世界知的所有権機
国 際 事 務
PCT
特許協力条約に基づいて公
WO 9607256A1

(51) 国際特許分類6
H04L 9/32, G09C 1/00, G06F 15/00
A1
(11) 国際公開番号 WO96/07256
(43) 国際公開日 1996年3月7日(07.03.96)

(21) 国際出願番号 PCT/JP95/01708
(22) 国際出願日 1995年8月29日(29.08.95)

(30) 優先権データ
特願平6/227414 1994年8月30日(30.08.94) JP

(71) 出願人（米国を除くすべての指定国について）
国際電信電話株式会社
(KOKUSAI DENSHIN DENWA CO., LTD.)[JP/JP]
〒163-03 東京都新宿区西新宿二丁目3番2号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
鈴木利則(SUZUKI, Toshinori)[JP/JP]
〒175 東京都板橋区赤塚四丁目14番8号 403号室 Tokyo, (JP)
大橋正良(OHASHI, Masayoshi)[JP/JP]
〒365 埼玉県鴻巣市赤見台二丁目19番2号 Saitama, (JP)
(74) 代理人
弁理士 山本恵一(YAMAMOTO, Keiichi)
〒105 東京都港区西新橋一丁目11番1号 Tokyo, (JP)

(81) 指定国
JP, US, 欧州特許(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

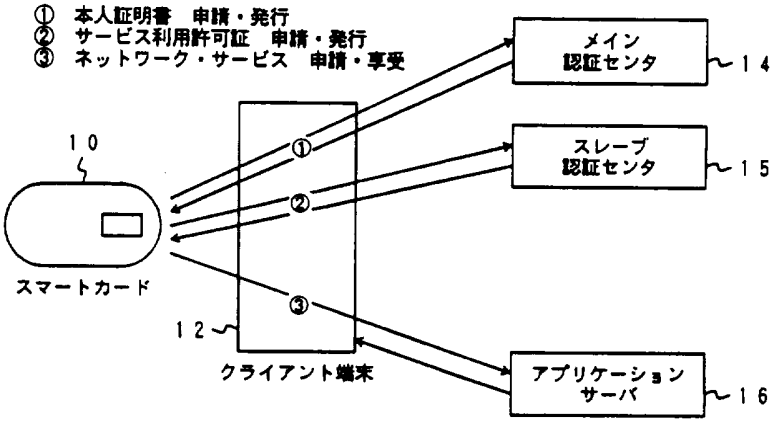
添付公開書類 国際調査報告書

(54) **Title** : CERTIFYING SYSTEM

(54) 発明の名称 認証システム

(57) **Abstract**

A certifying system by which a user is identified on the network side without dispersing the secret information of the user. The certifying system is provided with a single main certifying center sharing the user's secret key with the user and a plurality of slave certifying centers sharing secret keys which are different from the user's secret keys with the main certifying center. The main certifying center identifies the user according to a certifying method using the user's secret key. When the user is identified, the main certifying center issues identification formation which certifies the validity of the user to the user. Each of the slave certifying center certifies the validity of the identification information supplied from a user. When the identification information is valid, the slave certifying center issues permission information for permitting the user to access a specific server or an application server of the network.



1 ... application and issuance of identification
2 ... application and issuance of service utilization permit
3 ... application and reception of network service
10 ... smart card
12 ... client terminal
14 ... main certifying center
15 ... slave certifying center
16 ... application server

（５７）要約

ユーザの秘密情報を分散させることなく認証処理をネットワーク側で分散して行うことができる認証システムを提供する。

各ユーザ毎のユーザ秘密鍵を各ユーザと共有している単一のメイン認証センタと、上述したユーザ秘密鍵とは異なる秘密鍵をメイン認証センタとそれぞれ共有している複数のスレーブ認証センタとを備えている。メイン認証センタは、ユーザとの間でユーザ秘密鍵を用いて上述の認証方法による認証を行い、ユーザが正当である場合はその正当性を証明する認証情報をユーザに発行するように構成されている。スレーブ認証センタは、ユーザから提供される認証情報の認証を行い、この認証情報が正当である場合はネットワークの特定のサーバ又はアプリケーションサーバにアクセスすることを許可する許可情報をユーザに発行するように構成されている。

明　細　書

認証システム

技術分野

本発明は、ネットワークを介してユーザがサービスを受けるときに、そのユーザの身元をネットワークが確認するための認証システムに関する。

背景技術

ネットワークを介して通信又はサービスを受けるユーザ（以下ネットワークユーザと称する）が、そのサービス（通信を含む）を享受する正当な資格があることを確認するためには、ネットワーク側においてそのユーザの認証を行う必要がある。

ここで、認証されるものを証明者（ｐｒｏｖｅｒ）、認証を行うものを検証者（ｖｅｒｉｆｉｅｒ）と呼ぶと、証明者を確認する手順は、一般に、

（１）その証明者のみが有する情報を、

（２）何らかの方法で検証者が確認する、

という操作から成り立っている。

（１）証明者のみが有する情報は、

（１－１）人為的に与える情報（パスワード、暗証番号、秘密鍵等）、

（１－２）個人の属性に基づく情報（筆跡、指紋、声紋、網膜パターン等）、の２つに分類できる。個人の属性に基づく情報（１－２）のうち、筆跡を除く個人属性に基づく認証は、社会的受容性が低いこと、利便性が悪いこと、照合率が低いこと、及び認証装置のコストが高くなること等から、ネットワークを介した認証装置としては、現在のところあまり適していない。このため、証明者のみが有する情報として、パスワード、暗証番号、秘密鍵等の人為的に

与える情報（１－１）を用いることが多い。

この人為的に与える情報（ユーザ固有の情報）をユーザ側で保持する方法より分類すると、

（１－１－１）ユーザに記憶させる（パスワード、暗証番号等）、

（１－１－２）ユーザが所有する物に記憶させる（一般の鍵、磁気カード、ＩＣカード等）、

（１－１－３）これら（１－１－１）及び（１－１－２）の組み合わせ（金融機関のキャッシュディスペンサ等）、

の３種類が考えられる。なお、この分類は認証システムの観点から行ったものである。従って、ユーザがパスワードや暗証番号を覚えきれずに持ち物に書き留めた場合であっても、認証システムとしては（１－１－１）に分類される。

コンピュータネットワークでは、主に、ユーザに記憶させる（１－１－１）の方式が用いられる。しかしながら、この（１－１－１）の方式には、パスワード、暗証番号の見破りや漏洩等によって比較的簡単に不正が可能となり、しかも被害が実際に発生するまで本人がその不正に気づかない場合が多いという欠点がある。また、秘密情報そのものが直接ユーザの目に触れてしまうから情報漏洩の可能性が高く、さらに、本人の知らないところでパスワード、暗証番号の見破り、盗難、盗聴等が発生することが十分にあり得る。

これに対して、ユーザが所有する物に記憶させる（１－１－２）の方式は、所有物を紛失した際に起こり得る被害を予見できるので、適切な処置を施すことによって被害発生を未然に防ぐことが可能となる。また、その所有物だけでは偽れないように、（１－１－１）及び（１－１－２）の方式を組み合わせた（１－１－３）の方式を用いても良い。当然のことながら、所有物の偽造がユーザ及びネットワークの知らないところで起これば被害を未然に防ぐことはで

きない。従って、偽造されにくい所有物であることが好ましく、この意味で所有物としては、情報の秘匿性が高いＣＰＵ付ＩＣカード（以下スマートカードと称する）が最も優れている。

（２）検証者が確認する何らかの方法は、何を検証者（ネットワーク）に提示するかに応じて、

（２－１）ユーザ固有の情報をそのまま提示する、

（２－２）ユーザ固有の情報を演算した結果を提示する、

という２つ方法に大別できる。しかしながら、ユーザ固有の情報をそのまま提示する（２－１）の方法は、ユーザ固有の秘密情報が露呈してしまうので危険であり、特に、前述のユーザに記憶させる（１－１－１）の方式と組み合わせた場合にその秘密情報が人目に触れてしまう機会が最も多くなる。演算結果を提示する（２－２）の方法は、演算の種類によってさらに分類できるが、本発明は、検証者（ネットワーク）と証明者（ユーザ）とでユーザ固有の秘密情報を共有し、その秘密情報に対してネットワーク及びユーザがそれぞれ暗号演算を行い、それらを照合することで正当性を検証する方法を想定している。なお、演算結果を提示する（２－２）の方法と個人の属性に基づく情報（１－２）で認証する方式との組み合わせはなじまない。

以上説明したように、ユーザに記憶させる（１－１－１）の方式とユーザ固有の情報をそのまま提示する（２－１）の方法との組み合わせが最も危険であり、ユーザが所有する物に記憶させる（１－１－２）の方式又は（１－１－１）及び（１－１－２）の方式を組み合わせた（１－１－３）の方式（ただし偽造されにくい所有物）と演算結果を提示する（２－２）の方法との組み合わせが最も安全であると言える。スマートカードを用いたこの後者の組み合わせによる認証システムが、一部の移動通信ネットワーク、例えばＧＳＭ（Ｇｌｏｂａｌ　Ｓｙｓｔｅｍ　ｆｏｒ　Ｍｏｂｉｌｅ　ｃｏｍｍｕｎｉｃａｔｉｏｎｓ、汎ヨーロッパ・デジタル移動通信システム

）において実際に用いられている。

しかしながら、上述したごとき演算結果を提示する（２－２）の方法を用いた認証システムによると、認証を行う都度に暗号演算が必要となることからネットワーク側でユーザの秘密情報を管理している認証装置に認証処理の負荷が集中してしまうという不都合があった。

このような不都合を避けるためには、複数の認証装置に秘密情報を渡して演算を分担すればよいが、秘密の情報を複数の場所に広めると認証の安全性が弱まることとなる。また、認証装置はユーザの秘密情報を格納しているのでその管理及び運用には充分な注意を払うことが必要であるが、このようにユーザの秘密情報を格納している場所を複数持つことは管理及び運用に要する費用もその分増大することとなってコスト的に非常に不利となる。

発明の開示

従って本発明は、従来技術の上述した問題点を解決するためのものであり、その目的は、ユーザ固有の情報の演算結果を提示することによってそのユーザの正当性を確認する場合に、ユーザの秘密情報を分散させることなく認証処理をネットワーク側で分散して行うことができる認証システムを提供することにある。

本発明によれば、ネットワーク側とユーザ側とで同一の秘密鍵を共有し、ネットワーク側及びユーザ側において既知の情報を前記秘密鍵でそれぞれ暗号化し、ユーザ側から提示された暗号化情報をネットワーク側が自己の作成した暗号化情報と照合することによってそのユーザの正当性を確認する認証方法を用いる認証システムは、ネットワーク側に設けられており各ユーザ毎のユーザ秘密鍵を各ユーザと共有している単一のメイン認証センタと、ネットワーク側に設けられており上述したユーザ秘密鍵とは異なる秘密鍵をメイン認証センタとそれぞれ共有している複数のスレーブ認証センタとを備

えている。メイン認証センタは、ユーザとの間でユーザ秘密鍵を用いて上述の認証方法による認証を行い、ユーザが正当である場合はその正当性を証明する認証情報をユーザに発行するように構成されている。スレーブ認証センタは、ユーザから提供される認証情報の認証を行い、この認証情報が正当である場合はネットワークの特定のサーバ又はアプリケーションサーバにアクセスすることを許可する許可情報をユーザに発行するように構成されている。

このように、各ユーザのユーザ秘密鍵を各ユーザと共有しているのは、ただ1つ存在しているメイン認証センタのみであるから、秘密鍵が複数の場所に分散されることはない。しかも、メイン認証センタはこのユーザ秘密鍵を用いて認証を行ってそのユーザが正当であることを証明する認証情報をユーザに発行し、スレーブ認証センタはその認証情報が正当である場合はネットワークの特定のサーバ又はアプリケーションサーバへのアクセスを許可する許可情報をユーザに発行するので、認証の分散処理が行われる。

なお、アプリケーションサーバが上述のスレーブ認証センタの役割を受け持つことも可能であり、この場合許可情報およびスレーブ認証センタは不要である。本人証明書を繰り返し使用することによって認証センタへの認証処理を軽減することができる。

ユーザ側から提示された暗号化情報をネットワーク側が自己の作成した暗号化情報と照合することによってそのユーザの正当性を確認するのみならず、ネットワーク側から提示された暗号化情報をユーザが自己の作成した暗号化情報と照合することによってネットワークの正当性をも確認することが望ましい。これによって相互認証が行われるので、認証の安全性及び確実性がより向上する。

ユーザ側におけるユーザ秘密鍵の管理、並びに暗号文の作成及び解読がＣＰＵ付ＩＣカード（スマートカード）内で行われるように構成されていることも好ましい。ユーザ側の秘密鍵の管理や暗号文の作成等にスマートカードを用いることにより、秘密鍵が端末等に

