

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第6857018号  
(P6857018)

(45) 発行日 令和3年4月14日(2021.4.14)

(24) 登録日 令和3年3月23日(2021.3.23)

(51) Int.Cl.		F I			
HO4L	9/32	(2006.01)	HO4L	9/00	673E
HO4L	9/08	(2006.01)	HO4L	9/00	601D
GO6F	21/44	(2013.01)	GO6F	21/44	
GO6F	21/64	(2013.01)	GO6F	21/64	

請求項の数 12 (全 35 頁)

(21) 出願番号	特願2016-243810 (P2016-243810)	(73) 特許権者	511289530
(22) 出願日	平成28年12月15日(2016.12.15)		エスケー プラネット カンパニー、リミテッド
(65) 公開番号	特開2017-200165 (P2017-200165A)		大韓民国 463-400 キョンギード、ソンナムーシ、ブンダンーグ、パンキョーロ、264、(サムピョンードン)
(43) 公開日	平成29年11月2日(2017.11.2)	(74) 代理人	110000855
審査請求日	令和1年12月13日(2019.12.13)		特許業務法人浅村特許事務所
(31) 優先権主張番号	10-2016-0051911	(72) 発明者	ウ、ジョン ウォン
(32) 優先日	平成28年4月28日(2016.4.28)		大韓民国 21324 インチョン、プビョンーグ、スピョンーロ、333、221-502 (サムサンードン、サムサンタウン2ダンジアパートメント)
(33) 優先権主張国・地域又は機関	韓国 (KR)		
(31) 優先権主張番号	10-2016-0065212		
(32) 優先日	平成28年5月27日(2016.5.27)		
(33) 優先権主張国・地域又は機関	韓国 (KR)		

最終頁に続く

(54) 【発明の名称】 保安強化のための電子はんこシステム、その制御方法およびコンピュータプログラムが記録された記録媒体

(57) 【特許請求の範囲】

【請求項1】

端末によって、前記端末から実行中のアプリと関連するメンバーシップID、電子はんこ情報、暗号化された値および端末の識別情報を電子はんこサーバーに転送する段階と；

前記電子はんこサーバーによって、前記電子はんこ情報から電子はんこIDを抽出する段階と；

前記電子はんこサーバーによって、前記抽出された電子はんこIDに基づき、復号化キーを生成する段階と；

前記電子はんこサーバーによって、前記生成された復号化キーに基づき、前記端末から転送された暗号化された値を復号化する段階と；

前記電子はんこサーバーによって、復号化された値を前記端末から転送されたメンバーシップIDと比較して電子はんこの真偽可否を確認する段階と；

前記電子はんこサーバーによって、前記確認された電子はんこの真偽可否における情報を前記端末に転送する段階；および

前記端末によって、前記電子はんこの真偽可否における情報に基づき、電子はんこに関連するスタンプ貯めの機能遂行の可否、または、電子はんこの職印の機能遂行の可否を決定する段階を含む保安強化のための電子はんこシステムの制御方法。

【請求項2】

前記暗号化された値は、

前記端末によって、前記端末から電子はんこを認識できるアプリが実行中の状態で前記

端末の静電式画面に前記電子はんこが接触される時、前記電子はんこと連結する過程と；  
 前記端末によって、前記端末から実行中のアプリと関連するメンバーシップIDおよび前記端末の識別情報を前記電子はんこに転送する過程と；  
 前記電子はんこによって、使い捨ての暗証番号を生成する過程と；  
 前記電子はんこによって、前記生成された使い捨ての暗証番号と前記受信したメンバーシップIDとを組み合わせる前記暗号化された値を生成する過程；および  
 前記電子はんこによって、前記生成された暗号化された値を前記端末に提供する過程によって獲得されたことを特徴とする請求項1に記載の保安強化のための電子はんこシステムの制御方法。

【請求項3】

10

前記確認された電子はんこの真偽可否における情報を前記端末に転送する段階は、  
 前記電子はんこサーバーによって、前記確認の結果、前記復号化された値が前記端末から転送されたメンバーシップIDと同一である時、電子はんこが本物であると確認して、電子はんこが本物であることを示す情報を前記端末に転送する過程；および  
 前記電子はんこサーバーによって、前記確認の結果、前記復号化された値が前記端末から転送されたメンバーシップIDと異なる時、電子はんこが偽造されたことを確認して、電子はんこが偽造された状態であることを示す情報を前記端末に転送する過程のうち、いずれか一つの過程を含むことを特徴とする請求項1に記載の保安強化のための電子はんこシステムの制御方法。

【請求項4】

20

前記電子はんこの真偽可否における情報に基づき、電子はんこと関連するスタンプ貯めの機能遂行の可否、または、電子はんこの職印の機能遂行の可否を決定する段階は、  
 前記端末によって、前記電子はんこサーバーから転送される電子はんこが本物であることを示す情報を受信する時、電子はんこと関連するスタンプ貯めの機能、または、電子はんこの職印の機能を遂行する過程；および  
 前記端末によって、前記スタンプ貯めの機能遂行の結果、または、電子はんこの職印の機能遂行の結果を表示する過程を含むことを特徴とする請求項3に記載の保安強化のための電子はんこシステムの制御方法。

【請求項5】

30

前記電子はんこの真偽可否における情報に基づき、電子はんこと関連するスタンプ貯めの機能遂行の可否、または、電子はんこの職印の機能遂行の可否を決定する段階は、  
 前記端末によって、前記電子はんこサーバーから転送される電子はんこが偽造された状態であることを示す情報を受信する時、電子はんこと関連するスタンプ貯めの機能、または、電子はんこの職印の機能の遂行を中断する過程；および  
 前記端末によって、前記電子はんこが偽造された状態であることを示す情報を表示する過程を含むことを特徴とする請求項3に記載の保安強化のための電子はんこシステムの制御方法。

【請求項6】

請求項1ないし請求項5のうち、いずれか一項による方法を遂行するコンピュータプログラムが記録された記録媒体。

40

【請求項7】

端末から電子はんこを認識できるアプリが実行中の状態で前記端末の静電式画面に前記電子はんこが接触される時、前記端末と通信し、前記端末から転送される前記端末から実行中のアプリと関連するメンバーシップIDに回答して暗号化された値を前記端末に提供する前記電子はんこと；

前記端末から実行中のアプリと関連するメンバーシップID、電子はんこ情報、前記電子はんこから提供された暗号化された値および端末の識別情報を提供する前記端末；および

前記電子はんこ情報から電子はんこIDを抽出し、前記抽出された電子はんこIDに基づき、復号化キーを生成し、前記生成された復号化キーに基づき、前記端末から提供され

50

た暗号化された値を復号化し、復号化した値を前記端末から提供されたメンバーシップIDと比較して電子はんこの真偽可否を確認し、前記確認された電子はんこの真偽可否における情報を前記端末に転送する電子はんこサーバーを含む保安強化のための電子はんこシステム。

【請求項 8】

前記電子はんこは、

使い捨ての暗証番号を生成し、前記生成された使い捨ての暗証番号と前記端末から転送されるメンバーシップIDとを組み合わせる前記暗号化された値を生成することを特徴とする請求項 7 に記載の保安強化のための電子はんこシステム。

【請求項 9】

前記電子はんこサーバーは、

前記確認の結果、前記復号化された値が前記端末から転送されたメンバーシップIDと同一である時、電子はんこが本物であると確認して、電子はんこが本物であることを示す情報を前記端末に転送し、前記復号化された値が前記端末から転送されたメンバーシップIDと異なる時、電子はんこが偽造されたと確認して、電子はんこが偽造された状態であることを示す情報を前記端末に転送することを特徴とする請求項 7 に記載の保安強化のための電子はんこシステム。

【請求項 10】

前記端末は、

前記電子はんこサーバーから転送される電子はんこが本物であることを示す情報を受信する時、電子はんこと関連するスタンプ貯めの機能、または、電子はんこの職印の機能を遂行し、スタンプ貯めの機能遂行の結果、または、電子はんこの職印の機能遂行の結果を表示することを特徴とする請求項 9 に記載の保安強化のための電子はんこシステム。

【請求項 11】

前記端末は、

前記電子はんこサーバーから転送される電子はんこが偽造された状態であることを示す情報を受信する時、電子はんこと関連するスタンプ貯めの機能、または、電子はんこの職印の機能の遂行を中断し、前記電子はんこが偽造された状態であることを示す情報を表示することを特徴とする請求項 9 に記載の保安強化のための電子はんこシステム。

【請求項 12】

電子はんこによって、前記電子はんこを利用しようとする利用者の指紋を認識する段階と；

前記電子はんこによって、前記認識された利用者の指紋情報および電子はんこ情報を電子はんこサーバーに転送する段階と；

前記電子はんこサーバーによって、前記指紋情報における認証の手順を遂行する段階と；

前記電子はんこサーバーによって、前記指紋情報における認証の手順の遂行結果を前記電子はんこに転送する段階；および

前記指紋情報における認証の手順の遂行結果に指紋一致の情報が含まれた状態である時、前記電子はんこによって、前記指紋一致の情報に基づき、電子はんこを利用できるように前記電子はんこ内の使い捨ての暗証番号生成部を活性化する段階とを含む保安強化のための電子はんこシステムの制御方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、保安強化のための電子はんこシステム、その制御方法およびコンピュータプログラムが記録された記録媒体に関する。特に、電子はんこで端末から提供される端末の利用者と関連するメンバーシップIDと該電子はんこで生成するOTPなどのような使い捨ての暗証番号に基づき、暗号化された値を生成し、生成された暗号化された値を該端末に提供し、端末からメンバーシップID、電子はんこ情報、暗号化された値を電子はんこ

10

20

30

40

50

サーバーに提供し、電子はんこサーバーで電子はんこ情報から抽出された電子はんこIDに基づき、復号化キーを獲得した後、獲得した復号化キーに基づき、暗号化された値を復号化した後、復号化した値とメンバーシップIDとの比較を通じて、電子はんこの真偽可否を確認する保安強化のための電子はんこシステム、その制御方法およびコンピュータプログラムが記録された記録媒体に関する。

【背景技術】

【0002】

電子はんこを用いるメンバーシップ特典の提供方法は、電子はんこのパターンなどを用いて電子はんこの真偽可否を判断する。

こういう方式は、スマートフォンに電子はんこのパターンを認識して保存できる悪意的なアプリケーションを介して保安が脆弱になる問題がある。

10

【先行技術文献】

【特許文献】

【0003】

【特許文献1】韓国公開特許第10-2015-0059548号[名称：タッチと近距離通信基盤の電子はんこおよびこれを用いる電子捺印認証システム]

【発明の概要】

【発明が解決しようとする課題】

【0004】

本発明の目的は、電子はんこで端末から提供される端末の利用者と関連するメンバーシップIDと該電子はんこで生成するOTPなどのような使い捨ての暗証番号に基づき、暗号化された値を生成し、生成された暗号化された値を該端末に提供し、端末からメンバーシップID、電子はんこ情報、暗号化された値を電子はんこサーバーに提供し、電子はんこサーバーで電子はんこ情報から抽出された電子はんこIDに基づき、復号化キーを獲得した後、獲得した復号化キーに基づき、暗号化された値を復号化した後、復号化した値とメンバーシップIDとの比較を通じて、電子はんこの真偽可否を確認する保安強化のための電子はんこシステム、その制御方法およびコンピュータプログラムが記録された記録媒体を提供することにある。

20

【0005】

本発明の他の目的は、電子はんこを操作できる権限のある者のみが電子はんこを動作させることができるように電子はんこを介して利用者の指紋を認識し、電子はんこサーバーで予め登録した該電子はんこにおける利用権限のある利用者の指紋と該電子はんこで認識した利用者の指紋との比較を通じて、一致する場合、該電子はんこの使い捨ての暗証番号を生成するための使い捨ての暗証番号生成部を活性化する保安強化のための電子はんこシステム、その制御方法およびコンピュータプログラムが記録された記録媒体を提供することにある。

30

【課題を解決するための手段】

【0006】

本発明の実施例による保安強化のための電子はんこシステムの制御方法は、端末によって、前記端末から実行中のアプリと関連するメンバーシップID、電子はんこ情報、暗号化された値および端末の識別情報を電子はんこサーバーに転送する段階と；前記電子はんこサーバーによって、前記電子はんこ情報から電子はんこIDを抽出する段階と；前記電子はんこサーバーによって、前記抽出された電子はんこIDに基づき、復号化キーを生成する段階と；前記電子はんこサーバーによって、前記生成された復号化キーに基づき、前記端末から転送された暗号化された値を復号化する段階と；前記電子はんこサーバーによって、復号化された値を前記端末から転送されたメンバーシップIDと比較して電子はんこの真偽可否を確認する段階と；前記電子はんこサーバーによって、前記確認された電子はんこの真偽可否における情報を前記端末に転送する段階；および前記端末によって、前記電子はんこの真偽可否における情報に基づき、電子はんこに関連するスタンプ貯めの機能遂行の可否、または、電子はんこの職印の機能遂行の可否を決定する段階とを含むこと

40

50

ができる。

【0007】

本発明と関する一例として、前記暗号化された値は、前記端末によって、前記端末から電子はんこを認識できるアプリが実行中の状態で前記端末の静電式画面に前記電子はんこが接触される時、前記電子はんこと連結する過程と；前記端末によって、前記端末から実行中のアプリと関連するメンバーシップIDおよび前記端末の識別情報を前記電子はんこに転送する過程と；前記電子はんこによって、使い捨ての暗証番号を生成する過程と；前記電子はんこによって、前記生成された使い捨ての暗証番号と前記受信したメンバーシップIDとを組み合わせる過程と；前記暗号化された値を生成する過程と；および前記電子はんこによって、前記生成された暗号化された値を前記端末に提供する過程とによって獲得されることが

