

## 明 細 書

**発明の名称：** サービス提供システム及びユニット装置

### 技術分野

[0001] 本発明の実施形態は、サービス提供システム及びユニット装置に関する。

### 背景技術

[0002] 一般に、利用者が何らかのサービスをサービス提供者から受ける場合に、利用者が所有するクレジットカードに基づくクレジット決済を用いることがある。この種のクレジット決済においては、クレジットカードを所持した人の署名により、本人を確認したとみなしている。また、銀行の預金引出又は振込では、キャッシュカードを所持した人のキャッシュカード番号に基づいて暗証番号を照合することにより、本人を確認したとみなしている。

[0003] このように、クレジット決済及び預金引出／振込においては、店舗におけるリアルな取引又はオンラインのバーチャルな取引のいずれにしても、署名又は暗証番号による認証が用いられている。

### 先行技術文献

#### 特許文献

[0004] 特許文献1：特開2007－ 34735号公報

特許文献2：特開2007－304742号公報

特許文献3：特開2006－ 11768号公報

### 発明の概要

#### 発明が解決しようとする課題

[0005] しかしながら、以上のようなクレジット決済及び預金引出／振込においては、クレジットカード番号やキャッシュカード番号と暗証番号の使用者がカード所有者本人であることの確認ができない。このため、クレジットカード番号やキャッシュカード番号と暗証番号などのサービス用利用者識別情報が漏えいした場合、この他人がカード所有者本人になりすますことを防止できないという不都合がある。

[0006] また、店舗におけるリアルな取引の際には、サービス用利用者識別情報を記載したクレジットカードやキャッシュカード等のカードを携行・提示する必要がある。

[0007] 本発明が解決しようとする課題は、サービス用利用者識別情報を記載したカードの携行・提示を不要とし、サービス用利用者識別情報の漏えいの可能性を低減でき、利用者の本人確認を実行し得るサービス提供システム及びユニット装置を提供することである。

### 課題を解決するための手段

[0008] 実施形態のサービス提供システムは、複数のユニット装置、ユニット統合装置、利用者端末、検証装置及びサービス提供装置を備えている。

[0009] 前記複数のユニット装置は、生体認証を用いた認証処理を構成する認証構成プロセスを個別に実行する。前記ユニット統合装置は、前記各ユニット装置を内蔵又は外部接続して当該各ユニット装置に通信可能となっている。前記利用者端末は、前記ユニット統合装置を内蔵又は外部接続して当該ユニット統合装置に通信可能となっている。前記検証装置は、前記各認証構成プロセスの実行内容を認証子に基づいて検証する。前記サービス提供装置は、前記利用者端末及び前記検証装置に通信可能となっている。

[0010] 前記各ユニット装置は、機器証明書格納手段、評価報告書格納手段、秘密情報格納手段、認証構成プロセス実行手段、認証子生成手段、認証コンテキスト生成手段、認証構成プロセス結果情報生成手段及び結果情報送信手段を備えている。

[0011] 前記機器証明書格納手段は、前記各ユニット装置に対して機器証明書発行者により公開鍵暗号方式に基づいて発行された機器証明書であって、前記認証構成プロセスの属するユニット装置の公開鍵又はメッセージ認証符号を生成するための秘密情報の識別情報と、前記認証構成プロセスの属するユニット装置を特定するユニット装置特定情報と、前記機器証明書発行者を特定する機器証明書発行者情報とを含む機器証明書本文と、前記機器証明書発行者の秘密鍵により前記機器証明書本文に対して生成されたデジタル署名とを含

む前記機器証明書を格納する。

- [0012] 前記評価報告書格納手段は、前記ユニット装置特定情報と、前記認証構成プロセスの実行に用いる生体認証アルゴリズムを含む生体認証構成プロセスを特定する生体認証構成プロセス特定情報と、前記生体認証アルゴリズムによる生体認証の精度を示す生体認証精度とを含む評価報告書を格納する。
- [0013] 前記秘密情報格納手段は、前記認証子を生成するための秘密情報を格納する。
- [0014] 前記認証構成プロセス実行手段は、前記サービス提供装置により生成されたランダムなチャレンジ値と、前記認証構成プロセスの実行を要求する認証構成プロセス実行要求とを前記ユニット統合装置から前記各ユニット装置が受けると、前記認証構成プロセスを実行する。
- [0015] 前記認証子生成手段は、前記機器証明書、前記評価報告書、前記チャレンジ値及び前記実行内容に基づいて、前記秘密情報により前記認証子を生成する。
- [0016] 前記認証コンテキスト生成手段は、前記機器証明書、前記評価報告書、前記チャレンジ値、前記実行内容及び前記認証子が特定のフォーマットで記述された認証コンテキストを生成する。
- [0017] 前記認証構成プロセス結果情報生成手段は、前記認証コンテキスト及び認証構成プロセスの実行結果が特定のフォーマットで記述された認証構成プロセス結果情報を生成する。
- [0018] 前記結果情報送信手段は、前記認証構成プロセス結果情報を前記ユニット統合装置に送信する。
- [0019] 前記各ユニット装置のうち、少なくとも1台のユニット装置は、利用者識別情報証明書格納手段、を更に備えている。
- [0020] 前記利用者識別情報証明書格納手段は、前記利用者端末の利用者に対して第三者機関により公開鍵暗号方式に基づいて発行された利用者識別情報証明書であって、前記利用者を識別する利用者識別情報と、前記利用者の生体参照情報のハッシュ値と、前記第三者機関を特定する第三者機関情報とを含む

証明書本文と、前記第三者機関の秘密鍵により当該証明書本文に対して生成されたデジタル署名とを含む前記利用者識別情報証明書を格納する。

[0021] 前記少なくとも1台のユニット装置の認証子生成手段は、前記機器証明書、前記評価報告書、前記チャレンジ値、前記利用者識別情報証明書及び前記実行内容に基づいて、前記秘密情報により前記認証子を生成する。

[0022] 前記少なくとも1台のユニット装置の認証子生成手段は、前記機器証明書、前記評価報告書、前記チャレンジ値、前記利用者識別情報証明書、前記実行内容及び前記認証子が特定のフォーマットで記述された認証子生成手段及び認証処理結果情報送信手段を備えている。

[0023] 前記ユニット統合装置は、装置情報格納手段、第1認証構成プロセス実行要求送信手段、第2認証構成プロセス実行要求送信手段、認証処理結果情報要求送信手段、第2認証構成プロセス実行要求送信手段、認証処理結果情報生成手段及び認証処理結果情報送信手段を備えている。

[0024] 前記装置情報格納手段は、前記各ユニット装置のユニット装置特定情報と、当該各ユニット装置が実行する認証構成プロセスにおける機能を示す機能名と、当該機能の処理順序を示す処理順序とを関連付けて格納する。

[0025] 前記第1認証構成プロセス実行要求送信手段は、前記認証処理の実行を要求する認証処理実行要求と、前記チャレンジ値とを前記利用者端末から受け取ると、前記装置情報格納手段内の処理順序及びユニット装置特定情報に従って、当該ユニット装置特定情報が特定するユニット装置へ当該チャレンジ値及び前記認証構成プロセス実行要求を送信する。

[0026] 前記第2認証構成プロセス実行要求送信手段は、前記認証構成プロセス実行要求の送信先のユニット装置から前記認証構成プロセス実行要求を受けると、前記装置情報格納手段内の処理順序及びユニット装置特定情報に基づいて、当該送信先のユニット装置の次の処理順序のユニット装置へ前記チャレンジ値及び前記認証構成プロセス実行要求を送信する。

[0027] 前記認証処理結果情報生成手段は、この認証構成プロセス実行要求の送信先のユニット装置から前記認証構成プロセス実行要求を受けると、前記ユニット装置構成情報内の処理順序及びユニット装置特定情報に基づいて、当該

送信先のユニット装置が最後の処理順序のユニット装置のとき、前記各ユニット装置から受けた前記認証構成プロセス結果情報内の前記認証コンテキストと、前記最後の処理順序のユニット装置から受けた前記認証構成プロセス結果情報内の実行結果とが特定のフォーマットで記述された認証処理結果情報を生成する。

[0028] 前記認証処理結果情報送信手段は、前記認証処理結果情報を前記利用者端末に送信する。

[0029] 前記利用者端末は、サービス要求送信手段、認証処理実行要求送信手段、転送手段及び表示手段を備えている。

[0030] 前記サービス要求送信手段は、前記サービス提供装置に対してサービスを要求するサービス要求を当該サービス提供装置に送信する。

[0031] 前記認証処理実行要求送信手段は、前記利用者に対して前記生体認証の実行を要求する認証要求と、前記チャレンジ値とを前記サービス提供装置から受けると、前記チャレンジ値及び前記認証処理実行要求を前記ユニット統合装置に送信する。

[0032] 前記転送手段は、前記ユニット統合装置から受けた認証処理結果情報を前記サービス提供装置に転送する。

[0033] 前記表示手段は、前記サービス提供装置から受けたサービス情報を表示する。

[0034] 前記サービス提供装置は、利用者情報格納手段、サービス提供ポリシー格納手段、認証要求送信手段、読出手段及びサービス情報送信手段を備えている。

[0035] 前記利用者情報格納手段は、前記利用者識別情報証明書内の利用者識別情報と、この利用者識別情報とは異なる値を有して前記利用者を識別するサービス用利用者識別情報とを関連付けて格納する。

[0036] 前記サービス提供ポリシー格納手段は、前記利用者にサービスを提供する条件を示すサービス提供ポリシーであって、前記サービスを識別するサービス識別情報と、前記認証構成プロセスの実行に用いるユニット装置特定情報と、

生体認証アルゴリズムを含む生体認証構成プロセスを特定する生体認証構成プロセス情報と、前記生体認証アルゴリズムによる生体認証精度を正当とみなす基準を示す基準値とを含む前記サービス提供ポリシーを格納する。

- [0037] 前記認証要求送信手段は、前記利用者端末からサービス要求を受けると、前記チャレンジ値を生成して保持し、このチャレンジ値と前記認証要求とを前記利用者端末に送信する。
- [0038] 前記送信手段は、前記利用者端末から認証処理結果情報を受けると、前記保持したチャレンジ値と当該認証処理結果情報と前記サービス提供ポリシーとを検証装置に送信する。
- [0039] 前記読出手段は、前記検証装置から利用者識別情報及び検証結果を受けると、この検証結果が正当なとき、この利用者識別情報に基づいて前記利用者情報格納手段を検索し、当該利用者識別情報に関連付けられたサービス用利用者識別情報を読出す。
- [0040] 前記サービス情報送信手段は、当該読み出したサービス用利用者識別情報に基づいて、前記サービス情報を前記利用者端末に送信する。
- [0041] 前記検証装置は、公開鍵格納手段、受信手段、フォーマット検証手段、認証子検証手段、機器証明書検証手段、利用者識別情報証明書検証手段、評価報告書検証手段、チャレンジ値検証手段、実行結果検証手段及び利用者識別情報送信手段を備えている。
- [0042] 前記公開鍵格納手段は、前記各ユニット装置の機器証明書発行者の公開鍵と、前記第三者機関の公開鍵とを格納する。
- [0043] 前記受信手段は、前記サービス提供装置から前記チャレンジ値、前記認証処理結果情報及び前記サービス提供ポリシーを受信する。
- [0044] 前記フォーマット検証手段は、前記受信した認証処理結果情報が前記特定のフォーマットに適合していることを検証する。
- [0045] 前記認証子検証手段は、前記受信した認証処理結果情報に記述された認証コンテキスト内の認証子を検証する。
- [0046] 前記機器証明書検証手段は、前記受信した認証処理結果情報に記述された

認証コンテキストに含まれる機器証明書内のデジタル署名を前記機器証明書発行者の公開鍵に基づいて検証する。

[0047] 前記利用者識別情報証明書検証手段は、前記受信した認証処理結果情報に記述された認証コンテキストに含まれる利用者識別情報証明書内のデジタル署名を前記第三者機関の公開鍵に基づいて検証する。

