(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2007년10월09일
(11) 등록번호 10-0764882
(24) 등록일자 2007년10월01일

(51) Int. Cl.
H04L 9/32(2006.01) *H04L 9/28*(2006.01)
H04L 9/30(2006.01) *H04L 9/08*(2006.01)
(21) 출원번호 10-2006-0095882
(22) 출원일자 2006년09월29일
심사청구일자 2006년09월29일
(56) 선행기술조사문헌
KR1020000006633 A
(뒷면에 계속)

(73) 특허권자
한국과학기술원
대전 유성구 구성동 373-1
(72) 발명자
박기웅
서울 노원구 월계4동 500-11번지
임상석
광주 광산구 월곡2동 일신아파트 104동 1403호
박규호
충청남도 공주시 장기면 금암리 314-98 번지
(74) 대리인
이원희

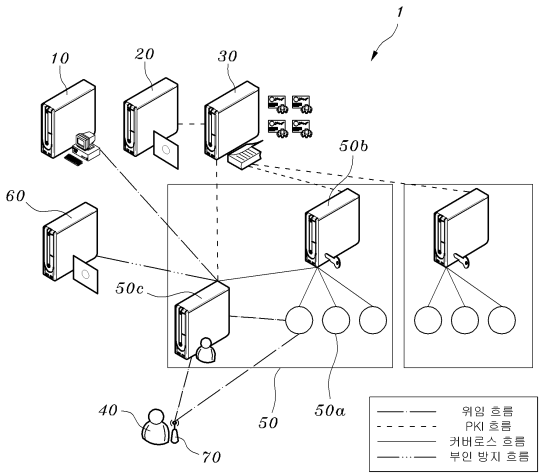
전체 청구항 수 : 총 10 항 심사관 : 이준석

(54) 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증 장치및 방법

(57) 요 약

본 발명은 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증장치 및 인증 방법에 관한 것으로서, 인증장치를 영역별로 구획하여 하나의 대칭키 기반 서버가 관리함으로써 인증연산의 지연을 최소화시키고, 사용자의 인증연산을 위임 서버에게 위임하여 인증에 소요되는 지연시간을 단축할 수 있으며, 위임 환경에서 심판 서버를 구비하여 공개키 기반구조와 동일한 보안성과 사용자의 부인을 방지하는 기능을 유지가능한 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증장치 및 인증 방법을 제공하기 위한 것으로서, 그 기술적 구성은 사용자의 위치를 파악하는 위치서버와, 인증서를 생성 및 관리하는 인증서 기관과, 인증서를 저장하는 LDAP 디렉토리 서버(Lightweight Directory Access Protocol Directory Server)와, 사용자의 신분 및 소속을 확인하는 인증장치와, 대칭키 기반의 인증 서버인 커버로스 서버로 이루어지는 공개키 기반구조 기반의 인증장치에 있어서, 사용자가 위임한 인증에 대한 개인키 및 공개키를 포함하되, 상기 개인키로 대행 인증서를 생성시키고, 사용자의 요청에 따라 인증에 대한 연산을 수행하는 위임서버; 사용자가 인증에 대하여 부인을 할 경우를 방지하기 위하여 내장된 키를 이용하여 인증에 대한 증거 데이터를 저장하고, 저장된 증거 데이터로 사용자의 부인을 방지하도록 구비되는 심판서버; 및 인증장치로부터 인증을 받아 인증이 요구되는 서비스를 제공받도록 인증, 권한, 과금 등의 기능이 구비되어, 저사양 프로세서로 구동하되 통신 기능이 구비되는 보안 단말기; 를 포함하여 이루어지는 것을 특징으로 한다.

대표도 - 도2



(56) 선행기술조사문헌
KR1020010067966 A
KR1020030059959 A
KR1020030062402 A
KR1020030083857 A
KR1020040102333 A
KR1020060077444 A

특허청구의 범위

청구항 1

사용자의 위치를 파악하는 위치서버(10)와, 인증서를 생성 및 관리하는 인증서 기관(20)과, 인증서를 저장하는 LDAP 디렉토리 서버(Lightweight Directory Access Protocol Directory Server, 30)와, 사용자의 신분 및 소속을 확인하는 인증장치(50a)와, 대칭키 기반의 인증 서버인 커버로스 서버(50b)로 이루어지는 공개키 기반구조 기반의 인증장치에 있어서,

사용자(40)가 위임한 인증에 대한 개인키 및 공개키를 포함하되, 상기 개인키로 대행 인증서를 생성시키고, 사용자(40)의 요청에 따라 인증에 대한 연산을 수행하는 위임서버(50c);

사용자(40)가 인증에 대하여 부인을 할 경우를 방지하기 위하여 내장된 키를 이용하여 인증에 대한 증거 데이터를 저장하고, 저장된 증거 데이터로 사용자(40)의 부인을 방지하도록 구비되는 심판서버(60); 및

인증장치(50a)로부터 인증을 받아 인증이 요구되는 서비스를 제공받도록 인증, 권한, 과금 등의 기능이 구비되어, 저사양 프로세서로 구동하되 통신 기능이 구비되는 보안 단말기(70); 를 포함하여 이루어지는 것을 특징으로 하는 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증장치.

청구항 2

제1항에 있어서,

상기 위임서버(50c)는 위치서버(10)를 이용하여 사용자(40)의 위치정보를 파악하고, 인증 서비스에 요구되는 티켓 및 세션 키를 미리 수신하여 인증에 요구되는 응답 메세지를 인증장치(50a)에 전달하도록 구비되는 것을 특징으로 하는 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증장치.

청구항 3

제1항에 있어서,

상기 심판서버(60)는 공유키로 암호화하고, 위임서버의 공개키로 재암호화하여 사용자가 특정키의 형태로 공유하는 것을 특징으로 하는 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증장치.

청구항 4

제1항에 있어서,

상기 인증장치(50a), 커버로스 서버(50b), 위임서버(50c)는 섹션(50)을 이루며, 각 섹션(50)의 인증연산을 위한 티켓 및 세션키를 생성 및 관리하는 것을 특징으로 하는 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증장치.

청구항 5

제4항에 있어서,

섹션(50)의 대칭키 기반 인증 서버인 커버로스 서버(50b)는 공개키 기반구조의 개체가 되는 구조로 이루어지는 것을 특징으로 하는 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증 장치.

