【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６部門第３区分
【発行日】令和1年8月8日(2019.8.8)

【公表番号】特表2018-521417(P2018-521417A)
【公表日】平成30年8月2日(2018.8.2)
【年通号数】公開・登録公報2018-029
【出願番号】特願2018-500295(P2018-500295)
【国際特許分類】
Ｇ０６Ｆ　21/32　(2013.01)
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　21/32
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｈ０４Ｌ　9/00　６７３Ｄ

【手続補正書】
【提出日】令和1年6月24日(2019.6.24)
【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】
識別認証システムにおいて、クライアントデバイスにより実行される、生体特徴に基づく安全性検証方法であって、
前記識別認証システムは、サーバを更に備え、
前記クライアントデバイスは、イネーブル記録を保存し、
前記イネーブル記録は、生体特徴検証に用いられ及び前記生体特徴検証を有効にする工程において取得される生体特徴テンプレートＩＤを含み、
前記安全性検証方法は：
認証リクエストを前記サーバへ送信するステップと；
前記サーバから認証リクエスト返信メッセージを受信するステップと；
ユーザによって入力される生体特徴を受信するステップと；
前記生体特徴に対応する生体特徴テンプレートＩＤを取得するステップと；
前記取得された生体特徴テンプレートＩＤを前記保存されたイネーブル記録内の前記生体特徴テンプレートＩＤと比較するステップと；
前記取得された生体特徴テンプレートＩＤと前記保存されたイネーブル記録内の前記生体特徴テンプレートＩＤが一致した場合、前記取得された生体特徴テンプレートＩＤを含む認証応答メッセージを生成するステップと；
前記認証応答メッセージを前記サーバへ送信するステップであって、その結果、前記サーバが前記認証応答メッセージを受信し、検証を実行する、前記送信するステップと；を備える、
安全性検証方法。
【請求項２】
前記生体特徴検証を有効にする前記工程は：
前記生体特徴検証を有効にするためのイネーブルリクエストを前記サーバへ送信し、前記サーバによって返されるイネーブルリクエスト返信メッセージを受信するステップと；
検証に用いられる、前記ユーザによって入力される前記生体特徴を受信するステップと

；
検証に用いられる、前記生体特徴に対応する前記生体特徴テンプレートＩＤを取得するステップと；
前記イネーブル記録を生成し、保存するステップと；
前記生体特徴テンプレートＩＤを含むイネーブル応答メッセージを生成するステップと；
前記イネーブル応答メッセージを前記サーバへ送信するステップであって、その結果、前記サーバが前記イネーブル応答メッセージを受信し、前記メッセージ内に含まれる前記生体特徴テンプレートＩＤを取得し、ユーザ記録を生成し保存する、前記送信するステップと；を備える、
請求項１に記載の安全性検証方法。
【請求項３】
前記サーバは、一致した第１の秘密鍵を用いて、前記認証リクエスト返信メッセージ又は前記イネーブルリクエスト返信メッセージに署名し、
前記クライアントデバイスが前記認証リクエスト返信メッセージを受信した後、前記安全性検証方法は：
一致した第１の公開鍵を用いて前記受信した認証リクエスト返信メッセージを検証するステップを更に備え、前記検証が成功した場合にのみ、後続の応答が行われ、そうでなければ、エラーが報告される；
又は、
前記クライアントデバイスが前記イネーブルリクエスト返信メッセージを受信した後、前記安全性検証方法は：
前記一致した第１の公開鍵を用いて前記受信したイネーブルリクエスト返信メッセージを検証するステップを更に備え、前記検証が成功した場合にのみ、後続の応答が行われ、そうでなければ、エラーが報告される；
請求項２に記載の安全性検証方法。
【請求項４】
前記イネーブルリクエスト返信メッセージは、チャレンジ値を有し、
前記生体特徴検証を有効にする前記工程は：
ユーザ秘密鍵及びユーザ公開鍵を備えるユーザ公開鍵・秘密鍵ペアを生成し、前記ユーザ秘密鍵を保存するステップと；
前記イネーブルリクエスト返信メッセージ内の前記チャレンジ値に従って署名アルゴリズムを選択し、前記選択された署名アルゴリズム及び一致した第２の秘密鍵を用いて前記生成されたイネーブル応答メッセージに署名し、次いで、前記署名されたイネーブル応答メッセージを前記サーバへ送信するステップと；を更に備え、
前記イネーブル応答メッセージは、前記ユーザ公開鍵を含み、その結果、前記サーバは、前記イネーブル応答メッセージを受信し、前記一致した第２の公開鍵を用いて前記イネーブル応答メッセージを検証し、前記ユーザ公開鍵は、前記サーバに保存される、
請求項２に記載の安全性検証方法。
【請求項５】
前記認証リクエスト返信メッセージは、チャレンジ値を有し、
前記安全性検証方法は：
前記チャレンジ値に従って署名アルゴリズムを選択し、前記選択された署名アルゴリズム及び前記ユーザ秘密鍵を用いて前記認証応答メッセージに署名するステップを更に備え、その結果、前記サーバもまた、前記認証応答メッセージを受信した後に前記チャレンジ値に従って署名アルゴリズムを選択し、前記署名アルゴリズム及び前記ユーザ公開鍵を用いて前記認証応答メッセージを検証する、
請求項４に記載の安全性検証方法。
【請求項６】
前記イネーブルリクエスト返信メッセージは、ユーザＩＤを更に含み、