[0048] 前記評価報告書検証手段は、前記受信した認証処理結果情報に記述された認証コンテキストに含まれる評価報告書を、前記受信したサービス提供ポリシーに基づいて検証する。

[0049] 前記チャレンジ値検証手段は、前記受信した認証処理結果情報に記述された認証コンテキスト内のチャレンジ値を、前記受信したチャレンジ値に基づいて検証する。

[0050] 前記実行結果検証手段は、前記受信した認証処理結果情報に記述された実行結果が正当を示すことを検証する。

[0051] 前記利用者識別情報送信手段は、前記フォーマット検証手段、前記認証子検証手段、前記機器証明書検証手段、前記利用者識別情報証明書検証手段、前記評価報告書検証手段、前記チャレンジ値検証手段及び実行結果検証手段による全ての検証結果が正当のとき、前記利用者識別情報証明書検証手段による検証に用いた利用者識別情報証明書内の利用者識別情報と、正当を示す検証結果とを前記サービス提供装置に送信する。

### 図面の簡単な説明

[0052] [図1]図1は、第1の実施形態に係るサービス提供システムの構成を示す模式図である。

[図2]図2は、同実施形態におけるサービスプロセスを説明するための模式図である。

[図3]図3は、同実施形態における格納部23を説明するための模式図である。

[図4]図4は、同実施形態におけるユニット統合装置30の構成を示す模式図である。

[図5]図5は、同実施形態における装置情報格納部33を説明するための模式図である。

[図6]図6は、同実施形態における各ユニット装置40、50の構成を示す模式図である。

[図7]図7は、同実施形態における機器証明書格納部44を説明するための模式図である。

[図8]図8は、同実施形態における機器証明書格納部54を説明するための模式図である。

[図9]図9は、同実施形態における利用者固有情報55aを説明するための模式図である。

[図10]図10は、同実施形態における第1認証コンテキストc1を説明するための模式図である。

[図11]図11は、同実施形態における第2認証コンテキストc2を説明するための模式図である。

[図12]図12は、同実施形態における第1認証構成プロセス結果情報b1を説明するための模式図である。

[図13]図13は、同実施形態における第2認証構成プロセス結果情報b2を説明するための模式図である。

[図14]図14は、同実施形態における認証処理結果情報bを説明するための模式図である。

[図15]図15は、同実施形態における格納部63を説明するための模式図である。

[図16]図16は、同実施形態におけるステップST1乃至ST7の動作を説明するためのフローチャートである。

[図17]図17は、同実施形態におけるステップST8乃至ST16の動作を説明するためのフローチャートである。

[図18]図18は、同実施形態におけるステップST17乃至ST26の動作を説明するためのフローチャートである。

[図19]図 19 は、同実施形態におけるステップ S T 2 7 乃至 S T 4 0 の動作を説明するためのフローチャートである。

[図20]図 20 は、同実施形態におけるステップ S T 4 1 乃至 S T 4 7 の動作を説明するためのフローチャートである。

[図21]図 21 は、第 2 の実施形態に係るサービス提供システムの構成を示す模式図である。

[図22]図 22 は、同実施形態における装置情報格納部 3 3 を説明するための模式図である。

[図23]図 23 は、同実施形態における格納部 2 3 を説明するための模式図である。

[図24]図 24 は、同実施形態における格納部 6 3 を説明するための模式図である。

[図25]図 25 は、同実施形態における認証処理結果情報 b を説明するための模式図である。

[図26]図 26 は、同実施形態における動作を説明するためのフローチャートである。

[図27]図 27 は、第 3 の実施形態における格納部 6 3 を説明するための模式図である。

[図28]図 28 は、同実施形態における格納部 2 3 を説明するための模式図である。

[図29]図 29 は、同実施形態におけるステップ S T 4 0 乃至 S T 4 7 の動作を説明するためのフローチャートである。

### **発明を実施するための形態**

[0053] 以下、各実施形態について図面を用いて説明する。なお、以下の各装置は、装置毎に、ハードウェア構成、又はハードウェア資源とソフトウェアとの組合せ構成のいずれでも実施可能となっている。組合せ構成のソフトウェアとしては、予めネットワーク又は記憶媒体から対応する装置のコンピュータにインストールされ、対応する装置の機能を実現させるためのプログラムが

用いられる。

[0054] (第1の実施形態)

図1は第1の実施形態に係るサービス提供システムの構成を示す模式図であり、図2は同システムにおけるサービスプロセスを説明するための模式図である。サービスプロセスは、図2に示すように、認証要求プロセス、2つの認証構成プロセスP1、P2、検証結果検証プロセス、利用者情報検索プロセス及びサービス提供プロセスから構成される。サービスプロセスでは、各認証構成プロセスP1、P2の実行結果を基に認証結果が検証され、認証検証結果を基に利用者情報が検索され、利用者情報に基づきサービスが提供される。なお、各認証構成プロセスP1、P2は、互いに異なる第1又は第2ユニット装置40、50で実行される。ここでは、認証構成プロセスP1が第1ユニット装置40で実行され、認証構成プロセスP2が第2ユニット装置50で実行される例を示している。

[0055] ここで、認証処理とは、認証したい対象（人、装置等）が正当であることを確認する処理をいう。また、正当であるとは、検証者が正しいと認める基準を満たした場合をいう。認証構成プロセスは、認証処理を構成するプロセスをいう。認証構成プロセスとしては、例えば生体情報を用いた認証処理の場合 1) 生体情報の読み取り、2) 特徴情報を抽出などがあり、また、1) および2) をまとめて1つの認証構成プロセスということもある。

[0056] 認証処理は、1つ以上の認証構成プロセスから構成され、それらがそれぞれ異なるユニット装置で実行されてもよい。また、後段の認証構成プロセスは、前段の認証構成プロセスの結果を参照して実行されてもよく、また参照しなくてもよい。

[0057] サービス提供システムは、利用者端末10、サービス提供装置20、ユニット統合装置30、第1ユニット装置40、第2ユニット装置50及び検証装置60を備えている。なお、各ユニット装置40、50は、生体認証を用いた認証処理を構成する認証構成プロセスP1、P2を個別に実行する。第1ユニット装置40としては、例えば、指紋センサやCCDカメラ等が適宜

使用可能となっている。第2ユニット装置50としては、SIMカード、ICカード、又はマイクロ(micro)SDカード等が適宜使用可能となっている。ユニット統合装置30としては、例えば携帯電話が使用可能となっており、各ユニット装置40、50を内蔵又は外部接続して当該各ユニット装置40、50に通信可能となっている。そして、外部の記憶媒体との接続の場合、例えば、記憶媒体にあたる各種カードやUSB(Universal Serial Bus)などのインタフェースを適宜に使用可能となっている。利用者端末10は、ユニット統合装置30を内蔵又は外部接続して当該ユニット統合装置30に通信可能となっている。検証装置60は、各認証構成プロセスP1、P2の実行内容を認証子に基づいて検証する。サービス提供装置20は、利用者端末10及び検証装置60に通信可能となっている。

[0058] ここで、利用者端末10は、通常のコンピュータ機能を有しており、例えば、通信部11及び表示部12を備えている。

[0059] 通信部11は、例えば、以下の機能(f11-1)～(f11-3)をもっている。

[0060] (f11-1) サービス提供装置20に対してサービスを要求するサービス要求を当該サービス提供装置20に送信するサービス要求送信機能。

[0061] (f11-2) 利用者に対して生体認証の実行を要求する認証要求と、サービス提供装置20により生成されたランダムなチャレンジ値とをサービス提供装置20から受けると、チャレンジ値及び認証処理実行要求をユニット統合装置30に送信する認証処理実行要求送信機能。

[0062] (f11-3) ユニット統合装置30から受けた認証処理結果情報をサービス提供装置20に転送する転送機能。

[0063] 表示部12は、例えば、サービス提供装置20から受けたサービス情報を表示する表示機能をもっている。

[0064] サービス提供装置20は、通信部21、サービス提供部22及び格納部23を備えている。

[0065] 通信部21は、サービス提供部22と各装置10、60との間の通信インタフェースである。以下の説明では、通信のときに通信部21を経由する旨

の記述を省略する。

[0066] サービス提供部 22 は、例えば、以下の機能(f22-1)～(f22-4)をもっている。

[0067] (f22-1) 利用者端末 10 からサービス要求を受けると、チャレンジ値を生成して保持し、このチャレンジ値と認証要求とを利用者端末 10 に送信する認証要求送信機能。

[0068] (f22-2) 利用者端末 10 から認証処理結果情報を受けると、保持したチャレンジ値と当該認証処理結果情報とサービス提供ポリシーとを検証装置 60 に送信する送信機能。

[0069] (f22-3) 検証装置 60 から利用者識別情報及び検証結果を受けると、この検証結果が正当なとき、この利用者識別情報に基づいて格納部 23 を検索し、当該利用者識別情報に関連付けられたサービス用利用者識別情報を読み出す読み出し機能。

[0070] (f22-4) 当該読み出したサービス用利用者識別情報に基づいて、サービス情報を利用者端末 10 に送信するサービス情報送信機能。

[0071] 格納部 23 は、図 3 に示すように、利用者情報 23a 及びサービス提供ポリシー 23b を格納している。

[0072] 利用者情報 23a は、利用者識別情報証明書内の利用者識別情報と、この利用者識別情報とは異なる値を有して利用者を識別するサービス用利用者識別情報とが関連付けて記述されている。なお、サービス用利用者識別情報は、例えば、クレジットカード番号又はキャッシュカード番号などであり、サービス提供装置 20 の運営者（例、信販会社、銀行など）が利用者に付与する識別情報である。利用者情報 23a としては、さらに、ユーザの氏名、住所、パスワード、口座番号、TTP（Trusted Third Party: 信頼できる第三者機関。以下、単に第三者機関ともいう）情報、利用者識別情報証明書内の利用者識別情報、サービス提供の分類を示すサービス提供分類、利用者端末 10 のアドレス情報、などが適宜使用可能となっている。また、サービス情報は、例えば、信販会社が提供可能な利用者向け情報（例、利用状況照会、

割引サービス加盟店の案内など）であり、図示しない記憶部（図示せず）に記憶されている。

[0073] サービス提供ポリシ 23 b は、利用者にサービスを提供する条件を示しており、例えば、サービスを提供する分類を示すサービス提供分類と、認証構成プロセスの実行に用いるユニット装置特定情報（第 1 ユニット装置 40 又は第 2 ユニット装置 50 を特定する情報）と、生体認証アルゴリズムを含む生体認証構成プロセスを特定する生体認証構成プロセス情報と、生体認証アルゴリズムによる生体認証精度を正当とみなす基準を示す基準値とを含んでいる。基準値としては、例えば、FAR（False Acceptance Rate : 他人受入れ率）及び／又は FRR（False Rejection Rate : 本人拒否率）などが適宜、使用可能となっている。

[0074] ユニット統合装置 30 は、図 4 に示すように、通信部 31、制御部 32、装置情報格納部 33 及び結果情報統合部 34 を備えている。

[0075] 通信部 31 は、制御部 32 と各装置 10、40、50 との間の通信インターフェースである。以下の説明では、通信のときに通信部 31 を経由する旨の記述を省略する。

[0076] 制御部 32 は、例えば、以下の機能 (f32-1) ~ (f32-4) をもっている。

[0077] (f32-1) 認証処理の実行を要求する認証処理実行要求と、チャレンジ値とを利用者端末 10 から受けると、装置情報格納部 33 内の処理順序及びユニット装置特定情報に従って、当該ユニット装置特定情報が特定するユニット装置 40 へ当該チャレンジ値及び認証構成プロセス実行要求を送信する第 1 認証構成プロセス実行要求送信機能。

[0078] (f32-2) 認証構成プロセス実行要求の送信先のユニット装置 40 から認証構成プロセス結果情報を受けると、装置情報格納部 33 内の処理順序及びユニット装置特定情報に基づいて、当該送信先のユニット装置 40 の次の処理順序のユニット装置 50 へチャレンジ値及び認証構成プロセス実行要求を送信する第 2 認証構成プロセス実行要求送信機能。