청구항 6

사용자의 위치를 파악하는 위치서버(10)와, 인증서를 생성 및 관리하는 인증서 기관(20)과, 인증서를 저장하는 LDAP 디렉토리 서버(Lightweight Directory Access Protocol Directory Server, 30)와, 사용자의 신분 및 소속을 확인하는 인증장치(50a)와, 대칭키 기반의 인증 서버인 커버로스 서버(50b)와, 인증 연산을 위임받아 수행하는 위임서버(50c)를 포함하여 이루어져, 사용자(40)의 본인 인증을 수행하는 공개키 기반구조 기반의 인증 방법에 있어서,

사용자가 본인 인증을 위하여 접근하는 챌린지 메세지를 수신하는 단계(S20);

사용자의 인증에 대한 위임 여부를 묻는 단계(S30);

위임이 되지 않았으면, 위임인증 연산요청을 하는 단계(S31);

위임서버(50c)가 요청받은 인증에 대한 티켓과 세션키가 존재하는 지의 여부를 묻는 단계(S32); 및

티켓과 세션키가 존재하면, 반응 메세지를 생성하여 인증장치(50a)로 전송하는 단계(S41, S42);

를 포함하여 이루어지는 것을 특징으로 하는 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증 방법.

청구항 7

제6항에 있어서,

상기 단계(S30)에서 사용자(40)의 위임이 되었으면, 위임서버(50c)가 개인키 및 공개키를 생성 및 사용자 서명의 위임연산을 수행하여 위임을 완료시키는 단계(S33, S35);를 더 포함하는 것을 특징으로 하는 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증 방법.

청구항 8

제6항에 있어서,

상기 단계(S31)는 사용자(40)가 위임서버(50c)로 위임을 한 후, 서비스에 대한 인증을 수행하기 위하여 챌린지 메세지를 위임서버(50c)에 전달하는 것을 더 포함하는 것을 특징으로 하는 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증 방법.

청구항 9

제6항에 있어서,

상기 단계(S40)에서 위임서버(50c)가 요청받은 인증에 대한 티켓을 가지고 있는 경우에는, 세션키를 요청하여 세션키를 획득하는 단계(S43, S44)를 더 포함하여 이루어지며, 상기 단계(S42)로 진입하는 것을 특징으로 하는 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증 방법.

청구항 10

제6항에 있어서,

상기 단계(S40)에서 위임서버(50c)에 요청받은 인증에 대한 티켓과 세션키가 존재하지 않는다면, 티켓을 요청하여 획득하는 단계(S47, S48)을 더 포함하여 이루어지며, 상기 단계(S44)로 진입하는 것을 특징으로 하는 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<16> 본 발명은 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증장치 및 인증 방법에 관한 것으로, 더욱 상세하게는 인증장치를 영역별로 구획하여 하나의 대칭키 기반 서버가 관리함으로써 인증연산의 지연을 최소화시키고, 사용자의 인증연산을 위임 서버에게 위임하여 인증에 소요되는 지연시간을 단축할 수 있으며, 보안 정책 및 성능의 발달에 따라 보안 구조 내부의 각각의 인증장치와 휴대장치의 교체없이 이에 따른 정책을 적용할 수 있어 유연한 정책관리가 가능하고, 위임 환경에서 심판 서버를 구비하여 공개키 기반구조와 동일한 보안성과 사용자의 부인을 방지하는 기능을 유지가능한 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증장치 및 인증 방법에 관한 것이다.

<17> 일반적으로, 전자거래 및 정보유통의 안전성과 신뢰성을 확보하고, 상대방의 신원을 확인하며, 정보 내용의 변경확인과 비밀유지기능을 가지는 지식 정보화 사회의 핵심기반 시스템인 공개키 기반구조(PKI: Pulbic Key Infrastructure)는 인증서를 발행하거나 인증서 취소 목록(CRL: Certification Revocation List)을 생성하는 인증기관과 인증기관으로부터 위임받아 사용자의 신분확인 절차를 대신하는 등록기관과 인증기관이 발행한 인증

서 및 인증서 취소 목록을 보관하기 위한 보관서인 디렉토리와 인증서를 발행받는 최종 개체인 사용자를 포함하여 이루어진다.

<18> 상기와 같은 구성으로 인터넷 사용자가 보유한 암호를 이용하여 거래자 신원을 확인하는 방법인 공개키 기반구조는 암호화 키(Encryption Key)와 복호화 키(Decryption Key)로 구성된 공개키와 공개키를 이용하여 송수신 데이터를 암호화하고, 인증서를 통하여 사용자를 인증하는 시스템으로 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하는 복합적인 보안 시스템 환경이다.

<19> 여기서, 공개키 기반 인증방법은 암호화 키와 복호화 키가 별개이므로, 데이터를 암호화하여 이를 복호화할 수 있는 키가 다르고, 이에 따라 데이터 보완이 가능하여 정보 유출의 가능성이 낮기 때문에, 공개키 기반구조를 이용하여 본인 인증이 요구되는 전자상거래를 할 경우에는 전자 상거래를 위한 전자 서명을 한 후, 공인 인증기관의 인증을 받아 상대방에게 제시함으로써 거래가 성립되는데, 개인 정보 및 거래 정보가 외부에 노출되지 않아 안전하게 거래할 수 있다.

<20> 도 1은 종래 기술에 따른 공개키 기반구조 기반의 인증 구조를 개략적으로 도시한 구성도이다. 도면에서 도시하고 있는 바와 같이, 공개키 기반구조 기반의 인증 구조(100)는 인증서를 생성 및 관리하는 기능을 가지는 인증서 기관(120)과 사용자(140)의 신분 및 소속을 확인하는 인증장치(150)와 사용자(140)가 상기 인증장치(150)에 접근하면 사용자(140)에 대한 사용자 인증서(133)를 송신하는 LDAP 디렉토리 서버(Lightweight Directory Access Protocol Directory Server, 130)와 상기 LDAP 디렉토리 서버(130)로부터 수신되는 인증장치 인증서(131)를 포함하여 이루어진다.

