(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
H04L 9/32
H04L 9/08
G09C 1/00

(11) 공개번호 10-2005-0008627
(43) 공개일자 2005년01월21일

(21) 출원번호 10-2004-7000958
(22) 출원일자 2004년01월20일
번역문 제출일자 2004년01월20일
(86) 국제출원번호 PCT/JP2003/005605
(87) 국제공개번호 WO 2003/101042
(86) 국제출원출원일자 2003년05월02일
(87) 국제공개일자 2003년12월04일

(30) 우선권주장 JP-P-2002-00149925 2002년05월24일 일본(JP)
JP-P-2003-00069304 2003년03월14일 일본(JP)

(71) 출원인 소니 가부시끼 가이샤
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고

(72) 발명자 이이노,요이찌로
일본 141-0001 도꾜도 시나가와꾸 기따시나가와 6쪼메 7-35 소니 가부시끼가이샤 내

다나까,나오끼
일본 141-0001 도꾜도 시나가와꾸 기따시나가와 6쪼메 7-35 소니 가부시끼가이샤 내

(74) 대리인 장수길
구영창

심사청구 : 없음

(54) 정보 처리 시스템 및 방법, 정보 처리 장치 및 방법, 기록매체, 및 프로그램

요약

본 발명은, 서비스 제공자가, 사용자를 인증하는 경우에, 그 인증의 효율과 안전성을 높일 수 있도록 한 정보 처리 시스템 및 방법, 정보 처리 장치 및 방법, 기록 매체, 및 프로그램에 관한 것이다. 키 할당자 단말기(12)에 의해, 서비스 제공자 단말기(13)가, 소정의 인증 방법에 기초하여, 사용자 장치(11)의 키 기억 장치(22)를 인증하는 경우에 이용하는 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키가 생성되고, 제1 암호키가, 네트워크(14)를 통하여 서비스 제공자 단말기(13)로 송부됨과 함께, 제2 암호키가, 네트워크(14) 및 사용자 단말기(21)를 통하여 키 기억 장치(22)로 송부된다. 본 발명은, 복수의 서비스 제공자의 각각이, 대응하는 서비스를, 인터넷 등의 통신을 통하여 사용자에게 제공하는 경우, 서비스 제공자의 각각이, 사용자를 인증하는 시스템에 적용 가능하다.

대표도

도 3

색인어

키 할당자 단말기, 서비스 제공자 단말기, 암호키, 비밀키, 공유키, 사용자 인증, 네트워크

명세서

기술분야

본 발명은, 정보 처리 시스템 및 방법, 정보 처리 장치 및 방법, 기록 매체, 및 프로그램에 관한 것으로, 특히, 서비스 제공자가, 사용자를 인증하는 경우에, 그 인증의 효율과 안전성을 높일 수 있도록 한 정보 처리 시스템 및 방법, 정보 처리 장치 및 방법, 기록 매체, 및 프로그램에 관한 것이다.

배경기술

일반적으로, 유료의 서비스를 제공하는 사람은, 그 서비스를 제공하는 상대로부터, 그 대가를 회수한다.

예를 들면, 상대와 대면하여 서비스를 제공하는 사람은, 그 서비스를 제공할 때, 상대로부터 현금을 징수하는 경우가 많다.

이것에 대하여, 인터넷과 같은 통신을 경유하여, 유료의 서비스를 제공하는 사람은, 통신 경유로 교환 가능한 전자현금이 아직 실용화되어 있지 않기 때문에, 서비스의 대가를, 상대에의 「차지(charge)」로 하여 나중에 회수하거나, 또는, 그 상대가 이전에 대가의 지불을 마치고, 그 서비스를 이용할 권리를 얻고 있는 것을 확인한 후, 서비스의 제공을 행하는 경우가 많다. 따라서, 통신 경유로 유료의 서 비스를 제공하는 사람은, 서비스의 제공을 행하기 전에, 서비스를 제공하는 상대를 특정하는 것, 즉, 인증이 필요하게 된다.

이 인증이 행하여지는 경우, 인증을 행하는 측과 그것을 받는 측은, 서로 대응하는 정보를 갖고 있을 필요가 있다.

또한, 이하, 인증이 행하여지는 경우, 이러한, 서로 대응하는 정보를 갖고 또한, 상대를 특정하는 측을, 검증자라고 칭하고, 이것에 대하여, 특정되는 측을, 증명자라고 칭한다. 또한, 검증자에 의해 증명자가 인증되기 위해서 이용되는 방법을, 인증 방법이라 칭한다.

종래, 인증 방법으로서, 패스워드 인증, 공통 키 인증, 및, 공개키 인증이 알려져 있다.

이하, 이들의 인증 방법, 즉, 패스워드 인증, 공통 키 인증, 및, 공개키 인증의 각각에 대하여, 개별적으로 설명한다.

(패스워드 인증)

처음으로, 패스워드 인증에 대하여 설명한다.

패스워드 인증에 있어서는, 증명자는, 미리 검증자에 대하여, 증명자마다 서로 다른 로그인명을 등록하고, 패스워드를 정하여 놓는다. 그리고, 증명자와 검증자는, 패스워드를 자신들 이외에는 누출시키지 않는 약정을 행한다.

이 경우, 특정한 로그인명과 패스워드의 대응을 아는 것은, 원칙적으로, 그 로그인명으로 인증되는 증명자와 검증자만에 한정된다. 따라서, 검증자는, 특정한 로그인명과 그것에 대응하는 패스워드를 제시하는 것이 가능한 사람을, 그 로그 인명으로 등록을 행한 증명자라고 판단한다.

즉, 패스워드 인증은, 검증자와 증명자만이 아는 지식을, 증명자가 검증자에게 직접 제시함으로써, 인증을 행하는 방식이다.

따라서, 인증 시에 패스워드가 누설하기 쉽다고 하는 결점을 갖지만, 로그인명과 패스워드는, 사람(증명자)이 직접 기억 가능하고, 인증을 위한 특별한 장치는 필요로 되지 않는다고 하는 이점을 갖고 있고, 이 때문에, 패스워드 인증은, 널리 이용되고 있다.

패스워드 인증에는, 검증자와 증명자가 동일한 정보를 갖기 때문에, 검증자와 증명자의 역할을 각각 교대시키는 것이 가능하다. 이하, 이러한 인증 방법을, 쌍방향성의 인증이라 칭한다. 단, 패스워드 인증에서는, 이 쌍방향성의 성질은, 일반적으로 사용되지 않는다.

(공통 키 인증)

다음으로, 공통 키 인증에 대하여 설명한다.

또한, 여기서는, 공통 키 암호를 사용하는 「Challenge amp; Response 인증」을, 공통 키 인증이라 칭한다.

공통 키 암호는, 대칭 암호라고도 칭해지고, 데이터를 암호화할 때에 이용하는 암호키와, 복호할 때에 이용하는 암호키가 동일하다고 하는 성질(또는, 상이한 암호키인 경우라도, 한쪽의 암호키로부터 다른 쪽의 암호키를 산출하는 일이 용이하다고 하는 성질)을 갖는 암호 알고리즘이다. 공통 키 암호로서는, 예를 들면, 아메리카 합중국 상무부 표준국에 의해 채용된 DES(Data Encryption Standard), 및, Triple DES, 및, NTT(일본 전신 전화(株)(상호))에 의해 개발된 FEAL(Fast Data Encipherment Algorithm) 등이 알려져 있다.

공통 키 인증은, 인증의 검증자와 증명자의 각각이, 동일한 공통 키 암호의 암호키 K_n을 갖는 경우, 그 암호키 K_n을, 암호키 K_n을 갖는 2자 이외에 누설시키는 일없이, 증명자가 암호키 K_n을 갖는 것을 검증자가 확인하는 방법이다.

공통 키 인증의 기본적인 구체예에 대하여 설명한다.

처음에, 검증자는, 난수 r을 발생시켜서 증명자에게 보낸다(이하, 이 처리를, Challenge라고도 기술한다).

증명자는, 이 난수 r을, 암호키 K_n로 암호화하고, 값 R=E(K_n, r)(E(K_n, r)는, 키 K_n을 이용하여, 난수 r을 암호화하는 것을 의미한다)를 연산하여, 검증자에게 되돌려 보낸다(이하, 이 처리를, Response라고도 기술한다).

검증자는, 값 R을, 암호키 K_n로 복호하여, 원래의 난수 r과 비교하여, 암호키 K_n과 원래의 난수 r이 일치하고 있는 경우, 증명자가 암호키 K_n을 갖고 있다고 판정한다.

따라서, 특정한 암호키 K_n을 갖는 사람이, 검증자 이외에 1명의 증명자 만이라고 되면, 암호키 K_n에 의해서, 그 증명자의 인증이 가능하게 된다.

이러한 공통 키 인증은, 예를 들면 ISO(International Organization for Standardization)/IEC(International Electro technical Commission) 9798-2에 표 준적인 것이 통합되어 있다. 공통 키 인증에 있어서는, 검증자와 증명자는 동일한 정보를 갖기 때문에, 공통 키 인증은, 쌍방향성의 인증 방법이다.

상술한 버스 워드 인증에 있어서는, 검증자와 증명자만의 비밀인 패스워드가 직접 비교되어, 상술한 바와 같이, 인증시에 패스워드가 누설하기 쉽다고 하는 결점을 갖고 있다. 이것에 대하여, 공통 키 인증에 있어서는, 상술한 바와 같이, 공통 키 암호의 암호키가 Challenge amp; Response 인증으로 사용되기 때문에, 암호키는, 외부에 누설되기 어려운 이점을 갖고 있다. 따라서, 공통 키 인증은, 패스워드 인증에 비교하여, 안전성의 점에서 우수하다.

단, 공통 키 인증에 있어서는, 사람이, Challenge amp; Response 인증에 필요한 계산을 행하는 것은 곤란하기 때문에, 통상, IC(IntegRated Circuit) 카드라 불리우는 특별한 장치에, 암호키를 기억시키고 있다. 또한, 이하, 이 공통 키 암호의 암호키를 기억하는 IC 카드를, 후술하는 공개키 암호의 키를 기억하는 IC 카드와 구별하기 위해서, 적절하게 CKC-IC 카드라 기술한다.

CKC-IC 카드는, 그 내부에서, 공통 키 인증에 필요한 계산을 행하는 기능을 갖고 있다. 그 때문에, CKC-IC 카드에 의해 공통 키 인증이 행하여지는 한, 암호키가 외부에 누설될 가능성은 적다. 그러나, CKC-IC 카드가, 물리적, 또는, 논리적으로 해석되어, 암호키가 누설될 가능성이 있고, 또한, CKC-IC 카드 자체가 도용될 가능성도 있다.

(공개키 인증)

다음으로, 공개키 인증에 대하여 설명한다.

또한, 여기서는, 공개키 암호를 사용하는 Challenge amp; Response 인증을, 공개키 인증이라 칭한다.

공개키 암호는, 비대칭 암호라고도 칭해지고, 데이터를 암호화할 때에 이용하는 암호키(이하, 적절하게 공개키라고 칭한다)와, 복호할 때에 이용하는 암호키(이하, 적절하게 비밀키라고 칭한다)가 다르고, 또한, 한쪽의 암호키로부터 다른 쪽의 암호키를 산출하는 (공개키로부터 비밀키를 산출하는, 또는, 비밀키로부터 공개키를 산출하는) 것이 매우 곤란하다고 하는 성질을 갖는 암호 알고리즘이다.

공개키 인증은, 증명자가, 비밀키 S_k를 갖고 검증자가, 비밀키 S_k와 쌍을 이루는 공개키 P_k를 갖는 경우, 검증자는, 증명자가 비밀키 S_k를 소유하는 것을, 비밀키 S_k 자체의 지식 없이 확인하는 것이 가능한 방법이다.

공개키 인증의 기본적인 방법의 구체예에 대하여 설명한다.

처음에, 검증자는, 난수 r을 생성하여, 그것을 공개키 P_k로 암호화하고, 값 R=E(P_k, r) (E(P_k, r)는, 공개키 P_k를 이용하여, r을 암호화하는 것을 의미함)를 연산하여, 증명자에게 보낸다(Challenge).

증명자는, 값 R의 복호 r'=D(S_k, R) (D(S_k, R)는, 비밀키 S_k를 이용하여, 값 R을 복호하는 것을 의미한다)을 연산하여, 검증자에게 되돌려준다(Response).

검증자는, 난수 r과, 값 R의 복호 r'를 비교하여, 난수 r과, 이들이 일치하는 경우, 증명자가 비밀키 S_k를 갖고 있다고 판정한다.

따라서, 특정한 비밀키 S_k를 갖는 사람이, 1명의 증명자가 되면, 검증자는, 상술한 수순에 의해서, 그 증명자의 인증을 행하는 것이 가능하게 된다.

공개키 암호에 대해서는, 예를 들면, IEEE(The Institute of Electrical and Electronic, Inc) -P1363에 있어서, 표준 방법이 통합되어 있다.

또한, 공개키 인증은, 예를 들면, ISO/IEC9798-3에 있어서, 표준 방법이 통합되어 있다.

공개키 인증은, 후술하는 바와 같이(후술하는 공개키 인증 기반에 의해 설명한 바와 같이), 검증자가 불특정 다수가 될 수 있다고 하는 특징을 갖고 있다.

또한, 공개키 인증은, 검증자와 증명자의 각각이 갖는 정보가 다르고, 또한, 상호의 입장을 바꾸는 것은 할 수 없기 때문에, 쌍방향을 갖는 인증이 아니다. 이하, 이러한 인증 방법을, 쌍방향성의 인증에 대하여, 단방향성의 인증이라 칭한다.

공개키 인증은, 공통 키 인증과 같이, 증명자가 갖는 비밀키가 암호학적으로 안전하게 유지된다. 따라서, 공개키 인증도, 안전성의 점에 대해서는, 패스워드 인증보다도 우수하다.

단, 공개키 인증에 있어서는, 공통 키 인증과 같이, 사람이, Challenge amp; Response 인증에 필요한 계산을 행하는 것은 곤란하기 때문에, 통상, IC 카드라 불리우는 특별한 장치에, 공개키 암호의 키를 기억시키고 있다. 또한, 이하, 공개키 암호의 키를 기억하는 IC 카드를, 상술한 CKC-IC 카드(공통 키 암호의 키를 기억하는 IC 카드)와 구별하기 위해서, 적절하게 PKC-IC 카드라고 기술한다.

PKC-IC 카드는, CKC-IC 카드와 같이, 그 내부에서, 공개키 인증에 필요한 계산을 행하는 기능을 갖고 있다. 그 때문에, PKC-IC 카드에 의해 공개키 인증이 행하여지는 한, 암호키가 외부에 누설될 가능성은 적다. 그러나, PKC-IC 카드가, 물리적, 또는, 논리적으로 해석되어, 키가 누설될 가능성이 있다. 또한, PKC-IC 카드 자체가, 도용될 가능성도 있다.

상술한 바와 같은 인증 방법에 있어서, 다수의 증명자의 인증을 효율적으로 안전하게 행하기 위해서, 인증에 필요한 정보가 미리 배치되고, 또한, 관리되는 구조가 필요하다. 이러한 구조를, 이하, 인증 기반이라 칭한다.

또한, 이하, 인증 기반에 의해 특정되는 사람을, 사용자로, 인증 기반을 관리하는 사람을, 관리자로, 인증 기반을 이용하여 사용자를 특정하여, 특정한 사용자에게 대하여, 서비스를 제공하는 사람을, 서비스 제공자로, 각각 칭한다.

종래, 인증 기반으로서, 개별 어카운트 방식, 범용 어카운트 방식, 및, 공개키 인증 기반 등이 알려져 있다.

그러나, 이들의 인증 기반, 즉, 개별 어카운트 방식, 범용 어카운트 방식, 및, 공개키 인증 기반의 각각은, 이하와 같은 과제를 갖고 있다.

(개별 어카운트 방식의 과제)

처음으로, 개별 어카운트 방식의 개략, 및, 그 과제에 대하여 설명한다.

인증 기반의 중에서, 종래 가장 넓게 이용되어 온 것이, 개별 어카운트 방식이다. 개별 어카운트 방식에 있어서는, 서비스 제공자마다, 인증의 기반이 구축된다.

즉, 사용자는, 서비스 제공자로부터 서비스를 받기 전에, 그 서비스 제공자에게 대하여, 사용자의 특정이나 과금에 필요한 정보(예를 들면, 주소, 성명, 또는, 크레디트 카드 번호 등의 정보)를 등록하거나, 제공되는 서비스에 대한 지불을 먼저 끝낸 후에, 서비스 제공자와의 사이에서 이용하는 인증 방법을 정한다.

또한, 이하, 서비스 제공자와 사용자와의 사이에서 정해진 인증 방법과, 그 인증 방법에 의해 이용되는 각종 정보(인증에 근거하여 특정되는 서비스 제공자와 사용자에게 관한 정보)를, 어카운트라고 칭한다.

이 경우, 서비스 제공자는, 이 인증 기반의 관리자이고, 또한, 사용자의 인증에 대한 검증자이다.

인증 방법으로서는, 상술한 3개의 인증 방법(패스워드 인증, 공통 키 인증, 및, 공개키 인증)의 전부가 적용 가능하다. 예를 들면, JR 동일본(株)(상호)의 Suica(상표) 시스템에 있어서는, 인증 방법으로서 공통 키 인증을 이용하고 있다.

단, 패스워드 인증 이외의 방법을 적용하는 경우, 인증 정보를 기억하는 IC 카드 등을 필요로 하기 때문에, 인증 기반의 전개에 대한 비용이 비싸게 된다. 그 때문에, 통신 경유의 서비스 제공이 목적이 되는 경우, 일반적으로, 패스워드 인증이 이용된다.

개별 어카운트 방식에 있어서는, 서비스 제공자가 파악하고 있는 사용자와 패스워드, 공통 키, 또는, 공개키의 대응이 올바를 것(오인이나 누설이 없을 것)이, 사용자 인증의 성립 조건으로 되어있다.

개별 어카운트 방식은, 서비스 제공자가 독자의 대응으로 실현할 수 있기 때 문에 도입이 용이하다.

그러나, 개별 어카운트 방식은, 이하의 3개의 과제를 갖고 있다.

제1 과제는, 사용자는, 어카운트 작성을 위해, 자기 자신을 특정하는 정보를, 서비스 제공자마다 등록할 필요가 있는 것이다. 따라서, 사용자는, 등록에 시간이 걸림과 함께, 신용에 의문이 있는 서비스 제공자에게 대해서도, 크레디트 카드 번호와 같은 악용되기 쉬운 정보를 등록해야한다.

제2 과제는, 1명의 사용자가, 많은 서비스 제공자의 각각과의 사이에서 어카운트의 작성을 행한 경우, 다수의 어카운트의 관리(다수의 패스워드를 기억하는, 또는, 다수의 IC 카드를 보유하는 것 등의 관리)가, 그 사용자의 부담이 되는 것이다.

제3 과제는, 서비스 제공자가, 인증 정보나 개인 정보를 관리하기 위한 비용이 든다고 하는 것이다. 즉, 인증 정보나 개인 정보는, 계속적으로, 내용의 갱신이 필요로 된다. 특히, 크레디트 카드 번호, 패스워드, 또는, 암호키는, 외부에 누설되지 않도록 주의 깊게 취급될 필요가 있다.

(범용 어카운트 방식의 과제)

다음으로, 범용 어카운트 방식의 개략, 및 과제에 대하여 설명한다.

상술한 개별 어카운트 방식의 과제를 해결하기 위해서, 많은 서비스 제공자의 각각이, 1개의 범용 어카운트로 사용자의 인증을 행하는 방식, 즉, 범용 어카운트 방식이 제안되어 있다. 범용 어카운트 방식으로서, 예를 들면, Kerberos 시스템 RFC1510 등이 알려져 있다. Kerberos는, 아메리카 합중국의 메사츠세츄 공과 대학에 의해 행해진 프로젝트의 명칭이고, 그 규격은, RFC(Request For Comment)라 불리우는 규격서의 시리즈의 1510번으로서 공개되어 있다. 또한, RFC는, IETF(Internet Engineering Task Force)에 의해서 제공되어 있다.

범용 어카운트 방식에 있어서는, 서비스 제공자 이외의 것이 관리자(이하, 이러한 관리자를, 범용 어카운트 관리자라고 칭한다)가 된다.

서비스 제공자가 사용자를 특정하는 경우, 처음에, 범용 어카운트 관리자가 사용자를 인증하여, 서비스 제공자가 범용 어카운트 관리자를 인증한다.

그리고, 범용 어카운트 관리자는, 사용자를 인증한 결과(사용자의 특정)를 서비스 제공자에게 전한다.

이와 같이, 범용 어카운트 방식에 있어서는, 개별 어카운트 방식과는 달리, 서비스 제공자는 사용자의 인증의 검증자가 아니다.

그 때문에, 이하의 세가지가, 전제로 되어 있다.

즉, 첫번째로서, 서비스 제공자가 범용 어카운트 관리자를 인증할 수 있을 것, 두번째로서, 범용 어카운트 관리자가 신용할 수 있을 (통지하는 인증 결과가 올바를) 것, 세번째로서, 범용 어카운트 관리자가 사용자를 인증할 수 있을 것의 세가지이다.

범용 어카운트 방식에 있어서는, 사용자는, 범용 어카운트의 등록을 한번만 행하면 된다. 또한, 어카운트의 정보는, 범용 어카운트 관리자에 의해 일괄하여 관리된다. 따라서, 범용 어카운트 방식은, 상술한 개별 어카운트 방식의 과제를 해결할 수 있다.

그러나, 범용 어카운트 방식은, 상술한 개별 어카운트 방식의 과제와는 다른, 이하와 같은 2개의 과제를 갖고 있다.

즉, 제1 과제는, 1개의 인증 방법에 대한 중요성과, 그 인증 방법의 사용 빈도가 과대하게 되는 것이다. 그 결과, 패스워드나 키가 누설될 기회가 증가하고, 더구나 누설된 경우에 피해의 확대의 우려가 크다.

제2 과제는, 인증 시에 범용 어카운트 관리자와의 통신이 필요하게 되기 때문에, 그 통신을 위해 인증의 응답성이 악화되는 것이다.

(공개키 인증 기반의 과제)

다음으로, 공개키 인증 기반의 개략, 및 과제에 대하여 설명한다.

상술한 바와 같이, 패스워드 인증이나 공통 키 인증에 있어서는, 검증자와 증명자는 일대일의 관계이지만, 공개키 인증에 있어서는, 검증자는, 자신이 갖는 공개키로부터, 증명자가 갖는 비밀키를 추측하는 것이 매우 곤란하기 때문에, 누구나 인증의 검증자가 되는 것이 가능하다.

이러한 공개키 인증의 성질에, 사용자와 공개키의 대응 관계를 얻는 방법이 조합된 것이, 공개키 인증 기반이라 칭해지고 있다.

따라서, 공개키 인증 기반에 있어서는, 사용자와 공개키의 대응 관계가 얻어지기 때문에, 서비스 제공자 자신이 검증자가 되는 것이 가능해지고, 상술한 범용 어카운트 방식의 제2 과제를 해결하는 것이 가능하게 된다.

사용자와 공개키의 대응 관계는, 일반적으로는, 비밀키가 내장된 IC 카드를 사용자에게 배포한 관리자가 파악하고 있다고 생각된다. 또한, 이하, 그 관리자 를, 인증 센터라고 칭한다.

인증 센터는, 사용자와 공개키의 대응 관계를, 인증 센터에 조회하는 일없이 취득하는 것을 바라는 사람(검증자가 되고 싶은 것)에 대하여, 사용자와 공개키의 관계를 보증하는 증명서를 발행한다.

여기서는, 공개키와 사용자를 특정하는 정보(ID나 이름 등), 및, 그 유효 기한을 포함하는 전자 데이터에 대하여, 인증 센터가 전자 서명을 부가한 것을, 증명서라고 칭한다.

전자 서명은, 공개키 암호의 응용의 일종이다. 따라서, 전자 서명에 대하여, 상술한 공개키 암호에 대응시켜서 설명한다.

예를 들면, 인증 센터는, 전자 데이터 M을 기억하고 있는 경우, 인증 센터 자신이 기억하는 비밀키 S_k 를 이용하여, 서명 SG(M)=E(S_k, h(M))을 연산한다. 또한, 함수 h()는, 일방향성 함수라고 되어, 출력치로부터 입력치를 알아내는 것이 매우 곤란하다고 하는 성질을 갖는 함수가 된다. 예를 들면, 함수 h()로서, ISO/IEC10118, FIPS180-1등에 있어서의 MD5나 SHA-1이라 불리우는 함수가 적용 가능하다.

인증 센터는, 증명서로서, 데이터의 조(M, SG(M))의 조를, 검증자에게 보낸다.

검증자는, 인증 센터가 기억하는 비밀키 S_k 와 쌍을 이루는 공개키 P_k 를 기억하고 있는 경우, h(M)=D(P_k, SG(M))가 만족하는가 아닌가를 확인함으로써, 전자 데 이터 M이 개찬되어 있지 않는 것, 서명 SG(M)이, 비밀키 S_k 의 소유자(인증 센터)에 의해서 부가된 것을 확인한다. 또한, 이러한 검증자의 수속을, 이하, 전자 서명의 검증이라 칭한다.

이와 같이, 인증의 검증자는, 인증 센터에 의해 부가된 전자 서명의 검증을 행하여, 그 증명서에 의해, 사용자와 공개키의 관계를 취득한다.

전자 서명에 대해서는, 예를 들면, IEEE-P1363에 있어서, 표준 방법이 통합되어 있다.

검증자는, 인증 센터의 공개키를 정확하게 파악하고 있어, 그 전자 서명의 검증을 할 수 있으면, 증명서로부터, 사용자와 공개키의 관계를 얻을 수 있다.

인증의 기반이 대규모로 된 경우, 1개의 인증 센터가 모든 사용자와 공개키의 관계를 파악하는 것은 곤란하게 된다. 이러한 경우, 복수의 인증 센터의 사이에서 인증 센터의 계층 구조를 만든다. 검증자는, 각 인증 센터의 각각으로부터, 독립하여 증명서를 발행하여 받지만, 공개키에 대해서는, 루트 인증 센터라 불리우는 소수의 인증 센터가 갖는 공개키만을 파악함으로써, 모든 증명서의 검증을 행한다.

이와 같이, 공개키 인증 기반은, 다수의 사용자와 공개키의 대응을 얻는 것이 가능한 방식으로서, 예를 들면 ITU(International Telecommunication Union)-T의 X.509 권고에 규정되어 있다. 공개 인증 기반은, 사용자 인증을 위한 정보를 분산적으로 관리할 수 있기 때문에, 인터넷과 같은 사용자 관리가 집중적으로 행해 지고 있지 않은 환경에 적합한 인증의 방법이다.

그러나, 사용자와 공개키의 관계는, 예를 들면, 사용자가 IC 카드를 없애거나, 또는, 자격을 잃어버린 것과 같은 사정에 의해서, 시간에 따라 변화한다. 즉, 발행된 증명서의 실효가 발생한다. 그 때문 증명서를 이용한 공개키 인증은, 이하의 네가지가 전제로 되어 있다.

즉, 첫번째로서, 서비스 제공자가, 증명서 내의 인증 센터의 전자 서명(루트 인증 센터로부터 찾아낸 것도 포함)을 정확하게 검증할 수 있을 것, 두번째로서, 증명서(루트 인증 센터로부터 찾아내는 경우의 증명서도 포함)가, 실효한 것이 아닐 것, 세번째로서, 인증 센터가 신용할 수 있을 (증명서의 내용이 올바를) 것, 네번째로서, 인증 센터가 파악하고 있는 사용자와 공개키의 대응이 올바를 (오인이나 누설이 없을) 것의 네가지이다.

증명서의 실효 상황을 가장 잘 파악 가능한 사람은, 사용자에게 대하여 카드를 배포하고, 또한, 증명서를 발행한 인증 센터이다. 그 때문에, 검증자는, 최신의 실효 상황을 얻기 위해서, 증명서 검증을 행할 때에, 그것을 인증 센터에 조회하면 된다. 그와 같은 조회를 위한 통신 프로토콜은, RFC(Request For Comments) 2560의 OCSP로서 규정되어 있다. 그러나, 이 경우, 검증자는, 사용자의 인증 시에, 인증 센터에의 조회를 행할 필요가 있다. 즉, 범용 어카운트 방식의 제2 과제와 동일한 곤란이 발생한다.

이 때문에, 인증 센터가, 증명서 실효 리스트라 불리우는 데이터를, 증명서의 이용자(서비스 제공자 등)에 발행하여, 증명서의 이용자가, 그 증명서를 이용할 때에, 증명서 실효 리스트와의 대조에 의해서 실효된 증명서의 사용을 정지하는 방법이 알려져 있다. 증명서 실효 리스트에 대해서는, 예를 들면, ITU-T의 X.509 권고에 규정되어 있다. 단, 분산적인 환경의 어디에서 증명서가 사용될까의 예상은 곤란하기 때문에, 증명서의 실효가 있었다고 해도, 인증 센터의 측으로부터 그것을 증명서의 이용자에게 주지시키는 것은 곤란하고, 특히, 돌발적인 증명서의 실효에 대처하기 위해서는, 증명서의 이용자는, 관계하는 증명서 실효 리스트를 항상적으로 수집할 필요가 있다.

이상의 점으로부터, 공개키 인증 기반은, 이하의 2개의 과제를 갖고 있다.

즉, 제1 과제는, 범용 어카운트 방식과 동일하게, 1개의 인증 방법의 중요성이 과도하게 높아지는 것이다.

제2 과제는, 실효 정보의 취급이 인증의 비용을 높이는, 또는, 응답성을 저하시키는 것이다. 이것은, 인증의 신뢰도를 확보하기 위해서, 검증자(예를 들면, 서비스 제공자)가, 관계되는 증명서 실효 리스트를 수집하여, 실효인가 아닌가의 검증을 가능하게 하는, 또는, OCSP에 의한 실효 상황 조회를 행할 필요가 있기 때문이다.

이와 같이, 개별 어카운트 방식, 범용 어카운트 방식, 및, 공개키 인증 기반의 각각은, 특유한 과제를 갖고 있다.

즉, 개별 어카운트 방식은, 상술한 3개의 과제를 갖고 있기 때문에, 대규모의 인증 기반으로서의 전개가 곤란하다.

범용 어카운트 방식은, 상술한 바와 같이, 다용도로 쓸 수 있기 때문에, 인 증 기반으로서 전개하는 것은 용이하게 되지만, 서비스 제공자는, 사용자 인증의 직접의 검증자가 아니기 때문에, 인증의 응답성이 저하한다고 하는 과제를 갖고 있다. 이 과제는, 특히, 빈번하게 인증이 행하여지는 상황에서 문제가 된다.

공개키 인증 기반은, 상술한 바와 같이, 검증자가, 인증의 신뢰성을 확보하기 위해서, 인증에 관계하는 증명서의 실효 상태를 수집하는, 또는, 인증 시에 인증 센터에의 조회를 행하기 때문에, 인증의 비용, 또는, 응답성이 악화한다고 하는 과제를 갖고 있다. 이 과제도, 특히, 빈번하게 인증이 행하여지는 것 같은 상황에서 문제가 된다.

발명의 상세한 설명

본 발명은, 이러한 상황을 감안하여 이루어진 것으로, 서비스 제공자가, 사용자를 인증하는 경우에, 그 인증의 효율과 안전성을 높일 수 있도록 하는 것이다.

본 발명의 제1 정보 처리 시스템은, 제1 정보 처리 장치가, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키를 생성하고, 생성한 제1 암호키를 제2 정보 처리 장치로 송부함과 함께, 생성한 제2 암호키를 제3 정보 처리 장치로 송부하고, 제2 정보 처리 장치는, 제1 정보 처리 장치에 의해 송부된 제1 암호키를 수취하고, 또한, 기억하고, 제3 정보 처리 장치는, 제1 정보 처리 장치에 의해 송부된 제2 암호키를 수취하고, 또한, 기억하고, 제2 정보 처리 장치는, 기억된 제1 암호키, 및, 제3 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 그 인증 방법에 기초하여, 제3 정보 처리 장치를 인증하는 것을 특징으로 한다.

인증 방법은, 공통 키 인증이고, 제1 암호키와 제2 암호키는 동일한 암호키인 것으로 할 수 있다.

인증 방법은, 공개키 인증이고, 제1 암호키와 제2 암호키는 서로 다른 암호키인 것으로 할 수 있다.

본 발명의 제1 정보 처리 시스템의 정보 처리 방법은, 제1 정보 처리 장치가, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키를 생성하고, 생성한 제1 암호키를 제2 정보 처리 장치로 송부함과 함께, 생성한 제2 암호키를 제3 정보 처리 장치로 송부하고, 제2 정보 처리 장치는, 제1 정보 처리 장치에 의해 송부된 제1 암호키를 수취하고, 또한, 기억하고, 제3 정보 처리 장치는, 제1 정보 처리 장치에 의해 송부된 제2 암호키를 수취하고, 또한, 기억하고, 제2 정보 처리 장치는, 기억된 제1 암호키, 및, 제3 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 그 인증 방법에 기초하여, 제3 정보 처리 장치를 인증하는 것을 특징으로 한다.

본 발명의 제1 정보 처리 시스템 및 방법에 있어서는, 제1 정보 처리 장치에 의해, 소정의 인증 방법에서 이용 가능한, 제1 암호키와, 그것과 쌍을 이루는 제2 암호키가 생성되어, 제1 암호키가 제2 정보 처리 장치로 송부됨과 함께, 제2 암호키가 제3 정보 처리 장치로 송부된다. 그리고, 제2 정보 처리 장치에 의해, 제2 정보 처리 장치에 의해 기억된 제1 암호키, 및, 제3 정보 처리 장치에 의해 기억된 제2 암호키가 이용되어, 인증 방법에 기초하여, 제3 정보 처리 장치가 인증된다.

본 발명의 제1 정보 처리 장치는, 다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키를 생성하는 생성 수단과, 생성 수단에 의해 생성된 제1 암호키를 다른 제1 정보 처리 장치로 송부함과 함께, 생성 수단에 의해 생성된 제2 암호키를 다른 제2 정보 처리 장치로 송부하는 송부 수단을 포함하는 것을 특징으로 한다.

인증 방법은, 공통 키 인증이고, 생성 수단에 의해 생성되는 제1 암호키와 제2 암호키는 동일한 암호키인 것으로 할 수 있다.

인증 방법은, 공개키 인증이고, 생성 수단에 의해 생성되는 제1 암호키와 제2 암호키는 서로 다른 암호키인 것으로 할 수 있다.

다른 제2 정보 처리 장치에, 인증을 위한 정보가 입력될지, 또는, 인증을 위해 이용되는 소정의 장치가 접속된 경우, 그 정보를 입력한 사용자, 또는, 접속된 장치를 특정하는 특정 수단을 또한 설치하고, 생성 수단은, 특정 수단에 의해 다른 제2 정보 처리 장치에 정보를 입력한 사용자, 또는, 다른 제2 정보 처리 장치에 접속된 장치가 특정된 경우, 제1 및 제2 암호키를 생성하도록 할 수 있다.

특정 수단은, SSL(Secure Socket Layer), 또는, TLS(Transport Layer Security)를 사용하여, 다른 제2 정보 처리 장치에 정보를 입력한 사용자, 또는, 다른 제2 정보 처리 장치에 접속된 장치를 특정하도록 할 수 있다.

생성 수단에 의해 제1 및 제2 암호키가 생성된 경우, 송부 수단에 의해 제1 암호키가 송부되는 상대인 다른 제1 정보 처리 장치가, 제1 및 제2 키를 이용하여 인증하는 다른 제2 정보 처리 장치에 대하여 제공하는 서비스의 댓가를 확정하여, 특정 수단에 의해 특정된 다른 제2 정보 처리 장치에 정보를 입력한 사용자, 또는, 특정 수단에 의해 특정된 다른 제2 정보 처리 장치에 접속된 장치에 의해서 특정되는 사용자에게 대하여, 서비스의 대가의 과금을 행하는 과금 수단을 또한 설치하도록 할 수 있다.

과금 수단은, 다른 제2 정보 처리 장치에 대하여, 서비스에 대한 댓가와 함께, 또한, 생성 수단에 의해 생성된 제1 및 제2 암호키에 대한 댓가의 과금을 행하도록 할 수 있다.

본 발명의 제1 정보 처리 장치의 정보 처리 방법은, 다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키를 생성하는 생성 단계와, 생성 단계의 처리에 의해 생성된 제1 암호키를 다른 제1 정보 처리 장치로 송부함과 함께, 생성 단계의 처리에 의해 생성된 제2 암호키를 다른 제2 정보 처리 장치로 송부하는 송부 단계를 포함하는 것을 특징으로 한다.

본 발명의 제1 기록 매체의 프로그램은, 다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처

리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키를 생성하는 생성 단계와, 생성 단계의 처리에 의해 생성된 제1 암호키를 다른 제1 정보 처리 장치로 송부함과 함께, 생성 단계의 처리에 의해 생성된 제2 암호키를 다른 제2 정보 처리 장치로 송부하는 송부 단계를 포함하는 것을 특징으로 한다.

본 발명의 제1 프로그램은, 다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키를 생성하는 생성 단계와, 생성 단계의 처리에 의해 생성된 제1 암호키를 다른 제1 정보 처리 장치로 송부함과 함께, 생성 단계의 처리에 의해 생성된 제2 암호키를 다른 제2 정보 처리 장치로 송부하는 송부 단계를 컴퓨터에 실행시키는 것을 특징으로 한다.

본 발명의 제1 정보 처리 장치 및 방법, 제1 기록 매체, 및, 제1 프로그램에 있어서는, 다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키가 생성되고, 생성된 제1 암호키가 다른 제1 정보 처리 장치로 송부됨과 함께, 생성된 제2 암호키가 다른 제2 정보 처리 장치로 송부된다.

본 발명의 제2 정보 처리 장치는, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 제1 암호키를 수취하는 수취 수단과, 수취 수단에 의해 수취된 제1 암호키를 기억하는 기억 수단과, 기억 수단에 의해 기억된 제1 암호키, 및, 다른 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 그 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 인증 수단을 포함하는 것을 특징으로 한다.

인증 방법은, 공통 키 인증이고, 제1 암호키와 제2 암호키는 동일한 암호키인 것으로 할 수 있다.

인증 방법은, 공개키 인증이고, 제1 암호키와 제2 암호키는 서로 다른 암호 키인 것으로 할 수 있다.

본 발명의 제2 정보 처리 장치의 정보 처리 방법은, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 제1 암호키를 수취하는 수취 단계와, 수취 단계의 처리에 의해 수취된 제1 암호키를 기억하는 기억 단계와, 기억 단계의 처리에 의해 기억된 제1 암호키, 및, 다른 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 그 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 인증 단계를 포함하는 것을 특징으로 한다.

본 발명의 제2 기록 매체의 프로그램은, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 제1 암호키를 수취하는 수취 단계와, 수취 단계의 처리에 의해 수취된 제1 암호키를 기억하는 기억 단계와, 기억 단계의 처리에 의해 기억된 제1 암호키, 및, 다른 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 그 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 인증 단계를 포함하는 것을 특징으로 한다.

본 발명의 제2 프로그램은, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 제1 암호키를 수취하는 수취 단계와, 수취 단계의 처리에 의해 수취된 제1 암호키를 기억하는 기억 단계와, 기억 단계의 처리에 의해 기억된 제1 암호키, 및, 다른 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 그 인 증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 인증 단계를 컴퓨터에 실행시키는 것을 특징으로 한다.

본 발명의 제2 정보 처리 장치 및 방법, 제2 기록 매체, 및, 제2 프로그램에 따르면, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 제1 암호키가 수취되고, 기억된다. 그리고, 기억된 제1 암호키, 및, 다른 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 그 인증 방법에 기초하여, 다른 제2 정보 처리 장치가 인증된다.

본 발명의 제3 정보 처리 장치는, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 제2 암호키를 수취하는 수취 수단과, 수취 수단에 의해 수취된 제2 암호키를 기억하는 기억 수단과, 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 그 인증 방법에 기초하여, 제3 정보 처리 장치 자신이 인증되는 경우, 기억 수단에 의해 기억된 제2 암호키를 이용하여, 소정의 응답을 다른 제2 정보 처리 장치로 송부하는 응답 수단을 포함하는 것을 특징으로 한다.

인증 방법은, 공통 키 인증이고, 제1 암호키와 제2 암호키는 동일한 암호키인 것으로 할 수 있다.

인증 방법은, 공개키 인증이고, 제1 암호키와 제2 암호키는 서로 다른 암호키인 것으로 할 수 있다.

다른 제2 정보 처리 장치에 의해 인증되기 위한 정보를 입력하는 입력 수단 을 또한 설치하도록 할 수 있다.

다른 제2 정보 처리 장치에 의해 인증되는 경우에 이용하는 소정의 장치를 접속하는 접속 수단을 또한 설치하도록 할 수 있다.

접속 수단에 접속되는 장치는, IC 카드이도록 하는 것을 할 수 있다.

기억 수단은, 내탬퍼성을 갖도록 할 수 있다.

본 발명의 제3 정보 처리 장치의 정보 처리 방법은, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 제2 암호키를 수취하는 수취 단계와, 수취 단계의 처리에 의해 수취된 제2 암호키의 기억을 제어하는 기억 제어 단계와, 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 그 인증 방법에 기초하여, 제3 정보 처리 장치가 인증되는 경우, 기억 제어 단계의 처리에 의해 기억이 제어된 제2 암호키를 이용하고, 소정의 응답을 다른 제2 정보 처리 장치로 송부하는 응답 단계를 포함하는 것을 특징으로 한다.

본 발명의 제3 기록 매체의 프로그램은, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 제2 암호키를 수취하는 수취 단계와, 수취 단계의 처리에 의해 수취된 제2 암호키의 기억을 제어하는 기억 제어 단계와, 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 그 인증 방법에 기초하여, 정보 처리 장치가 인증되는 경우, 기억 제어 단계의 처리에 의해 기억이 제어된 제2 암호키를 이용하여, 소정의 응답을 다른 제2 정보 처리 장치로 송부하는 응답 단계를 포함하는 것을 특징으로 한다.

본 발명의 제3 프로그램은, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 제2 암호키를 수취하는 수취 단계와, 수취 단계의 처리에 의해 수취된 제2 암호키의 기억을 제어하는 기억 제어 단계와, 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 그 인증 방법에 기초하여, 정보 처리 장치가 인증되는 경우, 기억 제어 단계의 처리에 의해 기억이 제어된 제2 암호키를 이용하여, 소정의 응답을 다른 제2 정보 처리 장치로 송부하는 응답 단계를 컴퓨터에 실행시키는 것을 특징으로 한다.

본 발명의 제3 정보 처리 장치 및 방법, 제3 기록 매체, 및, 제3 프로그램에 있어서는, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 제2 암호키가 수취되고, 기억된다. 그리고, 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 그 인증 방법에 기초하여, 제3 정보 처리 장치 자신이 인증되는 경우, 기억된 제2 암호키를 이용하여, 소정의 응답이 다른 제2 정보 처리 장치로 송부된다.

본 발명의 제2 정보 처리 시스템은, 제1 정보 처리 장치(상술한 제1 정보 처리 장치가 아니라, 후술하는 제4 정보 처리 장치에 상당한다)가, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보를 생성하여, 제2 정보 처리 장치(상술한 제2 정보 처리 장 치가 아니라, 후술하는 제6 정보 처리 장치에 상당한다)로 송부하고, 제2 정보 처리 장치가, 제1 정보 처리 장치로부터의 요구 정보를 수취하면, 제1 암호키와 제2 암호키의 각각을 생성하고, 생성한 제1 암호키를 제3 정보 처리 장치로 송부함과 함께, 생성한 제2 암호키를 기억하고, 제3 정보 처리 장치(상술한 제3 정보 처리 장치가 아니라, 후술하는 제5 정보 처리 장치에 상당한다)가, 상기 제2 정보 처리 장치에 의해 송부된 상기 제1 암호키를 수취하고, 또한, 기억하고, 제3 정보 처리 장치가, 기억된 제1 암호키, 및, 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 상술한 인증 방법에 기초하여, 제2 정보 처리 장치를 인증하는 것을 특징으로 한다.

인증 방법은, 공통 키 인증이고, 제1 암호키와 제2 암호키는 동일한 암호키인 것으로 할 수 있다.

인증 방법은, 공개키 인증이고, 제1 암호키와 제2 암호키는 서로 다른 암호키인 것으로 할 수 있다.

본 발명의 제2 정보 처리 시스템의 정보 처리 방법은, 제1 정보 처리 장치는, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보를 생성하여, 제2 정보 처리 장치로 송부하고, 제2 정보 처리 장치가, 제1 정보 처리 장치로부터의 요구 정보를 수취하면, 제1 암호키와 제2 암호키의 각각을 생성하고, 생성한 제1 암호키를 제3 정보 처리 장치로 송부함과 함께, 생성한 제2 암호키를 기억하고, 제3 정보 처리 장치가, 제2 정보 처리 장치에 의해 송부된 제1 암호키를 수취하고, 또한, 기억하고, 제3 정보 처리 장치가, 기억된 제1 암호키, 및, 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 인증 방법에 기초하여, 제2 정보 처리 장치를 인증하는 것을 특징으로 한다.

본 발명의 제2 정보 처리 시스템 및 방법에 있어서는, 제1 정보 처리 장치에 의해, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보가 생성되어, 제2 정보 처리 장치

로 송부된다. 그렇게 하면, 제2 정보 처리 장치에 의해, 제1 암호키와 제2 암호키의 각각이 생성되고, 생성된 제1 암호키가 제3 정보 처리 장치로 송부됨과 함께, 생성된 제2 암호키가 기억된다. 그리고, 제3 정보 처리 장치에 의해, 제2 정보 처리 장치에 의해 송부된 제1 암호키가 수취되고, 또한, 기억된다. 이 상태에서, 제3 정보 처리 장치에 의해, 기억된 제1 암호키, 및, 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 인증 방법에 기초하여, 제2 정보 처리 장치가 인증된다.

본 발명의 제4 정보 처리 장치는, 다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보를 생성하는 생성 수단과, 생성 수단에 의해 생성된 요구 정보를 다른 제2 정보 처리 장치로 송부하는 송부 수단을 포함하는 것을 특징으로 한다.

인증 방법은, 공개키 인증이고, 생성 수단에 의해 생성되는 제1 암호키와 제2 암호키는 서로 다른 암호키인 것으로 할 수 있다.

다른 제2 정보 처리 장치에, 인증을 위한 정보가 입력될지, 또는, 인증을 위해 이용되는 소정의 장치가 접속된 경우, 정보를 입력한 사용자, 또는, 접속된 장치를 특정하는 특정 수단을 또한 설치하고, 생성 수단은, 특정 수단에 의해, 다른 제2 정보 처리 장치에 정보를 입력한 사용자, 또는, 다른 제2 정보 처리 장치에 접속된 장치가 특정된 경우, 요구 정보를 생성하도록 할 수 있다.

특정 수단은, SSL(Secure Socket Layer), 또는, TLS(Transport Layer Security)를 사용하여, 다른 제2 정보 처리 장치에 정보를 입력한 사용자, 또는, 다른 제2 정보 처리 장치에 접속된 장치를 특정하도록 할 수 있다.

송부 수단에 의해 요구 정보가 다른 제2 정보 처리 장치로 송부된 경우, 다른 제1 정보 처리 장치가, 제1 키 및 제2 키를 이용하여 인증하는 다른 제2 정보 처리 장치에 대하여 제공하는 서비스의 댓가를 확정하여, 특정 수단에 의해 특정된 다른 제2 정보 처리 장치에 정보를 입력한 사용자, 또는, 특정 수단에 의해 특정된, 다른 제2 정보 처리 장치에 접속된 장치에 의해서 특정되는 사용자에게 대하여, 서비스의 댓가의 과금을 행하는 과금 수단을 또한 설치하도록 할 수 있다.

과금 수단은, 다른 제2 정보 처리 장치에 대하여, 서비스에 대한 댓가와 함께, 또한, 송부 수단으로부터 다른 제2 정보 처리 장치로 송부된 요구 정보를 받아, 다른 제2 정보 처리 장치가 생성한 제1 및 제2 암호키에 대한 댓가의 과금을 행하도록 할 수 있다.

본 발명의 제4 정보 처리 장치의 정보 처리 방법은, 다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보를 생성하는 생성 단계와, 생성 단계의 처리에 의해 생성된 요구 정보를 다른 제2 정보 처리 장치로 송부하는 송부 단계를 포함하는 것을 특징으로 한다.

본 발명의 제4 기록 매체의 프로그램은, 다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을, 다른 제2 정보 처리 장치에 대하여 요구하는 요구 정보를 생성하는 생성 단계를 포함하는 것을 특징으로 한다.

본 발명의 제4 프로그램은, 다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을, 다른 제2 정보 처리 장치에 대하여 요구하는 요구 정보를 생성하는 생성 단계와, 생성 단계의 처리에 의해 생성된 요구 정보를 다른 제2 정보 처리 장치로 송부하는 송부 단계를 포함하는 것을 특징으로 한다.

본 발명의 제4 정보 처리 장치 및 방법, 제4 기록 매체, 및 제4 프로그램에 있어서는, 다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보가 생성되고, 생성된 요구 정보가 다른 제2 정보 처리 장치로 송부된다.

본 발명의 제5 정보 처리 장치는, 다른 제1 정보 처리 장치의 요구에 의해, 다른 제2 처리 장치가, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키를 생성하고, 생성한 제1 암호키를 송부하여 온 경우, 제1 암호키를 수취하는 수취 수단과, 수취 수단에 의해 수취된 제1 암호키를 기억하는 기억 수단과, 기억 수단에 의해 기억된 제1 암호키, 및, 다른 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 인증 수단을 포함하는 것을 특징으로 한다.

인증 방법은, 공개키 인증이고, 제1 암호키와 제2 암호키는 서로 다른 암호키인 것으로 할 수 있다.

본 발명의 제5 정보 처리 장치의 정보 처리 방법은, 다른 제1 정보 처리 장치의 요구에 의해, 다른 제2 처리 장치가, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키를 생성하고, 생성된 제1 암호키를 송부하여 온 경우, 제1 암호키를 수취하는 수취 단계와, 수취 단계의 처리에 의해 수취된 제1 암호키를 기억하는 기억 단계와, 기억 단계의 처리에 의해 기억된 제1 암호키, 및, 다른 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 인증 단계를 포함하는 것을 특징으로 한다.

본 발명의 제5 기록 매체의 프로그램은, 정보 처리 장치를 제어하는 컴퓨터의 프로그램으로서, 다른 제1 정보 처리 장치의 요구에 기초하여, 다른 제2 처리 장치가 생성한, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 정보 처리 장치 자신에 의해 기억된 제1 암호키, 및, 다른 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 상술한 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 인증 단계를 포함하는 것을 특징으로 한다.

본 발명의 제5 프로그램은, 정보 처리 장치를 제어하는 컴퓨터의 프로그램으로서, 다른 제1 정보 처리 장치의 요구에 기초하여, 다른 제2 처리 장치가 생성한, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키 중의, 정보 처리 장치 자신에 의해 기억된 제1 암호키, 및, 다른 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 상술한 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 인증 단계를 포함하는 것을 특징으로 한다.

본 발명의 제5 정보 처리 장치 및 방법, 제5 기록 매체, 및, 제5 프로그램에 있어서는, 다른 제1 정보 처리 장치의 요구에 의해, 다른 제2 처리 장치가, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키를 생성하고, 생성한 제1 암호키가 송부되어 온 경우, 제1 암호키가, 제5 정보 처리 장치에 의해 수취되고, 기억된다. 그리고, 제5 정보 처리 장치에 의해 기억된 제1 암호키, 및, 다른 제2 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 상술한 인증 방법에 기초하여, 다른 제2 정보 처리 장치가 인증된다.

본 발명의 제6 정보 처리 장치는, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍이 되는 제2 암호키의 생성을 요구하는 요구 정보를 수취하는 수취 수단과, 수취 수단에 의해 수취된 요구 정보에 기초하여, 제1 암호키와 제2 암호키를 생성하는 키 생성 수단과, 키기 생성 수단에 의해 생성된 제1 암호키와 제2 암호키 중의, 제1 암호키를 다른 제2 정보 처리 장치로 송부하는 송부 수단과, 키 생성 수단에 의해 생성된 제1 암호키와 제2 암호키 중의, 제2 암호키를 기억하는 기억 수단과, 송부 수단에 의해 송부된 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 인증 방법에 기초하여, 자기 자신이 인증되는 경우, 기억 수단에 의해 기억된 제2 암호키를 이용하여, 소정의 응답을 생성하는 응답 생성 수단을 구비하며, 송부 수단은, 응답 생성 수단에 의해 생성된 응답을, 다른 제2 정보 처리 장치로 송부하는 것을 특징으로 한다.

인증 방법은, 공개키 인증이고, 제1 암호키와 제2 암호키는 서로 다른 암호키인 것으로 할 수 있다.

다른 제2 정보 처리 장치에 의해 인증되기 위한 정보를 입력하는 입력 수단을 또한 설치하도록 할 수 있다.

다른 제2 정보 처리 장치에 의해 인증되는 경우에 이용하는 소정의 장치를 접속하는 접속 수단을 또한 설치하도록 할 수 있다.

접속 수단에 접속되는 장치는, IC 카드이도록 할 수 있다.

기억 수단은, 내탬퍼성을 갖도록 할 수 있다.

본 발명의 제6 정보 처리 장치의 정보 처리 방법은, 다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호 키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보를 수취하는 수취 단계와, 수취 단계의 처리에 의해 수취된 요구 정보에 기초하여, 제1 암호키와 제2 암호키를 생성하는 키 생성 단계와, 키 생성 단계의 처리에 의해 생성된 제1 암호키와 제2 암호키 중의, 제1 암호키를 다른 제2 정보 처리 장치로 송부하는 키 송부 단계와, 키 생성 단계의 처리에 의해 생성된 제1 암호키와 제2 암호키 중의, 제2 암호키를 기억하는 기억 단계와, 키 송부 단계의 처리에 의해 송부된 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 인증 방법에 기초하여, 정보 처리 장치가 인증되는 경우, 기억 단계의 처리에 의해 기억된 제2 암호키를 이용하여, 소정의 응답을 생성하는 응답 생성 단계와, 응답 단계의 처리에 의해 생성된 응답을 다른 제2 정보 처리 장치로 송부하는 응답 송부 단계를 포함하는 것을 특징으로 한다.

본 발명의 제6 기록 매체의 프로그램은, 정보 처리 장치를 제어하는 컴퓨터의 프로그램으로서, 다른 제1 정보 처리 장치에서 정보 처리 장치로 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보에 기초하여, 다른 제2 정보 처리 장치로 송신되는 제1 암호키와, 정보 처리 장치에 기억되는 제2 암호키를 생성하는 키 생성 단계와, 송신된 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해,

인증 방법에 기초하여, 정보 처리 장치가 인증되는 경우, 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 소정의 응답을 생성하는 응답 생성 단계를 포함하는 것을 특징으로 한다.

본 발명의 제6 프로그램은, 정보 처리 장치를 제어하는 컴퓨터의 프로그램으로서, 다른 제1 정보 처리 장치에서 정보 처리 장치로 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보에 기초하여, 다른 제2 정보 처리 장치로 송신되는 제1 암호키와, 정보 처리 장치에 기억되는 제2 암호키를 생성하는 키 생성 단계와, 송신된 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 인증 방법에 기초하여, 정보 처리 장치가 인증되는 경우, 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 소정의 응답을 생성하는 응답 생성 단계를 포함하는 것을 특징으로 한다.

본 발명의 제6 정보 처리 장치 및 방법, 제6 기록 매체, 및 제6 프로그램에 있어서는, 다른 제1 정보 처리 장치에서 제6 정보 처리 장치로 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보에 기초하여, 다른 제2 정보 처리 장치로 송신되는 제1 암호키와, 정보 처리 장치에 기억되는 제2 암호키가 제6 정보 처리 장치에 의해 생성된다. 그 후, 송신된 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 상술한 인증 방법에 기초하여, 제6 정보 처리 장치가 인증되는 경우, 제6 정보 처리 장치에 의해 기억된 제2 암호키를 이용하여, 소정의 응답이 생성되어, 다른 제2 정보 처리 장치로 송신된다.

도면의 간단한 설명

도 1은 본 발명이 적용되는 인증키 할당 시스템에 의해 지원되는 비지니스 모델의 제1 예에 대하여 설명하는 도면.

도 2는 본 발명이 적용되는 인증키 할당 시스템에 의해 지원되는 비지니스 모델의 제2 예에 대하여 설명하는 도면.

도 3은 본 발명이 적용되는 인증키 할당 시스템에 의해 지원되는 비지니스 모델의 제3 예에 대하여 설명하는 도면.

도 4는 본 발명이 적용되는 인증키 할당 시스템의 구성예를 도시하는 블록도.

도 5는 키 할당표의 예를 도시하는 도면.

도 6은 서비스 제공자 키표의 예를 도시하는 도면.

도 7은 키 기억 장치 키표의 예를 도시하는 도면.

도 8은 키 할당자 어카운트 정보의 예를 도시하는 도면.

도 9는 인증 정보표의 예를 도시하는 도면.

도 10은 서비스 제공자 고유 정보의 예를 도시하는 도면.

도 11은 증명키표의 예를 도시하는 도면.

도 12는 서비스 정보표의 예를 도시하는 도면.

도 13은 키 기억 장치 고유 정보의 예를 도시하는 도면.

도 14는 사용자 카운트 정보의 예를 도시하는 도면.

도 15는 도 14의 인증키 할당 시스템의 사용자 단말기의 구성예를 도시하는 블록도.

도 16은 도 14의 인증키 할당 시스템의 키 기억 장치의 구성예를 도시하는 블록도.

도 17은 도 14의 인증키 할당 시스템의 IC 카드의 구성예를 도시하는 블록도.

도 18은 도 14의 인증키 할당 시스템의 키 할당자 단말기의 구성예를 도시하는 블록도.

도 19는 도 14의 인증키 할당 시스템의 서비스 제공자 단말기의 구성예를 도시하는 블록도.

도 20은 도 14의 인증키 할당 시스템의 범용 어카운트 관리자 단말기의 구성예를 도시하는 블록도.

도 21은 어카운트 관리표의 예를 도시하는 도면.

도 22는 어카운트 관리자 고유키가 예를 도시하는 도면.

도 23은 본 발명이 적용되는 인증키 시스템의 처리의 예에 대하여 설명하는 흐름도.

도 24는 도 15의 사용자 단말기, 도 16의 키 기억 장치, 및, 도 17의 IC 카드로 구성되는 사용자 장치의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 25는 도 18의 키 할당자 단말기의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 26은 도 19의 서비스 제공자 단말기의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 27은 도 15의 사용자 단말기, 도 16의 키 기억 장치, 및, 도 17의 IC 카 드로 구성되는 사용자 장치, 도 18의 키 할당자 단말기, 및, 도 19의 서비스 제공자 단말기의 서비스 선택/키 할당의 처리의 관계를 도시하는 애로우 차트.

도 28은 키 할당 의뢰서의 예를 도시하는 도면.

도 29는 키 할당 보고서의 예를 도시하는 도면.

도 30은 도 15의 사용자 단말기, 도 16의 키 기억 장치, 및, 도 17의 IC 카드로 구성되는 사용자 장치의 키 사용/서비스 제공 처리의 예에 대하여 설명하는 흐름도.

도 31은 도 19의 서비스 제공자 단말기의 키 사용/서비스 제공 처리의 예에 대하여 설명하는 흐름도.

도 32는 도 29의 사용자 장치의 키 사용/서비스 제공 처리의 목적별 인증의 검증 처리와, 도 30의 서비스 제공자 단말기의 키 사용/서비스 제공 처리의 목적별 인증의 응답 처리와의 관계의 예를 도시하는 애로우 차트.

도 33은 도 29의 사용자 장치의 키 사용/서비스 제공 처리의 목적별 인증의 검증 처리와, 도 30의 서비스 제공자 단말기의 키 사용/서비스 제공 처리의 목적별 인증의 응답 처리와의 관계의 다른 예를 도시하는 애로우 차트.

도 34는 도 29의 사용자 장치의 키 사용/서비스 제공 처리의 서비스 이용 처리와, 도 30의 서비스 제공자 단말기의 키 사용/서비스 제공 처리의 서비스 제공 처리와의 관계의 예를 도시하는 애로우 차트.

