【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24年6月28日(2012.6.28)

【公開番号】特開2010-200381(P2010-200381A)
【公開日】平成22年9月9日(2010.9.9)
【年通号数】公開・登録公報2010-036
【出願番号】特願2010-135412(P2010-135412)
【国際特許分類】
Ｈ０４Ｌ　9/10　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６２１Ａ
Ｈ０４Ｌ　9/00　６７５Ｂ

【手続補正書】
【提出日】平成24年5月15日(2012.5.15)
【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】
公開鍵暗号化方式において少なくとも２つの通信機器の間で送信されたデータの完全性を確認する方法であって、前記少なくとも２つの通信機器のうちの少なくとも１つは、メインプロセッサとセキュアモジュールとを含み、前記セキュアモジュールは、前記メインプロセッサの制御から独立しており、前記セキュアモジュールには、秘密鍵が格納されており、
前記方法は、
前記メインプロセッサおよび前記セキュアモジュールのそれぞれに対して利用可能とされるように、前記少なくとも２つの通信機器のうちの１つの上で、前記データをアセンブルする工程と、
前記データを表示することにより第１の出力を生成するように前記メインプロセッサを動作させる工程と、
前記データを表示することにより第２の出力を生成するように前記セキュアモジュールを動作させる工程であって、これにより、前記第１の出力と前記第２の出力との比較がなされることが可能である、工程と、
前記第１の出力および前記第２の出力を生成した後に、前記セキュアモジュールに関する手動制御を選択的に動作させることにより、前記秘密鍵を用いて、前記データに対する署名を生成することを前記セキュアモジュールに行わせる工程と
を含み、
前記第２の出力を生成する前記データの完全性を前記署名が示すような好適な比較結果が得られた後に、前記選択的な動作が開始されることが可能である、方法。
【請求項２】
前記少なくとも２つの通信機器のうちの前記少なくとも１つは、個人用機器である、請求項１に記載の方法。
【請求項３】
前記個人用機器は、携帯電話である、請求項２に記載の方法。
【請求項４】

前記個人用機器は、ＰＤＡである、請求項２に記載の方法。
【請求項５】
前記セキュアモジュールは、前記第２のデータの表示から所定の期間が経過した後は、署名の生成を阻止する、請求項１から４のいずれか１項に記載の方法。
【請求項６】
前記セキュアモジュールに対するアクセスは、確認管理部によって制御される、請求項１から５のいずれか１項に記載の方法。
【請求項７】
前記確認管理部は、パスワードを介してアクセスを制御する、請求項６に記載の方法。
【請求項８】
前記第１の出力および前記第２の出力のそれぞれは、比較するために共通のデータを表示する、請求項１から７のいずれか１項に記載の方法。
【請求項９】
前記セキュアモジュールは、前記メインプロセッサによって前記第１の出力上に表示されたデータの一部を前記第２の出力上に表示する、請求項８に記載の方法。
【請求項１０】
公開鍵暗号化方式において、個人用機器と前記機器のユーザとの間でデータのセキュアな通信経路を確立する方法であって、前記機器は、メインプロセッサと、前記メインプロセッサとは独立して動作するセキュアモジュールとを含み、前記セキュアモジュールには、秘密鍵が格納されており、
前記方法は、
前記機器と前記ユーザとの間のインターフェイスを提供する工程であって、前記インターフェイスは、前記ユーザと前記機器とを相互作用させるための手段を提供するために、入力デバイスと出力デバイスとを含み、前記入力デバイスと前記出力デバイスとは、前記メインプロセッサによって制御可能である、工程と、
前記セキュアモジュールとこれに結合されたセキュア入力デバイスおよびセキュア出力デバイスとの間でセキュアな通信経路を提供する工程であって、前記セキュアな経路は、任意の他の通信経路から論理的に隔離されている、工程と、
前記出力デバイスおよび前記セキュア出力デバイス上に共通のデータを表示する工程であって、これにより、前記個人用機器の前記ユーザは、前記出力デバイスと前記セキュア出力デバイスとの比較に基づいて、前記データの完全性を決定することができる、工程と、
前記共通のデータの完全性を確認するために、前記秘密鍵を用いて、前記共通のデータに署名することを前記セキュアモジュールに行わせるように、前記セキュア入力デバイスを動作させる工程と
を含む、方法。
【請求項１１】
公開鍵暗号化方式において、少なくとも２つの通信機器の間でのデータメッセージの完全性を確認するシステムであって、
前記少なくとも２つの通信機器のうちの少なくとも１つは、メインプロセッサとセキュアモジュールとを含み、
前記セキュアモジュールは、前記メインプロセッサの制御から独立しており、
前記セキュアモジュールには、秘密鍵が格納されており、
前記少なくとも２つの通信機器のうちの前記少なくとも１つは、前記メインプロセッサによって制御される、第１の出力を表示するための第１のディスプレイと、前記セキュアモジュールからの第２の出力を表示するための第２のディスプレイとを含み、
前記第１の出力と第２の出力とは比較されることが可能であり、
前記セキュアモジュールは、前記第１の出力と前記第２の出力との比較後に、前記秘密鍵を用いて、第２のディスプレイ上に表示されたデータに署名する署名生成器と、前記セキュアモジュールの動作を開始させる手動制御部とを有する、システム。

【請求項１２】
前記少なくとも２つの通信機器のうちの前記少なくとも１つは、個人用機器である、請求項１１に記載のシステム。
【請求項１３】
前記個人用機器は、携帯電話またはＰＤＡである、請求項１１に記載のシステム。
【請求項１４】
前記セキュアモジュールは、前記署名生成器の動作を阻止する確認管理部を含む、請求項１１から１３のいずれか１項に記載のシステム。
【請求項１５】
前記セキュアモジュールは、前記データの表示から所定期間が経過した後に、前記署名生成器の動作を阻止する制御部を含む、請求項１１から１４のいずれか１項に記載のシステム。