(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4058035号
(P4058035)

(45)発行日　平成20年3月5日(2008.3.5)　(24)登録日　平成19年12月21日(2007.12.21)

(51)Int.Cl.		F I		
H04L 9/10	(2006.01)	H04L	9/00	621A
G06F 21/24	(2006.01)	G06F	12/14	520D
G06K 17/00	(2006.01)	G06F	12/14	520F
H04L 9/32	(2006.01)	G06F	12/14	540B
		G06K	17/00	B

請求項の数 6　(全 17 頁)　最終頁に続く

(21)出願番号　特願2004-335046 (P2004-335046)
(22)出願日　平成16年11月18日 (2004.11.18)
(65)公開番号　特開2006-148492 (P2006-148492A)
(43)公開日　平成18年6月8日 (2006.6.8)
審査請求日　平成17年3月18日 (2005.3.18)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(73)特許権者　301063496
東芝ソリューション株式会社
東京都港区芝浦一丁目１番１号
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100100712
弁理士　岩▲崎▼　幸邦
(74)代理人　100100929
弁理士　川又　澄雄
(74)代理人　100108707
弁理士　中村　友之

最終頁に続く

(54)【発明の名称】公開鍵基盤システム及び公開鍵基盤方法

(57)【特許請求の範囲】
【請求項１】
公開鍵暗号方式に使用するための携帯装置を発行する発行機関装置と、前記発行機関装置により発行される携帯装置と、前記携帯装置に対して任意の内容を入力可能なユーザ端末とからなる公開鍵基盤システムであって、前記発行機関装置は、
公開鍵暗号方式用の第１暗号化／復号化部、共通鍵暗号方式用の第２暗号化／復号化部及びこの第２暗号化／復号化部にて使用される共通鍵を備えた前記携帯装置の発行を行う装置発行処理部と、
前記装置発行処理部により発行された前記携帯装置に関し、前記第１暗号化／復号化部にて使用される利用者の秘密鍵が前記共通鍵により暗号化されてなる暗号化秘密鍵、及び前記利用者の秘密鍵に対応する公開鍵の公開鍵証明書を前記ユーザ端末に向けて送信する鍵送信処理部と、
前記利用者の本人確認情報、および前記携帯装置の固有情報と前記携帯装置の利用者情報を対応させる対応情報を少なくとも格納する記憶装置と、
前記ユーザ端末より前記固有情報、前記利用者情報及び利用者の本人確認情報を含む臨時利用申請を受信し、受信した利用者情報と本人確認情報が前記記憶装置に格納される前記利用者情報と前記本人確認情報と一致する場合に、受信した固有情報及び受信した利用者情報を有効期限を付けて対応させた臨時対応情報を前記記憶装置に一時保存する臨時利用申請受付処理部
とを備え、

前記装置発行処理部は、前記記憶装置内に、前記携帯装置の固有情報と前記利用者情報の前記対応情報が存在する場合に携帯装置を発行し、前記記憶装置内に前記携帯装置の固有情報は存在するが前記対応情報が存在しない場合に前記携帯装置であって前記利用者情報が未確定のままである未確定携帯装置を発行し、

前記鍵送信処理部は、前記ユーザ端末より受信した前記携帯装置の前記固有情報に対応する前記対応情報が前記記憶装置に存在する、又は前記ユーザ端末より受信した前記未確定携帯装置の前記固有情報に対応する前記臨時対応情報が前記記憶装置に存在し且つ前記臨時対応情報の前記有効期限が切れていない場合には、前記携帯装置又は前記未確定携帯装置に格納するための前記暗号化秘密鍵及び前記公開鍵証明書を前記ユーザ端末に送信する

ことを特徴とする公開鍵基盤システム。

【請求項２】

前記携帯装置は、少なくとも１組の前記暗号化秘密鍵及び前記公開鍵証明書を格納し、

前記ユーザ端末は、前記未確定携帯装置に格納される前記暗号化秘密鍵及び前記公開鍵証明書を削除する削除司令部を備え、

前記削除司令部は、前記ユーザ端末からの指示、若しくは前記臨時発行申請時に前記ユーザ端末若しくは前記未確定携帯装置の少なくとも片方に設定される未確定携帯装置削除条件によって起動され、前記未確定携帯装置内の前記暗号化秘密鍵及び前記公開鍵証明書を削除する

ことを特徴とする請求項１に記載の公開鍵基盤システム。

【請求項３】

前記未確定携帯装置は、

前記共通鍵を格納し、

前記未確定携帯装置の前記有効期限を更新する為の更新申請を受信すると、前記未確定携帯装置内の前記共通鍵を更新する携帯装置内共通鍵更新処理部を更に備え、

前記発行機関装置は、前記更新申請を受信すると、前記記憶装置内の前記共通鍵を更新する記憶装置内共通鍵更新処理部

とを更に備えることを特徴とする請求項１に記載の公開鍵基盤システム。

【請求項４】

発行機関装置が、公開鍵暗号方式に使用するための携帯装置に対して任意の内容を入力可能なユーザ端末に対し、前記携帯装置を発行するための携帯装置発行方法であって、

前記発行機関装置は、

公開鍵暗号方式用の第１暗号化／復号化部、共通鍵暗号方式用の第２暗号化／復号化部及びこの第２暗号化／復号化部にて使用される共通鍵を備えた前記携帯装置を装置発行処理部が発行するステップと、

発行された前記携帯装置に関し、前記第１暗号化／復号化部にて使用される利用者の秘密鍵が前記共通鍵により暗号化されてなる暗号化秘密鍵、及び前記利用者の秘密鍵に対応する公開鍵の公開鍵証明書を鍵送信処理部が前記ユーザ端末に向けて送信するステップと、

少なくとも前記利用者の本人確認情報、および前記携帯装置の固有情報と前記携帯装置の利用者情報を対応させる対応情報を記憶装置に格納するステップと、

前記ユーザ端末より臨時利用申請受付処理部が前記固有情報、前記利用者情報及び利用者の本人確認情報を含む臨時利用申請を受信し、受信した利用者情報と本人確認情報が前記記憶装置に格納される前記利用者情報と前記本人確認情報と一致する場合に、受信した固有情報及び受信した利用者情報を有効期限を付けて対応させた臨時対応情報を前記記憶装置に一時保存するステップ

とを備え、

前記発行するステップは、前記記憶装置内に前記携帯装置の固有情報と前記利用者情報の前記対応情報が存在する場合に携帯装置を発行し、前記記憶装置内に前記携帯装置の固有情報は存在するが前記対応情報が存在しない場合に前記携帯装置であって前記利用者情