도 35는 도 29의 사용자 장치의 키 사용/서비스 제공 처리의 서비스 이용 처리와, 도 30의 서비스 제공자 단말기의 키 사용/서비스 제공 처리의 서비스 제공 처리와의 관계의 다른 예를 도시하는 애로우 차트.

도 36은 서비스 요구서의 예를 도시하는 도면.

도 37은 도 15의 사용자 단말기, 도 16의 키 기억 장치, 및, 도 17의 IC 카드로 구성되는 사용자 장치의 키 삭제 처리의 예에 대하여 설명하는 흐름도.

도 38은 도 18의 키 할당자 단말기의 키 삭제 처리의 예에 대하여 설명하는 흐름도.

도 39는 도 19의 서비스 제공자 단말기의 키 삭제 처리의 예에 대하여 설명하는 흐름도.

도 40은 도 18의 키 할당자 단말기의 키 사용 정지 처리의 예에 대하여 설명하는 흐름도.

도 41은 도 19의 서비스 제공자 단말기의 키 사용 정지 처리의 예에 대하여 설명하는 흐름도.

도 42는 키 사용 정지 요구서의 예를 도시하는 도면.

도 43은 키 사용 정지 요구서의 다른 예를 도시하는 도면.

도 44는 본 발명이 적용되는 인증키 할당 시스템의 구성의 다른 예를 도시하는 블록도.

도 45는 도 43의 인증키 할당 시스템의 인증 센터 단말기의 구성예를 도시하는 블록도.

도 46은 키 할당표의 예를 도시하는 도면.

도 47은 서비스 제공자 키표의 예를 도시하는 도면.

도 48은 키 기억 장치 키표의 예를 도시하는 도면.

도 49는 키 할당자 PKI 정보의 예를 도시하는 도면.

도 50은 CA 공개키 정보의 예를 도시하는 도면.

도 51은 키 할당 의뢰서의 예를 도시하는 도면.

도 52는 키 할당 보고서의 예를 도시하는 도면.

도 53은 인증 정보표의 예를 도시하는 도면.

도 54는 서비스 제공자 고유 정보의 예를 도시하는 도면.

도 55는 실효키표의 예를 도시하는 도면.

도 56은 서비스 제공자 PKI 정보의 예를 도시하는 도면.

도 57은 키 공유 파라미터의 예를 도시하는 도면.

도 58은 CA 공개키 정보의 예를 도시하는 도면.

도 59는 증명키표의 예를 도시하는 도면.

도 60은 인증 정보표의 예를 도시하는 도면.

도 61은 키 기억 장치 고유 정보의 예를 도시하는 도면.

도 62는 사용자 PKI 정보의 예를 도시하는 도면.

도 63은 CA 공개키 정보의 예를 도시하는 도면.

도 64는 증명서표의 예를 도시하는 도면.

도 65는 CA 키 정보의 예를 도시하는 도면.

도 66은 증명서의 예를 도시하는 도면.

도 67은 도 43의 인증키 할당 시스템의 사용자 장치와 키 할당자 단말기와의 서비스 선택/키 할당의 처리의 중의, 사용자 장치의 사용자 인식 응답 처리와, 키 할당자 단말기의 키 기억 장치의 사용자 인증 처리와의 관계를 도시하는 애로우 차트.

도 68은 도 43의 인증키 할당 시스템의 사용자 장치의 키 사용/서비스 제공 처리의 예에 대하여 설명하는 흐름도.

도 69는 도 43의 인증키 할당 시스템의 서비스 제공자 단말기의 키 사용/서비스 제공 처리의 예에 대하여 설명하는 흐름도.

도 70은 도 67의 사용자 장치의 키 사용/서비스 제공 처리의 목적별 인증의 검증 처리와, 도 68의 서비스 제공자 단말기의 키 사용/서비스 제공 처리의 목적별 인증의 응답 처리와의 관계의 예를 도시하는 애로우 차트.

도 71은 도 67의 사용자 장치의 키 사용/서비스 제공 처리의 목적별 인증의 검증 처리와, 도 68의 서비스 제공자 단

말기의 키 사용/서비스 제공 처리의 목적별 인증의 응답 처리와의 관계의 다른 예를 도시하는 애로우 차트.

도 72는 본 발명이 적용되는 인증키 할당 시스템의 구성의 다른 예를 도시하는 블록도.

도 73은 키 할당표의 예를 도시하는 도면.

도 74는 서비스 제공자 키표의 예를 도시하는 도면.

도 75는 키 기억 장치 키표의 예를 도시하는 도면.

도 76은 키 할당자 어카운트 정보의 예를 도시하는 도면.

도 77은 CA 공개키 정보의 예를 도시하는 도면.

도 78은 권리증서의 예를 도시하는 도면.

도 79는 키 할당 의뢰서의 예를 도시하는 도면.

도 80은 키 할당 보고서의 예를 도시하는 도면.

도 81은 인증 정보표의 예를 도시하는 도면.

도 82는 서비스 제공자 고유 정보의 예를 도시하는 도면.

도 83은 실효키표의 예를 도시하는 도면.

도 84는 서비스 제공자 PKI 정보의 예를 도시하는 도면.

도 85는 키 공유 파라미터의 예를 도시하는 도면.

도 86은 CA 공개키 정보의 예를 도시하는 도면.

도 87은 증명키표의 예를 도시하는 도면.

도 88은 인증 정보표의 예를 도시하는 도면.

도 89는 키 기억 장치 고유 정보의 예를 도시하는 도면.

도 90은 사용자 카운트 정보의 예를 도시하는 도면.

도 91은 CA 공개키 정보의 예를 도시하는 도면.

도 92는 도 71의 인증키 할당 시스템의 사용자 장치의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 93은 도 71의 인증키 할당 시스템의 키 할당자 단말기의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 94는 도 71의 인증키 할당 시스템의 서비스 제공자 단말기의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 95는 도 71의 인증키 할당 시스템의 사용자 장치, 키 할당자 단말기, 및, 서비스 제공자 단말기의 서비스 선택/키 할당의 처리의 관계를 도시하는 애로우 차트.

도 96은 도 71의 인증키 할당 시스템의 사용자 장치의 키 사용/서비스 제공 처리의 예에 대하여 설명하는 흐름도.

도 97은 도 71의 인증키 할당 시스템의 서비스 제공자 단말기의 키 사용/서비스 제공 처리의 예에 대하여 설명하는 흐름도.

도 98은 키 할당표의 예를 도시하는 도면.

도 99는 서비스 제공자 키표의 예를 도시하는 도면.

도 100은 키 기억 장치 키표의 예를 도시하는 도면.

도 101은 키 할당자 PK 정보의 예를 도시하는 도면.

도 102는 CA 공개키 정보의 예를 도시하는 도면.

도 103은 권리증서의 예를 도시하는 도면.

도 104는 키 할당 의뢰서의 예를 도시하는 도면.

도 105는 서비스 제공자 고유 정보의 예를 도시하는 도면.

도 106은 실효키표의 예를 도시하는 도면.

도 107은 키 공유 파라미터의 예를 도시하는 도면.

도 108은 CA 공개키 정보의 예를 도시하는 도면.

도 109는 증명키표의 예를 도시하는 도면.

도 110은 인증 정보표의 예를 도시하는 도면.

도 111은 키 기억 장치 고유 정보의 예를 도시하는 도면.

도 112는 사용자 카운트 정보의 예를 도시하는 도면.

도 113은 CA 공개키 정보의 예를 도시하는 도면.

도 114는 도 98의 인증키 할당 시스템의 사용자 장치의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 115는 도 98의 인증키 할당 시스템의 키 할당자 단말기의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 116은 도 98의 인증키 할당 시스템의 서비스 제공자 단말기의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 117은 도 98의 인증키 할당 시스템의 사용자 장치, 키 할당자 단말기, 및, 서비스 제공자 단말기의 서비스 선택/키 할당의 처리의 관계를 도시하는 애로우 차트.

도 118은 키 기억 장치의 다른 구성예를 도시하는 블록도.

도 119는 키 할당표의 예를 도시하는 도면.

도 120은 키 기억 장치 PKI 정보의 예를 도시하는 도면.

도 121은 키 일시 기억표의 예를 도시하는 도면.

도 122는 인증용 키표의 예를 도시하는 도면.

도 123은 도 15의 사용자 단말기, 도 16 또는 도 118의 키 기억 장치, 및 도 17의 IC 카드로 구성되는 사용자 장치의 서비스 선택/키 할당 처리의 다른 예에 대하여 설명하는 흐름도.

도 124는 도 123의 흐름도에 대응하는 도 18의 키 할당자 단말기의 서비스 선택/키 할당 처리의 예에 대하여 설명하

는 흐름도.

도 125는 도 123의 흐름도에 대응하는 도 19의 서비스 제공자 단말기의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 126은 도 123 내지 도 125의 흐름도에 대응하는 애로우 차트로서, 도 15의 사용자 단말기, 도 16 또는 도 118의 키 기억 장치, 및, 도 17의 IC 카드로 구성되는 사용자 장치, 도 18의 키 할당자 단말기, 및, 도 19의 서비스 제공자 단말기의 서비스 선택/키 할당의 처리의 관계를 도시하는 애로우 차트.

도 127은 도 126의 애로우 차트로 도시되는, 단계 S524의 「신규키 요구 및 수취 처리」와, 단계 S506의 「신규키 생성 및 송부 처리」의 관계의 상세를 도시하는 애로우 차트.

도 128은 SSL. TLS가 이용되는 경우의 프로토콜 스택을 도시하는 도면.

도 129는 SSL. TLS가 이용되는 경우에 있어서의, 도 126의 애로우 차트로 도시되는, 단계 S522의 「키 기억 장치와 상호 인증 + 키 공유 처리」와, 단계 S504의 「키 할당자 단말기와 상호 인증 + 키 공유 처리」의 관계의 상세를 도시하는 애로우 차트.

도 130은 키 할당표의 예를 도시하는 도면.

도 131은 도 15의 사용자 단말기, 도 16 또는 도 118의 키 기억 장치, 및, 도 17의 IC 카드로 구성되는 사용자 장치의 서비스 선택/키 할당 처리의 또 다른 예에 대하여 설명하는 흐름도.

도 132는 도 131의 흐름도에 대응하는 도 18의 키 할당자 단말기의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 133은 도 131의 흐름도에 대응하는, 도 19의 서비스 제공자 단말기의 서비스 선택/키 할당 처리의 예에 대하여 설명하는 흐름도.

도 134는 도 131 내지 도 133의 흐름도에 대응하는 애로우 차트로서, 도 15의 사용자 단말기, 도 16 또는 도 118의 키 기억 장치, 및, 도 17의 IC 카드로 구성되는 사용자 장치, 도 18의 키 할당자 단말기, 및, 도 19의 서비스 제공자 단말기의 서비스 선택/키 할당의 처리의 관계를 도시하는 애로우 차트.

도 135는 도 134의 애로우 차트로 도시되는, 단계 S524의 「신규키 요구 및 수취 처리」와, 단계 S506의 「신규키 생성 및 송부 처리」의 관계의 상세를 도시하는 애로우 차트.

실시예

(인증키 할당 시스템에 의해 지원되는 비지니스 모델)

처음에, 본 발명이 적용되는 인증키 할당 시스템에 의해 지원되는 비지니스 모델에 대하여 설명한다.

또한, 이 예에 있어서는, Kerberos 인증키 할당 시스템 등의 범용 어카운트 방식, 또는, 공개키 인증 기반에 의해 사용자 User가 특정됨으로써, 그 사용자 User에 대한 과금이 가능하게 된다.

도 1은 범용 어카운트 방식의 존재를 상정한 경우의 비지니스 모델의 참가자를 도시하고 있다. 즉, 참가자는, 사용자 User, 서비스 제공자 SP, 키 할당자 KA, 및, 범용 어카운트 관리자 KDC가 된다. 사용자 User는, 범용 어카운트 관리자 KDC에 대하여 등록 완료되고, 키 할당자 KA는, 범용 어카운트에 의해서 사용자 User를 특정한다.

도 2는, 공개키 인증 기반의 존재를 상정한 경우의 비지니스 모델의 참가자를 도시하고 있다. 즉, 참가자는, 사용자 User, 서비스 제공자 SP, 키 할당자 KA, 및, 인증 센터 CA가 된다. 사용자 User, 서비스 제공자 SP, 및, 키 할당자 KA의 각각은 인증 센터 CA에 대하여 등록되고, 사용자 User, 서비스 제공자 SP, 및, 키 할당자 KA의 각각은, 공개키 인증 기반을 이용하여 상호의 전자 서명의 검증을 행한다.

도 3은, 공개키 인증 기반과 범용 어카운트 방식이 병용되는 경우의 비지니스 모델의 참가자를 도시하고 있다. 즉, 참가자는, 사용자 User, 서비스 제공자 SP, 키 할당자 KA, 인증 센터 CA, 및 범용 어카운트 관리자 KDC가 된다. 이 경우, 키 할당자 KA는, 범용 어카운트에 의해서 사용자 User를 특정하고, 또한, 서비스 제공자 SP의 전자 서명을 공개

키 인증 기반에 의해서 검증한다.

또한, 참가자의 수는, 특별히 한정되지 않지만, 도 1 내지 도 3의 어느 경우도, 이 예에 있어서는, 예를 들면, 키 할당자 KA는, 1개가 되고, 또한, 사용자 User와 서비스 제공자 SP의 각각은, 복수가 된다.

또한, 일반적으로, 공개키 인증 기반의 인증 센터나, Kerberos 인증키 할당 시스템의 관리자는, 복수가 될 수 있지만, 도 1 내지 도 3의 어느 경우도, 이 예에 있어서는, 예를 들면, 범용 어카운트 관리자 KDC와 인증 센터 CA의 각각은, 1개가 된다.

본 발명의 비지니스 모델에 있어서는, 처음에, 사용자 User와 서비스 제공자 SP가, 소정의 서비스 이용 계약을 맺고, 그 이후, 어느 일정 횟수나 일정 기간 등의 제한의 하에서, 특정한 서비스 제공자 SP가, 특정한 사용자 User를 인증하는 경우, 예를 들면, 사용자 User가, 서비스 제공자 SP가 제공하는 뉴스의 정기 구독이나, 정기 사이의 데이터베이스 검색 이용을 행하는 경우 등에, 서비스 제공자 SP가 사용자 User를 효율적으로 인증하는 것이 가능하게 된다.

즉, 빈번하게 인증을 행하는 2자(사용자 User와 서비스 제공자 SP)의 사이에, 범용 어카운트나 공개키 인증 기반과는 별도의 인증 방법을 제공한다. 이 인증은, 2자 사이에서 직접 행하는 것이 가능하기 때문에 효율적이다. 또한 이 인증 방법의 사용을 정지하여야 할 경우에도, 특정한 서비스 제공자 SP와 사용자 User의 사이에서만 사용되는 인증 방법이기 때문에, 무효화의 통지는 용이하다. 이에 의해, 상술한 범용 어카운트 방식의 제2 과제, 및, 공개키 인증 기반의 제2 과제를 해결하는 것이 가능하게 된다.

직접적으로 인증을 행하는 것은 개별 어카운트 방식이라도 가능하지만, 본 발명의 비지니스 모델에 있어서는, 새로운 인증 방법의 할당 시에만, 범용 어카운트 방식 또는 공개키 인증 기반을 이용하여, 사용자 User를 특정한다. 이에 의해, 개별 어카운트 방식에서 필요하던 등록의 수고가 줄면서 동시에, 사용자는 서비스 이용 시에 익명성을 유지할 수 있다.

또한, 새롭게 할당되는 인증 방법은, 공통 키 인증 또는 공개키 인증이 된 다. 사용자 User는, 공통 키 인증에 필요한 정보를, IC 카드에 유사한 기능을 갖는 장치에 기억한다. 이에 의해, 키 할당이나 선택, 및, 인증을 위한 계산의 자동화가 가능하게 된다. 따라서, 상술한 개별 어카운트 방식의 제1 및 제2 과제를 해결하는 것이 가능하게 된다.

또한, 이하, 이 IC 카드에 유사한 기능을 갖는 장치를, 키 기억 장치라고 칭한다. 또한, 이 예에 있어서는, 사용자 User에는, 키 할당자 KA에서 키 기억 장치가 배포되어 있는 것으로 한다. 서비스 제공자 SP와 키 할당자 KA 와의 사이에서는, 키 할당자 KA가, 서비스 제공자 SP에서의 요청이 있었던 경우에, 사용자 User의 키 기억 장치와 서비스 제공자 SP의 각각에 대하여, 키 할당을 행하여, 사용자 User에서의 서비스 사용료의 징수의 대행을 행한다고 하는 계약을 맺고 있는 것으로 한다.

이 예에 있어서는, 인증 방법의 할당(키 할당)은, 서비스 제공자 SP에서의 특정한 서비스를 이용하는 사용자 User에 대한 키 할당의 요구가 있었던 경우, 키 할당자 KA에 의해 행해진다.

구체적으로는, 키 할당자 KA는, 범용 어카운트 또는 공개키 인증 기반을 사용하여 사용자 User를 특정하여, 사용자 User에 대한 과금(서비스 사용 요금과 키 할당의 수수료의 징수)과 교환 키 할당을 행한다. 그 후, 키 할당자 KA은 키 할당을 행한 것의 통지를 서비스 제공자 SP에 보낸다.

즉, 인증 방법의 할당을 행하는 경우, 키 할당자 KA가, 새로운 인증 방법의 암호키를 생성하여, 서비스 제공자 SP와, 사용자 User가 보유하는 키 기억 장치에 대하여, 그 암호키를 건네 준다.

또는, 인증 방법의 할당을 행하는 경우, 키 할당자 KA가, 사용자 User가 보유하는 키 기억 장치에 대하여, 새로운 인증 방법의 암호키의 생성을 요구한다. 키 기억 장치는, 그 요구를 받아, 새로운 인증 방법의 암호키를 자기 자신이 생성하고, 키 할당자 KA와 서비스 제공자 SP의 각각에 대하여, 그 암호키를 건네 준다.

또한, 본 명세서에 있어서는, 「키 기억 장치가, 새로운 인증 방법의 암호키를 생성한다」란, 「키 기억 장치가, 키 할당자 KA의 요구를 받은 시점에서, 새로운 인증 방법의 암호키를 신규로 생성하는 (온디맨드로 생성하는)」 것뿐만 아니라, 「키 기억 장치 자신 또는 키 기억 장치와는 상이한 다른 장치에 의해 미리 생성된 복수의 암호키의 후보를, 키 기억 장치는 미리 기억해 놓고, 키 할당자 KA의 요구를 받았을 때, 키 기억 장치는, 기억하고 있는 복수의 암호키의 후보 중의 소정의 1개를 추출하고(선택하고), 그것을 새로운 인증 방법의 암호키로 함으로써, 새로운 인증 방법의 암호키를 생성한다」는 것도 포함하는 개념이다.

또한, 이하, 사용자 User가 보유하는 키 기억 장치와, 서비스 제공자 SP의 양자에게 할당되는 인증 방법에 있어서, 키 기억 장치에 할당하는 쪽의 키를, 증명키라고, 서비스 제공자 SP에 할당하는 키를, 검증키라고, 각각 칭한다.

상술한 바와 같이, 인증 방법으로서는, 공통 키 인증을 이용하는 것도, 공개키 인증을 이용하는 것도 가능하다. 공통 키 인증을 이용하는 경우에는, 검증키와 증명키는, 일치한다(동일한 키가 된다). 이것에 대하여, 공개키 인증을 이용하는 경우에는, 검증키는, 공개키가 되고, 증명키는, 비밀키가 되기 때문에, 검증키와 증명키는 서로 다른 키가 된다.

여기서 중요한 점은, 키 할당자 KA가 할당하는 인증 방법은, 사용자 User에 과금을 행하기 위한 인증 방법이 아니라, 특정한 서비스를 제공하기 위한 인증 방법인 점이다. 즉, 키 할당자 KA에서 서비스 제공자 SP 에의 키 할당의 통지에는, 사용자 User를 특정하는 정보나 크레디트 카드 번호가 포함될 필요가 없다.

따라서, 사용자 User는, 서비스 제공자 SP에 대하여 익명성을 유지하는 것이 가능하게 됨과 동시에, 새롭게 할당된 인증 방법의 키가 어떠한 이유로 누설된 경우에도, 가능한 부정은, 키 할당 시에 확정한 서비스의 이용에 한정된다. 이에 의해, 1개의 인증 방법의 중요성이 과대하게 되는 것을 방지하는 것이 가능하게 된다.

새롭게 할당된 인증 방법에 의한 인증은, 다음의 세가지가 전제가 된다.

즉, 첫번째로서, 키 할당자 KA가, 범용 어카운트 또는 공개키 인증 기반으로 서비스 제공자 SP와 사용자 User를 정확하게 특정할 수 있을 것, 두번째로서, 키 할당자 KA가 신용할 수 있을(키를 서비스 제공자 SP와 사용자 User에 정확하게 할당할) 것, 세번째로서, 키 할당자 KA가 할당한 키를 할당 대상자 이외(키 할당자 KA 자신도 포함)에 사용시키지 않을 것의 세가지이다. 이와 같이, 키 할당자 KA는, 범용 어카운트 방식 또는 공개키 인증 방식에 있어서의, 범용 어카운트 관리자 KDC 또는 인증 센터 CA와 동등한 자격(상술한 세가지를 확실하게 실행할 수 있는 자격)을 가질 필요가 있다.

다음으로, 본 비지니스 모델의 동작에 대하여 설명한다.

처음에, 사용자 User는, 서비스의 이용을 선택한다.

사용자 User에 의해 선택된 서비스를 제공 가능한 서비스 제공자 SP는, 그 서비스의 내용이나 금액 등을, 키 할당자 KA에 통지하는 키 할당 의뢰서를 사용자 User에 공급한다.

사용자 User는, 키 할당 의뢰서를 키 할당자 KA에 제출하면, 키 할당자 KA는, 그것을 받아, 사용자 User가 보유하는 키 기억 장치에 대하여, 새로운 인증 방법에 대한 증명키와, 인증 방법의 식별 번호 등의 부가 정보를 입력한다.

또는, 사용자 User는, 키 할당 의뢰서를 키 할당자 KA에 제출하면, 키 할당자 KA는, 그것을 받아, 사용자 User가 보유하는 키 기억 장치에 대하여, 새로운 인증 방법의 암호키의 생성을 요구하는 요구 정보를 입력한다. 키 기억 장치는, 이 요구 정보를 받아, 새로운 인증 방법의 암호키, 즉, 새로운 인증 방법에 대한 증명키와, 그것과 쌍을 이루는 검증키를 생성한다. 그리고, 키 기억 장치는, 증명키를 자기 자신이 기억함과 함께, 검증키를 키 할당자 KA에 공급한다.

이들의 키 할당 시에, 키 할당자 KA는, 키 기억 장치를 보유하는 사용자 User를, 범용 어카운트 또는 공개키 인증 기반에 의해서 특정하여, 사용자 User에 대하여, 서비스에 부합하는 과금을 행한다. 그 후, 키 할당자 KA는, 과금액으로부터 수수료를 뺀 금액을, 서비스 제공자 SP에 지불한다.

그 때문에, 키 기억 장치에는, 사용자 User가 범용 어카운트 또는 공개키 인증 기반으로 인증을 받기 위해서 필요한 패스워드를 입력하는 입력부, IC 카드를 접속하는 접속부 등이 설치된다.

다음으로, 키 할당자 KA는, 사용자 User가 보유하는 키 기억 장치에 대하여, 서비스 제공자 SP에 대한 키 할당 보고서를 작성하여 공급한다.

키 할당 보고서에는, 할당된 인증 방법에 관한 정보(인증 방법의 식별 번호, 그 인증 방법에 대한 검증키)가 포함되어 있다.

키 기억 장치는, 키 할당 보고서를 서비스 제공자 SP에 제출하고, 그것에 의하여, 서비스 제공자 SP는, 새로운 인증 방법에 대한 검증키와 부속 정보를 얻는다. 즉, 서비스 제공자 SP는, 키 할당을 받은 사용자 User를 인증하기 위한 검증키를 얻는다.

인증 방법의 할당 이후, 사용자 User가 서비스를 이용하는 경우, 서비스 제공자 SP는, 사용자 User가 보유하는 키 기억 장치와의 사이에서 할당된 인증 방법에 의한 인증을 행한다. 그리고, 서비스 제공자 SP는, 이 인증에 성공하면 서비스를 제공한다.

이 경우(서비스의 제공이 행하여지는 경우), 이 인증이 행하여진 키 기억 장치(사용자 User가 보유하는 키 기억 장치)와, 서비스 제공자 SP의 사이에서, 일시적인 암호키의 공유를 행하여, 서비스 제공 시의 통신을 암호화한다. 이에 의해, 사용자 User의 인체나 서비스 내용의 누설을 방지하는 것이 가능하게 된다.

할당되는 인증 방법은, 그 사용 목적을 최초로 확정시킴으로써, 유효 기한이나 사용자가 정해진다. 그 때문에, 유효 기한이 지났을 때에는 삭제하는 것이 가능하게 된다. 또한, 인증 방법의 사용을 정지하여야 할 경우에는, 키 할당자 KA에서 서비스 제공자 SP에 무효화를 통지하는 것이 가능하게 된다.

(인증키 할당 시스템)

다음으로, 본 발명이 적용되는 인증키 할당 시스템에 대하여 설명한다.

설명이 번잡하게 되기 때문에, 3차의 제1 실시 형태 내지 제6 실시 형태의 각각으로 나누어, 그 순서대로 개별적으로 설명해 간다.

즉, 제1 실시 형태로서, 범용 어카운트 방식(Kerberos)만이 존재하는 상태(도 1에 대응하는 상태)에서, 할당되는 인증 방법이, 공통 키 인증인 경우의 인증키 할당 시스템에 대하여 설명한다.

제2 실시 형태로서, 공개키 인증 기반만이 존재하는 상태(도 2에 대응하는 상태)에서, 할당되는 인증 방법이, 공개키 인증인 경우의 인증키 할당 시스템에 대하여 설명한다.

제3 실시 형태로서, 도 3의 상태에 대응하여, 사용자 인증에는, 범용 어카운트 방식이 이용되고, 또한, 서비스 제공자의 전자 서명이 공개키 인증 기반으로 검증되는 경우(공개키 인증 기반과 범용 어카운트 방식이 이용되고, 또한, 새롭게 할당하는 인증 방법이 공개키 인증인 경우)의 인증키 할당 시스템에 대하여 설명한다.

제4 실시 형태로서, 도 3의 상태에 대응하여, 사용자 인증에는, 범용 어카운트 방식이 이용되고, 또한, 키 할당자의 전자 서명이 공개키 인증 기반으로 검증되는 경우(공개키 인증 기반과 범용 어카운트 방식이 이용되고, 또한, 할당하는 인증 방법이 공개키 인증인 경우)의 인증키 할당 시스템에 대하여 설명한다.

이상의 제1 내지 제4 실시 형태에 있어서는, 새로운 인증 방법의 암호키는, 키 할당자 KA가 보유하는 장치(후술하는, 키 할당자 단말기)에 의해 생성되지만, 상술한 바와 같이, 사용자 User가 보유하는 키 기억 장치 자신에 의해 생성되어도 된다.

그래서, 제5 실시 형태와 제6 실시 형태로서, 사용자 User가 보유하는 키 기억 장치가 새로운 인증 방법의 암호키를 생성하는 인증키 할당 시스템에 대하여 설명한다.

즉, 제5 실시 형태로서, 제2 실시 형태에 대응하는 실시 형태(공개키 인증 기반만이 존재하는 상태(도 2에 대응하는 상태)에서, 할당되는 인증 방법이, 공개키 인증인 경우의 인증키 할당 시스템)이고, 사용자 User가 보유하는 키 기억 장치가 새로운 인증 방법의 암호키를 생성하는 인증키 할당 시스템에 대하여 설명한다.

또한, 제6 실시 형태로서, 제4 실시 형태에 대응하는 실시 형태(도 3의 상태에 대응하여, 사용자 인증에는, 범용 어카운트 방식이 이용되고, 또한, 키 할당자의 전자 서명이 공개키 인증 기반으로 검증되는 경우(공개키 인증 기반과 범용 어카운트 방식이 이용되고, 또한, 새롭게 할당하는 인증 방법이 공개키 인증인 경우의 인증키 할당 시스템)에, 사용자 User가 보유하는 키 기억 장치가 새로운 인증 방법의 암호키를 생성하는 인증키 할당 시스템에 대하여 설명한다.

(제1 실시 형태)

이하, 도면을 참조하여, 본 발명의 제1 실시 형태가 적용되는 인증키 할당 시스템에 대하여 설명한다.

도 4는, 인증키 할당 시스템(1)의 구성예를 도시하고 있다.

도 4에 도시된 바와 같이, 인증키 할당 시스템(1)에 있어서는, 임의의 인원수(이 예에서는, 1명)의 사용자 User(도 1)가 사용하는 사용자 장치(11), 임의의 인원수(이 예에서는, 1명)의 키 할당자 KA(도 1)이 사용하는 키 할당자 단말기(12), 임의의 인원수(이 예에서는, 1명)의 서비스 제공자 SP(도 1)가 사용하는 서비스 제공자 단말기(13), 및, 임의의 인원수(이 예에서는, 1명)의 범용 어카운트 관리자 KDC(도 1)가 사용하는 범용 어카운트 관리자 단말기(15)의 각각이, 네트워크(14)를 통하여 서로 접속된다.

네트워크(14)의 종류는, 특별히 한정되지 않지만, 이 예에 있어서는, 예를 들면, 인터넷이 된다. 또한, 사용자 장치(11), 키 할당자 단말기(12), 서비스 제공자 단말기(13), 및, 범용 어카운트 관리자 단말기(15)의 각각은, 다른 장치와, 네트워크(14)를 통하지 않고서 직접 통신을 행하여도 된다. 이 경우, 네트워크(14)는, 생략 가능하다.

사용자 장치(11)는, 후술하는 바와 같이, 사용자 단말기(21), 키 기억 장치(22), 및, IC 카드(23)로 구성된다. 단, 키 기억 장치(22)가, 서비스 제공자 단말기(13)로부터 제공되는 서비스를 이용하는 기능, 및, 네트워크(14)를 통하여 다른 장치와 통신하는 기능을 갖고 있는 경우, 사용자 단말기(21)는 생략 가능하다.

도 5 내지 도 8은, 키 할당자 단말기(12)가 기억하는 데이터의 예를 도시하고 있다.

즉, 키 할당자 단말기(12)의 메모리(후술하는 도 18의 기억부(88) 등)에는, 도 5에 도시되는 것 같은 키 할당표, 도 6에 도시되는 것 같은 서비스 제공자키표, 도 7에 도시되는 것 같은 키 기억 장치 키표, 및, 도 8에 도시되는 것 같은 키 할당자 어카운트 정보가 기억되어 있다. 구체적으로는, 이 예에 있어서는, 예를 들면, 도 5의 키 할당표, 도 6의 서비스 제공자 키표, 및, 도 7의 키 기억 장치 키표의 각각은, Key-ID, SP-ID, 및, HW-ID의 각각으로 검색할 수 있는 데이터베이스로서 실장된다.

도 5의 키 할당표에 있어서는, 각 행(이하, 레코드라고 칭한다)이, 키 할당자 단말기(12)에 의해 할당된 인증 방법에 대응하고 있다.

Key-ID는, 할당된 인증 방법의 식별 번호를 나타내고 있고, 일의적으로 할당되어 있다.

Acc-ID는, 인증 방법의 할당 시에, 지불을 한 사용자(가 보유하는 IC 카드)의 범용 어카운트 방식에서의 식별 번호를 나타내고 있다.

HW-ID는, 인증 방법의 할당된 키 기억 장치(22)의 식별 번호를 나타내고 있다.

SP-ID는, 인증 방법의 할당을 받은 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있다.

유효 기한은, 인증 방법의 유효 기한을 나타내고 있다.

서비스 내용은, 그 인증 방법을 이용하는 인증으로, 서비스 제공자 단말기(13)(서비스 제공자 SP)로부터 사용자 단말기(21)(사용자 User)에 제공되는 서비스의 내용을 나타내고 있다.

증명키=검증키는, 인증 방법의 검증키 및 증명키를 나타내고 있다. 또한, 이 예에 있어서는, 인증 방법으로서 공통 키 암호가 이용되기 때문에, 사용자 User(키 기억 장치(22))와 서비스 제공자 SP(서비스 제공자 단말기(13))가 기억하는 키는 일치한다.

도 6의 서비스 제공자 키표에 있어서는, 각 레코드가, 키 할당자 단말기(12)(키 할당자 KA)와 계약을 체결한 서비스 제공자 단말기(13)(서비스 제공자 SP)에 대응한다.

SP-ID는, 계약을 체결한 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있어, 계약 체결 시에 일의적으로 할당되고 있다.

SP-address는, 서비스 제공자 단말기(13)의 연락처 어드레스(메일 어드레스나 URL 등)를 나타내고 있다. 이것은, 인증 방법의 실효가 발생했을 때나 조회 시의 연락처가 된다.

고유 암호키는, 계약 체결 시에 서비스 제공자와 키 할당자의 사이에서 정한 암호키를 나타내고 있고, 양자 간에서의 통신의 은닉성이나 완전성을 보증할 목적으로 이용된다.

도 7의 키 기억 장치 키표에 있어서는, 각 레코드가, 키 기억 장치(22)에 대응하고 있다.

HW-ID는, 키 기억 장치(22)의 식별 번호를 나타내고 있어, 키 기억 장치(22)에 일의적으로 할당된다.

고유 암호키는, 특정한 키 기억 장치(22)와 키 할당자 단말기(12)의 사이에 서 공유하고 있는 암호키를 나타내고 있고, 새로운 인증 방법을 할당할 시에, 양자 간에서의 인증과 키 공유를 위해 이용된다.

도 8의 키 할당자 어카운트 정보는, 범용 어카운트에서의 키 할당자 단말기(12)(키 할당자 KA)의 식별 번호인 Acc-ID와, 범용 어카운트 관리자 단말기(15)(범용 어카운트 관리자 KDC)와의 사이에서의 인증에 이용하는 등록 암호키로

이루어진다.

도 9와 도 10은, 서비스 제공자 SP가 기억하는 데이터의 예를 도시하고 있다.

즉, 서비스 제공자 단말기(13)의 메모리(후술하는 도 19의 기억부(108) 등)에는, 도 9에 도시되는 것 같은 인증 정보표, 및, 도 10에 도시되는 것 같은 서비스 제공자 고유 정보가 기억되어 있다. 이 예에 있어서는, 예를 들면, 도 9의 인증 정보표는, Key-ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 9의 인증 정보표에 있어서, 각 레코드는, 할당을 받은 인증 방법에 대응한다.

Key-ID, 유효 기한, 및 검증키의 각각은, 인증 방법의 식별 번호, 유효 기한, 및 검증키의 각각을 나타내고 있다. 서비스 내용은, 그 인증 방법으로 인증되는 사용자 User(사용자 단말기(21))에 제공하는 서비스의 내용을 나타내고 있다.

도 10의 서비스 제공자 고유 정보에 있어서, SP-ID는, 서비스 제공자 단말기(13)(서비스 제공자 SP)와 키 할당자 단말기(12)(키 할당자 KA)와의 키 할당 계약의 체결 시에 할당된 식별 번호를 나타내고 있다. 마찬가지로, 고유 암호키는, 키 할당 계약 체결 시에 키 할당자 단말기(12)(키 할당자 KA)와의 사이에서 정한 암호키를 나타내고 있고, 양자간에서의 통신의 은닉성과 완전성을 보증할 목적으로 이용된다.

도 11 내지 도 14는, 사용자 User가 보유하는 데이터의 예를 도시하고 있다.

즉, 사용자 장치(11)의 키 기억 장치(22)의 메모리(후술하는 도 16의 데이터 기억부(53), 또는, 키 기억부(54)), 또는, IC 카드(23)에는, 도 11의 증명키표, 도 12의 서비스 정보표, 도 13의 키 기억 장치 고유 정보, 및, 도 14의 사용자 카운트 정보가 기억되어 있다. 이 예에 있어서는, 예를 들면, 도 11의 증명키표와 도 12의 서비스 정보표는, Key-ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 11의 증명키표와 도 12의 서비스 정보표에 있어서, 각 레코드는, 키 기억 장치(22)(사용자 User)가 키 할당자 단말기(12)(키 할당자 KA)로부터 할당을 받은 인증 방법에 대응한다.

Key-ID는, 인증 방법의 식별 번호를 나타내고 있다. 증명키는, 인증 방법의 증명키를 나타내고 있다. 유효 기한은, 인증 방법의 인증키의 유효 기한을 나타내고 있다. 서비스 내용은, 이 인증 방법으로 인증되었을 때에 제공되는 서비스의 내용을 나타내고 있다.

도 13의 키 기억 장치 고유 정보에 있어서, HW-ID는, 키 기억 장치(22)의 고유의 식별 번호를 나타내고 있다. 고유 암호키는, 키 기억 장치(22)에 새로운 증명키를 기입할 때에, 기입을 행하는 상대가 키 할당자 KA(키 할당자 단말기(12))인 것을 인증하고, 또한, 기입되는 증명키가 누설이나 개찬되지 않기 위해서 이용되는 암호키를 나타내고 있다.

도 14의 사용자 카운트 정보는, 범용 어카운트에서의 키 할당자의 식별 번호인 Acc-ID와, 범용 어카운트 관리자 KDC(범용 어카운트 관리자 단말기(15))와의 사이에서의 인증에 이용하는 등록 암호키로 이루어진다. 또한, Acc-ID와 등록 암호키는, 사용자가 입력한 로그인명과 패스워드로부터 생성되는 것이어도 된다.

도 15는, 사용자 단말기(15)의 구성예를 도시하고 있다.

또한, 이 예에 있어서는, 사용자 단말기(15)는, 도 15에 도시되는 것 같은 퍼스널 컴퓨터로 이루어지지만, 서비스 제공자 단말기(13)로부터 제공되는 서비스를 이용할 수 있고, 또한, 키 기억 장치(22)와 접속 가능한 것이면 한정되지 않고, 예를 들면, 디지털 가전 제품 등이어도 된다.

도 15에 있어서, CPU(31)는, ROM(32)에 기억되어 있는 프로그램, 또는 기억부(38)로부터 RAM(33)에 로드된 프로그램에 따라서 각종의 처리를 실행한다.

RAM(33)에는 또한, CPU(31)가 각종의 처리를 실행하는 데 있어서 필요한 데이터 등도 적절하게 기억된다.

CPU(31), ROM(32), 및 RAM(33)은, 버스(34)를 통하여 서로 접속되어 있다. 이 버스(34)에는 또한, 입출력 인터페이스(35)도 접속되어 있다.

입출력 인터페이스(35)에는, 키 기억 장치(22)가 접속된다.

입출력 인터페이스(35)에는 또한, 키보드 등으로 이루어지는 입력부(36), 디스플레이 등으로 이루어지는 출력부(37), 하드디스크 등으로 구성되는 기억부(38), 네트워크(14)(도 4)를 통하여 다른 장치와 서로 통신하기 위한 통신 처리를

실행하 는 통신부(39)가 접속되어 있다.

입출력 인터페이스(35)에는 또한, 필요에 따라 드라이브(40)가 접속되어, 자기 디스크, 광 디스크, 광 자기 디스크, 또는 반도체 메모리 등의 리무버블 기록 매체(41)가 적절하게 장착되어, 이들로부터 판독된 컴퓨터 프로그램이, 필요에 따라 기억부(38)에 인스톨된다.

도 16은, 키 기억 장치(22)의 구성예를 도시하고 있다.

도 16에 있어서, CPU(51)은, ROM(52)에 기억되어 있는 프로그램, 또는, 사용자 단말기(21)로부터 통신 처리부(57)를 통하여 RAM(53)에 로드된 프로그램에 따라서 각종의 처리를 실행한다. RAM(53)에는 또한, CPU(51)가 각종의 처리를 실행하는 데에 있어서 필요한 데이터 등도 적절하게 기억된다. CPU(51), ROM(52), 및 RAM(53)은, 버스(60)를 통하여 서로 접속되어 있다.

이 버스(60)에는 또한, 도 12의 서비스 정보표를 기억하는 데이터 기억부(53), 도 11의 증명키표, 및, 도 13의 키 기억 장치 고유 정보를 기억하는 키 기억부(54), 및, CPU(51)의 제어에 기초하여, 키 할당자 KA에서의 정보(도 4의 키 할당자 단말기(12)에 의해 송신되어, 네트워크(14), 및, 사용자 단말기(21)를 통하여 통신 처리부(57)에 의해 수신된 정보)나, 데이터 기억부(53)에 기억되어 있는 도 12의 서비스 정보표의 유효 기한에 따라서, 키 기억부(54) 또는 데이터 기억부(53)의 내용을 추가 또는 삭제하는 데이터 관리부(55)가 설치되어 있다.

이 버스(60)에는 또한, CPU(51)의 제어에 기초하여, 암호키를 이용하여, 인증을 위한 연산 처리를 행하는 연산 처리부(56), 사용자 단말기(21)와의 통신 처리 를 행하는 통신 처리부(57), 키 기억 장치(22)를 사용하는 사용자 User를 특정하는 처리를 행하는 인증 처리부(58)가 설치되어 있다.

사용자 인증이, 로그인명과 패스워드로 행해지는 경우, 사용자 User는, 사용자 단말기(22)의 디스플레이(도 15의 출력부(37))를 확인하면서, 사용자 단말기(22)의 키보드(도 15의 입력부(36))를 조작하여, 로그인명과 패스워드를 입력한다. 사용자 단말기(21)에 입력된 로그인명과 패스워드는, 도 15의 입출력 인터페이스(35), 및, 통신 처리부(57)를 통하여 인증 처리부(58)에 공급되고, 인증 처리부(58)는, 공급된 로그인명과 패스워드에 기초하여, 도 14의 사용자 어카운트 정보인 Acc-ID와 등록 암호키를 생성하고, 사용자 인증의 처리를 행한다.

또한, 키 기억 장치(22)가, 사용자 단말기(21)에 접속되지 않고서, 그것 단체(單體)로 이용되고, 또한, 사용자 인증이, 로그인명과 패스워드로 행해지는 경우, 인증 처리부(58)에는, 키보드와 디스플레이가 직접 접속된다.

이것에 대하여, 공통 키 암호 또는, 공개키 암호에 기초하는 인증이 이용되는 경우, 인증 처리부(58)에는, IC 카드(23)가 접속된다. 도 14의 Acc-ID와 등록 암호키는, IC 카드(23)에 기억된다.

이 예에 있어서, 키 기억 장치(22)는, 인증 처리부(58)에 접속된 IC 카드(23)에 대하여, IC 카드(23)가 기억하는 암호키를 사용한 데이터의 암호화, 및, 암호화 데이터의 복호를 의뢰하는 것, 및, IC 카드(23)로부터 인증을 위해 필요한 부속 정보(사용자의 식별 번호나, 증명서 등)를 취득할 수 있는 것으로 한다.

후술하는 바와 같이, 사용자의 특정은 새로운 인증 방법의 할당 시에만 필요 하게 되기 때문에, 그것 이외일 때에는, 공통 키 암호 또는, 공개키 암호에 기초하는 인증이면, IC 카드(23)를 인증 처리부(58)로부터 빼어 놓는 것이 가능하고, 또한, 패스워드 인증이면, 키 기억 장치(22)가 패스워드를 기억하지 않고, 사용자 User에 매회 패스워드를 입력시킴으로써, 이들의 사용자 인증 방법에 관한 각종 정보를 키 기억 장치(22)로부터 분리하는 것이 가능하다.

또한, 키 기억부(54), 연산 처리부(56), 및 데이터 관리부(55)의 각각은, 내탬퍼성을 갖도록 이루어지면 된다. 이 경우, 내부에 기억 또는 처리되어 있는 데이터가 외부로부터 취득이나 개변되는 것을 방지하는 것이 가능하게 된다.

도 17은, IC 카드(23)의 구성예를 도시하고 있다.

IC 카드(23)도, 내부에 기억되어 있는 데이터나 처리 내용이 외부로부터 취득되지 않도록, 내탬퍼성을 갖도록 이루어지면 된다.

IC 카드(23)에는, 인증에 사용하는 암호키와 부속 정보(공통 키 인증인 경우에는 그 공통 키 암호의 암호키, 공개키 인증인 경우에는 공개키 암호의 비밀키와 증명서)를 기억하는 기억부(71), 기억부(71)가 기억하는 암호키를 이용하여, 인증을 위한 계산 처리를 행하는 계산 처리부(72), 키 기억 장치(22)의 인증 처리부(58)(도 16)와의 통신 처리를 행하는 통신 처리부(73)가 설치되어 있다. 사용자 인증에 IC 카드(23)가 이용되는 경우, 도 14의 어카운트 정보는, 기억부(71)에 기억된다.

도 18은, 키 할당자 단말기(12)의 구성예를 도시하고 있다.

도 18에 있어서, CPU(81) 내지 리무버블 기록 매체(91)의 각각은, 도 15의 사용자 단말기(21)의 CPU(31) 내지 리무버블 기록 매체(41)의 각각과, 마찬가지의 구성이 되기 때문에, 이들의 설명은 생략한다.

단, 예를 들면, 기억부(88) 등에는, 상술한 도 5 내지 도 8의 데이터가 기억된다.

도 19는, 서비스 제공자 단말기(13)의 구성예를 도시하고 있다.

도 19에 있어서, CPU(101) 내지 리무버블 기록 매체(111)의 각각은, 도 15의 사용자 단말기(21)의 CPU(31) 내지 리무버블 기록 매체(41)의 각각과, 마찬가지의 구성이 되기 때문에, 이들의 설명은 생략한다.

단, 예를 들면, 기억부(108) 등에는, 상술한 도 9와 도 10의 데이터가 기억되어 있다.

도 20은, 범용 어카운트 관리자 단말기(15)의 구성예를 도시하고 있다.

도 20에서, CPU(121) 내지 리무버블 기록 매체(131)의 각각은, 도 15의 사용자 단말기(21)의 CPU(31) 내지 리무버블 기록 매체(41)의 각각과, 마찬가지의 구성이 되기 때문에, 이들의 설명은 생략한다.

단, 예를 들면, 기억부(128) 등에는, 도 21과 도 22에 도시되는 것 같은 데이터가 기억되어 있다.

이 예에 있어서는, 도 21의 어카운트 관리표는, Acc-ID로 검색할 수 있는 데이터베이스로서 실장되어 있다. 또한, Acc-ID는, 범용 어카운트에서의 사용자 User(키 기억 장치(22))의 식별 번호를 나타내고 있고, 일의적으로 할당되어 있다. 암호키는, 공통 키 인증으로 사용자 User(키 기억 장치(22))를 인증하기 위한 정보 를 나타내고 있다.

도 22의 범용 어카운트 관리자 고유키는, 범용 어카운트 관리자 KDC(범용 어카운트 관리자 단말기(15))만의 암호키를 나타내고 있다.

다음으로, 도 23의 흐름도를 참조하여, 인증키 할당 시스템(1)의 동작의 개략에 대하여 설명한다.

단계 S1에 있어서, 도 4의 사용자 단말기(21)(사용자 User)가, 서비스를 선택하면, 키 할당자 단말기(12)(키 할당자 KA)는, 사용자 User의 키 기억 장치(22)와, 서비스 제공자 단말기(13)(서비스 제공자 SP)에 대하여, 그 서비스의 제공을 위한 인증 방법의 할당을 행한다. 또한, 이러한 일련의 처리를, 이하, 「서비스 선택/키 할당 처리」라고 칭한다. 「서비스 선택/키 할당 처리」의 상세에 대해서는, 도 24 내지 도 26의 흐름도와 도 27의 애로우 차트를 참조하여, 후술한다.

단계 S1의 처리에 의해 인증 방법의 할당이 행해지면, 단계 S2에 있어서, 사용자 User의 키 기억 장치(22)는, 할당된 인증 방법을 이용하여, 서비스 제공을 위한 인증에 응답한다. 이 인증에 성공한 경우, 서비스 제공자 단말기(13)(서비스 제공자 SP)는, 그 키 기억 장치(22)를 소지하는 사용자 User에 대하여(키 기억 장치(22)에 접속된 사용자 단말기(21)에 대하여), 서비스를 제공한다. 또한, 이러한 일련의 처리를, 이하, 「키 사용/서비스 제공 처리」라고 칭한다. 「키 사용/서비스 제공 처리」의 상세에 대해서는, 도 30과 도 31의 흐름도를 참조하여, 후술한다.

다음으로, 단계 S3에 있어서, 사용자 장치(11), 키 할당자 단말기(12), 및, 서비스 제공자 단말기(13)의 각각은, 후술하는 단계 S6의 처리(「키 삭제 처리」)를 행하는가 아닌가를 판정한다.

단계 S3의 처리의 판정 방법은, 특별히 한정되지 않지만, 이 예에 있어서는, 예를 들면, 후술하는 바와 같이, 외부로부터 키 삭제를 행하는 계기(트리거)가, 사용자 장치(11), 키 할당자 단말기(12), 및, 서비스 제공자 단말기(13)의 각각에 공급되는 것으로 하면, 단계 S3에 있어서, 사용자 장치(11), 키 할당자 단말기(12), 및, 서비스 제공자 단말기(13)의 각각은, 이 트리거를 취득한 경우, 「키 삭제 처리」를 행한다고 판정한다.

이 경우, 키 기억 장치(22)에 기억되는 암호키에는 유효 기한이 있어, 단계 S6에 있어서, 유효 기한이 넘은 인증 방법의 정보의 삭제가 행하여진다. 또한, 이러한 처리를, 이하, 「키 삭제 처리」라고 칭한다. 「키 삭제 처리」의 상세에 대해서는, 도 37 내지 도 39의 흐름도를 참조하여, 후술한다.

이것에 대하여, 단계 S3에 있어서, 「키 삭제 처리」를 행하지 않는다고 판정된 경우, 단계 S4에 있어서, 키 할당자 단말기(12)는, 후술하는 단계 S7의 처리(「키 사용 정지 처리」)를 행하는가 아닌가를 판정한다.

단계 S4의 처리의 판정 방법은, 특별히 한정되지 않지만, 이 예에 있어서는, 예를 들면, 키 할당자 단말기(12)는, 할당된 인증 방법의 증명키가, 어떠한 이유로 외부에 누설된 것을 검출한 경우, 또는, 키 기억 장치(22)가 도난당한 것을 검출한 경우(검출 수단은 도시하지 않음), 단계 S4에 있어서, 「키 사용 정지 처리」를 행한다고 판정한다.

이 경우, 단계 S7에 있어서, 인증 방법의 사용을 정지하는 처리가 실행된다. 구체적으로는, 키 할당자 단말기(12)(키 할당자 KA)가, 인증 방법의 사용을 정지하는 것을, 서비스 제공자 단말기(13)(서비스 제공자 SP)에 통지하여, 해당하는 인증 방법의 사용을 중지시킨다. 또한, 이러한 처리를, 이하, 「키 사용 정지 처리」라고 칭한다. 「키 사용 정지 처리」의 상세에 대해서는, 도 40과 도 41의 흐름도를 참조하여, 후술한다.

이것에 대하여, 단계 S4에 있어서, 「키 사용 정지 처리」를 행하지 않는다고 판정한 경우, 단계 S5에 있어서, 키 기억 장치(22)와 서비스 제공자 단말기(13)의 각각은, 상술한「키 사용/서비스 제공 처리」를 행하는가 아닌가를 판정한다.

단계 S5에 있어서, 「키 사용/서비스 제공 처리」를 행한다고 판정된 경우, 단계 S2로 되돌아가, 「키 사용/서비스 제공 처리」가 재차 실행된다.

이것에 대하여, 단계 S5에 있어서, 「키 사용/서비스 제공 처리」를 행하지 않는다고 판정된 경우, 단계 S3으로 되돌아가, 그 이후의 처리가 반복된다.

즉, 상술한 단계 S1 내지 S7의 처리는, 소정의 1개의 목적별 인증키에 대한 인증키 할당 시스템(1)의 처리를 나타내고 있고, 그 1개의 목적별 인증키에 대하여, 상술한 단계 S1의 「서비스 선택/키 할당 처리」가 실행되면, 단계 S6의 「키 삭제 처리」, 또는, 단계 S7의 「키 사용 정지 처리」 중의 어느 한쪽의 처리가 실행될 때까지, 그 목적별 인증키는 기억 상태가 되어, 필요에 따라 단계 S2의 「키 사용/서비스 제공 처리」가 복수회 실행된다.

인증키 할당 시스템(1)에 있어서는, 그와 같은 목적별 인증키가 복수개 존재 하여, 이들의 복수의 목적별 인증키에 대한 단계 S1 내지 S7의 처리는, 각각 독립하여 행해진다.

이하, 「서비스 선택/키 할당 처리」, 「키 사용/서비스 제공 처리」, 「키 삭제 처리」, 및, 「키 사용 정지 처리」의 각각의 상세에 대하여, 그 순서로 개별적으로 설명한다.

처음에, 도 24 내지 도 26의 흐름도, 및 도 27의 애로우 차트를 참조하여, 본 발명의 제1 실시 형태가 적용되는 인증키 할당 시스템(1)의 동작 중의, 「서비스 선택/키 할당 처리(도 23의 단계 S1의 처리)」에 대하여 설명한다. 도 24는, 사용자 장치(11)(도 4)의 「서비스 선택/키 할당 처리」를, 도 25는, 키 할당자 단말기(12)(도 4)의 「서비스 선택/키 할당 처리」를, 도 26은, 서비스 제공자 단말기(13)(도 4)의 「서비스 선택/키 할당 처리」를, 각각 도시하고 있다. 도 27은, 이들 사용자 장치(11), 키 할당자 단말기(12), 및, 서비스 제공자 단말기(13)의 「서비스 선택/키 할당 처리」의 관계를 도시하고 있다.

이하, 도 24 내지 도 26을 참조하여, 사용자 장치(11), 키 할당자 단말기(12), 및, 서비스 제공자 단말기(13)의 「서비스 선택/키 할당 처리」에 대하여, 개별적으로 설명하지만, 이들 장치의 상호의 처리의 관계는, 도 27의 대응하는 단계를 참조함으로써, 용이하게 이해하는 것이 가능하다.

처음에, 도 24를 참조하여, 사용자 장치(11)(도 4)의 「서비스 선택/키 할당 처리」에 대하여 설명한다.

단계 S11에 있어서, 도 15의 사용자 단말기(21)의 CPU(31)는, 입력부(36)로 부터의 사용자의 명령에 기초하여, 서비스를 선택하여, 통신부(39), 및, 네트워크(14)를 통하여 서비스 제공자 단말기(13)로 송신한다.

이 예에 있어서는, 예를 들면, 기억부(38)에는, Web Browser 등의 인터넷 상의 홈페이지 등을 열람하는 어플리케이션 소프트웨어(이하, 이러한 어플리케이션 소프트웨어를, 브라우저라고 칭한다)가 기억되어 있는 것으로 하면, CPU(31)는, 이 브라우저를 상승시켜, 통신부(39), 및, 네트워크(14)를 통하여, 서비스 제공자 단말기(13)(도 19의 기억부(108))에 기억되어 있는 서비스 제공자 SP가 관리하는 홈페이지를 브라우저 상에 표시시킨다.

사용자 User는, 이 홈페이지를 열람하여, 이용을 희망하는 서비스의 선택을 행하고, 선택한 서비스를, 키보드(입력부(36))를 조작하여 입력하면, CPU(31)은, 그 선택된 서비스를 취득하여, 통신부(39), 및, 네트워크(14)를 통하여 서비스 제공자 단말기(13)로 송신한다.

또한, 이와 같이 사용자 User에 의해 선택된 서비스를, 이하, 단순히 선택 서비스라고 칭한다.

또한, 이하, CPU(31)(그 밖의 장치의 CPU도 포함)가, 통신부(39)(그 밖의 장치의 통신부도 포함), 및, 네트워크(14)를 통하여, 소정의 형식의 데이터를 송신하는 것을, 단순히, CPU(31)가, 데이터를 송부한다고 칭한다.

또한, CPU(31)(그 밖의 장치의 CPU도 포함)가, 다른 장치에서 송신된 소정의 형식의 데이터를, 네트워크(14), 및, 통신부(39)(그 밖의 장치의 통신부도 포함)를 통하여 수신하는 것을, 단순히, CPU(31)가, 데이터를 수취한다고 칭한다. 구체적 으로는, 예를 들면, 사용자 User가, 홈페이지에 표시되어 있는 버튼을, 마우스 등의 입력 장치로 선택하여, CPU(31)가, 그것을, 통신부(39) 및 네트워크(14)를 통하여 통지하는 방법을 이용함으로써, CPU(31)는, 선택 서비스를 송부할 수 있다.

CPU(31)에 의해 송부된 선택 서비스는, 네트워크(14)를 통하여 서비스 제공자 단말기(13)로 공급된다.

후술하는 바와 같이, 서비스 제공자 단말기(13)는, 이 선택 서비스를 수취하면, 키 할당 의뢰서를 작성하여, 이것을 사용자 단말기(21)로 송부한다(도 26과 도 27의 단계 S41과 S42).

도 28은, 그와 같은 키 할당 의뢰서의 예를 도시하고 있다.

의뢰서 ID는, 이 키 할당 의뢰서를 발행한 서비스 제공자 단말기(13)(서비스 제공자 SP)에서 일의적으로 되도록, 부가되는 의뢰서의 식별 번호를 나타내고 있다.

유효 기한은, 이 키 할당 의뢰서로 할당을 의뢰하는 인증 방법에 필요한 유효 기한을 나타내고 있다.

SP-ID는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있고, 서비스 제공자 단말기(13)(서비스 제공자 SP)가, 키 할당자 단말기(12)(키 할당자 KA)와의 계약 시에 미리 결정된 것이다.

서비스 내용은, 이 인증 방법에서 인증되는 사용자 User(키 기억 장치(22))에 제공되는 서비스(사용자 단말기(21)(사용자 User)에 의해 선택된 서비스)의 내용을 나타내고 있다. 또한, 이 예에 있어서는, 예를 들면, 서비스 내용에는, 서비 스의 내용 그 자체 외에, 예를 들면, 서비스의 요금이나 제공을 행하는 사이트의 어드레스 등도 포함된다고 한다.

메시지 인증 코드(MAC: Message Authentication Code)는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 고유 암호키(도 10의 서비스 제공자 고유 정보에 포함되는 고유 암호키)를 이용하여, 키 할당 의뢰서의 데이터에 대하여 생성된 것이고, 키 할당 의뢰서의 개찬의 방지와 키 할당 의뢰서가 서비스 제공자에 의해서 생성된 것을 증명한다.

메시지 인증 코드는, 공통 키 암호의 기술을 이용하여, 데이터의 개찬과 메시지 생성자의 특정을 가능하게 하는 것이다.

예를 들면, 데이터 M이 존재할 때, 데이터 M의 작성자와 데이터 M의 송부처 만이 공통 키 암호의 암호키 K를 공유하고 있는 것으로 한다. 이 때, 데이터 M의 메시지 인증 코드는, 암호키 K를 이용하여, MAC(M)=E(K, h(M))(키 K에 의한 h(M)의 암호화 데이터)로서 생성된다. 또한, h()는, 데이터의 송부 측과 받는 측이 공통으로 갖는 일방향성 함수(예를 들면, 해시 함수 등)가 된다.

송신 측은, 데이터 M을 보낼 때에, (M, MAC(M))의 세트로 송부하고, 수취 측은, h(M)=D(K, h(M))이 만족하는가 아닌가를 확인함으로써, 데이터 M이 개찬되어 있지 않은 것과, 전자 서명 SG(M)이 비밀키 S_k 의 소유자에 의해서 부가된 것을 확인할 수 있다. 이하, 이러한 일련의 처리를, 메시지 인증 코드의 확인이라 칭한다.

도 24로 되돌아가, 단계 S12에 있어서, 도 16의 키 기억 장치(22)의 CPU(51) 는, 키 할당 의뢰서를 사용자 단말기(21)를 통하여 수취하고(이하, CPU(51)가, 소정의 데이터를 사용자 단말기(21)를 통하여 수취하는 것을, 단순히, CPU(51)가, 데이터를 수취한다고 칭한다), 단계 S13에 있어서, 그 키 할당 의뢰서를, 키 할당자 단말기(12)에 사용자 단말기(21)를 통하여 송부한다(이하, CPU(51)가, 소정의 데이터를 사용자 단말기(21)를 통하여 송부하는 것을, 단순히, CPU(51)가, 데이터를 송부한다고 칭한다).

