것이다.

[0072] 도 8은 인증을 위한 제 6 예시적인 메시지 흐름을 도시한 것이다.

[0073] 도 9는 인증을 위한 제 7 예시적인 메시지 흐름을 도시한 것이다.

[0074] 도 10은 인증 업그레이드를 위한 제 1 예시적인 메시지 흐름을 도시한 것이다.

[0075] 도 11은 인증 업그레이드를 위한 제 2 예시적인 메시지 흐름을 도시한 것이다.

[0076] 도 12는 본 방법을 실시하기 위한 장치의 일례를 도시한 것이다.

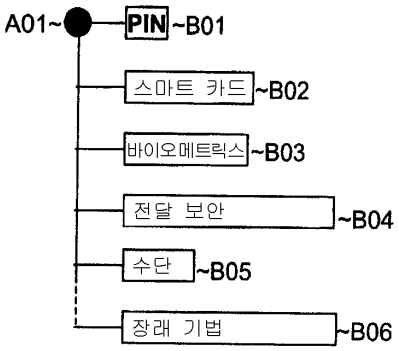
[0077] 도 13은 본 방법을 실행하기 위한 장치 간의 링크 및 장치의 제 1 예를 도시한 것이다.

[0078] 도 14는 본 방법을 실행하기 위한 장치 간의 링크 및 장치의 제 2 예를 도시한 것이다.

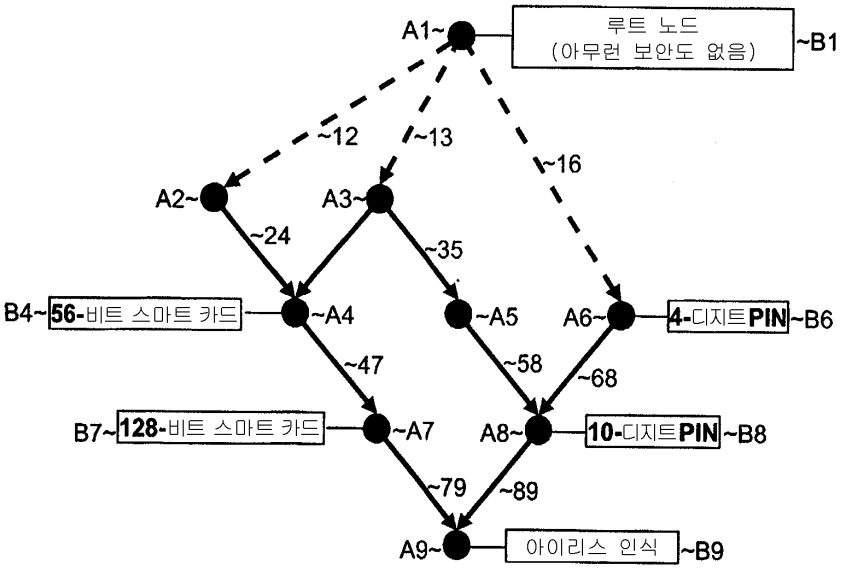
[0079] 도 15는 본 방법을 실행하기 위한 장치 간의 링크 및 장치의 제 3 예를 도시한 것이다.