報が未確定のままである未確定携帯装置を発行し、
前記送信するステップは、前記ユーザ端末より受信した前記携帯装置の前記固有情報に対応する前記対応情報が前記記憶装置に存在する、又は前記ユーザ端末より受信した前記未確定携帯装置の前記固有情報に対応する前記臨時対応情報が前記記憶装置に存在し且つ前記臨時対応情報の前記有効期限が切れていない場合には、前記携帯装置又は前記未確定携帯装置に格納するための前記暗号化秘密鍵及び前記公開鍵証明書を前記ユーザ端末に送信する
ことを特徴とする公開鍵基盤方法。
【請求項５】
前記未確定携帯装置に格納される前記暗号化秘密鍵及び前記公開鍵証明書を前記ユーザ端末の削除司令部が削除するステップを備え、
前記削除するステップは、前記ユーザ端末からの指示、若しくは前記臨時発行申請時に前記ユーザ端末若しくは前記未確定携帯装置内に設定される未確定携帯装置削除条件によって起動され、前記未確定携帯装置内の全ての前記暗号化秘密鍵及び前記公開鍵証明書を削除する
ことを特徴とする請求項４に記載の公開鍵基盤方法。
【請求項６】
前記未確定携帯装置の前記有効期限を更新する為の更新申請を受信すると、前記未確定携帯装置の携帯装置内共通鍵更新処理部が前記未確定携帯装置内の前記共通鍵を更新するステップと、
前記更新申請を受信すると、前記発行機関装置の記憶装置内共通鍵更新処理部が前記記憶装置内の前記共通鍵を更新するステップ
とを更に備えることを特徴とする請求項４に記載の公開鍵基盤方法。
【発明の詳細な説明】
【技術分野】
【０００１】
公開鍵基盤システムにおいて、臨時的に使用可能な携帯通信端末装置を速やかに発行するための携帯装置臨時発行機能付きの公開鍵基盤システム及び公開鍵基盤方法に関する。
【背景技術】
【０００２】
近年、ＩＣカード（スマートカードともいう）や携帯用電子機器の進歩に伴い、ＰＩＮ（Personal Identification Number）認証やデジタル署名等を用いた身元証明又は権限証明を伴う各種システムに関し、公開鍵暗号基盤（ＰＫＩ：Public Key Infrastructure）を適用することが考えられている。
【０００３】
このような公開鍵暗号基盤を用いた秘密鍵や公開鍵証明書の更新時にはＩＣカード等の携帯装置の回収及び再配布が必要である為、更新の際に携帯装置の回収及び再配布の手間を無くす手法が公開されている（特許文献１参照。）。
【特許文献１】特開２００３－９２５６５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
公開鍵基盤においては携帯装置にユーザ固有の情報を格納する為、携帯装置の二次発行が必要な際には、セキュリティの面から、通常入退室管理のされた安全な場所において特定の作業員によって行われる。この為、発行申請してから実際にユーザの手に届くまでに、通常数日から数週間以上必要であった。
【０００５】
しかし、企業の社内システムで公開鍵基盤に基づく認証を採用し、従業員証をこの携帯装置にて実現するような場合、従業員が携帯装置を、自宅に忘れたり紛失した際に、翌日又は再発行されるまで社内システムを利用できないといった不便が生じていた。

【０００６】
本発明は、上記問題点を解決する為になされたものであり、公開鍵基盤システムにおいて、臨時的に使用可能な携帯装置を速やかに発行するための携帯装置臨時発行機能付きの公開鍵基盤システム及び公開鍵基盤方法を提供することを目的とする。
【課題を解決するための手段】
【０００７】
上記問題点を解決する為、本発明の第１の特徴は、[イ]公開鍵暗号方式に使用するための携帯装置を発行する発行機関装置（２３）と、発行機関装置により発行された携帯装置（３０）に対して任意の内容を入力可能なユーザ端末（４２）とからなる公開鍵基盤システムであって、公開鍵暗号方式用の第１暗号化／復号化、共通鍵暗号方式用の第２暗号化／復号化及びこの第２暗号化／復号化にて使用される共通鍵を備えた携帯装置の発行を行う装置発行処理部（１６ａ）と、[ロ]装置発行処理部により発行された携帯装置に関し、第１暗号化／復号化にて使用される利用者の秘密鍵が共通鍵により暗号化されてなる暗号化秘密鍵、及び利用者の秘密鍵に対応する公開鍵の公開鍵証明書をユーザ端末に向けて送信する鍵送信処理部（１６ｂ）と、[ハ]携帯装置の固有情報と携帯装置の利用者情報を対応させる対応情報を少なくとも格納する記憶装置（１４）と、[ニ]ユーザ端末より固有情報、利用者情報及び利用者の本人確認情報を含む臨時利用申請を受信し、受信した利用者情報と本人確認情報が一致する場合に、受信した固有情報及び受信した利用者情報を有効期限を付けて対応させた臨時の対応情報を記憶装置（１４）に一時保存する臨時利用申請受付処理部（６０）とを備え、[ホ]装置発行処理部（１６ａ）は、記憶装置（１４）内に携帯装置の固有情報と利用者情報の対応情報が存在する場合に携帯装置（３０）を発行し、対応情報が存在しない場合に未確定携帯装置（３０ｘ）を発行し、[ヘ]鍵送信処理部（１６ｂ）は、固有情報に対応する対応情報が記憶装置（１４）に存在しない場合、又は有効期限が切れている場合には、暗号化秘密鍵及び公開鍵証明書をユーザ端末に送信しない公開鍵基盤システムであることを要旨とする。
【０００８】
本発明の第１の特徴は、[ト]携帯装置は、少なくとも１組の暗号化秘密鍵及び秘密公開鍵証明書を格納し、ユーザ端末は、未確定携帯装置（３０ｘ）に格納される暗号化秘密鍵及び公開鍵証明書を削除する削除司令部（７０）を備え、削除司令部は、ユーザ端末からの指示、若しくは臨時発行申請時にユーザ端末若しくは未確定携帯装置の少なくとも片方に設定される未確定携帯装置削除条件によって起動され、未確定携帯装置内の暗号化秘密鍵及び秘密公開鍵証明書を削除し、[チ]未確定携帯装置は共通鍵を格納し、未確定携帯装置（３０ｘ）の有効期限を更新する為の更新申請を受信すると、未確定携帯装置内の共通鍵を更新する携帯装置内共通鍵更新処理部（８１）と、更新申請を受信すると、記憶装置（１４）内の共通鍵を更新する記憶装置内共通鍵更新処理部（８０）とを更に備えてもよい。
【０００９】
本発明の第２の特徴は、[イ]公開鍵暗号方式に使用するための携帯装置に対して任意の内容を入力可能なユーザ端末に対し、携帯装置を発行するための携帯装置発行方法であって、公開鍵暗号方式用の第１暗号化／復号化、共通鍵暗号方式用の第２暗号化／復号化及びこの第２暗号化／復号化にて使用される共通鍵を備えた携帯装置を装置発行処理部（１６ａ）が発行するステップと、[ロ]発行された携帯装置に関し、第１暗号化／復号化にて使用される利用者の秘密鍵が共通鍵により暗号化されてなる暗号化秘密鍵、及び利用者の秘密鍵に対応する公開鍵の公開鍵証明書を鍵送信処理部（１６ｂ）がユーザ端末に向けて送信するステップと、[ハ]少なくとも携帯装置の固有情報と携帯装置の利用者情報を対応させる対応情報を記憶装置（１４）に格納するステップと、[ニ]ユーザ端末より臨時利用申請受付処理部（６０）が固有情報、利用者情報及び利用者の本人確認情報を含む臨時利用申請を受信し、受信した利用者情報と本人確認情報が一致する場合に、受信した固有情報及び受信した利用者情報を有効期限を付けて対応させた臨時の対応情報を記憶装置（１４）に一時保存するステップとを備え、[ホ]発行するステップは、記憶装置（１４）内に

携帯装置の固有情報と利用者情報の対応情報が存在する場合に携帯装置（３０）を発行し、対応情報が存在しない場合に未確定携帯装置（３０ｘ）を発行し、[へ]送信するステップは、固有情報に対応する対応情報が記憶装置（１４）に存在しない場合、又は有効期限が切れている場合には、暗号化秘密鍵及び公開鍵証明書をユーザ端末に送信しない公開鍵基盤方法であることを要旨とする。

【発明の効果】

【００１０】

本発明の公開鍵基盤システム及び公開鍵基盤方法によると、所望の公開鍵基盤システムにおいて臨時的に使用可能な携帯装置を速やかに発行することができる。

【００１１】

匿名カードの臨時利用申請を行ってから、所定の有効期間内のみ使用可能な匿名カードへ秘密鍵と公開鍵証明書を書き込むことが出来る。鍵／証明書取得処理は、有効期限内ならいつでも実行できるため、匿名カードを臨時利用中に鍵が更新された場合であっても、その鍵と証明書を取得することができる。