露呈することがなくまた偽造が極めて困難であるから安全性が非常に高くなる。

既知の情報を暗号化する上述した秘密鍵がユーザ側で発生した乱数を使用したものであることも好ましい。このような乱数をも用いた秘密鍵で暗号化することにより、安全性がさらに向上する。

図面の簡単な説明

図１は、本発明の認証システムの一実施例（実施例１）の構成を概略的に示すブロック図である。

図２は、図１の実施例における３段階の認証手順を概略的に示す図である。

図３は、図２の認証手順の第１段階における詳細な処理手順を示す図である。

図４は、図２の認証手順の第２段階における詳細な処理手順を示す図である。

図５は、図２の認証手順の第３段階における詳細な処理手順を示す図である。

図６は、本発明の認証システムの他の実施例（実施例２）の構成を概略的に示すブロック図である。

図７は、図６の実施例における認証手順の一例の第１段階における詳細な処理手順例を示す図である。

図８は、図７の認証手順の第２段階における詳細な処理手順例を示す図である。

図９は、図６の実施例における認証手順の他の例の第１段階における詳細な処理手順例を示す図である。

図１０は、図９の認証手順の第２段階における詳細な処理手順例を示す図である。

図１１は、図６の実施例の認証手順における本人証明書の内容を示す図である。

発明を実施するための最良の形態

以下図面を用いて本発明の実施例を詳細に説明する。

実施例１

図１は本発明の認証システムの一実施例の構成を概略的に示すブロック図である。

この実施例は、従来技術の部分で述べたユーザ固有の情報を演算した結果を提示する（２－２）の方法を用いるものであり、ユーザ固有の情報をスマートカードに記憶させる（１－１－２）方式が用いられている。しかしながら、本発明は、ユーザ固有情報をユーザに記憶させる（１－１－１）方式であっても（１－１－１）及び（１－１－２）の組み合わせ（１－１－３）方式であってもよい。ただし、（２－２）の方式の演算をユーザ実行することは利便性の点で問題がありしかも秘密情報がユーザに知られてしまうので情報漏洩の可能性もあるから、ユーザ側ではスマートカードのように、メモリ機能の他に演算機能を有するユーザ所有物が演算を代行することが好ましい。この場合、本実施例の（１－１－２）の方式又は（１－１－３）の方式となる。

図１において、１０は各ユーザが所有しており後述するファイル及びプログラムを有するスマートカード、１１はスマートカード１０を読み書きするためのリーダ／ライタ、並びに１２はこのリーダ／ライタ１１を内蔵又は外付けしておりクライアント側アプリケーション及び認証カーネルを有するクライアント端末をそれぞれ示している。

スマートカード１０は、例えば１６ＫＢ程度のメモリと例えば８ビットのＣＰＵとを内蔵した演算機能付きのＩＣカードで構成されている。クライアント端末１２は、汎用ワークステーション又は汎用パーソナルコンピュータで構成されており、回線を介して例えばＬＡＮ等のネットワーク１３に接続可能となっている。このクライアント端末１２は、ユーザがネットワーク１３にアクセスするポイ

ントであり、逆にアプリケーションサーバ側からのネットワークサービスを提供する端末である。なお、図１には１つのクライアント端末１２しか示されていないが、実際には、同様の構成を少なくとも有する複数のクライアント端末１２がそれぞれの回線を介してネットワーク１３に接続可能となっている。

ネットワーク１３には、後述する認証プログラムを有する単一のメイン認証センタ（メインＡｕＣ）１４と、後述する認証プログラムを有する複数のスレーブ認証センタ（スレーブＡｕＣ）１５、並びにサーバ側アプリケーション及び認証カーネルを有する少なくとも１つのアプリケーションサーバ（ＡＰＳ）１６が接続可能となっており、これらはこのネットワーク１３を介してクライアント端末１２と通信できるように構成されている。

メイン認証センタ１４のデータベース１４ａには、ユーザの秘密鍵等のユーザデータ、システムログ、ユーザのブラックリスト、各スレーブ認証センタの秘密鍵等のデータが少なくとも格納されている。スレーブ認証センタ１５のデータベース１５ａには、各アプリケーションサーバ１６の秘密鍵等のＡＰＳデータが少なくとも格納されている。メイン認証センタ１４、スレーブ認証センタ１５、及びアプリケーションサーバ１６は、汎用ワークステーションで構成されており、これら汎用ワークステーション間及び汎用パーソナルコンピュータとの間の通信は、ＲＰＣ（Ｒｅｍｏｔｅ　Ｐｒｏｃｅｄｕｒｅ　Ｃａｌｌ、遠隔手続き呼出し）を介して行っている。

スマートカード１０は、その所有者に固有の秘密情報（ユーザ秘密鍵Ｋｕ）をそのメモリに記憶していると共に内蔵ＣＰＵがこのＫｕを鍵として暗号演算ｆを行うようにプログラムされている。

ユーザ秘密鍵Ｋｕは、ネットワーク側では、ただ１つ設けられているメイン認証センタ１４のみが保持している。この１つのメイン認証センタ１４と複数のスレーブ認証センタ１５とは、各スレーブ認証センタ１５毎に固有の秘密情報（スレーブＡｕＣ秘密鍵Ｋｓ１

、Ｋｓ２、Ｋｓ３、…）を共有している。また、各スレーブ認証センタ１５とユーザにネットワークサービスを提供するアプリケーションサーバ１６との間でも、アプリケーションサーバ１６毎に固有の秘密情報（ＡＰＳ秘密鍵Ｋａ１、Ｋａ２、Ｋａ３、…）を共有している。

次に本実施例による認証動作について説明する。今、ユーザが特定のアプリケーションサーバ１６から所望のネットワークサービスを受けようとしていると仮定する。

まず、ユーザは自分の所有するスマートカード１０をリーダ／ライタ１１に挿入すると共にクライアント端末１２に対して次のようなアクセスを行ってこのスマートカード１０を活性化する。

カードユーザに対しては、あらかじめＰＩＮ（Ｐｅｒｓｏｎａｌ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ Ｎｕｍｂｅｒ）コードが付与されており、スマートカード１０内にはこれがあらかじめ登録されている。ユーザは、まずこのＰＩＮコードを提示してそのカードの正当な所有者であることを証明する。ＰＩＮコードの照合は、スマートカード１０内で行われる。入力が連続して例えば３回失敗すると、それ以降はユーザの資格でアクセスすることを拒否される。スマートカード１０のこのメモリは不揮発性であり、電源を断っても過去の連続失敗回数を記憶している。

スマートカード１０が活性化されると、図２に概略的に示す３段階の認証手順で認証処理が実行される。

第１段階は、①本人証明書の申請及び発行であり、これはユーザ側がメイン認証センタ１４にアクセスし、スレーブ認証センタ１５で認証手続を行うための認証情報（本人証明書）をもらう手続である。本人証明書は、有効期限付きであり、一度発行されるとスマートカード１０内に保持される。ユーザは、メイン認証センタ１４にアクセスする前にスマートカード１０内に格納されている本人証明書の有効期限を確認し、まだ有効であればメイン認証センタ１４に

アクセスせずに次の第２段階から処理を行うことができる。これによってメイン認証センタ１４の処理量を軽減することができる。

第２段階は、②サービス利用許可証の申請及び発行であり、これはユーザ側が本人証明書を添えてスレーブ認証センタ１５にアクセスし、アプリケーションサーバ１６の利用を許可する許可情報（サービス利用許可証）をもらう手続である。スレーブ認証センタ１５は、本人証明書が正当化か否かを鑑定し、正当であればサービス利用許可証を発行する。

第３段階は、③ネットワークサービスの申請及び享受であり、これはユーザがサービス利用許可証をもってアプリケーションサーバ１６へアクセスし、アプリケーションサーバ１６側では利用許可証が正当であれば要求されたサービスをクライアント端末１２へ提供する。

図３、図４及び図５は、上述した各段階における詳細な処理手順を示す図であり、以下この処理手順を順次説明する。手順説明の前に、これらの図に用いられている記号の意味を解説しておく。

ＡｕＣ	認証センタ
ＩＤｕ	スマートカードに付与された固有の番号（スマートカードとメインＡｕＣのみが保持している）
Ｋｕ	ユーザ秘密鍵（スマートカードとメインＡｕＣのみが保持している）
Ｋｓ	スレーブＡｕＣ秘密鍵（メインＡｕＣと各スレーブＡｕＣ間のみで共有している）
Ｋａ	ＡＰＳ秘密鍵（スレーブＡｕＣと各ＡＰＳ間のみで共有している）
Ｋｕ－ｓ	スマートカードとスレーブＡｕＣ間の暗号鍵（本人証明書を発行する度にメ

	インＡｕＣが生成する使い捨ての鍵）
Ｋｕ－ａ	スマートカードとＡＰＳ間の暗号鍵（サービス利用許可証を発行する度にスレーブＡｕＣが生成する使い捨ての鍵）
ｃ＿ａｄｄｒ	クライアント端末のネットワークアドレス
Ｔｓ	タイムスタンプ（現在時刻又は有効期限の時刻を表わす）
Ｃｅｒｔ	本人証明書（メインＡｕＣが発行し、スレーブＡｕＣのみが解読できる）
Ｌｉｃ	サービス利用許可証（スレーブＡｕＣが発行し、ＡＰＳのみが解読できる）
Ａ／Ｒｅｓ	アクセス／レスポンスメッセージ
｜	データ同士の連結を行う操作
Ｘ＝Ｙ？	タイムスタンプＸとＹが所定のマージン内で一致することを確認する操作
ｆ（ｄａｔａ，Ｋ）	ｄａｔａを鍵Ｋで暗号化する操作
ｆ-1（ｄａｔａ，Ｋ）	鍵Ｋで逆暗号化する操作

図３は第１段階の①本人証明書の申請及び発行の手順例である。まず、クライアント端末１２が現在の時刻Ｔｓ１を生成し、この生成したタイムスタンプＴｓ１とそのクライアント端末１２のネットワークアドレスｃ＿ａｄｄｒとをそのままスマートカード１０に転送する。図３では、この転送が［Ｔｓ１，ｃ＿ａｄｄｒ］で表わされている。転送されたデータは、スマートカード１０内で連結された後にこのスマートカード内に格納されているユーザ秘密鍵Ｋｕで暗号演算（以下単に暗号化と称する）されてＡ＝ｆ（Ｔｓ１｜ｃ＿ａｄｄｒ，Ｋｕ）が得られる。このスマートカード１０内に格納されているカード番号ＩＤｕが読出され、暗号化されたＡと共にメイ

ン認証センタ１４にアクセスされる。この転送が［ＩＤｕ，Ａ］で表わされている。ただし、カード番号ＩＤｕは暗号化されないで転送される。スマートカード１０とメイン認証センタ１４との間の通信は、全てクライアント端末１２経由で行われるが、クライアント端末１２自身は暗号化されたデータを解読することができない。

メイン認証センタ１４では、クライアント端末１２からの要求を受け付けた時刻Ｔｓ２を生成して記録する。次いで、カード番号ＩＤｕに対応するユーザ秘密鍵Ｋｕをデータベース１４ａから検索する。検索したユーザ秘密鍵Ｋｕを用いて、暗号化されているＡを解読するための復号処理Ｔｓ１｜ｃ＿ａｄｄｒ＝ｆ-1（Ａ，Ｋｕ）を行ってクライアント端末１２のタイムスタンプＴｓ１とネットワークアドレスｃ＿ａｄｄｒとを読出す。次いで、この読出されたＴｓ１とＴｓ２とが照合される。ただし、Ｔｓ２は当然のことながらＴｓ１より遅れているので、その遅延等によるマージン（例えば１０秒）を考慮した上での一致が照合されることになる。スマートカード側で暗号化してＡを生成する際に用いたユーザ暗号鍵Ｋｕが正しくないものであれば、メイン認証センタ１４で解読して得たＴｓ１はＴｓ２と大きく異なるので、Ｔｓ１とＴｓ２とは一致しないこととなる。この場合、認証が失敗した旨をユーザ側に通知して処理を終了する。

Ｔｓ１とＴｓ２とが一致した場合にのみ、本人証明書Ｃｅｒｔを発行するための以下の処理を行う。まず、スマートカードとスレーブ認証センタ間の暗号鍵Ｋｕ－ｓを生成し、次に、Ｋｕ－ｓ、Ｔｓ２及びｃ＿ａｄｄｒから構成されるオリジナルの本人証明書Ｃｅｒｔ（Ｋｕ－ｓ，Ｔｓ２，ｃ＿ａｄｄｒ）を作成する。この本人証明書Ｃｅｒｔは、メイン認証センタとそのスレーブ認証センタと間のみで共有されるスレーブＡｕＣ秘密鍵Ｋｓで暗号化ｆされてＣｅｒｔ′が生成される。即ち、Ｃｅｒｔ′＝ｆ（Ｃｅｒｔ，Ｋｓ）がなされる。次いで、Ｔｓ２及びＫｕ－ｓと共にＣｅｒｔ′がユーザ暗

