(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6632483号
(P6632483)
(45)発行日　令和2年1月22日(2020.1.22)　(24)登録日　令和1年12月20日(2019.12.20)

(51)Int.Cl.			F I		
H04L	9/14	(2006.01)	H04L	9/00	641
H04L	9/08	(2006.01)	H04L	9/00	601D
H04R	25/00	(2006.01)	H04R	25/00	M

請求項の数 15　外国語出願　(全 25 頁)

(21)出願番号　特願2016-128038(P2016-128038)
(22)出願日　平成28年6月28日(2016.6.28)
(65)公開番号　特開2017-34661(P2017-34661A)
(43)公開日　平成29年2月9日(2017.2.9)
審査請求日　令和1年5月16日(2019.5.16)
(31)優先権主張番号　PA201570438
(32)優先日　平成27年7月2日(2015.7.2)
(33)優先権主張国・地域又は機関
デンマーク(DK)
(31)優先権主張番号　15175142.7
(32)優先日　平成27年7月2日(2015.7.2)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

早期審査対象出願

(73)特許権者　503021401
ジーエヌ　ヒアリング　エー／エス
ＧＮ　Ｈｅａｒｉｎｇ　Ａ／Ｓ
デンマーク　２７５０　バレルプ　ラウトルップビェアウ　７
Ｌａｕｔｒｕｐｂｊｅｒｇ　７，　２７５０　Ｂａｌｌｅｒｕｐ，　Ｄｅｎｍａｒｋ
(74)代理人　110000110
特許業務法人快友国際特許事務所
(72)発明者　ペダーセン　ブライアン　ダム
デンマーク　４１００　リングステズ　バレッテン　７９
(72)発明者　ヴェネルボー　アラン　ムンク
デンマーク　２５００　バルビュー　レンボー　アリ　４

最終頁に続く

(54)【発明の名称】聴覚デバイスを製造する方法および証明書を備える聴覚デバイス

(57)【特許請求の範囲】
【請求項１】
聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットと、
メモリユニットと、
インターフェースとを備え、
前記メモリユニットは、外部エンティティとの通信を安全にするためにそこに記憶される聴覚デバイス証明書を有し、前記聴覚デバイス証明書は
聴覚デバイス識別子と、
複数の聴覚デバイス鍵と、
外部エンティティとの通信を安全にするための鍵素材として使用される複数の前記聴覚デバイス鍵の１つを示す少なくとも１つの聴覚デバイス鍵識別子とを備える聴覚デバイス。
【請求項２】
前記複数の聴覚デバイス鍵は、第１の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第１のセットを含み、前記少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の前記第１のセットのうちの聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子を含む請求項１に記載の聴覚デバイス。
【請求項３】
前記複数の聴覚デバイス鍵は、第２の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第２のセットを含み、前記少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の前記

第２のセットのうちの聴覚デバイス鍵を示す第２の聴覚デバイス鍵識別子を含む請求項１または２に記載の聴覚デバイス。
【請求項４】
前記聴覚デバイス証明書は、証明書タイプ識別子、署名デバイス識別子、１つまたは複数のハードウェア識別子、クライアントデバイスタイプ認証識別子、および／またはトークンパラメータのうちの１つまたは複数を備える請求項１から３のいずれか一項に記載の聴覚デバイス。
【請求項５】
前記聴覚デバイス証明書は、ハードウェアプラットフォーム識別子、ソフトウェアプラットフォーム識別子、および／または証明書タイムスタンプを備える請求項１から４のいずれか一項に記載の聴覚デバイス。
【請求項６】
前記聴覚デバイス証明書は、デジタル署名および／またはメッセージ認証コードを備える請求項１から５のいずれか一項に記載の聴覚デバイス。
【請求項７】
聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットと、メモリユニットと、インターフェースとを備える前記聴覚デバイスを製造する方法であって、
聴覚デバイス識別子を生成するステップと、
前記聴覚デバイス識別子に基づいて１つまたは複数の聴覚デバイス鍵を生成するステップと、
前記聴覚デバイス識別子と前記生成された聴覚デバイス鍵のうちの少なくとも１つとを含む聴覚デバイス証明書を生成するステップと、
前記生成された聴覚デバイス証明書を、前記メモリユニットが前記聴覚デバイス証明書を記憶していない前記聴覚デバイスに送信するステップであって、前記聴覚デバイス証明書は前記聴覚デバイスの外部エンティティとの通信を安全にするためのものであるステップと、
前記聴覚デバイスに送信された前記聴覚デバイス証明書を前記メモリユニットに記憶するステップとを含む方法。
【請求項８】
第１のクライアントデバイス鍵を含む１つまたは複数のクライアントデバイス鍵を取得するステップを含み、１つまたは複数の聴覚デバイス鍵を生成するステップは、前記第１のクライアントデバイス鍵に基づく請求項７に記載の方法。
【請求項９】
１つまたは複数の聴覚デバイス鍵を生成するステップは、第１の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第１のセットを生成するステップを含み、前記方法は聴覚デバイス鍵の前記第１のセットの聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子を取得するステップを含み、前記聴覚デバイス証明書を生成するステップは、聴覚デバイス鍵の前記第１のセットと前記第１の聴覚デバイス鍵識別子とを前記聴覚デバイス証明書に入れるステップを含む請求項７から８のいずれか一項に記載の方法。
【請求項１０】
１つまたは複数の聴覚デバイス鍵を生成するステップは、第２の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第２のセットを生成するステップを含み、前記方法は聴覚デバイス鍵の前記第２のセットの聴覚デバイス鍵を示す第２の聴覚デバイス鍵識別子を取得するステップを含み、前記聴覚デバイス証明書を生成するステップは、聴覚デバイス鍵の前記第２のセットと前記第２の聴覚デバイス鍵識別子とを前記聴覚デバイス証明書に入れるステップを含む請求項７から９のいずれか一項に記載の方法。
【請求項１１】
前記聴覚デバイス証明書を生成するステップは、デジタル署名を生成するステップと、前記デジタル署名を前記聴覚デバイス証明書中に入れるステップとを含む請求項７から１０のいずれか一項に記載の方法。