【００１２】

また、発行機関からユーザ端末へ送信される暗号化秘密鍵は、ユーザが持っている匿名カード固有の共通鍵で暗号化されているため、もしデータを盗聴又はコピーされても、暗号を復号化しない限り、秘密鍵自体を入手したり、他のカードへ書き込んで利用したりすることが不可能になるようにすることができる。

【発明を実施するための最良の形態】

【００１３】

次に、図面を参照して、本発明の実施の形態を説明する。以下の図面の記載において、同一又は類似の部分には同一又は類似の符号を付している。ただし、図面は模式的なものであることに留意すべきである。

【００１４】

更に、以下においては、携帯装置の一例としてＩＣカードを用い、ユーザ端末としてパーソナルコンピュータを用いた場合について説明するが、これに限らず、携帯装置としてチップを用い、ユーザ端末としてこのチップを装着可能な携帯電話を用いた例等に変形しても良い。あるいは、携帯装置とユーザ端末とか携帯電話として一体的に構成された場合に変形しても良い。

【００１５】

（本発明の実施の形態）

（公開鍵基盤システム）

本発明の実施の形態における携帯装置臨時発行機能付きの公開鍵基盤システム１００は、図１に示すように、確定携帯装置であるＩＣカード３０を発行する発行機関２３と、発行機関の発行要求により証明書作成用情報及び自局の識別子等に対してデジタル署名を施すことにより公開鍵証明書Certを作成する認証局２２と、公開鍵証明書Certを基に発行機関２３より発行されるＩＣカード３０と、ＩＣカード３０を臨時利用可能に設定するユーザ端末４２とから構成される。

【００１６】

図１において、矢印に付随する文字は情報の流れを示している。なお、以下の実施の形態においては、携帯装置として法人等で使用される従業員証用のＩＣカード３０を想定しており、発行機関２３は従業員証発行部門等に設置され、ユーザ端末４２および予め余分に発行されたＩＣカード３０は各事業場（先の発行部門の事業場とは地理的に離れていても良い）に設置され、保管される。ユーザ端末４２は各事業場の入り口に設置してもよいし、各従業員（ユーザ）が業務に使用するパーソナルコンピュータであってもよい。

【００１７】

公開鍵基盤システム１００では、通常のＩＣカード３０の発行時には共通鍵Ｃｋのみが格納される。尚、その時点では既に共通鍵Ｃｋ、カードＩＤ、ユーザＩＤの対応関係が記憶装置であるシステムＤＢ１４に設定されており、実質その対応付けされたユーザＩＤの

ユーザ専用のカードとして発行される。これはいわゆるカードの二次発行（パーソナライズ）である。

【００１８】

更に公開鍵基盤システム１００は、上記の通常の二次発行のほかに、予め余分に発行されたＩＣカードのカードＩＤを、ユーザＩＤと対応付けされてない（パーソナライズされていない）状態で発行する。この状態のＩＣカードを、以下「匿名カード」と呼ぶ。未確定携帯装置である匿名カード３０ｘは各事業場で保管される。

【００１９】

匿名カード３０ｘは、従業員がＩＣカード３０を紛失した、置き忘れた等した際に、ユーザ端末４２において臨時利用の申請を行うことで、一時的にその従業員に対応付け、その従業員が臨時に使用できるＩＣカードとして利用できる。

【００２０】

（発行機関）

発行機関２３は、ＩＣカード３０の新規発行時には、秘密鍵Ｓｋ及び公開鍵証明書Certに代えて共通鍵Ｃｋが保持されたＩＣカード３０をユーザに配布する一方、共通鍵Ｃｋで復号可能に暗号化された暗号化秘密鍵Ｃｋ［Ｓｋ］及び（暗号化されていない）公開鍵証明書Certを、ネットワーク５０を介して、ユーザ端末４２に配布する。すなわち、ＩＣカード３０内で暗号化秘密鍵Ｃｋ［Ｓｋ］を復号することにより、秘密鍵Ｓｋを得る。

【００２１】

発行機関２３のシステムサーバ１０ｘは、公開鍵生成部１１、共通鍵生成部１５、システムＤＢ１４、通信処理部１６、臨時利用申請受付処理部６０及び共通鍵更新処理部８０等を備えている。

【００２２】

共通鍵生成部１５は、ユーザＩＤ毎に共通鍵Ｃｋを生成してシステムＤＢ１４に登録する。

【００２３】

通信処理部１６は、装置発行処理部１６ａ及び鍵送信処理部１６ｂとから構成される。装置発行処理部１６ａは、認証局２２に対する通信機能、認証局２２からの公開鍵証明書CertをシステムＤＢ１４に登録する機能、ユーザＩＤ毎にシステムＤＢ１４内の共通鍵Ｃｋをカード発行機２０に送出する機能、公開鍵生成部１１により生成された秘密鍵Ｓｋをシステム ＤＢ１４内の共通鍵Ｃｋにより暗号化して暗号化秘密鍵Ｃｋ［Ｓｋ］の状態でシステムＤＢ１４に登録する機能を備えている。鍵送信処理部１６ｂは、ユーザ端末４２に対しネットワーク５０を介して、ユーザのカードＩＤを受信する機能と、システムＤＢ１４内の暗号化秘密鍵Ｃｋ［Ｓｋ］及び公開鍵証明書Certを送信する機能を備えている。

【００２４】

公開鍵生成部１１は、ユーザＩＤ毎に公開鍵Ｐｋ・秘密鍵Ｓｋのペアとしての公開鍵ペアを生成し、得られた公開鍵ペアをユーザＩＤ毎にシステムＤＢ１４に登録する。

【００２５】

システムＤＢ１４は、例えば図２に示すユーザテーブルを備え、ユーザテーブルには、ユーザＩＤ、ユーザ付帯情報および本人確認情報が登録される。さらにユーザＩＤ毎に、少なくとも一組以上の公開鍵Ｐｋ及び暗号化秘密鍵Ｃｋ［Ｓｋ］が図２のブロック１、ブロック２のように登録される。ここでは便宜上、公開鍵証明書CertとそのＩＤも登録される構成としている。又図示していないが、ユーザテーブルには暗号化復号化に使用される共通鍵も登録される。また、システムＤＢ１４は、例えば図３に示すカードテーブルを備える。カードテーブルには、適宜、カードＩＤ、カード付帯情報、ユーザＩＤ、ユーザＩＤマッピングの有効期限UT、共通鍵ＩＤ等が格納される。また、図示しないが更に、カード有効期限ＶＴ、証明書有効期限CertＶＴ、認証用ＰＩＮ及び任意のユーザ情報を記憶してもよい。なお、この種の変形は設計的事項であり、このシステムＤＢ１４の記憶内容を適宜、複数のＤＢに分散して変形するとしても、この変形例は本発明の範囲に包含されることは言うまでもない。