[0079] (f32-3) この認証構成プロセス実行要求の送信先のユニット装置 50 か

ら認証構成プロセス結果情報を受けると、ユニット装置構成情報内の処理順序及びユニット装置特定情報に基づいて、当該送信先のユニット装置50が最後の処理順序のユニット装置のとき、各ユニット装置40, 50から受けた認証構成プロセス結果情報内の認証コンテキストと、最後の処理順序のユニット装置から受けた認証構成プロセス結果情報内の実行結果とが特定のフォーマットで記述された認証処理結果情報を生成する認証処理結果情報生成機能。この認証処理結果情報生成機能(f32-3)は、例えば、各ユニット装置40, 50から受けた認証構成プロセス結果情報と、認証構成プロセス結果情報統合要求とを結果情報統合部34に送出し、結果情報統合部34から認証処理結果情報を受けることにより実現してもよい。

[0080] (f32-4) 認証処理結果情報を利用者端末10に送信する認証処理結果情報送信機能。

[0081] 装置情報格納部33は、図5に示すように、ユニット情報構成情報33aを格納している。ユニット情報構成情報33aは、各ユニット装置のユニット装置特定情報と、当該各ユニット装置が実行する認証構成プロセスにおける機能を示す機能名と、当該機能の処理順序を示す処理順序とが関連付けて記述されている。

[0082] 結果情報統合部34は、制御部32から受けた認証構成プロセス結果情報を統合して認証処理結果情報を制御部32に送出する。

[0083] 第1及び第2ユニット装置40, 50は、図6に示すように、通信部41, 51、制御部42, 52、秘密情報管理部45, 55、認証子生成部46, 56、機器証明書格納部44, 54、認証コンテキスト生成部47, 57及び結果情報生成部48, 58を備えている。また、第1ユニット装置40は認証構成プロセスP1実行部43を備えており、第2ユニット装置50は認証構成プロセスP2実行部53を備えている。

[0084] ここで、通信部41, 51は、制御部42, 52と各装置30, 50, 40との間の通信インタフェースである。以下の説明では、通信のときに通信部41, 51を経由する旨の記述を省略する。

- [0085] 制御部 4 2, 5 2 は、ユニット統合装置 3 0 から受けた認証構成プロセス実行要求に基づいて、認証構成プロセス結果情報を作成し、この認証構成プロセス結果情報をユニット統合装置 3 0 に送信するように、各部 4 1, 4 3 ~ 4 8、及び 5 1, 5 3 ~ 5 8 を制御する機能をもっている。
- [0086] 制御部 4 2, 5 2 は、例えば、以下の各機能 (f42-1, f52-1) をもっている。
- [0087] (f42-1, f52-1) サービス提供装置 2 0 により生成されたランダムなチャレンジ値と、認証構成プロセスの実行を要求する認証構成プロセス実行要求とをユニット統合装置 3 0 から受けると、実行要求を認証構成プロセス P 1 実行部 4 3、認証構成プロセス P 2 実行部 5 3 へ送出する機能。
- [0088] (f42-2, f52-2) 認証構成プロセス P 1 実行部 4 3、認証構成プロセス P 2 実行部 5 3 の実行結果及びチャレンジ値を認証コンテキスト生成部 4 7, 5 7 へ送出する機能。
- [0089] (f42-3, f52-3) 認証コンテキスト生成部 4 7, 5 7 から送出される認証コンテキストと各実行部 4 3, 5 3 の実行結果を結果情報生成部 4 8, 5 8 へ送出する機能。
- [0090] (f42-4, f52-4) 結果情報生成部 4 8, 5 8 から送出された認証構成プロセス結果情報をユニット統合装置 3 0 に送信する機能。
- [0091] 認証構成プロセス P 1 実行部 4 3 は、制御部 4 2 から実行要求を受けると、認証構成プロセス P 1 を実行し、その実行結果を制御部 4 2 に送出する。
- [0092] 認証構成プロセス P 2 実行部 5 3 は、制御部 5 2 から実行要求を受けると、秘密情報管理部 5 5 から利用者固有情報 5 5 a を読み出し、前述の認証構成プロセス P 2 を実行し、その実行結果と、利用者固有情報 5 5 a 内の利用者識別情報証明書を制御部 5 2 に送出する。
- [0093] 機器証明書格納部 4 4, 5 4 は、図 7 及び図 8 に示すように、それぞれ自装置 4 0, 5 0 の機器証明書（機器の公開鍵証明書）4 4 a, 5 4 a と、自装置の評価報告書 4 4 b, 5 4 b とを格納している。
- [0094] 機器証明書 4 4 a, 5 4 a は、各ユニット装置 4 0, 5 0 に対して機器証

明書発行者により公開鍵暗号方式に基づいて発行されており、認証構成プロセス P 1, P 2 の属するユニット装置 4 0, 5 0 の秘密情報と同一又は対応する情報と、認証構成プロセス P 1, P 2 の属するユニット装置 4 0, 5 0 を特定するユニット装置特定情報と、機器証明書発行者を特定する機器証明書発行者情報とを含む機器証明書本文と、機器証明書発行者の秘密鍵により機器証明書本文に対して生成されたデジタル署名とを含んでいる。ここで、

「秘密情報に対応する情報」とは、公開証明書などの公開鍵を特定する情報のことを指し、以下の実施の形態での説明においても同様とする。なお、機器証明書本文は、さらに、フィールド、バージョン、機器証明書のシリアル番号、署名アルゴリズム、有効期限、生体認証デバイス製造者の各項目のデータを備えてもよい。

[0095] 評価報告書 4 4 b, 5 4 b は、認証構成プロセス P 1, P 2 のユニット装置特定情報（図 7 における第 1 ユニット装置特定情報、図 8 における第 2 ユニット装置特定情報）と、実行に用いる生体認証アルゴリズムを含む生体認証構成プロセスを特定する生体認証構成プロセス情報と、生体認証アルゴリズムによる生体認証の精度を示す生体認証精度とを含んでいる。生体認証精度としては、例えば、標準化団体等で規定された標準化された照合精度評価基準に沿ったもの（例、前述した F R R, F A R 等）が適宜使用可能となっている。

[0096] また、評価報告書 4 4 b, 5 4 b には、安全性などの評価項目を付属させてもよい。そして、評価報告書 4 4 b, 5 4 b を発行する者は、例えば、公開鍵基盤に基づく認定局（Certificate Authority : CA）が認定したユニット装置 4 0, 5 0 に対して評価報告書を発行するようになっている。この認定局は、ユニット装置 4 0, 5 0 の製造者からの申請に基づいて、ユニット装置 4 0, 5 0 における生体認証アルゴリズムによる生体認証の精度を示す生体認証精度などを評価して認定する機能を持つ。併せて、この認定した内容の評価について、依頼された製造者に送出する機能も持ち、当該評価に電子署名を付与してもよい。

- [0097] 秘密情報管理部 4 5 は、予め認証子を生成するための秘密情報 1 が格納されている。また、秘密情報管理部 4 5 は、前述した機器証明書 4 4 a 内の第 1 ユニット装置 4 0 の公開鍵に対応する秘密鍵（図示せず）が格納されている。
- [0098] 秘密情報管理部 5 5 は、予め認証子を生成するための秘密情報 2、及び利用者本人に固有の利用者固有情報 5 5 a が格納されている。また、秘密情報管理部 5 5 は、前述した機器証明書 5 4 a 内の第 2 ユニット装置 5 0 の公開鍵に対応する秘密鍵（図示せず）が格納されている。
- [0099] なお、機器証明書 4 4 a、5 4 b における公開鍵（図 7 における第 1 ユニット装置の公開鍵、図 8 における第 2 ユニット装置の公開鍵）に代えて、メッセージ認証符号（Message Authentication Code : MAC）生成のための秘密情報の識別情報を用いることも出来る。
- [0100] ここで、秘密情報 1、2 は、それぞれ第 1 ユニット装置、第 2 ユニット装置に付与されている。秘密情報 1、2 は、例えば認証子がデジタル署名の場合は公開鍵暗号方式における秘密鍵及び公開鍵のペアであり、認証子がメッセージ認証符号の場合は予め検証装置 6 0 と共有された共通鍵である。認証子がデジタル署名の場合は、秘密鍵に対応する、予め認証局から発行された公開鍵証明書が秘密情報管理部 4 5、5 5 に格納されているとする。この公開鍵証明書は、前述した機器証明書 4 4 a、5 4 a とは別のものを想定しているが、前述した機器証明書 4 4 a、5 4 a を用いてもよい。公開鍵証明書として機器証明書 4 4 a、5 4 a を用いる場合、認証子は、ユニット装置 4 0、5 0 の公開鍵に対応する秘密鍵に基づいて生成される。
- [0101] 利用者固有情報 5 5 a は、図 9 に示すように、利用者識別情報証明書 5 5 b を含んでいる。利用者固有情報 5 5 a は、利用者の参照生体情報 5 5 c を更に含んでもよい。
- [0102] 利用者識別情報証明書 5 5 b は、利用者端末 1 0 の利用者に対して第三者機関（TTP）により公開鍵暗号方式に基づいて発行されており、利用者を識別する利用者識別情報と、利用者の生体参照情報のハッシュ値と、第三者

機関を特定する T T P 情報とを含む証明書本文と、第三者機関の秘密鍵により当該証明書本文に対して生成されたデジタル署名とを含んでいる。利用者識別情報証明書 5 5 b 内の利用者識別情報は、T T P が付与したものである。

[0103] 認証子生成部 4 6, 5 6 は、入力されたデータを対象として、秘密情報管理部 4 5, 5 5 から読み出した秘密情報を用いて認証子を生成するものである。認証子としては、例えばデジタル署名又はメッセージ認証符号が適宜、使用可能となっている。

[0104] ここで、認証子生成部 4 6 は、認証コンテキスト生成部 4 7 から受けた機器証明書 4 4 a、評価報告書 4 4 b、チャレンジ値、及び実行内容としての認証構成プロセス P 1 の実行結果のハッシュ値に基づいて、秘密情報管理部 4 5 内の秘密情報 1 により認証子を生成する機能と、生成した認証子を認証コンテキスト生成部 4 7 に送出する機能とをもっている。

[0105] 認証子生成部 5 6 は、認証コンテキスト生成部 5 7 から受けた機器証明書 5 4 a、評価報告書 5 4 b、チャレンジ値、利用者識別情報証明書 5 5 b 及び実行内容としての認証構成プロセス P 2 の実行結果のハッシュ値に基づいて、秘密情報管理部 5 5 内の秘密情報 2 により認証子を生成する機能と、生成した認証子を認証コンテキスト生成部 5 7 に送出する機能とをもっている。

[0106] 認証コンテキスト生成部 4 7, 5 7 は、認証構成プロセス P 1 実行部 4 3、認証構成プロセス P 2 実行部 5 3 の実行に関わる情報及び認証子生成部 4 6, 5 6 により出力される認証子を、特定のフォーマットに従い整形し、その結果を出力するものである。本文では、認証コンテキスト生成部 4 7, 5 7 により特定のフォーマットにしたがい整形された情報を認証コンテキストと記述する。

[0107] ここで、認証コンテキスト生成部 4 7 は、図 1 0 に示すように、機器証明書格納部 4 4 内の機器証明書 4 4 a 及び評価報告書 4 4 b と、制御部 4 2 から受けたチャレンジ値及び実行内容と、認証子生成部 4 6 から受けた認証子

とが特定のフォーマットで記述された第1認証コンテキストc1を生成する機能と、生成した第1認証コンテキストc1を制御部42に送出する機能とをもっている。

[0108] 第1認証コンテキストc1は、例えば、ヘッダブロックc1h、データブロックc1d及び認証子ブロックc1aから構成される。

[0109] ヘッダブロックc1hは、第1ユニット装置40の機器証明書44a及び評価報告書44bが記述される。また、ヘッダブロックc1hは、更に、第1ユニット装置40を特定する第1ユニット装置特定情報や、第1認証コンテキストc1の構造に関する情報が記述されてもよい。