도면

도면1

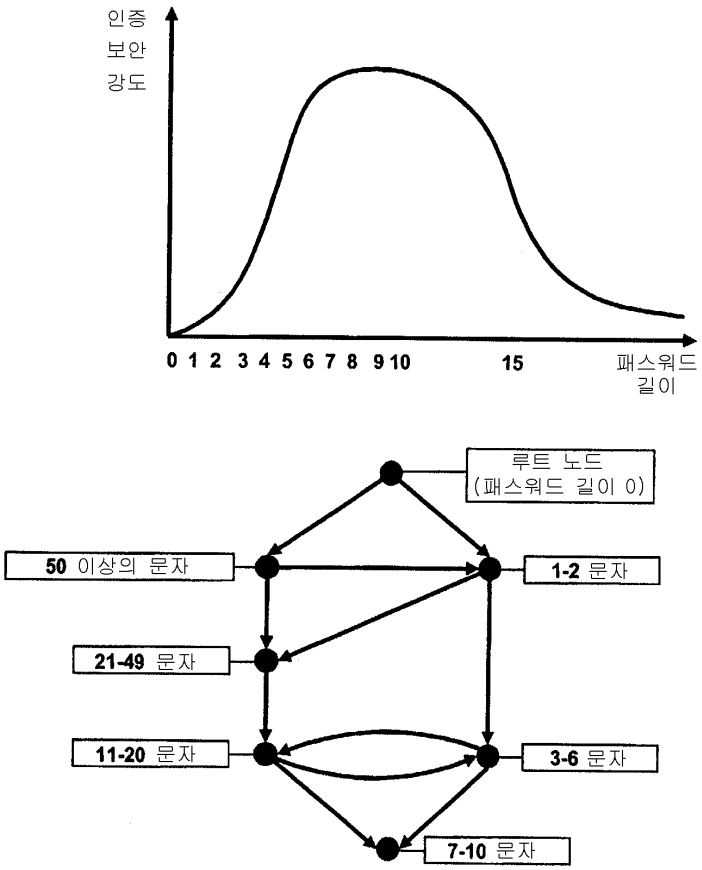

A01~
PIN ~B01
스마트 카드 ~B02
바이오메트릭스 ~B03
전달 보안 ~B04
수단 ~B05
장래 기법 ~B06

a

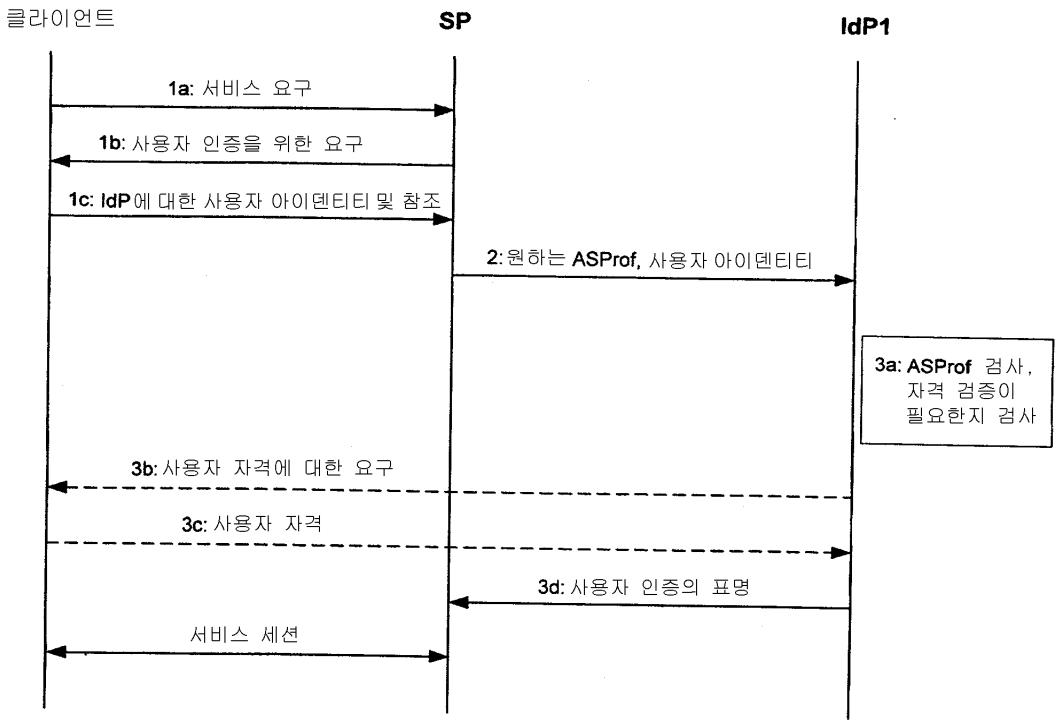

A1~
루트 노드
(아무런 보안도 없음)
~B1
~12
~13
~16
A2~
A3~
~24
~35
B4~ 56-비트 스마트 카드
~A4
~A5
A6~
4-디지트 PIN ~B6
~47
~58
~68
B7~ 128-비트 스마트 카드
~A7
A8~
10-디지트 PIN ~B8
~79
~89
A9~
아이리스 인식 ~B9