<21> 상기한 구성으로 사용자(140)가 인증을 받기 위하여 인증장치(150)에 접근하면, 상기 인증장치(150)는 사용자(140)에 대한 사용자 인증서(133)를 LDAP 디렉토리 서버(130)로부터 수신한다.

<22> 이때, 상기 LDAP 디렉토리 서버(130)는 각 사용자(140)와 인증장치(150)에 대한 사용자 인증서(133)와 인증장치 인증서(131)을 보유하고 있는데, 상기 인증장치(150)가 챌린지 메세지(Challenge Message)를 생성하고, 상기 인증장치(150)의 개인키(Private Key)를 이용하여 챌린지 메세지를 RSA(Rivest Shamir Adleman) 알고리즘을 이용하여 암호화 시킨 후, 사용자(140)의 공개키를 이용하여 다시 RSA 알고리즘으로 암호화시키고, 사용자(140)에게 전송한다.

<23> 여기서, 사용자(140)는 개인키와 RSA 알고리즘을 이용하여 복호화시킨 후, LDAP 디렉토리 서버(130)로부터 인증장치 인증서(131)를 받고, 다시 RSA 알고리즘을 이용하여 복호화시키며, 인증장치(150)로 재송신하면 인증장치(150)는 챌린지 메세지의 내용의 진위 여부를 판단하여 사용자(140)의 인증을 종료하게 된다.

<24> 이를 위하여, 보다 빠른 인증서의 검증과, 인증서 폐지 목록의 갱신 주기성 문제를 해결하기 위해 폐지/ 효력정지 상태를 파악하여 사용자가 실시간으로 인증서를 검증할 수 있도록 OCSP 서버(Online Certificate Status Protocol Server, 110)을 사용하는 것이 바람직하다.

<25> 그러나, 공개키 기반구조 기반의 인증 서비스를 제공하기 위하여 보안 구조를 구축하는 방법은 각각의 인증장치와 사용자가 공개키 및 개인키를 생성하여야하며, 인증을 위한 RSA 알고리즘을 수행할 수 있는 고속 프로세서를 내장시켜 시스템의 단가 상승의 요인으로 작용하였고, 보안 정책 및 성능의 발달에 따라 보안 구조 내부의 각각의 인증장치와 휴대장치의 교체가 요구되는 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

<26> 본 발명은 상기한 문제점을 해결하기 위하여 안출한 것으로, 인증장치를 영역별로 구획하여 하나의 대칭키 기반 서버가 관리함으로써 인증연산의 지연을 최소화시키고, 사용자의 인증연산을 위임 서버에게 위임하여 인증에 소요되는 지연시간을 단축할 수 있으며, 보안 정책 및 성능의 발달에 따라 보안 구조 내부의 각각의 인증장치와 휴대장치의 교체없이 이에 따른 정책을 적용할 수 있어 유연한 정책관리가 가능하고, 위임 환경에서 심판 서버를 구비하여 공개키 기반구조와 동일한 보안성과 사용자의 부인을 방지하는 기능을 유지가능한 저성능 보안 단말기의 공개키 기반 싱글 사인온 인증장치 및 인증 방법을 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

<27> 상기한 바와 같은 목적을 달성하기 위하여 본 발명은 사용자의 위치를 파악하는 위치서버와, 인증서를 생성 및 관리하는 인증서 기관과, 인증서를 저장하는 LDAP 디렉토리 서버(Lightweight Directory Access Protocol Directory Server)와, 사용자의 신분 및 소속을 확인하는 인증장치와, 대칭키 기반의 인증 서버인 커버로스 서

버로 이루어지는 공개키 기반구조 기반의 인증장치에 있어서, 사용자가 위임한 인증에 대한 개인키 및 공개키를 포함하되, 상기 개인키로 대행 인증서를 생성시키고, 사용자의 요청에 따라 인증에 대한 연산을 수행하는 위임서버; 사용자가 인증에 대하여 부인을 할 경우를 방지하기 위하여 내장된 키를 이용하여 인증에 대한 증거 데이터를 저장하고, 저장된 증거 데이터로 사용자의 부인을 방지하도록 구비되는 심판서버; 및 인증장치로부터 인증을 받아 인증이 요구되는 서비스를 제공받도록 인증, 권한, 과금 등의 기능이 구비되어, 저사양 프로세서로 구동하되 통신 기능이 구비되는 보안 단말기; 를 포함하여 이루어지는 것을 특징으로 한다.

<28> 여기서, 상기 위임서버는 위치서버를 이용하여 사용자의 위치정보를 파악하고, 인증 서비스에 요구되는 티켓 및 세션 키를 미리 수신하여 인증에 요구되는 응답 메세지를 인증장치에 전달하도록 구비되는 것을 특징으로 한다.

<29> 또한, 상기 심판서버는 공유키로 암호화하고, 위임서버의 공개키로 재암호화하여 사용자가 특정키의 형태로 공유하는 것을 특징으로 한다.

<30> 이때, 상기 인증장치, 커버로스 서버, 위임서버는 섹션을 이루며, 각 섹션의 인증연산을 위한 티켓 및 세션키를 생성 및 관리하는 것을 특징으로 한다.

<31> 그리고, 섹션의 대칭키 기반 인증 서버인 커버로스 서버는 공개키 기반구조의 개체가 되는 구조로 이루어진다.

<32> 한편, 사용자의 위치를 파악하는 위치서버와, 인증서를 생성 및 관리하는 인증서 기관과, 인증서를 저장하는 LDAP 디렉토리 서버(Lightweight Directory Access Protocol Directory Server)와, 사용자의 신분 및 소속을 확인하는 인증장치와, 대칭키 기반의 인증 서버인 커버로스 서버와, 인증 연산을 위임받아 수행하는 위임서버를 포함하여 이루어져, 사용자의 본인 인증을 수행하는 공개키 기반구조 기반의 인증 방법에 있어서, 사용자가 본인 인증을 위하여 접근하는 챌린지 메세지를 수신하는 단계; 사용자의 인증에 대한 위임 여부를 묻는 단계; 위임이 되지 않았으면, 위임인증 연산요청을 하는 단계; 위임서버가 요청받은 인증에 대한 티켓과 세션키가 존재하는 지의 여부를 묻는 단계; 및 티켓과 세션키가 존재하면, 반응 메세지를 생성하여 인증장치로 전송하는 단계; 를 포함하여 이루어진다.

