【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】令和4年9月14日(2022.9.14)

【国際公開番号】WO2020/004494
【出願番号】特願2020-527594(P2020-527594)
【国際特許分類】
H04L 9/32(2006.01)
G09C 1/00(2006.01)
【ＦＩ】
H04L 9/00 675B
G09C 1/00 640E
H04L 9/00 675D

【手続補正書】
【提出日】令和4年9月6日(2022.9.6)
【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】
携帯機器からオンラインサービスを安全に利用可能な仕組みを提供するオンラインサービス提供システムであって、
登録されたユーザに対し、インターネットを通じてオンラインサービスを提供するサービス提供サーバと、
前記ユーザが所持している携帯機器であるユーザ機器に設けられるＩＣチップと、
前記ユーザ機器が有する本体プロセッサにより実行され、前記ユーザ機器を前記オンラインサービスを利用するための端末として機能させるアプリケーションプログラムと、を有し、
前記ＩＣチップは、
少なくとも、前記ユーザ機器を使用する者の正当性を確認するためのユーザ認証に用いられる本人情報、前記ユーザの秘密鍵、前記秘密鍵とペアになる前記ユーザの公開鍵、及び、前記公開鍵を含む前記ユーザの電子証明書を非一時的に記憶するメモリと、
少なくとも、前記本体プロセッサにより実行されるプログラムから与えられる情報を前記本人情報と照合することにより前記ユーザ認証を行う認証機能、及び、前記本体プロセッサにより実行されるプログラムから与えられるデータに対し前記秘密鍵を用いた電子署名を行う電子署名機能を有するプロセッサと、
を有しており、
前記ＩＣチップの前記メモリは、前記本体プロセッサにより実行されるプログラムが直接に読み書きできないエリアを有しており、
少なくとも前記本人情報及び前記秘密鍵は、前記エリア内に格納され、
前記ＩＣチップの前記プロセッサは、前記本体プロセッサにより実行されるプログラムに対して、複数のＡＰＩを提供するものであり、
前記複数のＡＰＩは、前記認証機能を利用するための認証ＡＰＩ及び前記電子署名機能を利用するための電子署名ＡＰＩを少なくとも含み、前記ＩＣチップの前記メモリから前記秘密鍵を読みだすためのＡＰＩを含んでおらず、
前記アプリケーションプログラムは、前記ユーザ機器を、
前記ユーザ機器を使用する者から取得した情報に基づき、前記認証ＡＰＩを介して前

記ＩＣチップの前記認証機能を利用して、前記ユーザ認証を行うユーザ認証手段、及び、
　前記ユーザ認証により前記ユーザ機器を使用する者が正当であると確認された場合に、前記電子署名ＡＰＩを介して前記ＩＣチップの前記電子署名機能を利用して電子署名を生成し、生成された前記電子署名を含むログイン要求をインターネットを通じて前記サービス提供サーバに送信する送信手段、
として機能させ、
　前記サービス提供サーバは、
前記ユーザ機器から前記ログイン要求を受信した場合に、前記ユーザの電子証明書を用いて前記ログイン要求に含まれる前記電子署名を検証することによって前記ログイン要求の正当性を確認し、前記ログイン要求が正当であると確認された場合に前記ユーザ機器からの前記オンラインサービスの利用を許可するログイン制御手段と、
を有する
ことを特徴とするオンラインサービス提供システム。
【請求項２】
前記ユーザ認証により前記ユーザ機器を使用する者が正当であると確認されると、前記電子署名機能の機能制限が解除され、前記アプリケーションプログラムから前記電子署名ＡＰＩを介した前記電子署名機能の利用が可能となる
ことを特徴とする請求項１に記載のオンラインサービス提供システム。
【請求項３】
　前記ＩＣチップは、通信用のＳＩＭカード上に重ねて貼り付けられた状態でＳＩＭカードスロットに装着されるものである
ことを特徴とする請求項１又は２に記載のオンラインサービス提供システム。
【請求項４】
　前記ＩＣチップは、通信用のＳＩＭカードである
ことを特徴とする請求項１又は２に記載のオンラインサービス提供システム。
【請求項５】
　前記ＩＣチップは、セキュアエレメントである
ことを特徴とする請求項１又は２に記載のオンラインサービス提供システム。
【請求項６】
　前記複数のＡＰＩは、前記メモリの内部に前記秘密鍵と前記公開鍵を生成する鍵生成機能を利用するための鍵生成ＡＰＩを含む
ことを特徴とする請求項１～５のいずれかに記載のオンラインサービス提供システム。
【請求項７】
　前記ＩＣチップは、前記ＩＣチップを一意に特定しうる識別情報を有しており、
　前記ユーザ機器と前記サービス提供サーバとの間で、前記識別情報により前記ＩＣチップが特定された通信が行われる
ことを特徴とする請求項１～６のいずれかに記載のオンラインサービス提供システム。
【請求項８】
　前記アプリケーションプログラムは、前記サービス提供サーバと前記ＩＣチップとの対応付けを行う対応付け情報を有しており、前記対応付け情報に基づいて、前記サービス提供サーバとの通信において利用する前記ＩＣチップを特定する
ことを特徴とする請求項１～６のいずれかに記載のオンラインサービス提供システム。
【請求項９】
　前記ユーザ機器と前記サービス提供サーバとの間で、前記ユーザ機器が備える通信用のＳＩＭカードのＩＭＳＩ又はそのＩＭＳＩに対応付けられたＩＰアドレスにより前記ＳＩＭカードが特定された通信が行われる
ことを特徴とする請求項１～８のいずれかに記載のオンラインサービス提供システム。
【請求項１０】
　前記ユーザ機器が有する本体プロセッサにより実行され、前記ＩＣチップをセットアップするための機能を提供するセットアッププログラムを有している