10

【0008】

本発明と関する一例として、前記確認された電子はんこの真偽可否における情報を前記端末に転送する段階は、前記電子はんこサーバーによって、前記確認の結果、前記復号化された値が前記端末から転送されたメンバーシップIDと同一である時、電子はんこが本物であると確認して、電子はんこが本物であることを示す情報を前記端末に転送する過程と；および前記電子はんこサーバーによって、前記確認の結果、前記復号化された値が前記端末から転送されたメンバーシップIDと異なる時、電子はんこが偽造されたことを確認して、電子はんこが偽造された状態であることを示す情報を前記端末に転送する過程のうち、いずれか一つの過程とを含むことができる。

20

【0009】

本発明と関する一例として、前記電子はんこの真偽可否における情報に基づき、電子はんこと関連するスタンプ貯めの機能遂行の可否、または、電子はんこの職印の機能遂行の可否を決定する段階は、前記端末によって、前記電子はんこサーバーから転送される電子はんこが本物であることを示す情報を受信する時、電子はんこと関連するスタンプ貯めの機能、または、電子はんこの職印の機能を遂行する過程と；および前記端末によって、前記スタンプ貯めの機能遂行の結果、または、電子はんこの職印の機能遂行の結果を表示する過程とを含むことができる。

【0010】

本発明と関する一例として、前記電子はんこの真偽可否における情報に基づき、電子はんこと関連するスタンプ貯めの機能遂行の可否、または、電子はんこの職印の機能遂行の可否を決定する段階は、前記端末によって、前記電子はんこサーバーから転送される電子はんこが偽造された状態であることを示す情報を受信する時、電子はんこと関連するスタンプ貯めの機能、または、電子はんこの職印の機能の遂行を中断する過程と；および前記端末によって、前記電子はんこが偽造された状態であることを示す情報を表示する過程とを含むことができる。

30

【0011】

本発明の実施例によるコンピュータプログラムが記録された記録媒体には、前述の実施例による方法を遂行するコンピュータプログラムが保存されることが

本発明の実施例による保安強化のための電子はんこシステムは、端末から電子はんこを認識できるアプリが実行中の状態で前記端末の静電式画面に前記電子はんこが接触される時、前記端末と通信し、前記端末から転送される前記端末から実行中のアプリと関連するメンバーシップIDに回答して暗号化された値を前記端末に提供する前記電子はんこ；前記端末から実行中のアプリと関連するメンバーシップID、電子はんこ情報、前記電子はんこから提供された暗号化された値および端末の識別情報を提供する前記端末；および前記電子はんこ情報から電子はんこIDを抽出し、前記抽出された電子はんこIDに基づき、復号化キーを生成し、前記生成された復号化キーに基づき、前記端末から提供された暗号化された値を復号化し、復号化した値を前記端末から提供されたメンバーシップIDと比較して電子はんこの真偽可否を確認し、前記確認された電子はんこの真偽可否における情報を前記端末に転送する電子はんこサーバーとを含むことができる。

40

50

## 【 0 0 1 2 】

本発明と関する一例として、前記電子はんこは、使い捨ての暗証番号を生成し、前記生成された使い捨ての暗証番号と前記端末から転送されるメンバーシップIDとを組み合わせることで前記暗号化された値を生成することができる。

## 【 0 0 1 3 】

本発明と関する一例として、前記電子はんこサーバーは、前記確認の結果、前記復号化された値が前記端末から転送されたメンバーシップIDと同一である時、電子はんこが本物であると確認して、電子はんこが本物であることを示す情報を前記端末に転送し、前記復号化された値が前記端末から転送されたメンバーシップIDと異なる時、電子はんこが偽造されたと確認して、電子はんこが偽造された状態であることを示す情報を前記端末に転送することができる。

10

## 【 0 0 1 4 】

本発明と関する一例として、前記端末は、前記電子はんこサーバーから転送される電子はんこが本物であることを示す情報を受信する時、電子はんこに関連するスタンプ貯めの機能、または、電子はんこの職印の機能を遂行し、スタンプ貯めの機能遂行の結果、または、電子はんこの職印の機能遂行の結果を表示することができる。

## 【 0 0 1 5 】

本発明と関する一例として、前記端末は、前記電子はんこサーバーから転送される電子はんこが偽造された状態であることを示す情報を受信する時、電子はんこに関連するスタンプ貯めの機能、または、電子はんこの職印の機能の遂行を中断し、前記電子はんこが偽造された状態であることを示す情報を表示することができる。

20

## 【 0 0 1 6 】

本発明の実施例による保安強化のための電子はんこシステムの制御方法は、電子はんこによって、前記電子はんこを利用しようとする利用者の指紋を認識する段階と；前記電子はんこによって、前記認識された利用者の指紋情報および電子はんこ情報を電子はんこサーバーに転送する段階と；前記電子はんこサーバーによって、前記指紋情報における認証の手順を遂行する段階と；前記電子はんこサーバーによって、前記指紋情報における認証の手順の遂行結果を前記電子はんこに転送する段階；および前記指紋情報における認証の手順の遂行結果に指紋一致の情報が含まれた状態である時、前記電子はんこによって、前記指紋一致の情報に基づき、電子はんこを利用できるように前記電子はんこ内の使い捨ての暗証番号生成部を活性化する段階とを含むことができる。

30

## 【 発明の効果 】

## 【 0 0 1 7 】

本発明は、電子はんこで端末から提供される端末の利用者と関連するメンバーシップIDと該電子はんこで生成するOTPなどのような使い捨ての暗証番号に基づき、暗号化された値を生成し、生成された暗号化された値を該端末に提供し、端末からメンバーシップID、電子はんこ情報、暗号化された値を電子はんこサーバーに提供し、電子はんこサーバーで電子はんこ情報から抽出された電子はんこIDに基づき、復号化キーを獲得した後、獲得した復号化キーに基づき、暗号化された値を復号化した後、復号化した値とメンバーシップIDとの比較を通じて、電子はんこの真偽可否を確認することによって、電子はんこの複製などを通じた不正利用を防ぐことができ、不適切なメンバーシップ特典の提供などによる経済的損失を防げる効果がある。

40

## 【 0 0 1 8 】

また、本発明は、電子はんこを操作できる権限のある者のみが電子はんこを動作させることができるように電子はんこを通じて利用者の指紋を認識し、電子はんこサーバーで予め登録した該電子はんこにおける利用権限のある利用者の指紋と該電子はんこで認識した利用者の指紋との比較を通じて、一致する場合、該電子はんこの使い捨ての暗証番号を生成するための使い捨ての暗証番号生成部を活性化することによって、電子はんこの不正利用を防止できる効果がある。

## 【 図面の簡単な説明 】

50

## 【0019】

【図1】図1は、本発明の実施例による保安強化のための電子はんこシステムの構成を示したブロック図である。

【図2】図2は、本発明の実施例による電子はんこの構成を示したブロック図である。

【図3】図3は、本発明の他の実施例による電子はんこの構成を示したブロック図である。

【図4】図4は、本発明の実施例による端末の構成を示したブロック図である。

【図5】図5は、本発明の実施例による電子はんこサーバーの構成を示したブロック図である。

【図6】図6は、本発明の第一実施例による保安強化のための電子はんこシステムの制御方法を示した流れ図である。 10

【図7】図7は、本発明の第一実施例による保安強化のための電子はんこシステムの制御方法を示した流れ図である。

【図8】図8は、本発明の実施例による端末の画面を示した図である。

【図9】図9は、本発明の第二実施例による保安強化のための電子はんこシステムの制御方法を示した流れ図である。

【図10】図10は、本発明の第二実施例による保安強化のための電子はんこシステムの制御方法を示した流れ図である。

## 【発明を実施するための形態】

## 【0020】

本発明で使われる技術的用語は、ただ特定の実施例を説明するために使われたものであって、本発明を限定する意図ではないことを留意すべきである。また、本発明で使われる技術的用語は、本発明で特に異なる意味と定義されない限り、本発明の属する技術分野で通常の知識を有する者によって、一般的に理解される意味と解釈されるべきであって、過度に包括的な意味と解釈するか、過度に縮小された意味と解釈しないべきである。また、本発明で使われる技術的な用語が本発明の事象を正確に表現できない間違っただけの技術的用語である時には、当業者が正しく理解できる技術的用語と取り替えて理解するべきである。また、本発明で使われる一般的な用語は、事前に定義されているところによって、または、前後の文脈上によって解釈すべきであって、過度に縮小された意味と解釈しないべきである。 30

## 【0021】

また、本発明で使われる単数の表現は、文脈上、明らかに異なることを意味しない限り、複数の表現を含む。本発明で“構成する”、または、“含む”などの用語は、発明に記載の様々な構成要素等、または、様々な段階を必ず全部含むと解釈しないべきであり、そのうち、一部の構成要素等、または、一部の段階等は含まれないこともあり、または、追加的な構成要素、または、段階等をさらに含むことがあると解釈すべきである。

## 【0022】

また、本発明で使われる第一、第二などのように、序数を含む用語は、構成要素等を説明するに使われるが、構成要素等は用語等によって限定されてはいけない。用語等は、一つの構成要素を他の構成要素から区別する目的のみで使われる。例えば、本発明の権利範囲を外れないで、第一構成要素は、第二構成要素と命名されることができて、類似に第二構成要素も第一構成要素と命名されることができる。 40

## 【0023】

以下、添付の図面を参照して、本発明による好ましい実施例を詳しく説明し、図面符号に関係なく、同一か、類似な構成要素は、同一の参照番号を付与し、これにおける重複する説明は、省略する。

## 【0024】

また、本発明を説明するにおいて、関連の公知技術における具体的説明が本発明の要旨を濁すと判断される場合、その詳しい説明を省略する。また、添付の図面は、本発明の事象を容易に理解できるようにするためのものであるだけであって、添付の図面によって本 50

発明の事象が制限されると解釈されてはいけないことを留意すべきである。

【0025】

図1は、本発明の実施例による保安強化のための電子はんこシステム(10)の構成を示したブロック図である。

【0026】

図1に図示のように、保安強化のための電子はんこシステム(10)は、電子はんこ(100)と、端末(200)および電子はんこサーバー(300)とで構成する。図1に図示の電子はんこシステム(10)の構成要素の全てが必須構成要素であることではなく、図1に図示の構成要素より多い構成要素によって電子はんこシステム(10)が具現されることもあり、それより少ない構成要素によっても電子はんこシステム(10)が具現されることもある。

10

【0027】

端末(200)で特定のアプリが実行中の状態で、電子はんこ(100)の該端末(200)におけるタッチ動作が遂行される場合、電子はんこ(100)と端末(200)との近距離通信の機能を遂行する。以後、電子はんこ(100)は、端末(200)から転送される実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)と該電子はんこ(100)で生成されたOTPなどのような使い捨ての暗証番号に基づき、暗号化された値を生成し、生成された暗号化された値を該端末(200)に提供する。以後、端末(200)は、メンバーシップID、電子はんこ情報、暗号化された値などを電子はんこサーバー(300)に転送する。以後、電子はんこサーバー(300)は、電子はんこ情報から抽出された電子はんこIDに基づき、復号化キーを獲得した後、獲得した復号化キーに基づき、暗号化された値を復号化し、復号化した値とメンバーシップIDとの比較を通じて、電子はんこの真偽可否を確認する。以後、電子はんこサーバー(300)は、電子はんこの真偽可否における情報を端末(200)に提供する。

20

【0028】

電子はんこ(または、電子はんこ装置)(100)は、該電子はんこ(100)と関連する特定のアプリが設置された端末(200)に電子捺印(Electronic Stamping)の機能を提供する。

【0029】

図2に図示のように、電子はんこ(100)は、近距離通信部(110)と、使い捨ての暗証番号生成部(120)および暗号化部(130)とで構成する。図2に図示の電子はんこ(100)の構成要素全てが必須構成要素であることではなく、図2に図示の構成要素より多い構成要素によって電子はんこ(100)が具現されることもあり、それより少ない構成要素によっても電子はんこ(100)が具現されることもある。

30

【0030】

端末(200)で電子はんこ(100)を認識することができるアプリ(または、アプリケーション)が実行中の状態で、該端末(200)の静電式画面に該電子はんこ(100)が接触される場合、近距離通信部(または、電子はんこ通信部)(110)は、端末(200)と近距離通信を介して通信する。ここで、近距離通信の技術では、ブルートゥース(登録商標)(Bluetooth)、RFID(Radio Frequency Identification)、赤外線通信(Infrared Data Association: IrDA)、UWB(Ultra Wideband)、ジグビー(ZigBee)、近距離無線通信(Near Field Communication: NFC)、超音波通信(Ultra Sound Communication: USC)、可視光通信(Visible Light Communication: VLC)、ワイファイ(Wi-Fi(登録商標))、ワイファイダイレクト(Wi-Fi Direct)などが含まれることができる。

40

【0031】

即ち、電子はんこ(100)を介して、該端末(200)で実行中のアプリと関連して

50

スタンプ貯めの機能、電子はんこの職印の機能などを提供しようとする場合、近距離通信部(110)は、電子はんこ(100)の利用者の操作によって該電子はんこ(100)を該端末(200)の静電式画面に接触した後、端末(200)と近距離通信を介して連結する。