동시에, CPU(51)는, 키 할당 의뢰서를, 예를 들면, 데이터 기억부(53)에도 기억시킨다.

이 때, 후술하는 바와 같이, 키 할당자 단말기(12)는, 키 할당 의뢰서 수취, 그것에 포함되는 메시지 인증 코드의 검증을 행한다. 또한, 동일 서비스 제공자로부터 과거에 동일한 의뢰서 번호의 의뢰서가 와있지 않은 것을 확인한다. 이것들을 확인한 후에, 키 할당자 단말기(12)와 키 기억 장치(22)는, 네트워크(14) 및 사용자 단말기(21)를 통하여, 상호 인증을 행하여, 일시적인 (일회 한정의) 암호키 Kses의 공유를 행하는 처리를 실행한다(도 25와 도 27의 단계 S21과 S22). 또한, 이러한 처리를, 이하, 키 기억 장치(22)측의 처리로서는, 「키 할당자와 상호 인증 + 키 공용 처리」라고 칭하여, 키 할당자 단말기(12)측의 처리로서는, 「키 기억 장치와 상호 인증 + 키 공용 처리」라고 칭한다.

즉, 키 기억 장치(22)의 CPU(51)는, 단계 S14에 있어서, 「키 할당자와 상호 인증 + 키 공용 처리」를 실행한다.

제1 실시 형태에 있어서의 「키 할당자와 상호 인증 + 키 공용 처리(단계 S14의 처리)」(및, 「키 기억 장치와 상호 인증 + 키 공용 처리(도 25의 단계 S22의 처리)」의 상세가, 도 27에 도시되고 있다. 그래서, 도 27을 참조하여, 제1 실시 형태에 있어서의 「키 할당자와 상호 인증 + 키 공용 처리(단계 S14의 처리)」의 상세에 대하여 설명한다.

또한, 이 예에 있어서는, 키 할당자 단말기(12)는, 도 7의 키 기억 장치 키표에 의해서, 키 기억 장치(22)의 식별 번호(HWIDb)와, 키 기억 장치(22)가 갖는 고유 암호키 KHWb의 대응을 파악하고 있는 것으로 한다.

도 27의 단계 S14의 중의 단계 S14-1에 있어서, 처음에, 키 기억 장치(22)의 CPU(51)(도 16)가, 난수 Rb를 생성하여, 난수 Rb와 식별 번호 HWIDb의 연결(데이터 Rb ‖ HWIDb(이하, 데이터 A와 B의 연결을, 데이터A ‖ B라고 기술한다))을 송부한다.

키 할당자 단말기(12)는, 후술하는 바와 같이, 그것을 수취하면, 단계 S22의 중의 단계 S22-1로, 난수 Ra를 생성하여, 도 7의 키 기억 장치표로부터, 식별 번호 HWIDb에 대응하는 고유 암호키 KHWb를 추출하고, 단계 S22-2로, 난수 Ra, 난수 Rb, 및, 식별 번호 HWIDb의 연결을, 고유 암호키 KHWb를 이용하여, 암호화하여, 키 기억 장치(22)로 송부하는 (암호화 데이터 E(KHWb, Ra ‖ Rb ‖ HWIDb)을 반송한다). 즉, 고유 암호키 KHWb를 사용하여 공통 키 암호에 기초하는 상호 인증을 행한다(도 27과 도 25의 단계 S22).

키 기억 장치(22)의 CPU(51)는, 단계 S14-2로, 그것을 수취하면, 방금 전 송부한 난수 Rb와 식별 번호 HWIDb가 정확하게 복호되는 것을 확인함으로써(난수 Rb가 포함되는 데이터가, 고유 암호키 KHWb에서 정확하게 암호화되어 있는 것을 확인 함으로써), 상대가, 식별 번호 HWIDb에 대응하는 고유 암호키 KHWb를 파악하고 있는 키 할당자 단말기(12)(키 할당자 KA)인 것을 확인한다.

그리고, 키 기억 장치(22)의 CPU(51)는, 단계 S14-3에서, 고유 암호키 KHWb를 이용하여, 난수로 구성되는 일시적인 공유 암호키(세션 키) Kses를 생성하여, 난수 Rs, Rb와 연결하여, 그것을 암호화하여 송부한다(암호화 데이터 E(KHWb, Rb ‖ Rb ‖ Kses)을 송부한다).

또한, 이 예에 있어서는, 예를 들면, 암호화는, 키 기억 장치(22)(도 16)의 연산 처리부(56)로 행해진다(이하, 키 기억 장치(22)에 의해 행해지는 다른 암호화도 마찬가지라고 한다. 단, 도 14의 사용자 어카운트 정보가 IC 카드(23)(도 17)에 포함되는 경우, 등록 암호키를 이용하는 암호화 처리만은 IC 카드(23)의 계산 처리부(72)에서 행해진다).

키 할당자 단말기(12)는, 단계 S22-3에서, 이 암호화 데이터 E(KHWb, Rb ‖ Ra ‖ Kses)를 수취하여, 그것을 복호하여 공용 암호키 Kses를 추출한다(도 27과 도 25의 단계 S22).

이에 의해, 키 기억 장치(22)와 키 할당자 단말기(12)와의 사이에서, 공용 암호키 Kses의 공유가 가능하게 된다.

또한, 단계 S13과 S21의 처리에서 행해지는 사용자 장치(11)로부터 키 할당자 단말기(12)로의 키 할당 의뢰서의 송부는, 공용 암호키 Kses가 공용된 후, 공용 암호키 Kses를 이용하여 암호화를 행하여도 상관없다. 즉, 이 경우, 도 24에 도시되는 사용자 장치(11)에 있어서의 단계 S13과 S14의 처리 순서가 교체되고, 또한, 도 25에 도시되는 키 할당자 단말기(12)에 있어서의 단계 S21과 S22의 처리 순서가 교체되게 되지만, 이들 이후의 처리에는 영향을 끼치지 않는다.

도 24로 되돌아가, 키 기억 장치(22)의 CPU(51)는, 이상의 단계 S14에 있어서의 「키 할당자와 상호 인증 + 키 공용 처리」의 후에, 단계 S15에 있어서, 「키 할당자 단말기(12)가, 공용 암호키 Kses를 기억하는 키 기억 장치(22)(사용자 User)를 특정(인증)하는 처리」에 대응하는 처리를 실행한다.

또한, 이하, 이러한 처리를, 「사용자 인증 응답 처리」라고 칭한다. 또한, 키 할당자 단말기(12)의 「키 할당자 단말기(12)가, 공용 암호키 Kses를 기억하는 키 기억 장치(22)(사용자 User)를 특정(인증)하는 처리」를, 「키 기억 장치의 사용자 인증 처리」라고 칭한다.

즉, 키 기억 장치(22)의 CPU(51)는, 단계 S15에 있어서, 「사용자 인증 응답 처리」를 실행한다.

제1 실시 형태에 있어서의 「사용자 인증 응답 처리(단계 S15의 처리)」의 상세가, 도 27에 도시되고 있다. 그래서, 도 27을 참조하여, 제1 실시 형태에 있어서의 「사용자 인증 응답 처리」의 상세에 대하여 설명한다.

또한, 도 27에 있어서는, 범용 어카운트 방식, 구체적으로는, Kerberos 인증에 의해서, 사용자가 인증되는 예가 도시되고 있지만, 사용자를 인증하는 것이 가능한 것이면, 이 예에 한정되는 것이 아니다.

처음에, 후술하는 바와 같이, 키 할당자 단말기(12)는, 단계 S23-1에서, 자기 자신의 범용 어카운트에서의 식별 번호(Acc-ID) IDKA를 키 기억 장치(22)로 송 부한다(도 27과 도 25의 단계 S23).

키 기억 장치(22)의 CPU(51)는, 단계 S15-1에서, 이것을 수취하면, 사용자 User에서의 인증 서비스 요청 KRB_AS_REQ을, 범용 어카운트 관리자 단말기(15)로 송부한다.

구체적으로는, 이 예에 있어서는, 예를 들면, 서비스 요청 KRB_AS_REQ은, 데이터 UID ‖ E(KU, time)가 된다. 단, UID는, 사용자 User(IC 카드(23))의 식별 번호를 나타내고 있다. E(KU, time)는, 사용자의 등록 암호키 KU를 이용하여, 시각 time를 암호화한 데이터를 나타내고 있다.

범용 어카운트 관리자 단말기(15)는, 단계 S51에서, 서비스 요청 KRB_AS_REQ가 정확하다는 것, 즉, 식별 번호 UID에 대응하는 암호키 KU로, 서비스 요청 KRB_AS_REQ에 포함되는 시각 time가 복호 가능하고, 또한, 현재 시각과의 어긋남이, 소정의 일정 범위 내인 것을 확인한다.

그리고, 범용 어카운트 관리자 단말기(15)는, 단계 S52로, 인증 서비스 회신 KRB_AS_REP을, 키 기억 장치(22)로 송부(반송)한다.

이 예에 있어서는, 예를 들면, 인증 서비스 회신 KRB_AS_REP은, 데이터 E(KU, Kt) ‖ E(KKDC, Kt ‖ UID ‖ expire)가 된다. 단, E(KU, Kt)는, 암호키 KU를 이용하여, 범용 어카운트 관리자 단말기(15)(범용 어카운트 관리자 KDC)가 정한 일시적인 암호키 Kt를 암호화한 데이터를 나타내고 있다. E(KKDC, Kt ‖ UID ‖ expire)는, 범용 어카운트 관리자 단말기(15)(범용 어카운트 관리자 KDC)의 암호키 KKDC를 이용하여, 암호키 Kt, 사용자의 식별 번호 UID, 유효 기한 expire의 연결 데이터 Kt ‖ UID ‖ expire를 암호화한 데이터를 나타내고 있다. 또한, 이하, E(KKDC, Kt ‖ UID ‖ expire)를 TGT라고 기술한다.

키 기억 장치(22)의 CPU(51)는, 단계 S15-2에서, 인증 서비스 회신 KRB_AS_REP을 수취하면, 인증 서비스 회신 KRB_AS_REP 에 포함되는 암호화 데이터 E(KU, Kt)를 복호하여, 일시 키 Kt를 추출한다. 단, CPU(51)는, TGT의 복호는 할 수 없다.

키 기억 장치(22)의 CPU(51)는, 단계 S15-3에서, 티켓 인가 서비스 요청 KRB_TGS_REQ을, 범용 어카운트 관리자 단말기(15)로 송부한다.

이 예에 있어서는, 티켓 인가 서비스 요청 KRB_TGS_REQ은, 예를 들면, 데이터 IDKA ‖ E(Kt, UID ‖ time) ‖ TGT가 된다.

범용 어카운트 관리자 단말기(15)는, 단계 S53에서, 서비스 요청 KRB_TGS_REQ를 수취하면, TGT의 유효 기한을 검사하여, 유효이면 TGT로부터 암호키 Kt를 추출하여, 암호화 데이터 E(Kt, UID ‖ time)를 복호한 도중의 시각 time가 현재 시각과 비교하여, 일정 범위에 있는 것을 확인한다. 범용 어카운트 관리자 단말기(15)는, 그 확인에 성공하면, 키 기억 장치(22)와 키 할당자 단말기(12)에서 공유하는 일시 키 Kt2를 생성한다.

그리고, 범용 어카운트 관리자 단말기(15)는, 단계 S54로, 회신 KRB_TGS_REP을 키 기억 장치(22)로 송부(반송)한다.

이 예에 있어서는, 회신 KRB_TGS_REP는, 예를 들면, E(Kt, Kt2 ‖ IDKA) ‖ E(KKA, Kt2 ‖ UID)가 된다. 단, KKA는, 키 할당자 단말기(12)(키 할당 자(KA))의 범용 어카운트에의 등록 암호키를 나타내고 있다.

키 기억 장치(22)의 CPU(51)는, 단계 S15-4에서, 회신 KRB_TGS_REP을 수취하면, 암호화 데이터 E(Kt, Kt2 ‖ IDKA)를 복호하여, Kt2를 얻는다.

키 기억 장치(22)의 CPU(51)은, 단계 S15-5에서, 데이터 KRB_AP_REQ를 키 할당자 단말기(12)로 송부한다.

이 예에 있어서는, 데이터 KRB_AP_REQ는, 예를 들면, E(Kses, Kt2) ‖ E(Kt2, UID ‖ time) ‖ E(KKA, Kt2 ‖ UID)가 된다.

키 할당자 단말기(12)는, 단계 S23-2에서, 데이터 KRB_AP_REQ를 수취하면, 암호화 데이터 E(KKA, Kt2 ‖ UID)으로부터, 식별자 UID의 사용자 User(키 기억 장치(22))의 암호키 Kt2를 복호하고, 또한, 암호화 데이터 E(Kt2, UID ‖ time)을 복호한 것 중 시각 time가, 현재 시각과 비교하여 일정 범위 내에 있는 것을 확인한다. 그리고, 키 할당자 단말기(12)는, 암호화 데이터 E(Kses, Kt2)로부터, 암호키 Kses를 공유한 키 기억 장치(22)의 소지자가 식별 번호 UID의 사용자 User(사용자 단말기(21))인 것을 특정한다.

그리고, 키 할당자 단말기(12)는, 단계 S23-3에서, 사용자 User를 특정한 것을 나타내는 데이터 KRB_AP_REQ를 생성하여, 키 기억 장치(22)로 송부한다.

그 후, 후술하는 바와 같이, 키 할당자 단말기(12)는, 키 기억 장치(22)에 대하여, 할당하는 인증 방법의 식별 번호 KID와 인증에 사용하는 신규키 Kr를 생성하여, 송부하여 온다(도 25와 도 27의 단계 S24).

도 24로 되돌아가, 이 때, 키 기억 장치(22)의 CPU(51)는, 단계 S16에 있어 서, 이 신규키 Kr(및, 식별 번호 KID)를 수취한다.

이 예에 있어서는, 예를 들면, 식별 번호 KID는 지금까지 사용되고 있지 않은 번호가 되고, 신규키 Kr는 이 때 키 할당자 단말기(12)에 의해 생성된 난수가 된다.

구체적으로는, 예를 들면, 키 할당자 단말기(12)는, 상술한 키 기억 장치(22)와 공유하고 있는 일시 키 Kses를 이용하여, 식별 번호 KID와 신규키 Kr를 암호화 데이터 E(Kses, KID ‖ Kr)로서, 키 기억 장치(22)로 송부한다.

이 때, 키 기억 장치(22)의 CPU(51)는, 식별 번호 KID와 신규키 Kr의 암호화 데이터 E(Kses, KID ‖ Kr)를 수취하여, 일시 키 Kses를 이용하여, 식별 번호 KID와 신규키 Kr를 복호한다. 그리고, 키 기억 장치(22)가 기억하는 도 11의 증명키표에 신규 레코드를 추가한다. 신규 레코드의 내용은, 복호된 식별 번호 KID와 신규키 Kr가 된다.

다음으로, 키 할당자 단말기(12)는, 키 할당 보고서를 작성하여, 키 기억 장치(22)로 송부하여 온다(도 25와 도 27의 단계 S25).

도 29는, 그와 같은 키 할당 보고서의 예를 도시하고 있다. 또한, 도 29의 키 할당 보고서는, 할당된 인증 방법이 공통키 인증인 경우의 형식의 것이 된다.

이 경우, 검증키와 증명키가 동일하기 때문에, 서비스 제공자 SP 이외에 키가 누설하는 것을 방지할 필요가 있다. 이 때문에, 키 할당자 단말기(12)는, 키 할당 보고서에 서비스 제공자 단말기(13)(서비스 제공자 SP)의 고유키 KSP로 암호화한 검증키도 포함시켜, 키 기억 장치(22)로 송부한다.

도 29의 키 할당 보고서에 있어서, Key-ID는, 할당된 인증 방법의 식별 번호를 나타내고 있다.

의뢰서 ID는, 금회의 인증 방법 할당의 요구를 행한 키 할당 의뢰서의 식별 번호를 나타내고 있다.

SP-ID는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있다.

유효 기한은, 할당된 인증 방법의 유효 기한을 나타내고 있다.

암호화 검증키는, 할당된 인증 방법의 검증키 Kr를 나타내고 있고, 할당을 의뢰한 서비스 제공자 단말기(13)(서비스 제공자 SP)의 고유키 KSP로 암호화된 암호화 데이터 E(KSP, Kr)의 형식을 나타내고 있다.

또한, 키 할당자 단말기(12)는, 도 5의 키 할당표에 신규 레코드를 추가한다. 신규 레코드의 내용은, 할당된 인증 방법의 식별 번호 Key-ID, 할당된 키 기억 장치(22)를 소지하는 사용자 User(IC 카드(23))의 범용 어카운트에서의 식별 번호 Acc-ID, 할당된 키 기억 장치(22)의 식별 번호 HW-ID, 할당된 서비스 제공자의 식별 번호 SP-ID, 할당된 인증 방법의 유효 기한, 서비스 내용, 및, 검증키(증명키)가 된다. 그 후, 키 할당자 단말기(12)는, 키 할당 의뢰서, 및, 키 할당 보고서를 파기한다(도 25와 도 27의 단계 S25).

도 24로 되돌아가, 키 기억 장치(22)의 CPU(51)는, 단계 S17에 있어서, 키 할당 보고서(도 25와 도 27의 단계 S25의 처리에서, 키 할당자 단말기(12)가 송부한 것)를 수취한다. 그리고, 키 기억 장치(22)의 CPU(51)는, 키 할당 보고서(도 29) 및 그것에 대응하는 키 할당 의뢰서(SP-ID와 의뢰서 ID가 일치하는 키 할당 의뢰서)(도 28)로부터, Key-ID, 유효 기한, 및, 서비스 내용을 추출하여, 키 기억 장치(22)가 기억하는 도 12의 서비스 정보표에 새로운 레코드로서 추가한다.

이 때, 후술하는 바와 같이, 키 할당자 단말기(12)는, 인증한 사용자 User(IC 카드(23))에 대하여 서비스에 적당한 과금을 행한다(도 25의 단계 S26).

키 기억 장치(22)의 CPU(51)는, 단계 S18에 있어서, 단계 S17의 처리에서 수취한 키 할당 보고서를, 서비스 제공자 단말기(13)로 송부한다. 그 후, 키 기억 장치(22)는, 키 할당 의뢰서와 키 할당 보고서를 파기한다.

후술하는 바와 같이, 서비스 제공자 단말기(13)는, 이와 같이 하여, 키 기억 장치(22)로부터 송부된 키 할당 보고서를 수취한다(도 26과 도 27의 단계 S43). 그리고, 서비스 제공자 단말기(13)는, 키 할당 보고서 및 그것에 대응하는 키 할당 의뢰서로부터, Key-ID, 유효 기한, 서비스 내용, 및, 검증키를 추출하여, 검증키를, 도 9의 인증 정보표에 새로운 레코드로서 추가한다. 그 후, 서비스 제공자 단말기(13)는, 키 할당 의뢰서와 키 할당 보고서를 파기한다.

다음으로, 도 25를 참조하여, 키 할당자 단말 장치12(도 4)의 「서비스 선택/키 할당 처리」에 대하여 설명한다.

사용자 단말기(21)는, 상술한 바와 같이, 도 24와 도 27의 단계 S11의 처리에서, 선택 서비스를 서비스 제공자 단말기(13)로 송부하면, 서비스 제공자 단말기(13)는, 후술하는 바와 같이, 이 선택 서비스를 수취하여, 키 할당 의뢰서를 작성하여, 이것을 키 기억 장치(22)로 송부한다(도 26과 도 27의 단계 S41과 S42).

그리고, 상술한 바와 같이, 도 24와 도 27의 단계 S12에 있어서, 키 기억 장치(22)는, 키 할당 의뢰서를 수취하고, 단계 S13에 있어서, 그 키 할당 의뢰서를, 키 할당자 단말기(12)로 송부한다.

그래서, 도 18의 키 할당자 단말기(12)의 CPU(81)는, 단계 S21에 있어서, 키 기억 장치(22)로부터 송부되어 온 키 할당 의뢰서 수취한다. 그리고, CPU(81)는, 그것에 포함되는 메시지 인증 코드(도 28)의 검증을 행한다. 또한, 동일 서비스 제공자로부터 과거에 동일한 의뢰서 번호의 의뢰서가 와있지 않은 것을 확인한다.

이들의 확인 후에, CPU(81)는, 단계 S22에 있어서, 「키 기억 장치와 상호 인증 + 키 공용 처리」를 실행하고, 단계 S23에 있어서, 「키 기억 장치의 사용자 인증 처리」를 실행한다.

또한, 단계 S22에 있어서의 「키 기억 장치와 상호 인증 + 키 공용 처리」는, 상술한 도 27의 단계 14에 있어서의 「키 할당자와 상호 인증 + 키 공용 처리」에서 그 상세한 설명을 했기 때문에, 여기서는 그 설명은 생략한다.

마찬가지로, 단계 S23에 있어서의 「키 기억 장치의 사용자 인증 처리」는, 상술한 도 27의 단계 15에 있어서의 「사용자 인증 응답 처리」에서 그 상세한 설명을 했기 때문에, 여기서는 그 설명은 생략한다.

그리고, CPU(81)는, 단계 S24에 있어서, 키 기억 장치(22)에 대하여, 신규키 Kr(및, 식별 번호 KID)를 생성하여, 송부한다.

상술한 바와 같이, 키 기억 장치(22)는, 도 24와 도 27의 단계 16의 처리에서, 신규키 Kr(및, 식별 번호 KID)를 수취한다.

다음으로, CPU(81)는, 단계 S25에 있어서, 키 할당 보고서를 작성하여, 키 기억 장치(22)로 송부하고, 단계 S26에 있어서, 사용자 단말기(21)(사용자 User)에 대하여 과금을 행한다.

이 때, 상술한 바와 같이, 도 24와 도 27의 단계 S17과 S18의 처리에서, 키 기억 장치(22)는, 이 키 할당 보고서를 수취하여, 서비스 제공자 단말기(13)로 송부한다. 서비스 제공자 단말기(13)는, 후술하는 바와 같이, 그 키 할당 보고서를 수취한다(도 26과 도 27의 단계 S43의 처리).

다음으로, 도 26을 참조하여, 서비스 제공자 단말기(13)(도 4)의 「서비스 선택/키 할당 처리」에 대하여 설명한다.

상술한 바와 같이, 도 24와 도 27의 단계 S11의 처리에서, 사용자 단말기(21)는, 선택 서비스를, 서비스 제공자 단말기(13)로 송신하여 온다.

구체적으로는, 이 예에 있어서는, 상술한 바와 같이, 도 19의 서비스 제공자 단말기(13)의 기억부(108)에는, 제공하는 서비스의 리스트 등을 실은 홈페이지(데이터)가 기억되어 있다.

그래서, 사용자 단말기(21)에 의해 액세스된 경우, CPU(101)는, 이 홈페이지를 사용자 단말기(21)의 브라우저 상에 제시한다.

사용자 User는, 상술한 바와 같이, 사용자 단말기(21)를 통하여 제시된 홈페이지를 열람하여, 선택 서비스를 선택하면, 사용자 단말기(21)는, 그 선택 서비스를 송부하여 온다.

그래서, CPU(101)는, 단계 S41에 있어서, 그 선택 서비스를 수취하고, 단계 S42에 있어서, 키 할당 의뢰서를 생성하여, 사용자 단말기(21)로 송부한다.

그 후, 상술한 바와 같이, 사용자 단말기(21)가, 도 24와 도 27의 단계 S12 내지 S17의 처리를 실행한 후, 단계 S18의 처리에서, 키 할당 보고서를, 서비스 제공자 단말기(13)로 송부하여 온다.

그래서, CPU(101)는, 단계 S43에 있어서, 키 할당 보고서를 수취한다. 그리고, CPU(101)는, 키 할당 보고서 및 그것에 대응하는 키 할당 의뢰서로부터, Key-ID, 유효 기한, 서비스 내용, 및, 검증키를 추출하여, 검증키를, 도 9의 인증 정보표에 새로운 레코드로서 추가한다. 그 후, CPU(81)는, 키 할당 의뢰서와 키 할당 보고서를 파기한다.

다음으로, 도 30과 도 31의 흐름도와, 도 32 내지 도 35의 애로우 차트를 참조하여, 본 발명의 제1 실시 형태가 적용되는 인증키 할당 시스템(1)의 동작 중의, 「키 사용/서비스 제공 처리(도 23의 단계 S2의 처리)」에 대하여 설명한다. 도 30은, 사용자 장치(11)(도 4)의 「키 사용/서비스 제공 처리」를 도시하고 있다. 도 31은, 서비스 제공자 단말기(13)(도 4)의 「키 사용/서비스 제공 처리」를 도시하고 있다.

처음에, 도 30을 참조하여, 사용자 장치(11)(도 4)의 「키 사용/서비스 제공 처리」에 대하여 설명한다.

키 기억 장치(22)의 CPU(51)(도 16)는, 단계 S61에 있어서, 서비스를 선택한다.

구체적으로는, 예를 들면, 이 예에 있어서는, CPU(51)은, 키 기억 장치(22) 자신이 기억하는 도 12의 서비스 정보표로부터 서비스 내용을, 사용자 단말기(21)에 제공하고, 사용자 단말기(21)가, 그것을, 그 디스플레이(도 15의 출력부(37))에 표시시킨다. 사용자 User는, 디스플레이에 표시된 서비스 내용의 중에서 이용하고자 하는 서비스에 대응하는 레코드를, 키보드(도 15의 입력부(36))를 조작하여, 선택한다. 사용자 단말기(21)는, 사용자 User에 의해 선택된 서비스를 검지하여, 그것을 키 기억 장치(22)에 공급한다.

그리고, CPU(51)가, 통신 처리부(57)를 통하여 그것을 취득함으로써, 서비스를 선택한다.

단계 S62에 있어서, 키 기억 장치(22)의 CPU(51)는, 서비스 요구서를 생성하여, 서비스 제공자 단말기(13)로 송부한다.

도 36은, 서비스 요구서의 예를 도시하고 있다.

또한, 이 예에 있어서는, 송부선 어드레스는 서비스 내용의 일부로서 포함되는 것으로 한다. 도 36에 있어서, Key-ID는, 사용자 User가 선택한 (단계 S61의 처리에서 선택된) 서비스에 대응하는 서비스 정보표(도 12)의 레코드의 Key-ID를 나타내고 있다.

후술하는 바와 같이, 서비스 제공자 단말기(13)는, 서비스 요구서를 수취하여, 서비스 요구서에 포함되는 Key-ID에 대응하는 검증키를, 도 9의 인증 정보표로부터 추출하고, 또한 유효 기한이 지나지 않은 것을 검사한다(도 31의 단계 S81, S82). 또한, 이러한 일련의 처리를, 이하, 검증키 선택 + 유효 기한 검사라고 칭한다.

서비스 제공자 단말기(13)는, 도 9의 인증 정보표에 Key-ID에 대응하는 레코드가 없거나, 또는 유효 기한이 지났다고 판정한 경우, 검증키 선택 + 유효 기한 검사는 불합격이라고 판정하여, 서비스 제공은 행하지 않고서 처리를 종료한다.

이것에 대하여, 서비스 제공자 단말기(13)는, 검증키 선택 + 유효 기한 검사는 합격이라고 판정한 경우, 도 31의 단계 S83으로 진행하여, 「목적별 인증의 검증 처리」를 실행한다.

이 때, CPU(51)는, 단계 63에 있어서, 서비스 제공자 단말기(13)의 단계 S83의 「목적별 인증의 검증 처리」에 대응하는 「목적별 인증의 응답 처리」를 실행한다.

단계 S63과 단계 S83의 처리의 상세 예가, 도 32와 도 33에 도시되어 있다.

그래서, 도 32와 도 33을 참조하고, 단계 S63과 단계 S83의 처리의 상세를 설명한다.

도 32는, 암호키의 공유를 행하지 않는 경우의 예를 도시하고 있다.

도 32에 있어서, 서비스 제공자 단말기(13)는, 단계 S83-1로, 난수 Ra를 생성하여, Key-ID(이하, KID라고 기술한다)와 난수 Ra의 연결 데이터 KID ‖ Ra를, 키 기억 장치(22)로 송부하여 온다.

이 때, 키 기억 장치(22)의 CPU(51)는, 단계 S63-1로, 이것을 수취하면, KID에 대응하는 증명키(도 11의 증명키표로부터 얻어지는 증명키) Kr를 선택한다. 그리고, CPU(51)는, 단계 S63-2에서, 난수 Ra를, 증명키 Kr로 암호화하여,

그 연산 결과인 암호화 데이터 E(Kr, Ra)와, KID와의 연결 데이터 KID ‖ E(Kr, Ra)를, 서비 스 제공자 단말기(13)로 송부한다(되돌려 준다).

서비스 제공자 단말기(13)는, 단계 S83-2에서, 이것을 수취하면, 암호화 데이터 E(Kr, Ra)가, 검증키 Kr로 복호할 수 있는 것(난수 Ra가 얻어지는 것)을 확인함으로써, 키 기억 장치(22)가 할당된 인증 방법의 인증키 Kr를 갖는 것을 확인한다.

이것에 대하여, 도 33은, 암호키의 공유를 행하는 경우의 예를 도시하고 있다.

도 33에 있어서, 서비스 제공자 단말기(13)는, 단계 S83-11에서, 난수 Ra를 생성하여, KID와 난수 Ra의 연결 데이터 KID ‖ Ra를, 키 기억 장치(22)로 송부하여 온다.

이 때, 키 기억 장치(22)의 CPU(51)는, 단계 S63-11로, 이것을 수취하면, 공용 키 Kses를 생성한다. 그리고, CPU(51)는, 단계 S63-12에서, KID에 대응하는 증명키(도 11의 증명키표로부터 얻어지는 증명키) Kr를 선택하여, 수취된 난수 Ra와, 새롭게 생성한 공용 키 Kses의 연결 데이터 Ra ‖ Kses를 암호화하여, 그 연산 결과인 암호화 데이터 E(Kr, Ra ‖ Kses)를, 서비스 제공자 단말기(13)로 송부한다.

서비스 제공자 단말기(13)는, 단계 S83-12로, 이것을 수취하면, 암호화 데이터 E(Kr, Ra ‖ Kses)를 검증키 Kr로 복호하여, 난수 Ra와의 일치를 확인함으로써, 키 기억 장치(22)가 할당된 인증 방법의 인증키 Kr를 갖는 것을 확인함과 함께, 공용 키 Kses를 취득한다(공용 키 Kses를 일시적인 공유 암호키로 한다).

도 30으로 되돌아가, 후술하는 바와 같이, 서비스 제공자 단말기(13)에 의해 인증이 성공되었다고 판정되면(도 31의 단계 S84), CPU(51)는, 단계 S64에 있어서, 서비스 제공자 단말기(13)로부터 제공되는 서비스를 이용하는 처리를 실행한다. 또한, 이하, 이러한 처리를, 「서비스 이용 처리」라고 칭한다. 또한, 이「서비스 이용 처리」는 필요에 따라 복수회 반복된다.

이 예의 「서비스 이용 처리」의 상세가, 도 34와 도 35에 도시되고 있다. 그래서, 도 34와 도 35를 참조하여, 이 예의 「서비스 이용 처리」의 상세에 대하여 설명한다.

도 34는, 공유키를 이용하지 않은 경우, 즉, 도 32의 「목적별 인증의 응답 처리」(단계 S63의 처리)가 실행된 경우의 「서비스 이용 처리」를 도시하고 있다.

도 34에 있어서, 키 기억 장치(22)의 CPU(51)는, 단계 S64-1에서, 요구 Cmd ‖ Parm을, 서비스 제공자 단말기(13)로 송부한다. 또한, 요구 Cmd ‖ Parm은, 서비스 요구에 대응하는 명령 Cmd와 그 인수 Parm의 연결 데이터를 나타내고 있다.

단, 목적에 따라서는, 명령 Cmd를 지정할 필요가 없는 경우도 있어, 그 경우에는, 명령 Cmd는 생략된다.

서비스 제공자 단말기(13)는, 단계 S85-1로, 요구 Cmd ‖ Parm을 수취하면, 그것에 대응하는 처리를 행하고, 단계 S85-2로, 응답 Resp을 키 기억 장치(22)에 되돌려 준다(송부한다).

CPU(51)는, 단계 S64-2에서, 응답 Resp을 수취하여, 응답 Resp로부터 요구 Cmd ‖ Parm의 결과를 얻는다.

이것에 대하여, 도 35는, 공유키를 이용하는 경우, 즉, 도 33의 「목적별 인 증의 응답 처리」(단계 S63의 처리)가 실행된 경우의 「서비스 이용 처리」를 도시하고 있다.

도 35에 있어서, 키 기억 장치(22)의 CPU(51)는, 단계 S64-11에서, 요구 Cmd ‖ Parm을 생성하여, 그것을 공용 키 Kses로 암호화하여, 그 암호화 데이터 E(Kses, Cmd ‖ Parm)를, 서비스 제공자 단말기(13)로 송부한다.

서비스 제공자 단말기(13)는, 단계 S85-11에서, 암호화 데이터 E(Kses, Cmd ‖ Parm)를 수취하면, 공용 키 Kses로 복호하여, 요구 Cmd ‖ Parm을 얻어, 그것에 대응하는 처리를 행하여, 응답 Resp을 생성한다. 그리고, 서비스 제공자 단말기(13)는, 단계 S85-12에서, 응답 Resp을, 공용 키 Kses로 암호화하여, 그 암호화 데이터 E(Kses, Resp)를 키 기억 장치(22)에 되돌려 준다(송부한다)(도 31의 단계 S85).

CPU(51)는, 단계 S64-12로, 암호화 데이터 E(Kses, Resp)를 수취하여, 그것을 공용 키 Kses로 복호하여, 그 결과를 얻는다.

또한, 후술하는 바와 같이, 도 34와 도 35의 키 기억 장치(22)의 「서비스 이용 처리(단계 S64의 처리)」에 대응하는, 서비스 제공자 단말기의 처리(단계 S85의 처리)를, 이하, 「서비스 제공 처리」라고 칭한다.

다음으로, 도 31을 참조하여, 서비스 제공자 단말기(13)(도 4)의 「키 사용/서비스 제공 처리」에 대하여 설명한다.

상술한 바와 같이, 도 30의 단계 S61과 S62의 처리에서, 키 기억 장치(22)는, 서비스를 선택하여, 그것에 대응하는 서비스 요구서를 생성하여, 서비스 제공자 단말기(13)로 송부하여 온다.

이 때, 서비스 제공자 단말기(13)의 CPU(101)(도 19)는, 단계 S81에서, 서비스 요구서를 수취하여, 상술한「검증키 선택 + 유효 기한 검사」 처리를 실행한다.

단계 S82에 있어서, CPU(101)는, 「검증키 선택 + 유효 기한 검사」가 합격인지의 여부를 판정하여, 「검증키 선택 + 유효 기한 검사」가 불합격이라고 판정한 경우(합격이 아니라고 판정한 경우), 그 처리를 종료한다.

이것에 대하여, CPU(101)는, 단계 S82에 있어서, 「검증키 선택 + 유효 기한 검사」가 합격이라고 판정한 경우, 단계 S83에 있어서, 「목적별 인증의 검증 처리」를 실행한다.

또한, 단계 S83에 있어서의 「목적별 인증의 검증 처리」는, 상술한 도 30의 단계 63에 있어서의 「목적별 인증의 응답 처리」에서 그 상세한 설명을 했기 때문에, 여기서는 그 설명은 생략한다.

단계 S84에 있어서, CPU(101)는, 단계 S83의 처리의 결과로서, 인증이 성공인지의 여부를 판정하여, 인증이 실패(성공이 아니다)라고 판정한 경우, 그 처리를 종료한다.

이것에 대하여, CPU(101)는, 단계 S84에 있어서, 인증이 성공이라고 판정된 경우, 단계 S85에 있어서, 「서비스 제공 처리」를 실행한 후, 그 처리를 종료한다.

또한, 단계 S85에 있어서의 「서비스 제공 처리」는, 상술한 도 30의 단계 64에 있어서의 「서비스 이용 처리」에서 그 상세한 설명을 했기 때문에, 여기서는 그 설명은 생략한다.

다음으로, 도 37 내지 도 39의 흐름도를 참조하여, 본 발명의 제1 실시 형태가 적용되는 인증키 할당 시스템(1)의 동작 중의, 「키 삭제 처리(도 23의 단계 S6의 처리)」에 대하여 설명한다. 도 37은, 사용자 장치(11)(도 4)의 「키 삭제 처리」를, 도 38은, 키 할당자 단말기(12)(도 4)의 「키 삭제 처리」를, 도 39는, 서비스 제공자 단말기(13)(도 4)의 「키 삭제 처리」를, 각각 도시하고 있다.

단, 도 37 내지 도 39의 각각에 도시된 바와 같이, 사용자 장치(11), 키 할당자 단말기(12), 및, 서비스 제공자 단말기(13) 각각의 「키 삭제 처리」는, 어느 것이나 마찬가지의 처리가 되기 때문에, 여기서는, 도 38을 참조하여, 키 할당자 단말기(12)의 「키 삭제 처리」에 대해서만 설명한다.

단계 S121에 있어서, 키 할당자 단말기(12)의 CPU(81)(도 18)는, 키 정리의 요구를 취득한다.

이 예에 있어서는, 예를 들면, 입력부(86) 등, 외부로부터 키 삭제를 행하는 계기(트리거)가 공급되는 것으로 하면, CPU(81)는, 이 트리거를, 키 정리의 요구로서 취득한다. 또한, 이 트리거는, 정기적으로 공급되어도 되고, 임의의 때에 공급되더라도 된다.

단계 S122에 있어서, CPU(81)는, 기억부(88)에 기억되어 있는 도 5의 키 할당표로부터, 최초의 레코드를 추출하고, 단계 S123에 있어서, 그 레코드의 유효 기한을, 현재 일시와 비교하여, 그 레코드의 키가 유효 기한 내의 것인가 아닌가를 판정한다.

CPU(81)는, 단계 S123에 있어서, 키가 유효 기한 내의 것이 아니라고 판정한 경우, 단계 S125에 있어서, 그 레코드를 삭제하고, 단계 S126에 있어서, 그 레코드(삭제한 레코드)가 최종 레코드인지의 여부를 판정한다.

이것에 대하여, CPU(81)는, 단계 S123에 있어서, 그 레코드의 키가 유효 기한 내의 것이라고 판정한 경우, 레코드를 삭제하지 않고서(단계 S125의 처리를 실행하지 않고서), 단계 S126에 있어서, 그 레코드(삭제한 레코드)가 최종 레코드인지의 여부를 판정한다.

CPU(81)는, 단계 S126에 있어서, 최종 레코드가 아니라고 판정된 경우, 단계 S124에 있어서, 다음의 레코드를 추출하고, 단계 S123의 처리로 되돌아가, 그 이후의 처리를 반복한다.

즉, CPU(81)은, 최초의 레코드로부터 최후의 레코드까지의 각 레코드의 각각에 대하여, 유효 기한 내에 있는지의 여부를 순차 판정하여, 유효 기한이 지나갔다고 판정한 레코드를 삭제해 간다. 그리고, CPU(81)는, 최후의 레코드까지의 처리(단계 S123 내지 S125의 반복하여 처리)를 종료하면, 단계 S126에 있어서, 최종 레코드라고 판정하고, 그 처리를 종료한다.

또한, 서비스 제공자 단말기(13)의 키 삭제 처리에 있어서는, 삭제의 대상이 되는 표는, 도 9의 인증 정보표가 되고, 또한, 키 기억 장치(22)의 키 삭제 처리에 있어서는, 삭제의 대상이 되는 표는, 도 12의 서비스 정보표가 된다. 그리고, 이들의 레코드가 삭제될 때, 동일한 Key-ID를 갖는 증명키표의 레코드도 삭제된다.

다음으로, 도 40과 도 41의 흐름도를 참조하여, 본 발명의 제1 실시 형태가 적용되는 인증키 할당 시스템(1)의 동작 중의, 「키 사용 정지 처리(도 23의 단계 S7의 처리)」에 대하여 설명한다. 도 40은, 키 할당자 단말기(12)(도 4)의 「키 사용 정지 처리」를 도시하고 있다. 도 41은, 서비스 제공자 단말기(13)(도 4)의 「키 사용 정지 처리」를 도시하고 있다.

처음에, 도 40을 참조하여, 키 할당자 단말기(12)의 「키 사용 정지 처리」에 대하여 설명한다.

할당 완료한 인증 방법의 실효가 필요하게 된 경우, 키 할당자 단말기(12)의 CPU(81)(도 18)는, 입력부(86)로부터의 조작자의 명령에 기초하여, 단계 S161에 있어서, 해당하는 인증 방법에 관하여 키 사용 정지 요구서를 생성하여, 서비스 제공자 단말기(13)로 송부한다.

도 42는, 그와 같은 키 사용 정지 요구서의 예를 도시하고 있다.

도 42에 도시된 바와 같이, 키 사용 정지 요구서는, 예를 들면, 사용 정지하는 인증 방법의 식별 번호 Key-ID, 사용 정지로 하는 일시 Data-time, 사용 정지하는 인증 방법의 원래의 유효 기한, 및, 이들에 대한 메시지 인증 코드로 이루어진다.

메시지 인증 코드는, 인증 방법의 할당을 받은 서비스 제공자 단말기(13)(서비스 제공자 SP)의 고유 암호키(도 6의 서비스 제공자 키표로부터 얻어지는 고유 암호키) KSP를 이용하여, 생성된 것이다. 또한, 이 예에 있어서는, 키 할당자 단말기(12)는, 할당 완료한 인증 방법에 대하여, 도 5의 키 할당표로부터, 그 할당을 받은 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호 SP-ID를 얻을 수 있는 것으로 한다.

그리고, 단계 S162에 있어서, CPU(81)는, 키 및 부속 정보를 삭제한다.

구체적으로는, CPU(81)은, 도 5의 키 할당표의 중에서, 사용 정지하는 인증 방법에 대응하는 레코드를 삭제한다.

다음으로, 도 41을 참조하여, 서비스 제공자 단말기(13)의 「키 사용 정지 처리」에 대하여 설명한다.

상술한 바와 같이, 도 40, 의 단계 S161의 처리에서, 키 할당자 단말기(12)는, 예를 들면, 도 42의 키 사용 정지 요구서를 송부하여 온다.

이 때, 단계 S181에 있어서, 서비스 제공자 단말기(13)의 CPU(101)(도 19)는, 그 키 사용 정지 요구서를 받는다. 그리고, CPU(101)는, 그 키 사용 정지 요구서의 메시지 인증 코드를 자기 자신이 갖는 고유 암호키(도 10의 서비스 제공자 고유 정보로부터 얻어지는 고유 암호키) KSPO로 확인한다. 또한, 이하, 그와 같은 처리를, 요구서 검사라고 칭한다.

단계 S182에 있어서, CPU(101)는, 요구서 검사가 합격인지의 여부를 판정하여, 요구서 검사가 합격이라고 판정한 경우, 단계 S183에 있어서, 키 및 부속 정보를 삭제하고, 그 처리를 종료한다.

구체적으로는, CPU(101)은, 지정된 식별 번호 Key-ID의 인증 방법에 대응하는 레코드를, 도 9의 인증 정보표로부터 삭제한다.

이것에 대하여, 단계 S182에 있어서, CPU(101)는, 요구서 검사가 불합격(합격이 아니다)이라고 판정한 경우, 단계 S183의 처리를 실행하지 않고서(키 및 부속 정보를 삭제하지 않고서), 그 처리를 종료한다.

도 43은, 키 사용 정지 요구서의 다른 예를 도시하고 있다. 이 키 사용 정지 요구서는, 제2 실시 형태로 사용되는 것이다. 따라서, 도 43의 키 사용 정지 요구서는, 제2 실시 형태에 있어서 설명한다.

(제2 실시 형태)

도 44는, 본 발명의 제2 실시 형태가 적용되는 인증키 할당 시스템(201)의 구성예를 도시하고 있고, 도 4의 인증키 할당 시스템(1)에 대응하는 부분에는, 대응하는 부호가 붙이고 있다.

이 구성예에 있어서는, 도 4의 범용 어카운트 관리자 단말기(15) 대신에, 인증 센터 단말기(211)가, 네트워크(14)에 또한(더욱) 접속되어 있다.

도 45는, 인증 센터 단말기(211)의 구성예를 도시하고 있다.

도 45에 있어서, CPU221 내지 리무버블 기록 매체231의 각각은, 도 15의 사용자 단말기(21)의 CPU(31) 내지 리무버블 기록 매체(41)의 각각과, 마찬가지의 구성이 되기 때문에, 이들의 설명은 생략한다.

즉, 제2 실시 형태에 있어서는, 도 2에 도시된 바와 같이, 참가자가, 키 할당자 KA, 인증 센터 CA, 사용자 User, 및, 서비스 제공자 SP가 되어, 이하의 예에서는, 사용자 User, 키 할당자 KA, 서비스 제공자 SP에 의해 생성된 전자 서명이, 공개키 인증 기반에 의해서 검증된다.

단, 키 할당자 단말기(12)(키 할당자 KA)와, 서비스 제공자 단말기(13)(서비스 제공자 SP)와의 사이에서는, 서로의 증명서의 실효 상황을 미리 파악하고 있는 것으로 하여(정기적으로 관계하는 CRL을 수집하는 것으로 하여), 실효 상황의 검증 이 필요한 것은, IC 카드(23)(사용자 User)에 관해서 만이라고 한다.

도 46 내지 도 50은, 키 할당자 단말기(12)가 기억하는 데이터의 예를 도시하고 있다.

즉, 이 예에 있어서는, 예를 들면, 키 할당자 단말기(12)의 메모리(도 18의 기억부(88) 등)에는, 도 46에 도시되는 것 같은 키 할당표, 도 47에 도시되는 것 같은 서비스 제공자 키표, 도 48에 도시되는 것 같은 키 기억 장치 키표, 도 49에 도시되는 것 같은 키 할당자 PKI 정보, 및, 도 50에 도시되는 것 같은 CA 공개키 정보가 기록되어 있다.

이 예에 있어서는, 예를 들면, 도 46의 키 할당표, 도 47의 서비스 제공자 키표, 도 48의 키 기억 장치 키표의 각각은, 대응하는 Key-ID, SP-ID, 또는, HW-ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 46의 키 할당표에 있어서, 각 행의 레코드의 각각은, 할당이 행해진 인증 방법에 대응하고 있다.

Key-ID는, 할당된 인증 방법의 식별 번호를 나타내고 있어, 일의적이 되도록 할당된다.

Acc-ID는, 인증 방법의 할당 시에 지불을 한 사용자 단말기(21)(사용자 User)의 공개키 인증 기반에서의 식별 번호를 나타내고 있다.

HW-ID는, 인증 방법이 할당된 키 기억 장치(22)의 식별 번호를 나타내고 있다.

증명키는, 인증 방법의 증명키(공개키 암호의 비밀키)를 나타내고 있다.

키 할당 의뢰서와 키 할당 보고서의 각각은, 이 레코드에 대응하는 인증 방법의 할당을 의뢰한 서비스 제공자 단말기(13)(서비스 제공자 SP)로부터 발행된 키 할당 의뢰서, 그것에 대하여 키 할당자 단말기(12)(키 할당자 KA)가 발행한 키 할당 보고서의 각각을 나타내고 있다.

키 할당 의뢰서의 예가, 도 51에, 키 할당 보고서의 예가, 도 52에, 각각 도시되고 있다.

도 51의 키 할당 의뢰서에 있어서, 의뢰서 ID는, 이 키 할당 의뢰서를 발행한 서비스 제공자 단말기(13)(서비스 제공자 SP)가, 일의적이 되도록 부가하는 키 할당 의뢰서의 식별 번호를 나타내고 있다.

유효 기한은, 이 키 할당 의뢰서로 할당을 의뢰하는 인증 방법에 필요한 유효 기한을 나타내고 있다.

SP-ID는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있고, 서비스 제공자 단말기(13)(서비스 제공자 SP)가 키 할당자 단말기(12)(키 할당자 KA)과의 계약 시에 정한 것이다.

서비스 내용은, 이 인증 방법에서 인증되는 사용자 User(사용자 단말기(21))에 제공되는 서비스(사용자 User에 의해 선택된 서비스)의 내용을 나타내고 있다.

SP 전자 서명은, 키 할당 의뢰서의 개찬의 방지와, 키 할당 의뢰서가 서비스 제공자 단말기(13)(서비스 제공자 SP)에 의해서 생성된 것인 것을 증명할 목적으로, 서비스 제공자 단말기(13)에 의해서 키 할당 의뢰서 전체에 대하여 생성된

전자 서명을 나타내고 있다.

도 52의 키 할당 보고서에 있어서, Key-ID는, 인증 방법의 식별 번호를 나타내고 있다.

의뢰서 ID와 SP-ID의 각각은, 인증 방법의 할당을 요구한 키 할당 의뢰서의 식별 번호, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호의 각각을 나타내고 있다.

SP-Acc-ID는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 공개키 인증 기반에서의 식별 번호를 나타내고 있다.

유효 기한은, 할당된 인증 방법의 유효 기한을 나타내고 있다.

검증키는, 할당된 인증 방법의 검증키(공개키 암호의 공개키)를 나타내고 있다.

KA 전자 서명은, 키 할당 보고서의 개찬의 방지와, 키 할당 보고서가 키 할당자 단말기(12)(키 할당자 KA)에 의해서 생성된 것인 것을 증명할 목적으로, 키 할당자 단말기(12)(키 할당자 KA)에 의해서 키 할당 보고서 전체에 대하여 부가된 전자 서명을 나타내고 있다.

도 47의 서비스 제공자 키표에 있어서, 각 레코드는, 키 할당자 단말기(12)(키 할당자 KA)와 계약을 체결한 서비스 제공자 단말기(13)(서비스 제공자 SP)를 도시하고 있다.

SP-ID는, 계약을 체결한 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있어, 계약 체결 시에 일의적이 되도록 할당된다.

SP-address는, 서비스 제공자 단말기(13)의 연락처 어드레스(URL 등)를 나타 내고 있다. 이것은, 인증 방법의 실효가 발생했을 때나 조회 시의 연락처가 된다.

SP-Acc-ID는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 공개키 인증 기반에서의 식별 번호를 나타내고 있다.

도 48의 키 기억 장치 키표는, 도 7의 키 기억 장치표와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 49의 키 할당자 PKI 정보는, 키 할당자 단말기(12)가, 공개키 인증 기반으로 검증할 수 있는 전자 서명을 생성하기 위한 정보를 나타내고 있어, 증명서와 비밀키로 구성된다. 증명서에 대해서는, 도 66을 참조하여, 인증 센터 단말기(211)(인증 센터 CA)에 대응하는 것과 함께 후술한다.

도 50의 CA 공개키 정보는, 공개키 인증 기반의 인증 센터 CA(인증 센터 단말기(211))의 공개키를 나타내고 있고, 인증 센터 단말기(211)(인증 센터 CA)가 발행한 증명서의 검증을 행할 때에 이용된다.

도 53 내지 도 58은, 서비스 제공자 단말기(13)가 기억하는 데이터의 예를 도시하고 있다.

즉, 이 예에 있어서는, 예를 들면, 서비스 제공자 단말기(13)의 메모리(도 19의 기억부(108) 등)에는, 도 53에 도시되는 것 같은 인증 정보표, 도 54에 도시되는 것 같은 서비스 제공자 고유 정보, 도 55에 도시되는 것 같은 실효키표, 도 56에 도시되는 것 같은 서비스 제공자 PKI 정보, 도 57에 도시되는 것 같은 키 공용 파라미터, 및, 도 58에 도시되는 것 같은 CA 공개키 정보가 기억되어 있다.

이 예에 있어서는, 예를 들면, 도 53의 인증 정보표와 도 55의 실효키표의 각각은, Key-ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 53의 인증 정보표에 있어서, 각 레코드는, 할당을 받은 인증 방법에 대응한다.

Key-ID는, 인증 방법의 식별 번호를 나타내고 있다.

키 할당 의뢰서는, 인증 방법의 할당을 의뢰했을 때에 생성한 도 51의 키 할당 의뢰서를 나타내고 있다.

키 할당 보고서는, 의뢰한 키 할당이 행해졌을 때에, 키 할당자 단말기(12)(키 할당자 KA)로부터 발행된 도 52의 키 할당 보고서를 나타내고 있다.

도 54의 서비스 제공자 고유 정보에 있어서, SP-ID는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의, 키 할당자 단말기(12)(키 할당자 KA)와의 키 할당 계약의 체결 시에 할당된 식별 번호를 나타내고 있다.

도 55의 실효키표는, 키 할당자 단말기(12)(키 할당자 KA)로부터 키 사용 정지 요구가 있었던 인증 방법의 Key-ID와, 그 인증 방법의 본래의 유효 기한을 등록하는 표가 된다.

도 56의 서비스 제공자 PKI 정보는, 서비스 제공자 단말기(13)(서비스 제공자 SP)가, 공개키 인증 기반으로 검증할 수 있는 전자 서명을 생성하기 위해서 정보를 나타내고 있어, 증명서와 비밀키로 이루어진다.

도 57의 키 공유 파라미터에 있어서, p, g의 각각은, Diffie-Hellman 방식의 키 공유를 위한 파라미터를 나타내고 있다. 보다 구체적으로는, 파라미터 p는, 큰 소수라고 되고, 이 때 파라미터 p를 법으로 하는 잉여류의 0을 제외하는 요소는 곱 셈군을 이루고, 그 원시원(위 수가 p-1인 원)의 1개가 파라미터 g가 된다.

도 58의 CA 공개키 정보는, 공개키 인증 기반의 인증 센터CA(인증 센터 단말기(211))의 공개키를 나타내고 있어, 인증 센터 단말기(211)가 발행한 증명서의 검증을 행할 때에 이용된다.

도 59 내지 도 63은, 키 기억 장치(22) 또는 IC 카드(23)(사용자 User)가 기억하는 데이터의 예를 도시하고 있다.

즉, 이 예에 있어서는, 예를 들면, 키 기억 장치(22)의 데이터 기억부(53) 또는 키 기억부(54)(도 16), 또는, IC 카드(23)의 기억부(71)에는, 도 59에 도시되는 증명키표, 도 60에 도시되는 것 같은 인증 정보표, 도 61에 도시되는 것 같은 키 기억 장치 고유 정보, 도 62에 도시되는 것 같은 사용자 PKI 정보, 및, 도 63에 도시되는 것 같은 CA 공개키 정보가 기억되어 있다.

이 예에 있어서, 예를 들면, 도 59의 증명키표와 도 60의 인증 정보표는 모두, Key-ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 59의 증명키표와 도 60의 인증 정보표의 각각의 각 레코드는, 키 기억 장치(22)(사용자 User)가, 키 할당자 단말기(12)(키 할당자 단말기 KA)로부터 할당된 인증 방법에 대응한다.

도 59와 도 60의 Key-ID의 각각은, 인증 방법의 식별 번호를 나타내고 있다.

도 59의 증명키표의 증명키는, 인증 방법의 증명키를 나타내고 있어, 공개키 암호의 비밀키가 된다.

도 60의 인증 정보표에 있어서, 키 할당 의뢰서는, 키 기억 장치(22)(사용자 User)가, 인증 방법의 할당을 의뢰할 때에 서비스 제공자 단말기(13)(서비스 제공자 SP)로부터 수취하여, 키 할당자 단말기(12)(키 할당자 KA)에 제출한 도 51의 키 할당 의뢰서를 나타내고 있다.

키 할당 보고서는, 키 기억 장치(22)(사용자 User)가 의뢰한 키 할당이 행해졌을 때에, 키 할당자 단말기(12)(키 할당자 KA)로부터 발행된 도 52의 키 할당 보고서를 나타내고 있다.

도 61의 키 기억 장치 고유 정보는, 도 13의 키 기억 장치 고유 정보와 동일한 구성이 되기 때문에, 그 설명은, 생략한다.

도 62의 사용자 PKI 정보는, 사용자 User가 IC 카드(23)를 사용하여, 공개키 인증 기반으로 인증을 받기 위해서 필요한 정보를 나타내고 있고, 증명서와 비밀키로 이루어진다.

도 63의 CA 공개키 정보는, 공개키 인증 기반의 인증 센터 CA(인증 센터 단말기(211))의 공개키를 나타내고 있어, 인증 센터 단말기(211)(인증 센터 CA)가 발행한 증명서의 검증을 행할 때에 이용된다.

구체적으로는, 도 16의 키 기억부(54)가, 도 59의 증명키표와, 도 61의 키 기억 장치 고유 정보를 기억한다. 데이터 기억부(53)가, 도 60의 인증 정보표와 도 63의 CA 공개키 정보를 기억한다. 데이터 관리부(55)는, 키 할당자 단말기(12)(키 할당자 KA)로부터 송부된 정보나, 도 60의 인증 정보표의 키 할당 보고서의 유효 기한에 따라서, 키 기억부(54)와 데이터 기억부(53)에 기억되어 있는 데이터에 대하여, 내용의 추가 또는 삭제를 행한다.

도 62의 사용자 PKI 정보는, 키 기억 장치(22)에 접속되는 IC 카드(23)(기억부(71)(도 17))에 기억된다. 이 예에 있어서는, 키 기억 장치(22)는, 예를 들면, IC 카드(23)가 그 인증 처리부(58)(도 16)에 접속되어 있는 경우, IC 카드(23)에 대하여, 도 62의 사용자 PKI 정보를 이용하는 암호화, 및, 복호의 계산, 및, 증명서의 제공을 의뢰할 수 있다.

도 64와 도 65는, 인증 센터 단말기(211)가 기억하는 데이터의 예를 도시하고 있다.

즉, 이 예에 있어서는, 예를 들면, 인증 센터 단말기(211)의 메모리(도 45의 기억부228 등)에는, 적어도, 새로운 증명서를 발행하기 위한, 도 65에 도시되는 것 같은 CA 키 정보, 및, 발행 완료 증명서를 관리하는, 도 64에 도시되는 것 같은 증명서표가 기억되어 있다.

도 65의 CA 키 정보는, CA 비밀키와 CA 공개키로 이루어진다.

CA 공개키는, 공개되어, 서비스 제공자 단말기(13)(서비스 제공자 SP), 키 할당자 단말기(12)(키 할당자 KA), 또는, 키 기억 장치(11)(사용자 User) 등의, 인증키 할당 시스템(201)의 참가자에 의해 기억되는 공개키를 나타내고 있다.

이 예에 있어서는, 예를 들면, 도 64의 증명서표는, Acc-ID와 증명서 ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 64의 증명서표에 있어서, 각 레코드는, 인증 센터 단말기(211)(인증 센터 CA)의 발행 완료한 유효인 증명서에 대응한다.

Acc-ID는, 공개키 인증 기반에서의 엔티티(이 예 경우에는, 키 기억 장치(22)(사용자 User), 서비스 제공자 단말기(13)(서비스 제공자 SP), 및, 키 할당자 단말기(12)(키 할당자 KA))의 식별 번호를 나타내고 있고, 일의적으로 할당되어 있다.

증명서는, 증명서의 데이터의 내용을 나타내고 있고, 증명서 ID는, 증명서의 식별 번호를 나타내고 있다.

도 66은, 인증 센터 단말기(211)(인증 센터 CA)로부터 발행되는 증명서의 예를 도시하고 있다.

도 66의 증명서에 있어서, Acc-ID는, 공개키 인증 기반에서의 사용자(이 경우, IC 카드(23)(사용자 User) 이외에, 서비스 제공자 단말기(13)(서비스 제공자 SP)와 키 할당자 단말기(12)(키 할당자 KA))도 포함된다)의 식별 번호를 나타내고 있다.

유효 기한은, 증명서의 유효 기한을 나타내고 있다.

증명서 ID는, 증명서의 식별 번호를 나타내고 있다.

공개키는, 이 증명서에 의해서 Acc-ID의 사용자와 관계 지워진 공개키를 나타내고 있다(즉, Acc-ID의 사용자는 공개키 Kpub0과 대응하는 비밀키를 기억하는 IC 카드를 갖는다).

부속 정보는, Acc-ID의 사용자에게 관한 그 밖의 정보를 나타내고 있다.