b

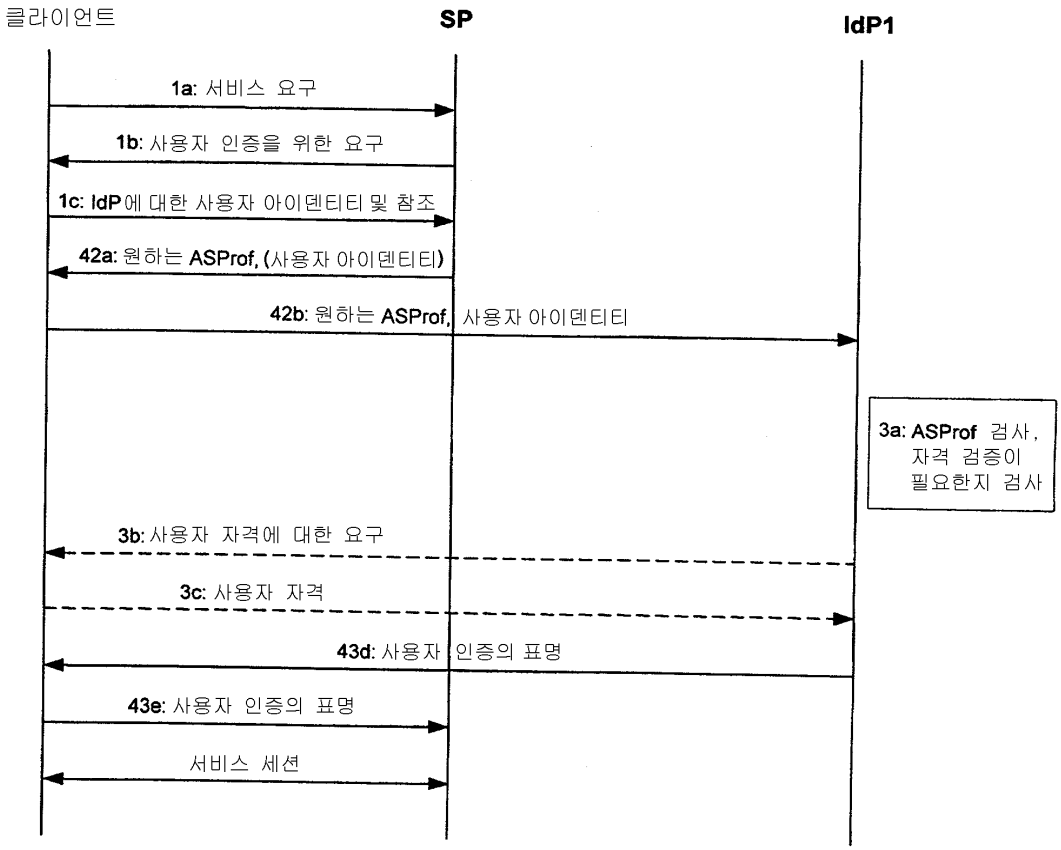
도면2


인증
보안
강도
0 1 2 3 4 5 6 7 8 9 10
15
패스워드
길이
루트 노드
(패스워드 길이 0)
50 이상의 문자
1-2 문자
21-49 문자
11-20 문자
3-6 문자
7-10 문자

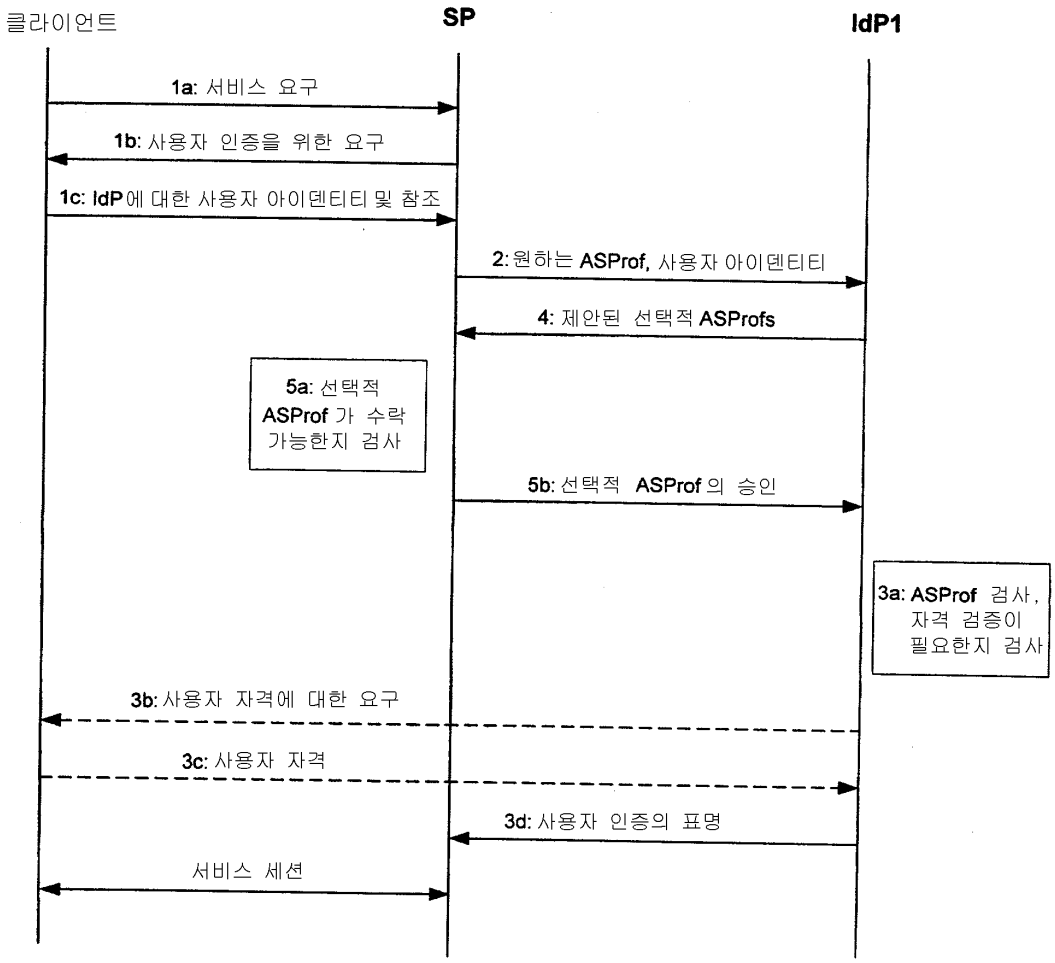
도면3


클라이언트
SP
IdP1
1a: 서비스 요구
1b: 사용자 인증을 위한 요구
1c: IdP에 대한 사용자 아이덴티티 및 참조
2: 원하는 ASProf, 사용자 아이덴티티
3a: ASProf 검사,
자격 검증이
필요한지 검사
3b: 사용자 자격에 대한 요구
3c: 사용자 자격
3d: 사용자 인증의 표명
서비스 세션