ことを特徴とする請求項１～９のいずれかに記載のオンラインサービス提供システム。
【請求項１１】
前記セットアッププログラムは、前記ユーザ機器を、
認証局に対して電子証明書の発行要求を送信する手段、および、
前記認証局より前記電子証明書を受信し、前記ＩＣチップの前記メモリに前記電子証明書を格納する手段、
として機能させる
ことを特徴とする請求項１０に記載のオンラインサービス提供システム。
【請求項１２】
前記セットアッププログラムは、前記ユーザ機器を、
前記ユーザ機器が備える通信用のＳＩＭカードから電話番号及び／又はＩＭＳＩを読み出す手段、
前記電話番号及び／又はＩＭＳＩを前記認証局に通知するための手段、
前記認証局から前記電話番号又は前記ＩＭＳＩにより特定される宛先に送信された情報を受信する手段、
として機能させる
ことを特徴とする請求項１１に記載のオンラインサービス提供システム。
【請求項１３】
前記情報は、ＳＭＳにより前記ユーザ機器に送信される
ことを特徴とする請求項１２に記載のオンラインサービス提供システム。
【請求項１４】
前記情報は、インターネットを介したデータ通信により前記ユーザ機器に送信される
ことを特徴とする請求項１２に記載のオンラインサービス提供システム。
【請求項１５】
ユーザが所持している携帯機器であるユーザ機器において使用されるＩＣチップであって、
少なくとも、前記ユーザ機器を使用する者の正当性を確認するためのユーザ認証に用いられる本人情報、前記ユーザの秘密鍵、前記秘密鍵とペアになる前記ユーザの公開鍵、及び、前記公開鍵を含む前記ユーザの電子証明書を非一時的に記憶するメモリと、
少なくとも、前記ユーザ機器が有する本体プロセッサにより実行されるプログラムから与えられる情報を前記本人情報と照合することにより前記ユーザ認証を行う認証機能、及び、前記本体プロセッサにより実行されるプログラムから与えられるデータに対し前記秘密鍵を用いた電子署名を行う電子署名機能を有するプロセッサと、
を有し、
前記ＩＣチップの前記メモリは、前記本体プロセッサにより実行されるプログラムが直接に読み書きできないエリアを有しており、
少なくとも前記本人情報及び前記秘密鍵は、前記エリア内に格納され、
前記ＩＣチップの前記プロセッサは、前記本体プロセッサにより実行されるプログラムに対して、複数のＡＰＩを提供するものであり、
前記複数のＡＰＩは、前記認証機能を利用するための認証ＡＰＩ及び前記電子署名機能を利用するための電子署名ＡＰＩを少なくとも含み、前記ＩＣチップの前記メモリから前記秘密鍵を読みだすためのＡＰＩを含んでいない
ことを特徴とするＩＣチップ。
【請求項１６】
ユーザが所持している携帯機器であるユーザ機器が有する本体プロセッサにより実行され、前記ユーザ機器を、サービス提供サーバがインターネットを通じて提供するオンラインサービスを利用するための端末として機能させるアプリケーションプログラムであって、
前記ユーザ機器には、請求項１５に記載のＩＣチップが設けられており、
前記アプリケーションプログラムは、前記ユーザ機器を、

前記ユーザ機器を使用する者から取得した情報に基づき、前記ＩＣチップが提供する前記認証ＡＰＩを介して前記ＩＣチップの前記認証機能を利用して、前記ユーザ認証を行うユーザ認証手段、及び、

前記ユーザ認証により前記ユーザ機器を使用する者が正当であると確認された場合に、前記ＩＣチップが提供する前記電子署名ＡＰＩを介して前記ＩＣチップの前記電子署名機能を利用して電子署名を生成し、生成された前記電子署名を含むログイン要求をインターネットを通じて前記サービス提供サーバに送信する送信手段、

として機能させることを特徴とするアプリケーションプログラム。