【請求項１２】
前記聴覚デバイス識別子を生成するステップは、乱数または疑似乱数を生成するステップを含む請求項７から１１のいずれか一項に記載の方法。
【請求項１３】
前記聴覚デバイスの第１のハードウェア識別子を取得するステップを含み、前記聴覚デバイス証明書を生成するステップは、前記第１のハードウェア識別子を前記聴覚デバイス証明書に入れるステップを含む請求項７から１２のいずれか一項に記載の方法。
【請求項１４】
前記聴覚デバイス証明書を生成するステップは、証明書タイプ識別子、署名デバイス識別子、１つまたは複数のハードウェア識別子、クライアントデバイスタイプ認証識別子、および／またはトークンパラメータのうちの１つまたは複数を前記聴覚デバイス証明書に入れるステップを含む請求項７から１３のいずれか一項に記載の方法。
【請求項１５】
前記聴覚デバイス証明書を生成するステップは、ハードウェアプラットフォーム識別子、ソフトウェアプラットフォーム識別子、および／または証明書タイムスタンプを前記聴覚デバイス証明書に入れるステップを含む請求項７から１４のいずれか一項に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、聴覚デバイスの分野に関し、詳細には、聴覚デバイスのセキュリティに関する。本開示は、１つまたは複数の証明書を備える聴覚デバイス、および聴覚デバイスを製造する方法に関する。
【背景技術】
【０００２】
聴覚デバイスの機能は、次第に高度化してきている。聴覚デバイスと、聴覚デバイスフィッティング装置、タブレット、スマートフォン、スマートウォッチおよびリモートコントローラなどの外部デバイスとの間のワイヤレス通信が発展している。聴覚デバイスのワイヤレス通信インターフェースは、オープン標準ベースのインターフェースを使用する。しかしながら、このことは、セキュリティに関して多くの問題を提起する。聴覚デバイスは、受信したデータを合法的であるとみなし、不正なものによるメモリへの書き込みまたは変更を許し得る。そのような攻撃があると、その結果、補聴器の誤動作、またはバッテリ消耗攻撃が引き起こされ得る。
【０００３】
しかしながら、聴覚デバイスは、計算能力、メモリ空間などに関して厳しい制約条件が課せられている非常に小型のデバイスである。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
セキュリティが改善されている方法および聴覚デバイスが必要である。
【課題を解決するための手段】
【０００５】
開示されるのは、聴覚デバイスである。聴覚デバイスは、処理ユニットと、メモリユニットと、インターフェースとを備える。メモリユニットは、そこに記憶される１つまたは複数の証明書を有しているものとしてよい。メモリユニットは、そこに記憶される聴覚デバイス証明書を有する。聴覚デバイス証明書は、聴覚デバイス識別子、聴覚デバイス鍵を示す少なくとも１つの聴覚デバイス鍵識別子、および１つまたは複数の聴覚デバイス鍵を備え得る。
【０００６】
聴覚デバイスを製造する方法も開示されている。聴覚デバイスは、聴覚デバイスのユー

ザの聴力損失を補うように構成された処理ユニットと、メモリユニットと、インターフェースとを備える。方法は、聴覚デバイス識別子を生成することを含む。方法は、聴覚デバイス識別子に基づいて１つまたは複数の聴覚デバイス鍵を生成することを含み得る。方法は、聴覚デバイス識別子と生成された聴覚デバイス鍵のうちの少なくとも１つとを含む聴覚デバイス証明書を生成することと、聴覚デバイス証明書を聴覚デバイスに送信することとを含む。

【０００７】

開示されているような方法および装置は、セキュリティが改善された聴覚デバイスを製造するための拡張可能なセキュリティアーキテクチャを備える。本明細書で開示されている聴覚デバイスは、有利には、受信されたデータの完全性を検証し、改竄を検出し、例えば保守、フィッティングセッション、および／または遠隔チューニングのため改竄されたデータを無視する。開示されている聴覚デバイスおよび聴覚デバイスを製造するための方法は、例えばフィッティング目的、更新目的、保守目的で、クライアントデバイスなどの正当なものへのアクセスをそのまま許しながら、聴覚デバイスの不正アクセスまたは制御などの攻撃を除去しようとする際に聴覚デバイスをサポートする。本明細書で開示されている聴覚デバイスは、認証されたフィッティングデバイス、認証されたアクセサリデバイス、認証された外部デバイス、および／または認証されたサーバなどの、認証されたもののみとのセッションを開くという利点を有する。これは、偽装およびなりすまし攻撃、バッテリ消耗攻撃、盗聴、介入者攻撃、および／または反射攻撃に対するロバスト性をもたらし得る。さらに、クライアントデバイス側で鍵が損なわれた場合の鍵の更新および／または交換の必要性が減じ、簡素化されている。さらに、有利には、聴覚デバイス鍵は、聴覚デバイスに対して一意であり、それにより、聴覚デバイス鍵からクライアントデバイス鍵を導出することが事実上不可能になる。

【０００８】

上記、および他の特徴ならびに利点は、添付図面を参照する例示的な実施形態の以下の「発明を実施するための形態」の説明により、当業者にとって容易に理解できるものとなるであろう。

【図面の簡単な説明】

【０００９】

【図１】本開示による例示的なアーキテクチャの概略図である。

【図２】例示的な聴覚デバイスの概略図である。

【図３】例示的な聴覚デバイス証明書の概略図である。

【図４】例示的な信号図の概略図である。

【図５】例示的な方法のフローチャートの概略図である。

【発明を実施するための形態】

【００１０】

以下では、図面を参照しながら、様々な実施形態について説明する。全体を通して同様の参照番号は、同様の要素を指す。したがって、同様の要素については、それぞれの図の説明に関して詳しくは説明しない。図面は、実施形態の説明を容易にすることのみ意図されていることにも留意されたい。これらは、特許請求の範囲に記載された発明の網羅的説明として、または特許請求の範囲に記載された発明の技術的範囲の限定として、意図されていない。さらに、図示されている実施形態は、図示されているすべての態様または利点を有している必要はない。特定の実施形態と併せて説明されている態様または利点は、必ずしもその実施形態に限定されず、そのように図示されていない、またはそのように明示的に説明されていないとしても他の任意の実施形態で実施され得る。

【００１１】

本明細書全体を通して、同じ参照番号は、同一のまたは対応する、部分に対して使用される。

【００１２】

本開示の目的は、当技術分野における上述の欠点および不利点のうちの１つまたは複数

を、単独で、または組み合わせて、軽減するか、緩和するか、または排除しようとする、聴覚デバイスを実現および聴覚デバイスを製造する方法を提供することである。

【００１３】

本開示は、聴覚デバイスの改善されたセキュリティに関する。すなわち、本明細書で開示されている聴覚デバイスは、脅威および攻撃から保護するためのセキュリティメカニズムなどの適切な保護手段および対抗策を実装することによってセキュリティ脅威、脆弱性、および攻撃に対してロバストである。本開示は、反射攻撃、不正アクセス、バッテリ消耗攻撃、および介入者攻撃に対してロバストである聴覚デバイスに関する。