【0032】

また、近距離通信部(110)は、端末(200)から転送される該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、端末(200)の識別情報などを受信する。ここで、端末(200)の識別情報は、MDN(Mobile Directory Number)、モバイルIP、モバイルMAC、Sim(subscriber identity module:加入者識別モジュール)カード固有情報、シリアル番号などを含む。

10

【0033】

また、近距離通信部(110)は、暗号化部(130)を通じて生成された暗号化された値を該端末(200)に転送する。

【0034】

使い捨ての暗証番号生成部(または、OTP生成部)(120)は、OTP(One Time Password)などのような使い捨ての暗証番号を生成する。

【0035】

暗号化部(130)は、近距離通信部(110)を通じて受信したメンバーシップID(または、該端末(200)で実行中のアプリと関連するメンバーシップID/該端末(200)の利用者と関連するメンバーシップID)および使い捨ての暗証番号生成部(120)を通じて生成された使い捨ての暗証番号に基づき、暗号化された値を生成する。

20

【0036】

即ち、暗号化部(130)は、近距離通信部(110)を通じて受信したメンバーシップIDおよび使い捨ての暗証番号生成部(120)を通じて生成された使い捨ての暗証番号とを組み合わせる暗号化された値を生成する。

【0037】

図3に図示のように、電子はんこ(100)は、指紋認識部(140)と、電子はんこ通信部(110)と、使い捨ての暗証番号生成部(120)と、暗号化部(130)および電子はんこ制御部(150)とで構成する。図3に図示の電子はんこ(100)の構成要素全てが必須構成要素であることではなく、図3に図示の構成要素より多くの構成要素によって電子はんこ(100)が具現されることもあり、それより少ない構成要素によっても電子はんこ(100)が具現されることもある。

30

【0038】

指紋認識部(140)は、利用者の指紋を認識するためのセンサー(または、指紋認識センサー)で構成する。

【0039】

また、指紋認識部(140)は、該電子はんこ(100)を利用しようとする利用者の指紋を認識する。

【0040】

40

電子はんこ通信部(110)は、有/無線通信網を介して内部の任意の構成要素、または、外部の任意の少なくとも一つの端末と通信連結する。この時、外部の任意の端末は、端末(200)と、電子はんこサーバー(300)などを含むことができる。ここで、無線インターネット技術では、無線LAN(Wireless LAN: WLAN)、DLNA(登録商標)(Digital Living Network Alliance)、ワイブロ(Wireless Broadband: Wibro)、ワイマックス(World Interoperability for Microwave Access: Wimax)、HSDPA(High Speed Downlink Packet Access)、HSUPA(High Speed Uplink Packet Access)、IEEE 802.16、ロングタームエボリューション

50

ン(Long Term Evolution: LTE)、LTE-A(Long Term Evolution-Advanced)、広帯域無線移動通信サービス(Wireless Mobile Broadband Service: WMBS)などがあり、端末通信部(210)は、前記で羅列されないインターネット技術まで含んだ範囲で少なくとも一つの無線インターネット技術によってデータを送受信するようになる。また、近距離通信技術では、Bluetooth、RFID、赤外線通信(IrDA)、UWB、ジグビー、近距離無線通信(NFC)、超音波通信(USC)、可視光通信(VLC)、ワイファイ、ワイファイダイレクトなどが含まれることができる。また、有線通信技術では、電力線通信(Power Line Communication: PLC)、USB通信、イーサネット(登録商標)(Ethernet)、シリアル通信(serial communication)、光/同軸ケーブルなどが含まれることができる。

10

**【0041】**

また、電子はんこ通信部(110)は、ユニバーサルシリアルバス(Universal Serial Bus: USB)を通じて任意の端末と情報を相互転送することができる。

**【0042】**

また、電子はんこ通信部(110)は、移動通信のための技術標準等、または、通信方式(例えば、GSM(登録商標)(Global System for Mobile communication)、CDMA(Code Division Multi Access)、CDMA2000(Code Division Multi Access 2000)、EV-DO(Enhanced Voice-Data Optimized or Enhanced Voice-Data Only)、WCDMA(登録商標)(Wideband CDMA)、HSDPA(High Speed Downlink Packet Access)、HSUPA(High Speed Uplink Packet Access)、LTE(Long Term Evolution)、LTE-A(Long Term Evolution-Advanced)など)によって築かれた移動通信網上で基地局、端末(200)、電子はんこサーバー(300)などと無線信号を送受信する。

20

**【0043】**

また、電子はんこ通信部(110)は、電子はんこ制御部(150)の制御によって、指紋認識部(140)を通じて認識された指紋情報、電子はんこ情報(例えば、電子はんこIDなどを含む)などを電子はんこサーバー(300)に転送する。

30

**【0044】**

また、電子はんこ通信部(110)は、電子はんこ制御部(150)の制御によって、先に転送された指紋情報、電子はんこ情報などに応答して、電子はんこサーバー(300)から転送される指紋不一致の情報(または、認証失敗の情報)、指紋一致の情報(または、認証成功の情報)などを受信する。

**【0045】**

端末(200)で電子はんこ(100)を認識することができるアプリ(または、アプリケーション)が実行中の状態で、該端末(200)の静電式画面に該電子はんこ(100)が接触される場合、電子はんこ通信部(110)は、端末(200)と近距離通信を介して通信する。

40

**【0046】**

即ち、電子はんこ(100)を介して、該端末(200)で実行中のアプリと関連してスタンプ貯めの機能、電子はんこの職印の機能などを提供しようとする場合、電子はんこ通信部(110)は、電子はんこ(100)の利用者の操作によって該電子はんこ(100)を該端末(200)の静電式画面に接触した後、端末(200)と近距離通信を介して連結する。

**【0047】**

50

また、電子はんこ通信部(110)は、端末(200)から転送される該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、端末(200)の識別情報などを受信する。ここで、端末(200)の識別情報は、MDN(Mobile Directory Number)、モバイルIP、モバイルMAC、Sim(subscriber identity module:加入者識別モジュール)カード固有情報、シリアル番号などを含む。

【0048】

また、電子はんこ通信部(110)は、暗号化部(130)を通じて生成された暗号化された値を該端末(200)に転送する。

【0049】

使い捨ての暗証番号生成部(または、OTP生成部)(130)は、OTP(One Time Password)などのような使い捨ての暗証番号を生成する。

【0050】

この時、使い捨ての暗証番号生成部(120)は、電子はんこ制御部(150)の制御によって、電子はんこ通信部(110)を通じて受信した指紋一致の可否を示す情報によって、該使い捨ての暗証番号生成部(120)が活性化された状態である場合に、使い捨ての暗証番号を生成することができる。

【0051】

即ち、電子はんこ通信部(110)を通じて指紋不一致の情報(または、認証失敗の情報)を受信した場合、使い捨ての暗証番号生成部(120)は、該電子はんこ制御部(150)の制御によって非活性化状態を維持し、電子はんこ通信部(110)を介して端末(200)から転送される該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、端末(200)の識別情報などを受信しても、使い捨ての暗証番号を生成しない。

【0052】

また、電子はんこ通信部(110)を通じて指紋一致の情報(または、認証成功の情報)を受信した場合、使い捨ての暗証番号生成部(120)は、該電子はんこ制御部(150)の制御によって活性化状態を維持し、電子はんこ通信部(110)を介して端末(200)から転送される該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、端末(200)の識別情報などを受信する次第、使い捨ての暗証番号を生成する。

【0053】

また、使い捨ての暗証番号生成部(120)は、使い捨ての暗証番号を一回生成した後、活性化状態から非活性化状態に転換(または、維持)し、指紋認識部(140)を通じて電子はんこサーバー(300)との利用者認証の手順が再遂行された後に、再遂行された利用者認証の手順が成功した後、再度活性化状態を維持することができる。

【0054】

また、使い捨ての暗証番号生成部(120)は、電子はんこ制御部(150)の制御によって、最後に使い捨ての暗証番号を生成した後、予め設定された時間(例えば、5分)が経過する場合(または、最後に使い捨ての暗証番号を生成した後、設定された時間内に追加で使い捨ての暗証番号の生成機能が遂行されない場合)、活性化状態から非活性化状態に転換(または、維持)し、指紋認識部(140)を通じて電子はんこサーバー(300)との利用者認証の手順が再遂行された後に、再遂行された利用者認証の手順が成功した後、再度活性化状態を維持することができる。

【0055】

また、使い捨ての暗証番号生成部(120)は、電子はんこ制御部(150)の制御によって、最初に利用者認証の手順が成功した後、予め設定された回数(例えば、10回)ほど、使い捨ての暗証番号を生成した後、活性化状態から非活性化状態に転換(または、維持)し、指紋認識部(140)を通じて電子はんこサーバー(300)との利用者認証の手順が再遂行された後に、再遂行された利用者認証の手順が成功した後、再度活性化状

10

20

30

40

50

態を維持することができる。

【0056】

このように、使い捨ての暗証番号生成部(120)は、様々な条件によって活性化状態を維持することができる。

【0057】

暗号化部(130)は、電子はんこ通信部(110)を通じて受信したメンバーシップID(または、該端末(200)で実行中のアプリと関連するメンバーシップID/該端末(200)の利用者と関連するメンバーシップID)および使い捨ての暗証番号生成部(120)を通じて生成された使い捨ての暗証番号に基づき、暗号化された値を生成する。

10

【0058】

即ち、暗号化部(130)は、電子はんこ通信部(110)を通じて受信したメンバーシップIDおよび使い捨ての暗証番号生成部(120)を通じて生成された使い捨ての暗証番号を組み合わせて暗号化された値を生成する。

【0059】

電子はんこ制御部(150)は、電子はんこ(100)の全般的な制御機能を実行する。

【0060】

また、電子はんこ制御部(150)は、メモリ(未図示)に保存されたプログラムおよびデータを用いて、電子はんこ(100)の全般的な制御機能を実行する。電子はんこ制御部(150)は、RAMと、ROMと、CPUと、GPUと、バスとを含むことができ、RAM、ROM、CPU、GPUなどは、バスを介して互いに連結することができる。

20

【0061】

また、電子はんこ制御部(150)は、指紋認識部(140)を通じて認識された利用者の指紋情報、電子はんこ情報(電子はんこIDなどを含む)などを電子はんこ通信部(110)を介して電子はんこサーバー(300)に転送する。

【0062】

また、電子はんこ制御部(150)は、先に転送された利用者の指紋情報、電子はんこ情報(電子はんこIDなどを含む)などに応答して、電子はんこサーバー(300)から転送される該指紋情報が電子はんこサーバー(300)に予め登録した指紋情報と一致しない状態であることを示す指紋不一致の情報(または、認証の手順が失敗した状態であることを示す認証失敗の情報)、該指紋情報が電子はんこサーバー(300)に予め登録した指紋情報と一致する状態であることを示す指紋一致の情報(または、認証の手順が正常的に遂行された状態であることを示す認証成功の情報)などを電子はんこ通信部(110)を介して受信する。

30

【0063】

また、電子はんこ制御部(150)は、受信した該指紋情報における認証結果に基づき、使い捨ての暗証番号生成部(120)の活性化の可否を決定する。

【0064】

即ち、指紋一致の情報(または、認証成功の情報)を受信した場合、電子はんこ制御部(150)は、受信した指紋一致の情報に基づき、電子はんこを利用することができるように使い捨ての暗証番号生成部(120)を活性化する。

40

【0065】

また、指紋不一致の情報(または、認証失敗の情報)を受信した場合、電子はんこ制御部(150)は、受信した指紋不一致の情報に基づき、電子はんこを利用することができないように使い捨ての暗証番号生成部(120)を非活性化状態で維持する。

【0066】

端末(200)は、スマートフォン(Smart Phone)、携帯端末(Portable Terminal)、移動端末(Mobile Terminal)、携帯情

50

報端末 (Personal Digital Assistant: PDA)、PMP (Portable Multimedia Player) 端末、テレマティクス (Telematics) 端末、ナビゲーション (Navigation) 端末、パーソナルコンピュータ (Personal Computer)、ラップトップ、スレート PC (Slate PC)、タブレット PC (Tablet PC)、ウルトラブック (ultrabook)、ウェアラブルデバイス (Wearable Device、例えば、腕時計型端末 (Smartwatch)、メガネ型端末 (Smart Glass)、HMD (Head Mounted Display) などを含む)、ワイibro) 端末、IPTV (Internet Protocol Television) 端末、スマートテレビ、デジタル放送用端末、テレビジョン (Television)、3D 10  
テレビジョン、ホームシアター (Home Theater) システム、AVN (Audio Video Navigation) 端末、A/V (Audio/Video) システム、フレキシブル端末 (Flexible Terminal) などのような様々な端末に適用できる。

#### 【0067】

図4に図示のように、端末(200)は、端末通信部(210)と、端末保存部(220)と、端末表示部(230)と、端末音声出力部(240)および端末制御部(250)とで構成する。図4に図示の端末(200)の構成要素全てが必須構成要素であることではなく、図4に図示の構成要素より多くの構成要素によって端末(200)が具現されることもあり、それより少ない構成要素によっても端末(200)が具現されることもあ 20  
る。