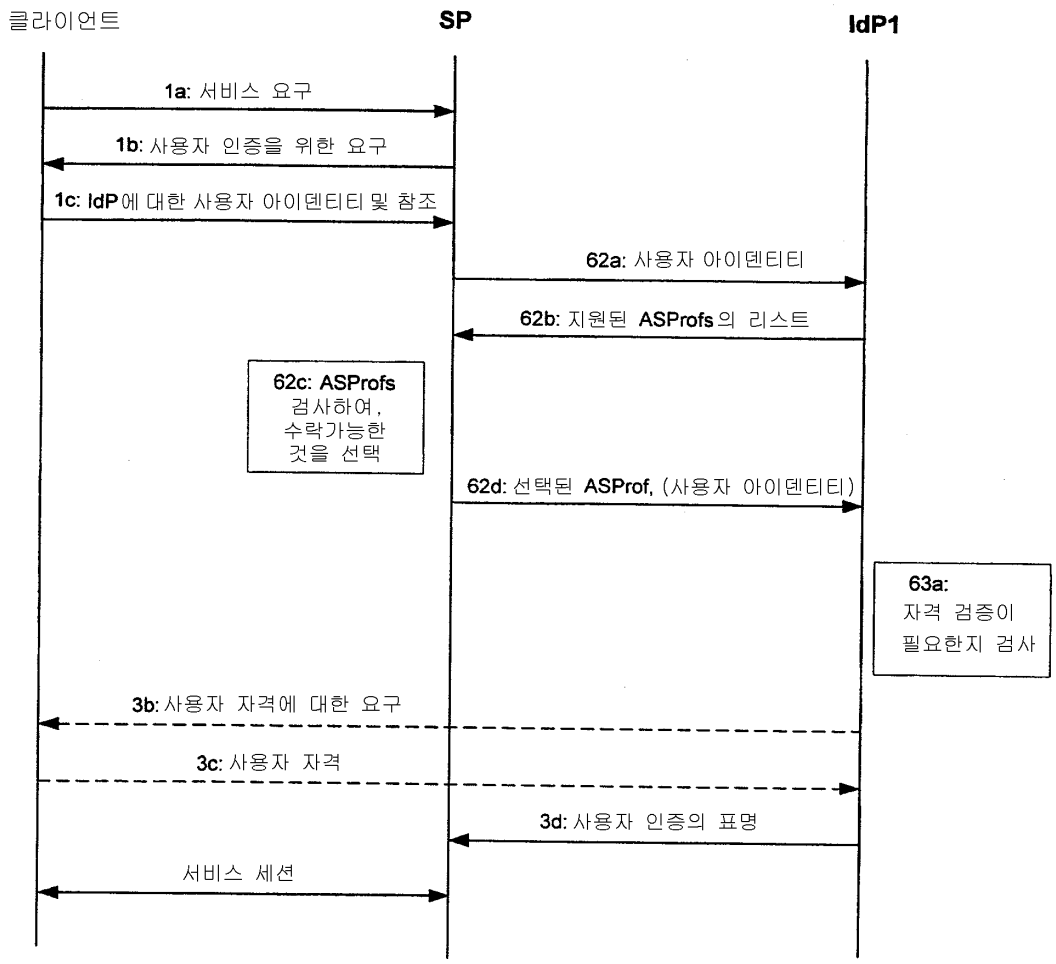
도면4


클라이언트
SP
IdP1
1a: 서비스 요구
1b: 사용자 인증을 위한 요구
1c: IdP에 대한 사용자 아이덴티티 및 참조
42a: 원하는 ASProf, (사용자 아이덴티티)
42b: 원하는 ASProf, 사용자 아이덴티티
3a: ASProf 검사, 자격 검증이 필요한지 검사
3b: 사용자 자격에 대한 요구
3c: 사용자 자격
43d: 사용자 인증의 표명
43e: 사용자 인증의 표명
서비스 세션