<33> 이때, 상기 단계에서 사용자의 위임이 되었으면, 위임서버가 개인키 및 공개키를 생성 및 사용자 서명의 위임연산을 수행하여 위임을 완료시키는 단계;를 더 포함한다.

<34> 여기서, 상기 단계는 사용자가 위임서버로 위임을 한 후, 서비스에 대한 인증을 수행하기 위하여 챌린지 메세지를 위임서버에 전달하는 것을 더 포함한다.

<35> 그리고, 상기 단계에서 위임서버가 요청받은 인증에 대한 티켓을 가지고 있는 경우에는, 세션키를 요청하여 세션키를 획득하는 단계를 더 포함한다.

<36> 또한, 상기 단계에서 위임서버에 요청받은 인증에 대한 티켓과 세션키가 존재하지 않는다면, 티켓을 요청하여 획득하는 단계을 더 포함하여 이루어지며, 상기 단계로 진입하는 것을 특징으로 한다.

<37> 이하, 본 발명에 따른 실시예를 첨부된 예시도면을 참고로 하여 상세하게 설명한다.

<38> 도 2는 본 발명의 공개키 기반구조 기반 싱글 사인온 인증 구조를 개략적으로 도시한 구성도이다. 도면에서 도시하고 있는 바와 같이, 공개키 기반구조 기반 싱글 사인온 인증 방법에 따른 인증 구조(1)는 사용자(40)의 위치를 파악하는 위치서버(10)와 인증서를 생성 및 관리하는 기능을 가지는 인증서 기관(20)과 인증서를 저장하는 LDAP 디렉토리 서버(Lightweight Directory Access Protocol Directory Server, 30)와 전자상거래 등에서 신분 및 소속을 확인받고자 하는 사용자(40)와 위임서버(50c), 커버로스 서버(50b), 인증 장치(50a)를 포함하는 섹션(50)과 사용자(40)의 인증에 대한 부인 방지를 위한 기능이 구비된 심판서버(60)와 사용자(40)가 인증을 위하여 휴대가능하도록 구비되는 보안 단말기(70)를 포함하여 이루어진다.

<39> 이때, 싱글 사인온(SSO: Single Sign On)은 하나의 아이디로 여러 사이트에 접속할 수 있는 시스템을 일컫는데, 권한관리시스템(EAM)과 함께 사용할 경우에 보안성 및 효율성을 동시에 가지는 통합인증시스템으로 활용가능한 것이다.

<40> 여기서, 위치서버(10)는 사용자(40)가 휴대하는 보안 단말기(70)의 위치를 관리하여 위치기반 서비스를 제공하는데, 각 사용자(40)가 자신의 위치를 공개할 경우에만 위치서버(10)로 자신의 위치를 공급하며, 위치 정보를 제공할 시에는 보다 빠른 인증 및 위치 기반 서비스를 제공하도록 구비된다.

<41> 그리고, 인증서 기관(20)은 인증서를 관리하고, 인증 구조(1)에 존재하는 각 개체의 인증서에 대한 서명을 하도록 구비된다.

<42> 또한, LDAP 디렉토리 서버(30)는 각 개체의 인증서를 저장하고, 동시에 각 개체가 인증을 요구할 시에는 요구되는 인증서로 응답하도록 구비된다.

<43> 더불어, 사용자(40)는 인증장치(50a)로부터 인증을 공급받고, 이에 따라 본인 인증이 요구되는 전자 상거래 등의 서비스를 제공받는 개체로서 서비스를 제공받는데 요구되는 인증, 권한, 과금 등의 기능을 초소형의 보안 단말기(70)를 통하여 공급받는다.

<44> 여기서, 상기 초소형의 보안 단말기(70)는 8 비트 프로세서와 통신 기능이 구비되어 비용이 절감되고, 저사양에서도 구현 가능한 것을 특징으로 한다.

<45> 한편, 섹션(50)에 포함되는 인증장치(50a)는 인증을 위한 서비스를 제공하고, 서비스를 제공하는 주제어장치에 부착되는 형태로 구성되며, 상기 주제어장치는 상기 초소형의 보안 단말기(70)의 사양으로 구성되는 것이 바람직하다.

<46> 그리고, 섹션(50)에 포함되는 커버로스 서버(50b)는 대칭키 기반의 인증 서버로서 각 섹션(50)에 설치되며, 상기 각 섹션(50)의 인증연산을 위한 티켓과 세션을 생성시키고, 이를 관리한다.

<47> 또한, 위임서버(50c)는 위임받은 사용자의 대리 개인키 및 공개키를 포함하며, 이에 따라 위임된 개인키는 사용자의 개인키로 서명이 되는 대행 인증서를 생성시키는데 보안 구조에 접근한 사용자(40)는 위임 기간 및 권한 등이 기재된 대행 인증서로 위임의 해지 및 위임 기간 초과 등의 변수가 작용하지 않는 한 사용자의 요청에 따라 국제 표준화 문서인 RFC3820을 이용하는 연산을 대행하여 처리한다.

<48> 여기서, 위임서버(50c)는 인증 지연시간을 감소시키기 위하여 위치서버(10)를 이용하여 사용자의 위치정보를 파악하고, 사용자가 사용할 서비스 장치를 예측하고, 이에 따른 인증 서비스에 요구되는 티켓 및 세션 키을 미리 받아 사용자의 인증에 요구되는 응답 메세지를 신속하게 생성하여 인증장치(50a)에 전달하도록 구비된다.

<49> 더불어, 심판서버(60)는 사용자(40)의 인증에 대한 부인 방지의 기능을 수행하는데, 상기 인증 구조(1)에서 각 개체에만 내장된 키를 이용하여 인증된 사실에 대한 증거를 저장하고, 이에 따라 사용자(40)가 인증에 대하여 부인을 할 때 저장된 증거 데이터를 이용하여 부인을 방지하는 매커니즘을 제공하도록 구비된다.

<50> 도 3은 본 발명에 따른 싱글 사인온 프로토콜의 흐름도를 개략적으로 도시한 도이며, 도 2를 참조하여 설명한다. 도면에서 도시한 바와 같이, 사용자(40)가 인증장치(50a)에 해당하는 서비스를 제공받기 위하여 접근하면 인증을 시작한다(S10).