号鍵Ｋｕで逆暗号化ｆ-1されてＲｅｓが生成される。即ち、Ｒｅｓ＝ｆ-1（Ｃｅｒｔ′｜Ｔｓ２｜Ｋｕ－ｓ，Ｋｕ）がなされる。このメイン認証センタで、暗号化ｆではなく逆暗号化ｆ-1がなされるのは、スマートカード等ではその演算能力の関係上、暗号化ｆのみを行うように構成しているためである。このようにして作成されたＲｅｓは、ユーザからのアクセスに対する応答メッセージとしてスマートカードに返信される（［Ｒｅｓ］）。

応答メッセージＲｅｓを受け取ったスマートカード１０は、このＲｅｓをユーザ秘密鍵Ｋｕで復号する処理ｆを行って、暗号化されているＣｅｒｔ′とタイムスタンプＴｓ２と暗号鍵Ｋｕ－ｓとを取り出してカード内のメモリに格納する。即ち、Ｃｅｒｔ′｜Ｔｓ２｜Ｋｕ－ｓ＝ｆ（Ｒｅｓ，Ｋｕ）の処理を行う。タイムスタンプＴｓ２はクライアント端末１２に転送されて、タイムスタンプＴｓ１と照合される（Ｔｓ１＝Ｔｓ２？）。これにより、メイン認証センタ１４の正当性が確認され、相互認証が行われることとなる。スマートカードとスレーブ認証センタ間の暗号鍵Ｋｕ－ｓは、カードの外に露呈されることなくスマートカードとスレーブ認証センタ間の通信に使用される。また、Ｃｅｒｔ′はＫｓで暗号化されているので、スマートカード１０及びクライアント端末１２では全く解読できない。

なお、次回の認証処理時にクライアント端末１２は、メイン認証センタ１４へアクセスする前にスマートカード１０内に格納されているタイムスタンプＴｓ２を読出しこれと現在の時刻とを比較することにより、カード内に格納されている本人証明書Ｃｅｒｔ′の有効期限をチェックする。有効期限内であれば、図３に示した第１段階の処理を飛ばしていきなり第２段階へ進むことができるのでメイン認証センタ１４の処理量をその分だけ低減することができる。

図４は第２段階の②サービス利用許可証の申請及び発行の手順例である。まず、クライアント端末１２が現在の時刻Ｔｓ３を生成し

、この生成したタイムスタンプＴｓ３と自己のネットワークアドレスｃ＿ａｄｄｒとをスマートカード１０に転送する。図４では、この転送が［Ｔｓ３，ｃ＿ａｄｄｒ］で表わされている。ただし、前述した第１段階の直後にこの第２段階を実行する場合には、Ｔｓ３がマージン内でＴｓ１に等しくまたｃ＿ａｄｄｒは既に送ってあるので、この部分の処理を省略することが可能である。転送されたデータは、スマートカード１０内で連結された後に、本人証明書Ｃｅｒｔ′と共にメイン認証センタ１４から送られてきてこのスマートカード内に格納されている秘密鍵Ｋｕ－ｓで暗号化される。これによって、Ａ′＝ｆ（Ｔｓ３｜ｃ＿ａｄｄｒ，Ｋｕ－ｓ）が得られる。このＡ′と本人証明書Ｃｅｒｔ′とがスレーブ認証センタ１５に提出される。この転送が［Ｃｅｒｔ′，Ａ′］で表わされている。スマートカード１０とスレーブ認証センタ１５との間の通信も、全てクライアント端末１２経由で行われるが、クライアント端末１２自身は暗号化されたデータを解読することができない。

スレーブ認証センタ１５では、クライアント端末１２からアクセスのあった時刻Ｔｓ４を生成して記録する。次いで、スレーブ認証センタ１５が保有するスレーブＡｕＣ秘密鍵Ｋｓを用いて、暗号化されている本人証明書Ｃｅｒｔ′を解読する。即ち、復号処理Ｃｅｒｔ＝ｆ-１（Ｃｅｒｔ′，Ｋｓ）を行う。この本人証明書Ｃｅｒｔには、その証明書の発行時刻Ｔｓ２と暗号鍵Ｋｕ－ｓとクライアント端末１２のネットワークアドレスｃ＿ａｄｄｒとが含まれている。次いで、Ｔｓ２がＴｓ４によってチェックされ、本人証明書Ｃｅｒｔが一定時間以内に発行されたものであるかどうかが確認される。これは、本人証明書Ｃｅｒｔの有効期限を確かめるためのものである。次に、この本人証明書Ｃｅｒｔに含まれている暗号鍵Ｋｕ－ｓによって Ａ′を復号する。即ち、Ｔｓ３｜ｃ＿ａｄｄｒ＝ｆ-１（Ａ′，Ｋｕ－ｓ）により、クライアント端末１２での時刻Ｔｓ３とそのネットワークアドレスｃ＿ａｄｄｒを得る。

次に、Ｔｓ３とＴｓ４とを照合し、さらに本人証明書Ｃｅｒｔに含まれているｃ＿ａｄｄｒとＡ′に含まれているｃ＿ａｄｄｒとを照合する。もし、本人証明書Ｃｅｒｔが偽造されたものであれば、本人証明書Ｃｅｒｔに含まれている暗号鍵Ｋｕ－ｓとネットワークアドレスｃ＿ａｄｄｒとが正常に読出せず、さらにこの暗号鍵Ｋｕ－ｓを用いた解読も不可能となるので、照合に失敗することとなる。この場合、スレーブ認証センタ１５はサービス利用許可証Ｌｉｃを発行せず、認証が失敗した旨をユーザ側に通知して処理を終了する。

照合が成功した場合にのみサービス利用許可証Ｌｉｃを発行する。即ち、まず、スマートカードと特定のアプリケーションサーバ間のＡＰＳ暗号鍵Ｋｕ－ａを生成し、次に、Ｋｕ－ａ、Ｔｓ４及びｃ＿ａｄｄｒから構成されるオリジナルのサービス利用許可証Ｌｉｃ（Ｋｕ－ａ，Ｔｓ４，ｃ＿ａｄｄｒ）を作成する。このサービス利用許可証Ｌｉｃは、スレーブ認証センタと特定のアプリケーションサーバ間のみで共有されるＡＰＳ秘密鍵Ｋａで暗号化ｆされてＬｉｃ′が生成される。即ち、Ｌｉｃ′＝ｆ（Ｌｉｃ，Ｋａ）がなされる。これにより該当するアプリケーションサーバのみが解読できることになる。次いで、Ｔｓ４及びＫｕ－ａと共にＬｉｃ′が暗号鍵Ｋｕ－ｓで逆暗号化ｆ-1されてＲｅｓ′が生成される。即ち、Ｒｅｓ′＝ｆ-1（Ｌｉｃ′｜Ｔｓ４｜Ｋｕ－ａ，Ｋｕ－ｓ）がなされる。このようにして作成されたＲｅｓ′は、ユーザからのアクセスに対する応答メッセージとしてスマートカードに返信される（［Ｒｅｓ′］）。

応答メッセージＲｅｓ′を受け取ったスマートカード１０は、このＲｅｓ′を秘密鍵Ｋｕ－ｓで復号する処理ｆを行って、暗号化されているＬｉｃ′とタイムスタンプＴｓ４と暗号鍵Ｋｕ－ａとを取り出してカード内のメモリに格納する。即ち、Ｌｉｃ′｜Ｔｓ４｜Ｋｕ－ａ＝ｆ（Ｒｅｓ′，Ｋｕ－ｓ）の処理を行う。タイムスタン

プＴｓ４はクライアント端末１２に転送されて、タイムスタンプＴｓ３と照合される（Ｔｓ３＝Ｔｓ４？）。これにより、スレーブ認証センタ１５の正当性が確認され、相互認証が行われることとなる。スマートカードとアプリケーションサーバ間の暗号鍵Ｋｕ－ａは、カードの外に露呈されることなくスマートカードとアプリケーションサーバ間の通信に使用される。また、Ｌｉｃ′はＫａで暗号化されているので、スマートカード１０及びクライアント端末１２では全く解読できない。

図５は第３段階の③ネットワークサービスの申請及び享受の手順例である。まず、クライアント端末１２が現在の時刻Ｔｓ５を生成し、この生成したタイムスタンプＴｓ５と自己のネットワークアドレスｃ＿ａｄｄｒとをスマートカード１０に転送する。図５では、この転送が［Ｔｓ５，ｃ＿ａｄｄｒ］で表わされている。ただし、前述した第２段階の直後にこの第３段階を実行する場合には、Ｔｓ５がマージン内でＴｓ３に等しくまたｃ＿ａｄｄｒは既に送ってあるので、この部分の処理を省略することが可能である。転送されたデータは、スマートカード１０内で連結された後に、サービス利用許可証Ｌｉｃ′と共にスレーブ認証センタ１５から送られてきてこのスマートカード内に格納されている秘密鍵Ｋｕ－ａで暗号化される。これによって、Ａ″＝ｆ（Ｔｓ５｜ｃ＿ａｄｄｒ，Ｋｕ－ａ）が得られる。このＡ″とサービス利用許可証Ｌｉｃ′とがアプリケーションサーバ（ＡＰＳ）１６に提出される。この転送が［Ｌｉｃ′，Ａ″］で表わされている。スマートカード１０とアプリケーションサーバ１６との間の通信も、全てクライアント端末１２経由で行われるが、クライアント端末１２自身は暗号化されたデータを解読することができない。

アプリケーションサーバ１６では、クライアント端末１２からアクセスのあった時刻Ｔｓ６を生成して記録する。次いで、アプリケーションサーバ１６が保有するＡＰＳ秘密鍵Ｋａを用いて、暗号化

されているサービス利用許可証Ｌｉｃ′を解読する。即ち、復号処理Ｌｉｃ＝ｆ-1（Ｌｉｃ′，Ｋａ）を行う。このサービス利用許可証Ｌｉｃには、その証明書の発行時刻Ｔｓ４と暗号鍵Ｋｕ－ａとクライアント端末１２のネットワークアドレスｃ＿ａｄｄｒとが含まれている。次いで、Ｔｓ４がＴｓ６によってチェックされ、サービス利用許可証Ｌｉｃが一定時間以内に発行されたものであるかどうかが確認される。これは、サービス利用許可証Ｌｉｃの有効期限を確かめるためのものである。次に、このサービス利用許可証Ｌｉｃに含まれている暗号鍵Ｋｕ－ａによって Ａ″を復号する。即ち、Ｔｓ５｜ｃ＿ａｄｄｒ＝ｆ-1（Ａ″，Ｋｕ－ａ）により、クライアント端末１２での時刻Ｔｓ５とそのネットワークアドレスｃ＿ａｄｄｒを得る。

次に、Ｔｓ５とＴｓ６とを照合し、さらにサービス利用許可証Ｌｉｃに含まれているｃ＿ａｄｄｒとＡ″に含まれているｃ＿ａｄｄｒとを照合する。もし、サービス利用許可証Ｌｉｃが偽造されたものであれば、サービス利用許可証Ｌｉｃに含まれている暗号鍵Ｋｕ－ａとネットワークアドレスｃ＿ａｄｄｒとが正常に読出せず、さらにこの暗号鍵Ｋｕ－ａを用いた解読も不可能となるので、照合に失敗することとなる。この場合、アプリケーションサーバ１６はネットワークサービスを提供せず、認証が失敗した旨をユーザ側に通知して処理を終了する。

この照合が成功した場合にのみ、Ｔｓ６がＫｕ－ａによって逆暗号化ｆ-1されて応答メッセージＲｅｓ″が生成される。即ち、Ｒｅｓ″＝ｆ-1（Ｔｓ６，Ｋｕ－ａ）がなされる。このようにして作成されたＲｅｓ″は、ユーザからのアクセスに対する応答メッセージとしてスマートカードに返信される（［Ｒｅｓ″］）。

応答メッセージＲｅｓ″を受け取ったスマートカード１０は、このＲｅｓ″を秘密鍵Ｋｕ－ａで復号する処理ｆを行って、タイムスタンプＴｓ６を取り出してカード内のメモリに格納する。即ち、Ｔ

ｓ６＝ｆ（Ｒｅｓ″，Ｋｕ－ａ）の処理を行う。タイムスタンプＴｓ６はクライアント端末１２に転送されて、タイムスタンプＴｓ５と照合される（Ｔｓ５＝Ｔｓ６？）。これにより、アプリケーションサーバ１６の正当性が確認され、相互認証が行われることとなる。この相互認証が行われた後にアプリケーションサーバ１６からクライアント端末１２にネットワークサービスが提供される。

なお、以上述べた認証手順を行う前提条件として、メイン認証センタ１４、スレーブ認証センタ１５、アプリケーションサーバ１６及びクライアント端末１２間で時刻同期が行われているものとする。これは、証明者と検証者との間で既知の認証用データ（暗号演算を施すデータ）として時刻情報（タイムスタンプ）を用いているためである。時刻情報の代わりに、例えば前述したＧＳＭで使用しているチャレンジ・レスポンス・プロトコルのように、検証する側（ネットワーク側）で生成した乱数をユーザ側に知らせることにより、その乱数を認証用データとして用いても良い。