#### 【0068】

端末通信部(210)は、有/無線通信網を介して内部の任意の構成要素、または、外部の任意の少なくとも一つの端末と通信連結する。この時、外部の任意の端末は、電子はんこ(100)と、電子はんこサーバー(300)などを含むことができる。ここで、無線インターネット技術では、無線LAN (Wireless LAN: WLAN)、DLNA (Digital Living Network Alliance)、ワイibro) (Wireless Broadband: Wibro)、ワイマックス (World Interoperability for Microwave Access: Wimax)、HSDPA (High Speed Downlink Packet 30  
Access)、HSUPA (High Speed Uplink Packet Access)、IEEE 802.16、ロングタームエボリューション (Long Term Evolution: LTE)、LTE-A (Long Term Evolution-Advanced)、広帯域無線移動通信サービス (Wireless Mobile Broadband Service: WMBs) などがあって、端末通信部(210)は、前記で羅列されないインターネット技術まで含んだ範囲で少なくとも一つの無線インターネット技術によってデータを送受信するようになる。また、近距離通信技術では、ブルートゥース、RFID、赤外線通信 (IrDA)、UWB、ジグビー、近距離無線通信 (NFC)、超音波通信 (USC)、可視光通信 (VLC)、ワイファイ、ワイファイダイレクトなどが含まれることができる。また、有線通信技術では、電力線 40  
通信 (Power Line Communication: PLC)、USB通信、イーサネット (Ethernet)、シリアル通信 (serial communication)、光/同軸ケーブルなどが含まれることができる。

#### 【0069】

また、端末通信部(210)は、ユニバーサルシリアルバス (Universal Serial Bus: USB) を通じて任意の端末と情報を相互転送することができる。

#### 【0070】

また、端末通信部(210)は、移動通信のための技術標準等、または、通信方式 (例えば、GSM (Global System for Mobile communication)、CDMA (Code Division Multi Access)、 50

CDMA2000 (Code Division Multi Access 2000)、EV-DO (Enhanced Voice-Data Optimized or Enhanced Voice-Data Only)、WCDMA (Wideband CDMA)、HSDPA (High Speed Downlink Packet Access)、HSUPA (High Speed Uplink Packet Access)、LTE (Long Term Evolution)、LTE-A (Long Term Evolution-Advanced) など) によって築かれた移動通信網上で基地局、電子はんこ(100)、電子はんこサーバー(300)などと無線信号を送受信する。

【0071】

また、端末(200)で電子はんこ(100)を認識することができるアプリ(または、アプリケーション)が実行中の状態で、端末表示部(230)の静電式画面に該電子はんこ(100)が接触される場合、端末通信部(210)は、端末制御部(250)の制御によって、電子はんこ(100)と近距離通信を介して連結(または、通信)する。

【0072】

また、端末通信部(210)は、端末制御部(250)の制御によって、該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、端末(200)の識別情報などを電子はんこ(100)に転送する。ここで、端末(200)の識別情報は、MDN、モバイルIP、モバイルMAC、SIMカード固有情報、シリアル番号などを含む。

【0073】

端末保存部(220)は、様々な利用者インターフェース(User Interface: UI)、グラフィック利用者インターフェース(Graphic User Interface: GUI)などを保存する。

【0074】

また、端末保存部(220)は、端末(200)が動作するのに必要なデータとプログラムなどを保存する。

【0075】

即ち、端末保存部(220)は、端末(200)で駆動する多数の応用プログラム(application program、または、アプリケーション)、端末(200)の動作のためのデータ等、命令語等を保存することができる。こういう応用プログラムのうち、少なくとも一部は、無線通信を介して外部サービス提供装置からダウンロードすることができる。また、こういう応用プログラムのうち、少なくとも一部は、端末(200)の基本的機能(例えば、電話着信、発信機能、メッセージ受信、発信機能)のために出庫当時から端末(200)上に存在することができる。一方、応用プログラムは、端末保存部(220)に保存され、端末(200)に設置され、端末制御部(250)によって端末(200)の動作(または、機能)を遂行するように駆動されることができる。

【0076】

また、端末保存部(220)は、フラッシュメモリタイプ(Flash Memory Type)、ハードディスクタイプ(Hard Disk Type)、マルチメディアカードマイクロタイプ(Multimedia Card Micro Type)、カードタイプのメモリ(例えば、SD、または、XDメモリなど)、磁気メモリ、磁気ディスク、光ディスク、ラム(Random Access Memory: RAM)、SRAM(Static Random Access Memory)、ROM(Read-Only Memory: ROM)、EEPROM(Electrically Erasable Programmable Read-Only Memory)、PROM(Programmable Read-Only Memory)のうち、少なくとも一つの保存媒体を含むことができる。また、端末(200)は、インターネット(internet)上で端末保存部(220)の保存機能を遂行するウェブストレージ(web storage)を運営するか、または、ウェブストレージと関連して動作す

10

20

30

40

50

ることできる。

【0077】

また、端末保存部(220)は、端末制御部(250)の制御によって該端末(200)に設置される(または、登録される)複数のアプリ(または、アプリケーション)と関連する情報を保存する。

【0078】

端末表示部(230)は、端末制御部(250)の制御によって端末保存部(220)に保存された利用者インターフェースおよび/または、グラフィック利用者インターフェースを用いて、様々なメニュー画面などのような様々なコンテンツを表示することができる。ここで、端末表示部(230)に表示されるコンテンツは、様々なテキスト、または、イメージデータ(各種情報データを含む)とアイコン、リストメニュー、コンボボックスなどのデータを含むメニュー画面などを含む。また、端末表示部(230)は、タッチスクリーンであることがある。

10

【0079】

また、端末表示部(230)は、液晶ディスプレイ(Liquid Crystal Display: LCD)、薄膜トランジスタ液晶ディスプレイ(Thin Film Transistor-Liquid Crystal Display: TFT LCD)、有機発光ダイオード(Organic Light-Emitting Diode: OLED)、フレキシブルディスプレイ(Flexible Display)、3次元ディスプレイ(3D Display)、電子インクディスプレイ(e-ink display)、LED(Light Emitting Diode)のうち、少なくとも一つを含むことができる。

20

また、端末表示部(230)は、立体映像を表示する立体ディスプレイ部で構成することができる。

【0080】

立体ディスプレイ部には、ステレオスコーピック方式(メガネ方式)、オートステレオスコーピック方式(無メガネ方式)、プロジェクション方式(ホログラフィック方式)などなどの3次元ディスプレイ方式を適用することができる。

【0081】

また、端末表示部(230)は、端末制御部(250)の制御によって、該端末(200)に予め設置された複数のアプリ媒体のうちから利用者の選択によって選ばれたアプリと関連するアプリ実行結果の画面を表示する。

30

【0082】

端末音声出力部(240)は、端末制御部(250)によって所定信号処理された信号に含まれた音声情報を出力する。ここで、端末音声出力部(240)には、レシーバー(receiver)、スピーカー(speaker)、ブザー(buzzer)などが含まれることができる。

【0083】

また、端末音声出力部(240)は、端末制御部(250)によって生成された案内音声出力する。

40

【0084】

また、端末音声出力部(240)は、端末制御部(250)の制御によって、該端末(200)に予め設置された複数のアプリ媒体のうちから利用者の選択によって選ばれたアプリと関連するアプリ実行結果に対応する音声情報を出力する。

【0085】

端末制御部(250)は、端末(200)の全般的な制御機能を実行する。

【0086】

また、端末制御部(250)は、端末保存部(220)に保存されたプログラムおよびデータを用いて、端末(200)の全般的な制御機能を実行する。端末制御部(250)は、RAMと、ROMと、CPUと、GPUと、バスとを含むことができ、RAM、R

50

OM、CPU、GPUなどは、バスを介して互いに連結することができる。CPUは、端末保存部(220)にアクセスし、端末保存部(220)に保存されたO/Sを用いて、ブートを遂行することができて、端末保存部(220)に保存された各種プログラム、コンテンツ、データなどを用いて様々な動作を遂行することができる。

また、端末制御部(250)は、複数のサービス提供装置(または、サーバー)(未図示)との連動によって、様々な種類のアプリ(または、アプリケーション)を端末(200)に設置(または、登録)する。

【0087】

また、端末制御部(250)は、該端末(200)に予め設置された複数のアプリ媒体のうち、利用者の選択による一つのアプリ(または、アプリケーション)を実行する。

10

【0088】

また、端末(200)で電子はんこ(100)を認識することができるアプリ(または、アプリケーション)が実行中の状態で、端末表示部(230)の静電式画面に電子はんこ(100)が接触(または、タッチ)される場合、端末制御部(250)は、端末通信部(210)を制御して、該電子はんこ(100)と近距離通信を介して連結(または、通信)する。

【0089】

また、端末制御部(250)は、該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、端末(200)の識別情報などを端末通信部(210)を介して電子はんこ(100)に転送する。

20

【0090】

また、端末制御部(250)は、先に転送された該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、端末(200)の識別情報などに応答して、電子はんこ(100)から転送される暗号化された値を端末通信部(210)を介して受信する。

【0091】

また、端末制御部(250)は、該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、電子はんこ情報、暗号化された値、端末(200)の識別情報などを端末通信部(210)を通じて電子はんこサーバー(300)に転送する。ここで、電子はんこ情報は、暗号化された値を復号するための復号化キーを生成するのに使われる電子はんこIDを含む。

30

【0092】

また、端末制御部(250)は、先に転送された該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、電子はんこ情報、暗号化された値、端末(200)の識別情報などに応答して、電子はんこサーバー(300)から転送される電子はんこの真偽可否における情報を端末通信部(210)を通じて受信する。

【0093】

また、端末制御部(250)は、受信した電子はんこの真偽可否における情報に基づき、該電子はんこと関連するスタンプ貯めの機能遂行の可否(または、電子はんこの職印の機能遂行の可否)を決定する。

40

【0094】

即ち、電子はんこが本物であると確認された場合、端末制御部(250)は、該電子はんこと関連するスタンプ貯めの機能、電子はんこの職印の機能などを遂行する。

【0095】

また、端末制御部(250)は、スタンプ貯めの機能遂行の結果(または、電子はんこの職印の機能遂行の結果)を端末表示部(230)および/または、端末音声出力部(240)を介して出力する。

【0096】

50

また、電子はんこが偽造されたものと確認された場合、端末制御部(250)は、該電子はんこに関連するスタンプ貯め(または、スタンプ貯めの機能/電子はんこの職印の機能)を中断し、電子はんこが偽造された状態であることを示す情報を端末表示部(230)および/または、端末音声出力部(240)を介して出力する。

【0097】

また、端末(200)は、該端末(200)に連結される全ての外部機器とのインターフェースの役割を遂行するインターフェース部(未図示)をさらに含むこともできる。例えば、インターフェース部は、有/無線ヘッドセットポート(Headset Port)、外部充電器ポート、有/無線データポート、メモリカード(Memory Card)ポート、識別モジュールを備える装置を連結するポート、オーディオI/O(Input/Output)ポート、ビデオI/O(Input/Output)ポート、イヤホンポートなどから構成することができる。ここで、識別モジュールは、端末(200)の使用権限を認証するための各種情報を保存したチップであり、利用者同定モジュール(User Identity Module: UIM)、加入者識別モジュール(Subscriber Identity Module: SIM)、ユニバーサル加入者同定モジュール(Universal Subscriber Identity Module: USIM)などを含むことができる。また、識別モジュールを備える装置は、スマートカード(Smart Card)の型式で製作されることができる。従って、識別モジュールは、ポートを介して端末(200)と連結することができる。このようなインターフェース部は、外部機器からデータを受信するか、電源を受信して端末(200)の内部の各構成要素に伝達するか、端末(200)の内部のデータが外部機器に転送されるようにする。

【0098】

また、インターフェース部は、端末(200)が外部クレイドル(Cradle)と連結される時、クレイドルからの電源が該端末(200)に供給される通路になるか、利用者によってクレイドルから入力される各種の命令信号が該端末(200)に伝達される通路になることができる。クレイドルから入力される各種の命令信号、または、該電源は、端末(200)がクレイドルに正確に装着されたことを認知するための信号で動作されることもできる。

【0099】

また、端末(200)は、利用者によるボタン操作、または、任意の機能の選択による信号を受信するか、ディスプレイされる画面をタッチ/スクロールするなどの操作によって生成された命令、または、制御信号を受信するための入力部(未図示)をさらに含むこともできる。

【0100】

入力部は、利用者の命令、選択、データ、情報のうち、少なくとも一つを入力されるための手段であり、数字、または、文字情報を入力され、様々な機能を設定するための多数の入力キーおよび機能キーを含むことができる。

【0101】

また、入力部は、キーパッド(Key Pad)、ドームスイッチ(Dome Switch)、タッチパッド(静圧/静電)、タッチスクリーン(Touch Screen)、ジョグホイール、ジョグスイッチ、ジョグシャトル(Jog Shuttle)、マウス(mouse)、スタイラスペン(Stylus Pen)、タッチペン(Touch Pen)などの様々な装置が使われる。特に、端末表示部(230)がタッチスクリーンの形で形成された場合、入力機能のうち、一部、または、全部は、端末表示部(230)を介して遂行されることができる。

【0102】

また、端末(200)の各々の構成部(または、モジュール)は、端末(200)のメモリ(または、端末保存部(220))上に保存されるソフトウェアであることがある。メモリは、端末(200)の内部メモリであることがあり、外付けメモリ、または、他の

10

20

30

40

50

形の保存装置であることがある。また、メモリは、不揮発性メモリであることがある。メモリ上に保存されるソフトウェアは、実行する時、端末(200)をして特定動作を遂行するようにする命令語セットを含むことができる。