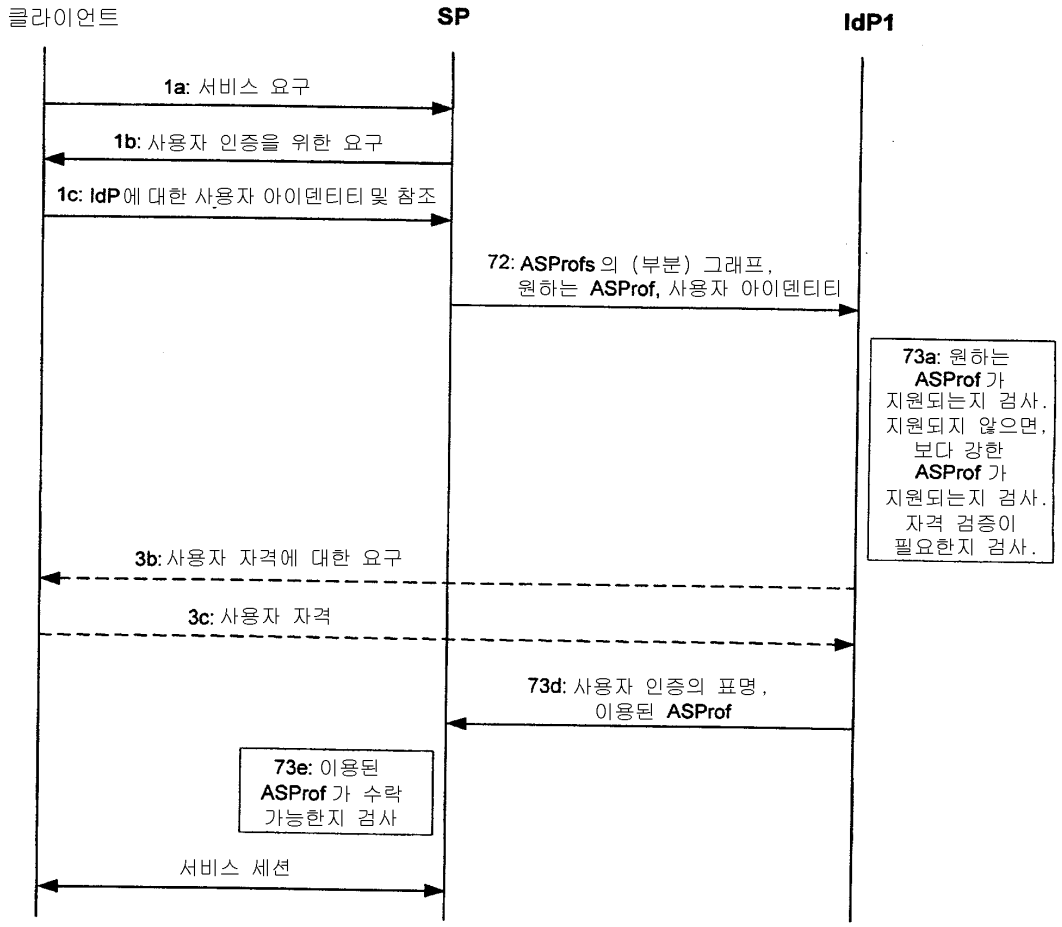
도면5


클라이언트
SP
IdP1
1a: 서비스 요구
1b: 사용자 인증을 위한 요구
1c: IdP에 대한 사용자 아이덴티티 및 참조
2: 원하는 ASProf, 사용자 아이덴티티
4: 제안된 선택적 ASProfs
5a: 선택적 ASProf 가 수락 가능한지 검사
5b: 선택적 ASProf 의 승인
3a: ASProf 검사, 자격 검증이 필요한지 검사
3b: 사용자 자격에 대한 요구
3c: 사용자 자격
3d: 사용자 인증의 표명
서비스 세션

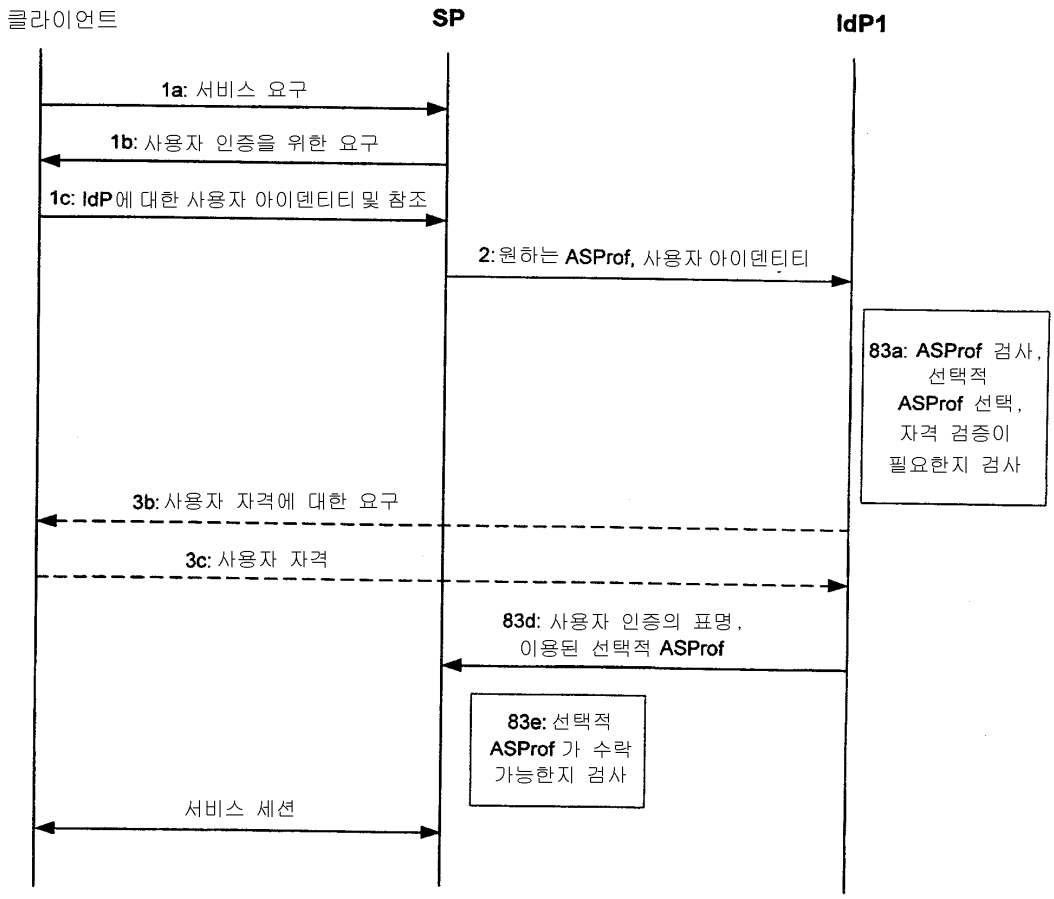
도면6


클라이언트
SP
IdP1
1a: 서비스 요구
1b: 사용자 인증을 위한 요구
1c: IdP에 대한 사용자 아이덴티티 및 참조
62a: 사용자 아이덴티티
62b: 지원된 ASProfs의 리스트
62c: ASProfs 검사하여, 수락가능한 것을 선택
62d: 선택된 ASProf, (사용자 아이덴티티)
63a: 자격 검증이 필요한지 검사
3b: 사용자 자격에 대한 요구
3c: 사용자 자격
3d: 사용자 인증의 표명
서비스 세션

