【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成21年11月5日(2009.11.5)

【公開番号】特開2009-212731(P2009-212731A)
【公開日】平成21年9月17日(2009.9.17)
【年通号数】公開・登録公報2009-037
【出願番号】特願2008-52729(P2008-52729)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｋ　17/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｚ
Ｇ０６Ｋ　17/00　Ｌ
Ｇ０６Ｋ　17/00　Ｂ

【手続補正書】
【提出日】平成21年7月31日(2009.7.31)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ＩＣチップを搭載した情報処理端末と、ネットワークを介して前記情報処理端末と接続可能なサービス提供サーバおよびカード発行サーバとを含むカード発行システムであって、
前記サービス提供サーバは、
前記情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成する認証チケット作成部と、
前記認証チケット作成部により作成された前記認証チケットを前記カード発行サーバに送信する認証チケット送信部と、
を備え、
前記カード発行サーバは、
前記認証チケット送信部により送信された前記認証チケットを復号化して前記認証チケットを検証する認証チケット検証部と、
前記認証チケット検証部により検証された前記認証チケットの検証結果を前記サービス提供サーバに通知する検証結果通知部と、
前記認証チケットの検証結果とともに前記カード発行サーバと接続するための接続情報を前記サービス提供サーバに送信する接続情報送信部と、
前記認証チケットのアクセス認証情報と、前記情報処理端末の前記ＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、
を備え、
前記情報処理端末は、
前記接続情報に基づいて前記カード発行サーバに接続する接続部と、
前記ＩＣチップに設けられる前記アクセス認証情報を記憶する認証情報記憶部と、
を備えることを特徴とする、カード発行システム。
【請求項２】
ＩＣチップを搭載した情報処理端末およびサービス提供サーバとネットワークを介して

接続可能な、カード発行サーバであって、
前記サービス提供サーバは、前記情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成し、
前記サービス提供サーバにより作成された認証チケットを受信する認証チケット受信部と、
前記認証チケット受信部により受信された前記認証チケットを復号化して前記認証チケットを検証する認証チケット検証部と、
前記認証チケット検証部により検証された前記認証チケットの検証結果を前記サービス提供サーバに通知する検証結果通知部と、
前記認証チケットの検証結果とともに前記カード発行サーバと接続するための接続情報を前記サービス提供サーバに送信する接続情報送信部と、
前記認証チケットのアクセス認証情報と、前記情報処理端末の前記ＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、
を備えることを特徴とする、カード発行サーバ。
【請求項３】
前記サービス提供サーバは、認証用秘密鍵を用いて前記アクセス認証情報に電子署名を付加して前記認証チケットを作成し、
前記認証チケット検証部は、前記認証用秘密鍵に対応する認証用公開鍵を用いて前記認証チケットに付加された電子署名を検証することを特徴とする、請求項２に記載のカード発行サーバ。
【請求項４】
前記カード発行サーバは、ネットワークを介して前記サービス提供サーバを代行するサービス代行サーバと接続され、
前記サービス提供サーバは、前記サービス代行サーバに許諾するサービスの情報を暗号化して認証ライセンスを作成し、前記サービス代行サーバは、前記認証ライセンスに、前記情報処理端末によるアクセスを認証するためのアクセス認証情報を付加し暗号化して前記認証チケットを作成し、
前記認証チケットを復号化して前記認証ライセンスを取得する認証ライセンス取得部と、
前記認証ライセンス取得部により取得された前記認証ライセンスを復号化して前記認証ライセンスを検証する認証ライセンス検証部と、
を備え、
前記認証チケット検証部は、前記認証ライセンス検証部により検証された認証ライセンスに基づいて、前記認証チケットを検証することを特徴とする、請求項２に記載のカード発行サーバ。
【請求項５】
前記サービス提供サーバは、第１認証用秘密鍵を用いて前記利用者認証情報に第１電子署名を付加して前記認証ライセンスを作成し、前記サービス代行サーバは、前記認証ライセンスに前記アクセス認証情報を付加し、さらに第２認証用秘密鍵を用いて第２電子署名を付加して前記認証チケットを作成し、
前記認証ライセンス検証部は、前記第１認証用秘密鍵に対応する第１認証用公開鍵を用いて前記認証ライセンスに付加された前記第１電子署名を検証し、
前記認証チケット検証部は、前記認証ライセンス検証部により検証された前記認証ライセンスに含まれる前記第２認証用秘密鍵に対応する第２認証用公開鍵を用いて前記認証チケットに付加された前記第２電子署名を検証することを特徴とする、請求項４に記載のカード発行サーバ。
【請求項６】
前記アクセス認証情報には、少なくとも、前記情報処理端末が利用する処理の情報、前記ＩＣチップの識別情報、前記ＩＣチップの発行元情報が含まれることを特徴とする、請求項２に記載のカード発行サーバ。