【0103】

図5に図示のように、電子はんこサーバー(または、電子はんこ管理サーバー)(300)は、通信部(310)、保存部(320)、表示部(330)、音声出力部(340)および制御部(350)とで構成する。図5に図示の電子はんこサーバー(300)の構成要素全てが必須構成要素であることではなく、図5に図示の構成要素より多くの構成要素によって電子はんこサーバー(300)が具現されることもあり、それより少ない構成要素によっても電子はんこサーバー(300)が具現されることもある。

10

【0104】

通信部(310)は、有/無線通信網を介して内部の任意の構成要素、または、外部の任意の少なくとも一つの端末と通信連結する。この時、外部の任意の端末は、電子はんこ(100)、端末(200)などを含むことができる。ここで、無線インターネット技術では、無線LAN(WLAN)、DLNA、ワイプロ(Wibro)、ワイマックス(Wimax)、HSDPA、HSUPA、IEEE 802.16、ロングタームエボリューション(LTE)、LTE-A、広帯域無線移動通信サービス(WMBSS)などがあって、通信部(310)は、前記で羅列されないインターネット技術まで含んだ範囲で、少なくとも一つの無線インターネット技術によってデータを送受信するようになる。また、近距離通信技術では、ブルートゥース、RFID、赤外線通信(IrDA)、UWB、ジグビー、近距離無線通信(NFC)、超音波通信(USC)、可視光通信(VLC)、ワイファイ、ワイファイダイレクトなどが含まれることができる。また、有線通信技術では、電力線通信(PLC)、USB通信、イーサネット、シリアル通信、光/同軸ケーブルなどが含まれることができる。

20

【0105】

また、通信部(310)は、ユニバーサルシリアルバス(USB)を通じて任意の端末と情報を相互転送することができる。

【0106】

また、通信部(310)は、制御部(350)の制御によって、電子はんこ(100)から転送される指紋情報、電子はんこ情報(電子はんこIDなどを含む)などを受信する。

30

【0107】

また、通信部(310)は、制御部(350)の制御によって、端末(200)から転送される該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、電子はんこ情報、暗号化された値、端末(200)の識別情報などを受信する。

【0108】

保存部(320)は、様々な利用者インターフェース(UI)、グラフィック利用者インターフェース(GUI)などを保存する。

【0109】

また、保存部(320)は、電子はんこサーバー(300)が動作するのに必要なデータとプログラムなどを保存する。

40

【0110】

また、保存部(320)は、フラッシュメモリタイプ、ハードディスクタイプ、マルチメディアカードマイクロタイプ、カードタイプのメモリ(例えば、SD、または、XDメモリなど)、磁気メモリ、磁気ディスク、光ディスク、ラム(RAM)、SRAM、ROM、EEPROM、PROMのうち、少なくとも一つの保存媒体を含むことができる。また、電子はんこサーバー(300)は、インターネット上で保存部(320)の保存機能を遂行するウェブストレージを運営するか、または、ウェブストレージと関連して動作することもできる。

50

## 【 0 1 1 1 】

また、保存部（ 3 2 0 ）は、制御部（ 3 5 0 ）の制御によって、電子はんこ別に一つ以上の指紋情報を保存する。

## 【 0 1 1 2 】

また、保存部（ 3 2 0 ）は、制御部（ 3 5 0 ）の制御によって、通信部（ 3 1 0 ）を通じて受信した電子はんこ（ 1 0 0 ）から転送される指紋情報、電子はんこ情報（電子はんこIDなどを含む）などを保存する。

## 【 0 1 1 3 】

また、保存部（ 3 2 0 ）は、制御部（ 3 5 0 ）の制御によって、通信部（ 3 1 0 ）を通じて受信した該端末（ 2 0 0 ）で実行中のアプリと関連するメンバーシップID（または、該端末（ 2 0 0 ）の利用者と関連するメンバーシップID）、電子はんこ情報、暗号化された値、端末（ 2 0 0 ）の識別情報などを保存する。

10

## 【 0 1 1 4 】

表示部（ 3 3 0 ）は、制御部（ 3 5 0 ）の制御によって保存部（ 3 2 0 ）に保存された利用者インターフェースおよび/または、グラフィック利用者インターフェースを用いて、様々なメニュー画面などのような様々なコンテンツを表示することができる。ここで、表示部（ 3 3 0 ）に表示されるコンテンツは、様々なテキスト、または、イメージデータ（各種情報データを含む）とアイコン、リストメニュー、コンボボックスなどのデータを含むメニュー画面などを含む。また、表示部（ 3 3 0 ）は、タッチスクリーンであることがある。

20

## 【 0 1 1 5 】

また、表示部（ 3 3 0 ）は、液晶ディスプレイ（LCD）、薄膜トランジスタ液晶ディスプレイ（TFT LCD）、有機発光ダイオード（OLED）、フレキシブルディスプレイ、3次元ディスプレイ、電子インクディスプレイ、LEDのうち、少なくとも一つを含むことができる。

## 【 0 1 1 6 】

また、表示部（ 3 3 0 ）は、制御部（ 3 5 0 ）の制御によって、通信部（ 3 1 0 ）を介して受信した電子はんこ（ 1 0 0 ）から転送される指紋情報、電子はんこ情報（電子はんこIDなどを含む）などを表示する。

## 【 0 1 1 7 】

また、表示部（ 3 3 0 ）は、制御部（ 3 5 0 ）の制御によって、通信部（ 3 1 0 ）を介して受信した該端末（ 2 0 0 ）で実行中のアプリと関連するメンバーシップID（または、該端末（ 2 0 0 ）の利用者と関連するメンバーシップID）、電子はんこ情報、暗号化された値、端末（ 2 0 0 ）の識別情報などを表示する。

30

## 【 0 1 1 8 】

音声出力部（ 3 4 0 ）は、制御部（ 3 5 0 ）によって所定信号処理された信号に含まれた音声情報を出力する。ここで、音声出力部（ 3 4 0 ）には、レシーバー、スピーカー、ブザーなどが含まれることができる。

## 【 0 1 1 9 】

また、音声出力部（ 3 4 0 ）は、制御部（ 3 5 0 ）によって生成された案内音声を出力する。

40

## 【 0 1 2 0 】

また、音声出力部（ 3 4 0 ）は、制御部（ 3 5 0 ）の制御によって、通信部（ 3 1 0 ）を介して受信した該端末（ 2 0 0 ）で実行中のアプリと関連するメンバーシップID（または、該端末（ 2 0 0 ）の利用者と関連するメンバーシップID）、電子はんこ情報、暗号化された値、端末（ 2 0 0 ）の識別情報などに対応する音声情報を出力する。

## 【 0 1 2 1 】

制御部（ 3 5 0 ）は、電子はんこサーバー（ 3 0 0 ）の全般的な制御機能を実行する。

## 【 0 1 2 2 】

また、制御部（ 3 5 0 ）は、保存部（ 3 2 0 ）に保存されたプログラムおよびデータを

50

用いて、電子はんこサーバー（300）の全般的な制御機能を実行する。制御部（350）は、RAMと、ROMと、CPUと、GPUと、バスとを含むことができ、RAM、ROM、CPU、GPUなどは、バスを介して互いに連結することができる。CPUは、保存部（320）にアクセスし、保存部（320）に保存されたO/Sを用いて、ブートを遂行することができ、保存部（320）に保存された各種プログラム、コンテンツ、データなどを用いて様々な動作を遂行することができる。

【0123】

また、制御部（350）は、端末（200）から転送される該端末（200）で実行中のアプリと関連するメンバーシップID（または、該端末（200）の利用者と関連するメンバーシップID）、電子はんこ情報、暗号化された値、端末（200）の識別情報などを通信部（310）を介して受信する。

10

【0124】

また、制御部（350）は、受信した電子はんこ情報から電子はんこIDを抽出する。

【0125】

また、制御部（350）は、抽出された電子はんこIDに基づき、復号化キーを生成する。

【0126】

即ち、制御部（350）は、抽出された電子はんこIDから復号化キーを獲得する。

【0127】

また、制御部（350）は、生成された（または、獲得された）復号化キーに基づき、先に受信した暗号化された値を復号化する。

20

【0128】

また、制御部（350）は、復号化された値を先に受信したメンバーシップIDと比較して該電子はんこの真偽可否を確認（または、判断）する。

【0129】

また、制御部（350）は、確認された（または、判断された）電子はんこの真偽可否における情報を通信部（310）を介して端末（200）に転送する。ここで、電子はんこの真偽可否における情報は、電子はんこが本物であることを示す情報、または、電子はんこが偽造された状態であることを示す情報を含む。

【0130】

即ち、確認の結果（または、判断結果）、復号化した値がメンバーシップIDと同一である場合、制御部（350）は、電子はんこが本物であると確認して、電子はんこが本物であることを示す情報を通信部（310）を介して端末（200）に転送する。

30

【0131】

また、確認の結果（または、判断結果）、復号化した値がメンバーシップIDと異なる場合、制御部（350）は、電子はんこが偽造されたと確認して、電子はんこが偽造された状態であることを示す情報を通信部（310）を介して端末（200）に転送する。

【0132】

また、制御部（350）は、電子はんこ（100）から転送される指紋情報、電子はんこ情報（電子はんこIDなどを含む）などを通信部（310）を介して受信する。

40

【0133】

また、制御部（350）は、受信した指紋情報、電子はんこ情報などに基づいて該指紋情報における認証の手順を遂行する。

【0134】

即ち、制御部（350）は、該電子はんこ情報に対応して保存部（320）に予め登録した指紋情報と先に受信した指紋情報とが一致するかの可否を判断（または、確認）する。ここで、該電子はんこ情報に対応して予め登録した指紋情報は、一つ以上であることがある。

【0135】

判断結果（または、確認の結果）、該電子はんこ情報に対応して保存部（320）に予

50

め登録した指紋情報と先に受信した指紋情報とが一致しない場合（または、該電子はんこ情報に対応して電子はんこサーバー（300）に予め登録した複数の指紋情報のうち、先に受信した指紋情報と一致する指紋情報が存在しない場合）、制御部（350）は、該指紋情報が予め登録した指紋情報と一致しない状態であることを示す指紋不一致の情報（または、認証の手順が失敗した状態であることを示す認証失敗の情報）を通信部（310）を介して該電子はんこ（100）に転送する。

【0136】

また、判断結果（または、確認の結果）、該電子はんこ情報に対応して保存部（320）に予め登録した指紋情報と先に受信した指紋情報が一致する場合（または、該電子はんこ情報に対応して電子はんこサーバー（300）に予め登録した複数の指紋情報のうち、先に受信した指紋情報と一致する指紋情報が存在する場合）、制御部（350）は、該指紋情報が予め登録した指紋情報と一致する状態であることを示す指紋一致の情報（または、認証の手順が正常的に遂行された状態であることを示す認証成功の情報）を通信部（310）を介して該電子はんこ（100）に転送する。

10

【0137】

また、制御部（350）は、端末（200）から転送される該端末（200）で実行中のアプリと関連するメンバーシップID（または、該端末（200）の利用者と関連するメンバーシップID）、電子はんこ情報、暗号化された値、端末（200）の識別情報などを通信部（310）を介して受信する。

【0138】

また、制御部（350）は、受信した電子はんこ情報から電子はんこIDを抽出する。

20

【0139】

また、制御部（350）は、抽出された電子はんこIDに基づき、復号化キーを生成する。

【0140】

即ち、制御部（350）は、抽出された電子はんこIDから復号化キーを獲得する。

【0141】

また、制御部（350）は、生成された（または、獲得された）復号化キーに基づき、先に受信した暗号化された値を復号化する。

【0142】

また、制御部（350）は、復号化された値を先に受信したメンバーシップIDと比較して該電子はんこの真偽可否を確認（または、判断）する。

30

【0143】

また、制御部（350）は、確認された（または、判断された）電子はんこの真偽可否における情報を通信部（310）を介して端末（200）に転送する。ここで、電子はんこの真偽可否における情報は、電子はんこが本物であることを示す情報、または、電子はんこが偽造された状態であることを示す情報を含む。

【0144】

即ち、確認の結果（または、判断結果）、復号化した値がメンバーシップIDと同一である場合、制御部（350）は、電子はんこが本物であると確認して、電子はんこが本物であることを示す情報を通信部（310）を介して端末（200）に転送する。

40

【0145】

また、確認の結果（または、判断結果）、復号化した値がメンバーシップIDと異なる場合、制御部（350）は、電子はんこが偽造されたと確認して、電子はんこが偽造された状態であることを示す情報を通信部（310）を介して端末（200）に転送する。

【0146】

また、電子はんこサーバー（300）は、ウェブサーバー、データベースサーバー、プロキシサーバーなどの形で具現される。また、電子はんこサーバー（300）にはネットワーク負荷分散メカニズム、ないし電子はんこサーバー（300）がインターネット、または、異なるネットワーク上で動作できるようにする様々なソフトウェアのうち、一つ以

50

上が設置されることができて、これを介してコンピュータ化したシステムで具現されることができ、また、ネットワークは、httpネットワークであることがあって、専用回線(private line)、イントラネット、または、任意の異なるネットワークであることがある。さらには、電子はんこサーバー(300)と、端末(200)との連結は、データが任意のハッカー、または、異なる第三者による攻撃を受けないように、保安ネットワークに連結されることができ、また、電子はんこサーバー(300)は、複数のデータベースサーバーを含むことができ、このようなデータベースサーバーが分散データベースサーバーアーキテクチャをはじめとする任意の種類のネットワーク連結を通じて電子はんこサーバー(300)と別途で連結される方式で具現されることができ、