前述した実施例では、スマートカード１０から転送する情報を暗号化する場合に、ユーザ秘密鍵Ｋｕ、スレーブＡｕＣ秘密鍵Ｋｓ又はＡＰＳ秘密鍵Ｋａを直接的に用いてその情報を暗号化している。しかしながら、スマートカード側で乱数Ｒを発生させ、その乱数Ｒをユーザ秘密鍵Ｋｕ、スレーブＡｕＣ秘密鍵Ｋｓ又はＡＰＳ秘密鍵Ｋａで暗号化した鍵により情報の暗号化を図るようにすれば、安全性がより向上する。ただしこの場合、乱数Ｒもメイン認証センタ１４、スレーブ認証センタ１５又はアプリケーションサーバ１６へ転送する必要がある。

また、前述した実施例では、各スレーブ認証センタ毎に別個のスレーブＡｕＣ秘密鍵Ｋｓを設定しているが、全てのスレーブ認証センタで共通のスレーブＡｕＣ秘密鍵Ｋｓを使用するようにしてもよい。ただしこの場合、安全性は多少低下する。

実施例２

図６は本発明による認証システムの他の実施例の構成を概略的に示すブロック図である。

同図において、スマートカード１０、リーダ／ライタ１１、クライアント端末１２及びネットワーク１３は、実施例１の場合と同じ構成及び機能を有しているのでここでは説明を省略する。

スマートカード１０は、例えば８ＫＢ以下のメモリと８ビットのＣＰＵとを内蔵した演算機能付きのＩＣカードで構成されている。本実施例では、構成が実施例１の場合よりもシンプルである分、実施例１よりもメモリ容量の少ないスマートカードで構成できる。

ネットワーク１３には、ユーザの正当性を証明する認証プログラムを有する認証センタ１７と、ユーザにサービスを提供するサーバ側アプリケーション１６が接続可能となっており、これらはネットワーク１３を介してクライアント端末１２と通信できるように構成されている。

認証センタ１７のデータベース１７ａには、ユーザの秘密鍵等のユーザデータ、システムログ、ユーザのブラックリスト、アプリケーションサーバ１６の秘密鍵が少なくとも格納されている。

スマートカード１０は、その所有者に固有の秘密鍵（ユーザ秘密鍵Ｋｕ）をそのメモリに記憶しているとともに内蔵ＣＰＵがこのＫｕを鍵として認証演算ｆを行うようにプログラムされている。

ユーザ秘密鍵Ｋｕは、ネットワーク側では認証センタ１７のみが保持している。

認証センタ１７とアプリケーションサーバ１６とは、各アプリケーションサーバごとに固有の秘密情報（ＡＰＳ秘密鍵Ｋａ１、Ｋａ２、Ｋａ３、・・・）を共有している。

今、ユーザが特定のアプリケーションサーバ１６から所望のサービスを受けようとしていると仮定する。

まず、ユーザは自分の所有するスマートカード１０をリーダ／ラ

イタ１１に挿入するとともにクライアント端末１２に対して次のようなアクセスを行ってこのスマートカード１０を活性化する。

カードユーザに対しては、あらかじめＰＩＮコードが付与されており、スマートカード１０内にはこれがあらかじめ登録されている。ユーザは、まずこのＰＩＮコードをスマートカード１０に提示して、正当な所有者であることをスマートカード１０に対して証明する。ＰＩＮコードの照合はスマートカード１０内で行われる。入力を連続して例えば３回失敗すると、スマートカード１０はそれ以降ＰＩＮコードの照合を拒否し、認証の手続きを実行しない。スマートカード１０のメモリは不揮発性であり、電源を断っても過去の連続失敗回数を記憶している。このメモリは、ＰＩＮコード照合が例えば３回以内に成功した時点でクリアされる。

スマートカード１０が活性化されると、本実施例では、以下に示す２段階の認証手順で認証処理が実行される。

第１段階は、本人証明書の申請及び発行である。これはユーザ側が認証センタ１７にアクセスし、自分の正当性を証明する本人証明書をもらう手続である。本人証明書は、有効期限付きであり、一度発行されるとスマートカード１０内に格納される。ユーザは認証センタにアクセスする前に、スマートカード１０内に格納されている本人証明書の有効期限を確認し、まだ有効であれば認証センタ１７にアクセスせずに、次の第２段階から処理を行うことができる。これによって認証センタ１７の処理量を軽減することができる。

第２段階では、本人証明書を添えてアプリケーションサーバ１６にアクセスし、アプリケーションサーバ１６側はその本人証明書が正当であれば要求されたサービスをクライアント端末１２へ提供する。

図７及び図８は、上述した処理手順の一例をそれぞれ示している。図９及び図１０は、さらに、ユーザ側においてもネットワーク側を認証する相互認証方法を適用した場合の処理手順の例を示してい

る。なお、図７の処理手順と図１０の処理手順との組み合わせ、並びに図９の処理手順と図８の処理手順との組み合わせによる認証手順も可能である。

図７は第１段階の本人証明書の申請及び発行の手順例である。まずスマートカード１０に格納されているカード番号ＩＤｕが読み出され、ユーザが要求しているサービスを提供するアプリケーションサーバ名と共に、認証センタ１７に送信する。アプリケーションサーバ名は後に本人証明書や認証情報を生成するときに参照する。

認証センタ１７では乱数ＲＮＤを生成し、スマートカード１０へ送り返す。スマートカード１０では送られた乱数ＲＮＤを、スマートカード１０に格納されているユーザ秘密鍵Ｋｕで暗号化し、その結果ＲＥＳを認証センタ１７に送り返す。認証センタ１７では、カード番号ＩＤｕに対応するユーザ秘密鍵Ｋｕをデータベース１７ａから検索し、スマートカード１０で行った演算と同じ演算を行い、互いの結果を照合する。スマートカード１０内に格納されているユーザ秘密鍵Ｋｕが正しいものであれば、これらの結果は一致する。もし、ユーザ秘密鍵Ｋｕが正しくないのであれば、これらの演算結果は異なるので、照合に失敗することとなる。この場合、認証が失敗した旨をユーザ側に通知して処理を終了する。

ＲＥＳが一致した場合にのみ、認証センタ１７は本人証明書とそれに付随する認証情報をスマートカード１０に対して発行する。図１１は発行する情報の内容の一例を示している。

本人証明書は、偽造を防止する目的からＡＰＳ秘密鍵Ｋａで暗号処理されている。よって本人証明書は、その内容がユーザ側で解読できないので、有効期間などの必要な項目についてのみ、重複してユーザに転送している。

この第１段階にユーザ側においてもネットワーク側を認証する相互認証方法を適用した場合について、その概略が図９に示されている。スマートカード１０からカード番号ＩＤｕとアプリケーション

サーバ名を認証センタ１７へ要求し、認証センタ１７で乱数ＲＮＤ１を生成し、スマートカード１０へ返送する。スマートカード１０では受け取ったＲＮＤ１をユーザ秘密鍵Ｋｕで暗号化するとともに、認証センタ１７を認証するために乱数ＲＮＤ２を生成し、これら２つの情報、ＲＥＳ１とＲＮＤ２を認証センタ１７へ送り返す。

認証センタ１７では、カード番号ＩＤｕに対応するユーザ秘密鍵Ｋｕをデータベース１７ａから検索し、スマートカード１０で行った演算と同じ演算を行い、互いの結果を照合する。スマートカード１０内に格納されているユーザ秘密鍵Ｋｕが正しいものであれば、これらの結果は一致する。もし、ユーザ秘密鍵Ｋｕが正しくないのであれば、これらの演算結果は異なるので、照合に失敗することとなる。この場合、認証が失敗した旨をユーザ側に通知して処理を終了する。

認証に成功した場合、認証センタ１７は、認証センタの正当性をスマートカード１０に示すため、スマートカード１０が生成した乱数ＲＮＤ２を同じユーザ秘密鍵Ｋｕで暗号化するとともに、本人証明書とそれに関係する認証情報を作成し、これらの情報をスマートカード１０へ転送する。

スマートカード１０では、受け取った情報のうちまずはじめに認証演算結果ＲＥＳ２を、自分で計算した結果と照合する。もしこれらが一致しなければ、認証センタは不正である可能性が高いので、発行された本人証明書や認証情報を破棄し、認証失敗とする。照合が一致したときにのみ、本人証明書や認証情報をスマートカード１０に格納する。

なお本人証明書と認証情報を認証センタ１７からスマートカード１０に転送するときに、悪意のある第三者がこれを傍受、取得し、本人証明書や認証情報を悪用する可能性がある。これを防止するために、スマートカード１０と認証センタ１７間で、セッション鍵を設定しこれに基づいて本人証明書や認証情報を暗号化することが考

えられる。その場合、互いに生成した乱数ＲＮＤ１、ＲＮＤ２およびスマートカード１０と認証センタ１７のみが共有しているユーザ秘密鍵Ｋｕでセッション鍵を生成することが望ましい。

図８は第２段階のアプリケーションサーバに対するアクセス手順例である。まずスマートカード１０に格納されている本人証明書が読み出され、アプリケーションサーバ１６へ送られる。本人証明書は認証センタ１７が発行可能で、かつアプリケーションサーバ１６が鑑定するもので、スマートカード１０やクライアント端末１２は解読不能である。

アプリケーションサーバ１６では、送られた本人証明書を、自分のＡＰＳ秘密鍵Ｋａで解読し、その中に含まれる既知又はおおよその内容が想定できる情報例えばアプリケーションサーバ名、発行時刻、有効期限など、をみることでその正当性を鑑定できる。例えば本人証明書が偽造されたものであるならば、そこから有為な情報を得ることはできず、本人証明書の解読が失敗する。また、偽造されていなくとも、有効期限が既に過ぎた本人証明書については、無効扱いにする。

本人証明書の鑑定が成功した場合でも、スマートカード１０からアプリケーションサーバ１６にアクセスするときに本人証明書はＡＰＳ秘密鍵Ｋａで暗号化された形でネットワーク上を流れるから、悪意のある第三者がそれをそのままコピーして盗用している可能性がまだ残っている。この可能性を排除するため、アプリケーションサーバ１６ではスマートカード１０を認証するための乱数ＲＮＤを生成し、スマートカード１０へ送る。これを受け取ったスマートカード１０では、本人証明書が認証センタ１７から発行された時に一緒に送られてきた認証情報にあるユーザ・ＡＰＳ共通鍵Ｋｕ－ａで乱数ＲＮＤを暗号化し、その結果をＲＥＳとしてアプリケーションサーバ１６へ送る。

ユーザ・ＡＰＳ共通鍵Ｋｕ－ａは、図７又は図９に手順例が示さ

れている認証センタへのアクセス手順において、認証センタ１７からスマートカード１０へ送られる本人証明書と認証情報の両方に重複して存在する。この点は図１１にも記載されているとおりである。重複して送る理由は、本人証明書はアプリケーションサーバ１６が、認証情報はスマートカード１０がそれぞれ独立して解読するからである。ＡＰＳ秘密鍵Ｋａで暗号化された本人証明書だけを第三者が盗んでも、その内容が解読できないので、ユーザ・ＡＰＳ共通鍵Ｋｕ－ａで乱数ＲＮＤを暗号化することはできない。

アプリケーションサーバ１６では、同じ乱数ＲＮＤを、解読・鑑定した本人証明書に記載されているユーザ・ＡＰＳ共通鍵Ｋｕ－ａで暗号化し、その結果をスマートカード１０から送られたものと照合する。これらが不一致であれば、本人証明書は正当であっても、盗難された本人証明書である可能性が高いので、認証失敗としてユーザに通知する。演算結果が一致すれば、認証成功としてユーザから要求のあったサービスを提供する。

この第２段階にユーザ側においてもネットワーク側を認証する相互認証方法を適用した場合について、その概略が図１０に示されている。アプリケーションサーバ１６は、スマートカード１０から受け取った本人証明書を鑑定し、正当かつ有効なものであれば乱数ＲＮＤ１を生成し、スマートカード１０に返送する。スマートカード１０では、受け取った乱数ＲＮＤ１を認証センタ１７から通知されたユーザ・ＡＰＳ共通鍵Ｋｕ－ａで暗号化すると共に、アプリケーションサーバ１６を認証するための乱数ＲＮＤ２を生成し、それらをアプリケーションサーバ１６へ転送する。

アプリケーションサーバ１６では、同じ乱数ＲＮＤを、解読・鑑定した本人証明書に記載されているユーザ・ＡＰＳ共通鍵Ｋｕ－ａで暗号化し、その結果をスマートカード１０から送られたものと照合する。これらが不一致であれば、本人証明書は正当であっても、盗難された本人証明書である可能性が高いので、認証失敗としてユ