[0110] データブロックc1dは、サービス提供装置20からのチャレンジ値、及び実行内容としての認証構成プロセスP1の実行結果のハッシュ値が記述される。また、データブロックc1dは、更に、認証構成プロセスP1実行要求に含まれる情報が記述されてもよい。

[0111] 認証子ブロックc1aは、認証子生成部46から受けた認証子が記述される。

[0112] 認証コンテキスト生成部57は、図11に示すように、機器証明書格納部54内の機器証明書54a及び評価報告書54bと、制御部52から受けたチャレンジ値及び実行内容と、認証子生成部56から受けた認証子とが特定のフォーマットで記述された第2認証コンテキストc2を生成する機能と、生成した第2認証コンテキストc2を制御部52に送出する機能とをもっている。

[0113] 第2認証コンテキストc2は、例えば、ヘッダブロックc2h、データブロックc2d及び認証子ブロックc2aから構成される。

[0114] ヘッダブロックc2hは、第2ユニット装置50の機器証明書54a及び評価報告書54bが記述される。また、ヘッダブロックc2hは、更に、第2ユニット装置50を特定する第2ユニット装置特定情報や、第2認証コンテキストc2の構造に関する情報が記述されてもよい。

[0115] データブロックc2dは、サービス提供装置20からのチャレンジ値、実

行内容としての認証構成プロセス P 2 の実行結果のハッシュ値、及び利用者の利用者識別情報証明書 5 5 b が記述される。更に、認証構成プロセス P 1 の実行結果のハッシュ値に当たるデータが格納されているが、これは、認証構成プロセス P 1 の実行結果が入力、認証構成プロセス P 2 の実行結果が出力の関係になって、一対のデータとして各々の実行結果のハッシュ値にあたるデータを格納しているものである。なお、データブロック c 2 d には、更に、認証構成プロセス P 2 実行要求に含まれる情報が記述されてもよい。

[0116] 認証子ブロック c 2 a は、認証子生成部 5 6 から受けた認証子が記述される。

[0117] 結果情報生成部 4 8 は、図 1 2 に示すように、制御部 4 2 から受けた第 1 認証コンテキスト c 1 及び認証構成プロセス P 1 の実行結果が特定のフォーマットで記述された第 1 認証構成プロセス結果情報 b 1 を生成する機能と、生成した第 1 認証構成プロセス結果情報 b 1 を制御部 4 2 に送出する機能とをもっている。

[0118] 第 1 認証構成プロセス結果情報 b 1 は、例えば、ヘッダブロック b 1 h、データブロック b 1 d 及びセキュリティブロック b 1 s から構成される。

[0119] ヘッダブロック b 1 h は、第 1 認証コンテキスト c 1 内の機器証明書 4 4 a におけるのと同様の第 1 ユニット装置特定情報が記述される。また、ヘッダブロック b 1 h は、更に、第 1 認証構成プロセス結果情報 b 1 の構造に関する情報が記述されてもよい。

[0120] データブロック b 1 d は、認証構成プロセス P 1 実行部 4 3 による認証構成プロセス P 1 の実行結果が記述される。

[0121] セキュリティブロック b 1 s は、第 1 認証コンテキスト c 1 が記述される。また、セキュリティブロック b 1 s は、更に、データブロック b 1 d が暗号化される場合の暗号化に関する情報、ヘッダブロック b 1 h 及びデータブロック b 1 d に対して認証子が付与される場合の認証子及び認証子に関する情報が記述されてもよい。

[0122] 結果情報生成部 5 8 は、図 1 3 に示すように、制御部 5 2 から受けた第 2

認証コンテキスト c 2 及び認証構成プロセス P 2 の実行結果が特定のフォーマットで記述された第 2 認証構成プロセス結果情報 b 2 を生成する機能と、生成した第 2 認証構成プロセス結果情報 b 2 を制御部 5 2 に送出する機能とをもっている。

[0123] 第 2 認証構成プロセス結果情報 b 2 は、例えば、ヘッダブロック b 2 h、データブロック b 2 d 及びセキュリティブロック b 2 s から構成される。

[0124] ヘッダブロック b 2 h は、第 2 認証コンテキスト c 2 内の機器証明書 5 4 a におけるのと同様の第 2 ユニット装置特定情報が記述される。また、ヘッダブロック b 2 h は、更に、第 2 認証構成プロセス結果情報 b 2 の構造に関する情報が記述されてもよい。

[0125] データブロック b 2 d は、認証構成プロセス P 2 実行部 5 3 による認証構成プロセス P 2 の実行結果が記述される。

[0126] セキュリティブロック b 2 s は、第 2 認証コンテキスト c 2 が記述される。また、セキュリティブロック b 2 s は、更に、データブロック b 2 d が暗号化される場合の暗号化に関する情報、ヘッダブロック b 2 h 及びデータブロック b 2 d に対して認証子が付与される場合の認証子及び認証子に関する情報が記述されてもよい。またさらに、セキュリティブロック b 2 s は、第 1 認証構成プロセス結果情報 b 1 のセキュリティブロック b 1 s に含まれる第 1 認証コンテキスト c 1 を含んでもよい。

[0127] なお、これら第 1 及び第 2 認証構成プロセス結果情報 b 1, b 2 は、前述した通り、ユニット統合装置 3 0 によって認証処理結果情報 b に統合される。

[0128] 認証処理結果情報 b は、図 1 4 に示すように、例えば、ヘッダブロック b h、データブロック b d 及びセキュリティブロック b s から構成される。なお、ヘッダブロック b h 及びデータブロック b d は、システムの要求に応じて、省略してもよい。

[0129] ヘッダブロック b h は、第 1 及び第 2 認証構成プロセス結果情報 b 1, b 2 内のヘッダブロック b 1 h, b 2 h から抽出された第 1 及び第 2 ユニット

装置特定情報が記述される。また、ヘッダブロック b h は、さらに、認証処理結果情報 b の構造に関する情報が記述されてもよい。

[0130] データブロック b d は、第 2 認証構成プロセス結果情報 b 2 内のデータブロック b 2 d から抽出された認証構成プロセス P 2 の実行結果が記述される。

[0131] セキュリティブロック b s は、第 1 及び第 2 認証構成プロセス結果情報 b 1, b 2 内のセキュリティブロック b 1 s, b 2 s から抽出された第 1 及び第 2 認証コンテキスト c 1, c 2 が記述される。また、セキュリティブロック b s は、データブロック b d が暗号化される場合の暗号化に関する情報、ヘッダブロック b h 及びデータブロック b d に対して認証子が付与される場合の認証子及び認証子に関する情報、が記述される。

[0132] 検証装置 6 0 は、図 1 に示したように、通信部 6 1、検証部 6 2 及び格納部 6 3 を備えている。

[0133] ここで、通信部 6 1 は、検証部 6 2 とサービス提供装置 2 0 との間の通信インタフェースである。以下の説明では、通信のときに通信部 6 1 を経由する旨の記述を省略する。

[0134] 検証部 6 2 は、以下の機能(f62-1)～(f62-9)をもっている。

[0135] (f62-1) サービス提供装置 2 0 からチャレンジ値、認証処理結果情報 b 及びサービス提供ポリシ 2 3 b を受信する受信機能。

[0136] (f62-2) 受信した認証処理結果情報 b が特定のフォーマットに適合していることを検証するフォーマット検証機能。

[0137] (f62-3) 受信した認証処理結果情報 b に記述された認証コンテキスト c 1, c 2 内の認証子を検証する認証子検証機能。

[0138] (f62-4) 受信した認証処理結果情報 b に記述された認証コンテキスト c 1, c 2 に含まれる機器証明書 4 4 a, 5 4 a 内のデジタル署名を格納部 6 3 内の機器証明書発行者の公開鍵に基づいて検証する機器証明書検証機能。

[0139] (f62-5) 受信した認証処理結果情報 b に記述された認証コンテキスト c 1, c 2 に含まれる利用者識別情報証明書 5 5 b 内のデジタル署名を格納部 6

3内の第三者機関の公開鍵に基づいて検証する利用者識別情報証明書検証機能。

[0140] (f62-6) 受信した認証処理結果情報bに記述された認証コンテキストc1, c2に含まれる評価報告書44b, 54bを、受信したサービス提供ポリシー23bに基づいて検証する評価報告書検証機能。

[0141] (f62-7) 受信した認証処理結果情報bに記述された認証コンテキストc1, c2内のチャレンジ値を、受信したチャレンジ値に基づいて検証するチャレンジ値検証機能。

[0142] (f62-8) 受信した認証処理結果情報bに記述された実行結果が正当を示すことを検証する実行結果検証機能。

[0143] (f62-9) フォーマット検証機能、認証子検証機能、機器証明書検証機能、利用者識別情報証明書検証機能、評価報告書検証機能、チャレンジ値検証機能及び実行結果検証機能による全ての検証結果が正当のとき、利用者識別情報証明書検証機能による検証に用いた利用者識別情報証明書55b内の利用者識別情報と、正当を示す検証結果とをサービス提供装置20に送信する利用者識別情報送信機能。

[0144] 格納部63は、検証部62から読出／書込可能な記憶装置であり、図15に示すように、各ユニット装置40, 50の機器証明書発行者の公開鍵と、TTPの公開鍵とを格納している。また、格納部63は、各ユニット装置40, 50の秘密情報1, 2と同一の又は対応する情報を格納してもよい。なお、格納部63内の情報は、認証子が各ユニット装置40, 50の秘密鍵により生成された場合には、省略される（理由は、認証子が機器証明書44a, 54a内の各ユニット装置40, 50の公開鍵により検証可能となるためである。）。

[0145] 次に、以上のように構成された認証システムの動作を図2及び図16乃至図20のフローチャートを用いて説明する。

[0146] 利用者端末10においては、表示部11に表示された画面に従い、利用者がサービスを選択することによって、図16に示すように、利用者端末10

からサービス提供装置 20 に対してサービス要求が送信されることにより (

ST 1)、サービスプロセスが開始される。サービス要求には、実行する認証方法の指定、利用者端末 10 とユニット統合装置 30 との間の通信方式の

指定などが含まれていてもよい。

[0147] サービス提供装置 20 においては、サービス提供部 22 がサービス要求を

受けると (ST 2)、予め決められた、又はサービス要求で指定された認証

方法に従い、以後の認証処理を実行する。サービス提供部 22 は、乱数等か

らなるチャレンジ値を生成して (ST 3)、チャレンジ値を保持するととも

に、このチャレンジ値と認証要求とを利用者端末 10 に送信する (ST 4)

。認証要求には、例えば、認証処理を指定する情報や、いくつかの照合アル

ゴリズムを指定する情報が含まれてもよい。

[0148] 利用者端末 10 は、チャレンジ値と認証要求を受信すると (ST 5)、チ

ャレンジ値及び認証処理実行要求をユニット統合装置 30 に送信する (ST

6)。

[0149] ユニット統合装置 30 は、チャレンジ値及び認証処理実行要求を受けると

(ST 7)、制御部 32 が装置情報格納部 33 のユニット装置構成情報 33

a を検索して第 1 ユニット装置 40 及び第 2 ユニット装置 50 の処理順序を

判断する。

[0150] しかる後、ユニット統合装置 30 は、図 17 に示すように、最先の処理順

序の第 1 ユニット装置 40 にチャレンジ値及び認証構成プロセス P1 実行要

求を送信する (ST 8)。

[0151] 第 1 ユニット装置 40 は、チャレンジ値及び認証構成プロセス P1 実行要

求を受信すると (ST 9)、制御部 42 が予め決められた、又はサービス提

供装置 20 からの認証要求で指定された認証処理に従い、認証構成プロセス

P1 実行部 43 にて認証構成プロセス P1 を実行させ、実行結果を得る (S

T 10)。すなわち、認証構成プロセス P1 は、図 5 に一例を示すように、

利用者の生体データを収集するデータ収集機能と、収集された生体データを

信号処理する信号処理機能とを順次実行する処理により、生成された生体情

報（例、指紋情報）を実行結果として得る。

[0152] 次に、制御部42は、認証コンテキスト生成部47に認証構成プロセスP1の実行結果とサービス提供装置20からのチャレンジ値とを送出する。

[0153] 認証コンテキスト生成部47は、第1認証コンテキストc1のヘッダブロックc1h及びデータブロックc1dを記述して両ブロックc1h, c1dからなるコンテキスト情報を生成し（ST11）、コンテキスト情報を認証子生成部46に送出する。