【請求項７】
前記アクセス認証情報には、前記ＩＣチップへの書き込みが可能か否かを判断する書き込み判断情報が含まれ、
前記認証情報検証部は、前記書き込み判断情報に基づいて、前記ＩＣチップへの書き込みを判断することを特徴とする、請求項２に記載のカード発行サーバ。
【請求項８】
前記アクセス認証情報には、前記ＩＣチップへのデータ書き込みまたは前記ＩＣチップに書き込まれたデータの利用が可能な機器の制限情報が含まれることを特徴とする、請求項２に記載のカード発行サーバ。
【請求項９】
チャレンジレスポンス認証により前記サービス提供サーバを認証するチャレンジレスポンス認証部を備えることを特徴とする、請求項２に記載のカード発行サーバ。
【請求項１０】
前記チャレンジレスポンス認証部は、チャレンジレスポンス認証により前記サービス代行サーバを認証することを特徴とする、請求項９に記載のカード発行サーバ。
【請求項１１】
前記サービス提供サーバの要求に応じて、前記情報処理端末の前記ＩＣチップへのアクセス状況を通知するアクセス状況通知部を備えることを特徴とする、請求項２に記載のカード発行サーバ。
【請求項１２】
前記アクセス状況通知部は、前記サービス提供サーバの要求に応じて、前記ＩＣチップに記憶された前記アクセス認証情報を前記サービス提供サーバに送信するアクセス認証情報送信部を備えることを特徴とする、請求項１１に記載のカード発行サーバ。
【請求項１３】
ＩＣチップを搭載した情報処理端末およびサービス提供サーバとネットワークを介して接続可能な、カード発行サーバであって、
前記サービス提供サーバは、前記情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成し、
前記情報処理端末を経由して前記サービス提供サーバにより作成された認証チケットを受信する認証チケット受信部と、
前記認証チケット受信部により受信された前記認証チケットを復号化して前記認証チケットを検証する認証チケット検証部と、
前記認証チケット検証部により検証された前記認証チケットの検証結果を前期情報処理端末に通知する検証結果通知部と、
前記認証チケットのアクセス認証情報と、前記情報処理端末の前記ＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、
を備えることを特徴とする、カード発行サーバ。
【請求項１４】
コンピュータを、
ＩＣチップを搭載した情報処理端末およびサービス提供サーバとネットワークを介して接続可能な、カード発行サーバであって、
前記サービス提供サーバは、前記情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成し、
前記サービス提供サーバにより作成された認証チケットを受信する認証チケット受信部と、
前記認証チケット受信部により受信された前記認証チケットを復号化して前記認証チケットを検証する認証チケット検証部と、
前記認証チケット検証部により検証された前記認証チケットの検証結果を前記サービス提供サーバに通知する検証結果通知部と、
前記認証チケットの検証結果とともに前記カード発行サーバと接続するための接続情報

を前記サービス提供サーバに送信する接続情報送信部と、
前記認証チケットのアクセス認証情報と、前記情報処理端末の前記ＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、
を備えるカード発行サーバとして機能させるための、プログラム。
【請求項１５】
コンピュータを、
ＩＣチップを搭載した情報処理端末およびサービス提供サーバとネットワークを介して接続可能な、カード発行サーバであって、
前記サービス提供サーバは、前記情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成し、
前記情報処理端末を経由して前記サービス提供サーバにより作成された認証チケットを受信する認証チケット受信部と、
前記認証チケット受信部により受信された前記認証チケットを復号化して前記認証チケットを検証する認証チケット検証部と、
前記認証チケット検証部により検証された前記認証チケットの検証結果を前期情報処理端末に通知する検証結果通知部と、
前記認証チケットのアクセス認証情報と、前記情報処理端末の前記ＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、
を備えるカード発行サーバとして機能させるためのプログラム。