前記クライアントデバイスが前記イネーブルリクエスト返信メッセージを受信した後、前記安全性検証方法は：

前記ユーザＩＤを前記イネーブル記録内に保存するステップであって、前記クライアントデバイスによって生成された前記イネーブル応答メッセージは、前記ユーザＩＤを更に含み、その結果、前記イネーブル応答メッセージを受信した後、前記サーバがその中の前記ユーザＩＤを取得し、前記ユーザＩＤを前記ユーザ記録内に保存する、前記保存するステップを更に備える、

請求項２に記載の安全性検証方法。

【請求項７】

前記イネーブル応答メッセージは、クライアントデバイスＩＤを更に含み、その結果、前記イネーブルリクエスト返信メッセージを受信した後、前記サーバは、その中の前記デバイスＩＤを取得し、前記デバイスＩＤを前記ユーザ記録内に保存する、

請求項６に記載の安全性検証方法。

【請求項８】

前記認証リクエスト返信メッセージは、前記ユーザＩＤを更に含み、

ユーザによって入力される生体特徴を受信し、

前記生体特徴に対応する生体特徴テンプレートＩＤを取得する前記ステップの後、前記安全性検証方法は：

前記取得された生体特徴テンプレートＩＤを、探し出すイネーブル記録内の前記生体特徴テンプレートＩＤと比較するために、前記ユーザＩＤに従って対応するイネーブル記録を検索するステップを更に備え、

前記クライアントデバイスによって生成された前記認証応答メッセージは、前記ユーザＩＤを更に含み、その結果、前記認証応答メッセージを受信した後、前記サーバは、その中の前記ユーザＩＤを取得し、前記ユーザＩＤに従って前記対応するユーザ記録を検索する、

請求項６に記載の安全性検証方法。

【請求項９】

前記認証応答メッセージは、前記クライアントデバイスＩＤを更に含み、その結果、前記認証応答メッセージを受信した後、前記サーバは、その中の前記デバイスＩＤを取得し、前記デバイスＩＤに従って前記対応するユーザ記録を検索する、

請求項７に記載の安全性検証方法。

【請求項１０】

識別認証システムにおいて、サーバにより実行される、生体特徴に基づく安全性検証方法であって、

前記識別認証システムは、クライアントデバイスを更に備え、

前記サーバは、ユーザ記録を保存し、

前記ユーザ記録は、生体特徴検証のために用いられ、前記生体特徴検証を有効にする工程において取得される生体特徴テンプレートＩＤを含み、

前記安全性検証方法は：

認証リクエストを前記クライアントデバイスから受信するステップと；

認証リクエスト返信メッセージを前記クライアントデバイスへ送信するステップと；

認証応答メッセージを前記クライアントデバイスから受信するステップであって、前記認証応答メッセージは、生体特徴テンプレートＩＤを含む、前記受信するステップと；

前記認証応答メッセージ内の前記生体特徴テンプレートＩＤを前記保存されたユーザ記録内の前記生体特徴テンプレートＩＤと比較することにより検証するステップであって、前記認証応答メッセージ内の前記生体特徴テンプレートＩＤと前記保存されたユーザ記録内の前記生体特徴テンプレートＩＤが一致した場合、前記検証に成功し、そうでなければエラーが報告される、前記検証するステップと；を備える、