【００１４】

本明細書で使用されるとき、「聴覚デバイス」という用語は、聴覚器具、補聴デバイス、ヘッドセット、一組のヘッドフォンなどの、ユーザが音を聴くのを補助するように構成されたデバイスを指す。

【００１５】

本明細書で使用されるとき、「証明書」という用語は、デバイスの素性および内容の正当性および／または真正性を検証することなどの、デバイスの素性および内容の検証を可能にするデータ構造体を指す。証明書は、署名者の発行者によって証明書の保有者に関連付けられている内容を提示するように構成される。証明書は、適宜、１つまたは複数の暗号鍵（例えば、聴覚デバイス鍵）などの、鍵素材、および／またはデジタル署名を備えており、したがって、証明書の受領者は、証明書の内容および素性を検証または認証することができる。これにより、証明書は、素性および内容の認証、否認防止、および／または完全性保護を達成することを可能にする。証明書は、有効期間、１つまたは複数のアルゴリズムパラメータ、および／または発行者をさらに含み得る。証明書は、デジタル証明書、公開鍵証明書、属性証明書、および／または認証証明書を含むものとしてよい。証明書の例として、Ｘ．５０９証明書、およびＳｅｃｕｒｅ／Ｍｕｌｔｉｐｕｒｐｏｓｅ Ｉｎｔｅｒｎｅｔ Ｍａｉｌ Ｅｘｔｅｎｓｉｏｎｓ（Ｓ／ＭＩＭＥ）証明書、および／またはＴｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ（ＴＬＳ）証明書が挙げられる。

【００１６】

本明細書で使用されるとき、「鍵」という用語は、暗号鍵、すなわち、暗号アルゴリズムの機能的出力を決定するデータ（例えば、文字列、パラメータ）を指す。例えば、鍵は、暗号化ではプレーンテキストから暗号文への変換、および復号ではその逆の変換を行うことを可能にする。鍵は、デジタル署名および／またはメッセージ認証コード（ＭＡＣ）を検証するためにも使用され得る。鍵は、同じ鍵が暗号化と復号の両方に使用されるとき、いわゆる対称鍵である。非対称暗号法または公開鍵暗号法では、鍵素材は、鍵ペアであり、いわゆる、公開鍵と秘密鍵とを備える秘密／公開鍵ペアである。非対称または公開鍵暗号システム（Ｒｉｖｅｓｔ Ｓｈａｍｉｒ Ａｄｅｌｍａｎ（ＲＳＡ）暗号システム、または楕円曲線暗号法（ＥＣＣ）など）では、公開鍵は、暗号化および／または署名検証に使用され、秘密鍵は、復号および／または署名生成に使用される。聴覚デバイス鍵は、聴覚デバイス通信のためのセッション鍵および／または証明書鍵などの、１つまたは複数の対称鍵の導出を可能にする鍵素材であるものとしてよい。聴覚デバイス鍵は、聴覚デバイス証明書に含まれるものとしてよく、また、例えば、製造時に、聴覚デバイスのメモリユニットに記憶され得る。聴覚デバイス鍵は、対称鍵を導出するために使用される鍵素材を備え得る。聴覚デバイス鍵は、例えば、ＡＥＳ－１２８ビット鍵などの、Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＡＥＳ）鍵を含む。

【００１７】

本開示は、聴覚デバイスに関する。聴覚デバイスは、処理ユニットと、メモリユニットと、インターフェースとを備える。メモリユニットは、限定はしないが、読出し専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、などを含む、取り外し可能および取り外し不可能データ記憶ユニットを含み得る。聴覚デバイスは、聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットを備え得る。インターフェースは、例えば、２．４から２．５ＧＨｚの範囲内の周波数でワイヤレス通信するように構成された、ワ

イヤレストランシーバを備え得る。１つまたは複数の例示的な聴覚デバイスにおいて、インターフェースは、データを受信し、および／または送信するように構成されたワイヤレストランシーバをそれぞれ備える、クライアントデバイスまたは聴覚デバイスと、ワイヤレス通信などの、通信を行うように構成される。処理ユニットは、受信されたデータに従って聴覚デバイスのユーザの聴力損失を補うように構成され得る。聴覚デバイスは、インターフェースを介して聴覚デバイス証明書を受信し、および／または製造デバイスが聴覚デバイス証明書に書き込むためにメモリユニットにアクセスすることを可能にするように構成され得る。メモリユニットは、そこに記憶される聴覚デバイス証明書を有する。メモリユニットは、指定されたメモリセル内、および／または指定されたアドレスなど、メモリユニットのメモリアドレスに、および／またはメモリユニットのメモリセル内に記憶される聴覚デバイス証明書を有するものとしてよい。聴覚デバイス証明書は、聴覚デバイス識別子を備え得る。聴覚デバイス証明書は、聴覚デバイス鍵を示す少なくとも１つの聴覚デバイス鍵識別子を備え得る。聴覚デバイス証明書は、１つまたは複数の聴覚デバイス鍵を備え得る。聴覚デバイス識別子は、聴覚デバイスの一意の識別子を指すものとしてよい。本明細書で使用されるとき、「識別子」という用語は、分類する、および／または一意に識別するなど、識別するために使用されるデータを指す。識別子は、単語、数、英字、記号、リスト、配列、またはこれらの任意の組合せの形態をとり得る。例えば、数としての識別子は、符号なし整数の配列など、長さが例えば８ビット、１６ビット、３２ビットなどの、符号なし整数（ｕｉｎｔ）などの整数の形態をとり得る。聴覚デバイス鍵識別子は、クライアントデバイスなどの、外部者との通信を保護するための鍵素材として使用されるべき聴覚デバイス鍵を示し得る。聴覚デバイス鍵識別子は、どの聴覚デバイス鍵が、聴覚デバイス証明書の一部であるかを示し得る。例えば、値「５」を有する第１の聴覚デバイス鍵識別子は、聴覚デバイス証明書が識別子「５」を備える第１の聴覚デバイス鍵を含むことを示しており、場合によっては、証明書中の聴覚デバイス鍵の数に応じて、識別子「６」、「７」、「８」などを備える聴覚デバイス鍵など、識別子が増分することもある。例えば、聴覚デバイス鍵識別子は、複数の聴覚デバイス鍵のうちの１つの聴覚デバイス鍵を指し、および／または識別する。