[0154] 認証子生成部46は、このコンテキスト情報を受けると、秘密情報管理部45から認証子生成のための秘密情報1を読み出す（ST12）。そして、認証子生成部46は、このコンテキスト情報に基づいて、秘密情報1により認証子を生成し、この認証子を認証コンテキスト生成部47に送出する。

[0155] 認証コンテキスト生成部47は、この認証子を認証子ブロックc1aへ記述し、3つのブロックc1h, c1d, c1aからなる第1認証コンテキストc1を生成する（ST13）。

[0156] 制御部42は、第1認証コンテキストc1を認証コンテキスト生成部47から受けると、第1認証コンテキストc1と認証構成プロセスP1の実行結果とを結果情報生成部48へ送出する。

[0157] 結果情報生成部48は、第1認証コンテキストc1及び認証構成プロセスP1の実行結果を特定のフォーマットで記述して第1認証構成プロセス結果情報b1を生成し（ST14）、この第1認証構成プロセス結果情報b1を制御部42に送出する。

[0158] 制御部42は、この第1認証構成プロセス結果情報b1を通信部41によりユニット統合装置30に送信する（ST15）。

[0159] 次に、ユニット統合装置30は、第1認証構成プロセス結果情報b1を受信すると（ST16）、制御部32が装置情報格納部33の検索結果に基づき、図18に示すように、次の処理順序の第2ユニット装置50に第1認証構成プロセス結果情報b1及び認証構成プロセスP2実行要求を送信する（ST17）。

[0160] 第2ユニット装置50は、チャレンジ値、第1認証構成プロセス結果情報b1、及び認証構成プロセスP2実行要求を受信すると（ST18）、制御部52が予め決められた、又はサービス提供装置20からの認証要求で指定された認証処理に従い、第1認証構成プロセス結果情報b1から抽出した認証構成プロセスP1の実行結果と、実行要求とを認証構成プロセスP2実行部53に送出する。

[0161] 認証構成プロセスP2実行部53は、秘密情報管理部55から利用者固有情報55aを読み出し（ST19）、この利用者固有情報のうちの利用者の参照生体情報55cと、認証構成プロセスP1の実行結果とに基づいて認証構成プロセスP2を実行させ（ST20）、実行結果を得る。すなわち、認証構成プロセスP2は、図5に一例を示すように、利用者の生体参照情報を格納する格納機能と、利用者の生体情報と参照生体情報55cとを照合する照合機能と、照合結果から認証成功か否かを判定する判定機能とを順次実行する処理により、認証成功（又は認証失敗）を実行結果として得る。なお、認証構成プロセスP2実行部53は、利用者の参照生体情報55cから算出したハッシュ値と、利用者識別情報証明書55b内の参照生体情報のハッシュ値とを比較し、両者が不一致の場合には認証構成プロセスP2の結果によらず、認証失敗を判定する処理を更に実行してもよい。

[0162] 次に、制御部52は、認証コンテキスト生成部57に認証構成プロセスP2の実行結果と利用者固有情報のうちの利用者識別情報証明書55bとチャレンジ値とを送出する。

[0163] 認証コンテキスト生成部57は、第2認証コンテキストc2のヘッダブロックc2h及びデータブロックc2dを記述して両ブロックc2h、c2dからなるコンテキスト情報を生成し（ST21）、コンテキスト情報を認証子生成部56に送出する。

[0164] 認証子生成部56は、このコンテキスト情報を受けると、秘密情報管理部55から認証子生成のための秘密情報2を読み出す（ST22）。そして、認証子生成部56は、このコンテキスト情報に基づいて、秘密情報2により

認証子を生成し、この認証子を認証コンテキスト生成部 5 7 に送出する。

[0165] 認証コンテキスト生成部 5 7 は、この認証子を認証子ブロック c 2 a へ記述し、3つのブロック c 2 h, c 2 d, c 2 a からなる第 2 認証コンテキスト c 2 を生成する (S T 2 3)。

[0166] 制御部 5 2 は、第 2 認証コンテキスト c 2 を認証コンテキスト生成部 5 7 から受けると、第 2 認証コンテキスト c 2 と認証構成プロセス P 2 の実行結果とを結果情報生成部 5 8 へ送出する。

[0167] 結果情報生成部 5 8 は、第 2 認証コンテキスト c 2 及び認証構成プロセス P 2 の実行結果を特定のフォーマットで記述して第 2 認証構成プロセス結果情報 b 2 を生成し (S T 2 4)、この第 2 認証構成プロセス結果情報 b 2 を制御部 5 2 に送出する。

[0168] 制御部 5 2 は、この第 2 認証構成プロセス結果情報 b 2 を通信部 5 1 によりユニット統合装置 3 0 に送信する (S T 2 5)。

[0169] ユニット統合装置 3 0 は、第 2 認証構成プロセス結果情報 b 2 を受信する (S T 2 6)。制御部 3 2 は、図 1 9 に示すように、全ての認証構成プロセスの処理が完了したことを確認して、第 1 認証構成プロセス結果情報 b 1 及び第 2 認証構成プロセス結果情報 b 2 を結果情報統合部 3 4 へ送出する。結果情報統合部 3 4 は、認証構成プロセス結果情報 b 1, b 2 内の認証コンテキスト c 1, c 2 と、最後の処理順序のユニット装置 5 0 から受けた認証構成プロセス結果情報 b 2 内の実行結果とが特定のフォーマットで記述された認証処理結果情報 b を生成する (S T 2 7)。

[0170] ユニット統合装置 3 0 は、生成した認証処理結果情報 b を利用者端末 1 0 へ送信する (S T 2 8)。

[0171] 利用者端末 1 0 は、認証処理結果情報 b を受けると (S T 2 9)、サービス提供装置 2 0 へ認証要求に対する結果として認証処理結果情報 b を送信する (S T 3 0)。

[0172] サービス提供装置 2 0 は、認証処理結果情報 b を受けると (S T 3 1)、ステップ S T 3 で予め保持したチャレンジ値と、この認証処理結果情報 b と

、格納部 23 内のサービス提供ポリシ 23 b とを検証装置 60 に送信する（S T 3 2）。

[0173] 検証装置 60 は、チャレンジ値、認証処理結果情報 b 及びサービス提供ポリシ 23 b を受信すると（S T 3 3）、検証部 62 が検証を開始する。

[0174] 検証部 62 は、受信した認証処理結果情報 b が特定のフォーマットに適合していることを検証する。例えば、認証処理結果情報 b に情報の抜けが無いことを検証する。

[0175] 検証部 62 は、受信した認証処理結果情報 b に記述された認証コンテキスト c 1, c 2 内の認証子を検証する。認証子の検証は、例えば認証子がデジタル署名の場合は対応する公開鍵で行い、認証子がメッセージ認証符号の場合は予めユニット装置 40, 50 と共有された共通鍵で行う。

[0176] 検証部 62 は、受信した認証処理結果情報 b に記述された認証コンテキスト c 1, c 2 に含まれる機器証明書 44 a, 54 a 内のデジタル署名を格納部 63 内の機器証明書発行者の公開鍵に基づいて検証する。

[0177] 検証部 62 は、受信した認証処理結果情報 b に記述された認証コンテキスト c 2 に含まれる利用者識別情報証明書 55 b 内のデジタル署名を格納部 63 内の第三者機関の公開鍵に基づいて検証する。

[0178] 検証部 62 は、受信した認証処理結果情報 b に記述された認証コンテキスト c 1, c 2 に含まれる評価報告書 44 b, 54 b を、受信したサービス提供ポリシ 23 b に基づいて検証する。なお、サービス提供ポリシ 23 b のサービス提供分類はレベル付けされているものとし、検証部 62 による検証結果としては、サービス提供ポリシ 23 b に合致する最高レベルのサービス提供分類を本検証結果とする。ここで、「レベル」とはサービス自体のレベルを指す。例えば、1 万円までしか使用できない、5 万円までしか使用できない、などの金銭によるものや、時間によるものなど、種々の着目点に基づく条件が「レベル」に該当し、以下の実施の形態での説明においても同様とする。

[0179] 検証部 62 は、受信した認証処理結果情報 b に記述された認証コンテキス

ト c 1, c 2 内のチャレンジ値を、受信したチャレンジ値に基づいて検証する。

[0180] 検証部 6 2 は、受信した認証処理結果情報 b に記述された実行結果が正当を示すことを検証する。

[0181] しかる後、検証部 6 2 は、上述した全ての検証結果が正当か否かを判定し (S T 3 4)、いずれか 1 つでも検証結果が正当でない場合には (S T 3 4; 否)、異常と判断してサービス提供装置 2 0 に異常を通知する (S T 3 5)。サービス提供装置 2 0 は異常通知を受信し (S T 3 6)、利用者端末 1 0 に異常を通知する (S T 3 7)。利用者端末 1 0 は異常通知を受信し (S T 3 8)、処理を終了する (S T 3 9)。

[0182] 一方、全ての検証結果が正当のとき (S T 3 4; 正当)、検証装置 6 0 は、検証に用いた利用者識別情報証明書 5 5 b から利用者識別情報を読み出すと (S T 4 0)、図 2 0 に示すように、この利用者識別情報と、正当を示す検証結果と、サービス提供ポリシー 2 3 b の検証結果であるサービス提供分類とをサービス提供装置 2 0 に送信する (S T 4 1)。

[0183] サービス提供装置 2 0 においては、利用者識別情報及び検証結果を受信すると (S T 4 2)、この検証結果が正当なとき、サービス提供部 2 2 が、この利用者識別情報に基づいて格納部 2 3 を検索し、当該利用者識別情報に関連付けられたサービス用利用者識別情報 (例、クレジットカード番号) を読出す (S T 4 3)。

[0184] サービス提供部 2 2 は、読み出したサービス用利用者識別情報に基づいて、図示しない記憶部から利用者向けのサービス情報を抽出し (S T 4 4)、利用者向けのサービス情報を利用者端末 1 0 に送信する (S T 4 5)。なお、利用者向けに提供されるサービス情報は、利用者情報 2 3 a のサービス提供分類のレベルと、検証装置 6 0 による検証結果であるサービス提供分類のレベルのうち、低い方のレベルのサービス情報である。なお、利用者識別情報証明書 5 5 b の利用者識別情報は T T P が付与したものであり、サービス提供装置 2 0 の運営者が付与したサービス用利用者識別情報とは異なるもの

である。

- [0185] 利用者端末 10 は、利用者向けのサービス情報を受信し（ST46）、処理を終了する（ST47）。
- [0186] 上述したように本実施形態によれば、認証コンテキスト c1、c2、機器証明書 44a、54a、評価報告書 44b、54b、利用者識別情報証明書 55b、サービス提供ポリシー 23b 及びチャレンジ値を用いて検証を実行する構成により、サービス用利用者識別情報を記載したクレジットカードやキャッシュカード等のカードの携行・提示を不要とし、利用者の本人確認を実行することができる。
- [0187] また、本実施形態においては、以下の〔1〕～〔7〕に示す観点から、認証構成プロセスが確実であることを検証することができる。
- [0188] 〔1〕 認証処理結果情報 b のフォーマットを検証する構成により、検証の元となる認証処理結果情報 b に不備がないことを確認できる。
- [0189] 〔2〕 認証子を検証する構成により、各ユニット装置 40、50 の実行内容及び実行結果に改竄がないことを確認できる。
- [0190] 〔3〕 機器証明書 44a、54b を検証する構成により、各ユニット装置 40、50 が正当な機器であることを確認できる。
- [0191] 〔4〕 利用者識別情報証明書 55b を検証する構成により、生体認証した利用者の正当な利用者識別情報であることを確認できる。
- [0192] 〔5〕 評価報告書 44b、54b を検証する構成により、各ユニット装置 40、50 がサービス提供ポリシーを満たすことを確認できる。
- [0193] 〔6〕 チャレンジ値を検証する構成により、認証処理結果情報 b の再送攻撃を受けていないことを確認できる。ここでいう再送攻撃（リプレイ攻撃）は、悪意の第三者が、ネットワーク上から利用者の認証処理結果情報 b を収集して保持し、後で再送信してその利用者になりすます攻撃を想定している。このような再送攻撃を受けた場合でも、チャレンジ値が認証処理毎に生成されるランダムな値であることから、チャレンジ値が不一致であれば、再送攻撃を受けた旨を検出できる。