安全性検証方法。

【請求項１１】

前記生体特徴検証を有効にする前記工程は：
前記生体特徴検証を有効にするためのイネーブルリクエストを前記クライアントデバイスから受信し、イネーブルリクエスト返信メッセージを前記クライアントデバイスへ送信するステップであって、その結果、前記クライアントデバイスが、検証のために用いられる、ユーザによって入力される生体特徴に従って、検証のために用いられる、前記生体特徴に対応する生体特徴テンプレートＩＤを取得し、イネーブル記録を生成し保存する、前記送信するステップと；
イネーブル応答メッセージを前記クライアントデバイスから受信し、前記イネーブル応答メッセージ内に含まれる前記生体特徴テンプレートＩＤを取得し、前記ユーザ記録を生成し、保存するステップと；を備える、
請求項１０に記載の安全性検証方法。
【請求項１２】
前記安全性検証方法は：
一致した第１の秘密鍵を用いて前記認証リクエスト返信メッセージ又は前記イネーブルリクエスト返信メッセージに署名するステップであって、その結果、
前記クライアントデバイスが一致した第１の公開鍵を用いて前記受信した認証リクエスト返信メッセージを検証し、後続の応答は、前記検証に成功する場合にのみ行われ、そうでなければ、エラーが報告される、又は、
前記クライアントデバイスが一致した第１の公開鍵を用いて前記受信したイネーブルリクエスト返信メッセージを検証し、後続の応答は、前記検証に成功する場合にのみ行われ、そうでなければ、エラーが報告される、前記署名するステップを更に備える、
請求項１１に記載の安全性検証方法。
【請求項１３】
前記イネーブルリクエスト返信メッセージは、チャレンジ値を有し、
前記クライアントデバイスは、ユーザ秘密鍵及びユーザ公開鍵を備えるユーザ公開鍵・秘密鍵ペアを生成し、前記ユーザ秘密鍵を保存し、
前記生体特徴検証を有効にする前記工程は：
選択された署名アルゴリズム及び一致した第２の秘密鍵を用いて、前記クライアントデバイスによって署名される前記イネーブル応答メッセージを受信するステップであって、前記署名アルゴリズムは、前記イネーブルリクエスト返信メッセージ内の前記チャレンジ値に従って前記クライアントデバイスによって選択され、前記イネーブル応答メッセージがユーザ公開鍵を含む、前記受信するステップと；
前記チャレンジ値に従って署名アルゴリズムを選択し、及び、第２の公開鍵を用いて前記イネーブル応答メッセージを検証するステップであって、前記ユーザ公開鍵は、前記サーバに保存される、前記検証するステップと；を更に備える、
請求項１１に記載の安全性検証方法。
【請求項１４】
前記安全性検証方法は：
選択された署名アルゴリズム及び前記ユーザ秘密鍵を用いて前記クライアントデバイスによって署名される前記認証応答メッセージを受信するステップであって、前記署名アルゴリズムは、前記認証リクエスト返信メッセージ内のチャレンジ値に従って前記クライアントデバイスによって選択される、前記受信するステップと；
前記チャレンジ値に従って署名アルゴリズムを選択し、及び、前記署名アルゴリズム及び前記ユーザ公開鍵を用いて前記認証応答メッセージの署名を検証するステップと；を更に備える、
請求項１３に記載の安全性検証方法。
【請求項１５】
前記イネーブルリクエスト返信メッセージは、ユーザＩＤを更に含み、その結果、前記クライアントデバイスは、前記イネーブルリクエスト返信メッセージを受信した後、前記ユーザＩＤを前記イネーブル記録内に保存し；

前記クライアントデバイスによって生成される前記イネーブル応答メッセージは、前記ユーザＩＤを更に含み；
前記サーバが前記イネーブル応答メッセージを受信した後、安全性検証方法は：
前記ユーザＩＤを前記イネーブル応答メッセージから取得し、前記ユーザＩＤを前記ユーザ記録内に保存するステップを更に備える、
請求項１１に記載の安全性検証方法。
【請求項１６】
前記イネーブル応答メッセージは、クライアントデバイスＩＤを更に含み、
前記サーバが前記イネーブル応答メッセージを受信した後、安全性検証方法は：
前記デバイスＩＤを前記イネーブル応答メッセージから取得し、前記デバイスＩＤを前記ユーザ記録内に保存するステップを更に備える、
請求項１５に記載の安全性検証方法。
【請求項１７】
前記認証リクエスト返信メッセージは、前記ユーザＩＤを更に含み、その結果、前記クライアントデバイスは、前記ユーザＩＤに従って前記対応するイネーブル記録を検索し、前記取得された生体特徴テンプレートＩＤを前記探し出したイネーブル記録内の前記生体特徴テンプレートＩＤと比較し；
前記クライアントデバイスによって生成される前記認証応答メッセージは、前記ユーザＩＤを更に含み；
前記サーバが前記認証応答メッセージを受信した後、前記安全性検証方法は：
前記ユーザＩＤを前記認証応答メッセージから取得し、前記ユーザＩＤに従って前記対応するユーザ記録を検索するステップを更に備える、
請求項１５に記載の安全性検証方法。
【請求項１８】
前記認証応答メッセージは、前記クライアントデバイスＩＤを更に含み、
前記サーバが前記認証応答メッセージを受信した後、前記安全性検証方法は：
前記デバイスＩＤを前記認証応答メッセージから取得し、前記デバイスＩＤに従って前記対応するユーザ記録を検索するステップを更に備える、
請求項１６に記載の安全性検証方法。
【請求項１９】
識別認証システムに適用されるクライアントデバイスであって、
前記識別認証システムは、サーバを更に備え、
前記クライアントデバイスは、イネーブル記録を保存し、
前記イネーブル記録は、生体特徴検証に用いられ及び前記生体特徴検証を有効にする工程において取得される生体特徴テンプレートＩＤを含み、
前記クライアントデバイスは：
請求項１～請求項９のいずれか１項に記載の方法に従って動作を実行するように構成された複数のモジュールを備える、
クライアントデバイス。
【請求項２０】
識別認証システムに適用されるサーバであって、
前記識別認証システムは、クライアントデバイスを更に備え、
前記サーバは、ユーザ記録を保存し、
前記ユーザ記録は、生体特徴検証に用いられ及び前記生体特徴検証を有効にする工程において取得される生体特徴テンプレートＩＤを含み、
前記サーバは：
請求項１０～請求項１８のいずれか１項に記載の方法に従って動作を実行するように構成された複数のモジュールを備える、
サーバ。
【手続補正２】