【００１８】

本明細書で使用されている「クライアントデバイス」という用語は、聴覚デバイスと通信することができるデバイスを指す。クライアントデバイスは、クライアントとして動作するコンピューティングデバイスを指すものとしてよい。クライアントデバイスは、フィッティングデバイス、ハンドヘルドデバイス、リレー、タブレット、パーソナルコンピュータ、携帯電話、パーソナルコンピュータもしくはタブレットまたは携帯電話上で実行されるアプリケーション、および／またはパーソナルコンピュータにプラグ接続されるＵＳＢドングルを含み得る。クライアントデバイスは、フィッティングタイプ、例えば、聴覚デバイスをフィッティングするためのタブレット製品モデル、カテゴリ、またはタイプ、聴覚デバイスをフィッティングするためのＵＳＢドングル製品モデル、カテゴリ、またはタイプなどの、クライアントデバイスのモデル、カテゴリ、またはタイプに対応するクライアントデバイスタイプを割り当てられ得る。クライアントデバイスは、フィッティングデータ、聴覚デバイス動作パラメータ、および／またはファームウェアデータのいずれかを送信することによって、聴覚デバイスの動作を制御することができる。

【００１９】

聴覚デバイス証明書は、複数の聴覚デバイス鍵などの、１つまたは複数の聴覚デバイス鍵を備える。複数の聴覚デバイス鍵は、聴覚デバイス鍵の第１のセットおよび／または第２のセットなどの、聴覚デバイス鍵の１つまたは複数のセットを含み得る。聴覚デバイス鍵のセットは、一次聴覚デバイス鍵を含む１つまたは複数の聴覚デバイス鍵を含む。聴覚デバイス鍵のセットは、二次聴覚デバイス鍵、三次聴覚デバイス鍵、および／または四次聴覚デバイス鍵を含み得る。第１のセットおよび／または第２のセットなどの、聴覚デバイス鍵のセットは、多数の異なる聴覚デバイス鍵を含むか、または多数の異なる聴覚デバイス鍵から成るものとしてよい。聴覚デバイス鍵のセットの中の聴覚デバイス鍵の数は、

３から１０の範囲内など、少なくとも３であり得る。３から６個の聴覚デバイス鍵から成る聴覚デバイス鍵のセットは、メモリサイズが限られており、聴覚デバイス証明書の面倒で時間のかかる更新を必要とすることなく聴覚デバイスの将来の動作を可能にするうえで十分な聴覚デバイス鍵を提供したい場合に、有利であり得る。

【００２０】

複数の聴覚デバイス鍵は、聴覚デバイスが異なる聴覚デバイス鍵を使用して複数のクライアントデバイスと安全に通信することを可能にする。代替的に、またはそれに加えて、聴覚デバイスは、例えば、現在使用されている聴覚デバイス鍵に従って通信するように構成されているクライアントデバイスに障害が生じた場合に、別の聴覚デバイス鍵に切り替える、例えば、一次聴覚デバイス鍵から第２の聴覚デバイス鍵に切り替えることができる。１つまたは複数の例示的な聴覚デバイスにおいて、複数の聴覚デバイス鍵は、第１の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第１のセットを含む。少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の第１のセットのうちの聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子を含む。聴覚デバイス鍵の第１のセットは、第１のクライアントデバイスタイプなどの、第１のクライアントデバイスとの間の通信を保護することのみを目的とする、聴覚デバイス鍵のセット、例えば、３つまたは４つの聴覚デバイス鍵を含み得る。例えば、聴覚デバイス鍵の第１のセットは、第１のクライアントデバイスによる聴覚デバイスデータの通信を保護するための聴覚デバイス鍵のセットであってよい。

【００２１】

聴覚デバイスデータは、例えば、ファームウェア、フィッティングデータ、および／または聴覚デバイス動作パラメータを含む。フィッティングデータは、例えば、聴覚デバイスがユーザの耳にフィッティングされているときにディスペンサーによって使用されるフィッティングデバイスによって生成されるデータであってよい。フィッティングデータは、聴力損失パラメータ、圧縮器パラメータ、フィルタ係数、および／または利得係数を含み得る。聴覚デバイス動作パラメータは、ボリュームコントロールパラメータ、モード、および／またはプログラムコントロールパラメータを含み得る。ファームウェアは、聴覚デバイス製造者によって提供され、聴覚デバイスを制御するために聴覚デバイス上にインストールされるべきコンピュータプログラムを指すものとしてよい。ファームウェアは、例えば、聴覚デバイスの動作および機能をアップグレードするために、および／または古いファームウェアのバグを修正するためにインストールされることになる。

【００２２】

複数の聴覚デバイス鍵は、第２の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第２のセットを含み得る。少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の第２のセットのうちの聴覚デバイス鍵を示す第２の聴覚デバイス鍵識別子を含み得る。聴覚デバイスは、第１のクライアントデバイスおよび／または第２のクライアントデバイスなどの、１つまたは複数のクライアントデバイスと通信するように構成される。聴覚デバイスが通信するように構成されている各クライアントデバイスまたはクライアントデバイスタイプについて、証明書は、クライアントデバイスまたはクライアントデバイスタイプの各々との安全な通信を可能にするように構成された聴覚デバイス鍵のセット、および各聴覚デバイス鍵識別子がどの聴覚デバイス鍵が聴覚デバイス証明書の一部であるかを示す１つまたは複数の聴覚デバイス鍵識別子を備え得る。聴覚デバイスは、聴覚デバイスに接続されているクライアントデバイスまたはクライアントデバイスタイプと、聴覚デバイス鍵の対応するセットに関連付けられている聴覚デバイス鍵識別子とに基づいて聴覚デバイス鍵の選択されたセットから聴覚デバイス鍵を選択するように構成され得る。

【００２３】

聴覚デバイス証明書は、証明書タイプ識別子を備え得る。証明書タイプ識別子は、聴覚デバイスファミリ証明書タイプ、聴覚デバイス証明書タイプ、ファームウェア証明書タイプ、研究開発証明書タイプ、クライアントデバイス証明書タイプなどの、さまざまな証明書タイプのうちの証明書の１つのタイプを示し得る。証明書タイプ識別子は、聴覚デバイスがどのようなタイプの証明書を受信し、記憶し、認証し、および／または取り出すかを