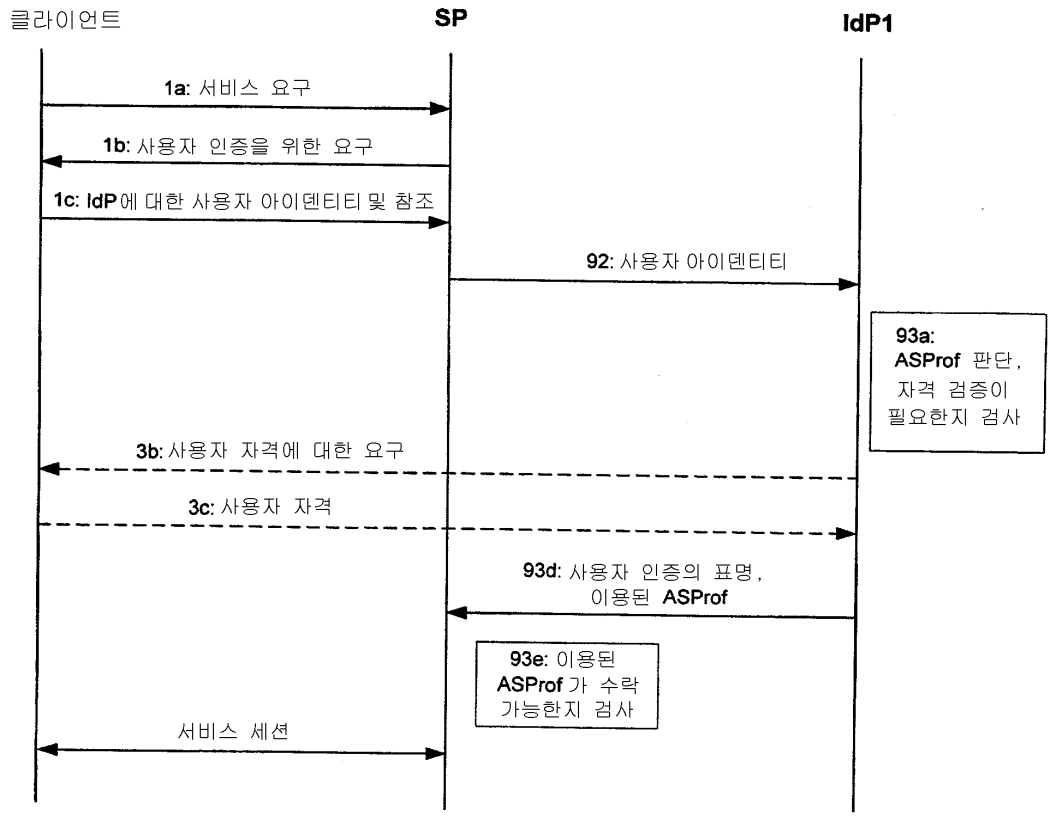
도면7


클라이언트
SP
IdP1
1a: 서비스 요구
1b: 사용자 인증을 위한 요구
1c: IdP에 대한 사용자 아이덴티티 및 참조
72: ASProfs의 (부분) 그래프, 원하는 ASProf, 사용자 아이덴티티
73a: 원하는 ASProf가 지원되는지 검사. 지원되지 않으면, 보다 강한 ASProf가 지원되는지 검사. 자격 검증이 필요한지 검사.
3b: 사용자 자격에 대한 요구
3c: 사용자 자격
73d: 사용자 인증의 표명, 이용된 ASProf
73e: 이용된 ASProf가 수락 가능한지 검사
서비스 세션