ーザに通知する。演算結果が一致すればユーザ認証が成功したと判断し、次にユーザに対してアプリケーションサーバ１６が正当であることを示すために、スマートカード１０から送られた乱数ＲＮＤ２を、解読・鑑定した本人証明書に記載されているユーザ・ＡＰＳ共通鍵Ｋｕ－ａで暗号化し、その結果をスマートカード１０に返送する。

スマートカード１０では、認証センタ１７から通知されたユーザ・ＡＰＳ共通鍵Ｋｕ－ａで乱数ＲＮＤ２を暗号化し、その結果をアプリケーションサーバ１６から送られた結果と照合することでアプリケーションサーバ１６の正当性を確認する。この相互認証が行われた後で、アプリケーションサーバ１６からクライアント端末１２にユーザ所望のサービスが提供される。

本実施例において、１回又は複数回有効な本人証明書は第三者に盗まれないように安全に格納することが肝要である。この点において、主体的にアクセス管理を行うことのできるＣＰＵ付きＩＣカード内で暗号処理を行って本人証明書を格納することは、効果的に作用する。

以上詳細に説明したように本発明によれば、ネットワーク側とユーザ側とで同一の秘密鍵を共有し、ネットワーク側及びユーザ側において既知の情報を前記秘密鍵でそれぞれ暗号化し、ユーザ側から提示された暗号化情報をネットワーク側が自己の作成した暗号化情報と照合することによってそのユーザの正当性を確認する認証方法を用いる認証システムは、ネットワーク側に設けられており各ユーザ毎のユーザ秘密鍵を各ユーザと共有している単一のメイン認証センタと、ネットワーク側に設けられており上述したユーザ秘密鍵とは異なる秘密鍵をメイン認証センタとそれぞれ共有している複数のスレーブ認証センタとを備えている。メイン認証センタは、ユーザとの間でユーザ秘密鍵を用いて上述の認証方法による認証を行い、ユーザが正当である場合はその正当性を証明する認証情報をユーザ

に発行するように構成されている。スレーブ認証センタは、ユーザから提供される認証情報の認証を行い、この認証情報が正当である場合はネットワークの特定のサーバ又はアプリケーションサーバにアクセスすることを許可する許可情報をユーザに発行するように構成されている。このため、ユーザ固有の情報の演算結果を提示することによってそのユーザの正当性を確認する場合に、ユーザの秘密情報を分散させることなく認証処理をネットワーク側で分散して行うことができる。

本発明は一定期間若しくは一定回数有効である本人証明書によって、ユーザの秘密情報を分散させることなく認証処理をネットワーク側で分散することが可能ならしめるものであり、スレーブ認証センタの機能をアプリケーションサーバで実現しても同様の効果が得られる。

今後、インターネットやＣＡＴＶ網を介した決済や情報及び商品の売買等が活発に行われようとしており、ネットワークを介したユーザ認証が身近になるのみならず単一のネットワークでユーザ認証処理を行う必要となる場合が多数発生すると予見されている。本発明によれば、特にこのような環境において、効率的な認証システムを実現することができる。

以上述べた二つの実施例は全て本発明を例示的に示すものであって限定的に示すものではなく、本発明は他の種々の変形態様及び変更態様で実施することができる。従って本発明の範囲は特許請求の範囲及びその均等範囲によってのみ規定されるものである。

請求の範囲

1．　ネットワーク側とユーザ側とで同一の秘密鍵を共有し、該ネットワーク側及び該ユーザ側において既知の情報を前記秘密鍵でそれぞれ暗号化し、該ユーザ側から提示された該暗号化情報を前記ネットワーク側が自己の作成した暗号化情報と照合することによって該ユーザの正当性を確認する認証方法を用いる認証システムであって、

ネットワーク側に設けられており各ユーザ毎のユーザ秘密鍵を該各ユーザと共有している単一のメイン認証センタと、該ネットワーク側に設けられており前記ユーザ秘密鍵とは異なる秘密鍵を前記メイン認証センタとそれぞれ共有している複数のスレーブ認証センタとを備えており、

前記メイン認証センタは、前記ユーザとの間で前記ユーザ秘密鍵を用いて前記認証方法による認証を行い、該ユーザが正当である場合はその正当性を証明する認証情報を該ユーザに発行するように構成されており、前記スレーブ認証センタは、前記ユーザから提供される前記認証情報の認証を行い、該認証情報が正当である場合はネットワークの特定のサーバ又はアプリケーションサーバにアクセスすることを許可する許可情報を該ユーザに発行するように構成されていることを特徴とする認証システム。

2．　前記ネットワーク側から提示された暗号化情報を前記ユーザが自己の作成した暗号化情報と照合することによって該ネットワークの正当性をも確認する相互認証方法を用いていることを特徴とする請求項1に記載の認証システム。

3．　ユーザ側における、前記ユーザ秘密鍵の管理、並びに暗号文の作成及び解読がＣＰＵ付ＩＣカード内で行われるように構成されていることを特徴とする請求項1に記載の認証システム。

4．　既知の情報を暗号化する前記秘密鍵がユーザ側で発生した乱数を使用したものであることを特徴とする請求項1に記載の認証シ

ステム。

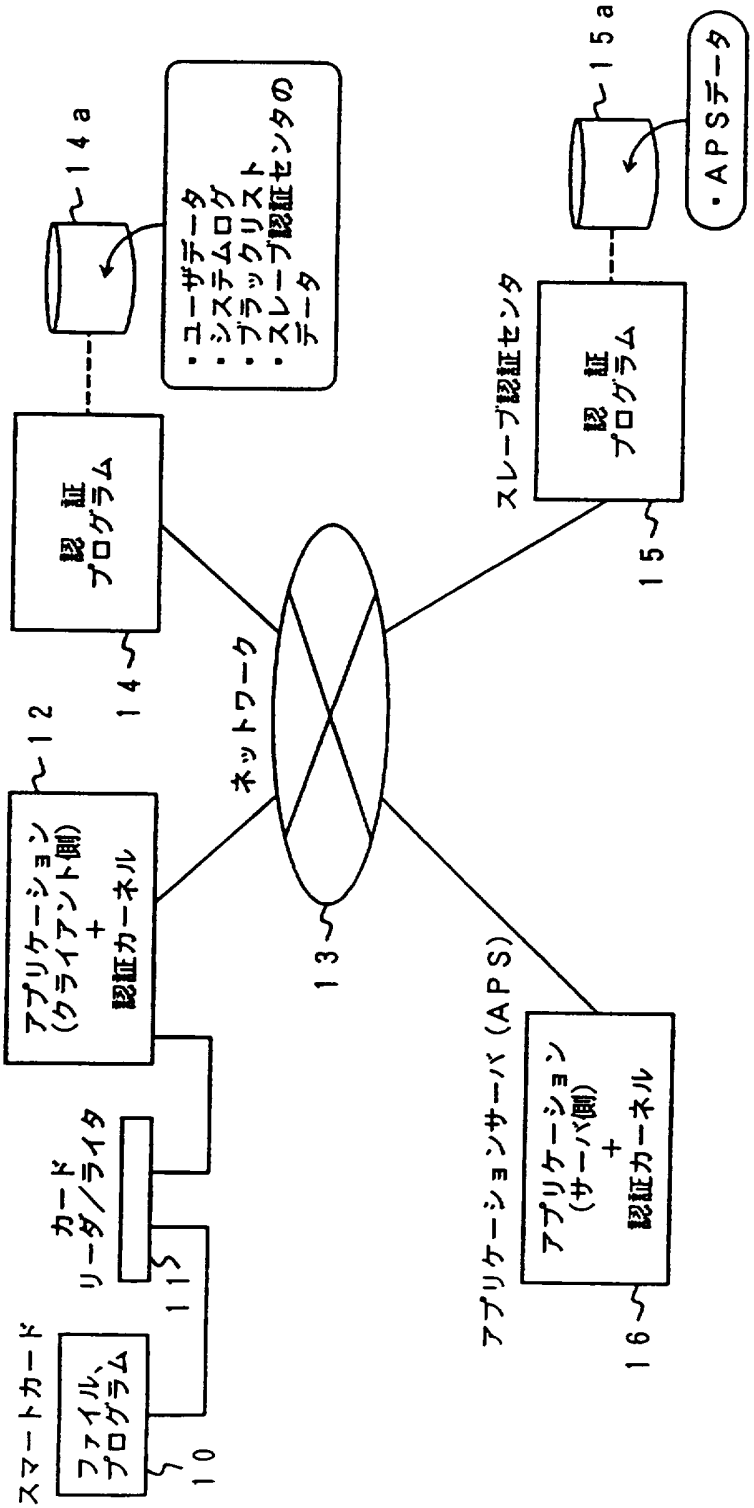
5． ネットワーク側とユーザ側とで同一の秘密鍵を共有し、該ネットワーク側及び該ユーザ側において既知の情報を前記秘密鍵でそれぞれ暗号化し、該ユーザ側から提示された該暗号化情報を前記ネットワーク側が自己の作成した暗号化情報と照合することによって該ユーザの正当性を確認する認証方法を用いる認証システムであって、

該ネットワーク側は、該ユーザの正当性が確認された後で該ユーザに対して、該ユーザの正当性を証明する、一定期間又は一定回数以内有効な認証情報を発行することを特徴とする認証システム。

6． ユーザ側における前記秘密鍵の管理、暗号文の作成及び解読、並びにネットワーク側が発行した認証情報の管理がＣＰＵ付ＩＣカード内で行われるように構成されていることを特徴とする請求項５に記載の認証システム。

7． ネットワーク側がユーザを認証すると共に、該ユーザ側においても該ネットワークを認証する相互認証方法を用いることを特徴とする請求項５に記載の認証システム。

図 1


スマートカード
ファイル、プログラム
10
カードリーダ/ライタ
11
クライアント端末
アプリケーション(クライアント側)＋認証カーネル
12
メイン認証センタ
認証プログラム
14
14a
・ユーザデータ
・システムログ
・ブラックリスト
・スレーブ認証センタのデータ
ネットワーク
13
スレーブ認証センタ
認証プログラム
15
15a
・APSデータ
アプリケーションサーバ(APS)
アプリケーション(サーバ側)＋認証カーネル
16

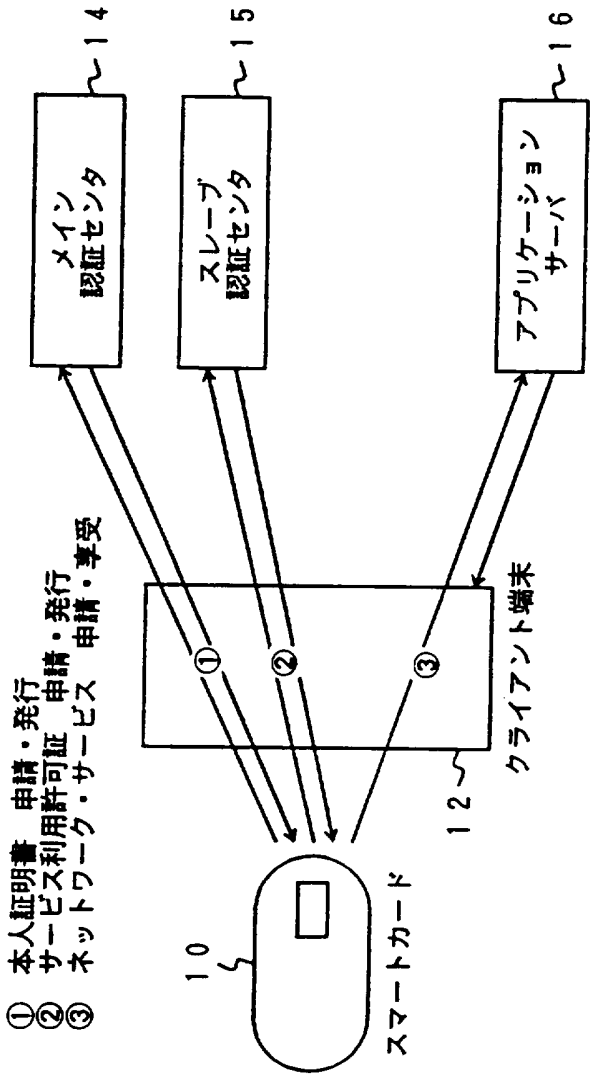

14
メイン
認証センタ
15
スレーブ
認証センタ
16
アプリケーション
サーバ
①②③ 本人証明書 申請・発行
サービス利用許可証 申請・発行
ネットワーク・サービス 申請・享受
①
②
③
12
クライアント端末
10
スマートカード