識別するために聴覚デバイスによって使用され得る。聴覚デバイス証明書は、証明書のデータフォーマットバージョンを示すバージョン識別子を含むものとしてよい。聴覚デバイスは、証明書タイプ識別子および／またはバージョン識別子を使用して、証明書がどのようなタイプのデータを含むか、および／またはどのようなタイプのデータが証明書のフィールドに入っているかを決定することができる。例えば、聴覚デバイスは、証明書タイプ識別子および／またはバージョン識別子に基づいて、証明書のどのようなフィールドがデジタル署名を含むか、および／または証明書のデジタル署名を検証するためにどの公開鍵が必要かを決定し得る。証明書タイプ識別子と公開／秘密鍵ペアとの間に一対一マッピングがあることが想定され得る。

【００２４】

聴覚デバイス証明書は、署名デバイス識別子を備え得る。署名デバイス識別子は、製造デバイス、例えば、集積回路カード、スマートカード、ハードウェアセキュリティモジュールなどの、聴覚デバイス証明書に署名したデバイスを識別する一意の識別子を指す。署名デバイス識別子は、例えば、署名デバイスの媒体アクセス制御（ＭＡＣ）アドレス、および／または署名デバイスのシリアル番号を含み得る。署名デバイス識別子は、例えば、聴覚デバイスが、署名デバイスが例えばブラックリストに載っているかどうかを決定すること、したがって、例えば、盗難または他の破損により、ブラックリストに載っている署名デバイスによって署名された証明書を拒絶することを可能にし得る。

【００２５】

聴覚デバイス証明書は、１つまたは複数のハードウェア識別子、例えば、第１のハードウェア識別子および／または第２のハードウェア識別子を備え得る。ハードウェア識別子は、聴覚デバイスに備えられている無線チップおよび／または聴覚デバイスのデジタルシグナルプロセッサなどの、聴覚デバイスに備えられているハードウェアを識別することができる。ハードウェア識別子は、ハードウェアの製造時に聴覚デバイスに備えられているハードウェアのレジスタに記憶され得る。ハードウェア識別子は、ハードウェアのシリアル番号、チップ識別子、またはこれらの任意の組合せを含み得る。メモリユニットからハードウェア識別子を含む聴覚デバイス証明書を受信するか、または取り出す聴覚デバイスは、記憶されているハードウェア識別子と聴覚デバイス証明書に含まれる対応するハードウェア識別子とを比較することによって聴覚デバイス証明書を検証し得る。そのような検証は、聴覚デバイスの起動時または電源投入時など、聴覚デバイス証明書を受信した後、および／またはメモリユニットから聴覚デバイス証明書を取り出した後に実行され得る。

【００２６】

聴覚デバイス証明書は、１つまたは複数のクライアントデバイスタイプ認証識別子を備え得る。クライアントデバイスタイプは、タブレット製品モデル、カテゴリ、またはタイプ、ＵＳＢドングル製品モデル、カテゴリ、またはタイプなどの、クライアントデバイスのモデル、カテゴリ、またはタイプを含み得る。クライアントデバイスタイプ認証識別子は、フィッティングなどのために、聴覚デバイスが通信に認証し得る、または受け入れ得るクライアントデバイスタイプの識別子などの、認証されたクライアントデバイスタイプの識別子である。例えば、クライアントデバイスタイプ認証識別子は、１つまたは複数の聴覚デバイスにおいて、フィッティングのために聴覚デバイスが許容すべきであるクライアントデバイスのタイプを示すビットフィールドである。

【００２７】

聴覚デバイス証明書は、トークンパラメータを備え得る。トークンパラメータは、聴覚デバイスとクライアントデバイスとの間のトークンベースの認証が有効化されているかどうかを示し得る。例えば、トークンパラメータが、０に設定されている場合、クライアントデバイスのトークンベースの認証は、聴覚デバイスによって有効化されることはなく、聴覚デバイスは、例えば、クライアントデバイスタイプ識別子および／またはクライアントデバイス識別子（シリアル番号など）の組合せを使用してクライアントデバイスの認証を実行することになる。例えば、トークンパラメータが、１に設定されている場合、クライアントデバイスのトークンベースの認証は、聴覚デバイスによって有効化されることに

なる、すなわち、聴覚デバイスは、クライアントデバイスから受信されたトークンに基づいてクライアントデバイスを認証する。聴覚デバイスは、例えばユーザの介入なくクライアントデバイスへの接続を受け入れるために使用される受信されたトークンパラメータに基づいてセッション特有のトークンも導出し得る。

【００２８】

聴覚デバイス証明書は、ハードウェアプラットフォーム識別子、ソフトウェアプラットフォーム識別子、および／または証明書タイムスタンプのうちの１つまたは複数を備え得る。ハードウェアプラットフォーム識別子は、動作している聴覚デバイスハードウェアプラットフォーム、すなわち、聴覚デバイス証明書と互換性のあるハードウェアプラットフォームなどの、ハードウェアプラットフォームを識別し得る。ソフトウェアプラットフォーム識別子は、聴覚デバイス証明書が動作するように構成されているソフトウェアプラットフォームのうちの１つまたはファミリを識別し得る。証明書タイムスタンプは、聴覚デバイス証明書が生成されるときに時刻を示す製造デバイスのタイムスタンプなどの、聴覚デバイス証明書の生産または製造のタイムスタンプを指す。証明書タイプスタンプは、例えば、時、分、日、月、年の形態であるものとしてよい。聴覚デバイスは、その後、ハードウェアプラットフォーム識別子、ソフトウェアプラットフォーム識別子、および／または証明書タイムスタンプを使用してバージョン管理および取り消しを実行し得る。

【００２９】

聴覚デバイス証明書は、デジタル署名を備え得る。デジタル署名は、署名者の正当性の検証などの、聴覚デバイス証明書の真正性の立証または検証を可能にする。デジタル署名は、適宜、聴覚デバイスの製造後にデバイスファミリ秘密鍵を使用して製造デバイスによって生成される。聴覚デバイスは、デジタル署名を含む聴覚デバイス証明書を受信したときにデジタル署名を検証するように構成され得る。デジタル署名は、対応するデバイスファミリ公開鍵を使用して聴覚デバイスによって検証可能である。デジタル署名が、申し立てられた公開鍵を使用して検証に成功しなかった場合、聴覚デバイスは、証明書を無視し、および／または通常動作を中断することができる。これは、聴覚デバイスが改竄されたまたは非認証パーティから受信された聴覚デバイス証明書を拒絶するという利点をもたらし得る。したがって、聴覚デバイスとの通信は、偽装攻撃、変更攻撃、およびなりすまし攻撃に対してロバストであり得る。