【0147】

10

また、本発明による電子はんこ(100)、端末(200)および電子はんこサーバー(300)に搭載されるプロセッサは、本発明による方法を実行するためのプログラム命令を処理することができる。一具現例で、このプロセッサは、シングルスレッド(single-threaded)のプロセッサであることがあり、他の具現例で本プロセッサは、マルチスレッド(multi-threaded)のプロセッサであることがある。さらに、本プロセッサは、メモリ、或いは、保存装置上に保存された命令を処理することができる。

【0148】

このように、電子はんこで端末から提供される端末の利用者と関連するメンバーシップIDと該電子はんこで生成するOTPなどのような使い捨ての暗証番号に基づき、暗号化された値を生成し、生成された暗号化された値を該端末に提供し、端末からメンバーシップID、電子はんこ情報、暗号化された値を電子はんこサーバーに提供し、電子はんこサーバーで電子はんこ情報から抽出された電子はんこIDに基づき、復号化キーを獲得した後、獲得した復号化キーに基づき、暗号化された値を復号化した後、復号化した値とメンバーシップIDとの比較を通じて、電子はんこの真偽可否を確認することができる。

20

【0149】

また、このように、電子はんこを操作できる権限のある者のみが電子はんこを動作させることができるように電子はんこを介して利用者の指紋を認識し、電子はんこサーバーで予め登録した該電子はんこにおける利用権限のある利用者の指紋と該電子はんこで認識した利用者の指紋との比較を通じて、一致する場合、該電子はんこの使い捨ての暗証番号を生成するための使い捨ての暗証番号生成部を活性化することができる。

30

以下では、本発明による保安強化のための電子はんこシステムの制御方法を図1ないし図10を参照して、詳しく説明する。

【0150】

図6および図7は、本発明の第一実施例による保安強化のための電子はんこシステムの制御方法を示した流れ図である。

【0151】

まず、端末(200)で電子はんこ(100)を認識することができるアプリ(または、アプリケーション)が実行中の状態で、該端末(200)の静電式画面に該電子はんこ(100)が接触される場合、端末(200)は、電子はんこ(100)と近距離通信を介して連結(または、通信)する。ここで、近距離通信技術では、ブルートゥース、RFID、赤外線通信(IrDA)、UWB、ジグビー、近距離無線通信(NFC)、超音波通信(USC)、可視光通信(VLC)、ワイファイ、ワイファイダイレクトなどが含まれることができる。

40

【0152】

即ち、電子はんこ(100)を介して、該端末(200)で実行中のアプリと関連してスタンプ貯めの機能、電子はんこの職印の機能などを提供しようとする場合、電子はんこ(100)は、該端末(200)の静電式画面に接触して端末(200)と近距離通信を介して連結する。

【0153】

50

一例として、第一端末(200)の利用者がコーヒー専門店を利用し、コーヒーなどを注文(または、決済)した後、該利用者に関連する第一端末から該コーヒー専門店と関連する第一コーヒーアプリを実行している状態で、該コーヒー専門店と関連する第一電子はんこ(100)を第一端末の画面に接触する時、第一電子はんこは、第一端末とBluetooth通信方式によって連結する(S610)。

【0154】

以後、端末(200)は、該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、端末(200)の識別情報などを電子はんこ(100)に転送する。ここで、端末(200)の識別情報は、MDN、モバイルIP、モバイルMAC、SIMカード固有情報、シリアル番号などを含む。

10

【0155】

一例として、第一端末は、第一端末から実行中の第一コーヒーアプリと関連するメンバーシップID、第一端末の識別情報などを第一電子はんこに転送する(S620)。

【0156】

以後、電子はんこ(100)は、端末(200)から転送される該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、端末(200)の識別情報などを受信する。

【0157】

また、電子はんこ(100)は、OTPなどのような使い捨ての暗証番号を生成する。

20

【0158】

一例として、第一電子はんこは、第一端末から転送される第一端末から実行中の第一コーヒーアプリと関連するメンバーシップID、第一端末の識別情報などを受信する。また、第一電子はんこは、第十一OTPを生成する(S630)。

【0159】

以後、電子はんこ(100)は、生成された使い捨ての暗証番号と先に受信したメンバーシップIDとを組み合わせて暗号化された値を生成する。

【0160】

また、電子はんこ(100)は、生成された暗号化された値を該端末(200)に転送する。

30

【0161】

一例として、第一電子はんこは、生成された第十一OTPと第一端末から実行中の第一コーヒーアプリと関連するメンバーシップIDとを組み合わせて暗号化された第十一値を生成する。また、第一電子はんこは、第十一値(または、暗号化された第十一値)を第一端末に転送する(S640)。

【0162】

以後、端末(200)は、先に転送された該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、端末(200)の識別情報などに応答して、電子はんこ(100)から転送される暗号化された値を受信する。

40

【0163】

また、端末(200)は、該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、電子はんこ情報、暗号化された値、端末(200)の識別情報などを電子はんこサーバー(300)に転送する。ここで、電子はんこ情報は、暗号化された値を復号するための復号化キーを生成するのに使われる電子はんこIDを含む。

【0164】

一例として、第一端末は、第一端末から実行中の第一コーヒーアプリと関連するメンバーシップID、第一端末の識別情報などに応答して、第一電子はんこから転送される第十一値(または、暗号化された第十一値)を受信する。

50

## 【 0 1 6 5 】

また、第一端末は、第一端末から実行中の第一コーヒアプリと関連するメンバーシップID、電子はんこ情報、第十一値（または、暗号化された第十一値）、第一端末の識別情報などを第一電子はんこサーバー（300）に転送する（S650）。

## 【 0 1 6 6 】

以後、電子はんこサーバー（300）は、端末（200）から転送される該端末（200）で実行中のアプリと関連するメンバーシップID（または、該端末（200）の利用者と関連するメンバーシップID）、電子はんこ情報、暗号化された値、端末（200）の識別情報などを受信する。

## 【 0 1 6 7 】

また、電子はんこサーバー（300）は、受信した電子はんこ情報から電子はんこIDを抽出する。

## 【 0 1 6 8 】

一例として、第一電子はんこサーバーは、第一端末から転送される第一端末から実行中の第一コーヒアプリと関連するメンバーシップID、電子はんこ情報、第十一値（または、暗号化された第十一値）、第一端末の識別情報などを受信する。

## 【 0 1 6 9 】

また、第一電子はんこサーバーは、受信した電子はんこ情報から第一電子はんこIDを抽出する（S660）。

## 【 0 1 7 0 】

また、電子はんこサーバー（300）は、抽出された電子はんこIDに基づき、復号化キーを生成する。

## 【 0 1 7 1 】

即ち、電子はんこサーバー（300）は、抽出された電子はんこIDから復号化キーを獲得する。

## 【 0 1 7 2 】

一例として、第一電子はんこサーバーは、抽出された第一電子はんこIDに基づき、第一復号化キーを生成する（S670）。

## 【 0 1 7 3 】

以後、電子はんこサーバー（300）は、生成された（または、獲得された）復号化キーに基づき、先に受信した暗号化された値を復号化する。

## 【 0 1 7 4 】

一例として、第一電子はんこサーバーは、生成された（または、獲得された）第一復号化キーに基づき、第十一値（または、暗号化された第十一値）を復号化して第二十一値（または、復号化された二十一値）を獲得する（S680）。

## 【 0 1 7 5 】

以後、電子はんこサーバー（300）は、復号化された値を先に受信したメンバーシップIDと比較して該電子はんこの真偽可否を確認（または、判断）する。

## 【 0 1 7 6 】

一例として、第一電子はんこサーバーは、第二十一値（または、復号化された二十一値）と第一端末から実行中の第一コーヒアプリと関連するメンバーシップIDが同一であるかの可否を確認する（S690）。

## 【 0 1 7 7 】

以後、電子はんこサーバー（300）は、確認された（または、判断された）電子はんこの真偽可否における情報を端末（200）に転送する。ここで、電子はんこの真偽可否における情報は、電子はんこが本物であることを示す情報、または、電子はんこが偽造された状態であることを示す情報を含む。

## 【 0 1 7 8 】

即ち、確認の結果（または、判断結果）、復号化した値がメンバーシップIDと同一である場合、電子はんこサーバー（300）は、電子はんこが本物であると確認して、電子

10

20

30

40

50

はんこが本物であることを示す情報を端末(200)に転送する。

【0179】

また、確認の結果(または、判断結果)、復号化した値がメンバーシップIDと異なる場合、電子はんこサーバー(300)は、電子はんこが偽造されたと確認して、電子はんこが偽造された状態であることを示す情報を端末(200)に転送する。

【0180】

一例として、第二十一値(または、復号化された第二十一値)と第一端末から実行中の第一コーヒアプリと関連するメンバーシップIDが同一である時、第一電子はんこサーバーは、電子はんこが本物であると確認し、電子はんこが本物であることを示す情報を第一端末に転送する。

10

【0181】

他の一例として、第二十一値(または、復号化された第二十一値)と第一端末から実行中の第一コーヒアプリと関連するメンバーシップIDが異なる時、第一電子はんこサーバーは、電子はんこが偽造されたと確認し、電子はんこが偽造された状態であることを示す情報を第一端末に転送する(S700)。

【0182】

以後、端末(200)は、先に転送された該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、電子はんこ情報、暗号化された値、端末(200)の識別情報などに応答して、電子はんこサーバー(300)から転送される電子はんこの真偽可否における情報を受信する。

20

【0183】

また、端末(200)は、受信した電子はんこの真偽可否における情報に基づき、該電子はんこと関連するスタンプ貯めの機能遂行の可否(または、電子はんこの職印の機能遂行の可否)を決定する。

【0184】

即ち、電子はんこが本物であると確認された場合、端末(200)は、該電子はんこと関連するスタンプ貯めの機能(または、電子はんこの職印の機能)を遂行し、スタンプ貯めの機能遂行の結果(電子はんこの職印の機能遂行の結果)を表示する。

【0185】

また、電子はんこが偽造されたものと確認された場合、端末(200)は、該電子はんこと関連するスタンプ貯め(または、スタンプ貯めの機能/電子はんこの職印の機能)を中断し、電子はんこが偽造された状態であることを示す情報を表示する。

30

【0186】

一例として、第一端末は、先に転送された第一端末から実行中の第一コーヒアプリと関連するメンバーシップID、電子はんこ情報、第十一値(または、暗号化された第十一値)、第一端末の識別情報などに応答して、第一電子はんこサーバーから転送される電子はんこが本物であることを示す情報を受信し、受信した電子はんこが本物であることを示す情報に基づき、該電子はんこを介する第一コーヒアプリのスタンプ貯めの機能を遂行し、図8に図示のように、第一コーヒアプリを介してスタンプが貯められた結果(810)を表示する。

40

【0187】

他の一例として、第一端末は、先に転送された第一端末から実行中の第一コーヒアプリと関連するメンバーシップID、電子はんこ情報、第十一値(または、暗号化された第十一値)、第一端末の識別情報などに応答して、第一電子はんこサーバーから転送される電子はんこが偽造された状態であることを示す情報を受信し、受信した電子はんこが偽造された状態であることを示す情報を第一コーヒアプリを介して表示する(S710)。

【0188】

図9および図10は、本発明の第二実施例による保安強化のための電子はんこシステムの制御方法を示した流れ図である。

50

## 【 0 1 8 9 】

まず、電子はんこ（ 1 0 0 ）は、該電子はんこ（ 1 0 0 ）を利用しようとする利用者の指紋を認識する。

## 【 0 1 9 0 】

また、電子はんこ（ 1 0 0 ）は、認識された指紋情報、電子はんこ情報（例えば、電子はんこIDなどを含む）などを電子はんこサーバー（ 3 0 0 ）に転送する。

## 【 0 1 9 1 】

一例として、コーヒー専門店と関連する第一電子はんこ（ 1 0 0 ）は、該第一電子はんこを利用しようとする該コーヒー専門店の管理者の指紋を認識する。

## 【 0 1 9 2 】

また、第一電子はんこは、認識された管理者の第一指紋情報、第一電子はんこのIDを含む電子はんこ情報などを第一電子はんこサーバー（ 3 0 0 ）に転送する（ S 9 1 0 ）。

## 【 0 1 9 3 】

以後、電子はんこサーバー（ 3 0 0 ）は、電子はんこ（ 1 0 0 ）から転送される指紋情報、電子はんこ情報（電子はんこIDなどを含む）などを受信する。

## 【 0 1 9 4 】

また、電子はんこサーバー（ 3 0 0 ）は、受信した指紋情報、電子はんこ情報などに基づいて該指紋情報における認証の手順を遂行する。

## 【 0 1 9 5 】

即ち、電子はんこサーバー（ 3 0 0 ）は、該電子はんこ情報に対応して電子はんこサーバー（ 3 0 0 ）に予め登録した指紋情報と先に受信した指紋情報とが一致するかの可否を判断（または、確認）する。ここで、該電子はんこ情報に対応して予め登録した指紋情報は、一つ以上であることがある。

## 【 0 1 9 6 】

一例として、第一電子はんこサーバーは、該電子はんこ情報に対応して該コーヒー専門店の複数の管理者と関連して登録された複数の指紋情報と第一電子はんこから転送された第一指紋情報とが一致するかの可否を確認する（ S 9 2 0 ）。