[0194] [7] 実行結果検証機能により生体認証の実行結果が正当なことを確認することができる。

[0195] また、本実施形態では、利用者識別情報証明書 55b 内の利用者識別情報が、クレジットカード番号等のサービス用利用者識別情報とは異なるものであるため、サービス用利用者識別情報をネットワーク上に送信しないので、サービス用利用者識別情報の漏えいの可能性を低減することができる。補足すると、利用者がサービス用利用者識別情報を知らなくてもサービスを利用できるので、クレジットカードを廃止した場合には、利用者の不注意等によるサービス用利用者識別情報の漏えいを無くすることができる。

[0196] また、本実施形態に述べたサービス提供システムは、生体認証の様々なモデルに適用することができる。

[0197] 例えば、生体認証の OCM (On Card Matching) モデルの場合、第 1 ユニット装置 40 は生体データの収集及び信号処理を実行する。第 2 ユニット装置 50 は予め登録された参照生体情報であるテンプレートを保持し、第 1 ユニット装置 40 からの信号処理結果とテンプレートとを照合し、照合結果に基づく判定結果を出力する。

[0198] 生体認証の STOC (STore On Card) モデルの場合、第 1 ユニット装置 40 は生体データの収集及び信号処理を実行する。第 2 ユニット装置 50 は予め登録された参照生体情報であるテンプレートを保持し、第 1 ユニット装置 40 又は第 3 ユニット装置にテンプレートを供給する。なお、第 3 ユニット装置は、本実施形態では述べておらず、ここで初めて述べるものである。第 1 ユニット装置 40 又は第 3 ユニット装置は、第 1 ユニット装置 40 からの信号処理結果とテンプレートとを照合し、照合結果に基づく判定結果を出力する。第 3 ユニット装置の構成及び動作は、第 1 ユニット装置 40 とほぼ同様である。

[0199] (第 2 の実施形態)

図 21 は第 2 の実施形態に係るサービス提供システムの構成を示す模式図であり、図 1 と同種の部分には同一符号を付してその詳しい説明を省略し、

ここでは異なる部分について主に述べる。なお、以下の各実施形態も同様に  
して重複した説明を省略する。

[0200] 本実施形態は、第1の実施形態の変形例であり、マルチモーダル生体認証  
を用いた形態となっている。マルチモーダル生体認証とは、二つ以上の生体  
情報による照合結果を融合して判定を行うことにより、より精度の高い生体  
認証を実現することが可能となる生体認証である。

[0201] それぞれの生体情報について、第1の実施形態の最後に記載したOCMモ  
デルとSTOCモデルのいずれを採用しているかによってユニット装置の構  
成は変わるが、実際に使用されるテンプレートを含むユニット装置について  
は第1の実施形態の第2ユニット装置50と同様の動作をし、テンプレート  
を含まないユニット装置で認証構成プロセスを実行するものについては第1  
の実施形態の第1ユニット装置40と同様の動作をする。

[0202] ここではOCMモデルを用いるものとし、図示するように、第1方式の第  
1及び第2ユニット装置40、50と、第2方式の第1及び第2ユニット装  
置40、50とを備えている。なお、第1方式の第1及び第2ユニット装置  
40、50と、第2方式の第1及び第2ユニット装置40、50は、互いに  
生体認証方式（例、指紋認証方式と顔認証方式）が異なるだけであり、機能  
ブロックは互いに同一である。

[0203] ユニット統合装置30においては、図22に示すように、装置情報格納部  
33内のユニット装置構成情報33a'が各方式の第1及び第2ユニット装  
置40、50に応じて記述されたものとなる。

[0204] サービス提供装置20においては、図23に示すように、格納部23内の  
利用者情報23a'における利用者識別情報証明書の利用者識別情報と、T  
TP情報とが第1方式と第2方式の分だけ記述される。

[0205] また、格納部23内のサービス提供ポリシ23b'は、1つのサービスA  
において、生体認証構成プロセス情報と生体認証精度の基準値とが第1方式  
と第2方式の分だけ記述される。

[0206] そして、サービスAとサービスBについて、例えば、第1方式では生体認

証構成プロセス情報の $\alpha$ と $\gamma$ を有し、第2方式では生体認証構成プロセス情報の $\beta$ と $\delta$ を有している場合、第1方式で $\alpha$ と $\gamma$ 、第2方式で $\beta$ と $\delta$ 、の各々の生体認証構成プロセス情報を選択して使用することが出来る。これは、サービスAとサービスBには限られず、対象となるサービスに当てはまるものである。

[0207] 検証装置60においては、図24に示すように、格納部63の各ユニット装置40、50の秘密情報と同一の又は対応する情報及び公開鍵が第1方式と第2方式の分だけ記述される。

[0208] また、ユニット統合装置30が出力する認証処理結果情報bは、図25に示すように、第1方式と第2方式に応じて、第1及び第2ユニット装置特定情報と、認証構成プロセスP2の実行結果と、第1及び第2認証コンテキストc1、c2とが記述される。

[0209] 次に、以上のように構成されたサービス提供システムの動作を図26のフローチャートを用いて説明する。

[0210] ステップST1～ST7の処理は、前述同様に実行される。

[0211] ステップST8～ST26の処理は、第1方式の後に第2方式を実行するように実行される。

[0212] ステップST27～ST39の処理は、前述同様に実行される。

[0213] ステップST40の処理においては、検証装置60は、互いに異なる全ての利用者識別情報を読み取る。

[0214] ステップST41～ST42の処理は、前述同様に実行される。

[0215] ステップST43の処理においては、サービス提供装置20は、複数の利用者識別情報から検索を実行する。

[0216] 以下、ステップST44～ST47の処理は、前述同様に実行される。

[0217] 上述したように本実施形態によれば、第1方式の第1及び第2ユニット装置40、50と、第2方式の第1及び第2ユニット装置40、50とを備えた構成により、第1の実施形態をマルチモーダル生体認証に適用することができる。

[0218] (第3の実施形態)

次に、第3の実施形態に係るサービス提供システムについて説明する。

[0219] 本実施形態は、第1の実施形態の変形例であり、利用者識別情報証明書55bの変更に対するサービス提供装置20への影響を軽減させる観点から、サービス提供装置20が利用者識別情報証明書55bの利用者識別情報を保持しない形態となっている。

[0220] 具体的には、検証装置60の格納部63は、図27に示すように、前述した各ユニット装置40、50の秘密情報と同一の又は対応する情報及び公開鍵に加え、連携利用者情報63aを格納している。連携利用者情報63aは、利用者識別情報証明書55b内の利用者識別情報と、この利用者識別情報とは異なる値を有して利用者を識別する連携利用者識別情報とが関連付けて記述されている。この連携利用者情報63aは、利用者の氏名、住所、パスワード、口座番号、TTP情報、サービスIDなどを更に関連付けて記述してもよい。

[0221] 検証部62は、前述した利用者識別情報送信機能(f62-9)に代えて、次の連携利用者識別情報送信機能(f62-9)'をもっている。

[0222] (f62-9)' フォーマット検証機能、認証子検証機能、機器証明書検証機能、利用者識別情報証明書検証機能、評価報告書検証機能、チャレンジ値検証機能及び実行結果検証機能による全ての検証結果が正当のとき、利用者識別情報証明書検証機能による検証に用いた利用者識別情報証明書55b内の利用者識別情報に基づいて格納部63aから読み出した連携利用者識別情報と、正当を示す検証結果とをサービス提供装置20に送信する連携利用者識別情報送信機能。

[0223] 一方、サービス提供装置20の格納部23は、図28に示すように、前述した利用者情報23a内の「利用者識別情報証明書55bの利用者識別情報」に代えて、連携利用者識別情報が記述された利用者情報23a''を格納している。なお、利用者情報23a''内の連携利用者識別情報は、検証装置60の格納部63内の連携利用者識別情報と同一のものである。また、利用者

情報 2 3 a” 内のサービス用利用者識別情報は、この連携利用者識別情報及び「利用者識別情報証明書 5 5 b の利用者識別情報」とは異なる値を有して利用者を識別するものであり、連携利用者識別情報と関連付けられている。

[0224] サービス提供部 2 2 は、前述した読出機能 (f22-3) に代えて、次の連携読出機能 (f22-3)’ をもっている。

[0225] (f22-3)’ 検証装置 6 0 から連携利用者識別情報及び検証結果を受けると、この検証結果が正当なとき、この連携利用者識別情報に基づいて格納部 2 3 を検索し、当該連携利用者識別情報に関連付けられたサービス用利用者識別情報を読出す連携読出機能。

[0226] 次に、以上のように構成されたサービス提供システムの動作を図 2 9 のフローチャートを用いて説明する。

[0227] ステップ S T 1 ～ S T 4 0 までの処理は、前述同様に実行される。

[0228] 検証装置 6 0 の検証部 6 2 は、ステップ S T 4 0 で読み出した利用者識別情報に基づいて格納部 6 3 a から連携利用者識別情報を読み出し (S T 4 1’ - 1)、当該読み出した連携利用者識別情報と、正当を示す検証結果とをサービス提供装置 2 0 に送信する (S T 4 1’ - 2)。

[0229] サービス提供装置 2 0 は、連携利用者識別情報及び検証結果を受信すると (S T 4 2’)、この検証結果が正当なとき、この連携利用者識別情報に基づいて格納部 2 3 を検索し、当該連携利用者識別情報に関連付けられたサービス用利用者識別情報 (例、クレジットカード番号) を読み出し (S T 4 3’)、サービス提供部 2 2 から利用者向けのサービス情報を抽出し (S T 4 4)、利用者向けのサービス情報を利用者端末 1 0 に送信する (S T 4 5)。なお、連携利用者識別情報は検証装置 6 0 の運営者が付与したものであり、サービス提供装置 2 0 の運営者が付与したサービス用利用者識別情報とは異なるものである。

[0230] 利用者端末 1 0 は、利用者向けサービスを受信し (S T 4 6)、処理を終了する (S T 4 7)。

[0231] 上述したように本実施形態によれば、サービス提供装置 2 0 が利用者識別

証明書 5 5 b の利用者識別情報を保持しない構成により、第 1 の実施形態と同様の効果に加え、利用者識別情報の変更に対するサービス提供装置 2 0 への影響を軽減させることができる。

[0232] なお、本実施形態は、検証装置 6 0 とサービス提供装置 2 0 との間の変形例であるので、第 1 の実施形態の変形例に限らず、第 2 の実施形態の変形例としても適用することができる。

[0233] 以上説明した少なくとも一つの実施形態によれば、各認証コンテキスト c 1, c 2 が機器証明書 4 4 a, 5 4 a、評価報告書 4 4 b, 5 4 b、サービス提供装置 2 0 からのチャレンジ値、認証構成プロセスの実行結果のハッシュ値及び認証子を有し、第 2 認証コンテキスト c 2 が更に利用者識別情報証明書を有し、認証処理結果情報 b が認証構成プロセス P 2 の実行結果と各認証コンテキスト c 1, c 2 を有する構成により、検証装置 6 0 が各検証機能による検証を実行できる。このため、サービス用利用者識別情報を記載したカードの携行・提示を不要とし、利用者の本人確認を実行することができる。