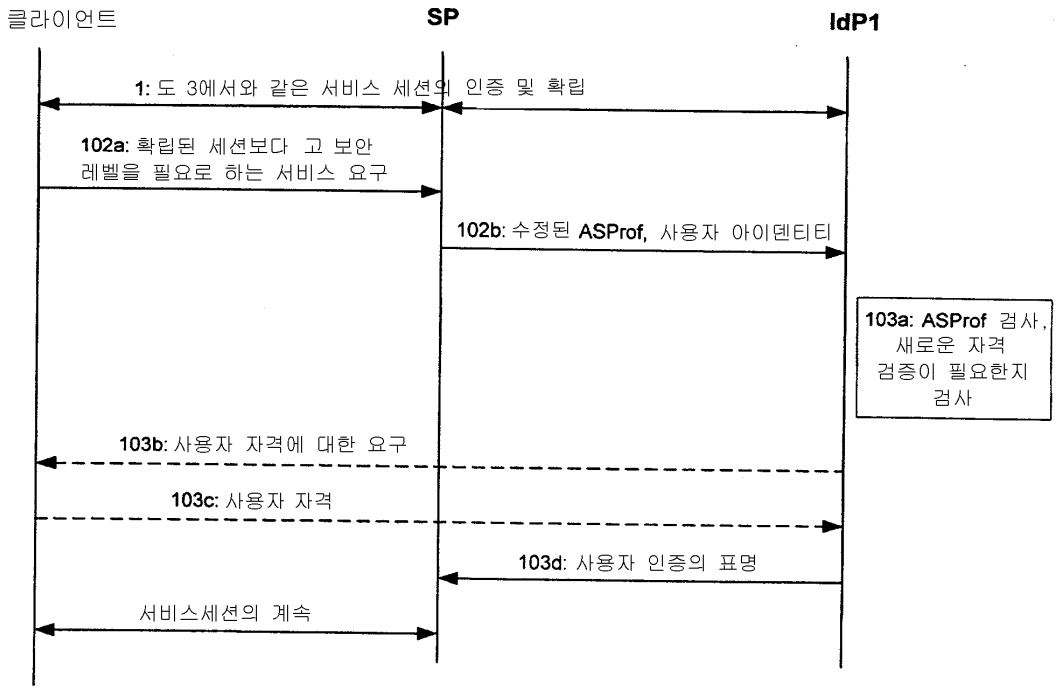
도면8


클라이언트
SP
IdP1
1a: 서비스 요구
1b: 사용자 인증을 위한 요구
1c: IdP에 대한 사용자 아이덴티티 및 참조
2: 원하는 ASProf, 사용자 아이덴티티
83a: ASProf 검사, 선택적 ASProf 선택, 자격 검증이 필요한지 검사
3b: 사용자 자격에 대한 요구
3c: 사용자 자격
83d: 사용자 인증의 표명, 이용된 선택적 ASProf
83e: 선택적 ASProf 가 수락 가능한지 검사
서비스 세션

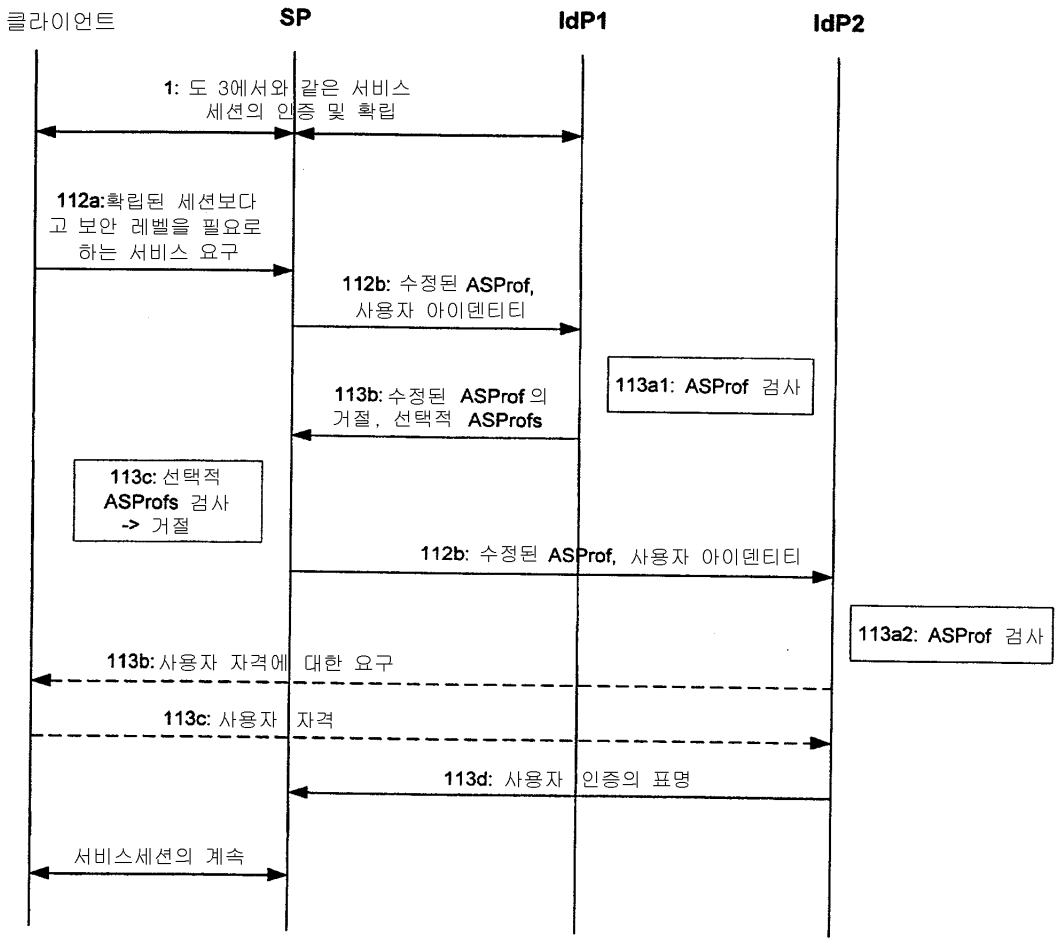
도면9


클라이언트
SP
IdP1
1a: 서비스 요구
1b: 사용자 인증을 위한 요구
1c: IdP에 대한 사용자 아이덴티티 및 참조
92: 사용자 아이덴티티
93a: ASProf 판단, 자격 검증이 필요한지 검사
3b: 사용자 자격에 대한 요구
3c: 사용자 자격
93d: 사용자 인증의 표명, 이용된 ASProf
93e: 이용된 ASProf가 수락 가능한지 검사
서비스 세션

