【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7年4月3日(2025.4.3)

【公開番号】特開2025-792(P2025-792A)
【公開日】令和7年1月7日(2025.1.7)
【年通号数】公開公報(特許)2025-002
【出願番号】特願2024-167710(P2024-167710)
【国際特許分類】
Ｈ０４Ｌ　9/32(2006.01)
Ｈ０４Ｌ　9/14(2006.01)
Ｇ０６Ｆ 21/60(2013.01)
Ｇ０６Ｆ 21/64(2013.01)
Ｇ０６Ｆ 21/35(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/32　２００Ａ
Ｈ０４Ｌ　9/14
Ｇ０６Ｆ 21/60　３６０
Ｇ０６Ｆ 21/64
Ｇ０６Ｆ 21/35

【手続補正書】
【提出日】令和7年3月25日(2025.3.25)
【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】
プロセッサと、
カウンタ値を記憶するメモリと、を備える非接触カードであって、
前記プロセッサは、
前記非接触カードと通信可能に結合されたサーバから、ユーザに関連する仲介デバイスを介して送信される非接触認証要求に応答して、カウンタ値を使用する第１の暗号文を作成し、前記カウンタ値が前記非接触認証要求に応答して更新され、
前記プロセッサは、
第１の暗号文を、前記仲介デバイスを介してサーバに送信して、１つまたは複数の機密ユーザデータレコードへのアクセスを許可し、
前記サーバによる前記第１の暗号文の検証時に、前記カウンタ値を使用して第２の暗号文を作成し、前記第２の暗号文は前記１つまたは複数の機密ユーザデータレコードを含み、前記仲介デバイスとの無線接続のエントリ後に前記カウンタ値が更新され、
前記プロセッサは、
前記仲介デバイスを介して、前記第２の暗号文を第３者のデータリクエスタに送信するように構成される、
非接触カード。
【請求項２】
前記メモリが秘密鍵を記憶し、
前記プロセッサが秘密鍵を使用して前記第１の暗号文を作成するようにさらに構成される、

請求項１に記載の非接触カード。
【請求項３】
前記１つまたは複数の機密ユーザデータレコードがブロックチェーンにおいて暗号化され、
前記メモリは、前記機密ユーザデータレコードを復号化するように構成された秘密鍵を記憶する、
請求項１に記載の非接触カード。
【請求項４】
前記１つまたは複数の機密ユーザデータレコーダはブロックチェーンに保存され、
前記非接触カードによる仲介デバイスとの無線接続へのエントリは、ブロックチェーントランザクションを承認する、
請求項１に記載の非接触カード。
【請求項５】
前記ブロックチェーントランザクションは、前記１つまたは複数の機密ユーザデータレコードを第３者のデータリクエスタに解放させる、
請求項４に記載の非接触カード。
【請求項６】
前記１つまたは複数の機密ユーザデータレコードは、１つまたは複数の資格情報に対応する、
請求項１に記載の非接触カード。
【請求項７】
前記１つまたは複数の資格情報は、年齢証明を含む、
請求項６に記載の非接触カード。
【請求項８】
前記１つまたは複数の資格情報は、処方薬の受け取りを許可する、
請求項６に記載の非接触カード。
【請求項９】
前記非接触認証要求は、所定のタイムアウト期間に関連付けられる、
請求項１に記載の非接触カード。
【請求項１０】
前記仲介デバイスとの無線接続のエントリは、前記仲介デバイスによって生成される通信フィールドへの非接触カードのジェスチャを含む、
請求項１に記載の非接触カード。
【請求項１１】
前記ジェスチャは、タップ、ウェーブ、およびスワイプのグループから選択される少なくとも１つを含む、
請求項１０に記載の非接触カード。
【請求項１２】
ユーザに関連する仲介デバイスを介して非接触カードと通信可能に結合されたサーバから送信される非接触認証要求に応答して、プロセッサとカウンタ値を記憶するメモリとを含む非接触カードが、カウンタ値を使用する第１の暗号文を作成することであって、前記カウンタ値が非接触認証要求に応答して更新される、ことと、
前記非接触カードが、前記仲介デバイスを介して前記サーバに第１の暗号文を送信して、１つまたは複数の機密ユーザデータレコードへのアクセスを許可し、
前記サーバによる前記第１の暗号文の検証時に、前記非接触カードが、前記カウンタ値を使用する第２の暗号文を作成することであって、前記第２の暗号文は前記１つまたは複数の機密ユーザデータレコードを含み、前記カウンタ値が前記仲介デバイスとの無線接続のエントリ後に更新される、ことと、
前記非接触カードが、前記仲介デバイスを介して前記第２の暗号文を第３者のデータリクエスタに送信することと、

を含む方法。
【請求項１３】
前記１つまたは複数の機密ユーザデータレコードは、財務情報、健康情報、および個人識別情報のグループから選択される少なくとも１つを含む、
請求項１２に記載の方法。
【請求項１４】
前記１つまたは複数の機微なユーザデータレコーダは、クラウドベースのストレージに保存される、
請求項１２に記載の方法。
【請求項１５】
前記１つまたは複数の機密ユーザデータレコードは、前記仲介デバイスの安全な要素に格納される、
請求項１４に記載の方法。
【請求項１６】
前記非接触認証要求は、所定のタイムアウト期間に関連付けられる、
請求項１２に記載の方法。
【請求項１７】
前記方法はさらに、
前記所定のタイムアウト期間の後に、前記サーバが前記非接触認証要求を無効にすることを含む、
請求項１６に記載の方法。
【請求項１８】
前記方法はさらに、
前記所定のタイムアウト期間の後に、前記サーバが前記非接触認証要求を延長することを含む、
請求項１６に記載の方法。
【請求項１９】
プロセッサと、カウンタ値を記憶するメモリとを備える非接触カードと、
プロセッサと、メモリとを備えるサーバと、
を備えるシステムであって、
前記サーバは、ユーザに関連する仲介デバイスを介して前記非接触カードと通信可能に結合され、
前記サーバは、非接触認証要求を非接触カードに送信するように構成され、
前記非接触カードは、
前記非接触認証要求に応答して、カウンタ値を使用して第１の暗号文を作成し、前記カウンタ値は非接触認証要求に応答して更新され、
前記非接触カードは、
前記仲介デバイスを介して前記第１の暗号文をサーバに送信して、１つまたは複数の機密ユーザデータレコードへのアクセスを許可し、
前記サーバによる前記第１の暗号文の検証時に、前記カウンタ値を使用して第２の暗号文を作成し、前記第２の暗号文は前記１つまたは複数の機密ユーザデータレコードを含み、前記カウンタ値は前記仲介デバイスとの無線接続のエントリ後に更新され、
前記非接触カードは、
前記第２の暗号文を、前記仲介デバイスを介して第３者のデータリクエスタに送信するように構成される、
システム。
【請求項２０】
前記サーバはさらに、前記１つまたは複数の機密ユーザデータレコードへのアクセスに対する前記第３者のデータリクエスタからのデータ要求に応答して生成された非接触認証要求に対応する要求を、前記仲介デバイスに送信するように構成される、

請求項１９に記載のシステム。