図 2

図 3

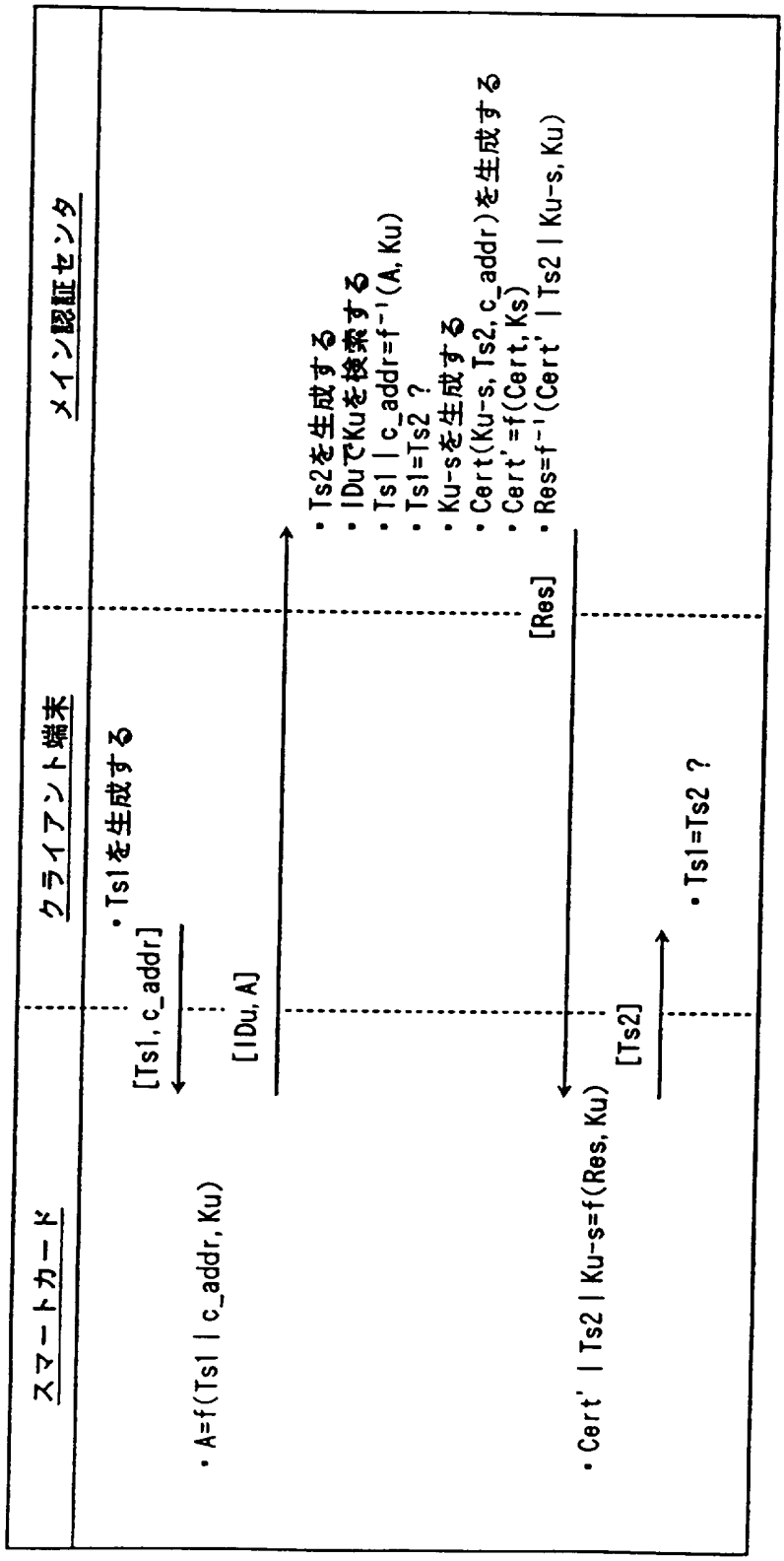

スマートカード
クライアント端末
メイン認証センタ
・Ts1を生成する
[Ts1, c_addr]
・A=f(Ts1 | c_addr, Ku)
[IDu, A]
・Ts2を生成する
・IDuでKuを検索する
・Ts1 | c_addr=f⁻¹(A, Ku)
・Ts1=Ts2 ?
・Ku-sを生成する
・Cert(Ku-s, Ts2, c_addr)を生成する
・Cert'=f(Cert, Ks)
・Res=f⁻¹(Cert' | Ts2 | Ku-s, Ku)
[Res]
・Cert' | Ts2 | Ku-s=f(Res, Ku)
[Ts2]
・Ts1=Ts2 ?

図 4

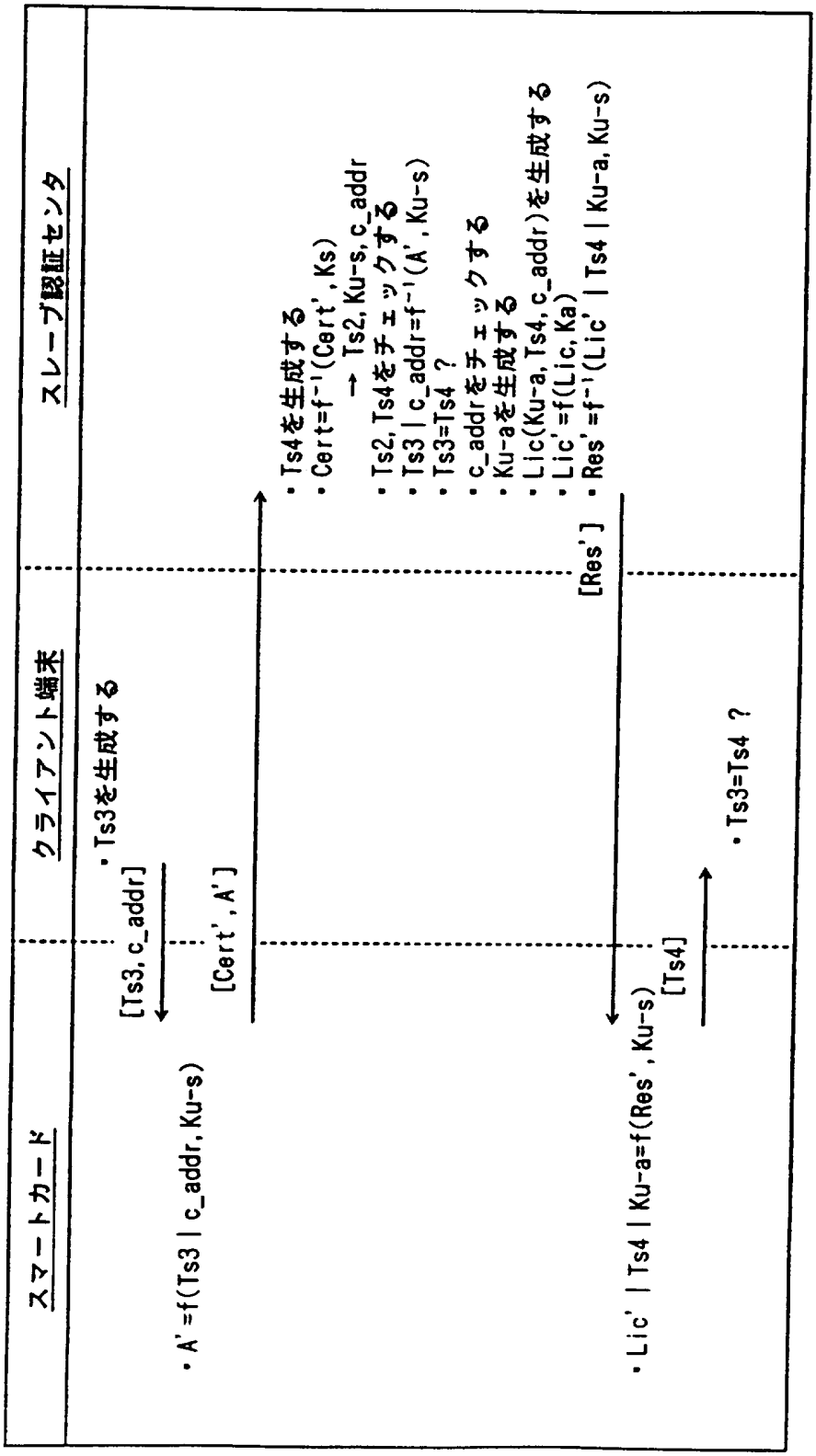
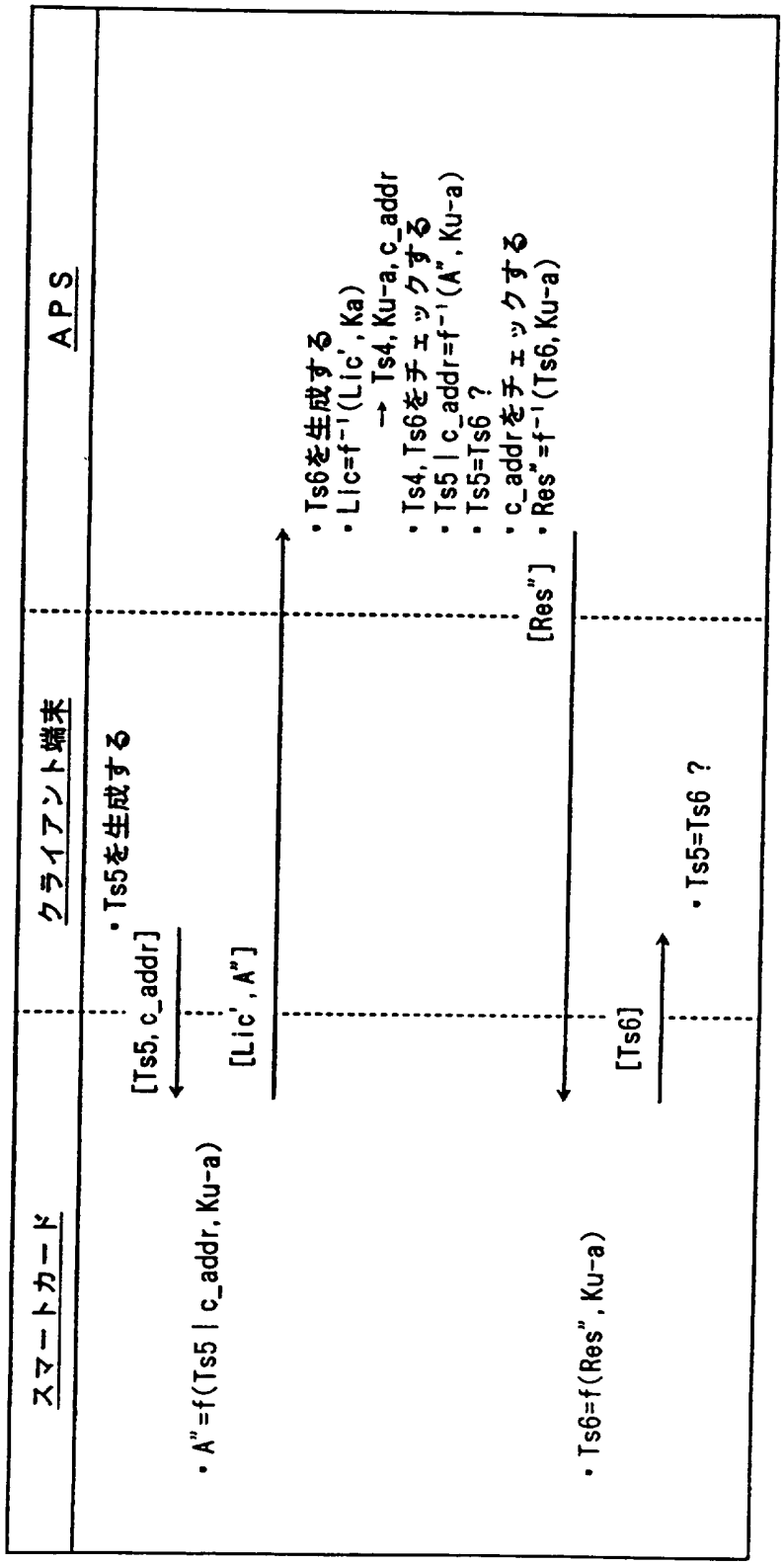

スマートカード
クライアント端末
スレーブ認証センタ
・Ts3を生成する
[Ts3, c_addr]
[Cert', A']
・A'=f(Ts3 | c_addr, Ku-s)
・Ts4を生成する
・Cert=f⁻¹(Cert', Ks)
→ Ts2, Ku-s, c_addr
・Ts2, Ts4をチェックする
・Ts3 | c_addr=f⁻¹(A', Ku-s)
・Ts3=Ts4 ?
・c_addrをチェックする
・Ku-aを生成する
・Lic(Ku-a, Ts4, c_addr)を生成する
・Lic'=f(Lic, Ka)
・Res'=f⁻¹(Lic' | Ts4 | Ku-a, Ku-s)
[Res']
・Lic' | Ts4 | Ku-a=f(Res', Ku-s)
[Ts4]
・Ts3=Ts4 ?