【補正対象書類名】明細書
【補正対象項目名】００９８
【補正方法】変更
【補正の内容】
【００９８】
前述の実施の形態は、単に、本発明の技術的解決策を説明するためだけに用いられており、本発明を制限する意図はない。当業者は、本発明の精神及び本質から逸脱することなく、本発明に従って様々な対応する修正及び変更を行うことができる。これらの対応する変更及び修正は、本発明の付帯する特許請求の範囲の保護範囲内に含まれる。
［第１の局面］
識別認証システムにおけるクライアント端末に適用される生体特徴に基づく安全性検証方法であって、前記識別認証システムは、サーバ端末を更に備え、前記クライアント端末はイネーブル記録を保存し、前記イネーブル記録は、生体特徴検証に用いられ及び前記生体特徴検証を有効にする工程において取得される生体特徴テンプレートＩＤを含み、前記安全性検証方法は：
認証リクエストを前記サーバ端末へ送信し、前記サーバ端末によって返される認証リクエスト返信メッセージを受信するステップと；
ユーザによって入力される生体特徴を受信し、前記生体特徴に対応する生体特徴テンプレートＩＤを取得し、前記取得された生体特徴テンプレートＩＤを前記保存されたイネーブル記録内の前記生体特徴テンプレートＩＤと比較し、前記２つの生体特徴テンプレートＩＤが一致すれば、前記取得された生体特徴テンプレートＩＤを含む認証応答メッセージを生成し、前記認証応答メッセージを前記サーバ端末へ送信するステップと：を備え、そのため、前記サーバ端末が前記認証応答メッセージを受信し、検証する、
安全性検証方法。
［第２の局面］
前記生体特徴検証を有効にする前記工程は：
前記生体特徴検証を有効にするためのイネーブルリクエストを前記サーバ端末へ送信し、前記サーバ端末によって返されるイネーブルリクエスト返信メッセージを受信するステップと；
検証に用いられ、前記ユーザによって入力される前記生体特徴を受信し、検証に用いられる前記生体特徴に対応する前記生体特徴テンプレートＩＤを取得し、且つ、前記イネーブル記録を生成し、保存するステップと；
前記生体特徴テンプレートＩＤを含むイネーブル応答メッセージを生成し、前記イネーブル応答メッセージを前記サーバ端末へ送信するステップと；を備え、そのため、前記サーバ端末が前記イネーブル応答メッセージを受信し、前記メッセージ内に含まれる前記生体特徴テンプレートＩＤを取得し、ユーザ記録を生成し、保存する、
第１の局面に記載の安全性検証方法。
［第３の局面］
前記サーバ端末は、一致した第１の秘密鍵を用いて、前記認証リクエスト返信メッセージ又は前記イネーブルリクエスト返信メッセージに署名し、
前記クライアント端末が前記認証リクエスト返信メッセージを受信した後、前記方法は：
一致した第１の公開鍵を用いて前記受信した認証リクエスト返信メッセージを検証するステップを更に備え、前記検証に成功した場合にのみ、後続の応答が行われ、そうでなければ、エラーが報告される；又は
前記クライアント端末が前記イネーブルリクエスト返信メッセージを受信した後、前記方法は：
前記一致した第１の公開鍵を用いて前記受信したイネーブルリクエスト返信メッセージを検証するステップを更に備え、前記検証が成功した場合にのみ、後続の応答が行われ、そうでなければ、エラーが報告される；

第２の局面に記載の安全性検証方法。
［第４の局面］
前記イネーブルリクエスト返信メッセージはチャレンジ値を有し、前記生体特徴検証を有効にする前記工程は：
ユーザ秘密鍵及びユーザ公開鍵を備えるユーザ公開鍵及び秘密鍵ペアを生成し、前記ユーザ秘密鍵を保存するステップと；
前記イネーブルリクエスト返信メッセージ内の前記チャレンジ値に従って署名アルゴリズムを選択し、前記選択された署名アルゴリズム及び一致した第２の秘密鍵を用いて前記生成されたイネーブル応答メッセージに署名し、次いで、前記署名されたイネーブル応答メッセージを前記サーバ端末へ送信するステップと；を更に備え、
前記イネーブル応答メッセージは、前記ユーザ公開鍵を含み、そのため、前記サーバ端末は、前記イネーブル応答メッセージを受信し、前記一致した第２の公開鍵を用いて前記イネーブル応答メッセージを検証し、前記ユーザ公開鍵は前記サーバ端末に保存される、
第２の局面に記載の安全性検証方法。
［第５の局面］
前記認証リクエスト返信メッセージはチャレンジ値を有し、前記安全性検証方法は：
前記チャレンジ値に従って署名アルゴリズムを選択し、前記選択された署名アルゴリズム及び前記ユーザ秘密鍵を用いて前記認証応答メッセージに署名するステップを更に備え、そのため、前記サーバ端末が、また、前記認証応答メッセージを受信した後に前記チャレンジ値に従って署名アルゴリズムを選択し、前記署名アルゴリズム及び前記ユーザ公開鍵を用いて前記認証応答メッセージを検証する、
第４の局面に記載の安全性検証方法。
［第６の局面］
前記イネーブルリクエスト返信メッセージは、ユーザＩＤを更に含み、
前記クライアント端末が前記イネーブルリクエスト返信メッセージを受信した後、前記安全性検証方法は：
前記ユーザＩＤを前記イネーブル記録内に保存するステップであって、前記クライアント端末によって生成された前記イネーブル応答メッセージは、前記ユーザＩＤを更に含む、保存するステップを更に備え、そのため、前記イネーブル応答メッセージを受信した後、前記サーバ端末がその中の前記ユーザＩＤを取得し、前記ユーザＩＤを前記ユーザ記録内に保存する、
第２の局面に記載の安全性検証方法。
［第７の局面］
前記イネーブル応答メッセージは、クライアント端末デバイスＩＤを更に含み、そのため、前記イネーブルリクエスト返信メッセージを受信した後、前記サーバ端末は、その中の前記デバイスＩＤを取得し、前記デバイスＩＤを前記ユーザ記録内に保存する、
第６の局面に記載の安全性検証方法。
［第８の局面］
前記認証リクエスト返信メッセージは、前記ユーザＩＤを更に含み、
ユーザによって入力される生体特徴を受信し、前記生体特徴に対応する生体特徴テンプレートＩＤを取得する前記ステップの後、前記安全性検証方法は：
前記取得された生体特徴テンプレートＩＤを、探し出すイネーブル記録内の前記生体特徴テンプレートＩＤと比較するために、前記ユーザＩＤに従って対応するイネーブル記録を検索するステップを更に備え、
前記クライアント端末によって生成された前記認証応答メッセージは、前記ユーザＩＤを更に含み、そのため、前記認証応答メッセージを受信した後、前記サーバ端末は、その中の前記ユーザＩＤを取得し、前記ユーザＩＤに従って前記対応するユーザ記録を検索する、
第６の局面に記載の安全性検証方法。
［第９の局面］