CA 서명은, 증명서의 데이터 전체에 대하여 인증 센터 단말기(211)(인증 센터 CA)가 생성한 전자 서명을 나타내고 있다.

다음으로, 본 발명의 제2 실시 형태가 적용되는 인증키 할당 시스템(201)의 동작을 설명한다.

인증키 할당 시스템(201)의 동작의 개략은, 본 발명의 제1 실시 형태가 적용되는 인증키 할당 시스템(1)의 그것과 기본적으로 마찬가지이다.

따라서, 인증키 할당 시스템(201)의 동작도, 도 23의 흐름도를 참조하여 설명한다.

처음에, 단계 S1에 있어서, 「서비스 선택/키 할당 처리」가 실행된다.

제2 실시 형태에 있어서의 「서비스 선택/키 할당 처리」의 처리의 흐름은, 제1 실시 형태의 그것과, 기본적으로 같게 된다. 즉, 제2 실시 형태에 있어서의 「서비스 선택/키 할당 처리」는, 상술한 도 27의 애로우 차트에 따라서 실행된다.

그래서, 여기서는, 제1 실시 형태에 있어서 설명한 처리에 대해서는, 그 설명을 적절하게 생략하여, 이하, 도 27의 애로우 차트를 참조하여, 제1 실시 형태와는 다른 처리를 중심으로 설명한다.

도 27에 도시된 바와 같이, 처음에, 단계 11에 있어서, 사용자 단말기(21)는, 서비스(선택 서비스)를 선택하여, 그것을 서비스 제공자 단말기(13)로 송부한다.

서비스 제공자 단말기(13)는, 단계 S41에 있어서, 그 통지를 수취하고, 단계 S42에 있어서, 도 51의 키 할당 의뢰서를 생성하여, 키 기억 장치(22)로 송부한다.

키 기억 장치(22)는, 단계 S12에 있어서, 이것을 수취하여, 일시적으로 기억함과 동시에, 단계 S13에 있어서, 키 할당자 단말기(12)로 송부한다.

키 할당자 단말기(12)는, 단계 S21에 있어서, 이것을 수취하면, 키 할당 의 뢰서의 서비스 제공자 단말기(13)의 전자 서명을 검증한다. 구체적으로는, 도 51의 키 할당 의뢰서와 함께, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 증명서도 보내어진다.

제2 실시 형태에 있어서의 단계 S22의 처리(「키 기억 장치와 상호 인증 + 키 공유 처리」), 및, 단계 S14의 처리(「키 할당자와 상호 인증 + 키 공유 처리」)는, 상술한 제1 실시 형태에 있어서의 이들과 마찬가지가 되기 때문에, 이들의 설명은 생략한다.

이것에 대하여, 제2 실시 형태에 있어서의 단계 S23의 처리(「키 기억 장치의 사용자 인증 처리」), 및, 단계 S15의 처리(사용자 인증 응답 처리))는, 도 27에 도시되는 처리, 즉, 제1 실시 형태에 있어서의 이들의 처리와 서로 다르다.

이들의 제2 실시 형태에 있어서의 단계 S23의 처리(「키 기억 장치의 사용자 인증 처리」), 및, 단계 S15의 처리(사용자 인증 응답 처리))의 상세가, 도 67에 도시되고 있다.

그래서, 도 67을 참조하여, 제2 실시 형태에 있어서의 단계 S23의 처리(「키 기억 장치의 사용자 인증 처리」), 및, 단계 S15의 처리(사용자 인증 응답 처리))의 상세를 설명한다.

도 67에 도시된 바와 같이, 처음에, 키 기억 장치(22)(사용자 장치(11))는, 단계 S15-11에서, 도 66의 증명서의 식별 번호 CID(증명서 ID)를 포함하는 데이터 OCSP_REQ를, 인증 센터 단말기(211)로 송부한다.

구체적으로는, 키 기억 장치(22)(사용자 장치(11))는, 인증 센터 단말기(211)에 대하여, 키 기억 장치(22)에 접속되어 있는 IC 카드(23)로부터 얻어지는 사용자의 증명서의 실효 상황을, OCSP 프로토콜(RFC2560)에 의해서 조회한다.

인증 센터 단말기(211)는, 단계 S191에서, 데이터 OCSP_REQ를 수취하면, 식별 번호 CID에 대응하는 증명서의 유효성을 검사하여(식별 번호 CID의 증명서가 도 64의 증명서표에 포함되는 것을 확인하여), 검사 결과 OCSP_REP를 키 기억 장치(22)로 송부한다.

구체적으로는, 인증 센터 단말기(211)는, 식별 번호 CID, 및, 증명서의 상태 status(VALID/INVALID/UNKNOWN)로 분류한다.

또한, 증명서의 상태 status(VALID/INVALID/UNKNOWN)는, 인증 센터 단말기(211)가 발행한 증명서가 아니면 UNKNOWN을 되돌려 주고, 도 64의 증명서표에 일치하는 증명서 식별 번호의 레코드가 있으면 VALID를 되돌려 주고, 도 64의 증명서표에 일치하는 증명서 식별 번호의 레코드가 없으면 INVALID를 되돌려 주는 함수가 된다.

인증 센터 단말기(211)는, 단계 S192로, 검사 결과 OCSP_REP로서, 데이터 CID ‖ status ‖ time ‖ Sig(CID ‖ status ‖ time)을 생성하여, 키 기억 장치(22)로 송부한다.

또한, 분류한 식별자 번호 CID 및 증명서의 상태 status, 및, 검사를 행한 시각 time를 연결한 데이터가 CID ‖ status ‖ time가 되고, 또한, 그것에 대하는 인증 센터 CA(인증 센터 단말기(211))의 전자 서명이 Sig(CID ‖ status ‖ time)가 된다.

키 기억 장치(22)는, 단계 S15-12에서, 검사 결과 OCSP_REP를 수취하면, 단계 S15-13로, 그 검사 결과OCSP_REP와, 접속되어 있는 IC 카드(23)로부터 얻어지는 사용자의 증명서 CERTb를, 키 할당자 단말기(12)로 송부한다.

키 할당자 단말기(12)는, 단계 S23-11로, 이들을 수취하면, 사용자의 증명서 CERTb에서 공개키를 추출하여, 검사 결과 OCSP_REP를 확인한다. 즉, 키 할당자 단말기(12)는, 검사 결과OCSP_REP와 CERTb의 전자 서명을 검증하여, 사용자 User(IC 카드(23))의 증명서가 유효인 것을 확인한다.

또한, 여기서는 사용자의 증명서의 실효 상황을 키 기억 장치(22)가, OCSP 프로토콜을 사용하여 취득하는 경우의 예에 대하여 설명했지만, 이 예에 한정되지 않고, 예를 들면, 사용자 User(키 기억 장치(22))로부터는, 사용자의 증명서만을 키 할당자 단말기(12)에 보내어, 키 할당자 단말기(12)가 동일한 프로토콜을 사용하여, 증명서의 실효 상황을 취득하도록 해도 된다.

그리고, 키 할당자 단말기(12)는, 단계 S23-12로, 난수 Ra를 생성하여, 키 기억 장치(22)로 송부한다.

키 기억 장치(22)는, 단계 S15-14에서, 난수 Ra를 수취하면, 단계 S15-15에서, 접속되어 있는 IC 카드(23)에, 사용자 User의 비밀키를 이용하여, 난수 Ra에의 전자 서명 Sig(Ra)을 연산시킨다. 그리고, 키 기억 장치(22)는, 난수 Ra와 전자 서명 Sig(Ra)을 연결한 데이터 Ra ‖ Sig(Ra)를, 키 할당자 단말기(12)로 송부한다.

키 할당자 단말기(12)는, 단계 S23-13에서, 데이터 Ra ‖ Sig(Ra)를 수취하면, 그 속의 전자 서명 Sig(Ra)을 추출하여, 이미 유효성의 검증이 끝난 증명서에 포함 되는 공개키로 검증한다. 그 검증 결과가 옳은 결과인 경우, 키 할당자 단말기(12)는, 사용자 User(IC 카드(23))의 Acc-ID를 특정할 수 있게 된다.

도 27로 되돌아가, 단계 S24에 있어서, 키 할당자 단말기(12)는, 키 기억 장치(22)에 할당하는 인증 방법의 식별 번호 KID를 결정하여, 적당한 방법으로 난수로부터 공개키 암호의 비밀키와 공개키의 쌍(Kpr, Kpub)을 새롭게 생성한다. 이 키쌍(Kpr, Kpub)이, 새롭게 할당되는 인증 방법의 증명키 및 검증키로서 이용된다. 그리고, 키 할당자 단말기(12)는, 식별 번호 KID와 증명키(신규키) Kpr를, 키 기억 장치(22)로 송부한다.

구체적으로는, 키 할당자 단말기(12)는, 상술한 키 기억 장치(22)와 공유하고 있는 일시 키 Kses를 이용하여, 식별 번호 KID와 증명키(신규키) Kpr를 암호화 데이터 E(Kses, KID ‖ Kpr)로서, 그것을, 키 기억 장치(22)에 보낸다.

키 기억 장치(22)는, 단계 S16에 있어서, 암호화 데이터 E(Kses, KID ‖ Kpr)를 수취하여, 일시 키 Kses를 이용하여 식별 번호 KID와 증명키(신규키) Kpr를 복호한다. 그리고, 키 기억 장치(22)는, 자신이 기억하는 도 59의 증명키표에 새로운 레코드를 추가한다.

또한, 키 할당자 단말기(12)는, 단계 S25에 있어서, 도 52의 키 할당 보고서를 생성하여, 키 기억 장치(22)로 송부한다.

동시에, 키 할당자 단말기(12)는, 도 46의 키 할당표에, 할당을 행한 인증 방법의 일의적인 식별 번호 KID, 증명키 Kpr, 할당한 상대의 사용자의 식별 번호 AID, 할당한 키 기억 장치의 식별 번호 HWID, 키 할당 의뢰서 App, 및, 키 할당 보고서 Rep로 이루어지는 레코드를 추가한다.

그리고, 키 할당자 단말기(12)는, 단계 S26(도 25)에 있어서, 식별 번호 AID의 (IC 카드(23)를 소유하는) 사용자 User에 대하여 과금을 행한다.

키 기억 장치(22)는, 단계 S17에 있어서, 도 52의 키 할당 보고서를 수취하면, 단계 S18에 있어서, 그것을 서비스 제공자 단말기(13)로 송부한다.

동시에, 키 기억 장치(22)는, 도 60의 인증 정보표에, 할당된 인증 방법의 식별 번호, 이미 서비스 제공자로부터 수취하여 완료한 키 할당 의뢰서, 및, 키 할당 보고서로 이루어지는 레코드를 추가한다.

서비스 제공자 단말기(13)는, 단계 S43에 있어서, 키 할당 보고서를 수취한다. 그리고, 서비스 단말기(13)는, 키 할당 보고서에 포함되는 키 할당자의 서명을 검증한다. 서비스 제공 단말기(13)는, 그 검증에 성공하면, 인증 방법의 식별 번호, 이미 송부한 키 할당 의뢰서, 및, 수취한 키 할당 보고서로 이루어지는 레코드를 도 53의 인증 정보표에 추가한다.

도 23으로 되돌아가, 단계 S1의 처리(「서비스 선택/키 할당 처리」)가 실행되면, 단계 S2에 있어서, 「키 사용/서비스 제공 처리」가 실행된다.

제2 실시 형태에 있어서의 「키 사용/서비스 제공 처리」의 상세가, 도 68과 도 69의 흐름도에 도시되고 있다. 그래서, 도 68과 도 69의 흐름도를 참조하여, 제2 실시 형태에 있어서의 「키 사용/서비스 제공 처리」의 상세를 설명한다.

도 68은, 사용자 장치(11)(도 44)의 「키 사용/서비스 제공 처리」를 도시하고 있다. 도 69는, 서비스 제공자 단말기(13)(도 44)의 「키 사용/서비스 제공 처 리」를 도시하고 있다.

처음에, 도 68을 참조하여, 사용자 장치(11)의 「키 사용/서비스 제공 처리」에 대하여 설명한다.

키 기억 장치(22)(구체적으로는, CPU(51)(도 16))는, 단계 S201에 있어서, 서비스를 선택한다.

예를 들면, 이 예에 있어서는, 키 기억 장치(22)는, 자기 자신이 기억하는 도 60의 서비스 정보표로부터 서비스 내용을, 사용자 단말기(21)의 디스플레이(출력부(37)(도 15))에 표시시키는 등을 하여, 그 안에서 이용하고자 하는 서비스에 대응하는 레코드를 사용자 User에 선택시킴으로써 서비스를 선택한다.

단계 S202에 있어서, 키 기억 장치(22)는, 선택된 레코드의 키 할당 의뢰서와, 키 할당 보고서(이하, 키 할당 의뢰서 + 키 할당 보고서라고 기술한다)를, 서비스 제공자 단말기(13)로 송부한다. 또한, 이 예에 있어서는, 송부처는, 예를 들면, 권리증서의 서비스 내용에 포함되어 있는 것으로 한다.

후술하는 바와 같이, 서비스 제공자 단말기(13)는, 키 할당 의뢰서 + 키 할당 보고서를 수취한다. 그리고, 서비스 제공자 단말기(13)는, 키 할당 의뢰서 + 키 할당 보고서를 검사한다.

이 검사는, 키 할당 의뢰서가, 도 51의 형식으로서 옳은가 아닌가의 판정, 할당 보고서가, 도 52의 형식으로서 옳은가 아닌가의 판정, 전자 서명의 검증, 키 할당 의뢰서에 포함되는 의뢰서 ID와 SP」 D가 키 할당 보고서에 포함되는 것과 일치하는가 아닌가의 판정, 및, 서비스 제공자 단말기(13)가 기억하는 도 55의 실효 키표 중에, 키 할당 보고서에 기술되어 있는 Key-ID가 포함되는 가 아닌가의 판정이 된다. 이들 모든 검사에 성공한 경우에는, 서비스 제공자 단말기(13)는, 키 할당 의뢰서로부터 제공하여야 할 서비스와 인증 방법(검증키) Kpub를 얻는다. 이하, 이러한 일련의 처리를, 의뢰서 보고서 검사 + 검증키 추출이라 칭한다.

서비스 제공자 단말기(13), 는, 의뢰서 보고서 검사 + 검증키 추출에 성공하면, 「목적별 인증의 검증 처리」를 실행한다(도 69의 단계 S221 내지 S223).

이 때, 키 기억 장치(22)는, 단계 S203에 있어서, 이 목적별 인증의 검증 처리에 대응하는 「목적별 인증 응답 처리」를 실행한다.

즉, 키 기억 장치(22)(사용자 User)와 서비스 제공자 단말기(13)(서비스 제공자 SP)의 사이에서 할당된 인증 방법에서의 인증이 행하여진다.

이 제2 실시 형태에 있어서의 「목적별 인증 응답 처리」의 상세가, 도 70과 도 71에 도시되고 있다.

그래서, 도 70과 도 71을 참조하여, 제2 실시 형태에 있어서의 「목적별 인증 응답 처리」의 상세에 대하여 설명한다.

도 70은, 키 기억 장치(22)와 서비스 제공자 단말기(13)가 대응하는 검증키 Kpub와 증명키 Kpr를 갖는 경우의 공개키 인증을 행하는 수순이 도시되고 있다(「목적별 인증의 검증 처리」와 「목적별 인증 응답 처리」의 대응이 도시되고 있다).

도 70에 도시된 바와 같이, 서비스 제공자 단말기(13)는, 단계 S223-1에서, 난수 Ra를 생성하여, 그 난수 Ra와 Key-ID(이하, KID라고 기술한다)와의 연결 데이 터 KID ‖ Ra를, 키 기억 장치(22)로 송부한다.

키 기억 장치(22)는, 단계 S203-1에서, 데이터 KID ‖ Ra를 수취하면, KD와 난수 Ra의 각각을 추출하여, KID에 대응하는 증명키(도 59의 증명키표로부터 얻어지는 증명키) Kpr를 선택한다. 그리고, 키 기억 장치(22)는, 난수 Ra에, 증명키 Kpr에서 전자 서명 Sig(Ra)=D(Kpr, h(Ra))를 생성한다.

키 기억 장치(22)는, 단계 S203-2에서, 그 전자 서명 Sig(Ra)과 KID의 연결 데이터 KID ‖ Sig(Ra)를, 서비스 제공자 단말기(13)로 송부한다.

서비스 제공자 단말기(13)는, 단계 S223-2에서, 이 연결 데이터를 수취하면, KID와 전자 서명 Sig(Ra)의 각각을 추출하여, 전자 서명 Sig(Ra)이 E(Kpub, Sig(Ra))=h(Ra)를 만족시키는 것을 검증하고, 즉, 전자 서명 Sig(Ra)이, 검증키 Kpub로 복호할 수 있는 것을 확인한다. 그 검증에 성공하면, 할당된 인증 방법에 의한 인증에 성공하게 된다.

이것에 대하여, 도 71은, 키 공유를 행하는 경우에 대한 「목적별 인증의 검증 처리」와「목적별 인증 응답 처리」의 대응이 도시되고 있다.

도 71에 도시된 바와 같이, 처음에, 서비스 제공자 단말기(13)는, 단계 S223-1에서, 난수 Ra, ra를 생성하여, 난수 ra로부터 Diffie-Hellman의 키 공유를 위한 계산치 ya=g ^ ra mod p(p를 법으로 하는 g의 ra 승의 잉여)를 연산한다.

그리고, 서비스 제공자 단말기(13)는, 이들과, Key-ID를 연결한 데이터 KID ‖ Ra ‖ g ‖ p ‖ ya를 키 기억 장치(22)로 송부한다.

키 기억 장치(22)는, 단계 S203-11에서, 데이터 KID ‖ Ra ‖ g ‖ p ‖ ya를 수취하 면, 난수 rb를 생성한다.

그리고, 키 기억 장치(22)는, 단계 S203-12로, yb=g ^ rb mod p(p를 법으로 하는 g의 rb 승의 잉여)를 연산한다.

또한, 키 기억 장치(22)는, 수취한 KID에 대응하는 증명키 Kpr를 선택하여, 수취한 Ra에 대하여, 증명키 Kpr를 이용하여 전자 서명 SIG(Ra)=D(Kpr, h(Ra))를 연산하여, 그 전자 서명 SIG(Ra), KID, 및, 연산한 결과치 yb의 연결 데이터 KID ‖ SIG(Ra) ‖ yb를, 서비스 제공자 단말기(13)로 송부한다.

서비스 제공자 단말기(13)는, 단계 S223-2에서, 수취한 전자 서명 SIG(Ra)을 검증키 Kpub로 검증하여, 즉, E(Kpub, SIG(Ra))=h(Ra)가 만족되는 것을 검증한다. 이 검증에 성공하면 할당된 인증 방법에 의한 인증에 성공한 것으로 된다.

그 경우에는, 키 기억 장치(22)는, 단계 S203-13에서, 공용 키 Kses=ya ^ Rb mod p(p를 법으로 하는 ya의 Rb 승의 잉여)를 일시적인 공유키로 하여, 서비스 제공자측 단말기(13)는, 단계 S223-3에서, 공용 키 Kses=yb ^ Ra mod p(p를 법으로 하는 yb의 Ra 승의 잉여)를 일시적인 공유키로 한다. 이에 의해, 키 기억 장치(22)와 서비스 제공자 단말기(13)는, 상호 공용 키 Kses를 공유할 수 있다.

도 68로 되돌아가, 키 기억 장치(22)는, 단계 S204에 있어서, 상술한(제1 실시 형태에서 설명한) 도 34 또는 도 35에 대응하는 「서비스 이용 처리」를 실행한다.

다음으로, 도 69를 참조하여, 서비스 제공자 단말기(13)의 「키 사용/서비스 제공 처리」에 대하여 설명한다.

상술한 바와 같이, 키 기억 장치(22)는, 도 68의 단계 S201의 처리에서, 서비스를 선택하고, 단계 S202의 처리에서, 키 할당 의뢰서 + 키 할당 보고서를, 서비스 제공자 단말기(13)로 송부하여 온다.

이 때, 서비스 제공자 단말기(13)(구체적으로는, CPU(101)(도 19))는, 단계 S221에 있어서, 키 할당 의뢰서 + 키 할당 보고서를 수취한다.

그리고, 서비스 제공자 단말기(13)는, 「의뢰서 보고서 검사 + 검증키 추출」의 처리를 실행하고, 단계 S222에 있어서, 「의뢰서 보고서 검사 + 검증키 추출」이 성공인가 아닌가를 판정한다.

단계 S222에 있어서, 「의뢰서 보고서 검사 + 검증키 추출」이 실패라고 판정된 경우(성공이 아니라고 판정된 경우), 그 처리는 종료된다.

이것에 대하여, 단계 S222에 있어서, 「의뢰서 보고서 검사 + 검증키 추출」이 성공이라고 판정된 경우, 단계 S223에 있어서, 서비스 제공자 단말기(13)는, 「목적별 인증의 검증 처리」를 실행한다.

또한, 「목적별 인증의 검증 처리」의 상세는, 그것에 대응하는 도 68의 단계 S203의 처리(「목적별 인증 응답 처리」)에서 설명했기 때문에(상술하였기 때문에), 그 설명은 생략한다.

서비스 제공자 단말기(13)는, 단계 S224에 있어서, 인증이 성공인지의 여부를 판정하여, 인증이 실패(성공이 아니다)라고 판정한 경우, 그 처리를 종료한다.

이것에 대하여, 서비스 제공자 단말기(13)는, 단계 S224에 있어서, 인증이 성공이라고 판정한 경우, 단계 S225에 있어서, 상술한(제1 실시 형태에서 설명한) 도 34 또는 도 35에 대응하는 「서비스 제공 처리」를 실행한다.

도 23으로 되돌아가, 단계 S2의 처리(「키 사용/서비스 제공 처리」)가 종료하면, 필요에 따라, 단계 S6의 처리(「키 삭제 처리」)와, 단계 S7의 처리(「키 사용 정지 처리」)가 실행된다.

제2 실시 형태가 적용되는 단계 S6의 처리(「키 삭제 처리」)는, 상술한 제1 실시 형태가 적용되는 「키 삭제 처리」와 마찬가지이다. 즉, 「키 삭제 처리」는, 상술한 도 37 내지 도 39 중의 어느 하나의 흐름도에 따라서 실행된다.

단, 제2 실시 형태에 있어서는, 삭제의 대상이 되는 것은, 키 할당자 단말기(12)인 경우, 도 46의 키 할당표라고 되고, 서비스 제공자 단말기(13)인 경우, 도 53의 인증 정보표, 및, 도 55의 실효키표라고 되고, 키 기억 장치(22)인 경우, 도 60의 인증 정보표, 및, 도 59의 증명키표가 된다.

제2 실시 형태가 적용되는 단계 S7의 처리(「키 사용 정지 처리」)는, 상술한 제1 실시 형태가 적용되는 「키 사용 정지 처리」와 마찬가지이다. 즉, 「키 사용 정지 처리」는, 상술한 도 40과 도 41의 흐름도에 따라서 실행된다.

단, 제2 실시 형태에 있어서는, 도 41의 단계 S183의 처리에서 도 53의 인증 정보표로부터 키 사용 정지 요구서로 지정된 Key-ID의 레코드를 삭제하는 것 외에, 실효키표에 그 Key-ID와 유효 기한으로 이루어지는 레코드를 추가하는 작업이 필요하다.

또한, 도 40의 단계 161의 처리에서, 키 할당자 단말기(12)에 의해 생성되어, 서비스 제공자 단말기(13)로 송부되는 키 사용 정지 요구서의 형식은, 제1 실 시 형태에서는, 도 42의 형식이 되었지만, 제2 실시 형태에서는, 도 43에 도시되는 형식이 된다.

도 43의 키 사용 정지 요구서는, 사용 정지하는 인증 방법의 식별 번호 Key-ID, 사용 정지의 일시 Date-time, 사용 정지하는 인증 방법의 원래의 유효 기한, 및, 이들에 대한 키 할당자의 전자 서명(KA 전자 서명)으로 이루어진다.

또한, 키 할당자 단말기(12)는, 할당 완료한 인증 방법에 대하여, 도 46의 키 할당표의 「키 할당 의뢰서」의 항목으로부터, 그 할당을 받은 서비스 제공자의 식별 번호 SP-ID를 얻을 수 있다.

이와 같이, 제2 실시 형태가 적용되는 인증키 할당 시스템(201)에 있어서는, 할당되는 인증 방법이 공개키 인증 방식이 되기 때문에, 「키 사용/서비스 제공 처리」의 「서비스 이용 처리(도 68의 단계 S204의 처리)」 및「서비스 제공 처리(도 69의 단계 S225의 처리)」보다 전의 처리(도 69의 단계 S221 내지 S224의 처리)는, 서비스 제공자 Sp(서비스 제공자 단말기(13))가 아니더라도 실행 가능하다. 그 때문에, 예를 들면, 키 기억 장치(22)를 갖는 사용자 User 자신이, 자신이 갖는 키 기억 장치(22)가 서비스를 이용하기 위한 할당된 인증 방법에 의한 인증에 성공하는가 아닌가를 검증하는 것이 가능하게 되어, 사용자의 안심감으로 연결된다고 하는 효과를 발휘하는 것이 가능하게 된다.

(제3 실시 형태)

도 72는, 본 발명의 제3 실시 형태가 적용되는 인증키 할당 시스템(301)의 구성예를 도시하고 있고, 도 4의 인증키 할당 시스템(1), 또는, 도 44의 인증키 할 당 시스템(201)에 대응하는 부분에는, 대응하는 부호가 붙이고 있다.

이 구성예에 있어서는, 도 1의 인증키 할당 시스템(1)에 대하여, 인증 센터 단말기(211)가, 네트워크(14)에 또한 접속되어 있다. 환언하면, 도 44의 인증키 할당 시스템(201)에 대하여, 범용 어카운트 관리자 단말기(15)가, 네트워크(14)에 또한 접속되어 있다.

제3 실시 형태에 있어서는, 도 3에 도시된 바와 같이, 참가자가, 키 할당자 KA, 인증 센터 CA, 사용자 User, 서비스 제공자 SP, 및, 범용 어카운트 관리자 KDC가 된다. 서비스 제공자 SP(서비스 제공자 단말기(13))는, 공개키 인증 기반에 의해서 검증할 수 있는 전자 서명을 생성하여, 사용자 User(키 기억 장치(22))는, 범용 어카운트 방식으로 인증된다. 이 경우에 있어서의, 공개키 인증의 인증 방법을 새롭게 할당하는 예에 대하여 설명한다.

또한, 키 할당자 단말기(12)(키 할당자 KA)는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 증명서의 실효 상황을 미리 파악하고 있다(정기적으로 관계하는 CRL을 수집하고 있다).

도 73 내지 도 77은, 키 할당자 단말기(12)가 기억하는 데이터의 예를 도시하고 있다.

즉, 이 예에 있어서는, 예를 들면, 키 할당자 단말기(12)의 메모리(도 18의 기억부(88) 등)에는, 도 73에 도시되는 것 같은 키 할당표, 도 74에 도시되는 것 같은 서비스 제공자 키표, 도 75에 도시되는 것 같은 키 기억 장치 키표, 도 76에 도시되는 것 같은 키 할당자 어카운트 정보, 및, 도 77에 도시되는 것 같은 CA 공 개키 정보가 기록되어 있다.

이 예에 있어서는, 예를 들면, 도 73의 키 할당표, 도 74의 서비스 제공자 키표, 및, 도 75의 키 기억 장치 키표의 각각은, 대응하는 Key-ID, SP-ID, 또는, HW-ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 73의 키 할당표에 있어서, 각 행의 레코드의 각각은, 할당이 행해진 인증 방법에 대응하고 있다.

Key-ID는, 할당된 인증 방법의 식별 번호를 나타내고 있어, 일의적이 되도록 할당된다.

Acc-ID는, 인증 방법의 할당 시에 지불을 한 사용자 User(키 기억 장치(22))의 범용 어카운트에서의 식별 번호를 나타내고 있다.

HW-ID는, 인증 방법이 할당된 키 기억 장치(22)의 식별 번호를 나타내고 있다.

SP-ID는, 인증 방법의 할당을 받은 서비스 단말자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있다.

유효 기한은, 인증 방법의 유효 기한을 나타내고 있다.

검증키는, 할당된 인증 방법의 검증키(공개키 암호의 공개키)를 나타내고 있다.

증명키는, 할당된 인증 방법의 증명키(공개키 암호의 비밀키)를 나타내고 있다.

권리증서는, 키 할당이 행해졌을 때, 서비스 제공자 단말기(13)(서비스 제공 자 SP)가, 그것에 의하여 제공하는 서비스를 증명하기 위해서 생성하는 데이터를 나타내고 있다.

권리증서는, 예를 들면, 도 78에 도시된 바와 같이 구성된다.

도 78의 권리 증서에 있어서, Key-ID, 검증키, 및, 유효 기한의 각각은, 서비스 제공 시에 이용하는 인증 방법의 식별 번호, 검증키, 및, 유효 기한의 각각을 나타내고 있다. 서비스 내용은, Key-ID의 인증 방법으로 인증되는 (키 기억 장치(22)를 갖는) 사용자 User(사용자 단말기(21))에 제공되는 서비스의 내용을 나타내고 있다. SP 전자 서명은, 권리 증서의 데이터 전체에 대하여 서비스 제공자 단말기(13)(서비스 제공자 SP)가 생성한 전자 서명을 나타내고 있다.

도 74의 서비스 제공자 키표에 있어서, 각 레코드는, 키 할당자 단말기(12)(키 할당자 KA)와 계약을 체결한 서비스 제공자 단말기(13)(서비스 제공자 SP)에 대응한다.

SP-ID는, 키 할당자 단말기(12)(키 할당자 KA)와 계약을 체결한 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있어, 계약 체결 시에 일의적이 되도록 할당된다.

SP-address는, 서비스 제공자 단말기(13)의 연락처 어드레스(URL 등)를 나타내고 있다. 이것은, 인증 방법의 실효가 발생한 때나 조회 시의 연락처가 된다.

SP-Acc-ID는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 공개키 인증 기반에서의 식별 번호를 나타내고 있다.

고유 암호키는, 계약 체결 시에 서비스 제공자 단말기(13)(서비스 제공자 SP)와 키 할당자 단말기(12)(키 할당자 KA)의 사이에서 정한 암호키를 나타내고 있어, 이 암호키는, 양자간에서의 통신의 은닉성이나 완전성을 보증할 목적으로 이용된다.

도 75의 키 기억 장치 키표는, 도 7의 키 기억 장치표와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 76의 키 할당자 어카운트 정보는, 도 8의 키 할당자 어카운트 정보와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 77의 CA 공개키 정보는, 도 50의 CA 공개키 정보와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 79는, 서비스 제공자 단말기(13)가 생성하는 키 할당 의뢰서의 예를 나타내고, 도 80은, 키 할당자 단말기(12)가 생성하는 키 할당 보고서의 예를 도시하고 있다. 이들의 상세에 대해서는, 후술한다.

도 81 내지 도 86은, 서비스 제공자 단말기(13)가 기억하는 데이터의 예를 도시하고 있다.

즉, 이 예에 있어서는, 예를 들면, 서비스 제공자 단말기(13)의 메모리(도 19의 기억부(108) 등)에는, 도 81에 도시되는 것 같은 인증 정보표, 도 82에 도시되는 것 같은 서비스 제공자 고유 정보, 도 83에 도시되는 것 같은 실효키표, 도 84에 도시되는 것 같은 서비스 제공자 PKI 정보, 도 85에 도시되는 것 같은 키 공유 파라미터, 도 86에 도시되는 것 같은 CA 공개키 정보가 기억되어 있다.

이 예에 있어서는, 예를 들면, 도 81의 인증 정보표와 도 83의 실효키표는, Key-ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 81의 인증 정보표에 있어서, 각 레코드는, 할당을 받은 인증 방법에 대응한다.

Key-ID는, 인증 방법의 식별 번호를 나타내고 있다. 권리증서는, 키 할당받은 인증 방법에 대하여 발행된 권리 증서를 나타내고 있다.

도 82의 서비스 제공자 고유 정보는, 도 10의 서비스 제공자 고유 정보와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 83의 실효키표, 도 84의 서비스 제공자 PKI 정보, 및, 도 85의 키 공유 파라미터의 각각은, 도 55의 실효키표, 도 56의 서비스 제공자 PKI 정보, 및, 도 57의 키 공유 파라미터의 각각과 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 86의 CA 공개키 정보는, 도 50의 CA 공개키 정보와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 87 내지 도 91은, 키 기억 장치(22) 또는 IC 카드(23)(사용자 User)가 기억하는 데이터의 예를 도시하고 있다.

즉, 이 예에 있어서는, 예를 들면, 키 기억 장치(22)의 데이터 기억부(53) 또는 키 기억부(54)(도 16), 또는, IC 카드(23)의 기억부(71)에는, 도 87에 도시되는 것 같은 증명키표, 도 88에 도시되는 것 같은 인증 정보표, 도 89에 도시되는 것 같은 키 기억 장치 고유 정보, 도 90에 도시되는 것 같은 사용자 카운트 정보, 및, 도 91에 도시되는 것 같은 CA 공개키 정보가 기억되어 있다.

이 예에 있어서, 예를 들면, 도 87의 증명키표와 도 88의 인증 정보표는 모 두, Key-ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 87의 증명키표, 도 89의 키 기억 장치 고유 정보, 및, 도 90의 사용자 카운트 정보의 각각은, 도 11의 증명키표, 도 13의 키 기억 장치 고유 정보, 및, 도 14의 사용자 카운트 정보의 각각과 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 88의 인증 정보표에 있어서, 각 레코드는, 키 할당자 단말기(12)(키 할당자 KA)로부터 할당을 받은 인증 방법에 대응한다.

Key-ID는, 인증 방법의 식별 번호를 나타내고 있다. 권리증서는, 키 할당받은 인증 방법에 대하여 발행한 권리 증서를 나타내고 있다.

도 91의 CA 공개키 정보는, 도 63의 CA 공개키 정보와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

구체적으로는, 도 16의 키 기억부(54)가, 도 87의 증명키표와 도 89의 키 기억 장치 고유 정보를 기억한다. 데이터 기억부(53)가, 도 88의 인증 정보표와 도 91의 CA 공개키 정보를 기억한다. 데이터 관리부(55)는, 키 할당자 단말기(12)(키 할당자 KA)로부터 송부된 정보나, 데이터 기억부(53)에 기억되어 있는 도 88의 인증 정보표 내의 권리증서의 유효 기한에 따라, 키 기억부(54)와 데이터 기억부(53)에 기억되어 있는 데이터에 대하여, 내용의 추가 또는 삭제한다.

도 90의 사용자 카운트 정보는, 키 기억 장치(22)에 접속되는 IC 카드(23)(기억부(71)(도 17))에 기억된다. 이 예에 있어서는, 키 기억 장치(22)는, 예를 들면, IC 카드(23)가 그 인증 처리부(58)(도 16)에 접속되어 있는 경우, IC 카드(23) 에 대하여, 도 90의 사용자 카운트 정보를 이용하는 암호화, 및, 복호의 계산, 및, 증명서의 제공을 의뢰할 수 있다.

도 72의 어카운트 관리자 단말기(15)의 메모리(도 20의 기억부(128) 등)에는, 도 4의 어카운트 관리자 단말기(15)가 기억하고 있는 정보와 마찬가지의 정보, 즉, 도 21의 어카운트 관리표, 및, 도 22의 범용 어카운트 관리키가 기억되어 있다.

도 72의 인증 센터 단말기(211)의 메모리(도 45의 기억부228 등)에는, 도 44의 인증 센터 단말기(211)가 기억하고 있는 정보와 마찬가지의 정보, 즉, 도 64의 증명증표, 및, 도 65의 CA 공개키가 기억되어 있다.

단, 도 64의 증명서표의 Acc-ID가 나타내는 식별 번호에 대응하는, 공개키 인증 기반에서의 엔티티는, 제1 실시 형태에 있어서는, 키 기억 장치(22)(사용자 User), 서비스 제공자 단말기(13)(서비스 제공자 SP), 및, 키 할당자 단말기(12)(키 할당자 KA))이라고 되었지만, 제3 실시 형태에 있어서는, 서비스 제공자 단말기(13)(서비스 제공자 SP)만이라고 된다.

다음으로, 본 발명의 제3 실시 형태가 적용되는 인증키 할당 시스템(301)의 동작을 설명한다.

인증키 할당 시스템(301)의 동작의 개략은, 본 발명의 제1 실시 형태가 적용되는 인증키 할당 시스템(1)(및, 본 발명의 제2 실시 형태가 적용되는 인증키 시스템201)의 그것과 기본적으로 마찬가지이다.

따라서, 인증키 할당 시스템(301)의 동작도, 도 23의 흐름도를 참조하여 설 명한다.

처음에, 단계 S1에 있어서, 「서비스 선택/키 할당 처리」가 실행된다.

제3 실시 형태에 있어서의 「서비스 선택/키 할당 처리」는, 제1 실시 형태의 그것과, 기본적으로 마찬가지의 처리가 되지만, 약간 차이가 있다.

이러한 제3 실시 형태에 있어서의 「서비스 선택/키 할당 처리」의 상세가, 도 92 내지 도 94의 흐름도와, 도 95의 애로우 차트에 도시되고 있다. 도 92 내지 도 94의 흐름도는, 도 95의 애로우 차트에 도시되는 각 장치의 「서비스 선택/키 할당 처리」를 도시하고 있다. 즉, 도 92는, 사용자 장치(11)(도 72)의 「서비스 선택/키 할당 처리」를, 도 93은, 키 할당자 단말기(12)(도 72)의 「서비스 선택/키 할당 처리」를, 도 94는, 서비스 제공자 단말기(13)(도 72)의 「서비스 선택/키 할당 처리」를, 각각 도시하고 있다.

따라서, 여기서는, 제1 실시 형태에 있어서 설명한 처리에 대해서는, 그 설명을 적절하게 생략하여, 이하, 도 95의 애로우 차트를 참조하여, 제1 실시 형태(또는 제2 실시 형태)와는 다른 처리를 중심으로 설명한다.

도 95에 있어서, 처음에, 사용자 단말기(21)(사용자 장치(11))는, 단계 S301에 있어서, 서비스(선택 서비스)를 선택하여, 그것을 서비스 제공자 단말기(13)로 송부한다.

서비스 제공자 단말기(13)는, 단계 S341에 있어서, 선택 서비스를 수취하고, 단계 S342에 있어서, 키 할당 의뢰서를 생성하여, 키 기억 장치(22)로 송부한다.

키 기억 장치(22)(사용자 장치(11))는, 단계 S302에 있어서, 키 할당 의뢰서 를 수취하여, 일시적으로 기억함과 동시에, 단계 S303에 있어서, 키 할당자 단말기(12)로 송부한다.

키 할당자 단말기(12)는, 단계 S321에 있어서, 키 할당 의뢰서를 수취하여, 그 키 할당 의뢰서의 서비스 제공자 단말기(13)(서비스 제공자 SP)의 전자 서명을 검증한다.

도 79는, 그와 같은 키 할당 의뢰서의 예를 도시하고 있다.

도 79의 키 할당 의뢰서에 있어서, 의뢰서 ID는, 이 의뢰서를 발행한 서비스 제공자 단말기(13)(서비스 제공자 SP)로 일의적이 되도록 부가되는 식별 번호를 나타내고 있다.

유효 기한은, 이 의뢰서로 할당을 의뢰하는 인증 방법에 필요한 유효 기한을 나타내고 있다.

SP-ID는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있어, 서비스 제공자 단말기(13)(서비스 제공자 SP)가, 키 할당자 단말기(12)(키 할당자 KA)와의 계약 시에 미리 약정된 것이다.

메시지 인증 코드는, 서비스 제공자 고유 암호키를 이용하여, 키 할당 의뢰서의 데이터에 대하여 생성된 코드를 나타내고 있고, 키 할당 의뢰서의 개찬의 방지와 키 할당 의뢰서가 서비스 제공자 단말기(13)(서비스 제공자 SP)에 의해서 생성된 것을 증명한다.

도 95로 되돌아가, 키 할당자 단말기(12)가, 키 할당 의뢰서를 수취하면, 키 기억 장치(22)와 키 할당자 단말기(12)의 각각은, 단계 S322의 처리(키 할당자 단 말기(12)측의 「키 기억 장치와 상호 인증 + 키 공용 처리」), 또는, 단계 S304의 처리(키 기억 장치(22)측의 「키 할당자와 상호 인증 + 키 공용 처리」)에서, 키 기억 장치(22)와 키 할당자 단말기(12)의 사이의 상호 인증 + 키 공유의 처리를 행한다.

또한, 단계 S322 및 S304의 처리의 각각은, 상술한 도 27의 단계 S22 및 S14의 처리의 각각과, 기본적으로 마찬가지의 처리가 되기 때문에, 그 설명은 생략한다.

이 단계에서, 키 기억 장치(22)와 키 할당자 단말기(12)는, 일시적인 암호키 Kses를 공유한다.

그리고, 키 기억 장치(22)와 키 할당자 단말기(12)의 각각은, 단계 S323의 처리(키 할당자 단말기(12)측의 「키 기억 장치의 사용자 인증 처리」), 또는, 단계 S305의 처리(키 기억 장치(22)측의 「사용자 인증 응답 처리」)를 실행한다.

또한, 단계 S323 및 S305의 처리의 각각은, 상술한 도 27의 단계 S23 및 S, 15의 처리의 각각과, 기본적으로 마찬가지의 처리가 되기 때문에, 그 설명은 생략한다.

이 단계에서, 키 할당자 단말기(12)는, 키 기억 장치(22)를 보유하는 사용자 User(사용자 단말기(21))를 특정할 수 있다.

단계 S324에 있어서, 키 할당자 단말기(12)는, 신규키를 생성하여, 키 기억 장치(22)로 송부한다.

구체적으로는, 예를 들면, 키 할당자 단말기(12)는, 키 기억 장치(22)에 할 당하는 인증 방법의 식별 번호 KID를, 이전과 중첩되지 않도록 하여 결정하고, 적당한 방법으로 난수로부터 공개키 암호의 비밀키와 공개키의 쌍(Kpr, Kpub)을 새롭게 생성한다. 즉, 이 키쌍(Kpr, Kpub)이, 신규키가 되어, 새롭게 할당되는 인증 방법의 증명키와 검증키로서 이용된다.

그리고, 키 할당자 단말기(12)는, 식별 번호 KID와 증명키 Kpr를 키 기억 장치(22)로 송부한다. 보다 구체적으로는, 키 할당자 단말기(12)는, 키 기억 장치(22)와 공유한 일시 키 Kses를 이용하여, 식별 번호 KID와 증명키 Kpr를 암호화 데이터 E(Kses, KID ‖ Kpr)로서 키 기억 장치(22)로 송부한다.

단계 S306에 있어서, 키 기억 장치(22)는, 신규키를 수취한다.

구체적으로는, 키 기억 장치(22)는, 암호화 데이터 E(Kses, KID ‖ Kpr)를 수취하여, 식별 번호 KID와 증명키 Kpr를 복호한다. 그리고, 키 기억 장치(22)가 기억하는 도 87의 증명키표에 새로운 레코드를 추가한다.

그리고, 단계 S325에 있어서, 키 할당자 단말기(12)는, 키 할당 보고서를 생성하여, 키 기억 장치(22)로 송부한다.

키 할당자 단말기(12)는, 동시에, 도 73의 키 할당표에 대하여, 할당을 행한 인증 방법의 식별 번호 KID, 증명키 Kpr, 검증키 Kpub, 할당한 상대의 사용자의 식별 번호 Acc-ID, 할당을 요구한 서비스 제공자의 SP-ID, 유효 기한, 및, 할당한 키 기억 장치의 식별 번호 HWID로 이루어지는 레코드를 추가한다(권리증서의 부분은 비어있는 채임).

도 80은, 키 할당 보고서의 예를 도시하고 있다.

도 80의 키 할당 보고서에 있어서, Key-ID는, 할당된 인증 방법의 식별 번호를 나타내고 있다.

의뢰서 ID는, 금회의 인증 방법 할당의 요구를 행한 키 할당 의뢰서의 식별 번호를 나타내고 있다.

유효 기한은, 할당된 인증 방법의 유효 기한을 나타내고 있다.

검증키는, 할당된 인증 방법의 검증키를 나타내고 있다.

메시지 인증 코드는, 키 할당 보고서의 데이터에 대하여 키 할당자 단말기(12)(키 할당자 KA)가, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 고유 암호키(도 74의 서비스 제공자표로부터 얻어지는 고유 암호키)를 이용하여 생성한 코드를 나타내고 있어, 개찬의 방지와 키 할당 보고서가 키 할당자 단말기(12)(키 할당자 KA)에 의해서 생성된 것을 증명한다.

도 95로 되돌아가, 단계 S307에 있어서, 키 기억 장치(22)는, 이 키 할당 보고서를 수취하여, 서비스 제공자 단말기(13)로 송부한다. 또한, 키 할당 보고서는, 키 할당자 단말기(12)로부터 서비스 제공자 단말기(13)로 직접 송부해도 된다.

서비스 제공자 단말기(13)는, 단계 S343에 있어서, 키 할당 보고서를 수취한다. 그리고, 서비스 제공자 단말기(13)는, 키 할당 보고서의 키 할당자의 메시지 인증 코드를 검증한다.

서비스 제공자 단말기(13)는, 그 검증에 성공하면, 단계 S344에 있어서, 도 78의 권리 증서를 생성하여, 키 기억 장치(22)로 송부한다.

이 때, 서비스 제공자 단말기(13)는, 인증 방법의 식별 번호 Key-ID와, 생성 한 권리 증서를 새로운 레코드로서 도 81의 인증 정보표에 추가한다.

키 기억 장치(22)는, 권리 증서를 수취하여, 키 할당자 단말기(12)로 송부한다.

이 때, 키 기억 장치(22)는, 인증 방법의 식별 번호 Key-ID와, 권리 증서를, 도 88의 인증 정보표에 새로운 레코드로서 추가한다. 또한, 서비스 제공자 단말기(13)가, 권리 증서를, 키 할당자 단말기(12), 및, 사용자 단말기(12)의 각각에 직접 송부해도 된다.

키 할당자 단말기(12)는, 권리 증서를 수취하여, 사용자 User(사용자 단말기(21))에 대하여 과금을 행한다.

구체적으로는, 키 할당자 단말기(12)는, 수취한 권리증서의 전자 서명이 서비스 제공자 단말기(13)(서비스 제공자 SP)에 의해서 생성되어 있는 것을 확인한 후에, 도 73의 키 할당표 중의 상술한 단계 S325의 처리에서 생성된 레코드(

권리증서의 부분은 비어있음)의 권리증서의 부분에 추가한다.

그리고, 키 할당자 단말기(12)는, 상술한 단계 S323의 처리에서 특정한 사용자 User(사용자 단말기(21))에 대하여, 권리증서의 서비스 내용과 키 할당의 수수료의 합계에 적당한 과금을 행한다.

도 23으로 되돌아가, 이상과 같이하여, 단계 S1의 처리(「서비스 선택/키 할당 처리」)가 완료 실행하면, 단계 S2에 있어서, 「키 사용/서비스 제공 처리」가 실행된다.

제3 실시 형태에 있어서의 「키 사용/서비스 제공 처리」의 상세가, 도 96과 도 97의 흐름도에 도시되고 있다. 그래서, 도 96과 도 97의 흐름도를 참조하여, 제3 실시 형태에 있어서의 「키 사용/서비스 제공 처리」의 상세를 설명한다.

도 96은, 사용자 장치(11)(도 72)의 「키 사용/서비스 제공 처리」를 도시하고 있다. 도 97은, 서비스 제공자 단말기(13)(도 72)의 「키 사용/서비스 제공 처리」를 도시하고 있다.

처음에, 도 96을 참조하여, 사용자 장치(11)의 「키 사용/서비스 제공 처리」에 다음으로 설명한다.

키 기억 장치(22)(구체적으로는, CPU(51)(도 16))는, 단계 S361에 있어서, 서비스를 선택한다.

예를 들면, 이 예에 있어서는, 키 기억 장치(22)는, 자기 자신이 기억하는 도 88의 인증 정보표에 포함되는 권리증에 포함되는 서비스 내용을 사용자 단말기(21)의 디스플레이(도 15의 출력부(37))에 표시시켜, 그 안에서 이용하고자 하는 서비스에 대응하는 레코드를 사용자 User에 선택시킴으로써, 서비스를 선택한다.

키 기억 장치(22)는, 단계 S362에 있어서, 선택된 서비스에 대응하는 권리증서(도 88의 인증 정보표의 선택된 레코드의 권리증서)를, 서비스 제공자 단말기(13)로 송부한다. 또한, 이 예에 있어서는, 이 송부처는, 권리증서의 서비스 내용에 포함되어 있는 것으로 한다.

후술하는 바와 같이, 서비스 제공자 단말기(13)는, 권리 증서를 수취한다. 그리고, 서비스 제공자 단말기(13)는, 권리증서를 검사한다.

이 검사는, 권리증서가 도 78의 형식으로서 옳은가 아닌가의 판정, 전자 서명의 검증, 및, 도 83의 실효키표 중에, 권리증서의 Key-ID가 포함되지 않았는가의 판정이 된다. 이들 모든 검사에 성공한 경우에는, 서비스 제공자 단말기(13)는, 권리 증서로부터 제공하여야 할 서비스와 인증 방법(검증키)을 얻는다. 이하, 이러한 일련의 처리를, 권리증서 검사 + 검증키 추출이라 칭한다.

서비스 제공자 단말기(13)는, 권리증서 검사 + 검증키 추출에 성공하면, 「목적별 인증의 검증 처리」를 실행한다(도 97의 단계 S381 내지 S383).

이 때, 키 기억 장치(22)는, 단계 S363에 있어서, 이「목적별 인증의 검증 처리」에 대응하는 「목적별 인증의 응답 처리」를 실행한다.

즉, 키 기억 장치(22)(사용자 User)와 서비스 제공자 단말기(13)(서비스 제공자 SP)의 사이에서 할당된 인증 방법에서의 인증이 행하여진다.

단계 S363의 처리(「목적별 인증의 응답 처리」), 및, 도 97의 단계 S383의 처리(목적별 인증의 검증 처리))의 각각은, 상술한 도 68의 단계 S203 및 도 69의 단계 S223의 처리의 각각과, 기본적으로 마찬가지의 처리가 되기 때문에, 그 설명은 생략한다. 또한, 상술한 바와 같이, 할당된 인증 방법에 의한 인증 방법으로서는, 일시적인 암호키 Kses의 공유를 행하는 방법과 행하지 않는 방법의 2 종류가 가능하게 된다.

즉, 키 기억 장치(22)(사용자 User)와 서비스 제공자 단말기(13)(서비스 제공자 SP)의 사이에서 할당된 인증 방법에서의 인증이 행하여진다.

키 기억 장치(22)는, 단계 S364에 있어서, 상술한 도 34또는 도 35에 대응하 는 「서비스 이용 처리」를 실행한다.

다음으로, 도 97을 참조하여, 서비스 제공자 단말기(13)의 「키 사용/서비스 제공 처리」에 대하여 설명한다.

상술한 바와 같이, 키 기억 장치(22)는, 도 96의 단계 S361의 처리에서, 서비스를 선택하고, 단계 S362의 처리에서, 권리 증서를, 서비스 제공자 단말기(13)로 송부하여 온다.

이 때, 서비스 제공자 단말기(13)(구체적으로는, CPU(101)(도 19))는, 단계 S381에 있어서, 권리 증서를 수취한다.

그리고, 서비스 제공자 단말기(13)는, 단계 S382에 있어서, 「권리증서 검사 + 검증키 추출」의 처리를 실행하여, 「권리증서 검사 + 검증키 추출」이 성공인가 아닌가를 판정한다.

단계 S382에 있어서, 「권리증서 검사 + 검증키 추출」이 실패라고 판정된 경우(성공이 아니라고 판정된 경우), 그 처리는 종료된다.

이것에 대하여, 단계 S382에 있어서, 「권리증서 검사 + 검증키 추출」이 성공이라고 판정된 경우, 단계 S383에 있어서, 상술한「목적별 인증의 검사 처리」가 실행된다.

서비스 제공자 단말기(13)는, 단계 S384에 있어서, 인증이 성공인지의 여부를 판정하여, 인증이 실패(성공이 아니다)라고 판정한 경우, 그 처리를 종료한다.

이것에 대하여, 서비스 제공자 단말기(13)는, 단계 S384에 있어서, 인증이 성공이라고 판정한 경우, 단계 S385에 있어서, 상술한 도 34또는 도 35에 대응하는 「서비스 제공 처리」를 실행한다.

도 23으로 되돌아가, 이상과 같이하여, 단계 S2의 처리(「키 사용/서비스 제공 처리」)가 종료하면, 필요에 따라, 단계 S6의 처리(「키 삭제 처리」), 또는, 단계 S7의 처리(「키 사용 정지 처리」)가 실행된다.

제3 실시 형태가 적용되는 단계 S6의 처리(「키 삭제 처리」)는, 상술한 제1 실시 형태가 적용되는 「키 삭제 처리」와 마찬가지이다. 즉, 「키 삭제 처리」는, 상술한 도 37 내지 도 39 중의 어느 하나의 흐름도에 따라서 실행된다.

단, 제3 실시 형태에 있어서는, 삭제의 대상이 되는 것은, 키 할당자 단말기(12)인 경우, 도 73의 키 할당표가 되고, 서비스 제공자 단말기(13)인 경우, 도 81의 인증 정보표, 및, 도 83의 실효키표가 되고, 키 기억 장치(22)인 경우, 도 88의 인증 정보표, 및, 도 87의 증명키표가 된다.

제3 실시 형태가 적용되는 단계 S7의 처리(「키 사용 정지 처리」)는, 상술한 제2 실시 형태가 적용되는 「키 사용 정지 처리」와 마찬가지이다. 즉, 「키 사용 정지 처리」는, 상술한 도 40과 도 41의 흐름도에 따라서 실행된다.

또한, 도 40의 단계 161의 처리에서, 키 할당자 단말기(12)에 의해 생성되어, 서비스 제공자 단말기(13)로 송부되는 키 사용 정지 요구서의 형식은, 제1 실시 형태와 같이, 도 42의 형식이 된다.

이와 같이, 제3 실시 형태가 적용되는 인증키 할당 시스템(301)에 있어서는, 할당되는 인증 방법이 공개키 인증 방식이 되기 때문에, 「키 사용/서비스 제공 처리」의 「서비스 이용 처리(도 96의 단계 S364의 처리)」 및「서비스 제공 처리(도 97의 단계 S385의 처리)」보다 전의 처리(도 97의 단계 S381 내지 S384의 처리)는, 서비스 제공자 Sp(서비스 제공자 단말기(13))가 아니더라도 실행 가능하다. 그 때문에, 키 기억 장치(22)를 갖는 사용자 User 자신이, 자신이 갖는 키 기억 장치(22)가 서비스를 이용하기 위한 할당된 인증 방법에 의한 인증에 성공하는가 아닌가를 검증하는 것이 가능하게 되어, 사용자의 안심감으로 연결된다고 하는 효과를 발휘하는 것이 가능하게 된다.

또한, 제2 실시 형태에 비교하여, 인증에 필요한 증명서는 1개로 끝나기 때문에 데이터량과 처리 시간을 삭감할 수 있다고 하는 효과를 발휘하는 것이 가능하게 된다.

(제4 실시 형태)

본 발명의 제4 실시 형태가 적용되는 인증키 할당 시스템의 구성은, 도 72의 구성과 마찬가지이기 때문에, 그 설명은 생략한다. 따라서, 도 72는, 본 발명의 제4 실시 형태가 적용되는 인증키 할당 시스템의 구성으로서도 인용된다.

제4 실시 형태에 있어서는, 키 할당자 AP(키 할당자 단말기(12))가, 공개키 인증 기반에 의해서 검증할 수 있는 전자 서명을 생성하여, 사용자 User(키 기억 장치(22))가 범용 어카운트 방식으로 인증된다. 이 경우에 있어서의, 공개키 인증의 인증 방법을 새롭게 할당하는 예에 대하여 설명한다.

또한, 키 할당자 단말기(12)(키 할당자 KA)의 증명서의 실효 상황은, 사용자 User(키 기억 장치(22)), 및, 서비스 제공자 SP(서비스 제공자 단말기(13))에 미리 파악되어 있다(정기적으로 관계하는 CRL이 수집되어 있다).

도 98 내지 도 102는, 키 할당자 단말기(12)가 기억하는 데이터의 예를 도시하고 있다.

즉, 이 예에 있어서는, 예를 들면, 키 할당자 단말기(12)의 메모리(도 18의 기억부(88) 등)에는, 도 98에 도시되는 것 같은 키 할당표, 도 99에 도시되는 것 같은 서비스 제공자 키표, 도 100에 도시되는 것 같은 키 기억 장치 키표, 도 101에 도시되는 것 같은 키 할당자 PKI 정보, 및, 도 102에 도시되는 것 같은 CA 공개키 정보가 기록되어 있다.

이 예에 있어서는, 예를 들면, 도 98의 키 할당표, 도 99의 서비스 제공자 키표, 및, 도 100의 키 기억 장치 키표의 각각은, 대응하는 Key-ID, SP-ID, 또는, HW-ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 98의 키 할당표에 있어서, 각 행의 레코드의 각각은, 할당이 행해진 인증 방법에 대응하고 있다.

Key-ID는, 할당된 인증 방법의 식별 번호를 나타내고 있고, 일의적이 되도록 할당된다.

Acc-ID는, 인증 방법의 할당 시에 지불을 한 사용자 User(사용자 단말기(21))의 범용 어카운트에서의 식별 번호를 나타내고 있다.

HW-ID는, 인증 방법이 할당된 키 기억 장치(22)의 식별 번호를 나타내고 있다.

증명키는, 할당된 인증 방법의 증명키(공개키 암호의 비밀키)를 나타내고 있다.

권리증서는, 키 할당을 행했을 때에 서비스 제공자 단말기(13)(서비스 제공자 SP)가 그것에 의하여 제공하는 서비스를 증명하기 위해서 생성하는 데이터를 나타내고 있다.

도 103은, 그 권리증서의 예를 도시하고 있다.

도 103의 권리 증서에 있어서, Key-ID, 검증키, 및, 유효 기한의 각각은, 서비스 제공 시에 이용되는 인증 방법의 식별 번호, 검증키, 및, 유효 기한의 각각을 나타내고 있다.

서비스 내용은, Key-ID의 인증 방법으로 인증되는 (키 기억 장치(22)를 갖는) 사용자 User(사용자 단말기(21))에 제공되는 서비스의 내용을 나타내고 있다.

SP-ID는, 서비스를 제공하는 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있고, 키 할당자 단말기(12)(키 할당자 KA)와의 계약 체결 시에 서비스 제공자 단말기(13)(서비스 제공자 SP)에 일의적으로 할당된다.

KA 전자 서명은, 권리증서의 데이터 전체에 대하여 키 할당자가 생성한 전자 서명을 나타내고 있다.

도 99의 서비스 제공자 키표, 도 100의 키 기억 장치 키표, 및, 도 101의 키 할당자 PKI 정보의 각각은, 도 47의 서비스 제공자 키표, 도 48의 키 기억 장치 키표, 및, 도 49의 키 할당자 PKI 정보와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 102의 CA 공개키 정보는, 도 50의 CA 공개키 정보와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 104는, 서비스 제공자 단말기(13)가 생성하는 키 할당 의뢰서의 구성예를 도시하고 있다. 그 설명은, 후술한다.

도 105 내지 도 108은, 서비스 제공자 단말기(13)가 기억하는 데이터의 예를 도시하고 있다.

즉, 이 예에 있어서는, 예를 들면, 서비스 제공자 단말기(13)의 메모리(도 19의 기억부(108) 등)에는, 도 105에 도시되는 것 같은 서비스 제공자 고유 정보, 도 106에 도시되는 것 같은 실효키표, 도 107에 도시되는 것 같은 키 공유 파라미터, 및, 도 108에 도시되는 것 같은 CA 공개키 정보가 기억되어 있다.

이 예에 있어서는, 예를 들면, 도 106의 실효키표는, Key-ID로 검색할 수 있는 데이터베이스로서 실장된다.