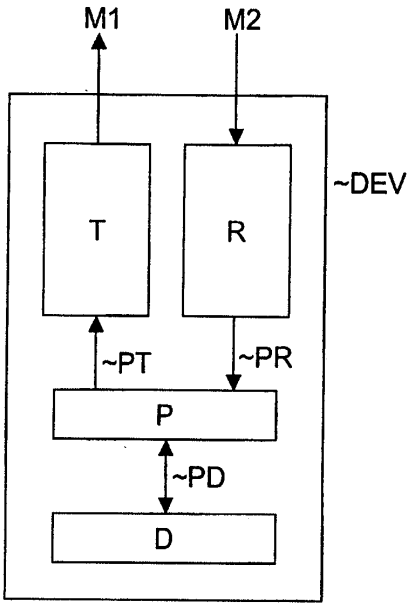
도면10


클라이언트
SP
IdP1
1: 도 3에서와 같은 서비스 세션의 인증 및 확립
102a: 확립된 세션보다 고 보안 레벨을 필요로 하는 서비스 요구
102b: 수정된 ASProf, 사용자 아이덴티티
103a: ASProf 검사, 새로운 자격 검증이 필요한지 검사
103b: 사용자 자격에 대한 요구
103c: 사용자 자격
103d: 사용자 인증의 표명
서비스세션의 계속

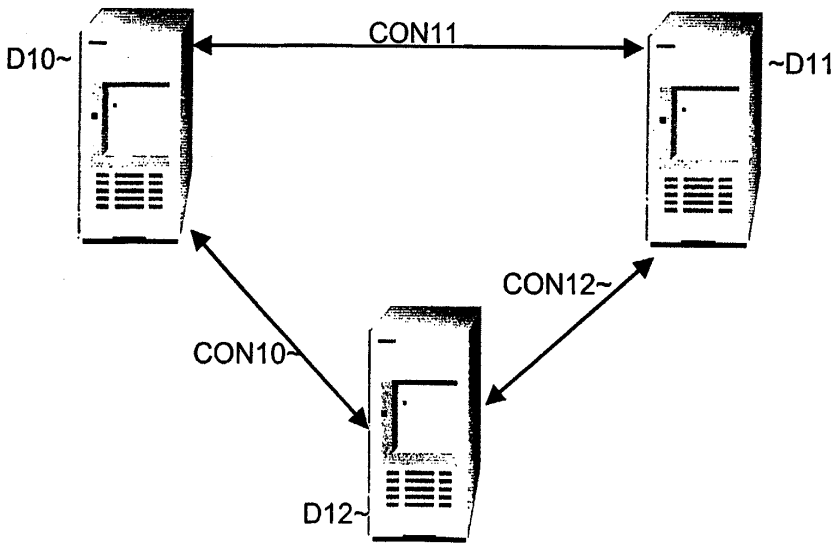
도면11


클라이언트
SP
IdP1
IdP2
1: 도 3에서와 같은 서비스 세션의 인증 및 확립
112a:확립된 세션보다 고 보안 레벨을 필요로 하는 서비스 요구
112b: 수정된 ASProf, 사용자 아이덴티티
113a1: ASProf 검사
113b: 수정된 ASProf 의 거절, 선택적 ASProfs
113c: 선택적 ASProfs 검사 -> 거절
112b: 수정된 ASProf, 사용자 아이덴티티
113a2: ASProf 검사
113b: 사용자 자격에 대한 요구
113c: 사용자 자격
113d: 사용자 인증의 표명
서비스세션의 계속

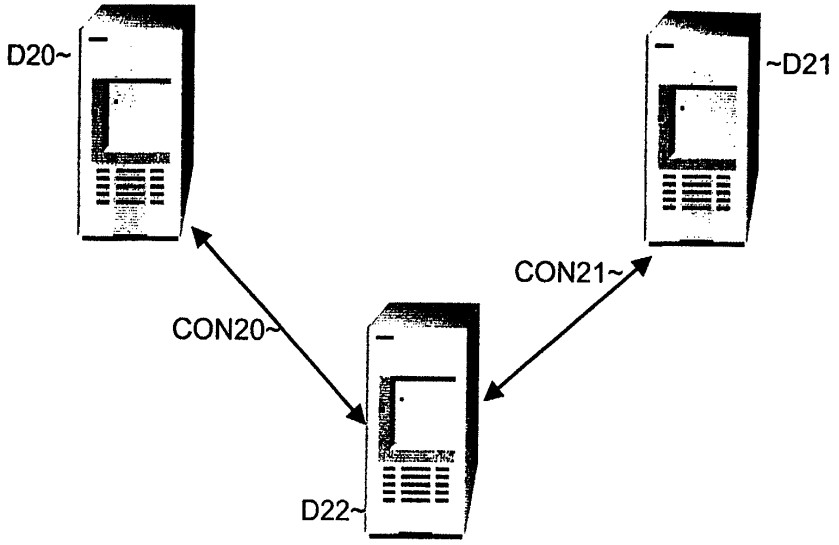
도면12


M1
M2
T
R
~DEV
~PT
~PR
P
~PD
D

도면13



도면14



도면15