図 5


スマートカード
クライアント端末
APS
・Ts5を生成する
[Ts5, c_addr]
・A"=f(Ts5 | c_addr, Ku-a)
[Lic', A"]
・Ts6を生成する
・Lic=f⁻¹(Lic', Ka)
→ Ts4, Ku-a, c_addr
・Ts4, Ts6をチェックする
・Ts5 | c_addr=f⁻¹(A", Ku-a)
・Ts5=Ts6 ?
・c_addrをチェックする
・Res"=f⁻¹(Ts6, Ku-a)
[Res"]
[Ts6]
・Ts5=Ts6 ?
・Ts6=f(Res", Ku-a)

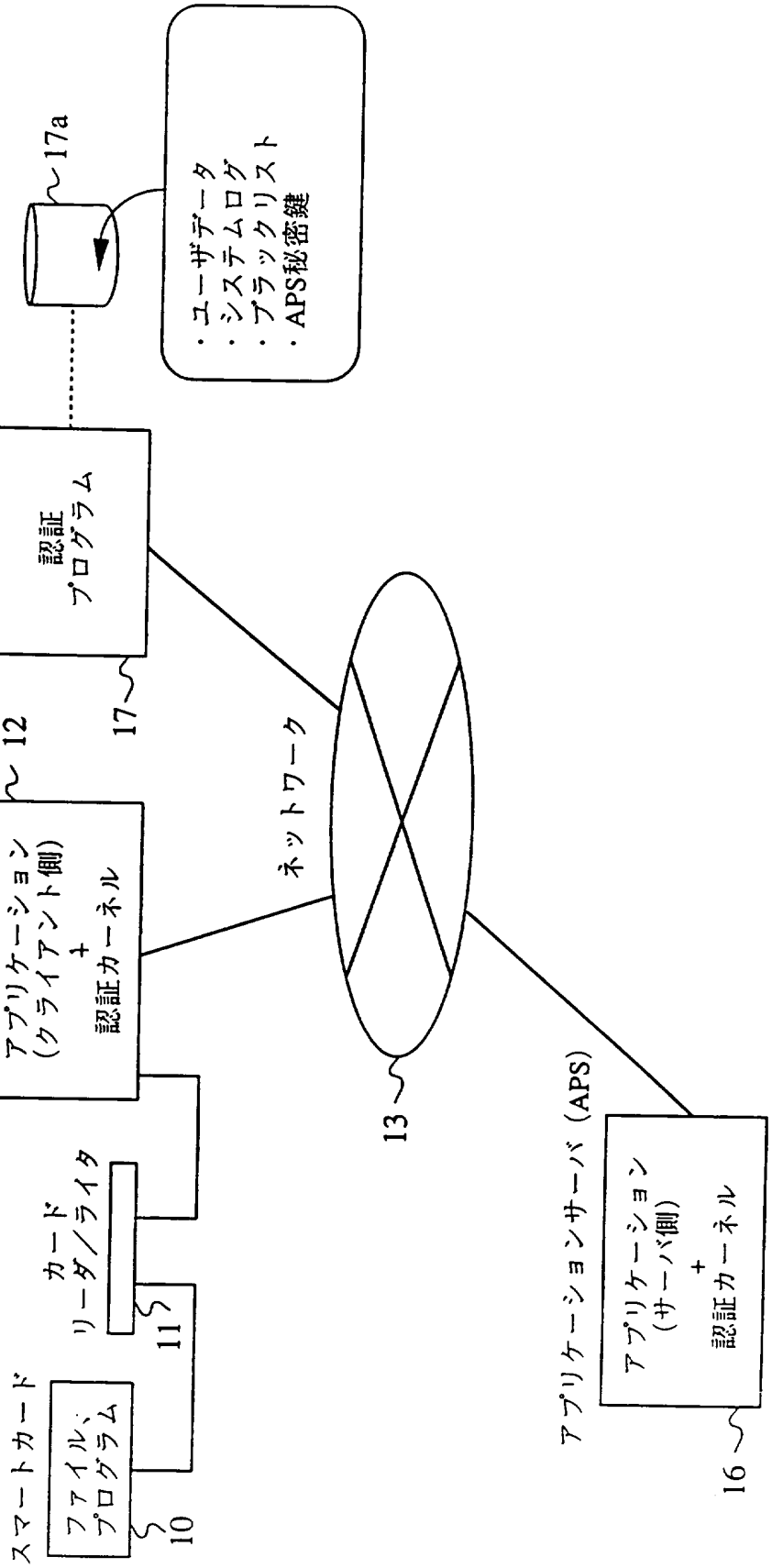

・ユーザデータ
・システムログ
・ブラックリスト
・APS秘密鍵
17a
認証センタ
認証
プログラム
17
12
クライアント端末
アプリケーション
(クライアント側)
+
認証カーネル
ネットワーク
13
カード
リーダ/ライタ
11
スマートカード
ファイル、
プログラム
10
アプリケーションサーバ（APS）
アプリケーション
(サーバ側)
+
認証カーネル
16

図 6

図 7

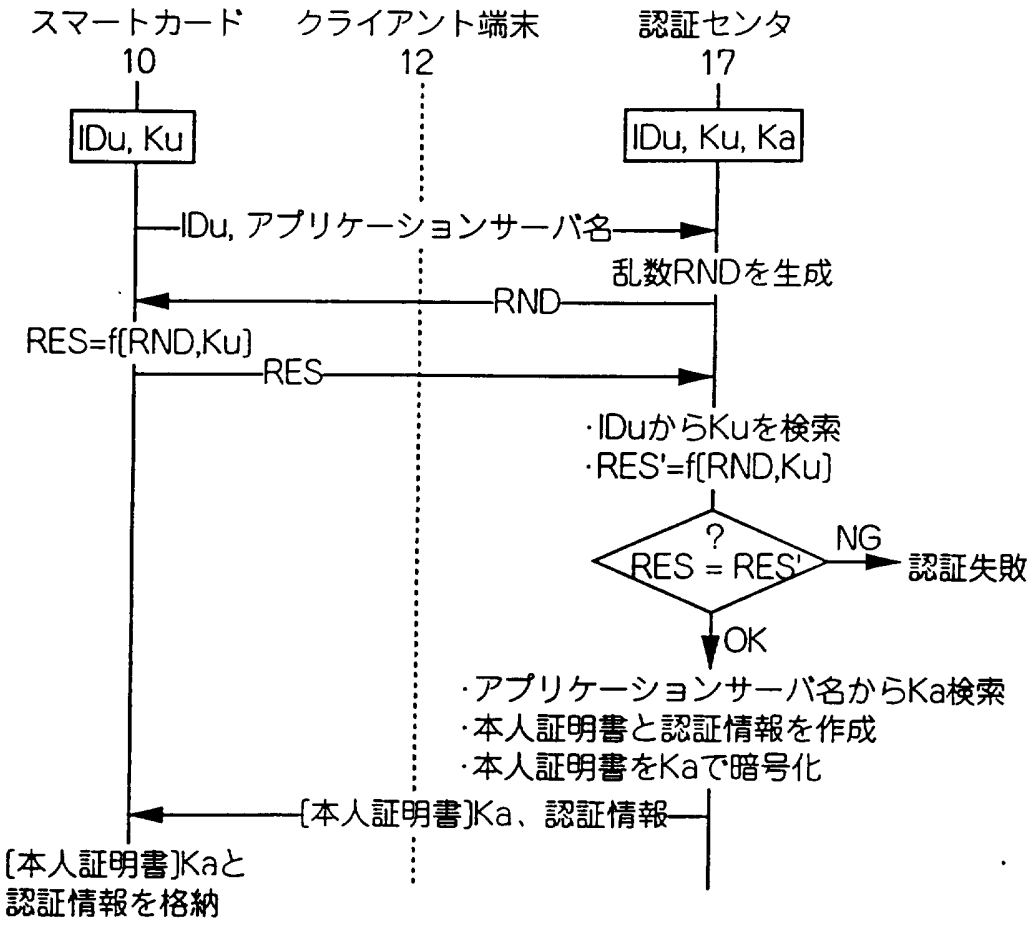

スマートカード
10
クライアント端末
12
認証センタ
17
IDu, Ku
IDu, Ku, Ka
IDu, アプリケーションサーバ名
乱数RNDを生成
RND
RES=f[RND,Ku]
RES
・IDuからKuを検索
・RES'=f[RND,Ku]
?
RES = RES'
NG
認証失敗
OK
・アプリケーションサーバ名からKa検索
・本人証明書と認証情報を作成
・本人証明書をKaで暗号化
[本人証明書]Ka、認証情報
[本人証明書]Kaと
認証情報を格納

図 8

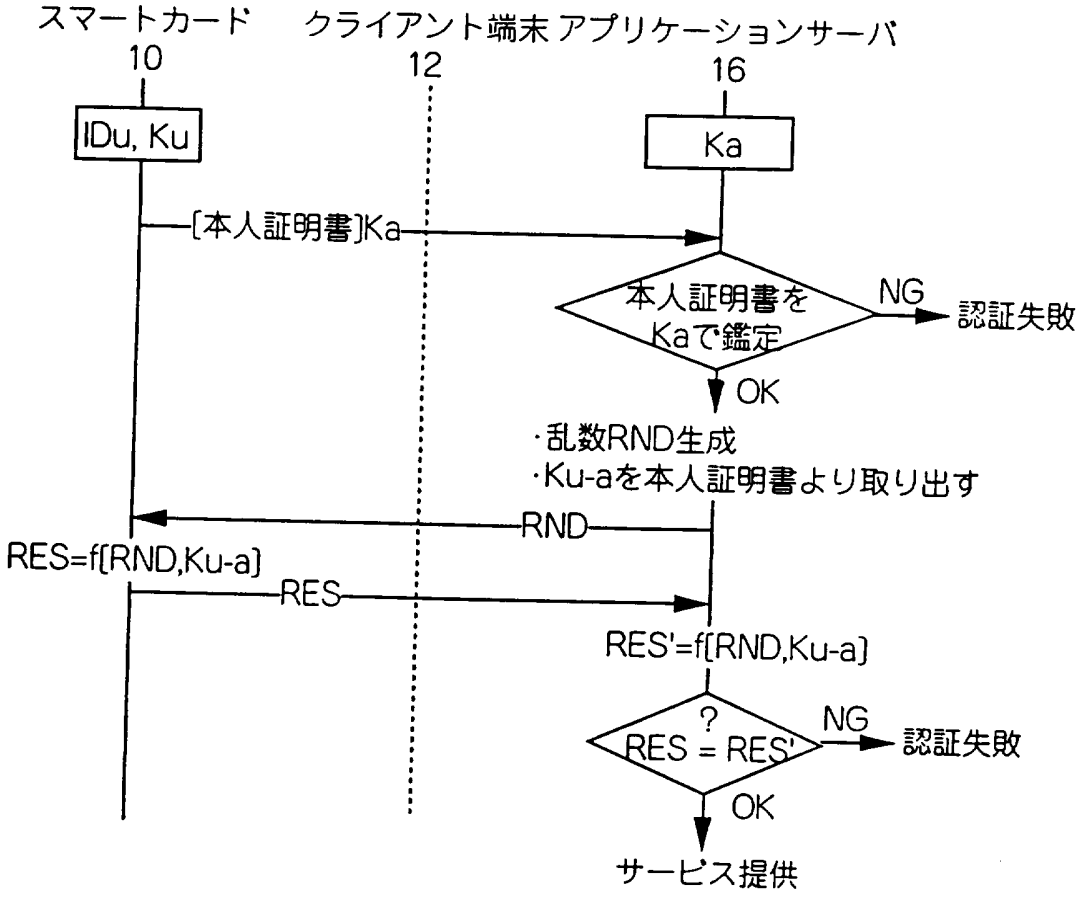

スマートカード
クライアント端末
アプリケーションサーバ
10
12
16
IDu, Ku
Ka
〔本人証明書〕Ka
本人証明書を
Kaで鑑定
NG
認証失敗
OK
・乱数RND生成
・Ku-aを本人証明書より取り出す
RND
RES=f[RND,Ku-a]
RES
RES'=f[RND,Ku-a]
?
RES = RES'
NG
認証失敗
OK
サービス提供