도 105의 서비스 제공자 고유 정보, 도 106의 실효키표, 도 107의 키 공유 파라미터의 각각은, 도 82의 서비스 제공자 고유 정보, 도 83의 실효키표, 도 85의 키 공유 파라미터의 각각과 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 108의 CA 공개키 정보는, 도 50의 CA 공개키 정보와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 109 내지 도 113은, 키 기억 장치(22) 또는 IC 카드(23)(사용자 User)가 기억하는 데이터의 예를 도시하고 있다.

즉, 이 예에 있어서는, 예를 들면, 키 기억 장치(22)의 데이터 기억부(53) 또는 키 기억부(54)(도 16), 또는, IC 카드(23)의 기억부(71)에는, 도 109에 도시되는 것 같은 증명키표, 도 110에 도시되는 것 같은 인증 정보표, 도 111에 도시되 는 것 같은 키 기억 장치 고유 정보, 도 112에 도시되는 것 같은 사용자 카운트 정보, 및, 도 113에 도시되는 것 같은 CA 공개키 정보가 기억되어 있다.

도 109의 증명키표, 도 110의 인증 정보표, 도 111의 키 기억 장치 고유 정보, 및, 도 112의 사용자 카운트 정보의 각각은, 도 87의 증명키표, 도 88의 인증 정보표, 도 89의 키 기억 장치 고유 정보, 및, 도 90의 사용자 카운트 정보의 각각과 동일한 구성이 되기 때문에, 그 설명은 생략한다.

도 113의 CA 공개키 정보는, 도 50의 CA 공개키 정보와 동일한 구성이 되기 때문에, 그 설명은 생략한다.

예를 들면, 도 16의 키 기억부(54)가, 도 109의 증명키표와 도 111의 키 기억 장치 고유 정보를 기억한다. 데이터 기억부(53)가, 도 110의 인증 정보표와 도 113의 CA 공개키 정보를 기억한다. 데이터 관리부(55)는, 키 할당자 단말기(12)(키 할당자 KA)로부터 송부된 정보나, 데이터 기억부(53)에 기억되어 있는 도 110의 인증 정보표 내의 권리증서의 유효 기한에 따라서, 키 기억부(54)와 데이터 기억부(53)에 기억되어 있는 데이터에 대하여, 내용의 추가 또는 삭제한다.

도 112의 사용자 카운트 정보는, 키 기억 장치(22)에 접속되는 IC 카드(23)(기억부(71)(도 17))에 기억된다. 이 예에 있어서는, 키 기억 장치(22)는, 예를 들면, IC 카드(23)가 그 인증 처리부(58)(도 16)에 접속되어 있는 경우, IC 카드(23)에 대하여, 도 112의 사용자 카운트 정보를 이용하는 암호화, 및, 복호의 계산, 및, 증명서의 제공을 의뢰할 수 있다.

도 72의 어카운트 관리자 단말기(15)의 메모리(도 20의 기억부(128) 등)에 는, 도 4의 어카운트 관리자 단말기(15)가 기억하고 있는 정보와 마찬가지의 정보, 즉, 도 21의 어카운트 관리표, 및, 도 22의 어카운트 관리자 고유키가 기억되어 있다.

도 72의 인증 센터 단말기(211)의 메모리(도 45의 기억부228 등)에는, 도 44의 인증 센터 단말기(211)가 기억하고 있는 정보와 마찬가지의 정보, 즉, 도 64의 증명증표, 및, 도 65의 CA 공개키가 기억되어 있다.

이다 꺼내어, 도 64의 증명서표의 Acc-ID가 나타내는 식별 번호에 대응하는, 공개키 인증 기반에서의 엔티티는, 제4 실시 형태에 있어서는, 키 할당자 단말기(12)(키 할당자 KA)만이 된다.

다음으로, 본 발명의 제4 실시 형태가 적용되는 인증키 할당 시스템(301)의 동작을 설명한다.

본 발명의 제4 실시 형태가 제공되는 인증키 할당 시스템(301)의 동작의 개략은, 본 발명의 제3 실시 형태가 적용되는 그것(및, 본 발명의 제1 실시 형태가 적용되는 인증키 시스템(1), 및, 본 발명의 제2 실시 형태가 적용되는 인증키 시스템(201))의 그것과 기본적으로 마찬가지이다.

따라서, 본 발명의 제4 실시 형태가 적용되는 인증키 할당 시스템(301)의 동작도, 도 23의 흐름도를 참조하여 설명한다.

처음에, 단계 S1에 있어서, 「서비스 선택/키 할당 처리」가 실행된다.

제4 실시 형태에 있어서의 「서비스 선택/키 할당 처리」는, 제3 실시 형태의 그것과, 기본적으로 마찬가지의 처리가 되지만, 약간 차이가 있다.

이러한 제4 실시 형태에 있어서의 「서비스 선택/키 할당 처리」의 상세가, 도 114 내지 도 116의 흐름도와, 도 117의 애로우 차트에 도시되고 있다. 도 114 내지 도 116의 흐름도는, 도 117의 애로우 차트에 도시되는 각 장치의 「서비스 선택/키 할당 처리」를 도시하고 있다. 즉, 도 114는, 사용자 장치(11)(도 72)의 「서비스 선택/키 할당 처리」를, 도 115는, 키 할당자 단말기(12)(도 72)의 「서비스 선택/키 할당 처리」를, 도 116은, 서비스 제공자 단말기(13)(도 72)의 「서비스 선택/키 할당 처리」를, 각각 도시하고 있다.

따라서 여기서는, 제3 실시 형태에 있어서 설명한 처리에 대해서는, 그 설명을 적절하게 생략하여, 이하, 도 117의 애로우 차트를 참조하여, 제3 실시 형태(또는 제1 또는 제2 실시 형태)와는 다른 처리를 중심으로 설명한다.

도 117에 있어서, 처음에, 사용자 단말기(21)(사용자 장치(11))는, 단계 S401에 있어서, 서비스(선택 서비스)를 선택하여, 그것을 서비스 제공자 단말기(13)로 송부한다.

서비스 제공자 단말기(13)는, 단계 S441에 있어서, 선택 서비스를 수취하고, 단계 S442에 있어서, 키 할당 의뢰서를 생성하여, 키 기억 장치(22)로 송부한다.

키 기억 장치(22)(사용자 장치(11))는, 단계 S402에 있어서, 키 할당 의뢰서를 수취하여, 일시적으로 기억함과 동시에, 단계 S403에 있어서, 키 할당자 단말기(12)로 송부한다.

키 할당자 단말기(12)는, 단계 S421에서, 키 할당 의뢰서를 수취하여, 그 키 할당 의뢰서의 서비스 제공자 단말기(13)(서비스 제공자 SP)의 메시지 인증 코드를 검증한다.

도 104는, 그와 같은 키 할당 의뢰서의 예를 도시하고 있다.

도 104의 키 할당 의뢰서에 있어서, 의뢰서 ID는, 이 의뢰서를 발행한 서비스 제공자 단말기(13)(서비스 제공자 SP)로 일의적이 되도록 부가되는 식별 번호를 나타내고 있다.

유효 기한은, 이 의뢰서로 할당을 의뢰하는 인증 방법에 필요한 유효 기한을 나타내고 있다.

서비스 내용은, 서비스 제공자 단말기(13)(서비스 제공자 SP)가 키 할당을 받는 사용자 User(사용자 단말기(21))에 제공할 예정의 서비스의 내용을 나타내고 있다.

SP-ID는, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 식별 번호를 나타내고 있고, 서비스 제공자 단말기(13)(서비스 제공자 SP)가, 키 할당자 단말기(12)(키 할당자 KA)와의 계약 시에 미리 정한 것이다.

메시지 인증 코드는, 서비스 제공자 고유 암호키를 이용하여, 키 할당 의뢰서의 데이터에 대하여 생성된 코드를 나타내고 있고, 키 할당 의뢰서의 개찬의 방지와 키 할당 의뢰서가 서비스 제공자 단말기(13)(서비스 제공자 SP)에 의해서 생성된 것을 증명한다.

도 117로 되돌아가, 키 할당자 단말기(12)가, 키 할당 의뢰서를 수취하면, 키 기억 장치(22)와 키 할당자 단말기(12)의 각각은, 단계 S422의 처리(키 할당자 단말기(12)측의 「키 기억 장치와 상호 인증 + 키 공용 처리」), 또는, 단계 S404 의 처리(키 기억 장치(22)측의 「키 할당자와 상호 인증 + 키 공용 처리」)로, 키 기억 장치(22)와 키 할당자 단말기(12)의 사이의 상호 인증 + 키 공유의 처리를 행한다.

또한, 단계 S422 및 S404의 처리의 각각은, 상술한 도 27의 단계 S22 및 S14의 처리의 각각과, 기본적으로 마찬가지의 처리가 되기 때문에, 그 설명은 생략한다.

이 단계에서, 키 기억 장치(22)와 키 할당자 단말기(12)는, 일시적인 암호키 Kses를 공유한다.

그리고, 키 기억 장치(22)와 키 할당자 단말기(12)의 각각은, 단계 S423의 처리(키 할당자 단말기(12)측의 「키 기억 장치의 사용자 인증 처리」), 또는, 단계 S405의 처리(키 기억 장치(22)측의 「사용자 인증 응답 처리」)를 실행한다.

또한, 단계 S423 및 S405의 처리의 각각은, 도 27의 단계 S23 및 S15의 처리의 각각과, 기본적으로 마찬가지의 처리가 되기 때문에, 그 설명은 생략한다.

이 단계에서, 키 할당자 단말기(12)는, 키 기억 장치(22)를 보유하는 사용자 User(사용자 단말기(21))를 특정할 수 있다.

단계 S424에 있어서, 키 할당자 단말기(12)는, 신규키를 생성하여, 키 기억 장치(22)로 송부한다.

구체적으로는, 상술한 제3 실시 형태와 같이, 키 할당자 단말기(12)는, 키 기억 장치(22)에 할당하는 인증 방법의 식별 번호 KID를, 이전과 중첩되지 않도록 결정하여, 적당한 방법으로 난수로부터 공개키 암호의 비밀키와 공개키의 쌍(Kpr, Kpub)을 새롭게 생성한다. 즉, 이 키쌍(Kpr, Kpub)이, 신규키가 되어, 새롭게 할당되는 인증 방법의 증명키와 검증키로서 이용된다.

그리고, 키 할당자 단말기(12)는, 식별 번호 KID와 증명키 Kpr를 키 기억 장치(22)로 송부한다. 보다 구체적으로는, 키 할당자 단말기(12)는, 키 기억 장치(22)와 공유한 일시 키 Kses를 이용하여, 식별 번호 KID와 증명키 Kpr를 암호화 데이터 E(Kses, KID ‖ Kpr)으로서 키 기억 장치(22)로 송부한다.

단계 S406에 있어서, 키 기억 장치(22)는, 신규키를 수취한다.

구체적으로는, 키 기억 장치(22)는, 암호화 데이터 E(Kses, KID‖Kpr)를 수취하여, 식별 번호 KID와 증명키 Kpr를 복호한다. 그리고, 키 기억 장치(22)가 기억하는 도 109의 증명키표에 새로운 레코드를 추가한다.

그리고, 단계 S425에 있어서, 키 할당자 단말기(12)는, 권리 증서를 생성하여, 키 기억 장치(22)로 송부한다.

즉, 키 할당자 단말기(12)는, 제3 실시 형태에 있어서는(도 95의 예로서는), 도 80의 키 할당 보고서를 생성했지만, 제4 실시 형태에 있어서는(도 117의 예로서는), 도 103의 권리 증서를 생성한다.

이 때, 키 할당자 단말기(12)는, 도 98의 키 할당표에, 할당을 행한 인증 방법의 식별 번호 KID, 할당 상대의 사용자의 식별 번호 Acc-ID, 할당 키 기억 장치의 식별 번호 HWID, 권리증서 Rcert, 및, 증명키 Kpr로 이루어지는 레코드를 추가한다. 또한, 키 할당자 단말기(12)는, 단계 S423의 처리에서 특정한 사용자 User(사용자 단말기(21))에 대하여, 권리증서의 서비스 내용과 키 할당의 수수료의 합계 에 적당한 과금을 행한다.

키 기억 장치(22)는, 단계 S407에 있어서, 권리 증서를 수취한다.

그리고, 키 기억 장치(22)는, 수취한 권리 증서에 대하여, 전자 서명이 키 할당자 단말기(12)(키 할당자 KA)에 의해서 생성되어 있는 것을 확인한 후에, 권리 증서에 포함되는 식별 번호 KID와 권리 증서로 이루어지는 새로운 레코드를, 도 110의 인증 정보표에 추가한다.

도 23으로 되돌아가, 이상과 같이하여, 단계 S1의 처리(「서비스 선택/키 할당 처리」)가 종료하면, 단계 S2에 있어서, 「키 사용/서비스 제공 처리」가 실행된다.

제4 실시 형태에 있어서의 「키 사용/서비스 제공 처리」의 흐름은, 기본적으로 제3 실시 형태의 그것과 마찬가지이다. 즉, 제4 실시 형태에 있어서의 「키 사용/서비스 제공 처리」도, 도 96과 도 97의 흐름도에 따라서 실행된다.

단, 제4 실시 형태에 있어서는, 권리증서 검사(서비스 제공자 단말기(13)가, 도 97의 단계 S381의 처리에서 수취한 권리서에 대하여 행하는 검사)는, 권리증서가 도 103의 형식으로서 옳은가 아닌가의 판정, 전자 서명의 검증, 및, 송부된 권리증서의 Key-ID가, 도 106의 실효키표에 포함되는가 아닌가가 된다.

도 23으로 되돌아가, 단계 S2의 처리(「키 사용/서비스 제공 처리」)가 종료하면, 필요에 따라, 단계 S6의 처리(「키 삭제 처리」), 또는, 단계 S7의 처리(「키 사용 정지 처리」)가 실행된다.

제4 실시 형태가 적용되는 단계 S6의 처리(「키 삭제 처리」)는, 상술한 제1 실시 형태가 적용되는 「키 삭제 처리」와 마찬가지이다. 즉, 「키 삭제 처리」는, 상술한 도 37 내지 도 39 중의 어느 하나의 흐름도에 따라서 실행된다.

단, 제4 실시 형태에 있어서는, 삭제의 대상이 되는 것은, 키 할당자 단말기(12)인 경우, 도 98의 키 할당표가 되고, 서비스 제공자 단말기(13)인 경우, 도 106의 실효키표가 되고, 키 기억 장치(22)인 경우, 도 110의 인증 정보표, 및, 도 109의 증명키표가 된다.

제4 실시 형태가 적용되는 단계 S7의 처리(「키 사용 정지 처리」)는, 상술한 제2 실시 형태가 적용되는 「키 사용 정지 처리」와 마찬가지이다. 즉, 「키 사용 정지 처리」는, 상술한 도 40과 도 41의 흐름도에 따라서 실행된다.

단, 제4 실시 형태에 있어서의 「키 사용 정지 처리」에 있어서는, 서비스 제공자 단말기(13)는, 제2 실시 형태에 있어서의 도 53의 인증 정보표에 대응하는 것을 기억하지 않기 때문에, 인증 정보표로부터 레코드를 삭제하는 처리는 생략된다.

또한, 도 40의 단계 161의 처리에서, 키 할당자 단말기(12)에 의해 생성되어, 서비스 제공자 단말기(13)로 송부되는 키 사용 정지 요구서의 형식은, 제1 실시 형태 마찬가지에 있어서는, 도 42의 형식이 되는 데 대하여, 제4 실시 형태에 있어서는, 도 42, 도 43 중의 어느 형식이 되어도 된다.

이와 같이, 제4 실시 형태가 적용되는 인증키 할당 시스템(301)에 있어서는, 할당되는 인증 방법이 공개키 인증 방식이 되기 때문에, 「키 사용/서비스 제공 처리」의 「서비스 이용 처리(도 96의 단계 S364의 처리)」 및「서비스 제공 처리(도 9, 7의 단계 S385의 처리)」보다 전의 처리(도 97의 단계 S381 내지 S384의 처리)는, 서비스 제공자 Sp(서비스 제공자 단말기(13))가 아니더라도 실행 가능하다. 그 때문에, 키 기억 장치(22)를 갖는 사용자 User 자신이, 자신이 갖는 키 기억 장치(22)가 서비스를 이용하기 위한 할당된 인증 방법에 의한 인증에 성공하는가 아닌가를 검증 가능하게 되어, 사용자의 안심감으로 연결된다고 하는 효과를 발휘하는 것이 가능하게 된다.

또한, 제3 실시 형태에 비교하여, 키 할당 시에 필요한 통신의 횟수를 삭감 할 수 있다고 하는 효과를 발휘하는 것이 가능하게 된다. 이상, 제1 내지 제4 실시 형태로 나누어, 본 발명이 적용되는 인증키 할당 시스템에 대하여 설명하였지만, 이들의 인증키 시스템은, 이하, (1) 내지 (6)에 기술되는 것 같은 효과를 발휘하는 것이 가능하게 된다.

(1) 인증을 필요로 하는 2자 사이에 전용의 인증 방법을 할당함으로써 그 2자 사이에서 직접적으로 인증을 행하도록 했기 때문에, Kerberos 방식과 같이 인증 센터에 의존하는 방법에 비교하여, 인증을 효율적으로 행할 수 있다.

(2) 2자 사이에 전용의 인증 방법을 할당하도록 했기 때문에, 공개키 인증 기반과 같이 불특정 다수의 것이 1개의 인증 방법을 사용하는 경우와는 달리, 인증 방법의 무효화가 필요한 경우에도 그 통지를 행해야되는 상대의 특정이 가능하게 되기 때문에, 그 무효화를 효율적으로 행할 수 있다.

(3) 2자 사이에 전용의 인증 방법을 할당할 때에 사용 목적을 확정하도록 했기 때문에, 인증을 행하는 측이 인증을 받는 측을 직접 특정할 필요가 없어져, 개 개의 인증 방법에서 이용할 수 있는 서비스가 한정되어, 인증 방법이 악용된 경우의 피해를 억제하는 것이 가능하게 됨과 함께, 인증을 받는 측의 익명성을 지키는 것이 가능하게 된다.

(4) 2자 사이에 전용의 인증 방법을 할당할 때만, 과금의 목적으로 사용자의 특정을 필요로 하지만, 그 이후에 인증 방법을 이용할 때에는 사용자의 특정을 필요로 하지 않도록 했기 때문에, 사용자의 안심감으로 연결된다.

(5) 2자 사이에 할당하는 인증 방법으로서 공개키 인증을 사용한 경우, 제공하여야 할 서비스 내용이나 인증의 수단을 서비스 제공자가 혼자서 관리할 필요가 없어진다.

(6) 2자 사이에 할당하는 인증 방법으로서 공개키 인증을 사용한 경우, 사용자 자신이 키 기억 장치에 할당된 인증 방법을 확인할 수 있도록 했기 때문에, 사용자의 안심감을 더욱 높일 수 있다.

(제5 실시 형태)

상술한 바와 같이, 제5 실시 형태는, 제2 실시 형태에 대응하는 실시 형태이고, 본 발명의 제5 실시 형태가 적용되는 인증키 할당 시스템의 구성은, 도 44의 구성과 마찬가지이기 때문에, 그 설명은 생략한다. 따라서, 도 44는, 본 발명의 제5 실시 형태가 적용되는 인증키 할당 시스템의 구성으로서도 인용된다.

그런데, 제2 실시 형태에 있어서는, 새로운 인증 방법의 암호키는, 키 할당자 단말기(12)에 의해 생성되었지만, 제5 실시 형태에 있어서는, 새로운 인증 방법의 암호키는, 사용자 장치(11)의 키 기억 장치(22)에 의해 생성된다.

따라서, 제5 실시 형태에 있어서는, 키 기억 장치(22)는, 또한, 새로운 인증 방법의 암호키를 생성하는 기능을 가질 필요가 있다.

즉, 제5 실시 형태에 있어서도, 제2 실시 형태와 같이, 새로운 인증 방법의 암호키로서, 공개키 암호의 비밀키와 공개키의 쌍(이하, 공개키쌍이라 칭한다)(Kpr, Kpub)이 이용되게 된다. 따라서, 키 기억 장치(22)는, 예를 들면, 적당한 방법(방법은, 특별히 한정되지 않고, 예를 들면, IEEE-P1363에 있어서, 표준적인 방법이 종합되어 있기 때문에, 그 방법을 적용하는 것이 가능하다)으로 난수로부터 공개키쌍(Kpr, Kpub)을 새롭게 생성하는 기능을 더욱 가질 필요가 있다.

이러한 기능은, 상술한 도 16의 구성의 키 기억 장치(22)라도 용이하게 실현 가능하다. 이 경우, 연산 처리부(56)가, 난수를 발생시키는 것이 가능한 소프트웨어를 이용하여, 난수를 발생시키고, 발생한 난수로부터 공개키쌍(Kpr, Kpub)을 새롭게 생성하여, 키 기억부(54)에 기억시킨다.

이러한 난수의 발생은, 하드웨어가 실행할 수도 있다. 이 경우, 키 기억 장치(22)는, 예를 들면, 도 118에 도시되는 구성이 된다. 즉, 도 118의 키 기억 장치(22)에 있어서는, 도 16의 그것에 대하여 또한, 새로운 암호키의 생성에 필요한 난수를 발생하는 것이 가능한, 하드웨어로서의 난수 발생부(401)가 설치되어 있다.

또한, 제1 내지 제4 실시 형태에 있어서는, 키 할당자 단말기(12)가, 소프트웨어를 이용하여 난수를 발생시키고(도 18의 CPU(81)가 난수를 발생시키고), 그 난수에 기초하여 암호키를 생성하는 것을 전제로 설명을 행하였는데, 당연하면서, 도 118의 키 기억 장치(22)와 같이, 제1 내지 제4 실시 형태에 있어서의 키 할당자 단 말기(12)도, 난수 발생부(401)와 기본적으로 마찬가지의 기능과 구성을 갖는 하드웨어(도시 생략)를 또한 탑재하여, 그 하드웨어(난수 발생부(401)에 상당하는 하드웨어)에 난수를 발생시키는 것도 가능하다.

제5 실시 형태에 있어서의, 그 밖의 장치, 즉, 사용자 단말기(21), IC 카드(23), 키 할당자 단말기(12), 서비스 제공자 단말기(13), 및, 인증 센터 단말기(211)의 각각은, 제2 실시 형태의 대응하는 장치의 각각과 기본적으로 마찬가지의

기능과 구성을 갖고 있다. 따라서, 그 밖의 장치의 설명에 대해서는 생략한다.

또한, 제5 실시 형태가 적용되는 인증키 할당 시스템을 구성하는 각 장치의 각각은, 제2 실시 형태의 대응하는 장치의 각각이 기억하는 데이터와 기본적으로 마찬가지의 데이터를 갖고 있지만, 약간 차이가 있다.

그래서, 이하, 제5 실시 형태가 적용되는 인증키 할당 시스템을 구성하는 각 장치의 각각이 기억하는 데이터에 대하여 설명한다.

즉, 키 할당자 단말기(12)는, 제5 실시 형태에 있어서도, 상술한 도 47에 도시되는 것 같은 서비스 제공자 키표, 상술한 도 48에 도시되는 것 같은 키 기억 장치 키표, 상술한 도 49에 도시되는 것 같은 키 할당자 PKI 정보, 및, 상술한 도 50에 도시되는 것 같은 CA 공개키 정보를 기억하고 있다.

단, 제5 실시 형태에 있어서는, 증명키는, 사용자 User가 보유하는 키 기억 장치(22)에 의해 생성되기 때문에, 키 할당자 단말기(12)는, 도 119에 도시되는 것 같은 키 할당표(도 46의 키 할당표에 대하여, 증명키의 항목을 포함하지 않는 키 할당 표)를 보유하게 된다.

도 119의 키 할당표에 있어서, 키 할당 의뢰서와 키 할당 보고서의 각각은, 도 46의 키 할당표와 같이, 레코드(행)에 대응하는 인증 방법의 할당을 의뢰한 서비스 제공자 단말기(13)(서비스 제공자 SP)로부터 발행된 키 할당 의뢰서, 그것에 대하여 키 할당자 단말기(12)(키 할당자 KA)가 발행한 키 할당 보고서의 각각을 나타내고 있다.

즉, 제5 실시 형태에 있어서도, 예를 들면, 상술한 도 51에 도시되는 키 할당 의뢰서와, 상술한 도 52에 도시되는 키 할당 보고서의 각각이 사용 가능하다.

서비스 제공자 단말기(13)는, 제5 실시 형태에 있어서도, 상술한 도 53에 도시되는 것 같은 인증 정보표, 상술한 도 54에 도시되는 것 같은 서비스 제공자 고유 정보, 상술한 도 55에 도시되는 것 같은 실효키표, 상술한 도 56에 도시되는 것 같은 서비스 제공자 PKI 정보, 상술한 도 57에 도시되는 것 같은 키 공용 파라미터, 및, 상술한 도 58에 도시되는 것 같은 CA 공개키 정보를 기억하고 있다.

키 기억 장치(22) 또는 IC 카드(23)(사용자 User)는, 제5 실시 형태에 있어서도, 상술한 도 59에 도시되는 것 같은 증명키표, 상술한 도 60에 도시되는 것 같은 인증 정보표, 상술한 도 61에 도시되는 것 같은 키 기억 장치 고유 정보, 상술한 도 62에 도시되는 것 같은 사용자 PKI 정보, 및, 상술한 도 63에 도시되는 것 같은 CA 공개키 정보를 기억하고 있다.

또한, 제5 실시 형태에 있어서는, 키 기억 장치(22)는, 도 120에 도시되는 바와 같이, 키 기억 장치 PKI 정보를 필요에 따라 기억한다.

도 120의 키 기억 장치 PKI 정보는, 키 기억 장치(22)가, 공개키 인증 기반 으로 검증할 수 있는 전자 서명을 생성하기 위한 정보를 나타내고 있고, 증명서와 비밀키로 구성된다.

즉, 키 기억 장치(22)가, 후술하는 도 123의 단계 S504의 「키 할당자와 상호 인증 + 키 공유 처리」에 있어서, SSL(Secure Socket Layer)와 TLS(Transport Layer)를 이용하여 키 할당자 단말기(12)와 상호 인증을 행하는 경우, 도 120의 키 기억 장치 PKI 정보가 이용된다.

또한, SSL, TLS를 이용하는 상호 인증의 상세에 대해서는, 도 128과 도 129를 참조하여 후술한다.

또한, 제5 실시 형태에 있어서는, 키 기억 장치(22)는, 자기 자신이 암호키(증명키와, 그것과 쌍을 이루는 검증키)를 생성하기 때문에, 생성한 암호키를 일시적으로 기억하기 위한, 도 121에 도시되는 키 일시 기억표를 보유한다.

상세하게는, 예를 들면, 키 기억 장치(22)는, 온디맨드로 암호키를 생성한 경우, 즉, 키 할당자 단말기(12)에 의해 새로운 인증 방법의 암호키(신규키)의 생성이 요구된 시점에, 암호키를 생성한 경우, 생성한 암호키(증명키 Kpr와 검증키 Kpub의 한 쌍의 암호키쌍)를 구성 요소로 하는, 도 121의 키 일시 기억표를 생성하여 (생성한 암호키를 키 일시 기억표의 레코드에 기술하여), 기억(보유)한다.

또한, 키 기억 장치(22)는, 복수의 암호키의 후보를 미리 기억하는 경우, 도 122에 도시되는 것 같은 인증용 키표도 보유한다. 즉, 키 기억 장치(22), 또는 키 기억 장치(22)와는 상이한 다른 장치(도시 생략)는, 미리, 복수의 암호키의 후보(증명키(후보) Kprn과 검증키(후보) Kpubn(단, n은, 임의의 정수치)의 공개키쌍(Kprn, Kpubn))를 생성하고, 생성한 복수의 암호키의 후보의 각각에 대하여, Index(Idn)를 부여한다. 그리고, 키 기억 장치(22), 또는, 키 기억 장치(22)와는 상이한 다른 장치는, 부여한 복수의 Index(Idn)와, 이들에 대응하는 복수의 암호키의 후보(증명키(후보) Kpr

n과 검증키(후보) Kpubn)의 각각을 인증용 키표의 대응하는 레코드(행)에 각각 기술함으로써, 인증용 키표를 생성한다. 즉, 인증용 키표는, Index, 증명키(후보), 및, 검증키(후보)로 구성된다.

환언하면, 도 122의 인증용 키표에는, 상술한 바와 같이, 키 기억 장치(22) 자신에 의해 생성된 암호키의 후보(공개키쌍(Kprn, Kpubn))가 기억되어도 되고, 키 기억 장치(22)와는 상이한 다른 장치에 의해 생성된 암호키의 후보(공개키쌍(Kprn, Kpubn))가 기억되어도 된다. 또는, 키 기억 장치(22) 자신에 의해 생성된 암호키의 후보(공개키쌍(Kprn, Kpubn))와, 키 기억 장치(22)와는 상이한 다른 장치에 의해 생성된 암호키의 후보(공개키쌍(Kprn, Kpubn))가 혼재하여 기억되어도 된다.

키 기억 장치(22)는, 이와 같이 하여 생성된 도 122의 인증용 키표를 미리 기억해 두고, 키 할당자 단말기(12)에 의해 새로운 인증 방법의 암호키(신규키)의 생성이 요구된 시점에, 인증용 키표에 기억된 복수의 암호키의 후보(공개키쌍(Kprn, Kpubn))로부터 소정의 1개(공개키쌍(Kprk, Kpubk)(단, k는, n으로 표현 가능한 정수 중의 소정의 값))를 신규키로서 추출함으로써, 신규키를 생성한다.

그리고, 키 기억 장치(22)는, 추출한 신규키(공개키쌍(Kprk, Kpub1{))을 구성 요소로 하는, 도 121의 키 일시 기억표를 생성하여, 기억한다.

또한, 키 기억 장치(22)가 신규키를 생성하는 경우, 그 처리의 많게는, 키 기억 장치(22) 내의 연산 처리부(56)에 의해 실행된다. 아직, 도 121의 키 일시 기억표와, 도 122의 인증용 키표는, 키 기억 장치(22) 내의 키 기억부(54)(도 16 또는 도 118)에 기억된다. 따라서, 상술한 바와 같이, 적어도 연산 처리부(56)와 키 기억부(54)는, 그 내부에서 기억 또는 처리하고 있는 데이터(지금의 경우, 신규키, 또는, 그 신규키를 기억하는 도 121의 키 일시 기억표, 또는, 도 122의 인증용 키표)가 외부로부터 취득이나 개변되지 않도록, 내탬퍼성을 지면 된다.

인증 센터 단말기(211)는, 제5 실시 형태에 있어서도, 상술한 도 64에 도시되는 것 같은 증명서표, 및, 상술한 도 65에 도시되는 것 같은 CA 키 정보를 기억하고 있다.

또한, 인증 센터 단말기(211)(인증 센터 CA)는, 도 66에 도시되는 것 같은 증명서를 발행한다.

다음으로, 본 발명의 제5 실시 형태가 적용되는 인증키 할당 시스템(201)(도 44)의 동작을 설명한다.

제5 실시 형태에 있어서의 인증키 할당 시스템(201)의 동작의 개략은, 본 발명의 제2 실시 형태의 그것과 기본적으로 마찬가지이다.

따라서, 본 발명의 제5 실시 형태가 적용되는 인증키 할당 시스템(201)의 동작도, 제2 실시 형태의 설명과 같이, 도 23의 흐름도를 참조하여 설명한다.

처음에, 단계 S1에 있어서, 「서비스 선택/키 할당 처리」가 실행된다.

제5 실시 형태에 있어서의 「서비스 선택/키 할당 처리」는, 제2 실시 형태 의 그것과, 기본적으로 마찬가지의 처리가 되지만, 약간 차이가 있다.

이러한 제5 실시 형태에 있어서의 「서비스 선택/키 할당 처리」의 상세가, 도 123 내지 도 125의 흐름도와, 도 126의 애로우 차트에 도시되어 있다. 도 123 내지 도 125의 흐름도는, 도 126의 애로우 차트에 도시되는 각 장치의 「서비스 선택/키 할당 처리」를 나타내고 있다. 즉, 도 123은, 사용자 장치(11)(도 44)의 「서비스 선택/키 할당 처리」를, 도 124는, 키 할당자 단말기(12)(도 44)의 「서비스 선택/키 할당 처리」를, 도 125는, 서비스 제공자 단말기(13)(도 44)의 「서비스 선택/키 할당 처리」를, 각각 도시하고 있다.

그래서, 여기서는, 제2 실시 형태에 있어서 설명한 처리에 대해서는, 그 설명을 적절하게 생략하고, 이하, 도 126의 애로우 차트를 참조하여, 제2 실시 형태와는 다른 처리를 중심으로 설명한다.

도 126에 도시된 바와 같이, 처음에, 단계 501에 있어서, 사용자 단말기(21)는, 서비스(선택 서비스)를 선택하여, 그것을 서비스 제공자 단말기(13)로 송부한다.

서비스 제공자 단말기(13)는, 단계 S541에 있어서, 선택 서비스를 수취하고, 단계 S542에 있어서, 도 51의 키 할당 의뢰서를 생성하여, 키 기억 장치(22)로 송부한다(구체적으로는, 키 할당 의뢰서와 함께, 서비스 제공자 단말기(13)(서비스 제공자 SP)의 증명서도 보내어진다).

키 기억 장치(22)는, 단계 S502에 있어서, 키 할당 의뢰서를 수취하여, 일시적으로 기억함과 동시에, 단계 S503에 있어서, 키 할당자 단말기(12)로 송부한다.

키 할당자 단말기(12)는, 단계 S521에 있어서, 키 할당 의뢰서를 수취하면, 키 할당 의뢰서의 서비스 제공자 단말기(13)의 전자 서명을 검증한다.

키 기억 장치(22)와 키 할당자 단말기(12)의 각각은, 단계 S522의 처리(「키 기억 장치와 상호 인증 + 키 공유 처리」), 또는, 단계 S504의 처리(「키 할당자와 상호 인증 + 키 공유 처리」)를 실행한다.

상세하게는, 예를 들면, 키 기억 장치(22)가, 도 120의 키 기억 장치 PKI 정보를 기억하지 않은 경우, 제5 실시 형태에 있어서의 단계 S522의 처리(「키 기억 장치와 상호 인증 + 키 공유 처리」), 및, 단계 S504의 처리(「키 할당자와 상호 인증 + 키 공유 처리」)는, 상술한 제2 실시 형태와 마찬가지의 처리가 된다. 따라서 이들의 설명은 생략한다.

이것에 대하여, 예를 들면, 키 기억 장치(22)가, 도 120의 키 기억 장치 PKI 정보를 기억하고 있는 경우, 상술한 바와 같이, 단계 S522의 처리(「키 기억 장치와 상호 인증 + 키 공유 처리」), 및, 단계 S504의 처리(「키 할당자와 상호 인증 + 키 공유 처리」)로서, SSL, TLS를 이용한 상호 인증의 실행도 가능하다.

또한, SSL, TLS를 이용한 상호 인증에 의한, 단계 S522의 처리(「키 기억 장치와 상호 인증 + 키 공유 처리」), 및, 단계 S504의 처리(「키 할당자와 상호 인증 + 키 공유 처리」)에 대해서는, 도 128과 도 129를 참조하여 후술한다.

그 후, 키 기억 장치(22)와 키 할당자 단말기(12)의 각각은, 단계 S523의 처리(「키 기억 장치의 사용자 인증 처리」), 또는, 단계 S505의 처리(「사용자 인증 응답 처리」)를 실행한다.

또한, 제5 실시 형태에 있어서의 단계 S523의 처리(「키 기억 장치의 사용자 인증 처리」), 및, 단계 S505의 처리(「사용자 인증 응답 처리」)는, 상술한 제2 실시 형태에 있어서의 이들과 마찬가지가 되기 때문에, 이들의 설명은 생략한다.

그런데, 상술한 바와 같이, 제2 실시 형태에 있어서는, 「키 기억 장치의 사용자 인증 처리(제5 실시 형태의 단계 S523(도 126)에 대응하는 단계 S23(도 27)의 처리)」, 및, 「사용자 인증 응답 처리(제5 실시 형태의 단계 S505(도 126)에 대응하는 단계 S15의 처리의 처리)」가 실행되면, 키 할당자 단말기(12)가, 단계 S24(도 27)의 처리에서, 신규키를 생성하여, 사용자 장치(11)(키 기억 장치(22))로 송부하고, 사용자 장치(22)(키 기억 장치(22))가, 단계 S16의 처리에서, 그 신규키를 수취한다.

이것에 대하여, 제5 실시 형태에 있어서는, 도 126에 도시된 바와 같이, 「키 기억 장치의 사용자 인증 처리(단계 S523의 처리)」, 및, 「사용자 인증 응답 처리(단계 S505의 처리)」가 실행되면, 키 할당자 단말기(12)측의 단계 S524와, 사용자 장치(11)(키 기억 장치(22))측의 단계 S506에 있어서, 키 할당자 단말기(12)가, 키 기억 장치(22)에 대하여, 신규키의 생성을 요구하는 요구 정보를 생성하여, 키 기억 장치(22)로 송부한다. 키 기억 장치(22)는, 그 요구 정보를 수취하면, 신규키를 자기 자신이 생성하여, 기억함과 함께, 생성한 신규키 중의 검증키를 키 할당자 단말기(12)로 송부한다.

또한, 이하, 이러한 키 할당자 단말기(12)와 키 기억 장치(22)의 상호의 처리(키 할당의 처리) 중의, 키 할당자 단말기(12)측의 처리(도 126의 예에서는, 단 계 S524의 처리)를, 「신규키 요구 및 수취 처리」라고 칭하고, 사용자 장치(11)(키 기억 장치(22))측의 처리(도 126의 예에서는, 단계 S506의 처리)를, 「신규키 생성 및 송부 처리」라고 칭한다.

이들의 「신규키 요구 및 수취 처리(단계 S524의 처리)」와, 「신규키 생성 및 수취 처리(단계 S506의 처리)」의 상세가, 도 127의 애로우 차트에 도시되고 있다.

그래서, 도 127의 애로우 차트를 참조하여, 제5 실시 형태에 있어서의 「신규키 요구 및 수취 처리(단계 S524의 처리)」와, 「신규키 생성 및 수취 처리(단계 S543의 처리)」의 상세에 대하여 설명한다.

도 127에 도시된 바와 같이, 처음에, 단계 S524-1에 있어서, 키 할당자 단말기(12)는, 키 생성 요구 'GENERATE-KEY'를 생성한다. 키 할당자 단말기(12)는, 생성한 키 생성 요구 'GENERATE-KEY'와, 단계 S522(도 126)의 「키 기억 장치와 상호 인증 + 키 공유 처리」에 의해 사용자 장치(11)(키 기억 장치(22))와 공유한 일시 암호키 Kses를 이용하여, 메시지 인증 코드 MAC('GENERATE-KEY')=E(Kses, h('GENERATE-KEY'))를 생성한다. 그리고, 키 할당자 단말기(12)는, 키 생성 요구 'GENERATE-KEY'와, 메시지 인증 코드 MAC('GENERATE-KEY')=E(Kses, h('GENERATE-KEY'))를 연결한다. 즉, 키 할당자 단말기(12)는, 신규키의 생성을 요구하는 요구 정보로서, 연결 데이터 'GENERATE-KEY' ‖ MAC('GENERATE-KEY')을 생성한다.

단계 S524-2에 있어서, 키 할당자 단말기(12)는, 연결 데이터 'GENERATE-KEY' ‖ MAC('GENERATE-KEY')를 송부하면, 단계 S506-1에 있어서, 사용자 장치(11)(키 기억 장치(22))가 그것을 수취한다.

단계 S506-2에 있어서, 키 기억 장치(22)는, 메시지 인증 코드의 검증을 행하여, 키 생성 요구 'GENERATE-KEY'의 개찬 및 정당성의 검증을 행한다.

검증이 성공한 경우, 키 기억 장치(22)는, 단계 S506-3에 있어서, 신규키, 즉, 공개키 암호의 비밀키와 공개키의 쌍인 공개키쌍(Kpr, Kpub)을 새롭게 생성한다. 이 공개키쌍(Kpr, Kpub)이, 새롭게 할당되는 인증 방법의 증명키 및 검증키로서 이용된다.

구체적으로는, 예를 들면, 키 기억 장치(22)가, 도 118에 도시된 바와 같이 구성되는 경우, 난수 발생부(401)는, 난수를 발생시키고, 연산 처리부(56)는, 예를 들면, IEEE-P1363에 의해 규정되어 있는 방법 등에 따라서, 난수 발생부(401)에 의해 발생된 난수로부터 공개키쌍(Kpr, Kpub)을 새롭게 생성한다.

그리고, 연산 처리부(56)는, 생성한 공개키쌍(Kpr, Kpub)의 2개의 키를 구성 요소로 하는, 도 121의 키 일시 기억표를 생성하여, 키 기억부(54)에 기억한다.

또는, 예를 들면, 키 기억 장치(22)가, 도 118에 도시된 바와 같이 구성되는 경우, 단계 S506의 「신규키 생성 및 송부 처리」보다도 시간적으로 전에, 연산 처리부(56)가, 예를 들면, IEEE-P1363에 의해 규정되어 있는 방법 등에 따라서, 난수 발생부(401)에 의해 발생된 복수의 난수의 각각으로부터, 복수의 공개키쌍(Kprn, Kpubn)(n은, 임의의 정수치)을 미리 생성하고, 생성한 복수의 공개키쌍(Kprn, Kpubn)의 각각에 대하여, Index로서 Idn을 부여한다.

그리고, 연산 처리부(56)는, 도 122의 인증용 키표의 n 레코드(행)에 있어 서, Indx의 항목에 IDn을, 증명키(후보)의 항목에, 생성한 복수의 공개키쌍(Kprn, Kpubn) 중의 비밀키 Kprn을, 검증키(후보)의 항목에, 생성한 복수의 공개키쌍(Kprn, Kpubn) 중의 공개키 Kpubn을, 각각 기술한 후, 인증용 키표를 키 기억부(54)에 기억한다.

또한, 지금의 경우, 도 122의 인증용 키표에 포함되는 암호키의 후보(증명키(후보) Kprn과 검증키(후보) Kpubn)의 모두는, 키 기억 장치(22)에 의해 생성되었지만, 상술한 바와 같이, 도 122의 인증용 키표에 포함되는 암호키의 후보(증명키(후보) Kprn과 검증키(후보) Kpubn) 중의 적어도 일부가, 키 기억 장치(22)와는 상이한 다른 장치에 의해 생성되어도 된다.

이와 같이 하여, 도 122의 인증용 키표가, 키 기억부(54)에 미리 기억된 상태에서, 키 기억 장치(22)는, 단계 S506-1에 있어서, 키 할당자 단말기(12)로부터 송부된 연결 데이터 'GENERATE-KEY' ‖ MAC('GENERATE-KEY')를 수취하면, 단계 S506-2에 있어서, 메시지 인증 코드의 검증을 행하여, 키 생성 요구 'GENERATE-KEY'의 개찬 및 정당성의 검증을 행한다.

검증이 성공한 경우, 단계 S506-3에 있어서, 연산 처리부(56)는, 키 기억부(54)에 기억되어 있는, 도 122의 인증용 키표의 각 레코드(행)의 각각에 포함되는 복수의 신규키의 후보, 즉, 복수의 공개키쌍(Kprn, Kpubn)의 중에서 소정의 1개(공개키쌍(Kprk, Kpubk)(k는, n으로 표시되는 정수치 중의 소정의 1개의 값))를 추출한다.

그리고, 연산 처리부(56)는, 추출한 공개키쌍(Kprk, Kpubk)의 2개의 키의 각 각을 구성 요소로 하는, 도 121의 키 일시 기억표를 생성하여, 키 기억부(54)에 기억함과 함께, 도 122의 인증용 키표 중의, 선택한 공개키쌍(Kprk, Kprk)에 대응하는 레코드(k 행)를 삭제한다.

이와 같이 하여, 도 121의 키 일시 기억표가 키 기억부(54)에 기억되면, 단계 S506-4에 있어서, 키 기억 장치(22)는, 공개키, 즉, 검증키 Kpub를 송부하면, 단계 S524-3에 있어서, 키 할당자 단말기(12)는, 그것을 수취한다.

구체적으로는, 예를 들면, 키 기억 장치(22)는, 단계 S506-3의 처리에서 생성한 (도 121의 키 일시 기억표에 기억된) 공개키쌍(Kpr, Kpub) 중의 검증키 Kpub와, 단계 S504(도 126)의 「키 할당자와 상호 인증 + 키 공유 처리」에 의해 키 할당자 단말기(12)와 공유한 일시 암호키 Kses를 이용하여 메시지 인증 코드 MAC(Kpub)=E(Kses, h(Kpub)를 생성한다. 그리고, 키 기억 장치(22)는, 검증키 Kpub와, 메시지 인증 코드 MAC(Kpub)를 연결한다. 즉, 키 기억 장치(22)는, 연결 데이터 Kpub ‖ MAC(Kpub)를 생성한다.

생성된 연결 데이터 Kpub ‖ MAC(Kpub)는, 사용자 장치(11)로부터 송부되어, 키 할당자 단말기(12)에 수취된다.

그렇게 하면, 키 할당자 단말기(12)는, 단계 S524-4에 있어서, 연결 데이터 Kpub ‖ MAC(Kpub)의 메시지 인증 코드 MAC(Kpub)의 검증을 행한다.

도 126으로 되돌아가, 검증이 성공하면, 키 할당자 단말기(12)는, 단계 S525에 있어서, 도 52의 키 할당 보고서를 생성하여, 키 기억 장치(22)로 송부한다.

동시에, 키 할당자 단말기(12)는, 도 119의 키 할당표에, 할당을 행한 인증 방법의 일의적인 식별 번호 KID, 할당한 상대의 사용자의 식별 번호 AID, 할당 키 기억 장치(22)의 식별 번호 HWID, 키 할당 의뢰서 App, 및, 키 할당 보고서 Rep로 이루어지는 레코드를 추가한다.

그리고, 키 할당자 단말기(12)는, 단계 S526에 있어서, 식별 번호 AID의(IC 카드(23)를 소유한다) 사용자 User에 대하여 과금을 행한다.

키 기억 장치(22)는, 단계 S507에 있어서, 도 52의 키 할당 보고서를 수취하면, 기억하고 있는 도 59의 증명키표에, 키 할당 보고서에 포함되는 키 식별 번호 KID, 및, 도 121의 키 일시 기억표에 기억시켜 둔 증명키 Kpr로 이루어지는 레코드를 추가한다.

또한, 키 기억 장치(22)는, 도 60의 인증 정보표에, 할당된 인증 방법의 식별 번호 KID, 이미 서비스 제공자로부터 수취하여 완료한 키 할당 의뢰서 App, 및, 키 할당 보고서 Rep로 이루어지는 레코드를 추가한다.

그리고, 단계 S508에 있어서, 키 기억 장치(22)는, 단계 S507의 처리에서 수취한 키 할당 보고서를 서비스 제공자 단말기(13)로 송부한다.

동시에, 키 기억 장치(22)는, 도 121의 키 일시 기억표에 기억하고 있었던 증명키 Kpr와 검증키 Kpub를 삭제한다.

서비스 제공자 단말기(13)는, 단계 S543에 있어서, 키 할당 보고서를 수취한다. 그리고, 서비스 단말기(13)는, 키 할당 보고서에 포함되는 키 할당자의 서명을 검증한다. 서비스 제공 단말기(13)는, 그 검증에 성공하면, 인증 방법의 식별 번호 KID, 이미 송부한 키 할당 의뢰서 App, 및, 수취한 키 할당 보고서 Rep로 이 루어지는 레코드를 도 53의 인증 정보표에 추가한다.

다음으로, 도 128과 도 129를 참조하여, SSL, TLS를 이용한 상호 인증을 이용하는, 「키 기억 장치와 상호 인증 + 키 공유 처리(단계 S522의 처리)」, 및, 「키 할당자와 상호 인증 + 키 공유 처리(단계 S504의 처리)」의 상세에 대하여 설명한다.

SSL, TLS는, 인터넷 상에서의 「도청」, 「개찬」, 또는「스푸핑(spoofing)」과 같은 위협에 대하여 회피가 가능한 시큐러티 기술이다.

SSL은, Netscap 사가 개발하여, 현재 인터넷 상의 암호 통신 프로토콜로서 넓게 보급하고 있다. TLS는, IETF에 의해 개발 및 표준화가 진행되고, RFC2246가 공개되어 있다.

SSL, TLS는, 다음의 (a) 내지 (d)로 기술되는 것 같은 특징을 갖고 있다.

(a) 전자 증명서에 의한 서버 인증과 송신증명 (b) 전자 증명서에 의한 클라이언트 인증과 송신증명 (c) 암호화에 의한 데이터의 비밀 보호 (d) 메시지 인증 코드(MAC)에 의한 데이터 개찬 방지

도 128은, 이러한 SSL, TLS가 이용되는 경우의 프로토콜 스택의 예를 도시하고 있다.

도 128에 도시된 바와 같이, SSL, TLS가 이용되는 경우의 프로토콜 스택은, 아래로부터 순서대로, Ethernet(등록상표) 등의 층(411), IP(Internet Protocol) 등의 층(412), TCP(Transmission Control Protocol)나 UDP(User Datagram Protocol) 등의 트랜스포트층(413), SSL이나 TLS 등의 층(414), 및, HTTP(HyperText Transfer Protocol), FTP(file Transfer Program), TELNET 등의 어플리케이션층(415)으로 이루어지는 다층 구조로 되어있다.

이와 같이, SSL, TLS는, TCP이나 UDP 등의 트랜스포트층(413)의 바로 위쪽이고, 어플리케이션층(415)의 바로 아래에 위치하고 있다. 즉, SSL, TLS는, TCP, UDP이 제공하여 주는 기능(소켓) 등을 사용하여, 거기에서 얻어진 데이터에 대하여 시큐러티 기능을 실시하고, 그 결과를 어플리케이션에 인도한다고 하는 기능을 한다. 이 때문에, SSL, TLS는, 어플리케이션에는 의존하지 않고서 이용할 수 있다고 하는 특징을 갖고 있다. 예를 들면, World Wide Web 용의 브라우저 등에는 표준으로 그 기능이 내장되어 있다.

SSL, TLS의 층(414)은, 도 128에 도시된 바와 같이, 크게 나눠, 하위 층(414-1)과 상위 층(414-2)의 2층으로 분리된다. 하위 층(414-1)은, 일반적으로 Record Protocol이라고 칭해지고, 암호화나 데이터의 개찬을 방지하는 메시지 다이제스트 기능 등을 제공하는 층이다. 한편, 상위 층(414-2)은, Handshake Protocol, Alert Protocol, Change Ci

pher Spec Protocol, Application Data Protocol의 4개의 프로토콜이 포함되는 층이다. 상위 층(414-2)은, 스푸핑을 방지하는 인증 기능과, SSL/TLS 세션을 개시하기 위해서 행해지는 네고시에이션 기능을 구비하고 있다.

네고시에이션 기능은, 통신에 앞서서, 통신 상대가 정당한 상대인 것을 확인하고, 또한, 쌍방이 이용할 수 있는 암호화 알고리즘을 확인하는 등, 전처리적인 것을 실행하는 기능이다.

이하, 도 129의 애로우 차트를 참조하여, 이들의 4개의 프로토콜 중의, 예를 들면, Handshake 프로토콜을 이용하는, 「키 기억 장치와 상호 인증 + 키 공유 처리(단계 S522의 처리)」, 및, 「키 할당자와 상호 인증 + 키 공유 처리(단계 S504의 처리)」의 상세에 대하여 설명한다.

즉, 도 129는, 일반적인 SSL에 있어서 Handshake 프로토콜을 이용하는, 「키 기억 장치와 상호 인증 + 키 공유 처리(단계 S522의 처리)」, 및, 「키 할당자와 상호 인증 + 키 공유 처리(단계 S504의 처리)」를 설명하는 애로우 차트이다.

처음에, 사용자 장치(11)(키 기억 장치(22))가, SSL 커넥션을 행하면, 키 할당자 단말기(12)는, 단계 S522-1에 있어서, hello request 메시지를 키 기억 장치(22)로 송부한다.

키 기억 장치(22)는, 단계 S504-1에 있어서, hello request 메시지를 수취하면, 단계 S504-2에 있어서, client hello 메시지를 키 할당자 단말기(12)로 송부한다.

또한, client hello 메시지는, SSL 버전, 서포트하는 암호 알고리즘, 압축 알고리즘, 및 타임스탬프 등의 정보를 키 할당자 단말기(12)에 알리는 메시지이다.

키 할당자 단말기(12)는, 단계 S522-2에 있어서, client hello 메시지를 수취하면, 단계 S522-3에 있어서, server hello 메시지를 키 기억 장치(22)로 송부한다.

키 기억 장치(22)는, 단계 S504-3에 있어서, server hello 메시지를 수취한다.

또한, server hello 메시지는, client hello 메시지에 대한 응답을 나타내는 메시지이고, 키 할당자 단말기(12)가 선택한 암호 알고리즘, 압축 알고리즘, 및, 세션 ID 등이 포함된다.

계속해서, 단계 S522-4에 있어서, 키 할당자 단말기(12)는, 도 49의 키 할당자 PKI 정보의 증명서 CERTKA를 첨부한 server certificate 메시지를, 키 기억 장치(22)로 송부한다.

키 기억 장치(22)는, 단계 S504-4에 있어서, 증명서 CERTKA(server certificate 메시지)를 수취하면, 단계 S504-5에 있어서, 증명서 CERTKA의 검증, 즉, 키 할당자 KA의 검증을 행하여, 검증의 성공 가부에 의해, 키 할당자 KA 인지의 여부의 확인을 행한다.

또한, 키 할당자 단말기(12)가 증명서 등을 기억하지 않은 경우, sever key exchange라는 메시지가, 단계 S522-5의 처리에서, 키 할당자 단말기(12)부로부터 송부되어, 단계 S504-6의 처리에서, 키 기억 장치(22)에 의해 수취된다.

단계 S522-6에 있어서, 키 할당자 단말기(12)는, 키 기억 장치(22)를 확인하기 위해서, 증명서를 요구하는 메시지(이러한 메시지를, certificate request라고도 칭한다)를 송부하면, 단계 S504-7에 있어서, 키 기억 장치(22)는, 그 메시지를 수취한다.

단계 S522-7에 있어서, 키 할당자 단말기(12)는, 서버의 응답의 종료를 나타내는 server hello done메시지를 송부하면, 단계 S504-8에 있어서, 키 기억 장치(22)는, 그 메시지를 수취한다.

단계 S504-9에 있어서, 키 기억 장치(22)는, 도 120의 키 기억 장치 PKI 정보에 포함되는 증명서 CERTHWO를 첨부한 server certificate 메시지를, 키 할당자 단말기(12)로 송부한다.

키 할당자 단말기(12)는, 단계 S522-8에 있어서, 증명서 CERTHWO(server certificate 메시지)를 수취한다.

단계 S504-10에 있어서, 키 기억 장치(22)는, SSL 암호화 통신을 행하기 위한 일시적인 암호키 Kss1을 생성하는 근본이 되는 정보를, client key exchange 메시지로서 송부하면, 단계 S522-9에 있어서, 키 할당자 단말기(12)는, 그 메시지를 수취한다. 즉, 키 기억 장치(22)와 키 할당자 단말기(12)는, SSL 암호화 통신을 행하기 위한 일시적인 암호키 Kss1을 생성하는 근본이 되는 정보를 공유한다.

단계 S504-11에 있어서, 키 기억 장치(22)는, 키 기억 장치(22)의 전자 서명을, client verify 메시지로서 키 할당자 단말기(12)로 송부하는 키 할당자 단말기(12)는, 단계 S522-10에 있어서, client verify 메시지를 수취하면, 단계 S522-11에 있어서, 단계 S522-8의 처리에서 수취한 증명서 CERTHWO의 검증, 즉, 키 기억 장치(22)의 검증을 행하여, 검증의 성공 가부에 의해, 키 기억 장치(22)인지의 여부의 확인을 행한다.

단계 S522-12에 있어서, 키 할당자 단말기(12)는, 단계 S522-9의 처리에서 수취한 Client key exchange 메시지에 대응하는 정보(키 기억 장치(22)와 공유한 정보)에 기초하여, SSL 암호화 통신을 행하기 위한 일시적인 암호키 Kss1(키 기억 장치(22)와 공유하는 세션 키 Ksse1)를 생성한다.

한편, 단계 S504-12에 있어서, 키 기억 장치(22)도, 단계 S504-10의 처리에서 송부한 Client key exchange 메시지에 대응하는 정보(키 할당자 단말기(12)와 공유한 정보)에 기초하여, SSL 암호화 통신을 행하기 위한 일시적인 암호키 Kss1(키 할당자 단말기(12)과 공유하는 세션 키 Ksse1)를 생성한다.

이상의 처리가 실행되면, 키 할당자 단말기(12)와 키 기억 장치(22)의 각각은, 단계 S522-13과 단계 S504-13의 각각에 있어, Handshake 프로토콜이 종료한 것을 나타내는 finished 메시지를 서로 송부하여 수취한다.

이와 같이, SSL 에서는, 이 시점(단계 S522-13과 단계 S504-13의 처리의 종료 시점)으로, 키 할당자 단말기(12)와 키 기억 장치(22)의 각각은, SSL 암호화 통신용이 일시적인 암호키 Kss1을 공유하게 된다.

또한, 이상으로 설명한 각 메시지의 각각은, RFC2246으로 규정되어 있다.

또한, 본 발명에 있어서는 단계 S504-14에 있어서, 키 기억 장치(22)는, 난수(일시적인 암호키) Kses를 생성한다. 키 기억 장치(22)는, SSL 프로토콜에 의해서 키 할당자 단말기(12)와 공유한 암호키 Kss1(단계 S504-12의 처리에서 생성한 SSL 암호화 통신을 행하기 위한 일시적인 암호키 Kss1)로, 생성한 암호키(난수) Kses를 암호화한다. 즉, 키 기억 장치(22)는, 데이터 E(Kss1, Kses)를 생성한다. 또한, 키 기억 장치(22)는, 메시지 인증 코드 MAC(E(Kss1, Kses))=E(Kssl, E(Kss1, Kses))을 생성한다. 키 기억 장치(22)는, 데이터 E(Kss1, Kses)와 메시지 인증 코드 MAC(E(Kss1, Kses))를 연결한다. 즉, 키 기억 장치(22)는, 연결 데이터 E(Kss1, Kses) ‖ MAC(E(Kss1, Kses))를 생성한다.

그리고, 키 기억 장치(22)는, 단계 S504-15에 있어서, 연결 데이터 E(Kssl, Kses) ‖ MAC(E(Kss1, Kses))을 키 할당자 단말기(12)로 송부한다.

그렇게 하면, 키 할당자 단말기(12)는, 단계 S522-14에 있어서, 연결 데이터 E(Kss1, Kses) ‖ MAC(E(Kss1, Kses))를 수취하고, 단계 S522- 15에 있어서, 메시지 인증 코드 MAC(E(Kssl, Kses))의 검증 난수 Kses(키 기억 장치(22)가, 단계 S504-15의 처리에서 생성한 일시적인 암호키 Kses)를 추출한다. 즉, 키 할당자 단말기(12)는, 메시지 인증 코드 MAC(E(Kss1, Kses))의 검증을 행하여, 검증 난수 Kses를 복호하여, 키 기억 장치(22)와 공유한다.

또한, 도 129에 도시된다, SSL, TLS를 이용한 상호 인증에 의한「키 기억 장치와 상호 인증 + 키 공유 처리」와 「키 할당자와 상호 인증 + 키 공유 처리」는, 키 기억 장치(22)가, 도 120에 도시되는 키 기억 장치 PKI 정보를 기억하고 있으면, 제5 실시 형태뿐만 아니라, 상술한 제1 내지 제4 실시 형태, 및, 후술하는 제6 실시 형태중 어디에 있어서도 적용 가능하다.

도 23으로 되돌아가, 단계 S1의 처리(「서비스 선택/키 할당 처리」)가 실행되면, 단계 S2에 있어서, 「키 사용/서비스 제공 처리」가 실행된다.

제5 실시 형태의 「키 사용/서비스 제공 처리」(단계 S2의 처리)는, 상술한 제2 실시 형태의 그것과 마찬가지이다. 즉, 제5 실시 형태에 있어서도, 「키 사용/서비스 제공 처리」는, 상술한 도 68과 도 69의 흐름도에 따라서 실행된다.