前記認証応答メッセージは、前記クライアント端末デバイスＩＤを更に含み、そのため、前記認証応答メッセージを受信した後、前記サーバ端末は、その中の前記デバイスＩＤを取得し、前記デバイスＩＤに従って前記対応するユーザ記録を検索する、
第７の局面に記載の安全性検証方法。
［第１０の局面］
識別認証システムにおけるサーバ端末に適用される生体特徴に基づく安全性検証方法であって、前記識別認証システムは、クライアント端末を更に備え、前記サーバ端末はユーザ記録を保存し、前記ユーザ記録は、生体特徴検証のために用いられ、前記生体特徴検証を有効にする工程において取得される生体特徴テンプレートＩＤを含み、前記安全性検証方法は：
認証リクエストを前記クライアント端末から受信し、認証リクエスト返信メッセージを前記クライアント端末へ送信するステップと；
認証応答メッセージを前記クライアント端末から受信するステップであって、前記認証応答メッセージは生体特徴テンプレートＩＤを含む、受信するステップと；
前記認証応答メッセージ内の前記生体特徴テンプレートＩＤを前記保存されたユーザ記録内の前記生体特徴テンプレートＩＤと比較し、前記２つの生体特徴テンプレートＩＤが一致すれば前記検証に成功し、そうでなければエラーが報告される、検証ステップと；を備える、
安全性検証方法。
［第１１の局面］
前記生体特徴検証を有効にする前記工程は：
前記生体特徴検証を有効にするためのイネーブルリクエストを前記クライアント端末から受信し、イネーブルリクエスト返信メッセージを前記クライアント端末へ送信するステップと、そのため、前記クライアント端末が、検証のために用いられ、ユーザによって入力される生体特徴に従って、検証のために用いられる前記生体特徴に対応する生体特徴テンプレートＩＤを取得し、イネーブル記録を生成し、保存し；
イネーブル応答メッセージを前記クライアント端末から受信し、前記イネーブル応答メッセージ内に含まれる前記生体特徴テンプレートＩＤを取得し、前記ユーザ記録を生成し、保存するステップと；を備える、
第１０の局面に記載の安全性検証方法。
［第１２の局面］
前記安全性検証方法は：
一致した第１の秘密鍵を用いて前記認証リクエスト返信メッセージ又は前記イネーブルリクエスト返信メッセージに署名するステップを更に備え、そのため、前記クライアント端末が一致した第１の公開鍵を用いて前記受信した認証リクエスト返信メッセージを検証し、後続の応答は、前記検証に成功する場合にのみ行われ、そうでなければ、エラーが報告される、又は、前記クライアント端末が一致した第１の公開鍵を用いて前記受信したイネーブルリクエスト返信メッセージを検証し、後続の応答は、前記検証に成功する場合にのみ行われ、そうでなければ、エラーが報告される、
第１１の局面に記載の安全性検証方法。
［第１３の局面］
前記イネーブルリクエスト返信メッセージはチャレンジ値を有し、前記クライアント端末は、ユーザ秘密鍵及びユーザ公開鍵を備えるユーザ公開鍵及び秘密鍵ペアを生成し、前記ユーザ秘密鍵を保存し、
前記生体特徴検証を有効にする前記工程は、以下のステップを更に備える：
選択された署名アルゴリズム及び一致した第２の秘密鍵を用いて、前記クライアント端末によって署名される前記イネーブル応答メッセージを受信するステップであって、前記署名アルゴリズムは、前記イネーブルリクエスト返信メッセージ内の前記チャレンジ値に従って前記クライアント端末によって選択され、前記イネーブル応答メッセージがユーザ公開鍵を含む、受信するステップと；前記チャレンジ値に従って署名アルゴリズムを選択

し、及び、第２の公開鍵を用いて前記イネーブル応答メッセージを検証するステップであって、前記ユーザ公開鍵は前記サーバ端末に保存される、検証するステップと；を更に備える、