【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００５２
【補正方法】変更
【補正の内容】
【００５２】
暗号化には、ＲＳＡ等の非対称鍵や、ＤＥＳまたはＡＳＥ等の対象鍵などのいかなる鍵の場合であっても実施可能である。なお、対称鍵の場合、秘密裏に鍵を相手方に配布する必要があるため、通信網から直接配布するのではなく、内容証明付き郵送等の手段で配布される。本実施形態では、公開かぎ暗号方式を利用して暗号化や電子署名の付加を行う場合について説明する。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００９４
【補正方法】変更
【補正の内容】
【００９４】
サービス提供サーバ２００′についても、第１実施形態のサービス提供サーバ２００とほぼ同様の機能を有するため、詳細な説明は省略する。第１実施形態のサービス提供サーバ２００′と特に異なる点は、認証チケット作成部２０４により作成された認証チケットを提供された認証チケット送信部２１２′が、認証チケットをカード発行サーバ３００′ではなく、情報処理端末１００′のクライアントアプリ１０４に送信する点である。クライアントアプリ１０４に送信された認証チケットは、クライアントアプリ１０４からカード発行サーバ３００′に送信される。これにより、サービス提供サーバ２００′とカード発行サーバ３００′との間の通信を削減し、サービス提供サーバ２００′の構築工数を削減することが可能となる。

【手続補正４】
【補正対象書類名】明細書

【補正対象項目名】００９５
【補正方法】変更
【補正の内容】
【００９５】
カード発行サーバ３００′についても、第１実施形態のカード発行サーバ３００とほぼ同様の機能を有するため、詳細な説明は省略する。第１実施形態のカード発行サーバ３００と特に異なる点は、情報処理端末１００′から送信された認証チケットを認証チケット受信部３１２′が受信して認証チケット検証部３０６に提供する点である。また、検証結果通知部３０８の検証結果および当該検証結果と同時に送信される接続情報は、接続情報送信部３１４′により情報処理端末１００′のクライアントアプリ１０４に送信される。第１実施形態では、検証結果および接続情報は、サービス提供サーバ２００を経由してクライアントアプリ１０４に送信されたが、本実施形態では、直接クライアントアプリ１０４に送信することができる。これにより、サービス提供サーバ２００′とカード発行サーバ３００′との間の通信を削減することが可能となる。以上、カード発行システム１０′にかかる各装置の機能構成について説明した。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００９６
【補正方法】変更
【補正の内容】
【００９６】
次に、カード発行システム１０′において実行されるカード発行方法について説明する。本実施形態にかかるカード発行方法について、第１実施形態と同様の処理については、詳細な説明は省略する。図１２は、カード発行システム１０′において実行されるカード発行方法の流れを示したタイミングチャートである。図１２に示したように、まず、クライアントアプリ１０４が、サービス提供サーバ２００′にアクセス認証情報を送信する（Ｓ３０２）。ステップＳ３０２においてクライアントアプリ１０４からアクセス認証情報を送信されたサービス提供サーバ２００′は、アクセス認証情報を暗号化したり、電子署名を付加したりすることにより認証チケットを作成する（Ｓ３０４）。ステップＳ３０４において作成した認証チケットを、クライアントアプリ１０４に送信する（Ｓ３０６）。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】０１１７
【補正方法】変更
【補正の内容】
【０１１７】
認証ライセンス検証部３２４は、受信した認証ライセンスを復号化して認証ライセンスを検証する機能を有する。認証ライセンスに電子署名が付加されている場合には、当該電子署名を認証用公開鍵（Ｐｋ１）を用いて検証して、認証ライセンスに含まれる認証用公開鍵（Ｐｋ２）の正当性を確認する。認証チケット検証部３０７は、認証ライセンス検証部３２４により、正当性を確認された認証用公開鍵（Ｐｋ２）を利用して認証チケットの電子署名検証を行って、チケットの正当性を検証する機能を有する。また、第１実施形態の認証チケット検証部３０６と同様に、認証チケットのアクセス認証情報について検証を行う。認証ライセンス検証部３２４は、認証チケットの検証結果を、検証結果通知部３０８に提供する。