단계 S2의 처리(「키 사용/서비스 제공 처리」)가 종료하면, 필요에 따라, 단계 S6의 처리(「키 삭제 처리」)와, 단계 S7의 처리(「키 사용 정지 처리」)가 실행된다.

제5 실시 형태의 「키 삭제 처리」(단계 S6의 처리)는, 상술한 제2 실시 형태의 그것과 마찬가지이다. 즉, 제5 실시 형태에 있어서도, 「키 삭제 처리」는, 상술한 도 37 내지 도 39 중의 어느 하나의 흐름도에 따라서 실행된다.

단, 제5 실시 형태에 있어서는, 삭제의 대상이 되는 것은, 키 할당자 단말기(12)인 경우, 도 119의 키 할당표가 되고, 서비스 제공자 단말기(13)인 경우, 도 53의 인증 정보표, 및, 도 55의 실효키표가 되고, 키 기억 장치(22)인 경우, 도 59의 증명키표, 및, 도 60의 인증 정보표가 된다.

제5 실시 형태의 「키 사용 정지 처리」(단계 S7의 처리)는, 상술한 제2 실시 형태의 그것과 마찬가지이다. 즉, 제5 실시 형태에 있어서도, 「키 사용 정지 처리」는, 상술한 도 40과 도 41의 흐름도에 따라서 실행된다.

이와 같이, 제5 실시 형태가 적용되는 인증키 할당 시스템(201)은, 제2 실시 형태에 대응하는 실시 형태이기 때문에, 당연하면서, 상술한(1) 내지 (6)의 효과를 발휘하는 것이 가능하게 된다.

또한, 제5 실시 형태가 적용되는 인증키 할당 시스템(201)은, 다음의 (7) 내지 (10)로 도시되는 것 같은 효과를 발휘하는 것이 가능하게 된다.

(7) 인증을 필요로 하는 2자 사이에 전용의 인증 방법을 할당하는 경우, 사용자의 소지하는 장치가, 그 인증 방법의 암호키(공개키쌍)를 생성하기 때문에, 비밀키는 외부에 누설하는 것이 실질 상 없기 때문에, 안전성을 높일 수 있다.

(8) 인증을 필요로 하는 2자 사이에 전용의 인증 방법을 할당하는 경우, 사 용자의 소지하는 장치가, 그 인증 방법의 암호키(공개키쌍)를 생성하기 때문에, 키 할당자의 부하를 경감할 수 있다.

(9) 인증을 위한 암호키가 미리 생성됨으로써, 키 할당 시의 키 생성에 의한 처리의 지연을 방지할 수 있다.

(10) 비밀키의 누설이 만일 일어난 경우에도, 누설원의 소재를 사용자가 소지하는 키 기억 장치에 한정할 수 있다.

(제6 실시 형태)

상술한 바와 같이, 제6 실시 형태는, 제4 실시 형태에 대응하는 실시 형태로서, 본 발명의 제6 실시 형태가 적용되는 인증키 할당 시스템의 구성은, 도 72의 구성과 마찬가지이기 때문에, 그 설명은 생략한다. 따라서, 도 72는, 본 발명의 제6 실시 형태가 적용되는 인증키 할당 시스템의 구성으로서도 인용된다.

그런데, 제4 실시 형태에 있어서는, 새로운 인증 방법의 암호키는, 키 할당자 단말기(12)에 의해 생성되었지만, 제6 실시 형태에 있어서는, 새로운 인증 방법의 암호키는, 사용자 장치(11)의 키 기억 장치(22)에 의해 생성된다.

따라서, 제6 실시 형태에 있어서는, 제5 실시 형태와 같이, 키 기억 장치(22)는, 또한, 새로운 인증 방법의 암호키를 생성하는 기능을 가질 필요가 있다.

즉, 제6 실시 형태에 있어서도, 제2 실시 형태나 제5 실시 형태와 같이, 새로운 인증 방법의 암호키로서, 공개키 암호의 비밀키와 공개키의 쌍인 공개키쌍(Kpr, Kpub)이 이용된다. 따라서, 키 기억 장치(22)는, 예를 들면, 적당 한 방법(방법은, 특별히 한정되지 않고, 예를 들면, IEEE-P1363에 있어서, 표준 방법이 종합되어 있기 때문에, 그 방법을 적용하는 것이 가능하다)으로 난수로부터 공개키쌍(Kpr, Kpub)을 새롭게 생성하는 기능을 또한 가질 필요가 있다.

이러한 기능은, 상술한 도 16의 구성의 키 기억 장치(22)라도 용이하게 실현 가능하다. 이 경우, 연산 처리부(56)가, 난수를 발생시키는 것이 가능한 소프트웨어를 이용하여, 난수를 발생시키고, 발생한 난수로부터 공개키쌍(Kpr, Kpub)을 새롭게 생성하여, 키 기억부(54)에 기억시킨다.

또한, 제6 실시 형태에 있어서도, 하드웨어가 난수를 발생시킬 수 있다. 이 경우, 키 기억 장치(22)는, 예를 들면, 상술한 도 118에 도시되는 구성이 된다. 즉, 하드웨어로서의 난수 발생부(401)가 난수를 발생한다.

제6 실시 형태에 있어서의, 그 밖의 장치, 즉, 사용자 단말기(21), IC 카드(23), 키 할당자 단말기(12), 서비스 제공자 단말기(13), 범용 어카운트 관리자 단말기(15), 및 인증 센터 단말기(211)의 각각은, 제4 실시 형태의 대응하는 장치의 각각과 기본적으로 마찬가지의 기능과 구성을 갖고 있다. 따라서, 그 밖의 장치에 대한 설명은 생략한다.

또한, 제6 실시 형태가 적용되는 인증키 할당 시스템을 구성하는 각 장치의 각각은, 제4 실시 형태의 대응하는 장치의 각각이 기억하는 데이터와 기본적으로 마찬가지의 데이터를 갖고 있지만, 약간 차이가 있다.

그래서, 이하, 제6 실시 형태가 적용되는 인증키 할당 시스템을 구성하는 각 장치의 각각이 보유하는 데이터에 대하여 설명한다.

즉, 키 할당자 단말기(12)는, 제6 실시 형태에 있어서도, 상술한 도 99에 도시되는 것 같은 서비스 제공자 키표, 상술한 도 100에 도시되는 것 같은 키 기억 장치 키표, 상술한 도 101에 도시되는 것 같은 키 할당자 PKI 정보, 및, 상술한 도 102에 도시되는 것 같은 CA 공개키 정보를 기억한다.

단, 제6 실시 형태에 있어서는, 증명키는, 사용자 User가 보유하는 키 기억 장치(22)에 의해 생성되기 때문에, 키 할당자 단말기(12)는, 도 130에 도시되는 것 같은 키 할당표(도 73의 키 할당표에 대하여, 증명키의 항목을 포함하지 않는 키 할당표)를 보유하게 된다.

또한, 도 130의 키 할당표에 있어서, 권리증서는, 도 73의 키 할당표와 같이, 키 할당을 행했을 때에 서비스 제공자 단말기(13)(서비스 제공자 SP)가 그것에 의하여 제공하는 서비스를 증명하기 위해서 생성하는 데이터를 나타내고 있다.

즉, 제6 실시 형태에 있어서도, 예를 들면, 상술한 도 103에 도시되는 권리증서가 사용 가능하다.

서비스 제공자 단말기(13)는, 제6 실시 형태에 있어서도, 상술한 도 105에 도시되는 것 같은 서비스 제공자 고유 정보, 상술한 도 106에 도시되는 것 같은 실효키표, 상술한 도 107에 도시되는 것 같은 키 공유 파라미터, 및, 상술한 도 108에 도시되는 것 같은 CA 공개키 정보를 기억하고 있다.

또한, 서비스 제공자 단말기(13)는, 제6 실시 형태에 있어서도, 도 104의 키 할당 의뢰서를 생성한다.

키 기억 장치(22) 또는 IC 카드(23)(사용자 User)는, 제6 실시 형태에 있어 서도, 상술한 도 109에 도시된 바와 같은 증명키표, 상술한 도 110에 도시되는 것 같은 인증 정보표, 상술한 도 111에 도시되는 것 같은 키 기억 장치 고유 정보, 상술한 도 112에 도시되는 것 같은 사용자 카운트 정보, 및, 상술한 도 113에 도시되는 것 같은 CA 공개키 정보를 기억하고 있다.

또한, 제6 실시 형태에 있어서도, 키 기억 장치(22)는, 후술하는 도 131의 단계 S604의 「키 할당자와 상호 인증 + 키 공유 처리」에 있어서, SSL, TLS를 이용하여 키 할당자 단말기(12)와 상호 인증을 행하는 경우, 상술한 도 120의 키 기억 장치 PKI 정보를 기억한다.

또한, 제6 실시 형태에 있어서는, 키 기억 장치(22)는, 자기 자신이 암호키(증명키와, 그것과 쌍을 이루는 검증키)를 생성하기 때문에, 생성한 암호키를 일시적으로 기억하기 위한, 상술한 도 121에 도시되는 키 일시 기억표를 보유한다.

즉, 제6 실시 형태에 있어서도, 키 기억 장치(22)는, 온디맨드로 암호키를 생성한 경우, 즉, 키 할당자 단말기(12)에 의해 새로운 인증 방법의 암호키(신규키)의 생성이 요구된 시점에, 암호키(한 쌍의 공개키쌍(Kpr, Kpub))를 생성한 경우, 생성한 암호키(공개키쌍(Kpr, Kpub)의 2개의 키)를 구성 요소로 하는, 도 121의 키 일시 기억표를 생성하여 (공개키쌍(Kpr, Kpub)의 2개의 키를 레코드(행)에 기술하여), 기억(보유)한다.

또한, 제6 실시 형태에 있어서도, 키 기억 장치(22)는, 복수의 암호키의 후보를 미리 기억하는 경우, 상술한 도 122에 도시되는 것 같은 인증용 키표도 보유한다.

즉, 키 기억 장치(22)는, 자기 자신, 또는 다른 장치(도시 생략)에 의해 생성된 도 122의 인증용 키표를 미리 기억해 놓고, 키 할당자 단말기(12)에 의해 새로운 인증 방법의 암호키(신규키)의 생성이 요구된 시점에, 인증용 키표에 기억된 복수의 암호키의 후보로부터 소정의 1개(소정의 한 쌍의 공개키쌍(Kprk, Kpubk))를 신규키로서 추출함으로써, 신규키를 생성한다.

그리고, 키 기억 장치(22)는, 생성한 신규키(추출한 신규키의 후보인, 한 쌍의 공개키쌍(Kprk, Kpubk))를 구성 요소로 하는, 도 121의 키 일시 기억표를 생성하여, 기억(보유)한다.

어카운트 관리자 단말기(15)는, 제6 실시 형태에 있어서도, 상술한 도 21의 어카운트 관리표, 및, 상술한 도 22의 어카운트 관리자 고유키를 보유하고 있다.

인증 센터 단말기(211)는, 제6 실시 형태에 있어서도, 상술한 도 65에 도시되는 것 같은 CA 키 정보, 및, 상술한 도 64에 도시되는 것 같은 증명서표를 보유하고 있다.

또한, 인증 센터 단말기(211)(인증 센터 CA)는, 도 66에 도시되는 것 같은 증명서를 발행한다.

다음으로, 본 발명의 제6 실시 형태가 적용되는 인증키 할당 시스템(301)(도 72)의 동작을 설명한다.

제6 실시 형태에 있어서의 인증키 할당 시스템(301)의 동작의 개략은, 본 발명의 제4 실시 형태의 그것과 기본적으로 마찬가지이다.

따라서, 본 발명의 제6 실시 형태가 적용되는 인증키 할당 시스템(301)의 동 작도, 제4 실시 형태의 설명과 같이, 도 23의 흐름도를 참조하여 설명한다.

처음에, 단계 S1에 있어서, 「서비스 선택/키 할당 처리」가 실행된다.

제6 실시 형태에 있어서의 「서비스 선택/키 할당 처리」는, 제4 실시 형태의 그것과, 기본적으로 마찬가지의 처리가 되지만, 약간 차이가 있다.

이러한 제6 실시 형태에 있어서의 「서비스 선택/키 할당 처리」의 상세가, 도 131 내지 도 133의 흐름도와, 도 134의 애로우 차트에 도시되고 있다. 도 131 내지 도 133의 흐름도는, 도 134의 애로우 차트에 도시되는 각 장치의 「서비스 선택/키 할당 처리」를 도시하고 있다. 즉, 도 131은, 사용자 장치(11)(도 72)의 「서비스 선택/키 할당 처리」를, 도 132는, 키 할당자 단말기(12)(도 72)의 「서비스 선택/키 할당 처리」를, 도 133은, 서비스 제공자 단말기(13)(도 72)의 「서비스 선택/키 할당 처리」를, 각각 도시하고 있다.

그래서, 여기서는, 제4 실시 형태에 있어서 설명한 처리에 대해서는, 그 설명을 적절하게 생략하고, 이하, 도 134의 애로우 차트를 참조하여, 제4 실시 형태와는 다른 처리를 중심으로 설명한다.

도 134에 도시된 바와 같이, 처음에, 단계 601에 있어서, 사용자 단말기(21)는, 서비스(선택 서비스)를 선택하여, 그것을 서비스 제공자 단말기(13)로 송부한다.

서비스 제공자 단말기(13)는, 단계 S641에 있어서, 선택 서비스를 수취하고, 단계 S642에 있어서, 도 104의 키 할당 의뢰서를 생성하여, 키 기억 장치(22)로 송부한다.

키 기억 장치(22)는, 단계 S602에 있어서, 키 할당 의뢰서를 수취하여, 일시적으로 기억함과 동시에, 단계 S603에 있어서, 키 할당자 단말기(12)로 송부한다.

키 할당자 단말기(12)는, 단계 S621에 있어서, 키 할당 의뢰서를 수취하면, 키 할당 의뢰서의 서비스 제공자 단말기(13)의 메시지 인증 코드를 검증한다.

키 할당자 단말기(12)가, 키 할당 의뢰서를 수취하면, 키 기억 장치(22)와 키 할당자 단말기(12)의 각각은, 단계 S622의 처리(키 할당자 단말기(12)측의 「키 기억 장치와 상호 인증 + 키 공용 처리」), 또는, 단계 S604의 처리(키 기억 장치(22)측의 「키 할당자와 상호 인증 + 키 공용 처리」)를 실행한다.

상세하게는, 예를 들면, 키 기억 장치(22)가, 도 120의 키 기억 장치 PKI 정보를 기억하지 않는 경우, 제6 실시 형태에 있어서의 단계 S522의 처리(「키 기억 장치와 상호 인증 + 키 공유 처리」), 및, 단계 S504의 처리(「키 할당자와 상호 인증 + 키 공유 처리」)는, 상술한 제4 실시 형태와 마찬가지의 처리가 된다. 따라서, 이들의 설명은 생략한다.

이것에 대하여, 예를 들면, 키 기억 장치(22)가, 도 120의 키 기억 장치 PKI 정보를 기억하고 있는 경우, 상술한 바와 같이, 단계 S622의 처리(「키 기억 장치와 상호 인증 + 키 공유 처리」), 및, 단계 S604의 처리(「키 할당자와 상호 인증 + 키 공유 처리」)는, 예를 들면, 상술한 도 129에 도시되는 처리(SSL, TLS를 이용한 처리)가 실행된다. 또한, 이들의 SSL, TLS를 이용한 처리에 대해서도 상술하였기 때문에, 이들의 설명은 생략한다.

그리고, 키 기억 장치(22)와 키 할당자 단말기(12)의 각각은, 단계 S623의 처리(키 할당자 단말기(12)측의 「키 기억 장치의 사용자 인증 처리」), 또는, 단계 S605의 처리(키 기억 장치(22)측의 「사용자 인증 응답 처리」)를 실행한다.

또한, 제6 실시 형태에 있어서의 단계 S623의 처리(「키 기억 장치의 사용자 인증 처리」), 및, 단계 S605의 처리(「사용자 인증 응답 처리」)는, 상술한 제4 실시 형태에 있어서의 이들과 마찬가지가 되기 때문에, 이들의 설명은 생략한다.

그런데, 상술한 바와 같이, 제4 실시 형태에 있어서는, 「키 기억 장치의 사용자 인증 처리(제6 실시 형태의 단계 S623(도 134)에 대응하는 단계 S423(도 117)의 처리)」, 및, 「사용자 인증 응답 처리(제6 실시 형태의 단계 S605(도 134)에 대응하는 단계 S405(도 117)의 처리)」가 실행되면, 키 할당자 단말기(12)가, 단계 S424(도 117)의 처리에서, 신규키를 생성하여, 사용자 장치(22)로 송부하고, 사용자 장치(22)가, 단계 S406의 처리에서, 그 신규키를 수취한다.

이것에 대하여, 도 134에 도시된 바와 같이, 제6 실시 형태에 있어서는, 제5 실시 형태와 같이, 「키 기억 장치의 사용자 인증 처리(단계 S623의 처리)」, 및, 「사용자 인증 응답 처리(단계 S605의 처리)」가 실행되면, 키 할당자 단말기(12)와 사용자 장치(11)(키 기억 장치(22))의 각각은, 「신규키 요구 및 수취 처리(단계 S624의 처리)」, 또는, 「신규키 생성 및 송부 처리(단계 S606의 처리)」를 실행한다.

제6 실시 형태에 있어서의, 「신규키 요구 및 수취 처리(단계 S624의 처리)」와, 「신규키 생성 및 수취 처리(단계 S643의 처리)」의 상세가, 도 135의 애로우 차트에 도시되고 있다.

그래서, 도 135의 애로우 차트를 참조하여, 제6 실시 형태에 있어서의 「신규키 요구 및 수취 처리(단계 S624의 처리)」와, 「신규키 생성 및 수취 처리(단계 S606의 처리)」의 상세에 대하여 설명한다.

도 135에 도시된 바와 같이, 처음에, 단계 S624-1에 있어서, 키 할당자 단말기(12)는, 키 생성 요구 'GENERATE-KEY'를 생성한다. 키 할당자 단말기(12)는, 생성한 키 생성 요구 'GENERATE-KEY'와, 단계 S622(도 134)의 「키 기억 장치와 상호 인증 + 키 공유 처리」에 의해 사용자 장치(11)(키 기억 장치(22))와 공유한 일시 암호키 Kses를 이용하여, 메시지 인증 코드 MAC('GENERATE-KEY')=E(Kses, h('GENERATE-KEY'))를 생성한다. 그리고, 키 할당자 단말기(12)는, 키 생성 요구 'GENERATE-KEY'와, 메시지 인증 코드 MAC('GENERATE-KEY')=E(Kses, h('GENERATE-KEY'))를 연결한다. 즉, 키 할당자 단말기(12)는, 신규키의 생성을 요구하는 요구 정보로서, 연결 데이터 'GENERATE-KEY'‖MAC('GENERATE-KEY')를 생성한다.

단계 S624-2에 있어서, 키 할당자 단말기(12)는, 연결 데이터 'GENERATE-KEY'‖MAC('GENERATE-KEY')를 송부하면, 단계 S606-1에 있어서, 사용자 장치(키 기억 장치(22))가 그것을 수취한다.

그리고, 키 기억 장치(22)는, 단계 S606-2에 있어서, 메시지 인증 코드의 검증을 행하여, 키 생성 요구 'GENERATE-KEY'의 개찬 및 정당성의 검증을 행한다.

검증이 성공한 경우, 키 기억 장치(22)는, 단계 S606-3에 있어서, 신규키, 즉, 공개키 암호의 비밀키와 공개키의 쌍인 공개 암호키쌍(Kpr, Kpub)을 새롭게 생성한다. 이 공개키쌍(Kpr, Kpub)이, 새롭게 할당되는 인증 방법의 증명키 및 검증 키로서 이용된다.

구체적으로는, 예를 들면, 키 기억 장치(22)가, 도 118에 도시된 바와 같이 구성되는 경우, 난수 발생부(401)는, 난수를 발생시키고, 연산 처리부(56)는, 예를 들면, IEEE-P1363에 의해 규정되어 있는 방법 등에 따라서, 난수 발생부(401)에 의해 발생된 난수로부터 공개키쌍(Kpr, Kpub)을 새롭게 생성한다.

그리고, 연산 처리부(56)는, 생성한 공개키쌍(Kpr, Kpub)의 2개의 키를 구성 요소로 하는, 도 121의 키 일시 기억표를 생성하여, 키 기억부(54)에 기억한다.

또는, 예를 들면, 키 기억 장치(22)가, 도 118에 도시된 바와 같이 구성되는 경우, 단계 S606의 「신규키 생성 및 송부 처리」보다도 시간적으로 전에, 연산 처리부(56)가, 예를 들면, IEEE-P1363에 의해 규정되어 있는 방법 등에 따라서, 난수 발생부(401)에 의해 발생된 복수의 난수의 각각으로부터, 복수의 공개키쌍(Kprn, Kpubn)을 미리 생성하고, 생성한 복수의 공개키쌍(Kprn, Kpubn)의 각각에 대하여, Index로서 Idn을 부여한다.

그리고, 연산 처리부(56)는, 도 122에 도시되는 인증용 키표의 n 레코드(행)에 있어서, Indx의 항목에 IDn을, 증명키의 항목에, 생성한 복수의 공개키쌍(Kprn, Kpubn) 중의 비밀키 Kprn을, 검증키의 항목에, 생성한 복수의 공개키쌍(Kprn, Kpubn) 중의 검증키 Kpubn을, 각각을 기술하여, 키 기억부(54)에 기억한다.

또한, 지금의 경우, 도 122의 인증용 키표에 포함되는 암호키의 후보(증명키(후보) Kprn과 검증키(후보) Kpubn)의 모두는, 키 기억 장치(22)에 의해 생성되었지만, 상술한 바와 같이, 도 122의 인증용 키표에 포함되는 암호키의 후보(증명키(후보) Kprn과 검증키(후보) Kpubn) 중의 적어도 일부가, 키 기억 장치(22)와는 상이한 다른 장치에 의해 생성되어도 된다.

이와 같이 하여, 도 122의 인증용 키표가, 키 기억부(54)에 미리 기억된 상태에서, 키 기억 장치(22)는, 단계 S606-1에 있어서, 키 할당자 단말기(12)로부터 송부된 연결 데이터 'GENERATE-KEY'‖MAC('GENERATE-KEY')을 수취하면, 단계 S606-2에 있어서, 메시지 인증 코드의 검증을 행하여, 키 생성 요구 'GENERATE-KEY'의 개찬 및 정당성의 검증을 행한다.

검증이 성공한 경우, 단계 S560-3에 있어서, 연산 처리부(56)는, 키 기억부(54)에 기억되어 있는, 도 122의 인증용 키표의 각 레코드(행)의 각각에 포함되는 복수의 신규키의 후보, 즉, 복수의 공개키쌍(Kprn, Kpubn)의 중에서 소정의 1개(공개키쌍(Kprnk, Kpubk)(k는, n으로 표시되는 정수치 중의 소정의 1개의 값))를 추출함으로써, 신규키를 생성한다. 즉, 생성된 신규키(추출된 공개키쌍(Kprnk, Kpubk))가, 새롭게 할당되는 인증 방법의 증명키 및 검증키로서 이용된다.

그리고, 연산 처리부(56)는, 선택한 공개키쌍(Kprnk, Kpubk)의 2개의 키의 각각을 구성 요소로 하는, 도 121의 키 일시 기억표를 생성하여, 키 기억부(54)에 기억함과 함께, 도 122의 인증용 키표 중의, 선택한 공개키쌍(Kprnk, Kprk)

에 대응하는 레코드(k 행)를 삭제한다.

이와 같이 하여, 도 121의 키 일시 기억표가 키 기억부(54)에 기억되면, 단계 S606-4에 있어서, 키 기억 장치(22)는, 공개키, 즉, 검증키 Kpub를 송부하면, 단계 S624-3에 있어서, 키 할당자 단말기(12)는, 그것을 수취한다.

구체적으로는, 예를 들면, 키 기억 장치(22)는, 단계 S606-3의 처리에서 생성한 (키 일시 기억표에 기억된) 공개키쌍(Kpr, Kpub) 중의 검증키 Kpub와, 단계 S604(도 134)의 「키 할당자와 상호 인증 + 키 공유 처리」에 의해 키 할당자 단말기(12)와 공유한 일시 암호키 Kses를 이용하여 메시지 인증 코드 MAC(Kpub)=E(Kses, h(Kpub))를 생성한다. 그리고, 키 기억 장치(22)는, 검증키 Kpub와, 메시지 인증 코드 MAC(Kpub)를 연결한다. 즉, 키 기억 장치(22)는, 연결 데이터 Kpub‖MAC(Kpub)를 생성한다.

생성된 연결 데이터 Kpub1폭 AC(Kpub)은, 사용자 장치(11)부로부터 송부되어, 키 할당자 단말기(12)에 수취된다.

그렇게 하면, 키 할당자 단말기(12)는, 단계 S624-4에 있어서, 연결 데이터 Kpub‖MAC(Kpub)의 메시지 인증 코드 MAC(Kpub)의 검증을 행한다.

도 134로 되돌아가, 검증이 성공하면, 키 할당자 단말기(12)는, 단계 S625에 있어서, 도 103의 권리 증서를 생성하여, 키 기억 장치(22)로 송부한다.

동시에, 키 할당자 단말기(12)는, 도 130의 키 할당표에, 할당을 행한 인증 방법의 식별 번호 KID, 할당한 상대의 사용자의 식별 번호 AID, 할당한 키 기억 장치의 식별 번호 HWID, 권리증서 Rcert, 및, 검증키 Kpub 등으로 이루어지는 레코드를 추가한다.

그리고, 키 할당자 단말기(12)는, 단계 S626에 있어서, 단계 S622의 「키 기억 장치와 상호 인증 + 키 공유 처리」에서 특정한 사용자 User(사용자 단말기(21))에 대하여, 권리증서의 서비스 내용과 키 할당의 수수료의 합계에 적당 한 과금을 행한다.

키 기억 장치(22)는, 단계 S607에 있어서, 권리 증서를 수취한다.

그리고, 키 기억 장치(22)는, 수취한 권리 증서에 대하여, 전자 서명이 키 할당자 단말기(12)(키 할당자 KA)에 의해서 생성되어 있는 것을 확인한 후에, 권리 증서에 포함되는 식별 번호 KID와 권리증서 Rcert로 이루어지는 새로운 레코드를, 도 110의 인증 정보표에 추가한다.

또한, 키 기억 장치(22)는, 권리 증서에 포함되는 식별 번호 KID, 및, 도 121의 키 일시 기억표에 기억되어 있는 증명키 Kpr로 이루어지는 새로운 레코드를, 도 109의 증명키표에 추가한다.

그 후, 키 기억 장치(22)는, 도 121의 키 일시 기억표에 기억하고 있었던 증명키 Kpr와 검증키 Kpub를 삭제한다.

도 23으로 되돌아가, 단계 S1의 처리(「서비스 선택/키 할당 처리」)가 실행되면, 단계 S2에 있어서, 「키 사용/서비스 제공 처리」가 실행된다.

제6 실시 형태의 「키 사용/서비스 제공 처리」(단계 S2의 처리)는, 상술한 제4 실시 형태의 그것과 마찬가지이다. 즉, 제6 실시 형태에 있어서도, 「키 사용/서비스 제공 처리」는, 상술한 도 114 내지 도 116의 흐름도(도 117의 애로우 차트)에 따라서 실행된다.

단계 S2의 처리(「키 사용/서비스 제공 처리」)가 종료하면, 필요에 따라, 단계 S6의 처리(「키 삭제 처리」)와, 단계 S7의 처리(「키 사용 정지 처리」)가 실행된다.

제6 실시 형태의 「키 삭제 처리」(단계 S6의 처리)는, 상술한 제4 실시 형태의 그것(즉, 제2 실시 형태의 그것)과 마찬가지이다. 즉, 제6 실시 형태에 있어서도, 「키 삭제 처리」는, 상술한 도 37 내지 도 39 중의 어느 하나의 흐름도에 따라서 실행된다.

단, 제6 실시 형태에 있어서는, 삭제의 대상이 되는 것은, 키 할당자 단말기(12)인 경우, 도 130의 키 할당표가 되고, 서비스 제공자 단말기(13)인 경우, 도 106의 실효키표가 되고, 키 기억 장치(22)인 경우, 도 109의 증명키표, 및, 도 110의 인증 정보표가 된다.

제6 실시 형태의 「키 사용 정지 처리」(단계 S7의 처리)는, 상술한 제4 실시 형태의 그것과 마찬가지이다. 즉, 제5 실시 형태에 있어서도, 「키 사용 정지 처리」는, 상술한 도 40과 도 41의 흐름도에 따라서 실행된다.

단, 제6 실시 형태에 있어서의 「키 사용 정지 처리」에 있어서는, 제4 실시 형태와 같이, 서비스 제공자 단말기(13)는, 제2 실시 형태에 있어서의 도 53의 인증 정보표에 대응하는 것을 기억하지 않기 때문에, 인증 정보표로부터 레코드를 삭제하는 처리는 생략된다.

또한, 도 40의 단계 S161의 처리에서, 키 할당자 단말기(12)에 의해 생성되어, 서비스 제공자 단말기(13)로 송부되는 키 사용 정지 요구서의 형식은, 제1 실시 형태 마찬가지에 있어서는, 도 42의 형식이 되는 데 대하여, 제6 실시 형태에 있어서는, 제4 실시 형태와 같이, 도 42, 도 43 중의 어느 형식이라고 되더라도 된다..

이와 같이, 제6 실시 형태가 적용되는 인증키 할당 시스템(301)은, 제4 실시 형태에 대응하는 실시 형태이기 때문에, 당연하면서, 상술한 (1) 내지 (6)의 효과를 발휘하는 것이 가능하게 된다.

또한, 제6 실시 형태가 적용되는 인증키 할당 시스템(301)은, 제5 실시 형태의 그것과 마찬가지로, 사용자 User가 보유하는 키 기억 장치(22)가 신규키를 생성하기 때문에, 당연하면서, 상술한 (7) 내지 (10)로 기술되는 것 같은 효과를 발휘하는 것이 가능하게 된다.

또한, 제5 실시 형태나 제6 실시 형태와 같이, 제1 실시 형태나 제3 실시 형태에 대한 실시 형태로서, 사용자 User가 보유하는 키 기억 장치(22)가 신규키를 생성하는 실시 형태도 용이하게 실현 가능하다.

즉, 제5 실시 형태나 제6 실시 형태와 같이, 제1 실시 형태나 제3 실시 형태에 대하고, 또한, 사용자 User가 보유하는 키 기억 장치(22)가 신규키를 생성하는 방법을 적용하는 것이 가능하다.

또한, 상술한 일련의 처리를 실행시키는 프로그램은, 네트워크나 기록 매체로부터 인스톨된다. 이 기록 매체는, 도 15, 도 18, 도 19, 도 20, 및, 도 45에 도시된 바와 같이, 장치 본체와는 별도로, 소유자 등에 프로그램을 제공하기 위해서 배포되어, 드라이브(40, 90, 110, 130, 또는, 230)에 장착되는, 프로그램이 기록되어 있는 자기 디스크(플로피 디스크를 포함), 광 디스크(CD-ROM(Compact Disk-Read Only Memory), DVD(Digital Versatile Disk)를 포함), 광자기 디스크(MD(Mini-Disk)를 포함), 또는 반도체 메모리 등의 리무버블 기록 매체(패키 지 미디어)(41, 91, 111, 131, 또는, 231)로 구성되는 것뿐만 아니라, 장치 본체에 미리 내장된 상태에서 사용자에게 제공되는, 프로그램이 기록되어 있는 ROM(32, 82, 102, 122, 또는, 222)이나, 기억부(38, 88, 108, 128, 또는, 228)에 포함되는 하드디스크 등으로 구성된다.

또한, 본 명세서에 있어서, 상술한 일련의 처리를 실행하는 단계는, 기재된 순서에 따라서 시계열적으로 행해지는 처리는 물론, 반드시 시계열적으로 처리되지 않더라도, 병렬적 또는 개별적으로 실행되는 처리도 포함하는 것이다.

또한, 본 명세서에 있어서, 시스템이란, 복수의 장치나 처리부로 구성되는 장치 전체를 나타내는 것이다.

산업상 이용 가능성

이상과 같이, 본 발명에 따르면, 서비스 제공자가, 사용자를 인증할 수 있다. 또한, 본 발명에 따르면, 서비스 제공자가, 사용자를 인증하는 경우에, 그 인증의 효율과 안전성을 높일 수 있다.

(57) 청구의 범위

청구항 1.

제1 내지 제3 정보 처리 장치로 이루어지는 정보 처리 시스템에 있어서,

상기 제1 정보 처리 장치는, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키를 생성하고, 생성한 상기 제1 암호키를 상기 제2 정보 처리 장치로 송부함과 함께, 생성한 상기 제2 암호키를 상기 제3 정보 처리 장치로 송부하고,

상기 제2 정보 처리 장치는, 상기 제1 정보 처리 장치에 의해 송부된 상기 제1 암호키를 수취하고, 또한, 기억하고,

상기 제3 정보 처리 장치는, 상기 제1 정보 처리 장치에 의해 송부된 상기 제2 암호키를 수취하고, 또한, 기억하고,

상기 제2 정보 처리 장치는, 기억한 상기 제1 암호키, 및, 상기 제3 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기초하여, 상기 제3 정보 처리 장치를 인증하는 것을 특징으로 하는 정보 처리 시스템.

청구항 2.
제1항에 있어서,

상기 인증 방법은, 공통 키 인증이고,

상기 제1 암호키와 상기 제2 암호키는 동일한 암호키인 것을 특징으로 하는 정보 처리 시스템.

청구항 3.
제1항에 있어서,

상기 인증 방법은, 공개키 인증이고,

상기 제1 암호키와 상기 제2 암호키는 서로 다른 암호키인 것을 특징으로 하는 정보 처리 시스템.

청구항 4.
제1 내지 제3 정보 처리 장치로 이루어지는 정보 처리 시스템의 정보 처리 방법에 있어서,

상기 제1 정보 처리 장치는, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키를 생성하고, 생성한 상기 제1 암호키를 상기 제2 정보 처리 장치로 송부함과 함께, 생성한 상기 제2 암호키를 상기 제3 정보 처리 장치로 송부하고,

상기 제2 정보 처리 장치는, 상기 제1 정보 처리 장치에 의해 송부된 상기 제1 암호키를 수취하고, 또한, 기억하고,

상기 제3 정보 처리 장치는, 상기 제1 정보 처리 장치에 의해 송부된 상기 제2 암호키를 수취하고, 또한, 기억하고,

상기 제2 정보 처리 장치는, 기억한 상기 제1 암호키, 및, 상기 제3 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기초하여, 상기 제3 정보 처리 장치를 인증하는 것을 특징으로 하는 정보 처리 방법.

청구항 5.
다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키를 생성하는 생성 수단과,

상기 생성 수단에 의해 생성된 상기 제1 암호키를 상기 다른 제1 정보 처리 장치로 송부함과 함께, 상기 생성 수단에 의해 생성된 상기 제2 암호키를 상기 다른 제2 정보 처리 장치로 송부하는 송부 수단

을 포함하는 것을 특징으로 하는 정보 처리 장치.

청구항 6.
제5항에 있어서,

상기 인증 방법은, 공통 키 인증이고,

상기 생성 수단에 의해 생성되는 상기 제1 암호키와 상기 제2 암호키는 동일한 암호키인 것을 특징으로 하는 정보 처리 장치.

청구항 7.
제5항에 있어서,

상기 인증 방법은, 공개키 인증이고,

상기 생성 수단에 의해 생성되는 상기 제1 암호키와 상기 제2 암호키는 서로 다른 암호키인 것을 특징으로 하는 정보 처리 장치.

청구항 8.
제5항에 있어서,

상기 다른 제2 정보 처리 장치에, 인증을 위한 정보가 입력될지, 또는, 인증을 위해 이용되는 소정의 장치가 접속된 경우, 상기 정보를 입력한 사용자, 또는, 접속된 상기 장치를 특정하는 특정 수단을 더 구비하며,

상기 생성 수단은, 상기 특정 수단에 의해, 상기 다른 제2 정보 처리 장치에 상기 정보를 입력한 사용자, 또는, 상기 다른 제2 정보 처리 장치에 접속된 상기 장치가 특정된 경우, 상기 제1 및 상기 제2 암호키를 생성하는 것을 특징으로 하는 정보 처리 장치.

청구항 9.
제8항에 있어서,

상기 특정 수단은, SSL(Secure Socket Layer), 또는,

TLS(Transport Layer Security)를 사용하여, 상기 다른 제2 정보 처리 장치에 상기 정보를 입력한 상기 사용자, 또는, 상기 다른 제2 정보 처리 장치에 접속된 상기 장치를 특정하는 것을 특징으로 하는 정보 처리 장치.

청구항 10.
제5항에 있어서,

상기 생성 수단에 의해 상기 제1 및 상기 제2 암호키가 생성된 경우, 상기 송부 수단에 의해 상기 제1 암호키가 송부되는 상대인 상기 다른 제1 정보 처리 장치가, 상기 제1 및 상기 제2 키를 이용하여 인증하는 상기 다른 제2 정보 처리 장치에 대하여 제공하는 서비스의 댓가를 확정하고, 상기 특정 수단에 의해 특정된 상기 다른 제2 정보 처리 장치에 상기 정보를 입력한 상기 사용자, 또는, 상기 특정 수단에 의해 특정된, 상기 다른 제2 정보 처리 장치에 접속된 상기 장치에 의해서 특정되는 사용자에게 대하여, 상기 서비스의 댓가의 과금을 행하는 과금 수단을 더 구비하는 것을 특징으로 하는 정보 처리 장치.

청구항 11.
제10항에 있어서,

상기 과금 수단은, 상기 다른 제2 정보 처리 장치에 대하여, 상기 서비스에 대한 댓가와 함께, 또한, 상기 생성 수단에 의해 생성된 상기 제1 및 상기 제2 암호키에 대한 댓가의 과금을 행하는 것을 특징으로 하는 정보 처리 장치.

청구항 12.
정보 처리 장치의 정보 처리 방법에 있어서,

다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키를 생성하는 생성 단계와,

상기 생성 단계의 처리에 의해 생성된 상기 제1 암호키를 상기 다른 제1 정보 처리 장치로 송부함과 함께, 상기 생성 단계의 처리에 의해 생성된 상기 제2 암호키를 상기 다른 제2 정보 처리 장치로 송부하는 송부 단계를 포함하는 것을 특징으로 하는 정보 처리 방법.

청구항 13.
정보 처리 장치를 제어하는 컴퓨터의 프로그램으로서,

다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키를 생성하는 생성 단계와,

상기 생성 단계의 처리에 의해 생성된 상기 제1 암호키를 상기 다른 제1 정보 처리 장치로 송부함과 함께, 상기 생성 단계의 처리에 의해 생성된 상기 제2 암호키를 상기 다른 제2 정보 처리 장치로 송부하는 송부 단계를 포함하는 것을 특징으로 하는 컴퓨터가 판독 가능한 프로그램이 기록되어 있는 기록 매체.

청구항 14.
정보 처리 장치를 제어하는 컴퓨터에,

다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키를 생성하는 생성 단계와,

상기 생성 단계의 처리에 의해 생성된 상기 제1 암호키를 상기 다른 제1 정보 처리 장치로 송부함과 함께, 상기 생성 단계의 처리에 의해 생성된 상기 제2 암호키를 상기 다른 제2 정보 처리 장치로 송부하는 송부 단계를 실행시키는 것을 특징으로 하는 프로그램.

청구항 15.
다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 상기 제1 암호키를 수취하는 수취 수단과,

상기 수취 수단에 의해 수취된 상기 제1 암호키를 기억하는 기억 수단과,

상기 기억 수단에 의해 기억된 상기 제1 암호키, 및, 상기 다른 제2 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기초하여, 상기 다른 제2 정보 처리 장치를 인증하는 인증 수단을 포함하는 것을 특징으로 하는 정보 처리 장치.

청구항 16.
제15항에 있어서,

상기 인증 방법은, 공통 키 인증이고, 상기 제1 암호키와 상기 제2 암호키는 동일한 암호키인 것을 특징으로 하는 정보 처리 장치.

청구항 17.
제15항에 있어서,

상기 인증 방법은, 공개키 인증이고,

상기 제1 암호키와 상기 제2 암호키는 서로 다른 암호키인 것을 특징으로 하는 정보 처리 장치.

청구항 18.
정보 처리 장치의 정보 처리 방법에 있어서,

다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 상기 제1 암호키를 수취하는 수취 단계와,

상기 수취 단계의 처리에 의해 수취된 상기 제1 암호키를 기억하는 기억 단계와,

상기 기억 단계의 처리에 의해 기억된 상기 제1 암호키, 및, 상기 다른 제2 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기 초하여, 상기 다른 제2 정보 처리 장치를 인증하는 인증 단계를 포함하는 것을 특징으로 하는 정보 처리 방법.

청구항 19.
정보 처리 장치를 제어하는 컴퓨터의 프로그램으로서,

다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 상기 제1 암호키를 수취하는 수취 단계와,

상기 수취 단계의 처리에 의해 수취된 상기 제1 암호키를 기억하는 기억 단계와,

상기 기억 단계의 처리에 의해 기억된 상기 제1 암호키, 및, 상기 다른 제2 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기초하여, 상기 다른 제2 정보 처리 장치를 인증하는 인증 단계를 포함하는 것을 특징으로 하는 컴퓨터가 판독 가능한 프로그램이 기록되어 있는 기록 매체.

청구항 20.
정보 처리 장치를 제어하는 컴퓨터에,

다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 상기 제1 암호키를 수취하는 수취 단계와,

상기 수취 단계의 처리에 의해 수취된 상기 제1 암호키를 기억하는 기억 단계와,

상기 기억 단계의 처리에 의해 기억된 상기 제1 암호키, 및, 상기 다른 제2 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기초하여, 상기 다른 제2 정보 처리 장치를 인증하는 인증 단계를 실행시키는 것을 특징으로 하는 프로그램.

청구항 21.
다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 상기 제2 암호키를 수취하는 수취 수단과,

상기 수취 수단에 의해 수취된 상기 제2 암호키를 기억하는 기억 수단과,

상기 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 상기 인증 방법에 기초하여, 자기 자신이 인증되는 경우, 상기 기억 수단에 의해 기억된 상기 제2 암호키를 이용하여, 소정의 응답을 상기 다른 제2 정보 처리 장치로 송부하는 응답 수단을 포함하는 것을 특징으로 하는 정보 처리 장치.

청구항 22.
제21항에 있어서,

상기 인증 방법은, 공통 키 인증이고,

상기 제1 암호키와 상기 제2 암호키는 동일한 암호키인 것을 특징으로 하는 정보 처리 장치.

청구항 23.
제21항에 있어서,

상기 인증 방법은, 공개키 인증이고,

상기 제1 암호키와 상기 제2 암호키는 서로 다른 암호키인 것을 특징으로 하는 정보 처리 장치.

청구항 24.
제21항에 있어서,

상기 다른 제2 정보 처리 장치에 의해 인증되기 위한 정보를 입력하는 입력 수단을 더 구비하는 것을 특징으로 하는 정보 처리 장치.

청구항 25.
제21항에 있어서,

상기 다른 제2 정보 처리 장치에 의해 인증되는 경우에 이용하는 소정의 장치를 접속하는 접속 수단을 더 구비하는 것을 특징으로 하는 정보 처리 장치.

청구항 26.
제21항에 있어서,

상기 접속 수단에 접속되는 상기 장치는, IC 카드인 것을 특징으로 하는 정보 처리 장치.

청구항 27.
제21항에 있어서,

상기 기억 수단은, 내탬퍼성을 갖는 것을 특징으로 하는 정보 처리 장치.

청구항 28.
정보 처리 장치의 정보 처리 방법에 있어서,

다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 상기 제2 암호키를 수취하는 수취 단계와,

상기 수취 단계의 처리에 의해 수취된 상기 제2 암호키의 기억을 제어하는 기억 제어 단계와,

상기 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 상기 인증 방법에 기초하여, 상기 정보 처리 장치가 인증되는 경우, 상기 기억 제어 단계의 처리에 의해 기억이 제어된 상기 제2 암호키를 이용하여, 소정의 응답을 상기 다른 제2 정보 처리 장치로 송부하는 응답 단계를 포함하는 것을 특징으로 하는 정보 처리 방법.

청구항 29.
정보 처리 장치를 제어하는 컴퓨터의 프로그램으로서,

다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 상기 제2 암호키를 수취하는 수취 단계와,

상기 수취 단계의 처리에 의해 수취된 상기 제2 암호키의 기억을 제어하는 기억 제어 단계와,

상기 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 상기 인증 방법에 기초하여, 상기 정보 처리 장치가 인증되는 경우, 상기 기억 제어 단계의 처리에 의해 기억이 제어된 상기 제2 암호키를 이용하여, 소정의 응답을 상기 다른 제2 정보 처리 장치로 송부하는 응답 단계를 포함하는 것을 특징으로 하는 컴퓨터가 판독 가능한 프로그램이 기록되어 있는 기록 매체.

청구항 30.
정보 처리 장치를 제어하는 컴퓨터에,

다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키 중의, 적어도 상기 제2 암호키를 수취하는 수취 단계와,

상기 수취 단계의 처리에 의해 수취된 상기 제2 암호키의 기억을 제어하는 기억 제어 단계와,

상기 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 상기 인증 방법에 기초하여, 상기 정보 처리 장치가 인증되는 경우, 상기 기억 제어 단계의 처리에 의해 기억이 제어된 상기 제2 암호키를 이용하여, 소정의 응답을 상기 다른 제2 정보 처리 장치로 송부하는 응답 단계를 실행시키는 것을 특징으로 하는 프로그램.

청구항 31.
제1 내지 제3 정보 처리 장치로 이루어지는 정보 처리 시스템에 있어서,

상기 제1 정보 처리 장치는, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보를 생성하여, 상기 제2 정보 처리 장치로 송부하고,

상기 제2 정보 처리 장치는, 상기 제1 정보 처리 장치에서의 상기 요구 정보 를 수취하면, 상기 제1 암호키와 상기 제2 암호키의 각각을 생성하고, 생성한 상기 제1 암호키를 상기 제3 정보 처리 장치로 송부함과 함께, 생성한 상기 제2 암호키를 기억하고,

상기 제3 정보 처리 장치는, 상기 제2 정보 처리 장치에 의해 송부된 상기 제1 암호키를 수취하고, 또한, 기억하고,

상기 제3 정보 처리 장치는, 기억된 상기 제1 암호키, 및, 상기 제2 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기초하여, 상기 제2 정보 처리 장치를 인증하는 것을 특징으로 하는 정보 처리 시스템.

청구항 32.
제31항에 있어서,

상기 인증 방법은, 공개키 인증이고,

상기 제1 암호키와 상기 제2 암호키는 서로 다른 암호키인 것을 특징으로 하는 정보 처리 시스템.

청구항 33.
제1 내지 제3 정보 처리 장치로 이루어지는 정보 처리 시스템의 정보 처리 방법에 있어서,

상기 제1 정보 처리 장치는, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2

암호키의 생성을 요구하는 요구 정보를 생성하여, 상기 제2 정보 처리 장치로 송부하고,

상기 제2 정보 처리 장치는, 상기 제1 정보 처리 장치에서의 상기 요구 정보 를 수취하면, 상기 제1 암호키와 상기 제2 암호키의 각각을 생성하고, 생성한 상기 제1 암호키를 상기 제3 정보 처리 장치로 송부함과 함께, 생성한 상기 제2 암호키를 기억하고,

상기 제3 정보 처리 장치는, 상기 제2 정보 처리 장치에 의해 송부된 상기 제1 암호키를 수취하고, 또한, 기억하고,

상기 제3 정보 처리 장치는, 기억된 상기 제1 암호키, 및, 상기 제2 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기초하여, 상기 제2 정보 처리 장치를 인증하는 것을 특징으로 하는 정보 처리 방법.

청구항 34.
다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보를 생성하는 생성 수단과,

상기 생성 수단에 의해 생성된 상기 요구 정보를 상기 다른 제2 정보 처리 장치로 송부하는 송부 수단

을 포함하는 것을 특징으로 하는 정보 처리 장치.

청구항 35.
제34항에 있어서,

상기 인증 방법은, 공개키 인증이고,

상기 생성 수단에 의해 생성되는 상기 제1 암호키와 상기 제2 암호키는 서로 다른 암호키인 것을 특징으로 하는 정보 처리 장치.

청구항 36.
제34항에 있어서,

상기 다른 제2 정보 처리 장치에, 인증을 위한 정보가 입력되거나, 또는, 인증을 위해 이용되는 소정의 장치가 접속된 경우, 상기 정보를 입력한 사용자, 또는, 접속된 상기 장치를 특정하는 특정 수단을 더 구비하며,

상기 생성 수단은, 상기 특정 수단에 의해, 상기 다른 제2 정보 처리 장치에 상기 정보를 입력한 사용자, 또는, 상기 다른 제2 정보 처리 장치에 접속된 상기 장치가 특정된 경우, 상기 요구 정보를 생성하는 것을 특징으로 하는 정보 처리 장치.

청구항 37.
제36항에 있어서,

상기 특정 수단은, SSL(Secure Socket Layer), 또는,

TLS(Transport Layer Security)를 사용하여, 상기 다른 제2 정보 처리 장치에 상기 정보를 입력한 상기 사용자, 또는, 상기 다른 제2 정보 처리 장치에 접속된 상기 장치를 특정하는 것을 특징으로 하는 정보 처리 장치.

청구항 38.
제34항에 있어서,

상기 송부 수단에 의해 상기 요구 정보가 상기 다른 제2 정보 처리 장치로 송부된 경우, 상기 다른 제1 정보 처리 장치가, 상기 제1 키 및 상기 제2 키를 이용하여 인증하는 상기 다른 제2 정보 처리 장치에 대하여 제공하는 서비스의 댓가 를 확정하고, 상기 특정 수단에 의해 특정된 상기 다른 제2 정보 처리 장치에 상기 정보를 입력한 상기 사용자, 또는, 상기 특정 수단에 의해 특정된, 상기 다른 제2 정보 처리 장치에 접속된 상기 장치에 의해서 특정되는 사용자에게 대하여, 상기 서비스의 댓가의 과금을 행하는 과금 수단을 더 구비하는 것을 특징으로 하는 정보 처리 장치.

청구항 39.
제38항에 있어서,

상기 과금 수단은, 상기 다른 제2 정보 처리 장치에 대하여, 상기 서비스에 대한 댓가와 함께, 또한, 상기 송부 수단으로부터 상기 다른 제2 정보 처리 장치로 송부된 상기 요구 정보를 받아, 상기 다른 제2 정보 처리 장치가 생성한 상기 제1 및 상기 제2 암호키에 대한 댓가의 과금을 행하는 것을 특징으로 하는 정보 처리 장치.

청구항 40.
정보 처리 장치의 정보 처리 방법에 있어서,

다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보를 생성하는 생성 단계와,

상기 생성 단계의 처리에 의해 생성된 상기 요구 정보를 상기 다른 제2 정보 처리 장치로 송부하는 송부 단계

를 포함하는 것을 특징으로 하는 정보 처리 방법.

청구항 41.
정보 처리 장치를 제어하는 컴퓨터의 프로그램으로서,

다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키의 생성을, 상기 다른 제2 정보 처리 장치에 대하여 요구하는 요구 정보를 생성하는 생성 단계를 포함하는 것을 특징으로 하는 컴퓨터가 판독 가능한 프로그램이 기록되어 있는 기록 매체.

청구항 42.
정보 처리 장치를 제어하는 컴퓨터에,

다른 제1 정보 처리 장치가, 소정의 인증 방법에 기초하여, 다른 제2 정보 처리 장치를 인증하는 경우에 이용하는, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키의 생성을, 상기 다른 제2 정보 처리 장치에 대하여 요구하는 요구 정보를 생성하는 생성 단계를 실행시키는 것을 특징으로 하는 프로그램.

청구항 43.
다른 제1 정보 처리 장치의 요구에 의해, 다른 제2 처리 장치가, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키를 생성하고, 생성한 상기 제1 암호키를 송부하여 온 경우, 상기 제1 암호키를 수취하는 수취 수단과,

상기 수취 수단에 의해 수취된 상기 제1 암호키를 기억하는 기억 수단과,

상기 기억 수단에 의해 기억된 상기 제1 암호키, 및, 상기 다른 제2 정보 처 리 장치에 의해 기억된 상기 제2 암호키를 이용하고, 상기 인증 방법에 기초하여, 상기 다른 제2 정보 처리 장치를 인증하는 인증 수단

을 포함하는 것을 특징으로 하는 정보 처리 장치.

청구항 44.
제43항에 있어서,

상기 인증 방법은, 공개키 인증이고,

상기 제1 암호키와 상기 제2 암호키는 서로 다른 암호키인 것을 특징으로 하는 정보 처리 장치.

청구항 45.
정보 처리 장치의 정보 처리 방법에 있어서, 다른 제1 정보 처리 장치의 요구에 의해, 다른 제2 처리 장치가, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키를 생성하고, 생성한 상기 제1 암호키를 송부하여 온 경우, 상기 제1 암호키를 수취하는 수취 단계와,

상기 수취 단계의 처리에 의해 수취된 상기 제1 암호키를 기억하는 기억 단계와,

상기 기억 단계의 처리에 의해 기억된 상기 제1 암호키, 및, 상기 다른 제2 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기초하여, 상기 다른 제2 정보 처리 장치를 인증하는 인증 단계

를 포함하는 것을 특징으로 하는 정보 처리 방법.

청구항 46.
정보 처리 장치를 제어하는 컴퓨터의 프로그램으로서,

다른 제1 정보 처리 장치의 요구에 기초하여, 다른 제2 처리 장치가 생성한, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키 중의, 상기 정보 처리 장치 자신에 의해 기억된 상기 제1 암호키, 및, 상기 다른 제2 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기초하여, 상기 다른 제2 정보 처리 장치를 인증하는 인증 단계를 포함하는 것을 특징으로 하는 컴퓨터가 판독 가능한 프로그램이 기록되어 있는 기록 매체.

청구항 47.
정보 처리 장치를 제어하는 컴퓨터에,

다른 제1 정보 처리 장치의 요구에 기초하여, 다른 제2 처리 장치가 생성한, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키 중의, 상기 정보 처리 장치 자신에 의해 기억된 상기 제1 암호키, 및, 상기 다른 제2 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 상기 인증 방법에 기초하여, 상기 다른 제2 정보 처리 장치를 인증하는 인증 단계를 실행시키는 것을 특징으로 하는 프로그램.

청구항 48.
다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보를 수취하는 수취 수단과,

상기 수취 수단에 의해 수취된 요구 정보에 기초하여, 상기 제1 암호키와 상기 제2 암호키를 생성하는 키 생성 수단과,

전 키기 생성 수단에 의해 생성된 상기 제1 암호키와 상기 제2 암호키 중의, 상기 제1 암호키를 다른 제2 정보 처리 장치로 송부하는 송부 수단과,

상기 키 생성 수단에 의해 생성된 상기 제1 암호키와 상기 제2 암호키 중의, 상기 제2 암호키를 기억하는 기억 수단과,

상기 송부 수단에 의해 송부된 상기 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 상기 인증 방법에 기초하여, 자기 자신이 인증되는 경우, 상기 기억 수단에 의해 기억된 상기 제2 암호키를 이용하여, 소정의 응답을 생성하는 응답 생성 수단

을 구비하며,

상기 송부 수단은, 상기 응답 생성 수단에 의해 생성된 상기 응답을, 상기 다른 제2 정보 처리 장치로 송부하는 것을 특징으로 하는 정보 처리 장치.

청구항 49.
제48항에 있어서,

상기 인증 방법은, 공개키 인증이고,

상기 제1 암호키와 상기 제2 암호키는 서로 다른 암호키인 것을 특징으로 하는 정보 처리 장치.

청구항 50.
제48항에 있어서,

상기 키 생성 수단은, 상기 수취 수단에 의해 상기 요구 정보가 수취된 후, 상기 제1 암호키와 상기 제2 암호키를 새롭게 생성하는 것을 특징으로 하는 정보 처리 장치.

청구항 51.
제48항에 있어서,

상기 기억 수단은, 복수의 제1 암호키의 후보와, 복수의 상기 제1 암호키의 후보의 각각과 쌍을 이루는 복수의 제2 암호키의 후보를 미리 기억하고,

상기 키 생성 수단은, 상기 수취 수단에 의해 상기 요구 정보가 수취된 후, 상기 기억 수단에 미리 기억되어 있는 복수의 상기 제1 암호키의 후보와, 복수의 상기 제2 암호키의 후보의 중에서, 소정의 상기 제1 암호키의 후보와, 그것과 쌍을 이루는 상기 제2 암호키의 후보를 추출하여, 추출한 상기 제1 암호키의 후보를 상기 제1 암호키로 함과 함께, 추출한 상기 제2 암호키의 후보를 상기 제2 암호키로 함으로써, 상기 제1 암호키와 상기 제2 암호키를 생성하는 것을 특징으로 하는 정보 처리 장치.

청구항 52.
제51항에 있어서,

상기 키 생성 수단은, 복수의 상기 제1 암호키의 후보와, 복수의 상기 제2 암호키의 후보를 생성하는 것을 특징으로 하는 정보 처리 장치.

청구항 53.
제48항에 있어서,

상기 다른 제2 정보 처리 장치에 의해 인증되기 위한 정보를 입력하는 입력 수단을 더 구비하는 것을 특징으로 하는 정보 처리 장치.

청구항 54.
제48항에 있어서,

상기 다른 제2 정보 처리 장치에 의해 인증되는 경우에 이용하는 소정의 장치를 접속하는 접속 수단을 더 구비하는 것을 특징으로 하는 정보 처리 장치.

청구항 55.
제54항에 있어서,

상기 접속 수단에 접속되는 상기 장치는, IC 카드인 것을 특징으로 하는 정보 처리 장치.

청구항 56.
제48항에 있어서,

상기 기억 수단은, 내탬퍼성을 갖는 것을 특징으로 하는 정보 처리 장치.

청구항 57.
정보 처리 장치의 정보 처리 방법에 있어서,

다른 제1 정보 처리 장치에 의해 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보를 수취하는 수취 단계와,

상기 수취 단계의 처리에 의해 수취된 요구 정보에 기초하여, 상기 제1 암호키와 상기 제2 암호키를 생성하는 키 생성 단계와,

상기 키 생성 단계의 처리에 의해 생성된 상기 제1 암호키와 상기 제2 암호키 중의, 상기 제1 암호키를 다른 제2 정보 처리 장치로 송부하는 키 송부 단계와,

상기 키 생성 단계의 처리에 의해 생성된 상기 제1 암호키와 상기 제2 암호키 중의, 상기 제2 암호키를 기억하는 기억 단계와,

상기 키 송부 단계의 처리에 의해 송부된 상기 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 상기 인증 방법에 기초하여, 상기 정보 처리 장치가 인증되는 경우, 상기 기억 단계의 처리에 의해 기억된 상기 제2 암호키를 이용하여, 소정의 응답을 생성하는 응답 생성 단계와,

상기 응답 단계의 처리에 의해 생성된 상기 응답을 상기 다른 제2 정보 처리 장치로 송부하는 응답 송부 단계를 포함

하는 것을 특징으로 하는 정보 처리 방법.

청구항 58.
정보 처리 장치를 제어하는 컴퓨터의 프로그램으로서,

다른 제1 정보 처리 장치에서 상기 정보 처리 장치로 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보에 기초하여, 다른 제2 정보 처리 장치로 송신되는 상기 제1 암호키와, 상기 정보 처리 장치에 기억되는 상기 제2 암호키를 생성하는 키 생성 단계와,

송신된 상기 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 상기 인증 방법에 기초하여, 상기 정보 처리 장치가 인증되는 경우, 상기 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 소정의 응답을 생성하는 응답 생성 단계를 포함하는 것을 특징으로 하는 컴퓨터가 판독 가능한 프로그램이 기록되어 있는 기록 매체.