【００３０】

聴覚デバイス証明書は、メッセージ認証コードを含み得る。メッセージ認証コード（ＭＡＣ）は、例えば聴覚デバイス証明書の内容と鍵とに基づいて製造デバイスによって生成され得る。ＭＡＣを含む聴覚デバイス証明書を受信した後、記憶されている鍵を保持する聴覚デバイスは、受信された聴覚デバイス証明書とＭＡＣ生成関数とに基づいてＭＡＣを再計算し、再計算されたＭＡＣを受信されたＭＡＣと比較することができる。再計算されたＭＡＣが、受信されたＭＡＣと一致しない場合、聴覚デバイスは、聴覚デバイス証明書が破損していると結論する。聴覚デバイスは、聴覚デバイス証明書の完全性が破損している場合に証明書を無視し、および／または通常動作を中断し得る。例えば、聴覚デバイス証明書が、不正なものによって改竄されるか、または修正されている（例えば、挿入、削除、および／または置換によって）と判定された場合、聴覚デバイス証明書を無視することは、受信された聴覚デバイス証明書を拒絶することと、例えば外部デバイスへのアクセスを拒否することとを含み得る。

【００３１】

本開示は、聴覚デバイスを製造する方法に関する。聴覚デバイスは、聴覚デバイスのユーザの聴力損失を補うように適宜構成された処理ユニットと、メモリユニットと、インターフェースとを備える。方法は、聴覚デバイス識別子を生成することを含む。聴覚デバイス識別子を生成することは、乱数または疑似乱数を生成することを含み得る。聴覚デバイス識別子を生成することは、１つまたは複数のハードウェア識別子に基づいてもよい。

【００３２】

方法は、聴覚デバイス識別子に基づいて１つまたは複数の聴覚デバイス鍵を生成するこ

とを含み得る。方法は、聴覚デバイス識別子と生成された聴覚デバイス鍵のうちの少なくとも１つとを含む聴覚デバイス証明書を生成することと、聴覚デバイス証明書を聴覚デバイスに送信することととを含む。方法は、製造デバイスによって実行され得る。製造デバイスは、聴覚デバイスの製造に寄与するように構成されたデバイスを指す。製造デバイスの例として、パーソナルコンピュータ、携帯電話、パーソナルコンピュータもしくは携帯電話上で実行されるアプリケーション、パーソナルコンピュータに関連するハードウェアセキュリティモジュール（ＨＳＭ）、および／またはパーソナルコンピュータにプラグ接続されるＵＳＢドングルが挙げられる。聴覚デバイス証明書を送信することは、聴覚デバイス証明書を聴覚デバイスのメモリユニットに書き込むことなど、聴覚デバイス証明書を聴覚デバイスのメモリユニットに記憶することを含み得る。メモリユニットは、そこに記憶される聴覚デバイス証明書を有するものとしてよい。

【００３３】

１つまたは複数の例示的な方法において、方法は、第１のクライアントデバイス鍵および／または第２のクライアントデバイス鍵を含む１つまたは複数のクライアントデバイス鍵を取得することを含み、１つまたは複数の聴覚デバイス鍵を生成することは、第１のクライアントデバイス鍵および／または第２のクライアントデバイス鍵に基づく。第１のクライアントデバイス鍵は、第１のクライアントデバイスまたはクライアントデバイスタイプとの通信を保護することのみを目的とするＡＥＳ基本鍵などの第１のクライアントデバイス基本鍵であってよい。製造デバイスは、第１のクライアントデバイス鍵を生成／取得することができる。製造デバイスは、例えばハッシュ関数を使用することによって、第１のクライアントデバイス鍵に基づいて１つまたは複数の聴覚デバイス鍵を生成し得る。例えば、第１のクライアントデバイスとの通信のための第１の聴覚デバイス鍵｛ＨＤ＿ＫＥＹ＿１｝は、以下の式

ＨＤ＿ＫＥＹ＿１＝ｈａｓｈ（ＨＤ＿ＩＤ，ＣＤ＿ＫＥＹ＿１）

で生成されるものとしてよい。

ここで、ｈａｓｈはハッシュ関数であり、ＨＤ＿ＩＤは聴覚デバイス識別子であり、ＣＤ＿ＫＥＹ＿１は第１のクライアントデバイス鍵である。これは、第２のクライアントデバイス鍵に基づく第２の聴覚デバイス鍵に、および／または第１の二次クライアントデバイス鍵に基づく第１の二次聴覚デバイス鍵にも適用可能であるものとしてよい。聴覚デバイスは、クライアントデバイスとの通信を保護する（暗号化、認証、検証などを行う）ために、聴覚デバイス鍵のうちの１つを鍵素材として使用して、証明書鍵および／またはセッション鍵などの、１つまたは複数の鍵を導出するように構成され得る。データの暗号化は、例えば暗号化方式を使用して実行され得る。暗号化方式は、対称暗号化方式および／または非対称暗号化方式を含み得る。暗号化方式の例として、Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＡＥＳ）、ＲＳＡ暗号システム、楕円曲線暗号法（ＥＣＣ）、およびＴｒｉｐｌｅ Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ａｌｇｏｒｉｔｈｍが挙げられる。対称鍵の使用は、ハードウェアアクセラレータを使用することができるという利点をもたらし、それにより、軽快な暗号化を実現する。

【００３４】

１つまたは複数の例示的な方法において、１つまたは複数の聴覚デバイス鍵を生成することは、第１の一次聴覚デバイス鍵および／または第１の二次聴覚デバイス鍵を含む聴覚デバイス鍵の第１のセットを生成することを含む。聴覚デバイス鍵のセットは、一次聴覚デバイス鍵、二次聴覚デバイス鍵などの、１つまたは複数の聴覚デバイス鍵を含み得る。単一の鍵で、聴覚デバイス鍵の１つのセットを構成し得る。聴覚デバイス鍵の第１のセットは、例えば、第１のクライアントデバイスまたは第１のクライアントデバイスタイプとの間の通信を保護することのみを目的とする鍵のセットを含む。例えば、聴覚デバイス鍵の第１のセットＨＤ＿ＫＥＹ＿Ａは、聴覚デバイス鍵の第１のセットＨＤ＿ＫＥＹ＿Ａ＝｛ＨＤ＿ＫＥＹ＿１＿１，ＨＤ＿ＫＥＹ＿１＿２，ＨＤ＿ＫＥＹ＿１＿３，ＨＤ＿ＫＥＹ＿１＿４｝として、以下の式