【００２６】
臨時利用申請受付処理部６０は、ネットワーク６２を介してユーザ端末４２からの要求を受け付け、申請の為の処理を行う機能を備える。共通鍵更新処理部８０は、臨時利用申請受付処理部６０等よりカードＩＤを受け取り、そのカードＩＤに対応するシステムＤＢ１４内の共通鍵を更新する機能を備える。
【００２７】
（ユーザ端末）
ユーザ端末４２は、通信処理部１７、カード読み込み／書込み装置（以下、「カードＲ／Ｗ」と記載）４１、臨時利用申請受付処理部部６１及び削除司令部７０等を備える。
【００２８】
カードＲ／Ｗ４１は、発行機関２３より発行されたＩＣカード３０に対して任意の内容を入力する機能及びＩＣカード３０より任意の内容を出力する機能を備える。
【００２９】
通信処理部１７は、ＩＣカード３０をカードＲ／Ｗ４１に挿入することにより、図示しないネットワークを介して任意の相手コンピュータに対し、ＩＣカード３０を用いた所定の公開鍵暗号方式を使用可能とする機能、操作者の操作に基づいて、システムサーバ１０ｘからネットワーク５０を介して受けた暗号化秘密鍵Ｃｋ［Ｓｋ］及び公開鍵証明書Certを受信する機能を備えている。
【００３０】
臨時利用申請処理部６１は、ユーザがユーザＩＤや本人確認情報を入力するインタフェースを持ち、ネットワーク６２を介して臨時利用申請受付処理部６０に対して申請処理を要求する機能を備える。尚、ユーザ端末４２として、携帯装置と一体化された携帯電話を使用する場合は、匿名携帯装置を操作して臨時利用申請を行うことができるものとする。
【００３１】
削除司令部７０は、ユーザの指示又は自動起動によって、臨時のＩＣカード３０内の全ての秘密鍵及び公開鍵証明書を削除する機能を備える。
【００３２】
（ＩＣカード）
ＩＣカード３０は、ユーザの秘密鍵及び公開鍵証明書群を格納可能なＩＣカードである。ＩＣカード３０は、接触、非接触、ハイブリッド型カードが考えられる。又ＩＣカード３０以外にも、USBトークン及び携帯電話等の携帯可能装置であれば使用可能であるものとする。ＩＣカード３０の利用形態としては、企業の従業員証、各種情報サービスの利用者認証用カード等が考えられる。
【００３３】
ＩＣカード３０は、公開鍵用暗号化／復号部３１、共通鍵用暗号化／復号部３２、メモリ３３及び共通鍵更新処理部８１等を備えている。
【００３４】
メモリ３３は、カード発行機２０に書込まれた共通鍵Ｃｋ、秘密鍵Ｓｋ及び公開鍵証明書Certを格納する。公開鍵用暗号化／復号部３１は、公開鍵ペアの暗号復号処理を行う機能を備える。
【００３５】
共通鍵用暗号化／復号部３２は、共通鍵Ｃｋの暗号復号処理を行う機能を備える。共通鍵用暗号化／復号部３２は、平文状態の秘密鍵Ｓｋの漏洩を阻止するためのものであり、ＩＣカード３０内には、使用可能な秘密鍵Ｓｋを復号により生成して記憶させ、ＩＣカード３０外には、使用不可能な暗号化秘密鍵Ｃｋ［Ｓｋ］を暗号化により生成して出力する。なお、秘密鍵Ｓｋが暗号化秘密鍵Ｃｋ［Ｓｋ］として出力される場合があるのとは異なり、共通鍵ＣｋがＩＣカード３０外に出力される場合はない。すなわち、共通鍵ＣｋとＩＣカード３０とは一体不可分な構成である。具体的には共通鍵用暗号化／復号部３２は、ユーザ端末４２からの読出制御に基づいて、メモリ内の共通鍵Ｃｋにより秘密鍵Ｓｋを暗号化し、得られた暗号化秘密鍵Ｃｋ［Ｓｋ］をユーザ端末４２に送出する機能と、ユーザ

端末４２からの書込制御に基づいて、ユーザ端末４２から入力された暗号化秘密鍵Ｃｋ［Ｓｋ］を共通鍵Ｃｋにより復号し、得られた秘密鍵Ｓｋをメモリに書込む機能とをもっている。

【００３６】

共通鍵更新処理部８１は、削除司令部７０によって起動され、匿名のＩＣカード３０内の共通鍵を更新する機能を備える。

【００３７】

尚、システムサーバ１０ｘ、ユーザ端末４２及びＩＣカード３０は、個別又は同一の記憶媒体に格納した各プログラムを各々のコンピュータに読み込ませることで実現可能となっている。これは以下の実施形態においても同様である。

【００３８】

匿名カード３０ｘは、予備の臨時使用の為に作成されるＩＣカード３０であり、使用するユーザが特定されていないこと以外は、ＩＣカード３０と同機能を備えている。

【００３９】

（公開鍵基盤システムの動作）

携帯装置臨時発行機能付きの公開鍵基盤システム１００は、以下の処理を実行する。

【００４０】

１．通常のＩＣカード発行処理
２．匿名カード発行処理
３．臨時利用申請処理
４．鍵／証明書取得処理
５．カードデータ消去処理

この順番で公開鍵基盤システム１００の動作について図面を参照して詳細に説明する。

【００４１】

尚、以下より説明される匿名カード３０ｘの臨時利用の開始及び終了の動作は、匿名カード３０ｘを利用できるかどうか、ではなく、秘密鍵Ｓｋを利用できるかどうか、に基づいていることに留意すべきである。すなわち、臨時利用の申請を行った匿名カード３０ｘでのみ特定のユーザの秘密鍵Ｓｋが利用可能となり、利用終了時に秘密鍵Ｓｋを削除した後は、その匿名カード３０ｘや、通信路上を流れたデータを使用しても任意のユーザの秘密鍵Ｓｋを利用できない。これにより、公開鍵基盤に基づく応用システムに携帯装置自体の有効性を確認させる等の特別な制約を課することなく、匿名カード３０ｘの発行を実現する。

【００４２】

（通常のＩＣカード発行処理）

図４及び図５は、公開鍵基盤システム１００が通常のＩＣカード発行処理を行う動作を示すフロー図である。

【００４３】

（ａ）まず、ステップＳ１１において、秘密鍵Ｓｋ及び公開鍵証明書Certの新規発行時に、操作者の操作により、発行機関２３のシステムサーバ１０ｘの共通鍵生成部１５が、ユーザＩＤ毎に共通鍵Ｃｋを生成する。ステップＳ１２においては、この共通鍵ＣｋをシステムＤＢ１４に登録する。

【００４４】

（ｂ）ステップＳ１３において、システムサーバ１０ｘの通信処理部１６は、ユーザＩＤ毎に、システムＤＢ内の共通鍵Ｃｋをカード発行機２０に送出する。ステップＳ１４において、カード発行機２０は、この共通鍵ＣｋをＩＣカード３０のメモリに書込むことにより、ユーザＩＤに対応するＩＣカード３０を発行する。ステップＳ１５において、このＩＣカード３０は、ユーザの住所又は居所に郵送等により配布される。ユーザは、このＩＣカード３０を受けると、発行機関２３に対して公開鍵証明書Cert及び秘密鍵Ｓｋの配布を要求する。なお、この配布要求は、Ｅメール、電話、郵便又はＦＡＸ等、任意の手法で構わない。