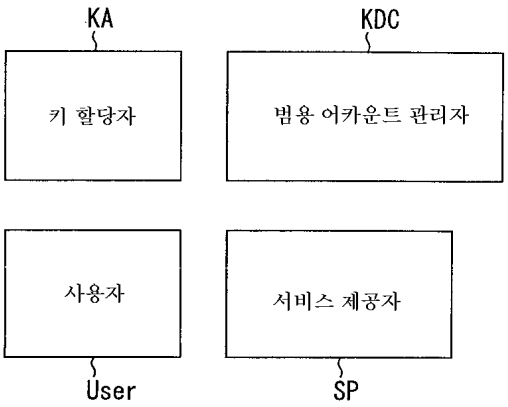
청구항 59.
정보 처리 장치를 제어하는 컴퓨터에,

다른 제1 정보 처리 장치에서 상기 정보 처리 장치로 송부된, 소정의 인증 방법에서 이용 가능한, 제1 암호키, 및, 상기 제1 암호키와 쌍을 이루는 제2 암호키의 생성을 요구하는 요구 정보에 기초하여, 다른 제2 정보 처리 장치로 송신되는 상기 제1 암호키와, 상기 정보 처리 장치에 기억되는 상기 제2 암호키를 생성하는 키 생성 단계와,

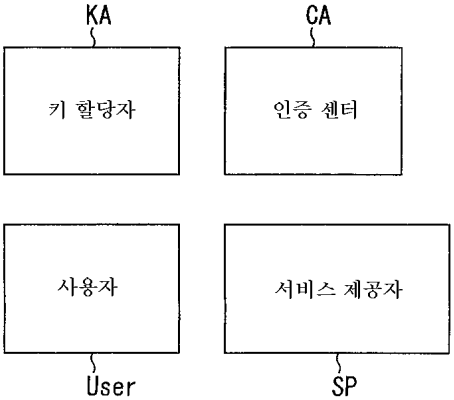
송신된 상기 제1 암호키를 기억하는 다른 제2 정보 처리 장치에 의해, 상기 인증 방법에 기초하여, 상기 정보 처리 장치가 인증되는 경우, 상기 정보 처리 장치에 의해 기억된 상기 제2 암호키를 이용하여, 소정의 응답을 생성하는 응답 생성 단계를 실행시키는 것을 특징으로 하는 프로그램.

도면

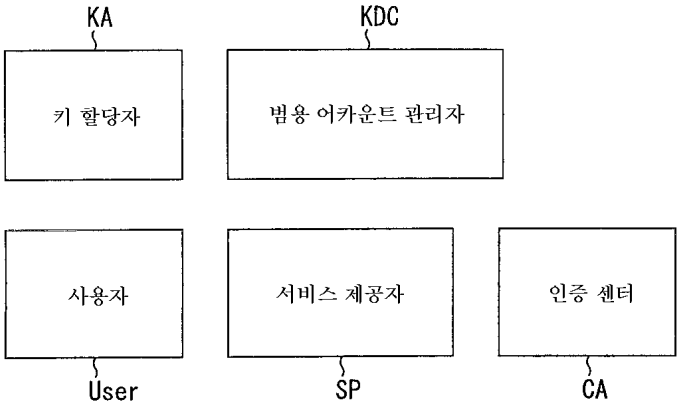
도면1



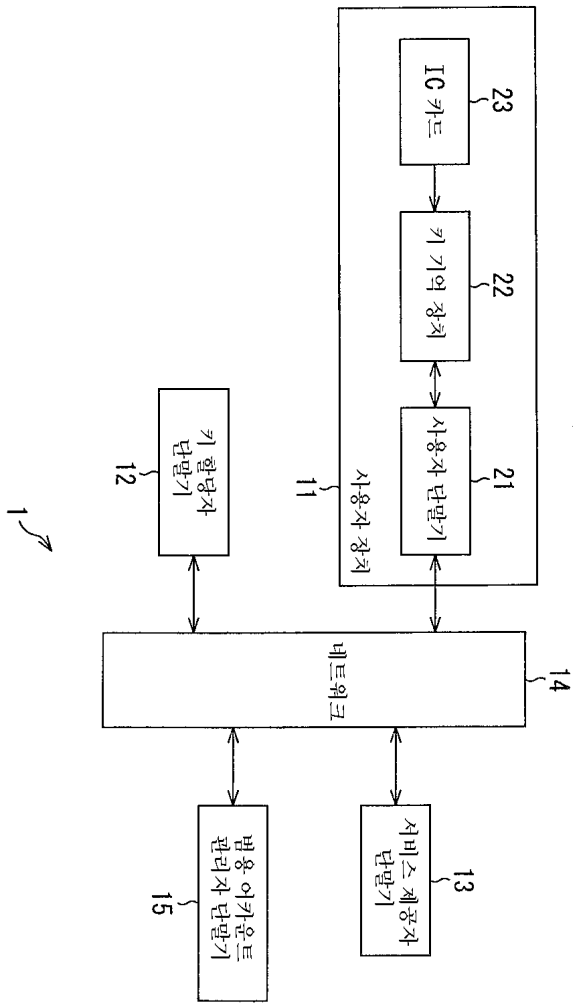
도면2



도면3


KA
KDC
키 할당자
범용 어카운트 관리자
사용자
서비스 제공자
인증 센터
User
SP
CA

도면4


1
IC 카드
23
키 기억 장치
22
사용자 단말기
21
사용자 장치
11
키 할당자 단말기
12
네트워크
14
범용 어카운트 관리자 단말기
15
서비스 제공자 단말기
13

도면5

키 할당표						
Key-ID	Acc-ID	HW-ID	SP-ID	유효 기한	서비스 내용	증명키= 검증키
KID1	AID1	HWID1	SPID1	date1	Service1	Kr1
KID2	AID2	HWID2	SPID2	date2	Service2	Kr2
KID3	AID3	HWID3	SPID3	date3	Service3	Kr3
:	:	:	:	:	:	:

도면6

서비스 제공자 키표		
SP-ID	SP-address	고유 암호키
SPID1	Addr1	KSP1
SPID2	Addr2	KSP2
SPID3	Addr3	KSP3
:	:	:

도면7

키 기억 장치 키표	
HW-ID	고유 암호키
HWID1	KHW1
HWID2	KHW2
HWID3	KHW3
:	:

도면8

키 할당자 어카운트 정보	
Acc-ID	등록 암호키
IDKA	KKA

도면9

인증 정보표			
Key-ID	유효 기한	서비스 내용	검증키
KID1	date1	Service1	Kr1
KID2	date2	Service2	Kr2
KID3	date3	Service3	Kr3
:	:	:	:

도면10

서비스 제공자 고유 정보	
SP-ID	고유 암호키
SPID0	KSP0

도면11

증명키표	
Key-ID	증명키
KID1	Kr1
KID2	Kr2
KID3	Kr3
:	:

도면12

서비스 정보표		
Key-ID	유효 기한	서비스 내용
KID1	date1	Service1
KID2	date2	Service2
KID3	date3	Service3
:	:	:

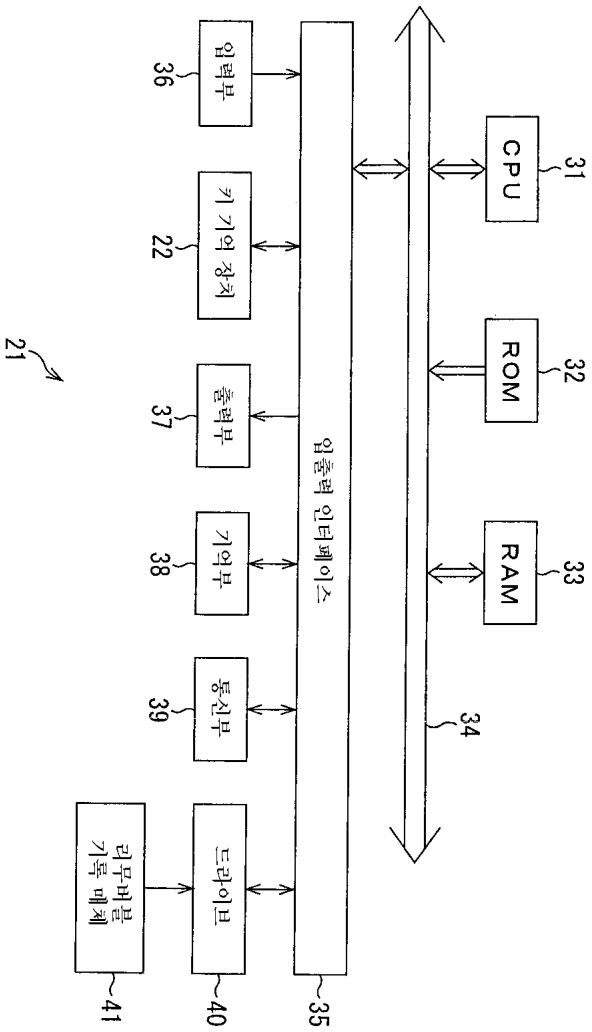
도면13

키 기억 장치 고유 정보	
HW-ID	고유 암호키
HWID0	KHW0

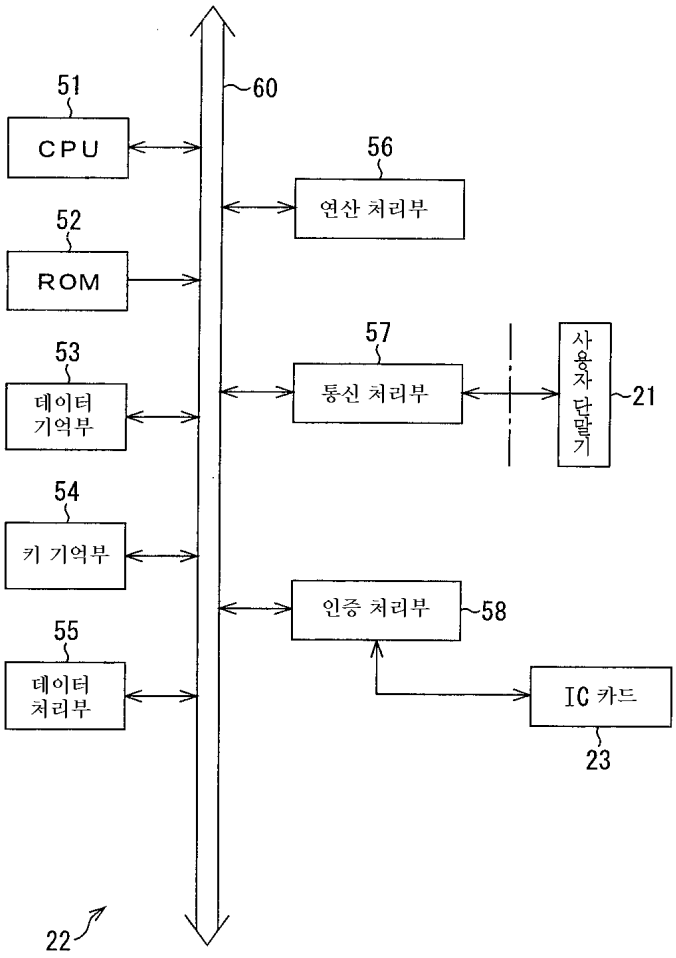
도면14

사용자 어카운트 정보	
Acc-ID	등록 암호키
AIDO	KUO

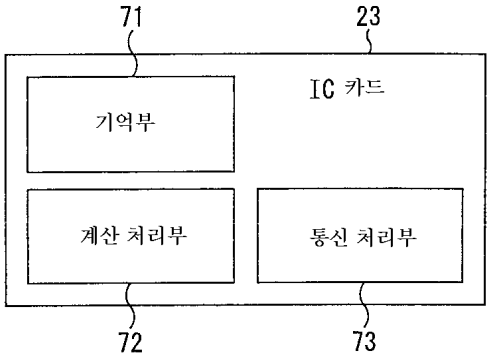
도면15



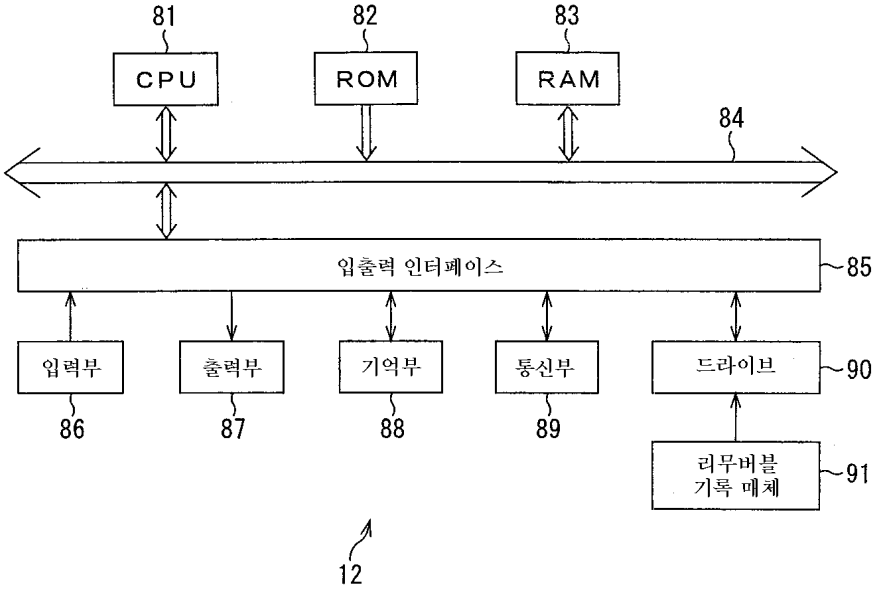
도면16


51
CPU
60
56
연산 처리부
52
ROM
57
53
데이터 기억부
통신 처리부
사용자 단말기
21
54
키 기억부
인증 처리부
58
55
데이터 처리부
IC 카드
23
22

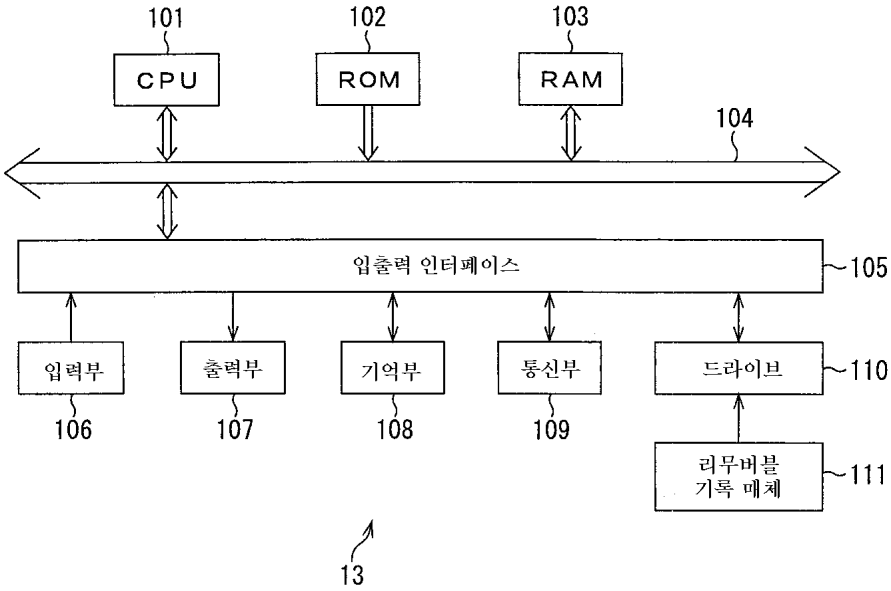
도면17


71
23
IC 카드
기억부
계산 처리부
통신 처리부
72
73

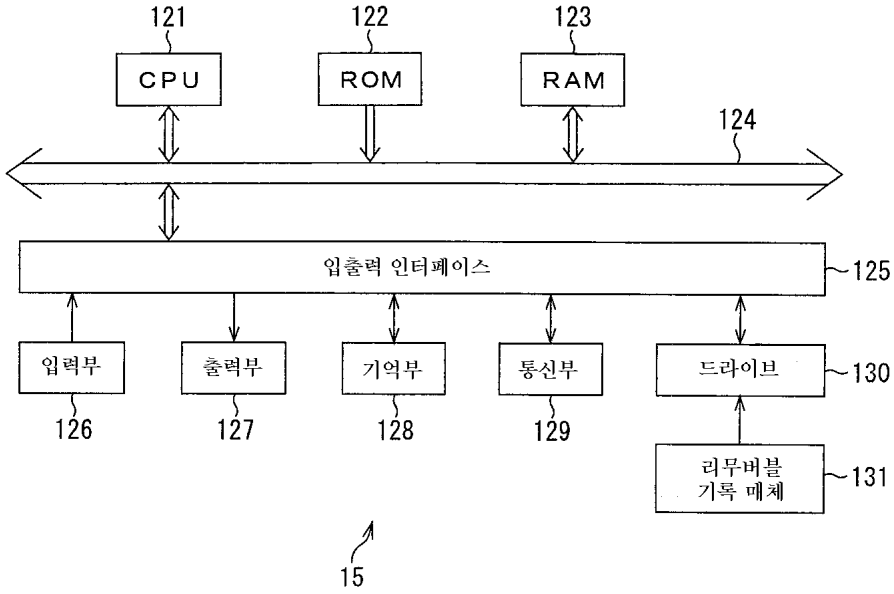
도면18


81
CPU
82
ROM
83
RAM
84
입출력 인터페이스
85
입력부
86
출력부
87
기억부
88
통신부
89
드라이브
90
리무버블
기록 매체
91
12

도면19


101
CPU
102
ROM
103
RAM
104
입출력 인터페이스
105
입력부
106
출력부
107
기억부
108
통신부
109
드라이브
110
리무버블
기록 매체
111
13

도면20



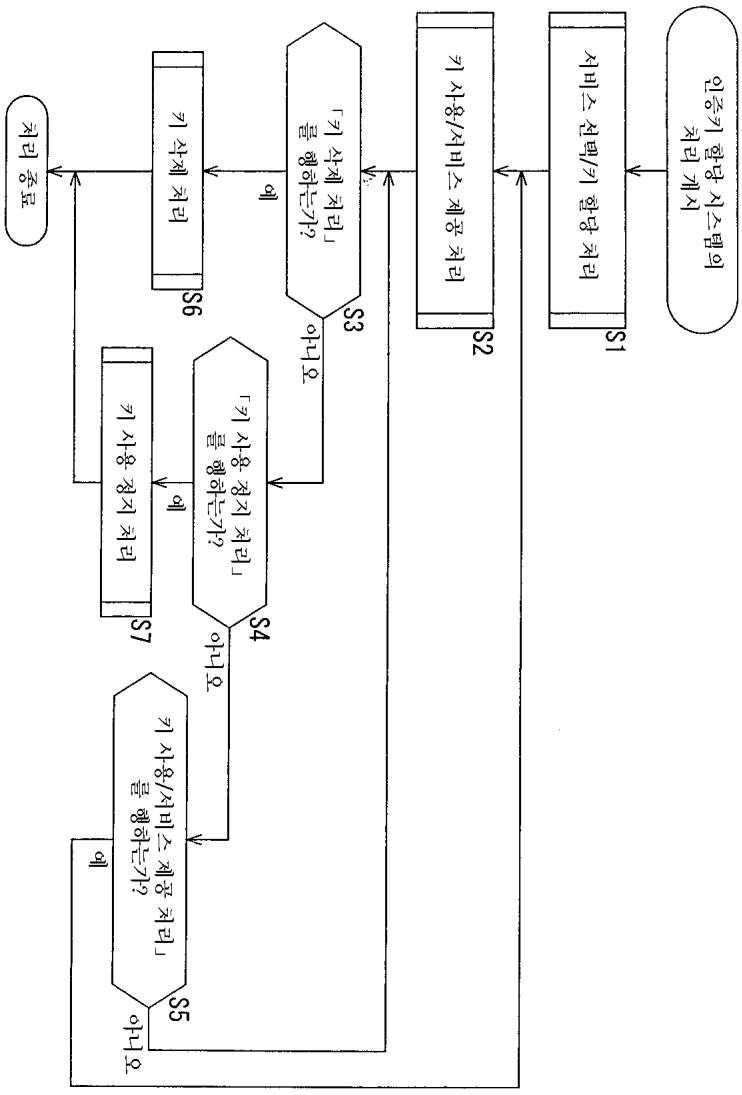
도면21

어카운트 관리표	
Acc-ID	암호키
AID1	KU1
AID2	KU2
AID3	KU3
:	:

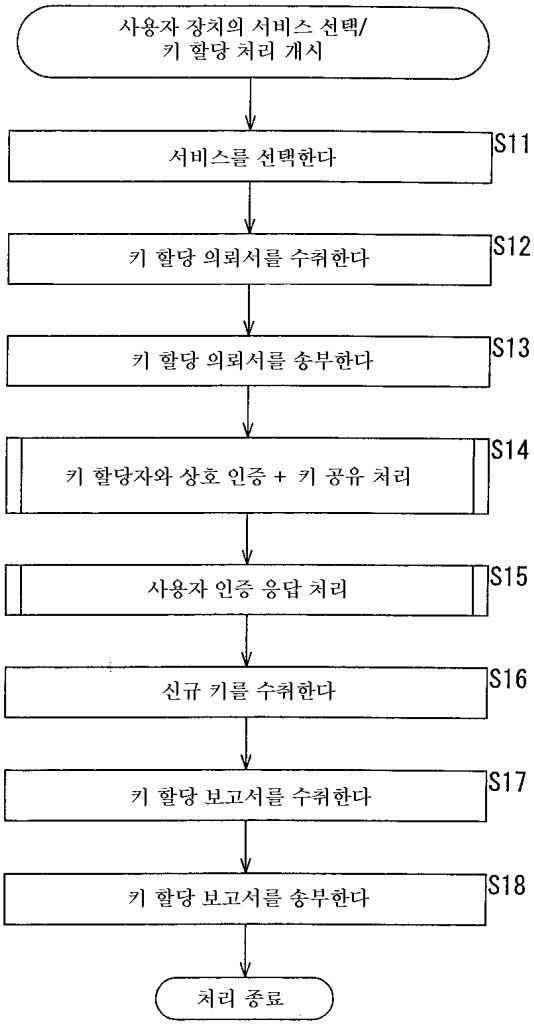
도면22

어카운트 관리자 고유키
암호키
KKDC

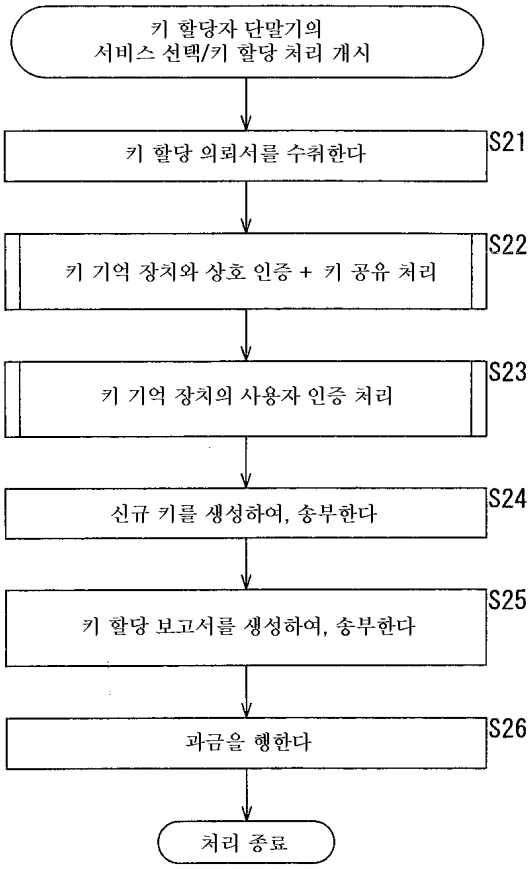
도면23


인증키 할당 시스템의 처리 개시
서비스 선택/키 할당 처리
S1
키 사용/서비스 제공 처리
S2
「키 삭제 처리」를 행하는가?
S3
예
키 삭제 처리
S6
아니오
「키 사용 정지 처리」를 행하는가?
S4
예
키 사용 정지 처리
S7
아니오
키 사용/서비스 제공 처리」를 행하는가?
S5
예
아니오
처리 종료

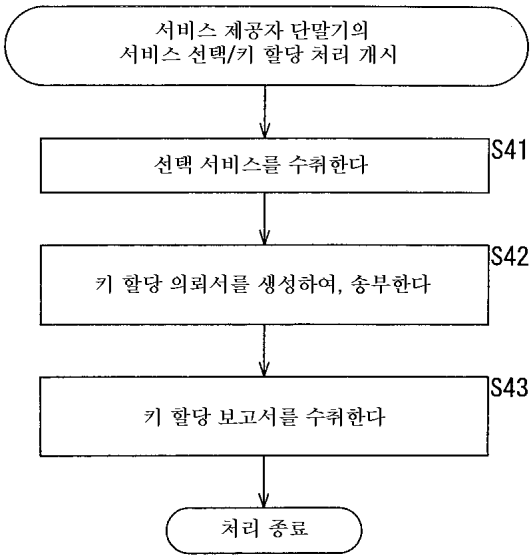
도면24


사용자 장치의 서비스 선택/
키 할당 처리 개시
서비스를 선택한다
S11
키 할당 의뢰서를 수취한다
S12
키 할당 의뢰서를 송부한다
S13
키 할당자와 상호 인증 + 키 공유 처리
S14
사용자 인증 응답 처리
S15
신규 키를 수취한다
S16
키 할당 보고서를 수취한다
S17
키 할당 보고서를 송부한다
S18
처리 종료

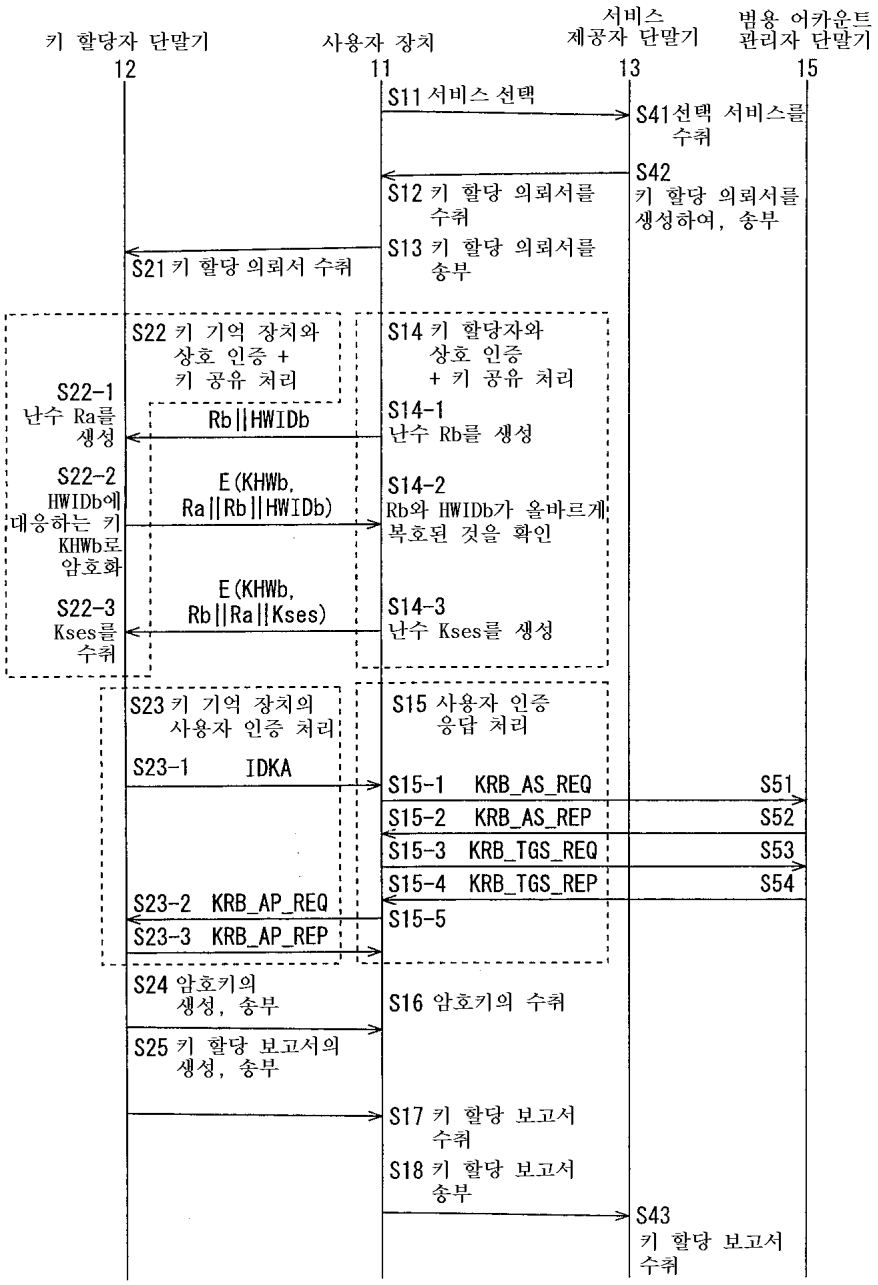
도면25


키 할당자 단말기의
서비스 선택/키 할당 처리 개시
키 할당 의뢰서를 수취한다
S21
키 기억 장치와 상호 인증 + 키 공유 처리
S22
키 기억 장치의 사용자 인증 처리
S23
신규 키를 생성하여, 송부한다
S24
키 할당 보고서를 생성하여, 송부한다
S25
과금을 행한다
S26
처리 종료

도면26


서비스 제공자 단말기의
서비스 선택/키 할당 처리 개시
선택 서비스를 수취한다
S41
키 할당 의뢰서를 생성하여, 송부한다
S42
키 할당 보고서를 수취한다
S43
처리 종료

도면27



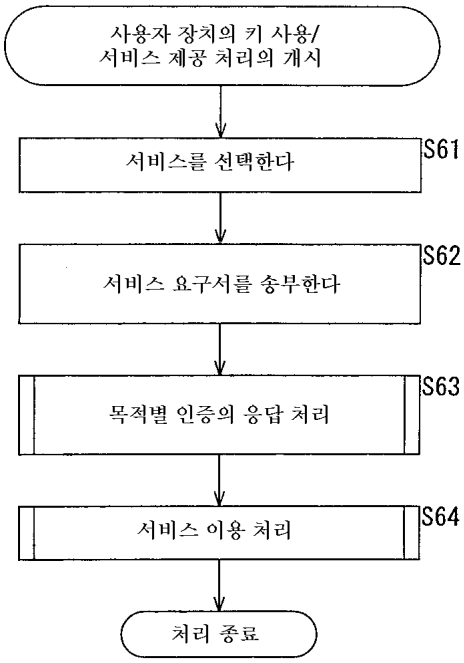
도면28

키 할당 의뢰서				
의뢰서 ID	유효 기한	SP-ID	서비스 내용	메시지 인증 코드
IDO	dateO	SPIDO	ServiceO	MACO

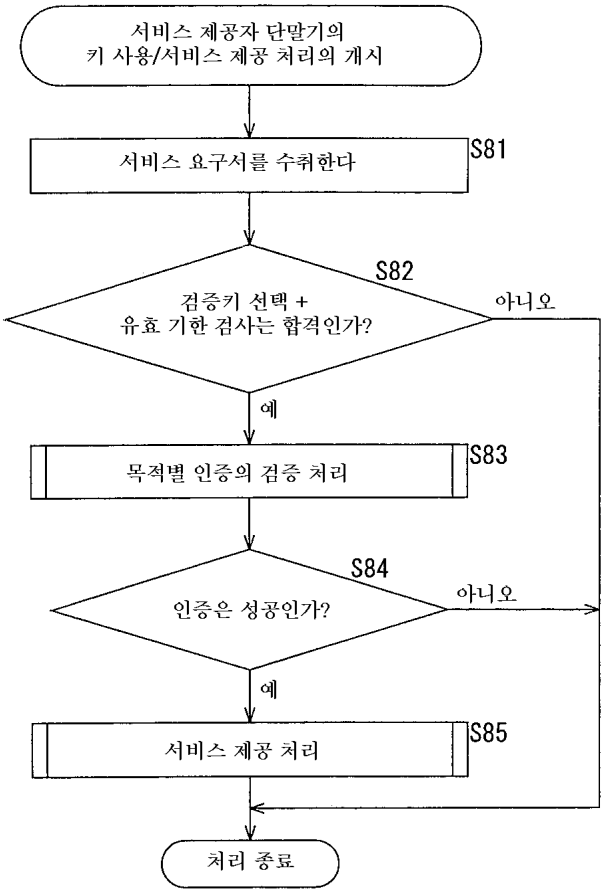
도면29

키 할당 보고서				
Key-ID	의뢰서 ID	SP-ID	유효 기한	암호화 검증키
KIDO	IDO	SPIDO	dateO	E(KSP, Kr)

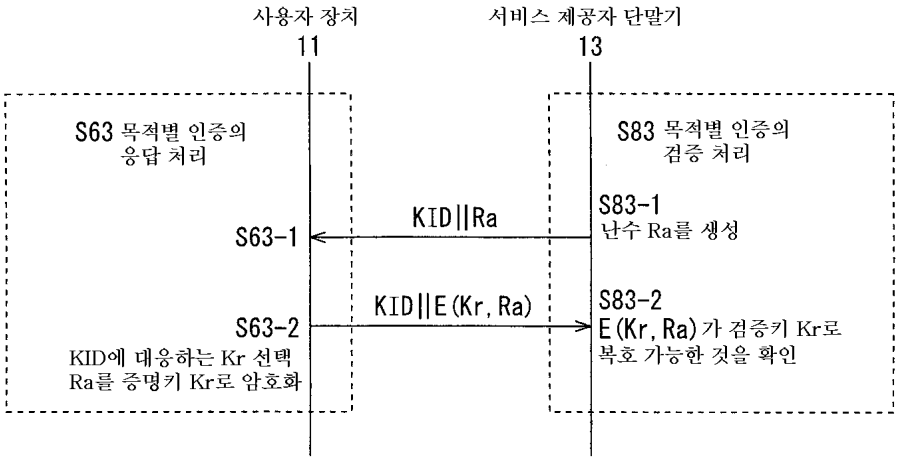
도면30


사용자 장치의 키 사용/
서비스 제공 처리의 개시
서비스를 선택한다
S61
서비스 요구서를 송부한다
S62
목적별 인증의 응답 처리
S63
서비스 이용 처리
S64
처리 종료

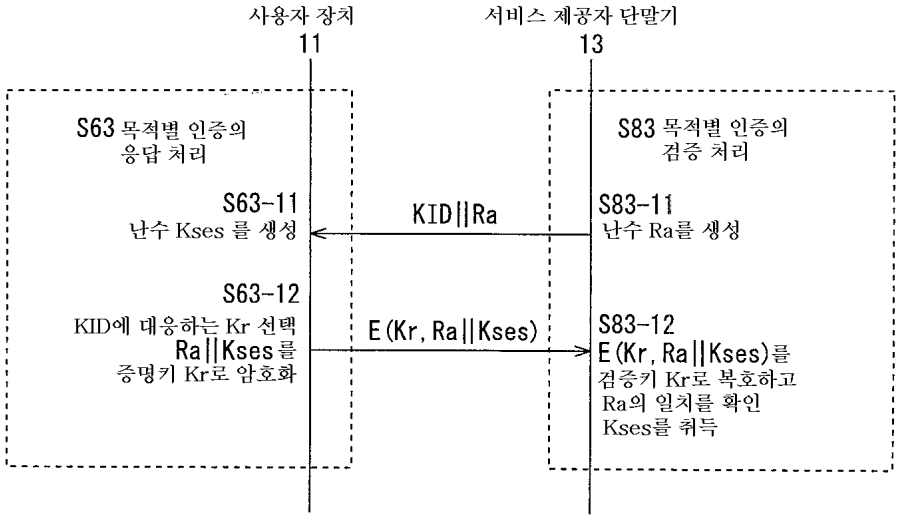
도면31


서비스 제공자 단말기의
키 사용/서비스 제공 처리의 개시
서비스 요구서를 수취한다
S81
검증키 선택 +
유효 기한 검사는 합격인가?
S82
아니오
예
목적별 인증의 검증 처리
S83
인증은 성공인가?
S84
아니오
예
서비스 제공 처리
S85
처리 종료

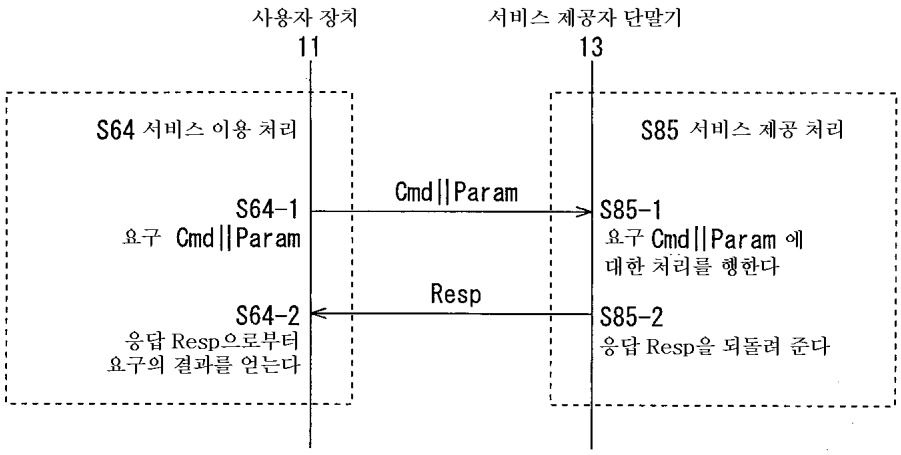
도면32



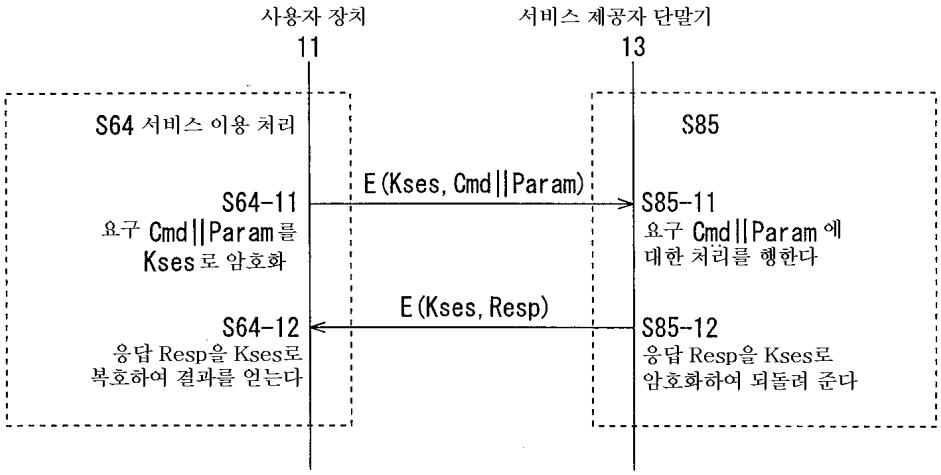
도면33



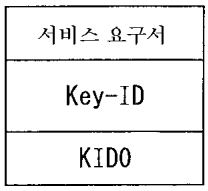
도면34



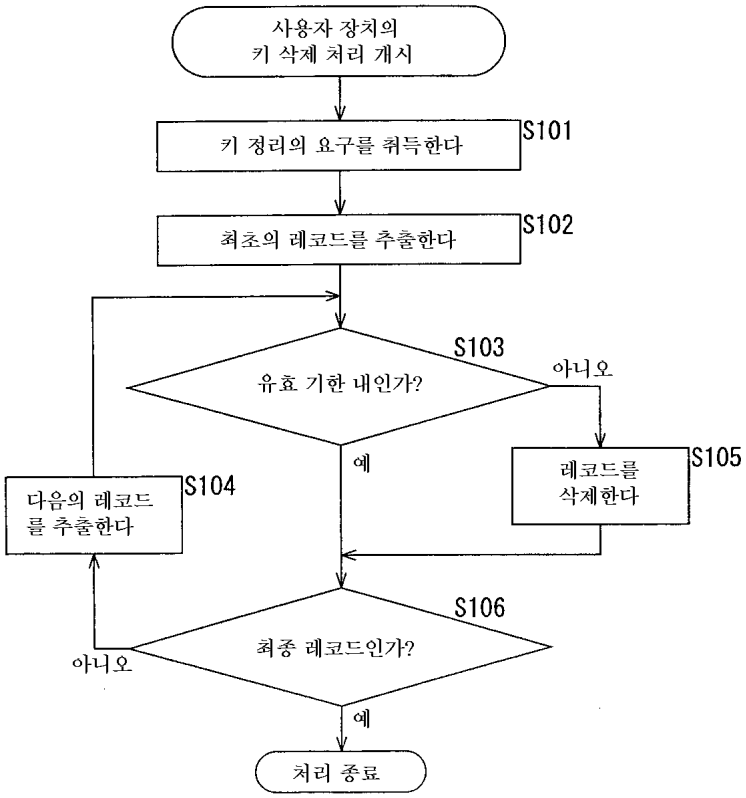
도면35



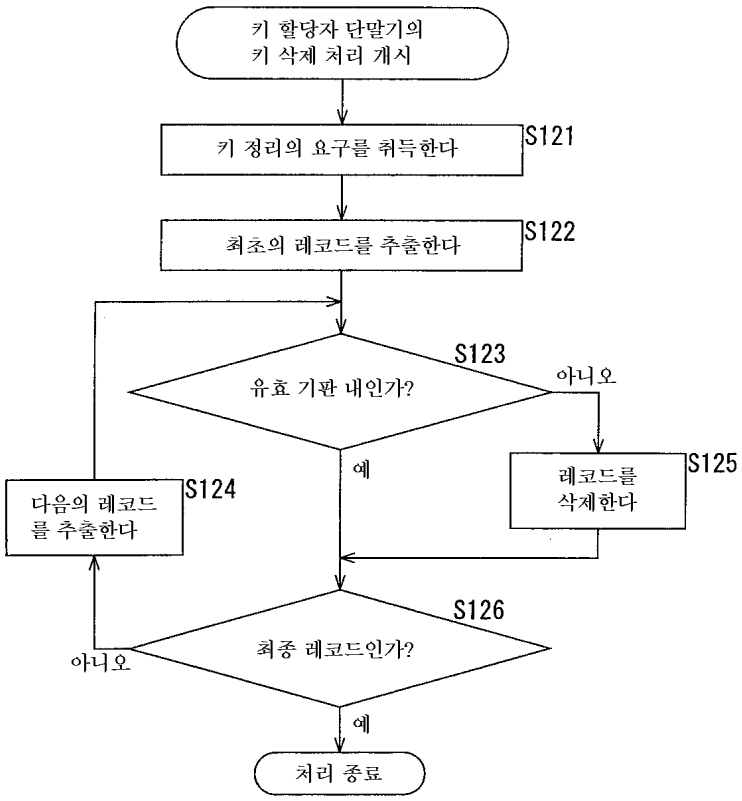
도면36



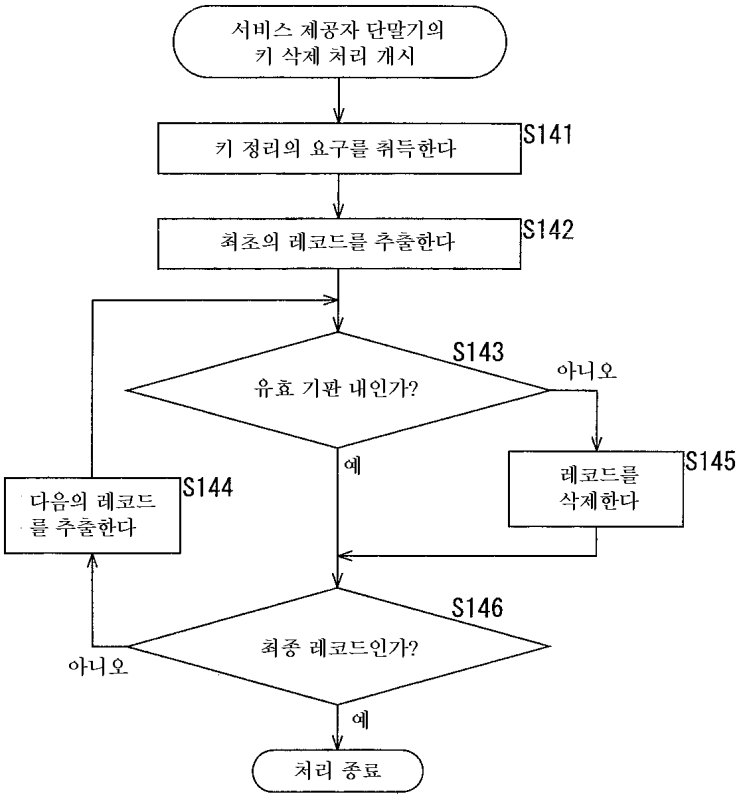
도면37



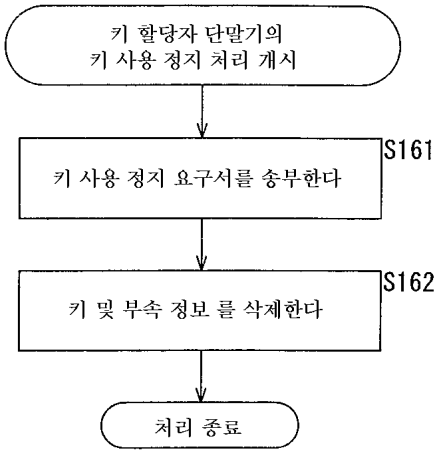
도면38


키 할당자 단말기의
키 삭제 처리 개시
키 정리의 요구를 취득한다
S121
최초의 레코드를 추출한다
S122
유효 기판 내인가?
S123
아니오
예
레코드를
삭제한다
S125
다음의 레코드
를 추출한다
S124
최종 레코드인가?
S126
아니오
예
처리 종료

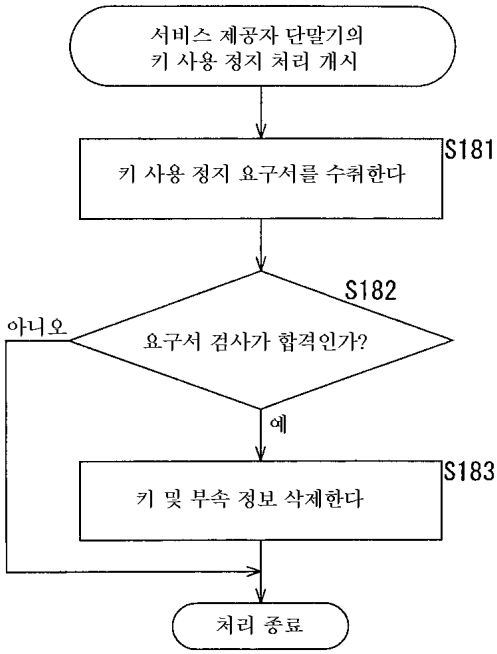
도면39


서비스 제공자 단말기의
키 삭제 처리 개시
키 정리의 요구를 취득한다
S141
최초의 레코드를 추출한다
S142
유효 기판 내인가?
S143
아니오
예
레코드를
삭제한다
S145
다음의 레코드
를 추출한다
S144
최종 레코드인가?
S146
아니오
예
처리 종료

도면40



도면41



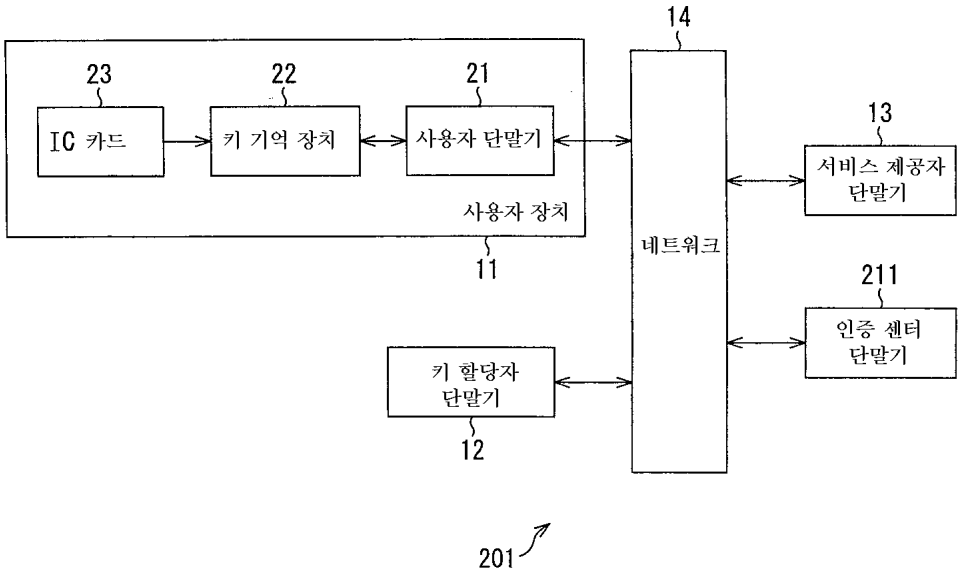
도면42

키 사용 정지 요구서			
Key-ID	Date-time	유효 기한	메시지 인증 코드
KID0	YMDT	date0	MAC0

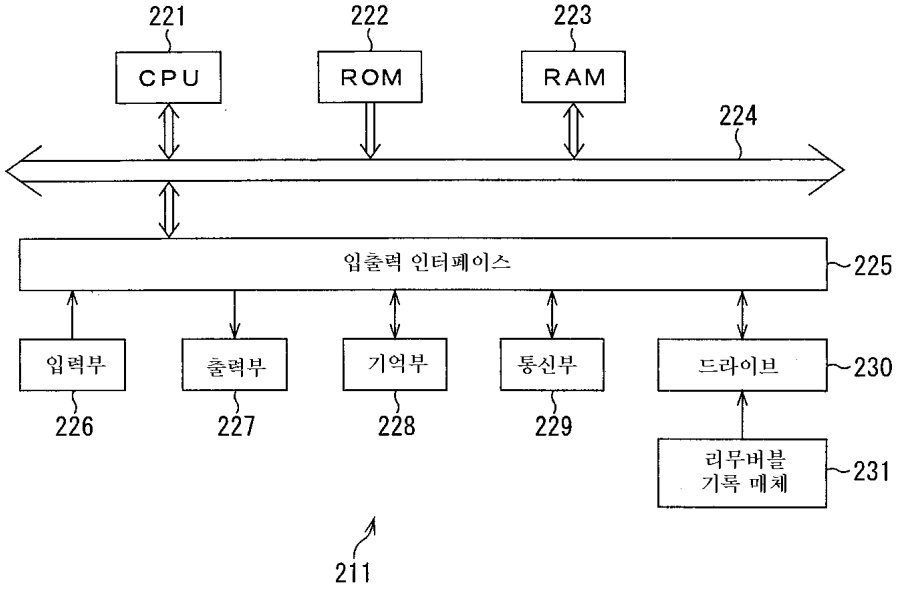
도면43

키 사용 정지 요구서			
Key-ID	Date-time	유효 기한	KA 전자 서명
KID0	YMDT	date0	SIG0

도면44



도면45



도면46

키 할당표					
Key-ID	Acc-ID	HW-ID	키 할당 의뢰서	키 할당 보고서	증명키
KID1	AID1	HWID1	App1	Rep1	Kpr1
KID2	AID2	HWID2	App2	Rep2	Kpr2
KID3	AID3	HWID3	App3	Rep3	Kpr3
:	:	:	:	:	:

도면47

서비스 제공자키표		
SP-ID	SP-address	SP-Acc-ID
SPID1	Addr1	SPAID1
SPID2	Addr2	SPAID2
SPID3	Addr3	SPAID3
:	:	:

도면48

키 기억 장치키표	
HW-ID	고유 암호키
HWID1	HWK1
HWID2	HWK2
HWID3	HWK3
:	:

도면49

키 할당자 PKI 정보	
증명서	비밀키
CERTKA	SKKA

도면50

CA 공개키 정보
CA 공개키
PKCA

도면51

키 할당 의뢰서				
의뢰서 ID	SP-ID	유효 기한	서비스 내용	SP 전자 서명
IID0	SPID0	date0	Service0	SIG0

도면52

키 할당 보고서						
Key-ID	의뢰서 ID	SP-ID	유효 기한	SP-Acc-ID	검증키	KA 전자 서명
KID0	IID0	SPID0	date0	SPAID0	Kpub0	SIG0

도면53

인증 정보표		
Key-ID	키 할당 의뢰서	키 할당 보고서
KID1	App1	Rep1
KID2	App2	Rep2
KID3	App3	Rep3
:	:	:

도면54

서비스 제공자 고유 정보
SP-ID
SPID0

도면55

실효 키표	
Key-ID	유효 기한
KID1	date1
KID2	date2
KID3	date3
:	:

도면56

서비스 제공자 PKI 정보	
증명서	비밀키
CERTSP0	SKSP0

도면57

키 공유 파라미터	
p	g

도면58

CA 공개키 정보
CA 공개키
PKCA

도면59

증명키표	
Key-ID	증명키
KID1	Kpr1
KID2	Kpr2
KID3	Kpr3
:	:

도면60

인증 정보표		
Key-ID	키 할당 의뢰서	키 할당 보고서
KID1	App1	Rep1
KID2	App2	Rep2
KID3	App3	Rep3
:	:	:

도면61

키 기억 장치 고유 정보	
HW-ID	고유 암호키
HWID0	HWK0

도면62

사용자 PK1 정보	
증명서	비밀키
CERTU0	SKU0

도면63

CA 공개키 정보
CA 공개키
PKCA

도면64

증명서표		
Acc-ID	증명서	증명서 ID
AID1	CERT1	CID1
AID2	CERT2	CID2
AID3	CERT3	CID3

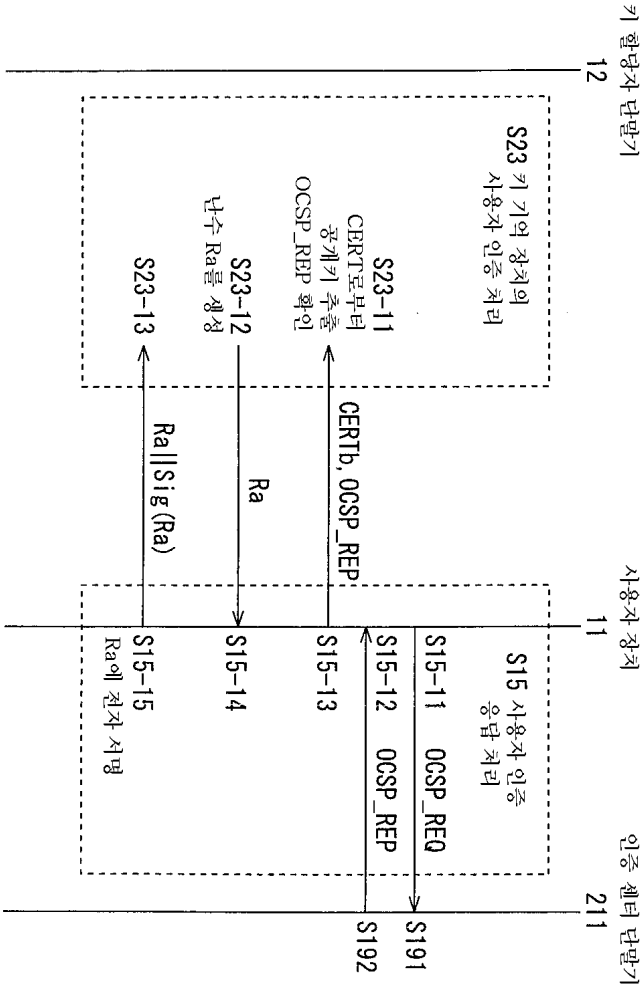
도면65

CA 키 정보	
CA 공개키	CA 비밀키
PKCA	SKCA

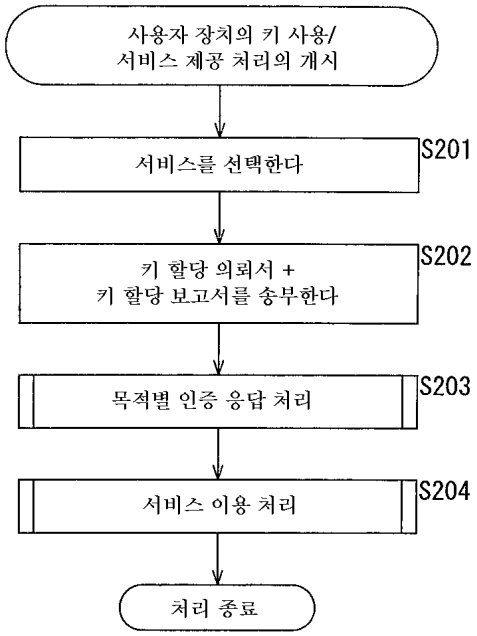
도면66

증명서					
Acc-ID	유효 기한	증명서 ID	공개키	부속 정보	CA 서명
AID1	ymdt	CID0	Kpub0	info0	SIG0

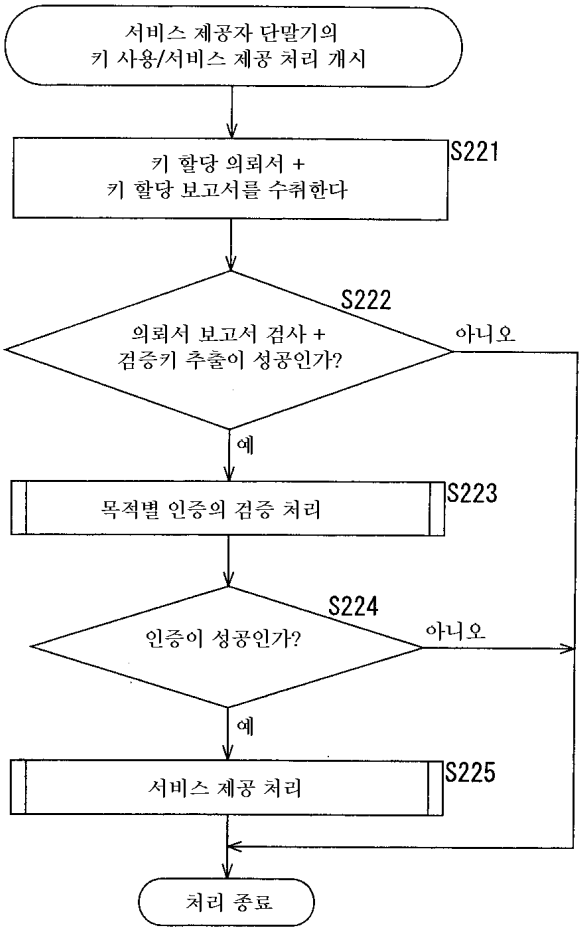
도면67


키 할당자 단말기
12
사용자 장치
11
인증 센터 단말기
211
S23 키 기억 장치의 사용자 인증 처리
S23-11 CERT로부터 공개키 추출 OCSP_REP 확인
S23-12 난수 Ra를 생성
S23-13
CERTb, OCSP_REP
Ra
Ra||Sig(Ra)
S15 사용자 인증 응답 처리
S15-11 OCSP_REQ
S15-12 OCSP_REP
S15-13
S15-14
S15-15 Ra에 전자 서명
S191
S192

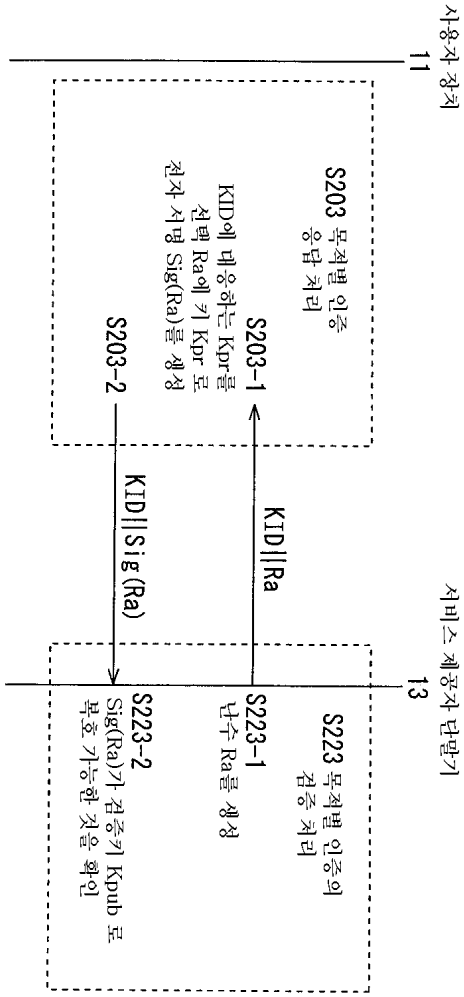
도면68


사용자 장치의 키 사용/
서비스 제공 처리의 개시
서비스를 선택한다
S201
키 할당 의뢰서 +
키 할당 보고서를 송부한다
S202
목적별 인증 응답 처리
S203
서비스 이용 처리
S204
처리 종료