ＨＤ＿ＫＥＹ＿１＿Ｘ ＝ ｈａｓｈ（ＨＤ＿ＩＤ，ＣＤ＿ＫＥＹ＿１＿Ｘ）

で生成されるものとしてよい。
ここで、ｈａｓｈはハッシュ関数であり、Ｘは第１のセットに対して生成されるべきそれぞれの聴覚デバイス鍵を識別するインデックスであり（例えば、第１の一次聴覚デバイス鍵（ＨＤ＿ＫＥＹ＿１＿１）、第１の二次聴覚デバイス鍵（ＨＤ＿ＫＥＹ＿１＿２）、第１の三次聴覚デバイス鍵（ＨＤ＿ＫＥＹ＿１＿３）、第１の四次聴覚デバイス鍵（ＨＤ＿ＫＥＹ＿１＿４）に対してＸ＝｛１，２，３，４｝）、ＨＤ＿ＩＤは聴覚デバイス識別子であり、ＣＤ＿ＫＥＹ＿１＿ＸはＸ番目の第１のクライアントデバイス鍵である。これは、第２のクライアントデバイス鍵に基づく聴覚デバイス鍵の第２のセットにも適用可能である。

【００３５】
方法は、聴覚デバイス鍵の第１のセットの（第１の）聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子を取得することを含み得る。第１の聴覚デバイス鍵識別子を取得することは、第１の聴覚デバイス鍵識別子を、どの聴覚デバイス鍵が聴覚デバイス証明書に含まれるかを示す値に設定することなど、第１の聴覚デバイス鍵識別子を生成することを含み得る。聴覚デバイス証明書を生成することは、聴覚デバイス鍵の第１のセットと第１の聴覚デバイス鍵識別子とを聴覚デバイス証明書に入れることを含み得る。

【００３６】
１つまたは複数の例示的な方法において、１つまたは複数の聴覚デバイス鍵を生成することは、第２の一次聴覚デバイス鍵および／または第２の二次聴覚デバイス鍵を含む聴覚デバイス鍵の第２のセットを生成することを含む。方法は、聴覚デバイス鍵の第２のセットの第２の一次聴覚デバイス鍵などの、（第２の）聴覚デバイス鍵を示す第２の聴覚デバイス鍵識別子を取得することを含み得る。聴覚デバイス証明書を生成することは、聴覚デバイス鍵の第２のセットと第２の聴覚デバイス鍵識別子とを聴覚デバイス証明書に入れることを含み得る。

【００３７】
１つまたは複数の例示的な方法において、聴覚デバイス証明書を生成することは、デジタル署名を生成することと、デジタル署名を証明書中に入れることとを含む。デジタル署名を生成することは、例えば秘密／公開鍵ペアおよび署名生成関数を伴う。署名生成および検証システムの例として、ＲＳＡ暗号システムが挙げられる。ＲＳＡ暗号システムは、２つの大きな素数の積である法（ｍｏｄｕｌｕｓ）Ｎと、ｅｄ≡１（ｍｏｄ　φ（Ｎ））となるような整数ｅおよびｄに基づくものであり、ここで、φはオイラーのφ関数である。ＲＳＡ公開鍵は、法Ｎおよび公開指数としてのｅを含み、対応するＲＳＡ秘密鍵は、法Ｎおよび秘密指数としてのｄを含む。例えば、デジタル署名σを生成してハッシュされたメッセージｍに付加することは、デジタル署名σを例えば$\sigma \equiv m^{d}$（ｍｏｄ　Ｎ）で計算することを含む。

【００３８】
デジタル署名を検証することは、σ^{e}を計算することと、それを受信されたメッセージｍ（ｍｏｄ　Ｎ）と比較することとを含む。デジタル署名σは、有効なものとして検証されるか、または検証は、デジタル署名を底、公開指数をべき指数として累乗したものが受信されたメッセージと同一である、すなわち、$\sigma^{e} \equiv m$（ｍｏｄ　Ｎ）であるときに成功である。

【００３９】
方法は、聴覚デバイスの、第１のハードウェア識別子および／または第２のハードウェア識別子などの、１つまたは複数のハードウェア識別子を取得することを含み得る。聴覚デバイスのハードウェア識別子を取得することは、聴覚デバイスのハードウェア識別子を受信すること、および／またはデータ記憶装置から聴覚デバイスのハードウェア識別子を取り出すことを含み得る。聴覚デバイスまたは製造デバイスは、レジスタなど、メモリユニットからハードウェア識別子を取り出すか、または読み出すことができる。聴覚デバイスは、ハードウェア識別子を製造デバイスに送信し得る。ハードウェア識別子は、シリアル番号、媒体アクセス制御（ＭＡＣ）アドレス、チップ識別子、またはこれらの任意の組

合せを含み得る。聴覚デバイス証明書を生成することは、第１のハードウェア識別子および／または第２のハードウェア識別子を聴覚デバイス証明書に入れることを含み得る。第１のハードウェア識別子は、ハードウェアモジュールのシリアル番号であってよい。製造デバイスは、第１のハードウェア識別子を聴覚デバイス証明書に入れるように構成され得る。第１のハードウェア識別子を含む聴覚デバイス証明書を受信する聴覚デバイスは、記憶されている第１のハードウェア識別子と聴覚デバイス証明書に含まれる第１のハードウェア識別子とを比較することによって聴覚デバイス証明書を検証するように構成され得る。

【００４０】

１つまたは複数の例示的な方法において、聴覚デバイス証明書を生成することは、証明書タイプ識別子、署名デバイス識別子、１つまたは複数のハードウェア識別子、クライアントデバイスタイプ認証識別子、および／またはトークンパラメータのうちの１つまたは複数を聴覚デバイス証明書に入れることを含み得る。聴覚デバイスは、聴覚デバイス証明書の中の証明書タイプ識別子、クライアントデバイスタイプ認証識別子、および／またはトークンパラメータを使用して、聴覚デバイスにアクセスするクライアントデバイスを制御し、認証することができる。聴覚デバイスは、署名デバイス識別子を使用して聴覚デバイス証明書を認証し得る。聴覚デバイスは、ハードウェア識別子を使用して、聴覚デバイス証明書が実際にその聴覚デバイスを対象としていることを検証し得る。