【００４５】
（ｃ）ステップＳ１６において、発行機関２３は、この配布要求を受けると、前述同様に、公開鍵生成部１１により公開鍵ペアを生成して通信処理部１６に送出する。通信処理部１６は、ステップＳ１７にてこの公開鍵ペアのうち、公開鍵ＰｋをユーザＩＤ毎にシステムＤＢに登録し、ステップＳ１８にて秘密鍵Ｓｋを共通鍵Ｃｋにより暗号化して暗号化秘密鍵Ｃｋ［Ｓｋ］の状態でユーザＩＤ毎にシステムＤＢ１４に登録する。
【００４６】
（ｄ）続いて図５に示すように、ステップＳ１９にて、通信処理部１６は前述同様に公開鍵証明書Certの発行要求を認証局２２に送出し、ステップＳ２０にて折り返し返信された公開鍵証明書Certを受けとる。ステップＳ２１にて、通信処理部１６はこの公開鍵証明書CertをシステムＤＢ１４に登録する。
【００４７】
（ｅ）しかる後、ステップＳ２２にて、通信処理部１６は、システムＤＢ１４内のユーザＩＤに対応する暗号化秘密鍵Ｃｋ［Ｓｋ］及び公開鍵証明書Certを読出してユーザ端末４２向けにネットワーク５０に送信する。
【００４８】
（ｆ）ステップＳ２３にて、ユーザ端末４２は、暗号化秘密鍵Ｃｋ［Ｓｋ］及び公開鍵証明書Certを受けると、ユーザの操作により、暗号化秘密鍵Ｃｋ［Ｓｋ］及び公開鍵証明書CertをＩＣカード３０に入力する。ＩＣカード３０においては、ステップＳ２４にて公開鍵証明書Certがメモリに書込まれると共に、共通鍵用暗号化／復号部３２がこの暗号化秘密鍵Ｃｋ［Ｓｋ］をメモリ内の共通鍵Ｃｋで復号し、ステップＳ２５にて得られた秘密鍵ＳｋをメモリにＳ込む。これにより、ＩＣカード３０への秘密鍵Ｓｋ及び公開鍵証明書Certの配布が完了する。
【００４９】
以下、ユーザは、このＩＣカード３０をユーザ端末４２のカードＲ／Ｗ４１に挿入することにより、ＩＣカード３０を用いた所定の公開鍵暗号方式の利用形態が、ネットワーク５０上の図示しない他のコンピュータに対して実現可能となる。尚、利用形態には、公開鍵ペア用の公開用鍵暗号化／復号部３１によるデジタル署名／署名認証、暗号化／復号等がある。
【００５０】
（匿名カード発行処理）
匿名カード発行処理は、上述した通常のカード発行処理と比較して、カードＩＤに対してユーザＩＤがまだ割り当てられていないという点、匿名カード３０ｘがユーザに配布されるのではなく事業場等にストックされる点が異なる。
【００５１】
（ａ）先ずステップＳ３１において、ステップＳ２１と同様に共通鍵Ｃｋを作成する。ステップＳ３２において、ステップＳ２２と同様に共通鍵Ｃｋを用いてカードエントリを作成し、登録処理を行う。この際、図２のユーザテーブルのユーザＩＤは登録せず、空の状態のままにしておく。ステップＳ３３において、ステップＳ２３と同様に共通鍵Ｃｋをカード発行機２０に送出する。
【００５２】
（ｂ）ステップＳ３４においては、ステップＳ２４と同様に、共通鍵Ｃｋを含み、ユーザＩＤが確定していない匿名のＩＣカードである匿名カード３０ｘを発行する。ステップＳ３５において、発行された匿名カード３０ｘは、ユーザに配布されずに、予備のＩＣカードとして事業所等へストックされる。
【００５３】
上記の処理で発行された匿名カード３０ｘは、まだ誰のものとも確定しておらず、どのユーザの鍵も格納することができない。これは、通信処理部１６に、指定されたカードＩＤに対応するユーザは存在しないと判断させ、暗号化秘密鍵Ｃｋ［Ｓｋ］及び公開鍵証明書Certを返させないことによって実現される。よって、この状態では、例え匿名カード３

０ｘが悪意の第三者の手に渡っても、どのユーザの秘密鍵も使用することはできないため、一定のレベルの安全性を保つことができる。

【００５４】

（臨時利用申請処理）

次に、ユーザが所有するＩＣカード３０を忘れた、紛失した等の理由により、臨時的に匿名カード３０ｘを使用するために申請を行う処理について図７のフロー図を用いて説明する。

【００５５】

（ａ）先ずステップＳ４１において、ユーザが匿名カード３０ｘを各事業場の管理者等から受け取り、ユーザ端末４２へ挿入する。ステップＳ４２において、ユーザは臨時利用申請処理部６１を起動し、ユーザＩＤと本人確認情報を入力する。本人確認情報としては、暗証番号等が好ましいが、他に、ユーザ端末４２が各ユーザのパーソナルコンピュータの場合、あらかじめ設定しておいた認証用鍵等でも構わない。又、認証用鍵は暗黙にファイル等から読み込まれても良い。

【００５６】

（ｂ）ステップＳ４３において、臨時利用申請処理部６１が匿名カード３０ｘからカードＩＣを読み取り、ステップＳ４４において、ユーザＩＤ及び本人確認情報と共に発行機関２３の臨時利用申請受付処理部６０へ送信する。ここで本人確認情報が認証用鍵の場合は、直接送信するのではなく、臨時利用申請受付処理部６０との間でチャレンジレスポンス認証を行っても良い。

【００５７】

（ｃ）ステップＳ４５においては、臨時利用申請受付処理部６０が受け取った情報から本人確認情報の確認とユーザＩＤとカードＩＤのマッピングの許可判定を行う。一例として、ユーザＩＤとカードＩＤのマッピング判定としては、まずカードＩＤの１文字目が１であることを確認し、続いてカードＩＤを事業場コードが一致しているかどうかを行う。この判定により、誤って匿名カード３０ｘを本来とは別のユーザにマッピングしてしまうことを防き、本人確認情報が漏洩しても特定のカード（例えば所属事業場にストックされたカード）以外は匿名カード３０ｘとして使用させないことが出来る。

【００５８】

匿名カード３０ｘをユーザにマッピングするための本人確認の手法としては、通常使用される暗証番号認証及び生体認証の他にも、公開鍵基盤では複数のＩＣカードや鍵を使い分けている場合があるため、それらを本人確認情報として使用できる。具体的には、最も最近そのユーザに発行されたＩＣカード３０の初期ＰＩＮ、そのユーザの他のＩＣカード３０に格納された秘密鍵を用いたチャレンジレスポンス認証、ユーザ端末４２に設定されたそのユーザの認証用共通鍵または秘密鍵を用いたチャレンジレスポンス認証、申請に応じてユーザに暗号化または平文の電子メールで送信された暗証番号の照合、予め発行装置システムに登録された代理人の暗証番号または指紋等の生体情報の照合、予め発行装置システムに登録された代理人のＩＣカードに格納された秘密鍵を用いたチャレンジレスポンス認証、または以上の組合せによる判定等が挙げられる。

【００５９】

また、法人の従業員証用にＩＣカード３０を使用するのであれば、カード管理者が存在することが想定されるため、そのカード管理者を本人の代理人として認証してもよい。この手法は、ユーザが暗証番号を忘れたり、他の代替手段を利用できない場合に有用となる。

【００６０】

確認及び判定が共に適正であった場合、ステップＳ４６において、臨時利用申請受付処理部６０はカードＩＤに対応するカードエントリにユーザＩＤと規定の方法で算出されたマッピング有効期限を書き込んで終了する。一方、確認及び判定のうち少なくとも片方が適正でなかった場合、この処理を終了する。処理を終了するとき、成否を臨時利用申請処理部６１へ送信し、ユーザ端末４２で画面表示してもよい。