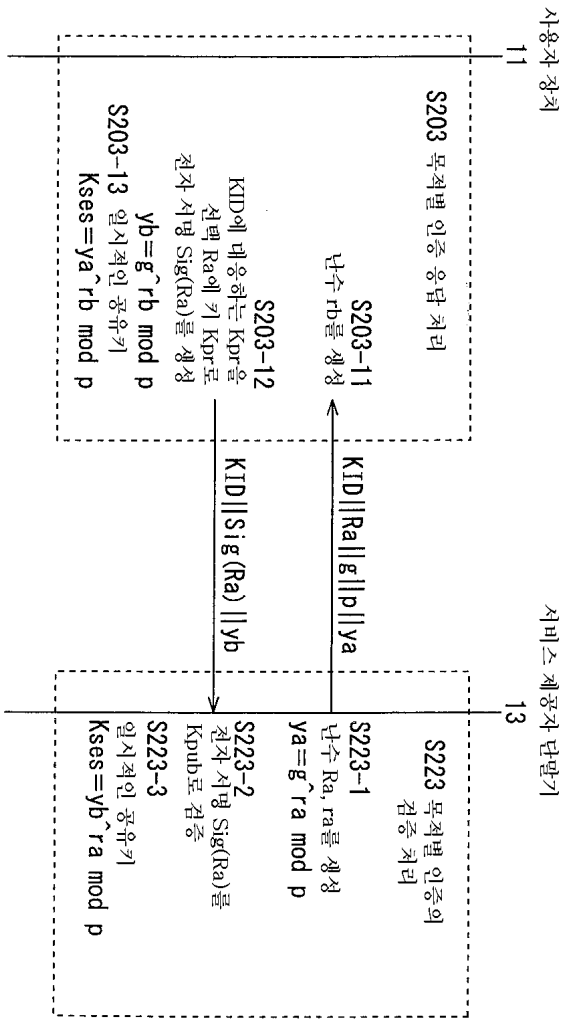
도면69


서비스 제공자 단말기의
키 사용/서비스 제공 처리 개시
키 할당 의뢰서 +
키 할당 보고서를 수취한다
S221
의뢰서 보고서 검사 +
검증키 추출이 성공인가?
S222
아니오
예
목적별 인증의 검증 처리
S223
인증이 성공인가?
S224
아니오
예
서비스 제공 처리
S225
처리 종료

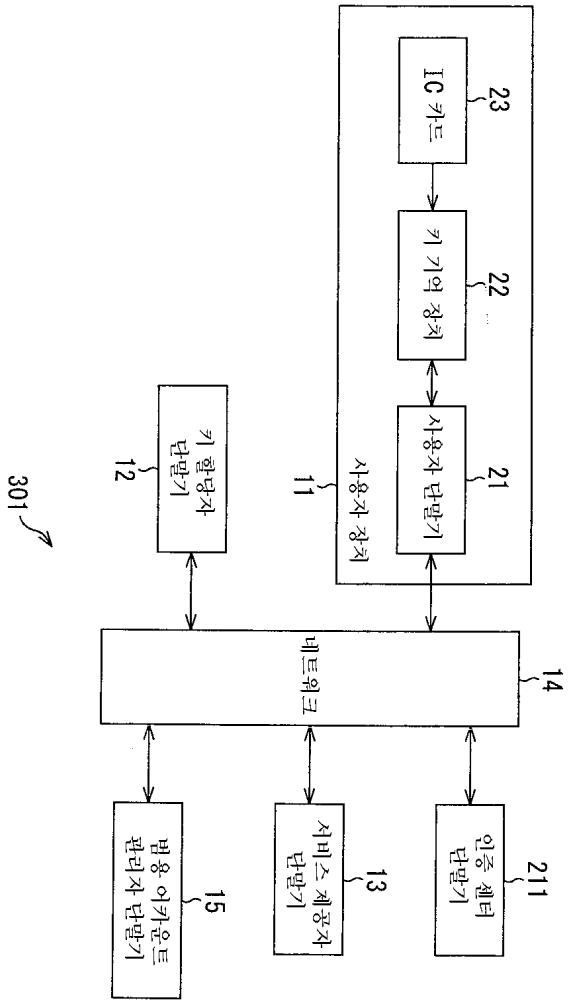
도면70


사용자 장치
11
서비스 제공자 단말기
13
S203 목적별 인증
응답 처리
S203-1
KID에 대응하는 Kpr를
선택 Ra에 키 Kpr 로
전자 서명 Sig(Ra)를 생성
S203-2
KID||Ra
KID||Sig(Ra)
S223 목적별 인증의
검증 처리
S223-1
난수 Ra를 생성
S223-2
Sig(Ra)가 검증키 Kpub 로
복호 가능한 것을 확인

도면71


사용자 장치
11
서비스 제공자 단말기
13
S203 목적별 인증 응답 처리
S203-11
난수 rb를 생성
S203-12
KID에 대응하는 Kpr을
선택 Ra에 키 Kpr로
전자 서명 Sig(Ra)를 생성
yb=g^rb mod p
S203-13 일시적인 공유키
Kses=ya^rb mod p
KID||Ra||g||p||ya
KID||Sig(Ra)||yb
S223 목적별 인증의
검증 처리
S223-1
난수 Ra, ra를 생성
ya=g^ra mod p
S223-2
전자 서명 Sig(Ra)를
Kpub로 검증
S223-3
일시적인 공유키
Kses=yb^ra mod p

도면72



도면73

키 할당표							
Key-ID	Acc-ID	HW-ID	SP-ID	유효 기한	권리 증서	검증키	증명키
KID1	AID1	HWID1	SPID1	date1	Rcert1	Kpub1	Kpr1
KID2	AID2	HWID2	SPID2	date2	Rcert2	Kpub2	Kpr2
KID3	AID3	HWID3	SPID3	date3	Rcert3	Kpub3	Kpr3
:	:	:	:	:	:	:	:

도면74

서비스 제공자키표			
SP-ID	SP-address	SP-Acc-ID	고유 암호키
SPID1	Addr1	SPAID1	KSP1
SPID2	Addr2	SPAID2	KSP2
SPID3	Addr3	SPAID3	KSP3
:	:	:	:

도면75

키 기억 장치키표	
HW-ID	고유 암호키
HWID1	HWK1
HWID2	HWK2
HWID3	HWK3
:	:

도면76

키 할당자 어카운트 정보	
Acc-ID	등록 암호키
IDKA	KKA

도면77

CA 공개키 정보
CA 공개키
PKCA

도면78

권리 증서				
Key-ID	검증키	유효 기한	서비스 내용	SP 전자 서명
KID0	Kpub0	date0	Service0	SIG0

도면79

키 할당 의뢰서			
의뢰서 ID	유효 기한	SP-ID	메시지 인증 코드
IDO	dateO	SPIDO	MACO

도면80

키 할당 보고서				
Key-ID	의뢰서 ID	유효 기한	검증키	메시지 인증 코드
KIDO	IDO	dateO	KpubO	MACO

도면81

인증 정보표	
Key-ID	권리 증서
KID1	Rcert1
KID2	Rcert2
KID3	Rcert3
:	:

도면82

서비스 제공자 고유 정보	
SP-ID	고유 암호키
SPIDO	KSPO

도면83

실효 키표	
Key-ID	유효 기한
KID1	date1
KID2	date2
KID3	date3
:	:

도면84

서비스 제공자 PKI 정보	
증명서	비밀키
CERT0	SK0

도면85

키 공유 파라미터	
p	g

도면86

CA 공개키 정보
CA 공개키
PKCA

도면87

증명키표	
Key-ID	증명키
KID1	Kpr1
KID2	Kpr2
KID3	Kpr3
:	:

도면88

인증 정보표	
Key-ID	권리 증서
KID1	Rcert1
KID2	Rcert2
KID3	Rcert3
:	:

도면89

키 기억 장치 고유 정보	
HW-ID	인증 암호키
HWID0	HWK0

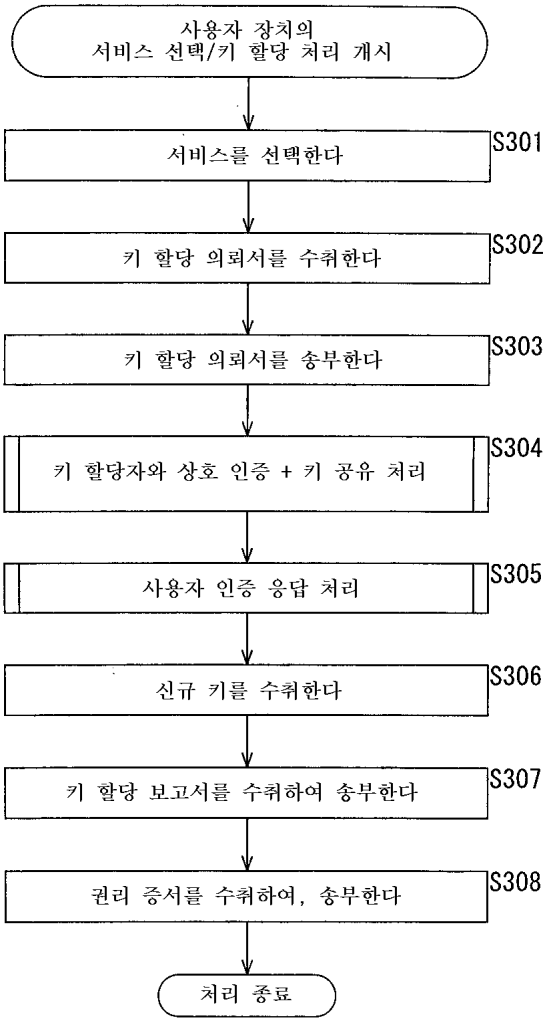
도면90

사용자 어카운트 정보	
Acc-ID	암호 키
UIDO	KUSERO

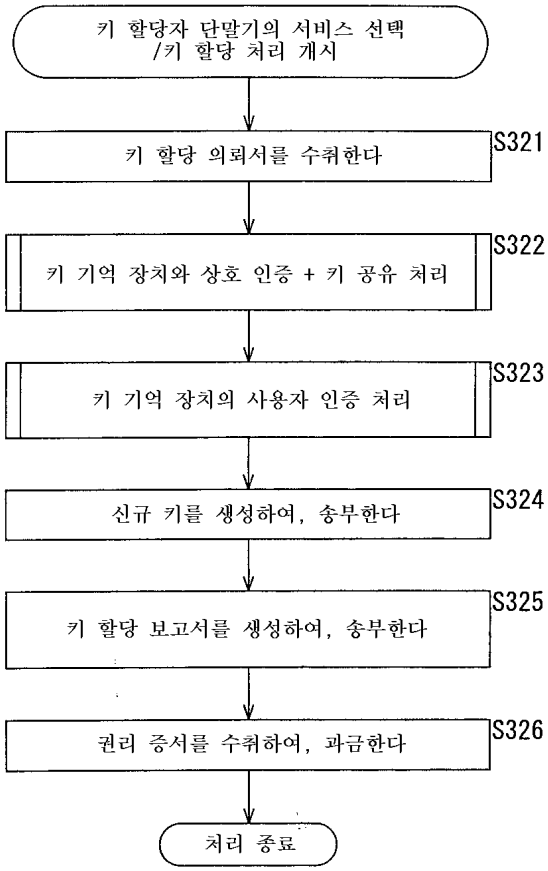
도면91

CA 공개키 정보
CA 공개키
PKCA

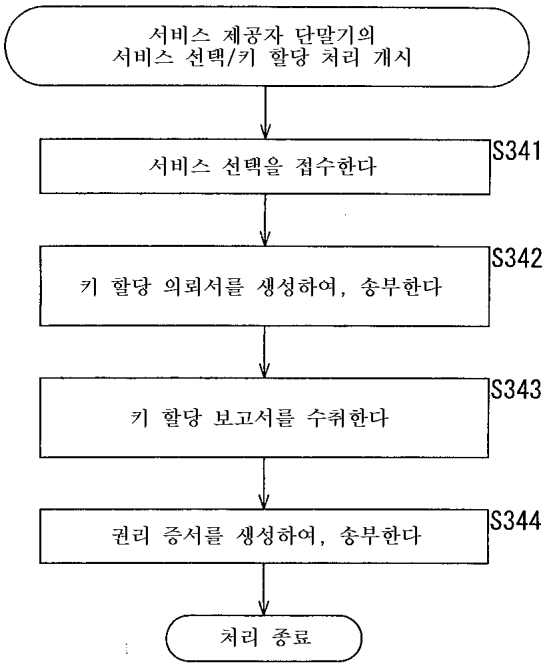
도면92



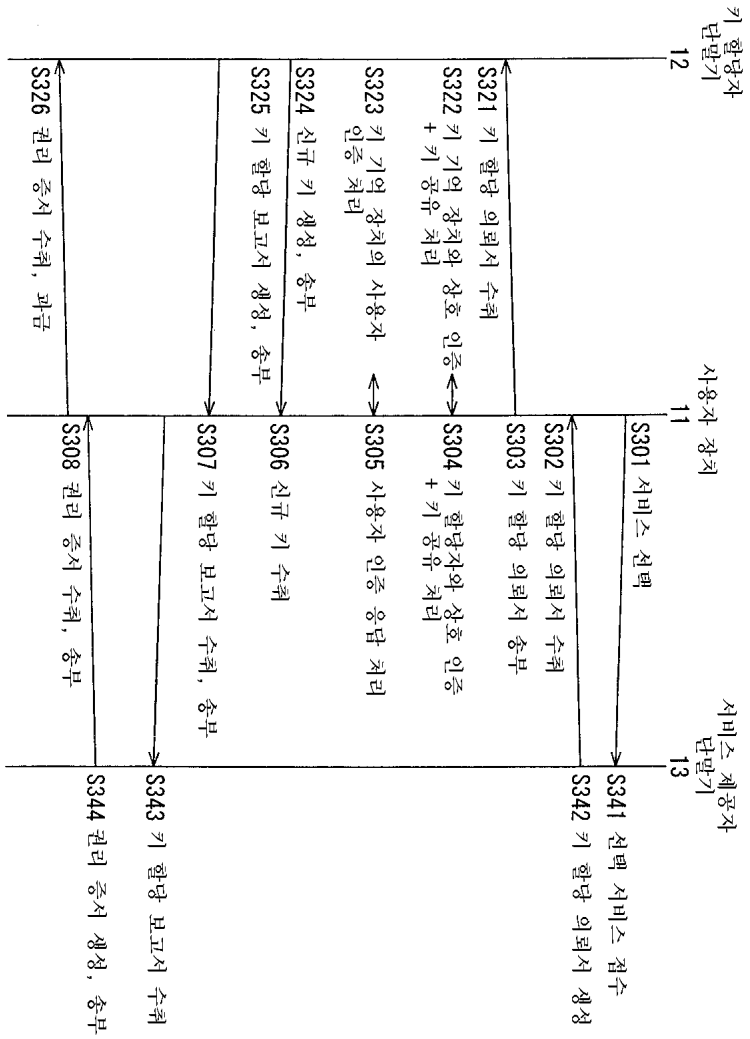
도면93


키 할당자 단말기의 서비스 선택
/키 할당 처리 개시
키 할당 의뢰서를 수취한다
S321
키 기억 장치와 상호 인증 + 키 공유 처리
S322
키 기억 장치의 사용자 인증 처리
S323
신규 키를 생성하여, 송부한다
S324
키 할당 보고서를 생성하여, 송부한다
S325
권리 증서를 수취하여, 과금한다
S326
처리 종료

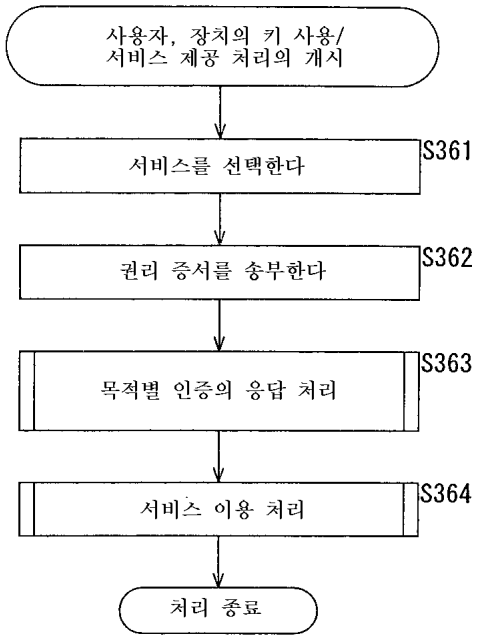
도면94


서비스 제공자 단말기의
서비스 선택/키 할당 처리 개시
서비스 선택을 접수한다
S341
키 할당 의뢰서를 생성하여, 송부한다
S342
키 할당 보고서를 수취한다
S343
권리 증서를 생성하여, 송부한다
S344
처리 종료

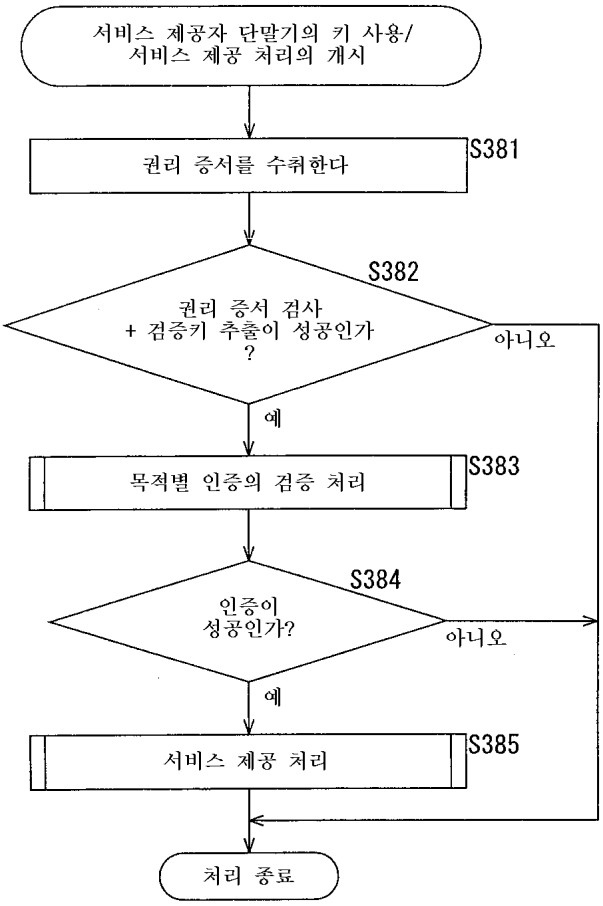
도면95


키 할당자 단말기 12
사용자 장치 11
서비스 제공자 단말기 13
S321 키 할당 의뢰서 수취
S322 키 기억 장치와 상호 인증 + 키 공유 처리
S323 키 기억 장치의 사용자 인증 처리
S324 신규 키 생성, 송부
S325 키 할당 보고서 생성, 송부
S326 권리 증서 수취, 과금
S301 서비스 선택
S302 키 할당 의뢰서 수취
S303 키 할당 의뢰서 송부
S304 키 할당자와 상호 인증 + 키 공유 처리
S305 사용자 인증 응답 처리
S306 신규 키 수취
S307 키 할당 보고서 수취, 송부
S308 권리 증서 수취, 송부
S341 선택 서비스 접수
S342 키 할당 의뢰서 생성
S343 키 할당 보고서 수취
S344 권리 증서 생성, 송부

도면96


사용자, 장치의 키 사용/ 서비스 제공 처리의 개시
서비스를 선택한다
S361
권리 증서를 송부한다
S362
목적별 인증의 응답 처리
S363
서비스 이용 처리
S364
처리 종료

도면97



도면98

키 할당표				
Key-ID	Acc-ID	HW-ID	권리 증서	증명키
KID1	AID1	HWID1	Rcert1	Kpr1
KID2	AID2	HWID2	Rcert2	Kpr2
KID3	AID3	HWID3	Rcert3	Kpr3
:	:	:	:	:

도면99

서비스 제공자키표		
SP-ID	SP-address	고유 암호키
SPID1	Addr1	KSP1
SPID2	Addr2	KSP2
SPID3	Addr3	KSP3
:	:	:

도면100

키 기억 장치키표	
HW-ID	고유 암호키
HWID1	HWK1
HWID2	HWK2
HWID3	HWK3
:	:

도면101

키 할당 PKI 정보	
증명서	비밀키
CERTKA	SKKA

도면102

CA 공개키 정보
CA 공개키
PKCA

도면103

권리 증서					
Key-ID	검증키	유효 기한	서비스 내용	SP-ID	KA 전자 서명
KIID0	Kpub0	date0	Service0	SPID0	SIG0

도면104

키 할당 의뢰서				
의뢰서 ID	유효 기한	서비스 내용	SP-ID	메시지 인증 코드
ID0	date0	Service0	SPID0	MAC0

도면105

서비스 제공자 고유 정보	
SP-ID	고유 암호키
SPID0	KSP0

도면106

실효 키표	
Key-ID	유효 기한
KID1	date1
KID2	date2
KID3	date3
:	:

도면107

키 공유 파라미터	
p	g

도면108

CA 공개키 정보
CA 공개키
PKCA

도면109

증명키표	
Key-ID	증명키
KID1	Kpr1
KID2	Kpr2
KID3	Kpr3
:	:

도면110

인증 정보표	
Key-ID	권리 증서
KID1	Rcert1
KID2	Rcert2
KID3	Rcert3
:	:

도면111

키 기억 장치 고유 정보	
HW-ID	인증 암호키
HWIDO	HWKO

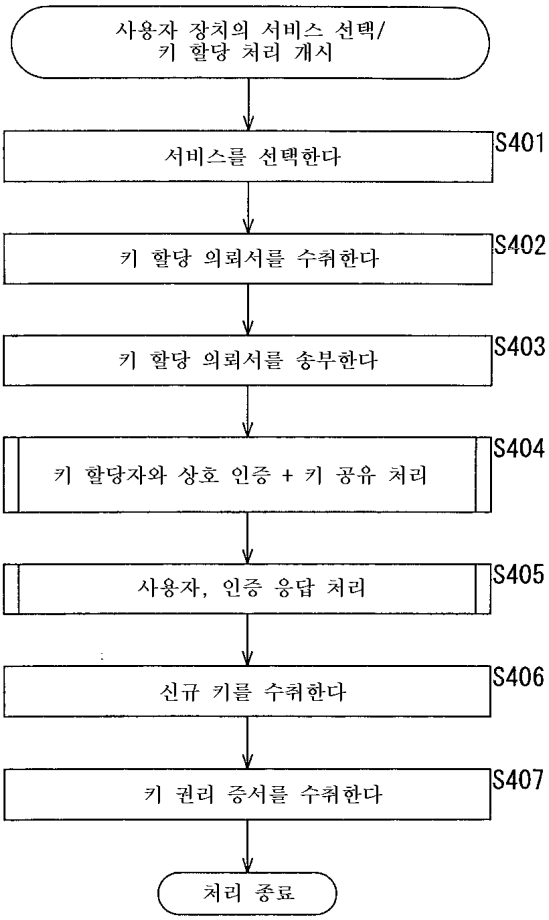
도면112

사용자 어카운트 정보	
Acc-ID	암호키
UIDO	KUSERO

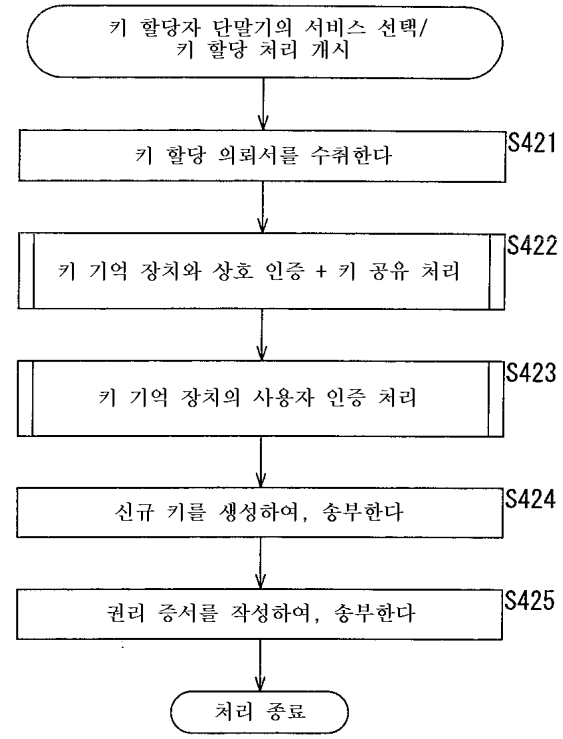
도면113

CA 공개키 정보
CA 공개키
PKCA

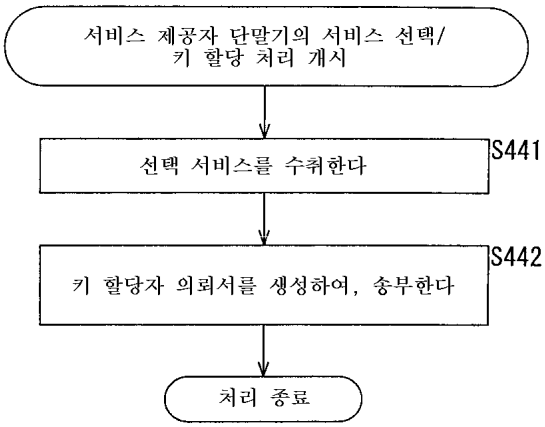
도면114



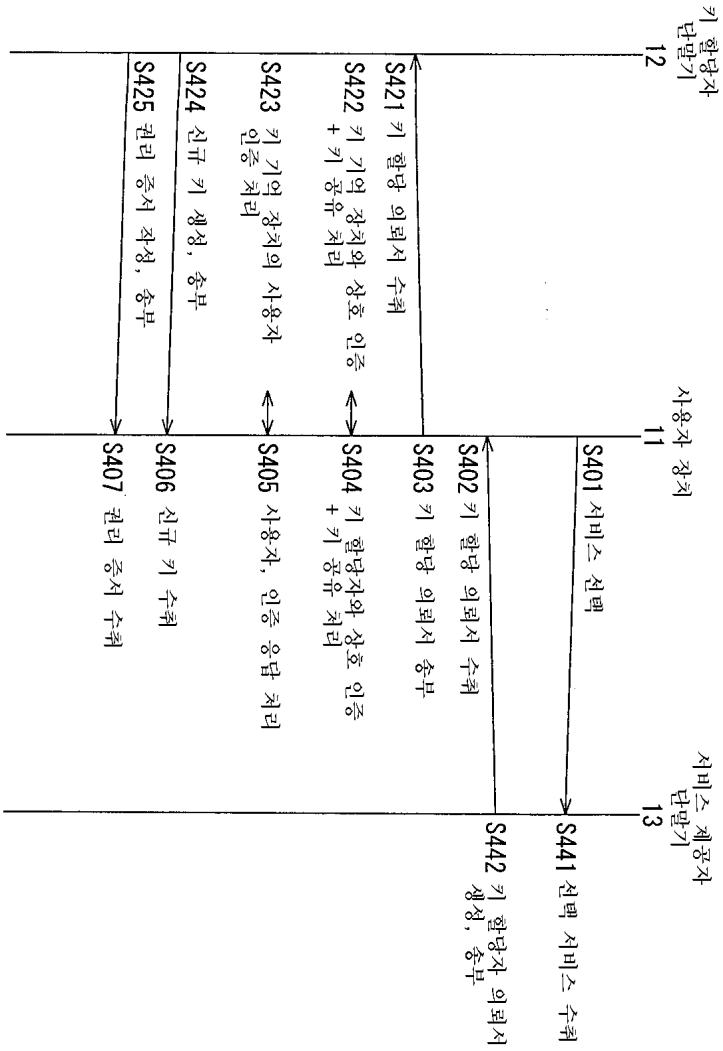
도면115


키 할당자 단말기의 서비스 선택/
키 할당 처리 개시
키 할당 의뢰서를 수취한다
S421
키 기억 장치와 상호 인증 + 키 공유 처리
S422
키 기억 장치의 사용자 인증 처리
S423
신규 키를 생성하여, 송부한다
S424
권리 증서를 작성하여, 송부한다
S425
처리 종료

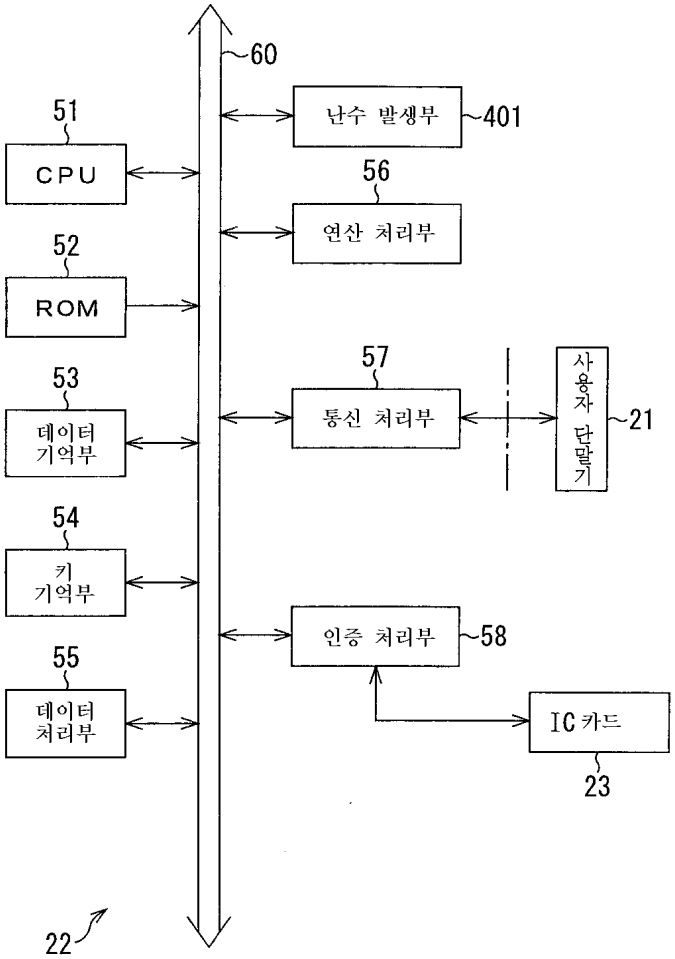
도면116


서비스 제공자 단말기의 서비스 선택/
키 할당 처리 개시
선택 서비스를 수취한다
S441
키 할당자 의뢰서를 생성하여, 송부한다
S442
처리 종료

도면117


키 할당자 단말기
12
사용자 장치
11
서비스 제공자 단말기
13
S401 서비스 선택
S441 선택 서비스 수취
S402 키 할당 의뢰서 수취
S442 키 할당자 의뢰서 생성, 송부
S403 키 할당 의뢰서 송부
S421 키 할당 의뢰서 수취
S404 키 할당자와 상호 인증 + 키 공유 처리
S422 키 기억 장치와 상호 인증 + 키 공유 처리
S405 사용자, 인증 응답 처리
S423 키 기억 장치의 사용자 인증 처리
S406 신규 키 수취
S424 신규 키 생성, 송부
S407 권리 증서 수취
S425 권리 증서 작성, 송부

도면118



도면119

키 할당표				
Key-ID	Acc-ID	HW-ID	키 할당 의뢰서	키 할당 보고서
KID1	AID1	HWID1	App1	Rep1
KID2	AID2	HWID2	App2	Rep2
KID3	AID3	HWID3	App3	Rep3
:	:	:	:	:

도면120

키 기억 장치 PKI 정보	
증명서	인증키
CERTHWO	SKHWO

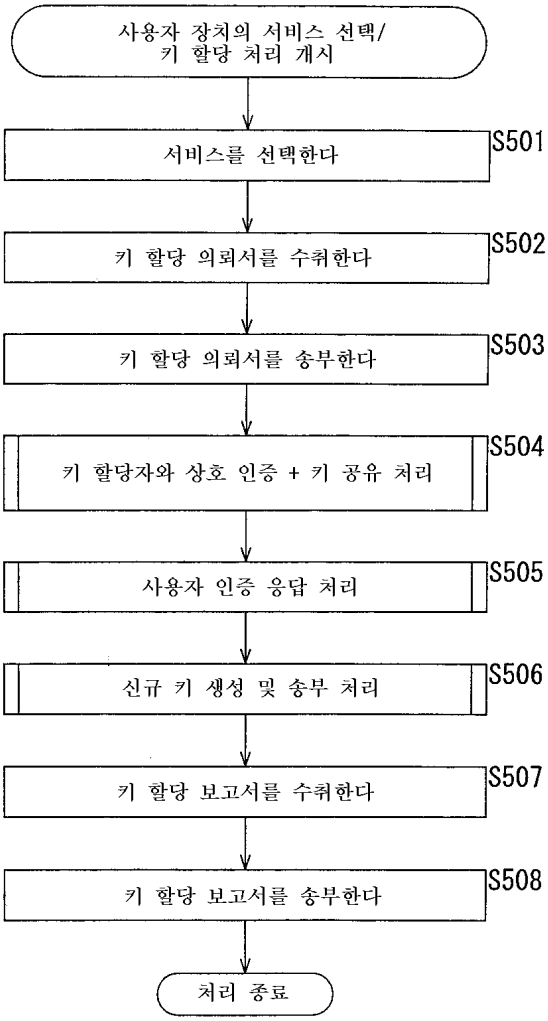
도면121

키 일시 기억표	
증명키	검증키
Kpr	Kpub

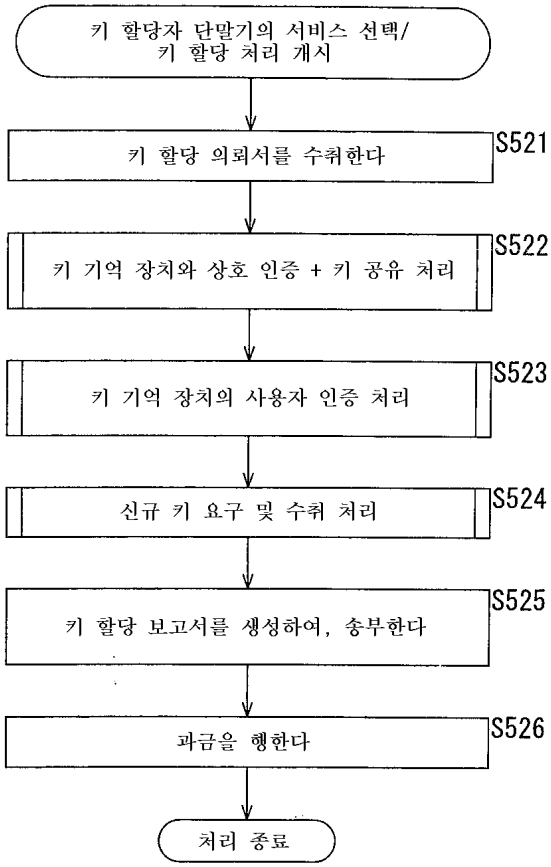
도면122

인증용 키표		
Index	증명키 (후보)	검증키 (후보)
ID0	Kpr1	Kpub1
ID2	Kpr2	Kpub2
:	:	:

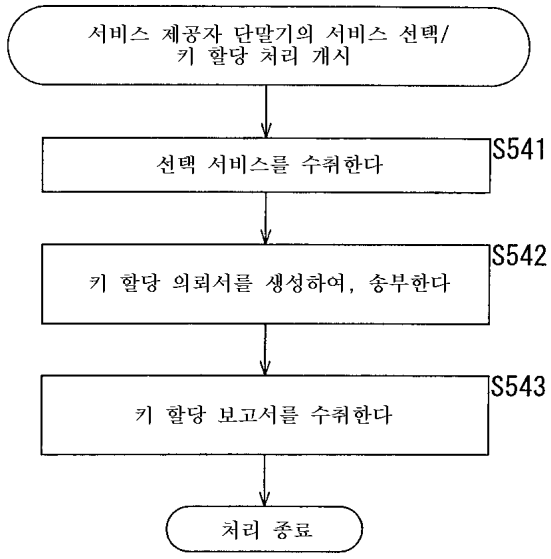
도면123



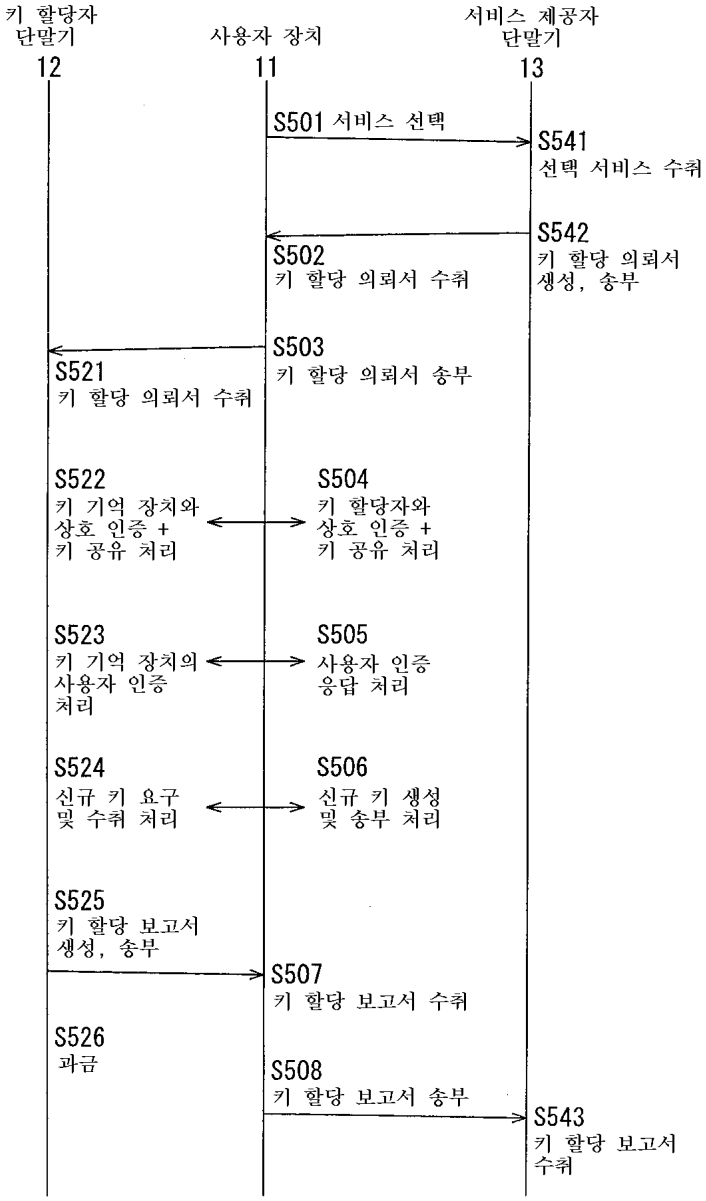
도면124


키 할당자 단말기의 서비스 선택/
키 할당 처리 개시
키 할당 의뢰서를 수취한다
S521
키 기억 장치와 상호 인증 + 키 공유 처리
S522
키 기억 장치의 사용자 인증 처리
S523
신규 키 요구 및 수취 처리
S524
키 할당 보고서를 생성하여, 송부한다
S525
과금을 행한다
S526
처리 종료

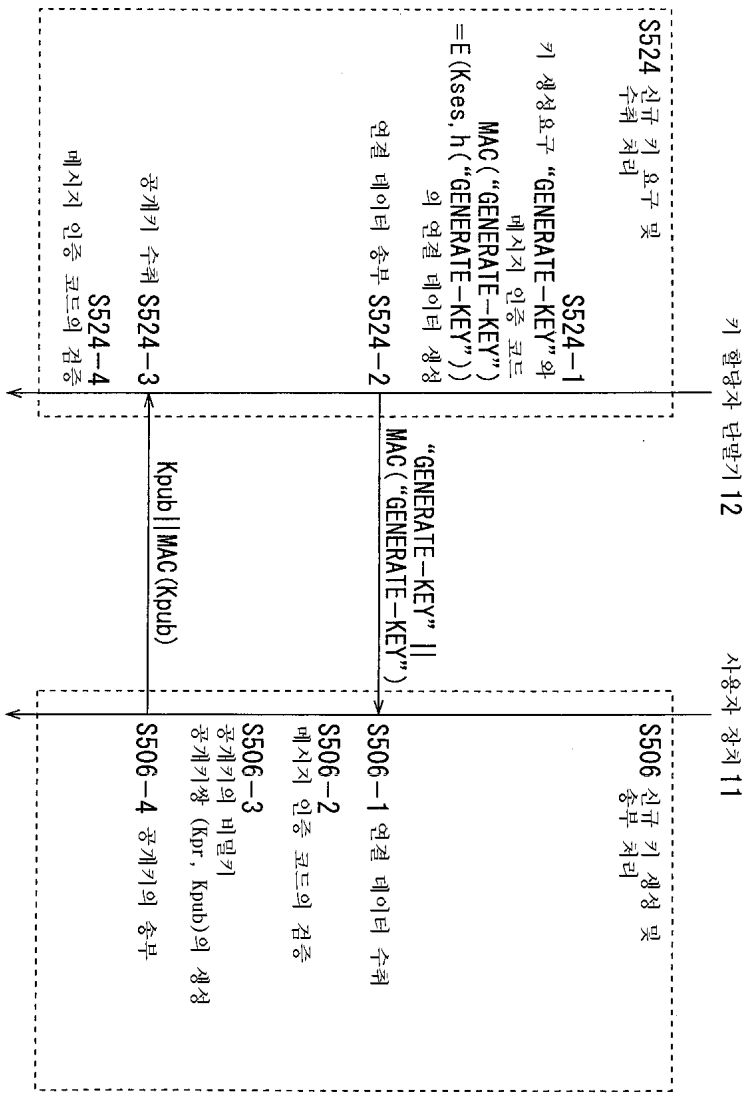
도면125


서비스 제공자 단말기의 서비스 선택/
키 할당 처리 개시
선택 서비스를 수취한다
S541
키 할당 의뢰서를 생성하여, 송부한다
S542
키 할당 보고서를 수취한다
S543
처리 종료

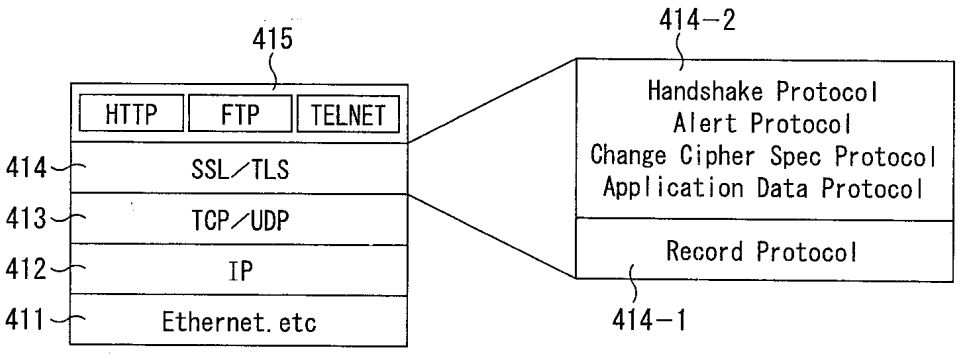
도면126


키 할당자
단말기
12
사용자 장치
11
서비스 제공자
단말기
13
S501 서비스 선택
S541
선택 서비스 수취
S542
키 할당 의뢰서
생성, 송부
S502
키 할당 의뢰서 수취
S503
키 할당 의뢰서 송부
S521
키 할당 의뢰서 수취
S522
키 기억 장치와
상호 인증 +
키 공유 처리
S504
키 할당자와
상호 인증 +
키 공유 처리
S523
키 기억 장치의
사용자 인증
처리
S505
사용자 인증
응답 처리
S524
신규 키 요구
및 수취 처리
S506
신규 키 생성
및 송부 처리
S525
키 할당 보고서
생성, 송부
S507
키 할당 보고서 수취
S526
과금
S508
키 할당 보고서 송부
S543
키 할당 보고서
수취

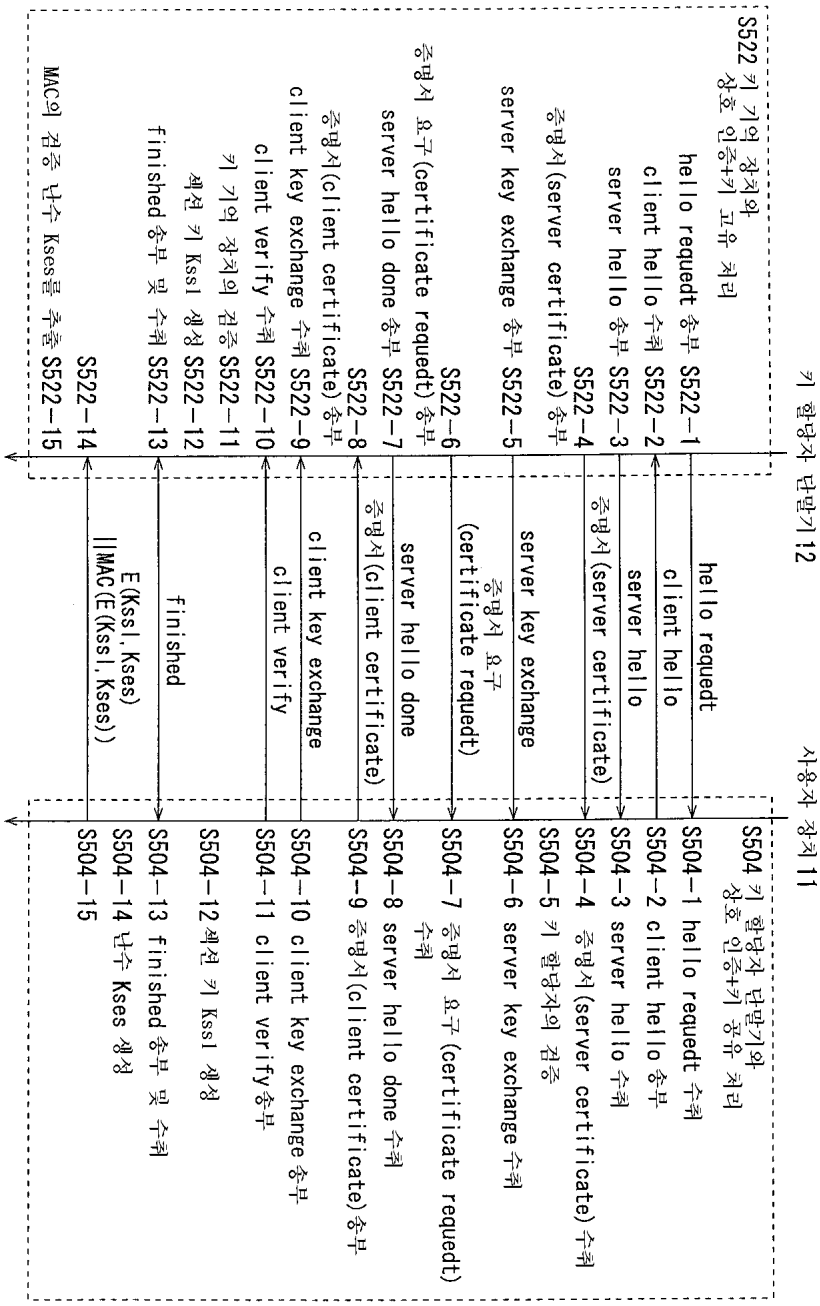
도면127


키 할당자 단말기 12
사용자 장치 11
S524 신규 키 요구 및 수취 처리
S524-1 키 생성요구 "GENERATE-KEY"와 메시지 인증 코드 =E(Kses,h("GENERATE-KEY")) MAC("GENERATE-KEY")의 연결 데이터 생성
S524-2 연결 데이터 송부
S524-3 공개키 수취
S524-4 메시지 인증 코드의 검증
"GENERATE-KEY" || MAC("GENERATE-KEY")
Kpub||MAC(Kpub)
S506 신규 키 생성 및 송부 처리
S506-1 연결 데이터 수취
S506-2 메시지 인증 코드의 검증
S506-3 공개키의 비밀키 공개키쌍 (Kpr, Kpub)의 생성
S506-4 공개키의 송부

도면128


415
HTTP
FTP
TELNET
414
SSL/TLS
413
TCP/UDP
412
IP
411
Ethernet.etc
414-2
Handshake Protocol
Alert Protocol
Change Cipher Spec Protocol
Application Data Protocol
Record Protocol
414-1

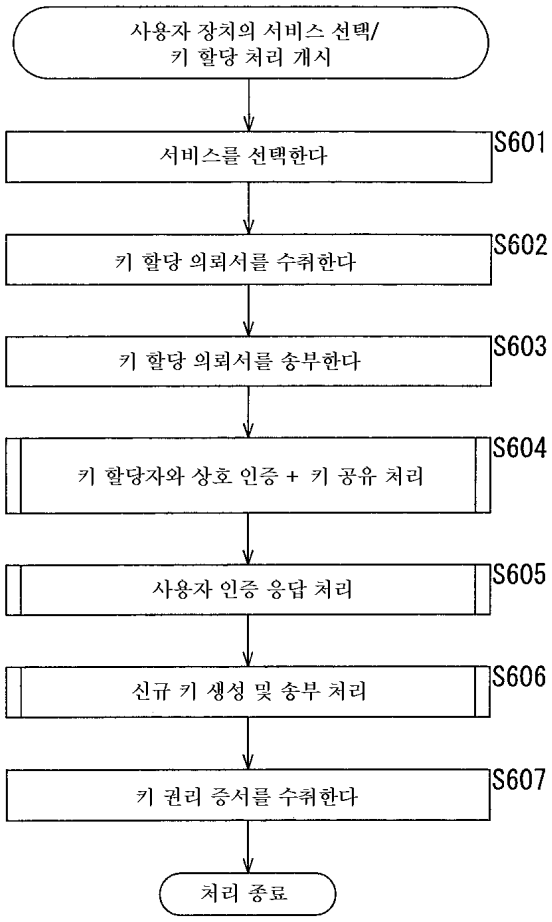
도면129



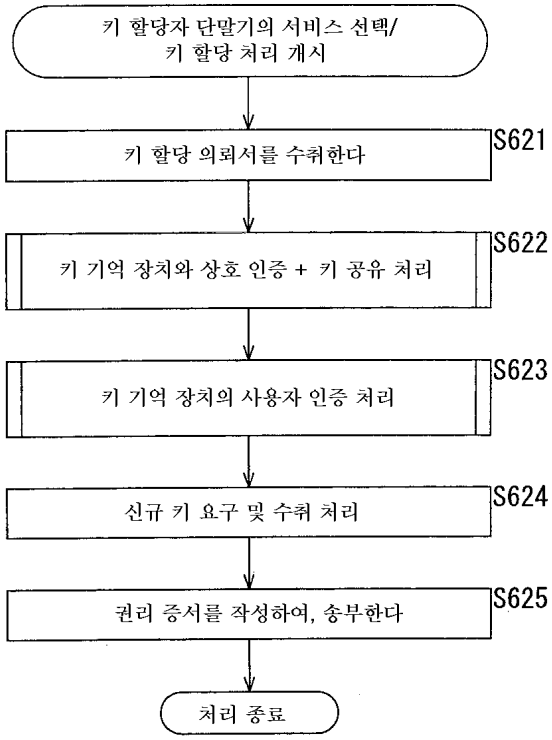
도면130

키 할당표						
Key-ID	Acc-ID	HW-ID	SP-ID	유효 기한	권리 증서	검증키
KID1	AID1	HWID1	SPID1	date1	Rcert1	Kpub1
KID2	AID2	HWID2	SPID2	date2	Rcert2	Kpub2
KID3	AID3	HWID3	SPID3	date3	Rcert3	Kpub3
:	:	:	:	:	:	:

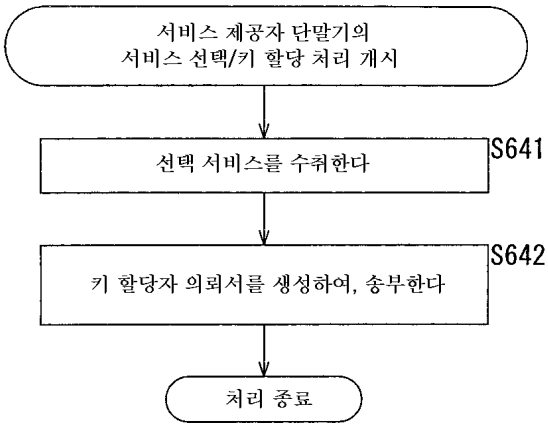
도면131


사용자 장치의 서비스 선택/
키 할당 처리 개시
서비스를 선택한다
S601
키 할당 의뢰서를 수취한다
S602
키 할당 의뢰서를 송부한다
S603
키 할당자와 상호 인증 + 키 공유 처리
S604
사용자 인증 응답 처리
S605
신규 키 생성 및 송부 처리
S606
키 권리 증서를 수취한다
S607
처리 종료

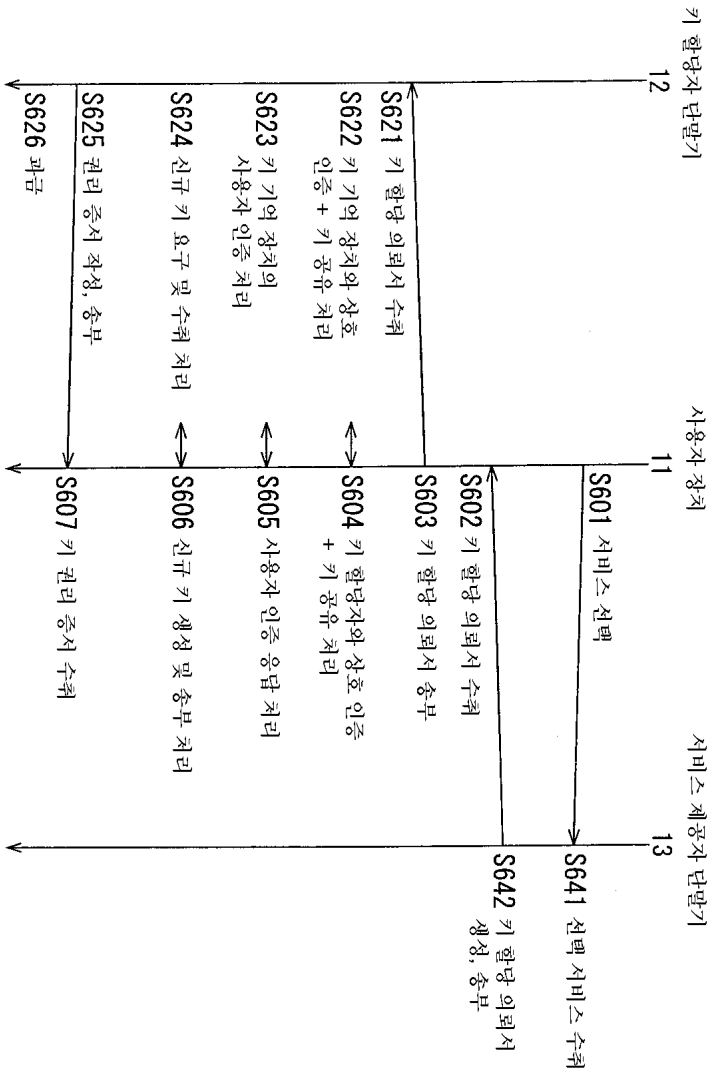
도면132


키 할당자 단말기의 서비스 선택/
키 할당 처리 개시
키 할당 의뢰서를 수취한다
S621
키 기억 장치와 상호 인증 + 키 공유 처리
S622
키 기억 장치의 사용자 인증 처리
S623
신규 키 요구 및 수취 처리
S624
권리 증서를 작성하여, 송부한다
S625
처리 종료

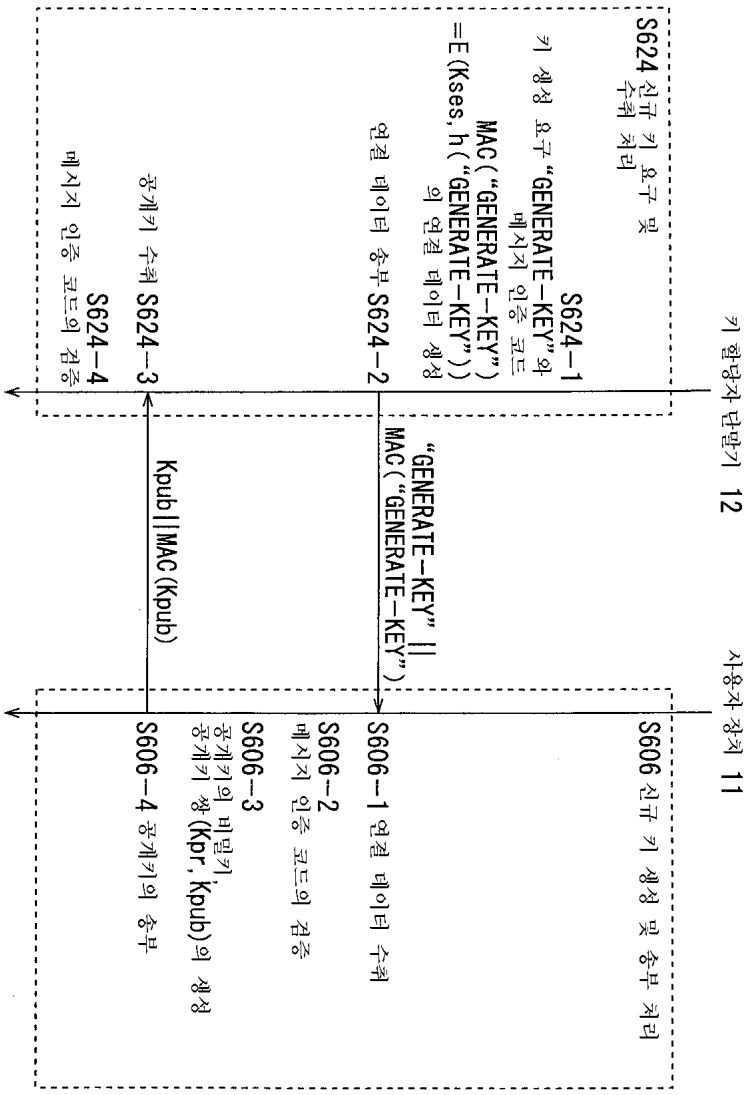
도면133


서비스 제공자 단말기의
서비스 선택/키 할당 처리 개시
선택 서비스를 수취한다
S641
키 할당자 의뢰서를 생성하여, 송부한다
S642
처리 종료

도면134


키 할당자 단말기
12
사용자 장치
11
서비스 제공자 단말기
13
S601 서비스 선택
S602 키 할당 의뢰서 수취
S603 키 할당 의뢰서 송부
S604 키 할당자와 상호 인증
+ 키 공유 처리
S605 사용자 인증 응답 처리
S606 신규 키 생성 및 송부 처리
S607 키 권리 증서 수취
S621 키 할당 의뢰서 수취
S622 키 기억 장치와 상호
인증 + 키 공유 처리
S623 키 기억 장치의
사용자 인증 처리
S624 신규 키 요구 및 수취 처리
S625 권리 증서 작성, 송부
S626 과금
S641 선택 서비스 수취
S642 키 할당 의뢰서
생성, 송부

도면135


키 할당자 단말기 12
사용자 장치 11
S624 신규 키 요구 및 수취 처리
S624-1 키 생성 요구 "GENERATE-KEY"와 메시지 인증 코드 MAC("GENERATE-KEY")=E(Kses, h("GENERATE-KEY"))의 연결 데이터 생성
S624-2 연결 데이터 송부
"GENERATE-KEY" || MAC("GENERATE-KEY")
S606 신규 키 생성 및 송부 처리
S606-1 연결 데이터 수취
S606-2 메시지 인증 코드의 검증
S606-3 공개키의 비밀키 공개키 쌍 (Kpr, Kpub)의 생성
S606-4 공개키의 송부
Kpub||MAC(Kpub)
공개키 수취 S624-3
S624-4 메시지 인증 코드의 검증