第１１の局面に記載の安全性検証方法。

［第１４の局面］

前記安全性検証方法は：

選択された署名アルゴリズム及び前記ユーザ秘密鍵を用いて前記クライアント端末によって署名される前記認証応答メッセージを受信するステップであって、前記署名アルゴリズムは、前記認証リクエスト返信メッセージ内の前記チャレンジ値に従って前記クライアント端末によって選択される、受信するステップと；前記チャレンジ値に従って署名アルゴリズムを選択し、及び、前記署名アルゴリズム及び前記ユーザ公開鍵を用いて前記認証応答メッセージの署名を検証するステップと；を更に備える、

第１３の局面に記載の安全性検証方法。

［第１５の局面］

前記イネーブルリクエスト返信メッセージは、ユーザＩＤを更に含み；そのため、前記クライアント端末は、前記イネーブルリクエスト返信メッセージを受信した後、前記ユーザＩＤを前記イネーブル記録内に保存し；前記クライアント端末によって生成される前記イネーブル応答メッセージは、前記ユーザＩＤを更に含み；前記サーバ端末が前記イネーブル応答メッセージを受信した後、安全性検証方法は：

前記ユーザＩＤを前記イネーブル応答メッセージから取得し、前記ユーザＩＤを前記ユーザ記録内に保存するステップを更に備える、

第１１の局面に記載の安全性検証方法。

［第１６の局面］

前記イネーブル応答メッセージは、クライアント端末デバイスＩＤを更に含み、

前記サーバ端末が前記イネーブル応答メッセージを受信した後、安全性検証方法は：

前記デバイスＩＤを前記イネーブル応答メッセージから取得し、前記デバイスＩＤを前記ユーザ記録内に保存するステップを更に備える、

第１５の局面に記載の安全性検証方法。

［第１７の局面］

前記認証リクエスト返信メッセージは、前記ユーザＩＤを更に含み、そのため、前記クライアント端末は、前記ユーザＩＤに従って前記対応するイネーブル記録を検索し、前記取得された生体特徴テンプレートＩＤを前記探し出したイネーブル記録内の前記生体特徴テンプレートＩＤと比較し；前記クライアント端末によって生成される前記認証応答メッセージは、前記ユーザＩＤを更に含み；前記サーバ端末が前記認証応答メッセージを受信した後、前記安全性検証方法は：

前記ユーザＩＤを前記認証応答メッセージから取得し、前記ユーザＩＤに従って前記対応するユーザ記録を検索するステップを更に備える、

第１５の局面に記載の安全性検証方法。

［第１８の局面］

前記認証応答メッセージは、前記クライアント端末デバイスＩＤを更に含み、

前記サーバ端末が前記認証応答メッセージを受信した後、前記安全性検証方法は：

前記デバイスＩＤを前記認証応答メッセージから取得し、前記デバイスＩＤに従って前記対応するユーザ記録を検索するステップを更に備える、

第１６の局面に記載の安全性検証方法。

［第１９の局面］

識別認証システムに適用されるクライアント端末であって、前記識別認証システムは、サーバ端末を更に備え、前記クライアント端末はイネーブル記録を保存し、前記イネーブル記録は、生体特徴検証に用いられ、前記生体特徴検証を有効にする工程において取得される生体特徴テンプレートＩＤを含み、前記クライアント端末は：