【００６１】
ここでマッピング有効期限は、例えば申請受付日の23時59分までとしてもよいし、他には例えば、ユーザの申請日と規定の有効期間日数から算出される日の小さい方を使用してもよい。マッピング有効期限は後述する鍵／証明書取得処理で利用され、設定された期限以降、その匿名カードを使用して鍵／証明書を取得することができないよう制御される。
【００６２】
（鍵／証明書取得処理）
次に、鍵／証明書の取得処理について、図８のフロー図を参照して説明する。
【００６３】
（ａ）ステップＳ５１においては、まずユーザが匿名カード３０ｘをユーザ端末４２に挿入し、ステップＳ５２にて通信処理部１７を起動する。続いて、ステップＳ５３において、通信処理部１７が匿名カード３０ｘからカードＩＤを読み取る。尚、これらの処理は臨時利用申請処理と一体化して省略する構成も可能で、その場合、通信処理部１７は臨時利用申請処理部６１から自動的に起動され、カードＩＤは起動パラメータとして渡すという構成にする。ステップＳ５４にて通信処理部１７はカードＩＤを発行機関２３の通信処理部１６へ送信する。
【００６４】
（ｂ）ステップＳ５５において、通信処理部１６の鍵送信処理部１６ｂは受信したカードＩＤからシステムＤＢ１４のカードテーブルを検索し、ユーザＩＤがマッピングされているかどうかをチェックする。マッピングされていない場合は、鍵／証明書取得ができないものとして処理を終了し、マッピングされている場合は、続いてステップＳ５６にて、マッピング有効期限をチェックする。有効期限チェックでは、例えばサーバマシンの時刻や、または時刻サーバからの情報を元に、要求受付時刻が有効期間内かどうかをチェックする。
【００６５】
（ｃ）チェックの結果、有効期間外と判定されたならば、マッピング解除処理を行う。具体的には、まずステップＳ６２にて、マッピングされているユーザＩＤを削除し、続いてステップ６３にて、共通鍵更新処理部８０へカードＩＤを送信する。ステップＳ６４にて、共通鍵更新処理部８０は、そのカードＩＤに対応する共通鍵Ckを規定のルールによって更新する。ここで、共通鍵の更新方式は、ＩＣカード３０に内蔵している共通鍵更新処理部８１と同じの共通鍵を出力するものでなければならない。例えば、元の共通鍵と、カードＩＤを連結したものをＳＨＡ－１方式でハッシュした結果を使用する等が考えられる。また、共通鍵の更新は実施しない、という構成も考えられる。この場合、ＩＣカード３０に共通鍵更新処理部８１を実装する必要がなくなり、同じ仕様のＩＣカード及び匿名カードを使用してシステムを構築することができるメリットある。しかしこの場合、第三者が一度使用された匿名カードとそこへ送信された暗号化秘密鍵Ｃｋ［Ｓｋ］のペアを入手することで、その匿名カードへその暗号化秘密鍵Ｃｋ［Ｓｋ］を書き込んで秘密鍵を利用することを阻止する構造が必要となる。
【００６６】
（ｄ）一方、マッピング有効期間チェックにより有効期間内と判定されたならば、ステップＳ５７において、通信処理部１６がユーザＩＤに対応する全ての秘密鍵を、指定されたカードＩＤに対応する共通鍵で暗号化して、暗号化秘密鍵Ｃｋ［Ｓｋ］を作成する。暗号化秘密鍵Ｃｋ［Ｓｋ］作成後は、図５のステップＳ２２～２５と同様に、ステップＳ５８～Ｓ６１において匿名カード３０ｘへ秘密鍵Ｓｋと公開鍵証明書Certを書き込む。
【００６７】
以上の処理によって、匿名カードの臨時利用申請を行ってから、所定の有効期間内のみ、その匿名カードへ秘密鍵Ｓｋと公開鍵証明書Certを書き込むことが出来る。上記の鍵／証明書取得処理は、有効期限内ならいつでも実行できるため、匿名カードを臨時利用中に鍵が更新された場合であっても、その鍵と証明書を取得することができる。また、発行機関２３の鍵送信処理部１６ｂからユーザ端末４２の通信処理部１７へ送信される暗号化秘

密鍵Ｃｋ[Ｓｋ]は、ユーザが持っている匿名カード固有の共通鍵で暗号化されているため、もしデータを盗聴又はコピーされても、暗号を復号化しない限り、秘密鍵自体を入手したり、他のカードへ書き込んで利用したりすることができない。

【００６８】

なお、上記の手順で作成した匿名カード３０ｘを利用するためのＰＩＮについては、予め規定値を設定してそれをユーザが変更して使用する場合や、通信処理部１６で新規に作成し、通信処理部１７を経由してＩＣカードに書き込むと共に画面に初期ＰＩＮとして表示する方法などが考えられる。

【００６９】

（カードデータ消去処理）

次に、カードデータ消去の処理について図９のフロー図を参照して説明する。（ａ）先ずステップＳ７１において、臨時の匿名カード３０ｘの利用を終了する際に、ユーザは匿名カード３０ｘをユーザ端末４２に挿入する。ステップＳ７２において、ユーザが削除司令部７０を起動し、匿名カード３０ｘのＰＩＮを入力する。ステップＳ７３では、ユーザ端末４２の削除司令部７０は、ＰＩＮを挿入されているＩＣカード（匿名カード）３０ｘへ送信し、匿名カード３０ｘはそのＰＩＮを照合する。（ｂ）ステップＳ７４にて、削除司令部７０は、ＩＣカード３０へ臨時利用のクリア指示を送信する。するとステップＳ７５にて、ＩＣカード３０はまず自身のカードＩＤの１文字目が１か否かをチェックする。カードＩＤの１文字目が１でない場合、匿名カードではないため、この処理を終了する。

【００７０】

（ｃ）カードＩＤの１文字目が１であった場合、匿名カードと判定してステップＳ７６へ進み、カードに格納されている全ての秘密鍵Ｓｋと公開鍵証明書Ｃｅｒｔを削除する。更にステップＳ７７にて、共通鍵更新処理部８１が共通鍵Ｃｋを更新する。この際、共通鍵更新処理部８１は前述したように発行機関の共通鍵更新処理部８０と同じ共通鍵を出力する必要がある。

【００７１】

カードデータ消去処理では、ユーザの指示があって、はじめて匿名カード３０ｘの内容をクリアする。これはＩＣカード３０自体が時計機能を持っておらず、また受動的に動作するためである。なお、ユーザの指示ではなく、ユーザ端末４２でＩＣカード３０を利用する際に、ユーザ端末４２側の処理によってクリアすべきかを判断し、必要に応じて削除する方法も考えられる。例えば、発行機関２３と通信して有効期限切れを確認したり、臨時利用申請処理時にＩＣカード３０へ有効期限を書き込んで、それをチェックしたりする方法が考えられる。

【００７２】

また、携帯装置がＩＣカード３０ではなく、時計機能の内蔵したようなものであれば、その携帯装置内の機能によって自装置内で削除してもよい。

【００７３】

上記のカードデータ消去処理によって、内容がクリアされた匿名カード３０ｘは、共通鍵Ｃｋが変更されて再度暗号化秘密鍵Ｃｋ[ＳＫ]を入力しても復号することができない為、どのユーザの秘密鍵も再設定することができないカードとなる。よって、暗号化秘密鍵を盗聴する又は過去に使用された匿名カード３０ｘを入手して解析することにより悪意の第三者が不正利用することを防ぐことができる。尚、匿名カード３０ｘは、再度臨時利用申請を行うことによって更新することができる。

【００７４】

臨時利用の更新に際しては、利用者が、図１のユーザ端末４２のカードＲ／Ｗ４１に匿名カード３０ｘを挿入し、ユーザ端末４２上で更新の申請を行うと、図１の匿名カード３０ｘの共通鍵更新処理部８１が共通鍵を更新する。同時に、発行機関２３の臨時使用申請受付処理部６０を介して、匿名カード３０ｘの有効期限等を更新する為の更新申請を共通鍵更新処理部８０が受信し、システムＤＢ１４内の共通鍵を更新する。

【００７５】

尚、更新処理は、発行機関２３の鍵送信処理部１６ｂにおいて、匿名カード３０ｘのユーザＩＤのマッピングの有効期限が切れたと最初に判定されたときのみに１度だけ起動させてもよい。これによると定常的に更新管理を実行する必要が無い為、更新タイミングを適切に且つ簡易に実現することができる。

【００７６】

又、共通鍵を更新するには、現在格納されている共通鍵とカードＩＤを含む情報を入力し、一方向性ハッシュ関数によって変換された値を基に新しい共通鍵を生成してもよい。これにより共通鍵を簡易に作成する事ができる。