## 【 0 1 9 7 】

判断結果（または、確認の結果）、該電子はんこ情報に対応して電子はんこサーバー（ 3 0 0 ）に予め登録した指紋情報と先に受信した指紋情報とが一致しない場合（または、該電子はんこ情報に対応して電子はんこサーバー（ 3 0 0 ）に予め登録した複数の指紋情報のうち、先に受信した指紋情報と一致する指紋情報が存在しない場合）、電子はんこサーバー（ 3 0 0 ）は、該指紋情報が予め登録した指紋情報と一致しない状態であることを示す指紋不一致の情報（または、認証の手順が失敗した状態であることを示す認証失敗の情報）を該電子はんこ（ 1 0 0 ）に転送する。

## 【 0 1 9 8 】

一例として、該電子はんこ情報に対応して該コーヒー専門店の複数の管理者と関連して登録された複数の指紋情報のうち、第一電子はんこから転送される第一指紋情報と一致する指紋情報が存在しない時、第一電子はんこサーバーは、第一指紋情報が予め登録した指紋情報と一致しない状態であることを示す指紋不一致の情報（または、認証失敗の情報）を第一電子はんこに転送する（ S 9 3 0 ）。

## 【 0 1 9 9 】

以後、電子はんこ（ 1 0 0 ）は、先に転送された指紋情報、電子はんこ情報（電子はんこIDなどを含む）などに応答して、電子はんこサーバー（ 3 0 0 ）から転送される指紋不一致の情報（または、認証失敗の情報）を受信する。

## 【 0 2 0 0 】

また、電子はんこ（ 1 0 0 ）は、受信した指紋不一致の情報に基づき、該電子はんこ（ 1 0 0 ）内の使い捨ての暗証番号生成部（ 1 2 0 ）を非活性化状態で維持する。

## 【 0 2 0 1 】

一例として、第一電子はんこは、先に転送された管理者の第一指紋情報、第一電子はん

10

20

30

40

50

このIDを含む電子はんこ情報などに応答して、第一電子はんこサーバーから転送される指紋不一致の情報（または、認証失敗の情報）を受信し、受信した指紋不一致の情報に基づき、該第一電子はんこ内の使い捨ての暗証番号生成部（120）を非活性化状態で維持する（S940）。

【0202】

また、判断結果（または、確認の結果）、該電子はんこ情報に対応して電子はんこサーバー（300）に予め登録した指紋情報と先に受信した指紋情報が一致する場合（または、該電子はんこ情報に対応して電子はんこサーバー（300）に予め登録した複数の指紋情報のうち、先に受信した指紋情報と一致する指紋情報が存在する場合）、電子はんこサーバー（300）は、該指紋情報が予め登録した指紋情報と一致する状態であることを示す指紋一致の情報（または、認証の手順が正常的に遂行された状態であることを示す認証成功の情報）を該電子はんこ（100）に転送する。

10

【0203】

一例として、該電子はんこ情報に対応して該コーヒー専門店の複数の管理者と関連して登録された複数の指紋情報のうち、第一電子はんこから転送される第一指紋情報と一致する指紋情報が存在する時、第一電子はんこサーバーは、第一指紋情報が予め登録した指紋情報と一致する状態であることを示す指紋一致の情報（または、認証成功の情報）を第一電子はんこに転送する（S950）。

【0204】

以後、電子はんこ（100）は、先に転送された指紋情報、電子はんこ情報（電子はんこIDなどを含む）などに応答して、電子はんこサーバー（300）から転送される指紋一致の情報（または、認証成功の情報）を受信する。

20

【0205】

また、電子はんこ（100）は、受信した指紋一致の情報に基づき、電子はんこを利用することができるように電子はんこ（100）内の使い捨ての暗証番号生成部（120）を活性化する。

【0206】

一例として、第一電子はんこは、先に転送された管理者の第一指紋情報、第一電子はんこのIDを含む電子はんこ情報などに応答して、第一電子はんこサーバーから転送される指紋一致の情報（または、認証成功の情報）を受信し、受信した指紋一致の情報に基づき、第一電子はんこを利用するための待機状態で該第一電子はんこ内の使い捨ての暗証番号生成部（120）を活性化する（S960）。

30

【0207】

以後、端末（200）で電子はんこ（100）を認識することができるアプリ（または、アプリケーション）が実行中の状態で、該端末（200）の静電式画面に該電子はんこ（100）が接触される場合、端末（200）は、電子はんこ（100）と近距離通信を介して連結（または、通信）する。ここで、近距離通信技術では、ブルートゥース、RFID、赤外線通信（IrDA）、UWB、ジグビー、近距離無線通信（NFC）、超音波通信（USC）、可視光通信（VLC）、ワイファイ、ワイファイダイレクトなどが含まれることができる。

40

【0208】

即ち、電子はんこ（100）を介して、該端末（200）で実行中のアプリと関連してスタンプ貯めの機能、電子はんこの職印の機能などを提供しようとする場合、電子はんこ（100）は、該端末（200）の静電式画面に接触して端末（200）と近距離通信を介して連結する。

【0209】

一例として、第一端末の利用者がコーヒー専門店を利用してコーヒーなどを注文（または、決済）した後、該利用者に関連する第一端末から該コーヒー専門店と関連する第一コーヒーアプリを実行している状態で、該コーヒー専門店と関連する第一電子はんこを第一端末の画面に接触する時、第一電子はんこは、第一端末とブルートゥース通信方式によ

50

て連結する（S970）。

【0210】

以後、端末（200）は、該端末（200）で実行中のアプリと関連するメンバーシップID（または、該端末（200）の利用者と関連するメンバーシップID）、端末（200）の識別情報などを電子はんこ（100）に転送する。ここで、端末（200）の識別情報は、MDN、モバイルIP、モバイルMAC、SIMカード固有情報、シリアル番号などを含む。

【0211】

一例として、第一端末は、第一端末から実行中の第一コーヒアプリと関連するメンバーシップID、第一端末の識別情報などを第一電子はんこに転送する（S980）。 10

【0212】

以後、電子はんこ（100）は、端末（200）から転送される該端末（200）で実行中のアプリと関連するメンバーシップID（または、該端末（200）の利用者と関連するメンバーシップID）、端末（200）の識別情報などを受信する。

【0213】

また、電子はんこ（100）は、OTPのような使い捨ての暗証番号を生成する。この時、電子はんこ（100）は、先に受信した指紋一致の情報によって、該電子はんこ（100）内の使い捨ての暗証番号生成部（120）が活性化状態である場合、該使い捨ての暗証番号を生成することができる。また、電子はんこ（100）は、先に受信した指紋不一致の情報によって、該電子はんこ（100）内の使い捨ての暗証番号生成部（120）が非活性化状態である場合には、該使い捨ての暗証番号を生成することができない。 20

【0214】

一例として、第一電子はんこ内の使い捨ての暗証番号生成部（120）が非活性化状態である時、第一電子はんこは、第一端末から転送される第一端末から実行中の第一コーヒアプリと関連するメンバーシップID、第一端末の識別情報などを受信しても、OTPを生成しない。

【0215】

他の一例として、第一電子はんこ内の使い捨ての暗証番号生成部（120）が活性化状態である時、第一電子はんこは、第一端末から転送される第一端末から実行中の第一コーヒアプリと関連するメンバーシップID、第一端末の識別情報などを受信し、第十一OTPを生成する（S990）。 30

【0216】

以後、電子はんこ（100）は、生成された使い捨ての暗証番号と先に受信したメンバーシップIDとを組み合わせて暗号化された値を生成する。

【0217】

また、電子はんこ（100）は、生成された暗号化された値を該端末（200）に転送する。

【0218】

一例として、第一電子はんこは、生成された第十一OTPと第一端末から実行中の第一コーヒアプリと関連するメンバーシップIDとを組み合わせて暗号化された第十一値を生成する。また、第一電子はんこは、第十一値（または、暗号化された第十一値）を第一端末に転送する（S1000）。 40

【0219】

以後、端末（200）は、先に転送された該端末（200）で実行中のアプリと関連するメンバーシップID（または、該端末（200）の利用者と関連するメンバーシップID）、端末（200）の識別情報などに応答して、電子はんこ（100）から転送される暗号化された値を受信する。

【0220】

また、端末（200）は、該端末（200）で実行中のアプリと関連するメンバーシップID（または、該端末（200）の利用者と関連するメンバーシップID）、電子はん 50

こ情報、暗号化された値、端末(200)の識別情報などを電子はんこサーバー(300)に転送する。ここで、電子はんこ情報は、暗号化された値を復号するための復号化キーを生成するのに使われる電子はんこIDを含む。

【0221】

一例として、第一端末は、第一端末から実行中の第一コーヒーアプリと関連するメンバーシップID、第一端末の識別情報などに応答して、第一電子はんこから転送される第十一値(または、暗号化された第十一値)を受信する。

【0222】

また、第一端末は、第一端末から実行中の第一コーヒーアプリと関連するメンバーシップID、電子はんこ情報、第十一値(または、暗号化された第十一値)、第一端末の識別情報などを第一電子はんこサーバー(300)に転送する(S1010)。

10

【0223】

以後、電子はんこサーバー(300)は、端末(200)から転送される該端末(200)で実行中のアプリと関連するメンバーシップID(または、該端末(200)の利用者と関連するメンバーシップID)、電子はんこ情報、暗号化された値、端末(200)の識別情報などを受信する。

【0224】

また、電子はんこサーバー(300)は、受信した電子はんこ情報から電子はんこIDを抽出する。

【0225】

一例として、第一電子はんこサーバーは、第一端末から転送される第一端末から実行中の第一コーヒーアプリと関連するメンバーシップID、電子はんこ情報、第十一値(または、暗号化された第十一値)、第一端末の識別情報などを受信する。

20

【0226】

また、第一電子はんこサーバーは、受信した電子はんこ情報から第一電子はんこIDを抽出する(S1020)。

【0227】

以後、電子はんこサーバー(300)は、抽出された電子はんこIDに基づき、復号化キーを生成する。

【0228】

即ち、電子はんこサーバー(300)は、抽出された電子はんこIDから復号化キーを獲得する。

30

【0229】

一例として、第一電子はんこサーバーは、抽出された第一電子はんこIDに基づき、第一復号化キーを生成する(S1030)。

【0230】

以後、電子はんこサーバー(300)は、生成された(または、獲得された)復号化キーに基づき、先に受信した暗号化された値を復号化する。

【0231】

一例として、第一電子はんこサーバーは、生成された(または、獲得された)第一復号化キーに基づき、第十一値(または、暗号化された第十一値)を復号化して第二十一値(または、復号化された二十一値)を獲得する(S1040)。

40

【0232】

以後、電子はんこサーバー(300)は、復号化された値を先に受信したメンバーシップIDと比較して該電子はんこの真偽可否を確認(または、判断)する。

【0233】

一例として、第一電子はんこサーバーは、第二十一値(または、復号化された二十一値)と第一端末から実行中の第一コーヒーアプリと関連するメンバーシップIDが同一であるかの可否を確認する(S1050)。

【0234】

50

以後、電子はんこサーバー（300）は、確認された（または、判断された）電子はんこの真偽可否における情報を端末（200）に転送する。ここで、電子はんこの真偽可否における情報は、電子はんこが本物であることを示す情報、または、電子はんこが偽造された状態であることを示す情報を含む。

【0235】

即ち、確認の結果（または、判断結果）、復号化した値がメンバーシップIDと同一である場合、電子はんこサーバー（300）は、電子はんこが本物であると確認して、電子はんこが本物であることを示す情報を端末（200）に転送する。

【0236】

また、確認の結果（または、判断結果）、復号化した値がメンバーシップIDと異なる場合、電子はんこサーバー（300）は、電子はんこが偽造されたと確認して、電子はんこが偽造された状態であることを示す情報を端末（200）に転送する。

10

【0237】

一例として、第二十一値（または、復号化された第二十一値）と第一端末から実行中の第一コーヒアプリと関連するメンバーシップIDが同一である時、第一電子はんこサーバーは、電子はんこが本物であると確認し、電子はんこが本物であることを示す情報を第一端末に転送する。

【0238】

他の一例として、第二十一値（または、復号化された第二十一値）と第一端末から実行中の第一コーヒアプリと関連するメンバーシップIDが異なる時、第一電子はんこサーバーは、電子はんこが偽造されたと確認し、電子はんこが偽造された状態であることを示す情報を第一端末に転送する（S1060）。

20

【0239】

以後、端末（200）は、先に転送された該端末（200）で実行中のアプリと関連するメンバーシップID（または、該端末（200）の利用者と関連するメンバーシップID）、電子はんこ情報、暗号化された値、端末（200）の識別情報などに応答して、電子はんこサーバー（300）から転送される電子はんこの真偽可否における情報を受信する。

【0240】

また、端末（200）は、受信した電子はんこの真偽可否における情報に基づき、該電子はんこと関連するスタンプ貯めの機能遂行の可否（または、電子はんこの職印の機能遂行の可否）を決定する。

30

【0241】

即ち、電子はんこが本物であると確認された場合、端末（200）は、該電子はんこと関連するスタンプ貯めの機能（または、電子はんこの職印の機能）を遂行し、スタンプ貯めの機能遂行の結果（電子はんこの職印の機能遂行の結果）を表示する。

【0242】

また、電子はんこが偽造されたものと確認された場合、端末（200）は、該電子はんこと関連するスタンプ貯め（または、スタンプ貯めの機能/電子はんこの職印の機能）を中断し、電子はんこが偽造された状態であることを示す情報を表示する。