図 9

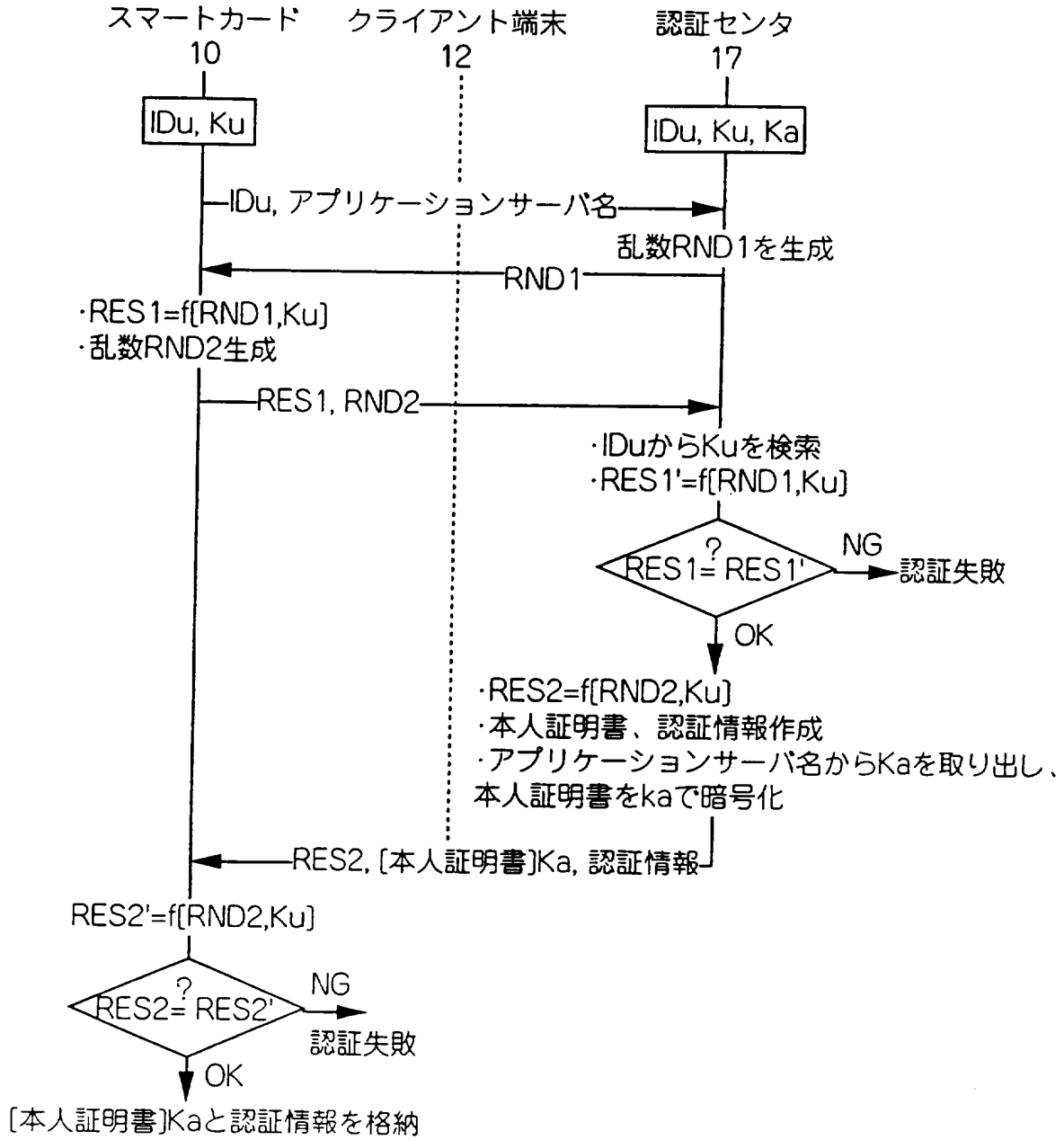

スマートカード
10
クライアント端末
12
認証センタ
17
IDu, Ku
IDu, Ku, Ka
IDu, アプリケーションサーバ名
乱数RND1を生成
RND1
·RES1=f[RND1,Ku]
·乱数RND2生成
RES1, RND2
·IDuからKuを検索
·RES1'=f[RND1,Ku]
RES1=? RES1'
NG
認証失敗
OK
·RES2=f[RND2,Ku]
·本人証明書、認証情報作成
·アプリケーションサーバ名からKaを取り出し、
本人証明書をkaで暗号化
RES2, [本人証明書]Ka, 認証情報
RES2'=f[RND2,Ku]
RES2=? RES2'
NG
認証失敗
OK
[本人証明書]Kaと認証情報を格納

図 1 0

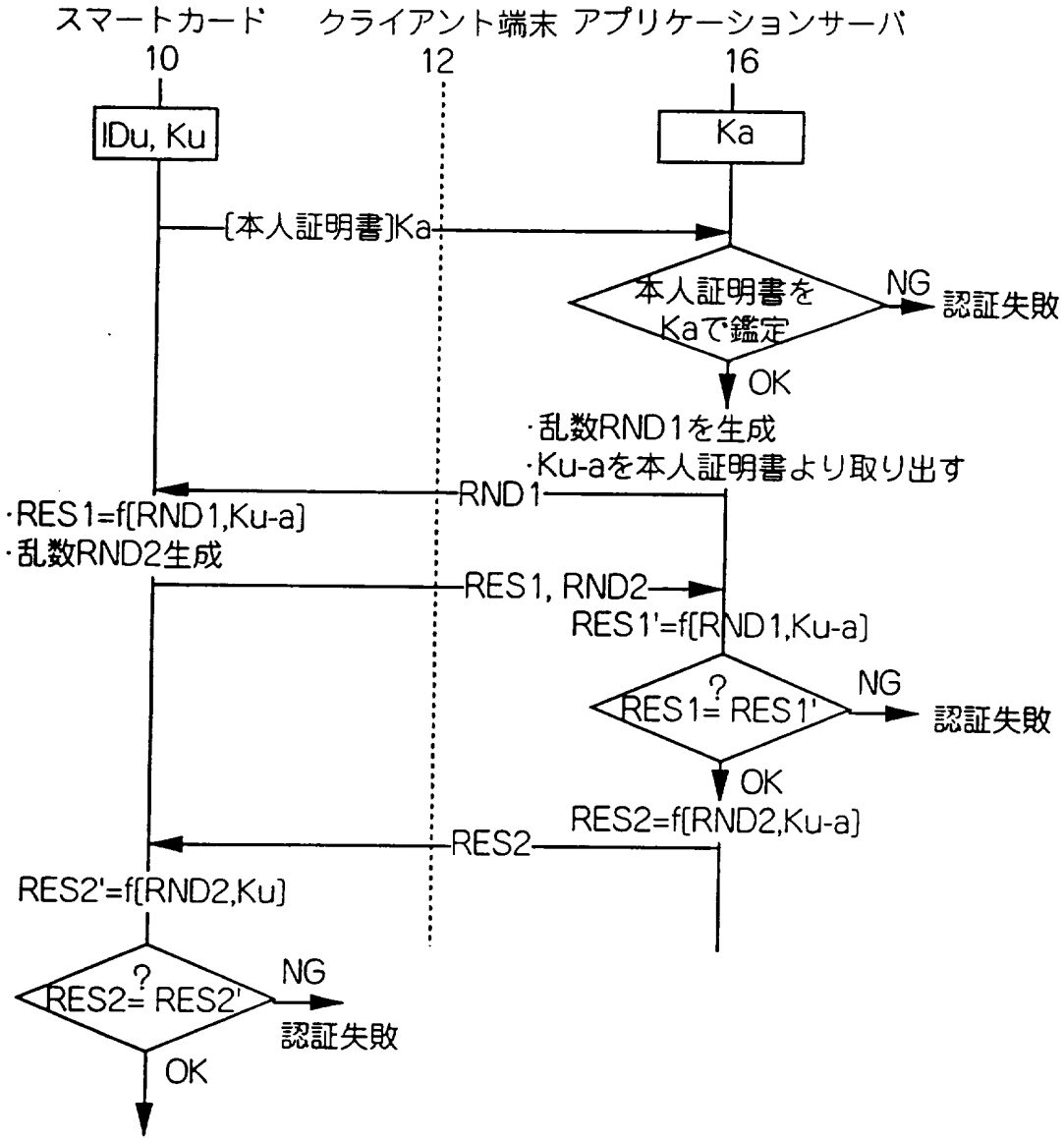
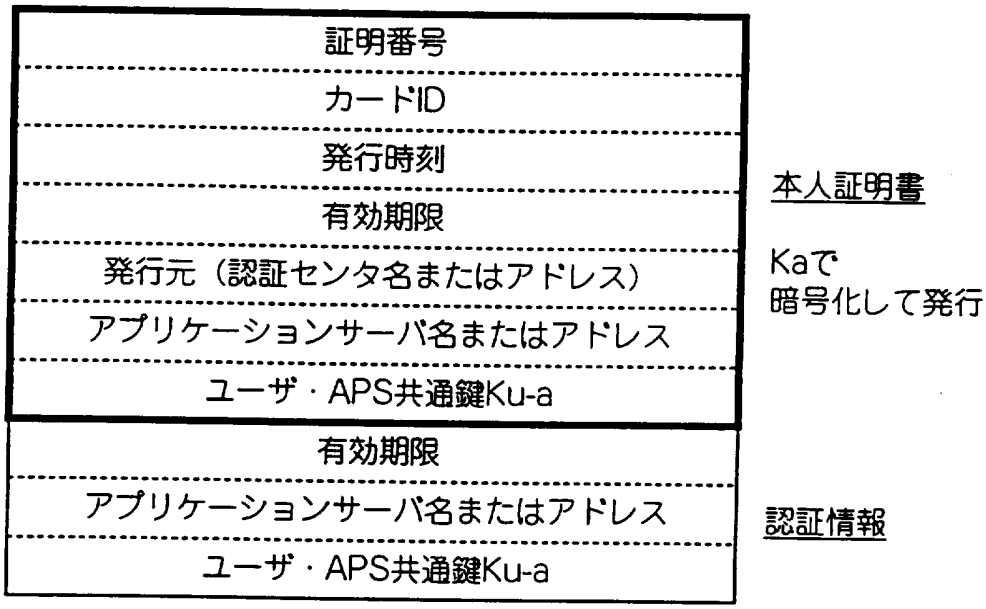

スマートカード
クライアント端末
アプリケーションサーバ
10
12
16
IDu, Ku
Ka
{本人証明書}Ka
本人証明書を
Kaで鑑定
NG
認証失敗
OK
・乱数RND1を生成
・Ku-aを本人証明書より取り出す
RND1
・RES1=f{RND1,Ku-a}
・乱数RND2生成
RES1, RND2
RES1'=f{RND1,Ku-a}
RES1=? RES1'
NG
認証失敗
OK
RES2=f{RND2,Ku-a}
RES2
RES2'=f{RND2,Ku}
RES2=? RES2'
NG
認証失敗
OK

図 1 1


証明番号
カードID
発行時刻
有効期限
発行元（認証センタ名またはアドレス）
アプリケーションサーバ名またはアドレス
ユーザ・APS共通鍵Ku-a
本人証明書
Kaで
暗号化して発行
有効期限
アプリケーションサーバ名またはアドレス
ユーザ・APS共通鍵Ku-a
認証情報

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP95/01708

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl^6 H04L9/32, G09C1/00, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl^6 H04L9/00-9/38, G09C1/00-5/00, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926 - 1995
Kokai Jitsuyo Shinan Koho 1971 - 1995

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST File on Science and Technology, WPI, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	IEICE Technical Research Report CS94-107 September 1, 1994 (01. 09. 94), IEICE, pages 105 to 110	1 - 7
X	JP, 63-294152, A (Nippon Telegraph & Telephone Corp.), November 30, 1988 (30. 11. 88)(Family: none)	1, 4
Y		2-3, 5-7
Y	IEICE Technical Research Report CS91-19 June 26, 1991 (26. 06. 91), IEICE, pages 15 to 22, particularly page 21	2, 7
Y	JP, 2-4018, B2 (Nippon Telegraph & Telephone Corp.), January 25, 1990 (25. 01. 90)(Family: none)	3, 6
Y	JP, 5-333775, A (Toshiba Corp.), December 17, 1993 (17. 12. 93), Lines 33 to 45, column 3 (Family: none)	5

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
October 31, 1995 (31. 10. 95)	November 21, 1995 (21. 11. 95)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号 PCT/JP 95/01708

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁶ H04L9/32, G09C1/00, G06F15/00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁶ H04L9/00-9/38, G09C1/00-5/00, G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1995年

日本国公開実用新案公報 1971-1995年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICST科学技術文献ファイル, WPI, INSPEC

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
P, X	電子情報通信学会技術研究報告 CS94-107 1. 9月. 1994(01. 09. 94), 社団法人 電子情報通信学会 第105-110頁	1-7
X	JP, 63-294152, A(日本電信電話株式会社), 30. 11月. 1988(30. 11. 88)(ファミリーなし)	1, 4
Y		2-3, 5-7

☑ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」先行文献ではあるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

31. 10. 95

国際調査報告の発送日

21.11.95

名称及びあて先

日本国特許庁(ISA/JP)

郵便番号100

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

松尾淳一 5J8842

電話番号 03-3581-1101 内線 3536

様式PCT/ISA/210（第2ページ）（1992年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	電子情報通信学会技術研究報告　CS91-19 26. 6月. 1991(26. 06. 91), 社団法人 電子情報通信学会　第15-22頁 特に第21頁	2，7
Y	JP, 2-4018, B2（日本電信電話株式会社）， 25. 1月. 1990(25. 01. 90)（ファミリーなし）	3，6
Y	JP, 5-333775, A（株式会社 東 芝）， 17. 12月. 1993(17. 12. 93), 第3欄，第33-45行 （ファミリーなし）	5