【００７７】

（変更例）

臨時の匿名カード発行申請は、通常ＩＣカード３０を紛失／破損したか、家に忘れてきた等の際に実行される。ここでＩＣカード３０を紛失／破損したことが明らかな場合は再発行申請が必要となる。よって、ユーザ端末４２が発行機関２３に匿名カードの発行を申請する際に、公開鍵証明書Certの失効とその匿名カードの期限切れ後に利用可能となる通常のカード３０の再発行受付を同時に受け付け可能とすることが好ましい。その際、受付時に申請するユーザに対応する現在有効な公開鍵証明書Certを失効して新しい秘密鍵Ｓｋと公開鍵証明書Certを発行し、さらに後日通常のカードが再発行されるよう発行機関２３に登録し、更に、マッピングの有効期限が再発行時用に設定された条件によって決定されるようにする。これにより匿名カード発行申請時に通常のカードの再発行申請も行うことができ、匿名カードの有効期限切れ後、スムースに通常のカードへ移行できるようになる。

【００７８】

受付時に公開鍵証明書Certの失効が即座に行われることにより、利用者が紛失したＩＣカード３０に含まれる秘密鍵Ｓｋの利用を禁止することができる。

【００７９】

即座に新しい公開鍵証明書Certが発行されるため、その後に実行される秘密鍵Ｓｋ及び公開鍵証明書CertのＩＣカード３０ｘへの書き込みにより、最新の公開鍵証明書Certを即座に入手することができる。

【図面の簡単な説明】

【００８０】

【図１】本発明の実施の形態に係る公開鍵基盤システムの構造を示す構造図である。

【図２】システムＤＢのユーザテーブルのデータ構造を示す図である。

【図３】システムＤＢのカードテーブルのデータ構造を示す図である。

【図４】公開鍵基盤システムによる通常のカード発行処理動作を示すフローチャートである。

【図５】公開鍵基盤システムによる通常のカード発行処理動作を示すフローチャートである。

【図６】公開鍵基盤システムによる匿名カード発行処理動作を示すフローチャートである。

【図７】公開鍵基盤システムによる臨時利用申請処理動作を示すフローチャートである。

【図８】公開鍵基盤システムによる鍵／証明書取得処理動作を示すフローチャートである。

【図９】公開鍵基盤システムによるカードデータ消去処理動作を示すフローチャートである。

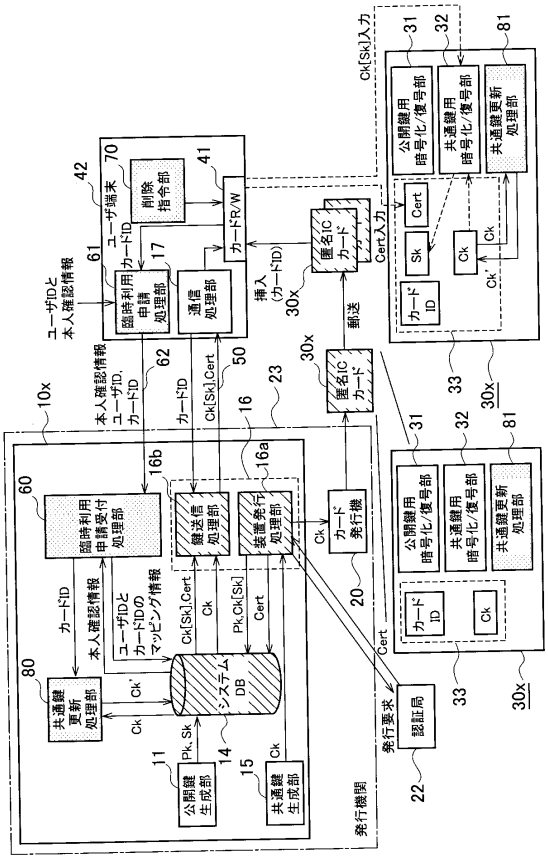
【符号の説明】

【００８１】

１０ｘ…システムサーバ
１１…公開鍵生成部
１４…システムＤＢ
１５…共通鍵生成部

１６…通信処理部
１６ａ…装置発行処理部
１６ｂ…鍵送信処理部
１７…通信処理部
２０…カード発行機
２２…認証局
２３…発行機関
３０x…匿名カード
３０…ＩＣカード
３１…公開鍵用暗号化／復号部
３２…共通鍵用暗号化／復号部
３３…メモリ
４１…カードＲ／Ｗ
４２…ユーザ端末
５０…ネットワーク
６０…臨時利用申請受付処理部
６１…臨時利用申請処理部
６２…ネットワーク
７０…削除司令部
８０…共通鍵更新処理部
８１…共通鍵更新処理部
１００…公開鍵基盤システム

【図１】



【図２】

ユーザID
ユーザ付帯情報（事業場コード）
本人確認情報（暗証番号）
公開鍵証明書ID（1）
公開鍵証明書Cert1
公開鍵ID（1）
公開鍵Pk1
秘密鍵ID（1）
秘密鍵Sk1
公開鍵証明書ID（2）
公開鍵証明書Cert2
公開鍵ID（2）
公開鍵Pk2
秘密鍵ID（2）
秘密鍵Sk2

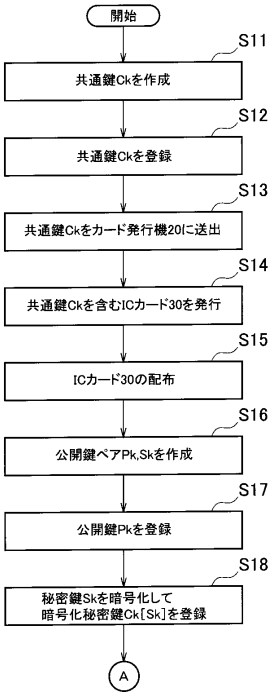
1

2

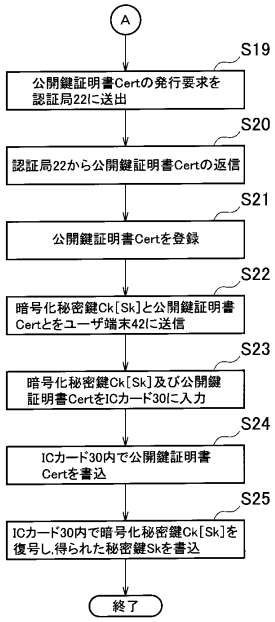
【図３】

カードID（1文字目が0なら通常カード、1なら匿名カードを表すものとする）
カード付帯情報（事業場コード）
ユーザID（空の場合有り）
ユーザIDマッピングの有効期限UT
共通鍵ID
共通鍵Ck1

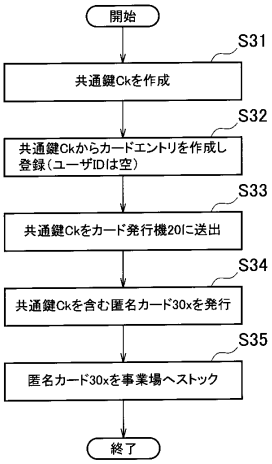
【図４】


開始
S11
共通鍵Ckを作成
S12
共通鍵Ckを登録
S13
共通鍵Ckをカード発行機20に送出
S14
共通鍵Ckを含むICカード30を発行
S15
ICカード30の配布
S16
公開鍵ペアPk,Skを作成
S17
公開鍵Pkを登録
S18
秘密鍵Skを暗号化して
暗号化秘密鍵Ck[Sk]を登録
A