[0234] また、サービス用利用者識別情報は、いずれの装置 1 0 ~ 6 0 も送受信しないので、サービス用利用者識別情報の漏えいの可能性を低減することができる。

[0235] なお、上記の各実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（CD-ROM、DVD など）、光磁気ディスク（MO）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

[0236] また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

[0237] また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働している OS（オペレーティングシステム）

や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が上記実施形態を実現するための各処理の一部を実行しても良い。

[0238] さらに、各実施形態における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

[0239] また、記憶媒体は1つに限らず、複数の媒体から上記の各実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

[0240] なお、各実施形態におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、上記の各実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

[0241] また、各実施形態におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

[0242] なお、本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

## 請求の範囲

### [請求項1]

生体認証を用いた認証処理を構成する認証構成プロセスを個別に実行する複数のユニット装置と、前記各ユニット装置を内蔵又は外部接続して当該各ユニット装置に通信可能なユニット統合装置と、前記ユニット統合装置を内蔵又は外部接続して当該ユニット統合装置に通信可能な利用者端末と、前記各認証構成プロセスの実行内容を認証子に基づいて検証する検証装置と、前記利用者端末及び前記検証装置に通信可能なサービス提供装置とを備えたサービス提供システムであって、

前記各ユニット装置は、

前記各ユニット装置に対して機器証明書発行者により公開鍵暗号方式に基づいて発行された機器証明書であって、前記認証構成プロセスの属するユニット装置の公開鍵又はメッセージ認証符号を生成するための秘密情報の識別情報と、前記認証構成プロセスの属するユニット装置を特定するユニット装置特定情報と、前記機器証明書発行者を特定する機器証明書発行者情報とを含む機器証明書本文と、前記機器証明書発行者の秘密鍵により前記機器証明書本文に対して生成されたデジタル署名とを含む前記機器証明書を格納する機器証明書格納手段と、

前記認証構成プロセスの実行に用いる前記ユニット装置特定情報と、生体認証アルゴリズムを含む生体認証構成プロセスを特定する生体認証構成プロセス情報と、前記生体認証アルゴリズムによる生体認証の精度を示す生体認証精度とを含む評価報告書を格納する評価報告書格納手段と、

前記認証子を生成するための秘密情報を格納する秘密情報格納手段と、

前記認証構成プロセスの実行を要求する認証構成プロセス実行要求とを前記ユニット統合装置から前記各ユニット装置が受けると、前記

認証構成プロセスを実行する認証構成プロセス実行手段と、

前記機器証明書、前記評価報告書、前記チャレンジ値及び前記実行内容のハッシュ値に基づいて、前記秘密情報により前記認証子を生成する認証子生成手段と、

前記機器証明書、前記評価報告書、前記チャレンジ値、前記実行内容のハッシュ値及び前記認証子が特定のフォーマットで記述された認証コンテキストを生成する認証コンテキスト生成手段と、

前記認証コンテキスト及び認証構成プロセスの実行結果が特定のフォーマットで記述された認証構成プロセス結果情報を生成する認証構成プロセス結果情報生成手段と、

前記認証構成プロセス結果情報を前記ユニット統合装置に送信する結果情報送信手段と、

を備えており、

前記各ユニット装置のうち、少なくとも1台のユニット装置は、

前記利用者端末の利用者に対して第三者機関により公開鍵暗号方式に基づいて発行された利用者識別情報証明書であって、前記利用者を識別する利用者識別情報と、前記利用者の生体参照情報のハッシュ値と、前記第三者機関を特定する第三者機関情報とを含む証明書本文と、前記第三者機関の秘密鍵により当該証明書本文に対して生成されたデジタル署名とを含む前記利用者識別情報証明書を格納する利用者識別情報証明書格納手段、を更に備えており、

前記少なくとも1台のユニット装置の認証子生成手段は、前記機器証明書、前記評価報告書、前記チャレンジ値、前記利用者識別情報証明書及び前記実行内容のハッシュ値に基づいて、前記秘密情報により前記認証子を生成し、

前記少なくとも1台のユニット装置の認証コンテキスト生成手段は、前記機器証明書、前記評価報告書、前記チャレンジ値、前記利用者識別情報証明書、前記実行内容のハッシュ値及び前記認証子が特定の

フォーマットで記述された認証コンテキストを生成し、

前記ユニット統合装置は、

前記各ユニット装置のユニット装置特定情報と、当該各ユニット装置が実行する認証構成プロセスにおける機能を示す機能名と、当該機能の処理順序を示す処理順序とを関連付けて格納する装置情報格納手段と、

前記認証処理の実行を要求する認証処理実行要求と、前記チャレンジ値とを前記利用者端末から受けると、前記装置情報格納手段内の処理順序及びユニット装置特定情報に従って、当該ユニット装置特定情報が特定するユニット装置へ当該チャレンジ値及び前記認証構成プロセス実行要求を送信する第1認証構成プロセス実行要求送信手段と、

前記認証構成プロセス実行要求の送信先のユニット装置から前記認証構成プロセス結果情報を受けると、前記装置情報格納手段内の処理順序及びユニット装置特定情報に基づいて、当該送信先のユニット装置の次の処理順序のユニット装置へ前記チャレンジ値及び前記認証構成プロセス実行要求を送信する第2認証構成プロセス実行要求送信手段と、

この認証構成プロセス実行要求の送信先のユニット装置から前記認証構成プロセス結果情報を受けると、前記ユニット装置構成情報内の処理順序及びユニット装置特定情報に基づいて、当該送信先のユニット装置が最後の処理順序のユニット装置のとき、前記各ユニット装置から受けた前記認証構成プロセス結果情報内の前記認証コンテキストと、前記最後の処理順序のユニット装置から受けた前記認証構成プロセス結果情報内の実行結果とが特定のフォーマットで記述された認証処理結果情報を生成する認証処理結果情報生成手段と、

前記認証処理結果情報を前記利用者端末に送信する認証処理結果情報送信手段と、

を備えており、

前記利用者端末は、

前記サービス提供装置に対してサービスを要求するサービス要求を当該サービス提供装置に送信するサービス要求送信手段と、

前記利用者に対して前記生体認証の実行を要求する認証要求と、前記チャレンジ値とを前記サービス提供装置から受けると、前記チャレンジ値及び前記認証処理実行要求を前記ユニット統合装置に送信する認証処理実行要求送信手段と、

前記ユニット統合装置から受けた認証処理結果情報を前記サービス提供装置に転送する転送手段と、

前記サービス提供装置から受けたサービス情報を表示する表示手段と、

を備えており、

前記サービス提供装置は、

前記利用者識別情報証明書内の利用者識別情報と、この利用者識別情報とは異なる値を有して前記利用者を識別するサービス用利用者識別情報とを関連付けて格納する利用者情報格納手段と、

前記利用者にサービスを提供する条件を示すサービス提供ポリシーであって、前記サービスを識別するサービス識別情報と、前記認証構成プロセスの実行に用いるユニット装置特定情報と、生体認証アルゴリズムを含む生体認証構成プロセスを特定する生体認証構成プロセス情報と、前記生体認証アルゴリズムによる生体認証精度を正当とみなす基準を示す基準値とを含む前記サービス提供ポリシーを格納するサービス提供ポリシー格納手段と、

前記利用者端末からサービス要求を受けると、前記チャレンジ値を生成して保持し、このチャレンジ値と前記認証要求とを前記利用者端末に送信する認証要求送信手段と、

前記利用者端末から認証処理結果情報を受けると、前記保持したチャレンジ値と当該認証処理結果情報と前記サービス提供ポリシーとを検

証装置に送信する送信手段と、

前記検証装置から利用者識別情報及び検証結果を受けると、この検証結果が正当なとき、この利用者識別情報に基づいて前記利用者情報格納手段を検索し、当該利用者識別情報に関連付けられたサービス用利用者識別情報を読み出す読出手段と、

当該読み出したサービス用利用者識別情報に基づいて、前記サービス情報を前記利用者端末に送信するサービス情報送信手段と、

とを備えており、

前記検証装置は、

前記各ユニット装置の機器証明書発行者の公開鍵と、前記第三者機関の公開鍵とを格納する公開鍵格納手段と、

前記サービス提供装置から前記チャレンジ値、前記認証処理結果情報及び前記サービス提供ポリシーを受信する受信手段と、

前記受信した認証処理結果情報が前記特定のフォーマットに適合していることを検証するフォーマット検証手段と、

前記受信した認証処理結果情報に記述された認証コンテキスト内の認証子を検証する認証子検証手段と、

前記受信した認証処理結果情報に記述された認証コンテキストに含まれる機器証明書内のデジタル署名を前記機器証明書発行者の公開鍵に基づいて検証する機器証明書検証手段と、

前記受信した認証処理結果情報に記述された認証コンテキストに含まれる利用者識別情報証明書内のデジタル署名を前記第三者機関の公開鍵に基づいて検証する利用者識別情報証明書検証手段と、

前記受信した認証処理結果情報に記述された認証コンテキストに含まれる評価報告書を、前記受信したサービス提供ポリシーに基づいて検証する評価報告書検証手段と、

前記受信した認証処理結果情報に記述された認証コンテキスト内のチャレンジ値を、前記受信したチャレンジ値に基づいて検証するチャ

レンジ値検証手段と、

前記受信した認証処理結果情報に記述された実行結果が正当を示すことを検証する実行結果検証手段と、

前記フォーマット検証手段、前記認証子検証手段、前記機器証明書検証手段、前記利用者識別情報証明書検証手段、前記評価報告書検証手段、前記チャレンジ値検証手段及び実行結果検証手段による全ての検証結果が正当のとき、前記利用者識別情報証明書検証手段による検証に用いた利用者識別情報証明書内の利用者識別情報と、正当を示す検証結果とを前記サービス提供装置に送信する利用者識別情報送信手段と、

を備えたことを特徴とするサービス提供システム。

[請求項2]

生体認証を用いた認証処理を構成する認証構成プロセスを個別に実行する複数のユニット装置と、前記各ユニット装置を内蔵又は外部接続して当該各ユニット装置に通信可能なユニット統合装置と、前記ユニット統合装置を内蔵又は外部接続して当該ユニット統合装置に通信可能な利用者端末と、前記各認証構成プロセスの実行内容を認証子に基づいて検証する検証装置と、前記利用者端末及び前記検証装置に通信可能なサービス提供装置とを備えたサービス提供システムであって、

前記各ユニット装置は、

前記各ユニット装置に対して機器証明書発行者により公開鍵暗号方式に基づいて発行された機器証明書であって、前記認証構成プロセスの属するユニット装置の公開鍵又はメッセージ認証符号を生成するための秘密情報の識別情報と、前記認証構成プロセスの属するユニット装置を特定するユニット装置特定情報と、前記機器証明書発行者を特定する機器証明書発行者情報とを含む機器証明書本文と、前記機器証明書発行者の秘密鍵により前記機器証明書本文に対して生成されたデジタル署名とを含む前記機器証明書を格納する機器証明書格納手段と

、

前記認証構成プロセスの実行に用いる前記ユニット装置特定情報と、生体認証アルゴリズムを含む生体認証構成プロセスを特定する生体認証構成プロセス情報と、前記生体認証アルゴリズムによる生体認証の精度を示す生体認証精度とを含む評価報告書を格納する評価報告書格納手段と、

前記認証子を生成するための秘密情報を格納する秘密情報格納手段と、

前記認証構成プロセスの実行を要求する認証構成プロセス実行要求とを前記ユニット統合装置から前記各ユニット装置が受けると、前記認証構成プロセスを実行する認証構成プロセス実行手段と、

前記機器証明書、前記評価報告書、前記チャレンジ値及び前記実行内容のハッシュ値に基づいて、前記秘密情報により前記認証子を生成する認証子生成手段と、

前記機器証明書、前記評価報告書、前記チャレンジ値、前記実行内容のハッシュ値及び前記認証子が特定のフォーマットで記述された認証コンテキストを生成する認証コンテキスト生成手段と、