40

【0243】

一例として、第一端末は、先に転送された第一端末から実行中の第一コーヒアプリと関連するメンバーシップID、電子はんこ情報、第十一値（または、暗号化された第十一値）、第一端末の識別情報などに応答して、第一電子はんこサーバーから転送される電子はんこが本物であることを示す情報を受信し、受信した電子はんこが本物であることを示す情報に基づき、該電子はんこを介する第一コーヒアプリのスタンプ貯めの機能を遂行し、図8に図示のように、第一コーヒアプリを介してスタンプが貯められた結果（810）を表示する。

【0244】

他の一例として、第一端末は、先に転送された第一端末から実行中の第一コーヒアプリ

50

りと関連するメンバーシップID、電子はんこ情報、第十一値（または、暗号化された第十一値）、第一端末の識別情報などに応答して、第一電子はんこサーバーから転送される電子はんこが偽造された状態であることを示す情報を受信し、受信した電子はんこが偽造された状態であることを示す情報を第一コーヒアプリを介して表示する（S1070）。

【0245】

本発明の実施例による電子はんこ、端末、電子はんこサーバー、それを含むシステムは、コンピュータプログラムで作成できて、コンピュータプログラムを構成するコード等およびコードセグメント等は、当該分野のコンピュータプログラマーによって容易に推論できる。また、該コンピュータプログラムは、コンピュータが読み込める情報保存媒体（computer readable media）に保存され、コンピュータや本発明の実施例による電子はんこ、端末、電子はんこサーバーなどによって読み込まれ、実行されることによって電子はんこ、端末、電子はんこサーバー、それを含むシステムを具現することができる。

10

【0246】

情報保存媒体は、磁気記録媒体、光記録媒体およびキャリア波媒体を含む。本発明の実施例による電子はんこ、端末、電子はんこサーバー、それを含むシステムを具現するコンピュータプログラムは、電子はんこ、端末、電子はんこサーバーなどの内蔵メモリに保存および設置されることができる。または、本発明の実施例による電子はんこ、端末、電子はんこサーバー、それを含むシステムを具現するコンピュータプログラムを保存および設置したスマートカードなどの外付けメモリがインターフェースを介して電子はんこ、端末、電子はんこサーバー、それを含むシステムなどに装着されることもできる。

20

【0247】

本発明の実施例は、先に説明したように、電子はんこで端末から提供される端末の利用者と関連するメンバーシップIDと該電子はんこで生成するOTPなどのような使い捨ての暗証番号に基づき、暗号化された値を生成し、生成された暗号化された値を該端末に提供し、端末からメンバーシップID、電子はんこ情報、暗号化された値を電子はんこサーバーに提供し、電子はんこサーバーで電子はんこ情報から抽出された電子はんこIDに基づき、復号化キーを獲得した後、獲得した復号化キーに基づき、暗号化された値を復号化した後、復号化した値とメンバーシップIDとの比較を通じて、電子はんこの真偽可否を確認して、電子はんこの複製などを通じた不正利用を防ぐことができ、不適切なメンバーシップ特典の提供などによる経済的損失を防ぐことができる。

30

【0248】

また、本発明の実施例は、先に説明したように、電子はんこを操作できる権限のある者のみが電子はんこを動作させることができるように電子はんこを介して利用者の指紋を認識し、電子はんこサーバーで予め登録した該電子はんこにおける利用権限のある利用者の指紋と該電子はんこで認識した利用者の指紋との比較を通じて、一致する場合、該電子はんこの使い捨ての暗証番号を生成するための使い捨ての暗証番号生成部を活性化して、電子はんこの不正利用を防止することができる。

【0249】

前述の内容は、本発明の属する技術分野で通常の知識を有する者ならば、本発明の本質的特性から外れない範囲で修正および変形ができるはずである。従って、本発明に開示の実施例は、本発明の技術事象を限定するためのものではなく、説明するためのものであり、このような実施例によって本発明の技術事象の範囲が限定されることはない。本発明の保護範囲は、下の請求範囲によって解釈されるべきであり、それと同等の範囲内にある全ての技術事象は、本発明の権利範囲に含まれるものと解釈されるべきである。

40

【産業上の利用可能性】

【0250】

本発明は、電子はんこで端末から提供される端末の利用者と関連するメンバーシップIDと該電子はんこで生成するOTPなどのような使い捨ての暗証番号に基づき、暗号化さ

50

れた値を生成し、生成された暗号化された値を該端末に提供し、端末からメンバーシップID、電子はんこ情報、暗号化された値を電子はんこサーバーに提供し、電子はんこサーバーで電子はんこ情報から抽出された電子はんこIDに基づき、復号化キーを獲得した後、獲得した復号化キーに基づき、暗号化された値を復号化した後、復号化した値とメンバーシップIDとの比較を通じて、電子はんこの真偽可否を確認することによって、電子はんこの複製などを通じた不正利用を防ぐことができ、不適切なメンバーシップ特典の提供などによる経済的損失を防ぐことができるものであり、電子はんこ分野、端末分野、アプリ分野などで広範囲に用いられる。

【符号の説明】

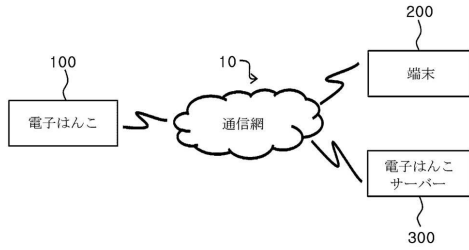
【0251】

- 10 電子はんこシステム
- 100 電子はんこ
- 110 近距離端末通信部 / 電子はんこ通信部
- 120 使い捨ての暗証番号生成部
- 130 暗号化部
- 140 指紋認識部
- 150 電子はんこ制御部
- 200 端末
- 210 端末通信部
- 220 端末保存部
- 230 端末表示部
- 240 端末音声出力部
- 250 端末制御部
- 300 電子はんこサーバー
- 310 通信部
- 320 保存部
- 330 表示部
- 340 音声出力部
- 350 制御部

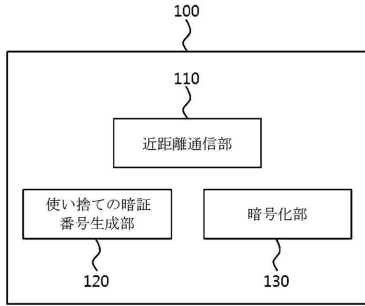
10

20

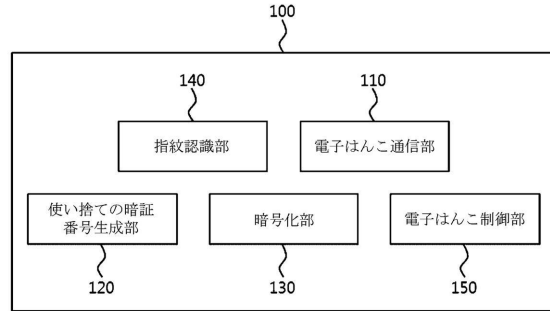
【図1】



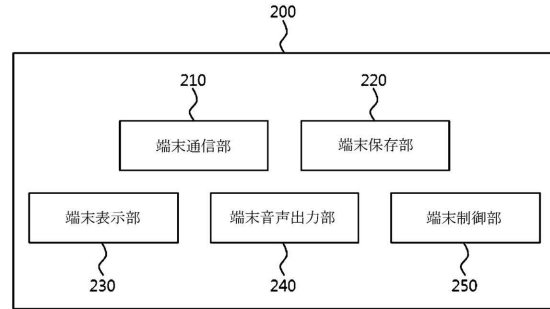
【図2】



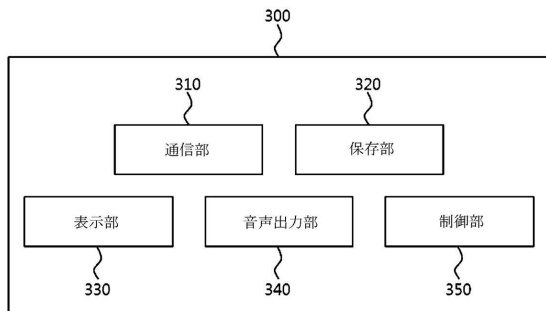
【図3】



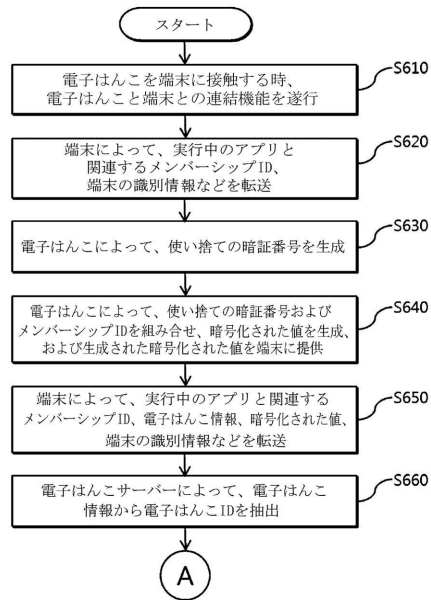
【図4】



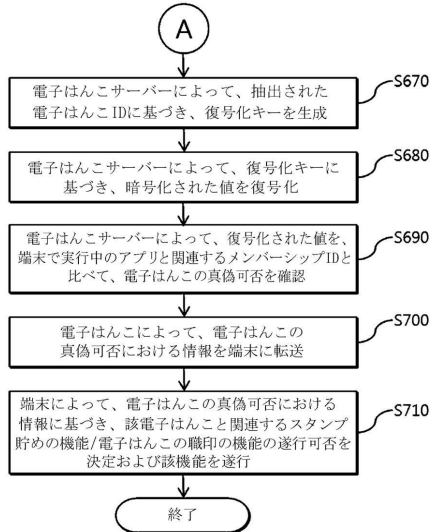
【図5】



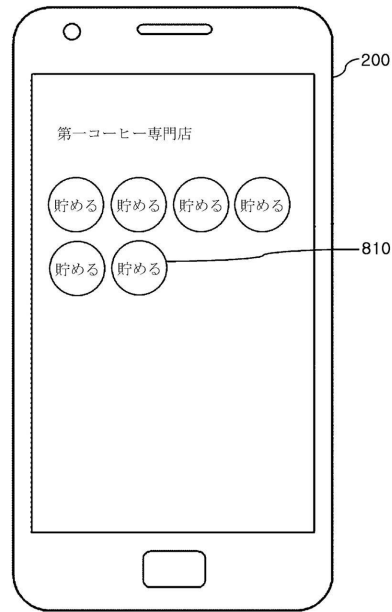
【図6】



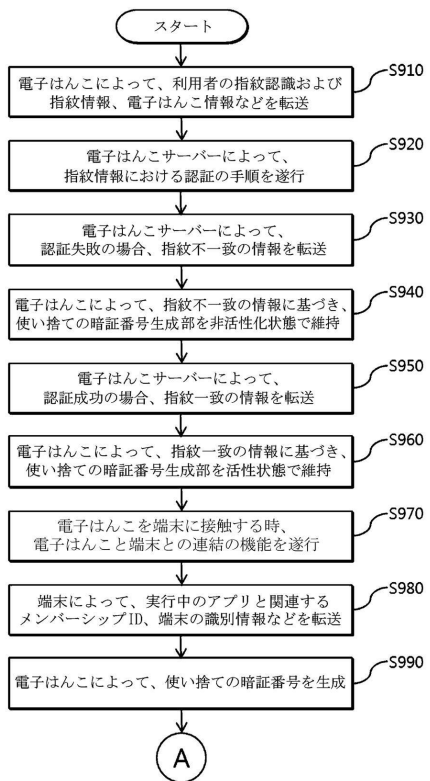
【図7】



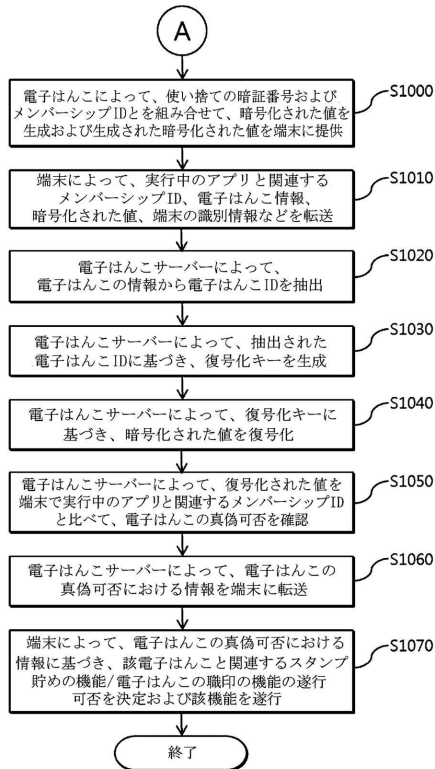
【図8】



【図9】



【図10】



---

フロントページの続き

審査官 児玉 崇晶

- (56)参考文献 特許第5908158(JP, B1)  
特許第5804398(JP, B2)  
特開2004-126889(JP, A)  
特開2001-142974(JP, A)  
特開2004-040209(JP, A)  
特開2004-214792(JP, A)

- (58)調査した分野(Int.Cl., DB名)
- |      |       |
|------|-------|
| H04L | 9/32  |
| G06F | 21/44 |
| G06F | 21/64 |
| H04L | 9/08  |