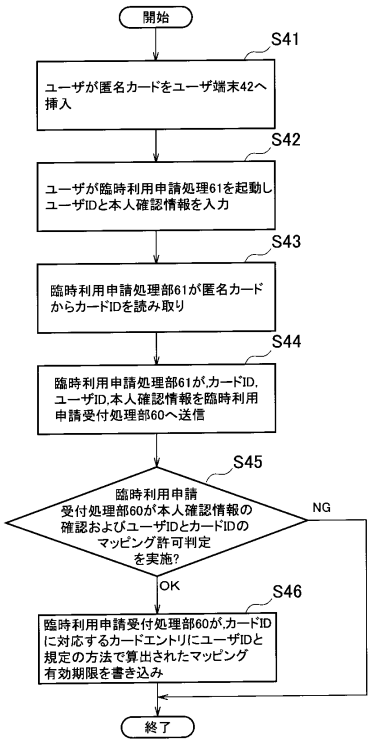
【図５】


A
S19
公開鍵証明書Certの発行要求を
認証局22に送出
S20
認証局22から公開鍵証明書Certの返信
S21
公開鍵証明書Certを登録
S22
暗号化秘密鍵Ck[Sk]と公開鍵証明書
Certとをユーザ端末42に送信
S23
暗号化秘密鍵Ck[Sk]及び公開鍵
証明書CertをICカード30に入力
S24
ICカード30内で公開鍵証明書
Certを書込
S25
ICカード30内で暗号化秘密鍵Ck[Sk]を
復号し,得られた秘密鍵Skを書込
終了

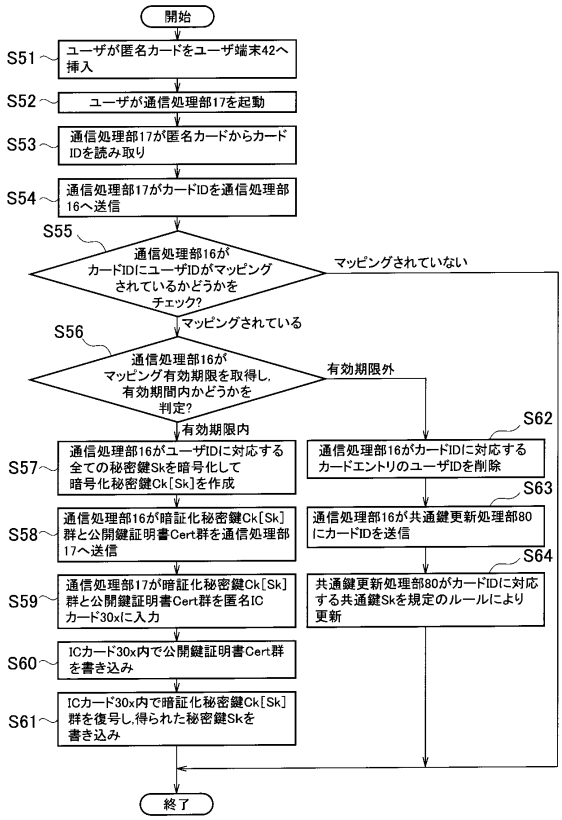
【図６】


開始
S31
共通鍵Ckを作成
S32
共通鍵Ckからカードエントリを作成し
登録(ユーザIDは空)
S33
共通鍵Ckをカード発行機20に送出
S34
共通鍵Ckを含む匿名カード30xを発行
S35
匿名カード30xを事業場へストック
終了

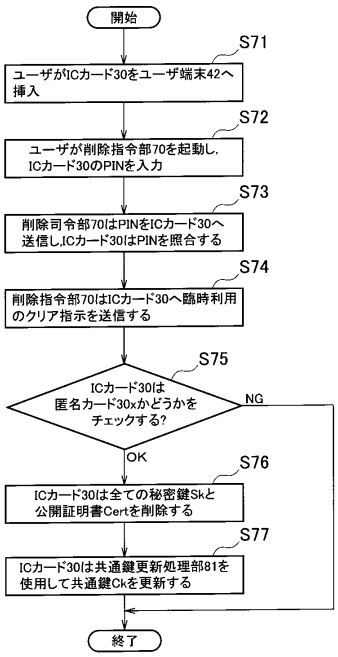
【図７】


開始
S41
ユーザが匿名カードをユーザ端末42へ
挿入
S42
ユーザが臨時利用申請処理61を起動し
ユーザIDと本人確認情報を入力
S43
臨時利用申請処理部61が匿名カード
からカードIDを読み取り
S44
臨時利用申請処理部61が,カードID,
ユーザID,本人確認情報を臨時利用
申請受付処理部60へ送信
S45
臨時利用申請
受付処理部60が本人確認情報の
確認およびユーザIDとカードIDの
マッピング許可判定
を実施?
NG
OK
S46
臨時利用申請受付処理部60が,カードID
に対応するカードエントリにユーザIDと
規定の方法で算出されたマッピング
有効期限を書き込み
終了

【図８】


開始
S51
ユーザが匿名カードをユーザ端末42へ挿入
S52
ユーザが通信処理部17を起動
S53
通信処理部17が匿名カードからカードIDを読み取り
S54
通信処理部17がカードIDを通信処理部16へ送信
S55
通信処理部16がカードIDにユーザIDがマッピングされているかどうかをチェック?
マッピングされていない
マッピングされている
S56
通信処理部16がマッピング有効期限を取得し，有効期間内かどうかを判定?
有効期限外
有効期限内
S57
通信処理部16がユーザIDに対応する全ての秘密鍵Skを暗号化して暗号化秘密鍵Ck[Sk]を作成
S58
通信処理部16が暗証化秘密鍵Ck[Sk]群と公開鍵証明書Cert群を通信処理部17へ送信
S59
通信処理部17が暗証化秘密鍵Ck[Sk]群と公開鍵証明書Cert群を匿名ICカード30xに入力
S60
ICカード30x内で公開鍵証明書Cert群を書き込み
S61
ICカード30x内で暗証化秘密鍵Ck[Sk]群を復号し，得られた秘密鍵Skを書き込み
S62
通信処理部16がカードIDに対応するカードエントリのユーザIDを削除
S63
通信処理部16が共通鍵更新処理部80にカードIDを送信
S64
共通鍵更新処理部80がカードIDに対応する共通鍵Skを規定のルールにより更新
終了

【図９】


開始
S71
ユーザがICカード30をユーザ端末42へ挿入
S72
ユーザが削除指令部70を起動し，ICカード30のPINを入力
S73
削除司令部70はPINをICカード30へ送信し，ICカード30はPINを照合する
S74
削除指令部70はICカード30へ臨時利用のクリア指示を送信する
S75
ICカード30は匿名カード30xかどうかをチェックする?
NG
OK
S76
ICカード30は全ての秘密鍵Skと公開証明書Certを削除する
S77
ICカード30は共通鍵更新処理部81を使用して共通鍵Ckを更新する
終了

フロントページの続き

(51)Int.Cl. F I
G06K 17/00 S
H04L 9/00 673E

(74)代理人 100095500
弁理士 伊藤 正和
(74)代理人 100101247
弁理士 高橋 俊一
(74)代理人 100098327
弁理士 高松 俊雄
(72)発明者 石原 達也
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内

審査官 石田 信行

(56)参考文献 特開２００３－０９２５６５（ＪＰ，Ａ）
特開２００３－０７８５１６（ＪＰ，Ａ）
特開２００４－０９４６９２（ＪＰ，Ａ）
特開２００４－２６５１７７（ＪＰ，Ａ）
特開２００１－２７３４６８（ＪＰ，Ａ）
特開２００１－２６６０７８（ＪＰ，Ａ）
特開昭６４－０８１０８４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／１０
Ｈ０４Ｌ ９／３２
Ｇ０６Ｋ １７／００
Ｇ０６Ｆ ２１／２４