<51> 그리고, 사용자(40)가 인증을 위하여 요청하는 챌린지 메세지를 수신하는 단계(S20)로 이동하며, 사용자(40)가 인증 구조(1)에 인증을 위한 위임 여부를 묻는 단계(S30)에서 사용자(40)의 위임 요청이 있었을 경우에는 개인키 및 공개키 생성과 사용자 서명의 위임 연산을 하는 단계(S33)로 진입하여 개인키 및 공개키를 생성시키고, 위임 연산을 하여 위임을 완료시킨다(S35).

<52> 이를 위하여, 위임서버(50c)가 생성한 공개키를 사용자에게 전송하고, 해당 공개키를 자신의 개인키로 서명을 하면 대행 인증서가 생성되고, 이를 위임서버(50c)에 재전송하는데, 이에 따라 사용자(40)가 수행할 RSA 연산을 위임서버(50c)에게 위임시킴으로써 타 서비스에 대한 인증 연산을 수행할 시에 요구되는 RSA 연산은 사용자가 위임한 위임서버(50c)가 수행한다.

<53> 여기서, RSA(Rivest Shamir Adleman)는 인터넷 암호화 및 인증시스템으로 두 개의 140자리 이상의 수인 소수를 이용하고, 이 수들의 곱 및 추가 연산을 통하여 공개키 및 개인키를 구성하고, 인터넷에서 사용하는 정보를 암호화하고 복호화할 수 있다.

<54> 따라서, 사용자(40)가 위임서버(50c)에 위임 시 명시한 위임기간 내에 재인증을 요청할 경우 상기 단계(S33)를 경유하지 않고, 위임인증 연산요청하는 단계(S31)로 진입할 수 있다.

<55> 여기서, 위임인증을 위한 연산을 요청하는 단계(S31)는 사용자(40)가 위임서버(50c)로 위임을 한 후, 서비스에 대한 인증을 수행하기 위하여 서비스 장치가 송신한 챌린지 메세지를 수신하고, 수신한 메세지를 위임서버(50c)에 전달하는 것을 포함하여 이루어진다.

<56> 그리고, 위임서버(50c)가 요청받은 인증에 대한 티켓과 세션키가 존재하는 지의 여부를 묻는 단계(S40)로 진입하고, 티켓과 세션키가 존재한다면(S41), 반응 메세지를 생성하여 인증장치(50a)에 전송함으로써 인증이 완료된다(S50).

<57> 이때, 상기 단계(S40)에서 위임서버(50c)가 요청받은 인증에 대한 티켓을 가지고있는 경우에는 세션키를 요청하는 단계(S44)로 진입하여 세션키를 획득하고(S45), 반응 메세지를 생성하여 인증장치(50a)에 전송하는 단계(S42)로 진입하여 인증이 완료된다.

<58> 한편, 상기 단계(S40)에서 티켓과 세션키가 존재하지 않는다면(S46), 티켓을 요청하는 단계(S47)로 이동하며, 티켓을 획득하면(S48) 세션키를 요청하는 단계(S44)로 진입하여 세션키를 획득하고(S45), 반응 메세지를 생성하여 인증장치(50a)에 전송하는 단계(S42)로 진입하여 인증이 완료된다.

<59> 도 4는 도 3의 싱글 사인온 프로토콜의 흐름도에 포함되는 위임 및 인증 매커니즘을 개략적으로 도시한 도이다. 도면에서 도시한 바와 같이, 사용자(40)가 위임서버(50c)에 자신의 권한을 위임시키면 인증장치(50a)는 사용자(40)에게 챌린지 메세지(81)을 송신한다.

<60> 그리고, 사용자(40)는 수신한 챌린지 메세지(81)를 위임서버(50c)로 전송하면 인증 요청 메세지(82)가 위임서버(50c)로 전달되고, 상기 위임서버(50c)는 사용자(40) 원하는 서비스에 해당하는 커버로스 서버(50b)를 통하여 티켓 및 세션 키 요청(83)을 하며, 이에 따라 커버로스 서버(50b)는 티켓 및 세션 키를 전송(84)하고, 이에 따라 응답 메세지(85)를 인증장치(50a)로 송신하여 인증이 완료되며, 인증확정메세지(86)를 사용자(40)에게 송신하도록 한다.

<61> 도 5 는 본 발명의 공개키 기반구조 기반 싱글 사인온 인증 방법에 따른 부인방지 매커니즘을 개략적으로 도시한 도이다. 도면에서 도시하고 있는 바와 같이, 사용자(40)의 인증이 위임된 환경에서 사용자(40)가 위임을 부인하는 것을 방지하도록 구비되는 매커니즘을 나타낸다.

<62> 여기서, 사용자(40)는 본인을 확인하기 위한 인증 시, 챌린지 메세지를 송신받게 되는데, 그 내부에는 서비스 캡슐(91)이 포함된다.

<63> 상기 서비스 캡슐(91)은 상기 서비스 캡슐(91)에 대한 일련번호(92)가 내장되어 있는 필드와 상기 일련번호(92) 및 인증장치(50a)가 생성한 무작위 데이터 값에 대한 해시 값(93)이 저장되어 있는 필드를 포함하여 이루어진다.

<64> 이때, 해시 값(93)에 대한 해시 함수(Hash Function)는 일방향 함수이기때문에, 사용자(40)는 인증장치(50a)가 송신한 해시 값(93)의 원본을 파악할 수 없고, 사용자(40)는 수신한 서비스 캡슐(91)을 사용자(40)와 심판서버(60)만이 지각할 수 있는 키를 이용하여 암호화시킨 후 포워딩하는데, 암호화하기 전의 서비스 캡슐(91)도 포워딩하여 저장시킨다.

<65> 여기서, 해시 함수(Hash Function)는 이동국이 사용할 수 있는 다수개의 재원 중에서 하나를 선택하는 방법에 관한 것으로, 다수개의 재원을 각 이동국에 고르게 분포할 수 있는 기능을 가진다.