認証リクエストを前記サーバ端末へ送信し、前記サーバ端末によって返される認証リク

エスト返信メッセージを受信するように構成されたリクエストモジュールと；
ユーザによって入力される生体特徴を受信し、前記生体特徴に対応する生体特徴テンプレートＩＤを取得し、前記取得された生体特徴テンプレートＩＤを前記保存されたイネーブル記録内の前記生体特徴テンプレートＩＤと比較し、前記２つの生体特徴テンプレートＩＤが一致した場合に前記生体特徴テンプレートＩＤを含む認証応答メッセージを生成し、前記認証応答メッセージを前記サーバ端末へ送信するように構成された応答モジュールとを備え、そのため、前記サーバ端末が前記認証応答メッセージを受信し、検証を行う；
クライアント端末。
［第２０の局面］
前記リクエストモジュールは、更に、前記生体特徴検証を有効にするためのイネーブルリクエストを前記サーバ端末へ送信し、前記サーバ端末によって返されるイネーブルリクエスト返信メッセージを受信するように構成され、前記応答モジュールは、更に、検証に用いられ、前記ユーザによって入力される前記生体特徴を受信し、検証に用いられる前記生体特徴に対応する前記生体特徴テンプレートＩＤを取得し、前記イネーブル記録を生成し、保存し、前記生体特徴テンプレートＩＤを含むイネーブル応答メッセージを生成し、前記イネーブル応答メッセージを前記サーバ端末へ送信するように構成され、そのため、前記サーバ端末が前記イネーブル応答メッセージを受信し、前記メッセージ内に含まれる前記生体特徴テンプレートＩＤを取得し、ユーザ記録を生成し、保存する、
第１９の局面に記載のクライアント端末。
［第２１の局面］
前記サーバ端末は、一致した第１の秘密鍵を用いて前記認証リクエスト返信メッセージ又は前記イネーブルリクエスト返信メッセージに署名し、
前記リクエストモジュールは、前記認証リクエスト返信メッセージを受信した後、更に、一致した第１の公開鍵を用いて前記受信した認証リクエスト返信メッセージを検証するように構成され、後続の応答は、前記検証が成功する場合にのみ行われ、そうでなければ、エラーが報告される、又は
前記リクエストモジュールは、前記イネーブルリクエスト返信メッセージを受信した後、更に、前記一致した第１の公開鍵を用いて前記受信したイネーブルリクエスト返信メッセージを検証するように構成され、後続の応答は、前記検証が成功する場合にのみ行われ、そうでなければ、エラーが報告される、
第２０の局面に記載のクライアント端末。
［第２２の局面］
前記イネーブルリクエスト返信メッセージはチャレンジ値を有し、前記応答モジュールは、更に、ユーザ秘密鍵及びユーザ公開鍵を含むユーザ公開鍵及び秘密鍵ペアを生成し、前記ユーザ秘密鍵を保存し、前記イネーブルリクエスト返信メッセージ内の前記チャレンジ値に従って署名アルゴリズムを選択し、前記選択された署名アルゴリズム及び一致した第２の秘密鍵を用いて前記生成されたイネーブル応答メッセージに署名し、次いで、前記署名されたイネーブル応答メッセージを前記サーバ端末へ送信するように構成され、前記イネーブル応答メッセージは前記ユーザ公開鍵を含み、そのため、前記サーバ端末は、前記イネーブル応答メッセージを受信し、前記一致した第２の公開鍵を用いて前記イネーブル応答メッセージを検証し、前記ユーザ公開鍵は前記サーバ端末に保存される、
第２０の局面に記載のクライアント端末。
［第２３の局面］
前記認証リクエスト返信メッセージはチャレンジ値を有し、前記応答モジュールは、更に、前記チャレンジ値に従って署名アルゴリズムを選択し、前記選択された署名アルゴリズム及び前記ユーザ秘密鍵を用いて前記認証応答メッセージに署名するように構成され、そのため、前記サーバ端末が、また、前記認証応答メッセージを受信した後に前記チャレンジ値に従って署名アルゴリズムを選択し、前記署名アルゴリズム及び前記ユーザ公開鍵を用いて前記認証応答メッセージを検証する、
第２２の局面に記載のクライアント端末。

［第２４の局面］
前記イネーブルリクエスト返信メッセージは、ユーザＩＤを更に含み、前記応答モジュールは、更に前記ユーザＩＤを前記イネーブル記録内に保存するように構成され、前記生成されたイネーブル応答メッセージは、前記ユーザＩＤを更に含み、そのため、前記イネーブル応答メッセージを受信した後、前記サーバ端末は、その中の前記ユーザＩＤを取得し、前記ユーザＩＤを前記ユーザ記録内に保存する、
第２０の局面に記載のクライアント端末。
［第２５の局面］
前記イネーブル応答メッセージは、クライアント端末デバイスＩＤを更に含み、そのため、前記イネーブルリクエスト返信メッセージを受信した後、前記サーバ端末は、その中の前記デバイスＩＤを取得し、前記デバイスＩＤを前記ユーザ記録内に保存する、
第２４の局面に記載のクライアント端末。
［第２６の局面］
前記認証リクエスト返信メッセージは、前記ユーザＩＤを更に含み、前記ユーザによって入力される前記生体特徴を受信し、前記生体特徴に対応する前記生体特徴テンプレートＩＤを取得した後、前記応答モジュールは、更に、前記取得された生体特徴テンプレートＩＤを、探し出すイネーブル記録内の前記生体特徴テンプレートＩＤと比較するために、前記ユーザＩＤに従って前記対応するイネーブル記録を検索するように構成され、
前記応答モジュールによって生成された前記認証応答メッセージは、前記ユーザＩＤを更に含み、そのため、前記認証応答メッセージを受信した後、前記サーバ端末は、その中の前記ユーザＩＤを取得し、前記ユーザＩＤに従って前記対応するユーザ記録を検索する、
第２４の局面に記載のクライアント端末。
［第２７の局面］
前記認証応答メッセージは、クライアント端末デバイスＩＤを更に含み、そのため、前記認証応答メッセージを受信した後、前記サーバ端末は、その中の前記デバイスＩＤを取得し、前記デバイスＩＤに従って前記対応するユーザ記録を検索する、
第２６の局面に記載のクライアント端末。
［第２８の局面］
識別認証システムに適用されるサーバであって、前記識別認証システムは、クライアント端末を更に備え、前記サーバはユーザ記録を保存し、前記ユーザ記録は、生体特徴検証のために用いられ、前記生体特徴検証を有効にする工程において取得される生体特徴テンプレートＩＤを含み、前記サーバは：
認証リクエストを前記クライアント端末から受信し、認証リクエスト返信メッセージを前記クライアント端末へ送信するように構成された返信モジュールと；
認証応答メッセージを前記クライアント端末から受信し、前記認証応答メッセージは生体特徴テンプレートＩＤを含み、前記認証応答メッセージ内の前記生体特徴テンプレートＩＤを前記保存されたユーザ記録内の前記生体特徴テンプレートＩＤと比較することによって検証し、前記２つの生体特徴テンプレートＩＤが一致した場合に前記検証は成功し、そうでなければ、エラーが報告されるように構成された検証モジュールと；を備える、
サーバ。
［第２９の局面］
前記返信モジュールは、更に、前記生体特徴検証を有効にするためのイネーブルリクエストを前記クライアント端末から受信し、イネーブルリクエスト返信メッセージを前記クライアント端末へ送信するように構成され、そのため、前記クライアント端末が、検証のために用いられ、ユーザによって入力される生体特徴に従って、検証のために用いられる前記生体特徴に対応する生体特徴テンプレートＩＤを取得し、イネーブル記録を生成し、保存し；前記検証モジュールは、更に、イネーブル応答メッセージを前記クライアント端末から受信し、前記イネーブル応答メッセージ内に備えられる前記生体特徴テンプレートＩＤを取得し、前記ユーザ記録を生成し、保存するように構成された、