前記認証コンテキスト及び認証構成プロセスの実行結果が特定のフォーマットで記述された認証構成プロセス結果情報を生成する認証構成プロセス結果情報生成手段と、

前記認証構成プロセス結果情報を前記ユニット統合装置に送信する結果情報送信手段と、

を備えており、

前記各ユニット装置のうち、少なくとも1台のユニット装置は、

前記利用者端末の利用者に対して第三者機関により公開鍵暗号方式に基づいて発行された利用者識別情報証明書であって、前記利用者を識別する利用者識別情報と、前記利用者の生体参照情報のハッシュ値と、前記第三者機関を特定する第三者機関情報とを含む証明書本文と

、前記第三者機関の秘密鍵により当該証明書本文に対して生成されたデジタル署名とを含む前記利用者識別情報証明書を格納する利用者識別情報証明書格納手段、を更に備えており、

前記少なくとも 1 台のユニット装置の認証子生成手段は、前記機器証明書、前記評価報告書、前記チャレンジ値、前記利用者識別情報証明書及び前記実行内容のハッシュ値に基づいて、前記秘密情報により前記認証子を生成し、

前記少なくとも 1 台のユニット装置の認証コンテキスト生成手段は、前記機器証明書、前記評価報告書、前記チャレンジ値、前記利用者識別情報証明書、前記実行内容のハッシュ値及び前記認証子が特定のフォーマットで記述された認証コンテキストを生成し、

前記ユニット統合装置は、

前記各ユニット装置のユニット装置特定情報と、当該各ユニット装置が実行する認証構成プロセスにおける機能を示す機能名と、当該機能の処理順序を示す処理順序とを関連付けて格納する装置情報格納手段と、

前記認証処理の実行を要求する認証処理実行要求と、前記チャレンジ値とを前記利用者端末から受けると、前記装置情報格納手段内の処理順序及びユニット装置特定情報に従って、当該ユニット装置特定情報が特定するユニット装置へ当該チャレンジ値及び前記認証構成プロセス実行要求を送信する第 1 認証構成プロセス実行要求送信手段と、

前記認証構成プロセス実行要求の送信先のユニット装置から前記認証構成プロセス結果情報を受けると、前記装置情報格納手段内の処理順序及びユニット装置特定情報に基づいて、当該送信先のユニット装置の次の処理順序のユニット装置へ前記チャレンジ値及び前記認証構成プロセス実行要求を送信する第 2 認証構成プロセス実行要求送信手段と、

この認証構成プロセス実行要求の送信先のユニット装置から前記認

証構成プロセス結果情報を受けると、前記ユニット装置構成情報内の処理順序及びユニット装置特定情報に基づいて、当該送信先のユニット装置が最後の処理順序のユニット装置のとき、前記各ユニット装置から受けた前記認証構成プロセス結果情報内の前記認証コンテキストと、前記最後の処理順序のユニット装置から受けた前記認証構成プロセス結果情報内の実行結果とが特定のフォーマットで記述された認証処理結果情報を生成する認証処理結果情報生成手段と、

前記認証処理結果情報を前記利用者端末に送信する認証処理結果情報送信手段と、

を備えており、

前記利用者端末は、

前記サービス提供装置に対してサービスを要求するサービス要求を当該サービス提供装置に送信するサービス要求送信手段と、

前記利用者に対して前記生体認証の実行を要求する認証要求と、前記チャレンジ値とを前記サービス提供装置から受けると、前記チャレンジ値及び前記認証処理実行要求を前記ユニット統合装置に送信する認証処理実行要求送信手段と、

前記ユニット統合装置から受けた認証処理結果情報を前記サービス提供装置に転送する転送手段と、

前記サービス提供装置から受けたサービス情報を表示する表示手段と、

を備えており、

前記サービス提供装置は、

前記利用者識別情報証明書内の利用者識別情報とは異なる値を有して前記利用者を識別する連携利用者識別情報と、この連携利用者識別情報及び前記利用者識別情報とは異なる値を有して前記利用者を識別するサービス用利用者識別情報とを関連付けて格納するサービス用利用者情報格納手段と、

前記利用者にサービスを提供する条件を示すサービス提供ポリシーであって、前記サービスを識別するサービス識別情報と、前記認証構成プロセスの実行に用いるユニット装置特定情報と、生体認証アルゴリズムを含む生体認証構成プロセスを特定する生体認証構成プロセス情報と、前記生体認証アルゴリズムによる生体認証精度を正当とみなす基準を示す基準値とを含む前記サービス提供ポリシーを格納するサービス提供ポリシー格納手段と、

前記利用者端末からサービス要求を受けると、前記チャレンジ値を生成して保持し、このチャレンジ値と前記認証要求とを前記利用者端末に送信する認証要求送信手段と、

前記利用者端末から認証処理結果情報を受けると、前記保持したチャレンジ値と当該認証処理結果情報と前記サービス提供ポリシーとを検証装置に送信する送信手段と、

前記検証装置から連携利用者識別情報及び検証結果を受けると、この検証結果が正当なとき、この連携利用者識別情報に基づいて前記サービス用利用者情報格納手段を検索し、当該連携利用者識別情報に関連付けられたサービス用利用者識別情報を読み出す連携読出手段と、

当該読み出したサービス用利用者識別情報に基づいて、前記サービス情報を前記利用者端末に送信するサービス情報送信手段と、

とを備えており、

前記検証装置は、

前記各ユニット装置の機器証明書発行者の公開鍵と、前記第三者機関の公開鍵とを格納する公開鍵格納手段と、

前記サービス提供装置から前記チャレンジ値、前記認証処理結果情報及び前記サービス提供ポリシーを受信する受信手段と、

前記受信した認証処理結果情報が前記特定のフォーマットに適合していることを検証するフォーマット検証手段と、

前記受信した認証処理結果情報に記述された認証コンテキスト内の

認証子を検証する認証子検証手段と、

前記受信した認証処理結果情報に記述された認証コンテキストに含まれる機器証明書内のデジタル署名を前記機器証明書発行者の公開鍵に基づいて検証する機器証明書検証手段と、

前記受信した認証処理結果情報に記述された認証コンテキストに含まれる利用者識別情報証明書内のデジタル署名を前記第三者機関の公開鍵に基づいて検証する利用者識別情報証明書検証手段と、

前記受信した認証処理結果情報に記述された認証コンテキストに含まれる評価報告書を、前記受信したサービス提供ポリシーに基づいて検証する評価報告書検証手段と、

前記受信した認証処理結果情報に記述された認証コンテキスト内のチャレンジ値を、前記受信したチャレンジ値に基づいて検証するチャレンジ値検証手段と、

前記受信した認証処理結果情報に記述された実行結果が正当を示すことを検証する実行結果検証手段と、

前記利用者識別情報証明書内の利用者識別情報と、この利用者識別情報とは異なる値を有して前記利用者を識別する前記連携利用者識別情報と同一の連携利用者識別情報とを関連付けて格納する連携利用者情報格納手段と、

前記フォーマット検証手段、前記認証子検証手段、前記機器証明書検証手段、前記利用者識別情報証明書検証手段、前記評価報告書検証手段、前記チャレンジ値検証手段及び前記実行結果検証手段による全ての検証結果が正当のとき、前記利用者識別情報証明書検証手段による検証に用いた利用者識別情報証明書内の利用者識別情報に基づいて前記連携利用者情報格納手段から読み出した連携利用者識別情報と、正当を示す検証結果とを前記サービス提供装置に送信する連携利用者識別情報送信手段と、

を備えたことを特徴とするサービス提供システム。

- [請求項3]           請求項1又は請求項2に記載のサービス提供システムにおいて、  
前記認証子検証手段は、前記各ユニット装置により生成された認証子を当該各ユニット装置における前記秘密情報と同一の又は対応する情報に基づいて検証することを特徴とするサービス提供システム。
- [請求項4]           請求項1又は請求項2に記載のサービス提供システムにおいて、  
前記秘密情報記憶手段内の秘密情報は、公開鍵暗号方式における秘密鍵であり、  
前記認証子生成手段により生成された認証子は、この秘密鍵に基づいて生成されたデジタル署名であることを特徴とするサービス提供システム。
- [請求項5]           生体認証を用いた認証処理を構成する認証構成プロセスを個別に実行する複数のユニット装置と、前記各ユニット装置を内蔵又は外部接続して当該各ユニット装置に通信可能なユニット統合装置と、前記ユニット統合装置を内蔵又は外部接続して当該ユニット統合装置に通信可能な利用者端末と、前記各認証構成プロセスの実行内容を認証子に基づいて検証する検証装置と、前記利用者端末及び前記検証装置に通信可能なサービス提供装置とを備えたサービス提供システムに用いられる前記各ユニット装置のうち、少なくとも1台のユニット装置であって、  
前記各ユニット装置に対して機器証明書発行者により公開鍵暗号方式に基づいて発行された機器証明書であって、前記認証構成プロセスの属するユニット装置の公開鍵又はメッセージ認証符号を生成するための秘密情報の識別情報と、前記認証構成プロセスの属するユニット装置を特定するユニット装置特定情報と、前記機器証明書発行者を特定する機器証明書発行者情報とを含む機器証明書本文と、前記機器証明書発行者の秘密鍵により前記機器証明書本文に対して生成されたデジタル署名とを含む前記機器証明書を格納する機器証明書格納手段と、

前記認証構成プロセスの実行に用いる前記ユニット装置特定情報と、生体認証アルゴリズムを含む生体認証構成プロセスを特定する生体認証構成プロセス情報と、前記生体認証アルゴリズムによる生体認証の精度を示す生体認証精度とを含む評価報告書を格納する評価報告書格納手段と、

前記利用者端末の利用者に対して第三者機関により公開鍵暗号方式に基づいて発行された利用者識別情報証明書であって、前記利用者を識別する利用者識別情報と、前記利用者の生体参照情報のハッシュ値と、前記第三者機関を特定する第三者機関情報とを含む証明書本文と、前記第三者機関の秘密鍵により当該証明書本文に対して生成されたデジタル署名とを含む前記利用者識別情報証明書を格納する利用者識別情報証明書格納手段と、

前記認証子を生成するための秘密情報を格納する秘密情報格納手段と、

前記認証構成プロセスの実行を要求する認証構成プロセス実行要求とを前記ユニット統合装置から受けると、前記認証構成プロセスを実行する認証構成プロセス実行手段と、

前記機器証明書、前記評価報告書、前記チャレンジ値、前記利用者識別情報証明書及び前記実行内容のハッシュ値に基づいて、前記秘密情報により前記認証子を生成する認証子生成手段と、

前記機器証明書、前記評価報告書、前記チャレンジ値、前記利用者識別情報証明書、前記実行内容のハッシュ値及び前記認証子が特定のフォーマットで記述された認証コンテキストを生成する認証コンテキスト生成手段と、

前記認証コンテキスト及び認証構成プロセスの実行結果が特定のフォーマットで記述された認証構成プロセス結果情報を生成する認証構成プロセス結果情報生成手段と、

前記認証構成プロセス結果情報を前記ユニット統合装置に送信する

結果情報送信手段と、

を備えており、

前記認証構成プロセス結果情報は、前記ユニット統合装置により認証コンテキスト及び実行結果が抽出され、

当該抽出された認証コンテキスト及び実行結果は、前記ユニット統合装置により特定のフォーマットで認証処理結果情報に記述され、

当該認証処理結果情報は、前記ユニット統合装置から前記利用者端末を介して前記サービス提供装置に送信され、前記サービス提供装置により当該認証処理結果情報に前記チャレンジ値及びサービス提供ポリシーが付加されて前記検証装置に送信された後、前記検証装置により当該認証コンテキスト及び実行結果が抽出され、前記検証装置により、当該実行結果と、当該認証処理結果情報のフォーマットと、当該認証コンテキスト内の前記認証子、前記機器証明書、前記評価報告書、前記利用者識別情報証明書及び前記チャレンジ値がそれぞれ検証されることを特徴とするユニット装置。