<66> 그리고, 상기 사용자(40)와 심판서버(60)만이 지각할 수 있는 키는 위임을 요청할 때 공개키 기반구조 인증을 통하여 생성되고, 이에 따라 위임 서버(50c)는 응답 메세지(96)를 작성하기 전에 사용자가 위임에 대한 부인을 할 경우를 방지하기 위한 부인방지 데이터(94)를 심판서버(60)에 전달하여 특정 사용자에 대한 증거자료(95)를 수집할 수 있도록 구비된다.

<67> 예를 들어, 악의의 사용자가 특정 인증장치(50a)에 대한 인증 사실을 부인할 경우에는 심판서버(60)에 저장되어 있는 증거자료(95)를 통하여 증명할 수 있다.

<68> 다시 말하면, 사용자(40)는 위임요청시에 사용자(40)가 생성시킨 키를 공개키로 암호화하여 위임서버(50c)를 통하여 심판서버(60)로 전달되고, 사용자가 인증할 때마다 서비스 장치가 전송한 서비스 캡슐(91)을 사용자(40)와 심판서버(60)만이 지각할 수 있는 키로 암호화시켜 심판서버(60)에 저장이되기 때문에, 악의의 사용자가 본인 인증을 부인할 경우에는 무작위 데이터 및 일련번호(92)를 해시함수에 입력시키고, 입력에 대한 출력값이 저장된 서비스 캡슐(91)과 같다면 사용자(40)는 해당 서비스 캡슐(91) 메세지가 위임서버(50c)에게 포워딩됨을 증명함과 동시에, 사용자에 대한 인증부인방지 기능을 제공 가능하다.

<69> 이상에서는 본 발명의 바람직한 실시예를 예시적으로 설명하였으나, 본 발명의 범위는 이같은 특정 실시예에만 한정되지 않으며 해당 분야에서 통상의 지식을 가진자라면 본 발명의 특허 청구 범위내에 기재된 범주 내에서 적절하게 변경이 가능 할 것이다.

발명의 효과

<70> 이상에서 설명한 바와 같이 상기와 같은 구성을 갖는 본 발명은 인증장치를 영역별로 구획하여 하나의 대칭키 기반 서버가 관리함으로써 인증연산의 지연을 최소화시키고, 사용자의 인증연산을 위임 서버에게 위임하여 인증에 소요되는 지연시간을 단축할 수 있으며, 보안 정책 및 성능의 발달에 따라 보안 구조 내부의 각각의 인증장치와 휴대장치의 교체없이 이에 따른 정책을 적용할 수 있어 유연한 정책관리가 가능하고, 위임 환경에서 심판서버를 구비하여 공개키 기반구조와 동일한 보안성과 사용자의 부인을 방지하는 기능을 유지할 수 있는 등의 효과를 거둘 수 있다.

도면의 간단한 설명

<1> 도 1은 종래 기술에 따른 공개키 기반구조 기반의 인증 구조를 개략적으로 도시한 구성도.

<2> 도 2는 본 발명의 공개키 기반구조 기반 싱글 사인온 인증 구조를 개략적으로 도시한 구성도.

<3> 도 3은 본 발명에 따른 싱글 사인온 프로토콜의 흐름도를 개략적으로 도시한 도.

<4> 도 4는 도 3의 싱글 사인온 프로토콜의 흐름도에 포함되는 위임 및 인증 매커니즘을 개략적으로 도시한 도.

<5> 도 5는 본 발명의 공개키 기반구조 기반 싱글 사인온 인증 방법에 따른 부인방지 매커니즘을 개략적으로 도시한 도.