第２８の局面に記載のサーバ。
［第３０の局面］
前記返信モジュールは、更に、一致した第１の秘密鍵を用いて前記認証リクエスト返信メッセージ又は前記イネーブルリクエスト返信メッセージに署名するように構成され、そのため、前記クライアント端末が一致した第１の公開鍵を用いて前記受信した認証リクエスト返信メッセージを検証し、後続の応答は、前記検証が成功する場合にのみ行われ、そうでなければ、エラーが報告される、又は、前記クライアント端末が一致した第１の公開鍵を用いて前記受信したイネーブルリクエスト返信メッセージを検証し、後続の応答は、前記検証が成功する場合にのみ行われ、そうでなければ、エラーが報告される、
第２９の局面に記載のサーバ。
［第３１の局面］
前記イネーブルリクエスト返信メッセージはチャレンジ値を有し、前記クライアント端末は、ユーザ秘密鍵及びユーザ公開鍵を含むユーザ公開鍵及び秘密鍵ペアを生成し、前記ユーザ秘密鍵を保存し；前記検証モジュールは、更に、選択された署名アルゴリズム及び一致した第２の秘密鍵を用いて前記クライアント端末によって署名される前記イネーブル応答メッセージを受信するように構成され、前記署名アルゴリズムは、前記イネーブルリクエスト返信メッセージ内の前記チャレンジ値に従って前記クライアント端末によって選択され、前記イネーブル応答メッセージはユーザ公開鍵を含み；また、前記チャレンジ値に従って署名アルゴリズムを選択し、第２の公開鍵を用いて前記イネーブル応答メッセージを検証し、前記ユーザ公開鍵を保存するように構成された、
第２９の局面に記載のサーバ。
［第３２の局面］
前記検証モジュールは、更に、選択された署名アルゴリズム及び前記ユーザ秘密鍵を用いて前記クライアント端末によって署名される前記認証応答メッセージを受信するように構成され、前記署名アルゴリズムは、前記認証リクエスト返信メッセージ内の前記チャレンジ値に従って前記クライアント端末によって選択され；また、前記チャレンジ値に従って署名アルゴリズムを選択し、前記署名アルゴリズム及び前記ユーザ公開鍵を用いて前記認証応答メッセージの署名を検証するように構成された、
第３１の局面に記載のサーバ。
［第３３の局面］
前記イネーブルリクエスト返信メッセージは、ユーザＩＤを更に含み；そのため、前記クライアント端末は、前記イネーブルリクエスト返信メッセージを受信した後、前記ユーザＩＤを前記イネーブル記録内に保存し；前記クライアント端末によって生成される前記イネーブル応答メッセージは、前記ユーザＩＤを更に含み；前記イネーブル応答メッセージを受信した後、前記検証モジュールは：更に、前記ユーザＩＤを前記イネーブル応答メッセージから取得し、前記ユーザＩＤを前記ユーザ記録内に保存するように構成された、
第２９の局面に記載のサーバ。
［第３４の局面］
前記イネーブル応答メッセージは、クライアント端末デバイスＩＤを更に含み；前記イネーブル応答メッセージを受信した後、前記検証モジュールは、更に、前記デバイスＩＤを前記イネーブル応答メッセージから取得し、前記デバイスＩＤを前記ユーザ記録内に保存するように構成された、
第３３の局面に記載のサーバ。
［第３５の局面］
前記認証リクエスト返信メッセージは、前記ユーザＩＤを更に含み、そのため、前記クライアント端末は、前記ユーザＩＤに従って前記対応するイネーブル記録を検索し、前記取得された生体特徴テンプレートＩＤを前記探し出したイネーブル記録内の前記生体特徴テンプレートＩＤと比較し、前記クライアント端末によって生成される前記認証応答メッセージは、更に前記ユーザＩＤを含み；前記認証応答メッセージを受信した後、前記検証モジュールは、更に、前記認証応答メッセージ内の前記ユーザＩＤを取得し、前記ユーザ

ＩＤに従って前記対応するユーザ記録を検索するように構成された、
第３３の局面に記載のサーバ。
［第３６の局面］
前記認証応答メッセージは、クライアント端末デバイスＩＤを更に含み；前記認証応答メッセージを受信した後、前記検証モジュールは、更に、前記認証応答メッセージ内の前記デバイスＩＤを取得し、前記デバイスＩＤに従って前記対応するユーザ記録を検索するように構成された、
第３５の局面に記載のサーバ。