<6> <도면에 대한 도면 부호의 간단한 설명>

<7> 1: 인증 구조 10: 위치서버

<8> 20: 인증서 기관 30: LDAP 디렉토리 서버

<9> 40: 사용자 50: 섹션

<10> 50a: 인증장치 50b: 커버로스 서버

<11> 50c: 위임 서버 60: 심판서버

<12> 70: 보안 단말기 91: 서비스 캡슐

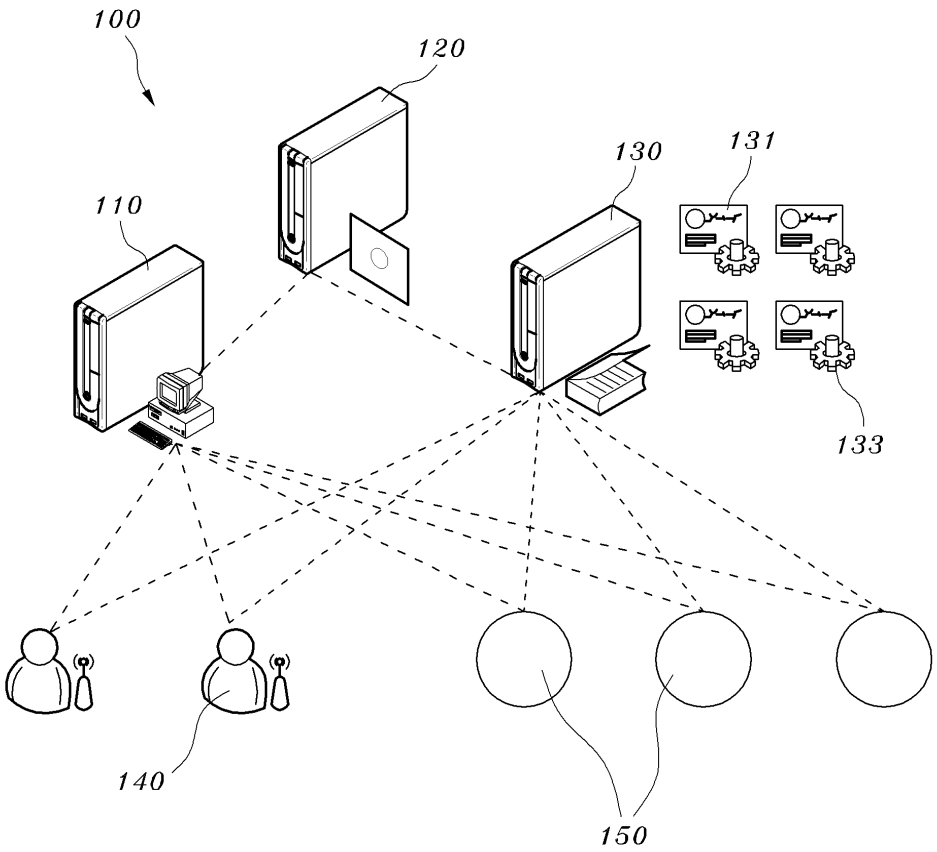
<13> 92: 일련번호 93: 해시 값

<14> 94: 부인방지 데이터 95: 증거자료

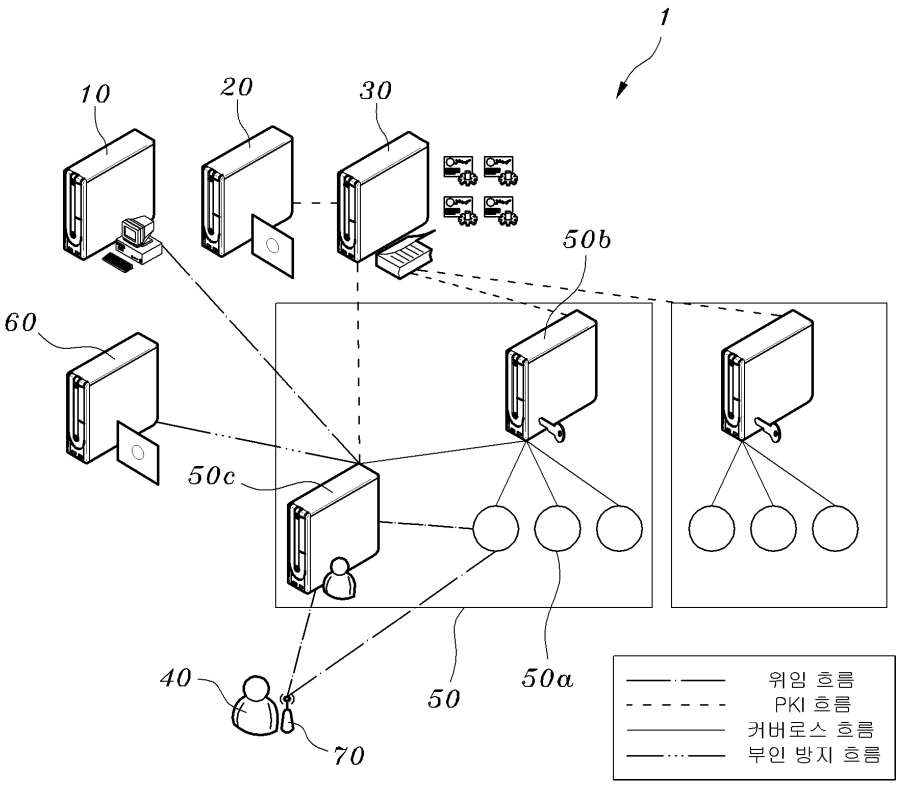
<15> 96: 응답 메세지

도면

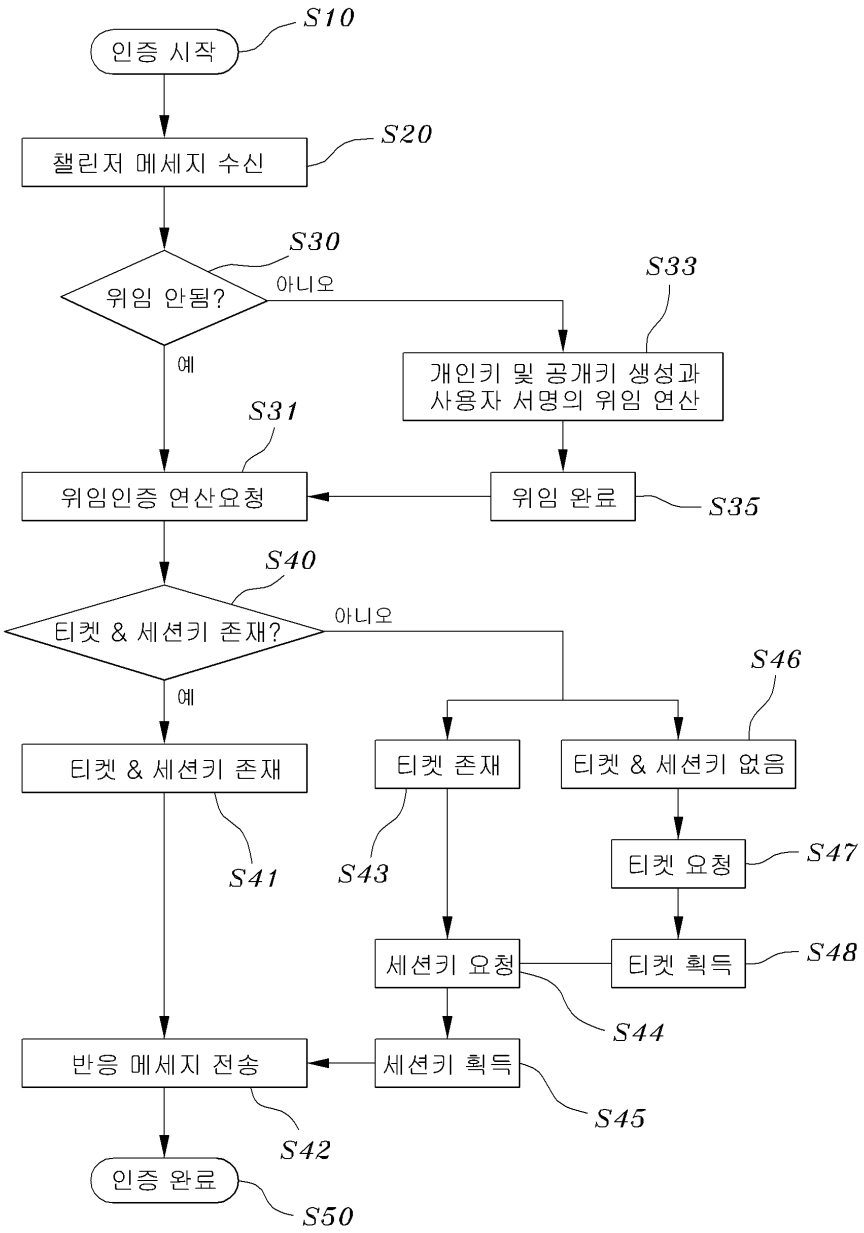
도면1



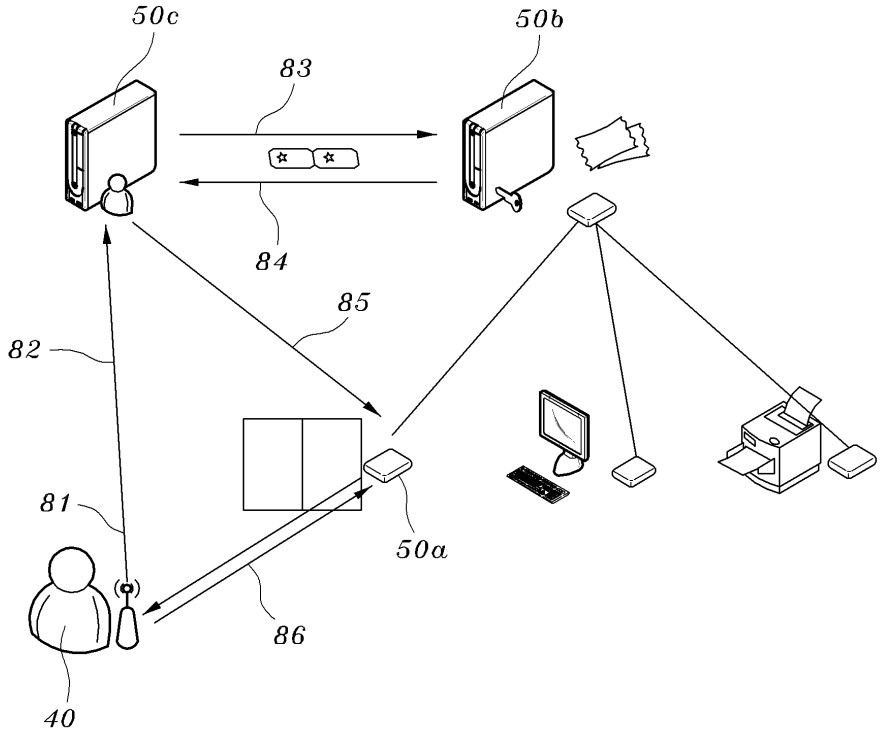
도면2



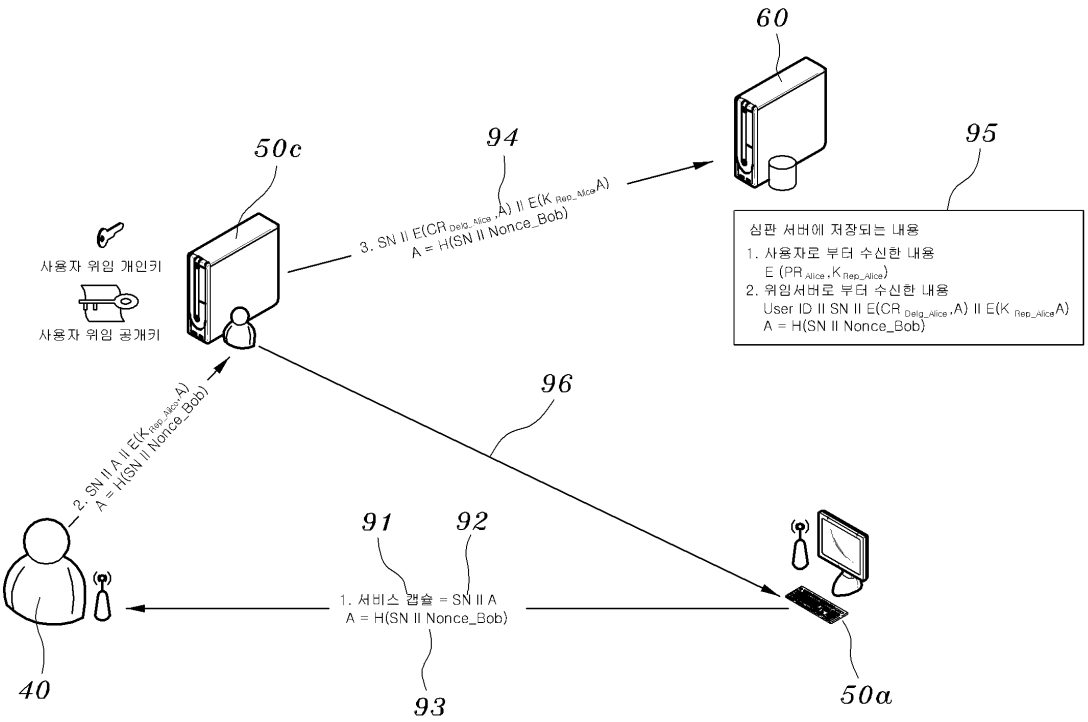
도면3


S10
인증 시작
S20
챌린저 메세지 수신
S30
위임 안됨?
아니오
예
S33
개인키 및 공개키 생성과
사용자 서명의 위임 연산
S31
위임인증 연산요청
위임 완료
S35
S40
티켓 & 세션키 존재?
아니오
예
S46
티켓 & 세션키 존재
티켓 존재
티켓 & 세션키 없음
S41
S43
티켓 요청
S47
세션키 요청
티켓 획득
S48
S44
반응 메세지 전송
세션키 획득
S45
S42
인증 완료
S50

도면4


50c
83
50b
84
85
82
81
50a
86
40

도면5


60
94
95
50c
3. SN II E(CR Delg_Alice ,A) II E(K Rep_Alice A)
A = H(SN II Nonce_Bob)
심판 서버에 저장되는 내용
1. 사용자로 부터 수신한 내용
E (PR Alice , K Rep_Alice)
2. 위임서버로 부터 수신한 내용
User ID II SN II E(CR Delg_Alice ,A) II E(K Rep_Alice A)
A = H(SN II Nonce_Bob)
사용자 위임 개인키
사용자 위임 공개키
96
2. SN II A II E(K Rep_Alice A)
A = H(SN II Nonce_Bob)
91
92
1. 서비스 캡슐 = SN II A
A = H(SN II Nonce_Bob)
40
93
50a