【００４１】

１つまたは複数の例示的な方法において、聴覚デバイス証明書を生成することは、ハードウェアプラットフォーム識別子、ソフトウェアプラットフォーム識別子、および／または証明書タイムスタンプを聴覚デバイス証明書に入れることを含む。聴覚デバイスは、聴覚デバイス証明書の中のハードウェアプラットフォーム識別子、ソフトウェアプラットフォーム識別子、および／または証明書タイムスタンプを使用して、聴覚デバイスのハードウェア、またはファームウェアとの互換性を検証し、取り消しを実行することができる。

【００４２】

図１は、聴覚デバイス２の製造、保守、および／または運用に使用され得る例示的なデバイスを概略的に示している。図１は、例示的なシステム１および聴覚デバイス２を示している。システム１は、聴力損失補償に関連して聴覚デバイス２を製造し、保守し、および／または運用する（聴覚デバイスをフィッティングするため、聴覚デバイスパラメータを更新する、など）ための１つまたは複数の製造デバイス１２、クライアントデバイス１０、およびサーバデバイス１６を備え得る。

【００４３】

製造デバイス１２は、本明細書で開示されている聴覚デバイス２を製造する方法のステップを実行するように構成され得る。製造デバイス１２は、聴覚デバイス識別子を生成し、聴覚デバイス識別子に基づいて１つまたは複数の聴覚デバイス鍵を生成し、聴覚デバイス識別子と生成された聴覚デバイス鍵のうちの少なくとも１つとを含む聴覚デバイス証明書を生成するように構成され得る。製造デバイス１２は、聴覚デバイス証明書を聴覚デバイスに送信するように構成され得る。製造デバイス１２は、本明細書で開示されている聴覚デバイスを製造する方法のステップのうちのどれかを実行するように構成された処理要素（プロセッサおよびメモリなど）を備え得る。

【００４４】

聴覚デバイス２は、聴覚デバイス２のユーザの聴力損失を補うように構成され得る。聴覚デバイス２は、例えば、一方向または双方向通信リンクなどの通信リンク２３を使用して製造デバイス１２と通信するように構成され得る。通信リンク２３は、有線リンクおよび／またはワイヤレス通信リンクであってよい。通信リンク２３は、シングルホップ通信リンクまたはマルチホップ通信リンクであってよい。ワイヤレス通信リンクは、Ｂｌｕｅｔｏｏｔｈ（登録商標）、Ｂｌｕｅｔｏｏｔｈ Ｌｏｗ Ｅｎｅｒｇｙ、ＩＥＥＥ ８０２．１１、Ｚｉｇｂｅｅ（登録商標）などの、短距離通信システムを介して実現され得る。聴覚デバイス２は、製造デバイス１２から聴覚デバイス証明書を受信し、聴覚デバイス

証明書を聴覚デバイス２に含まれるメモリユニットに記憶するように構成され得る。代替的に、またはそれに加えて、製造デバイス１２は、聴覚デバイス証明書を聴覚デバイスのメモリユニットに記憶することができる。例えば、製造デバイス１２は、聴覚デバイス証明書をメモリユニットに書き込むことができる。メモリユニットは、そこに聴覚デバイス証明書を記憶しておくことができる。聴覚デバイス証明書は、聴覚デバイス識別子、聴覚デバイス鍵を示す少なくとも１つの聴覚デバイス鍵識別子、および１つまたは複数の聴覚デバイス鍵を備え得る。例えば、聴覚デバイス２の製造時に、製造デバイス１２は、聴覚デバイス２に接続し、聴覚デバイス証明書を聴覚デバイス２に送信する。聴覚デバイスは、聴覚デバイス証明書を受信し、記録し得る。次いで、聴覚デバイス２は、必要なとき、聴覚デバイス証明書で提供される材料を使用して、クライアントデバイスとの通信を保護し得る。

【００４５】

聴覚デバイス２は、双方向通信リンクなどの通信リンク２１を介してクライアントデバイス１０に接続するように構成され得る。通信リンク２１は、有線リンクおよび／またはワイヤレス通信リンクであってよい。通信リンク２１は、シングルホップ通信リンクまたはマルチホップ通信リンクであってよい。ワイヤレス通信リンクは、Ｂｌｕｅｔｏｏｔｈ、Ｂｌｕｅｔｏｏｔｈ　Ｌｏｗ　Ｅｎｅｒｇｙ、ＩＥＥＥ　８０２．１１、Ｚｉｇｂｅｅなどの、短距離通信システムを介して実現され得る。聴覚デバイス２は、ネットワーク上でクライアントデバイス１０に接続するように構成し得る。クライアントデバイス１０は、ディスペンサーがユーザのクライアントデバイス１０を介して聴覚デバイスに接続する補聴デバイスのリモートフィッティングを可能にし得る。クライアントデバイス１０は、フィッティングデバイス１４などのクライアント（例えば、ハンドヘルドデバイス、リレー、タブレット、パーソナルコンピュータ、携帯電話、および／またはパーソナルコンピュータにプラグ接続されるＵＳＢドングル）として動作するコンピューティングデバイスを含み得る。クライアントデバイス１０は、双方向通信リンクなどの通信リンク２４を介してサーバデバイス１６と通信するように構成され得る。通信リンク２４は、有線リンクおよび／またはワイヤレス通信リンクであってよい。通信リンク２４は、インターネットなどのネットワークを含み得る。クライアントデバイス１０は、保守および更新を目的としてサーバデバイス１６と通信するように構成され得る。サーバデバイス１６は、サーバとして動作する、すなわち、クライアントデバイス１０および／または聴覚デバイス２からの要求を処理するように構成されたコンピューティングデバイスを含み得る。サーバデバイス１６は、聴覚デバイス製造者によって制御され得る。サーバデバイス１６は、製造保守および／または運用目的のために通信リンク２２を介して製造デバイス１２と通信するように構成され得る。サーバデバイス１６および製造デバイス１２は、同一の場所に置かれる、および／または聴覚デバイス２の製造保守、および／または運用目的のために１つのエンティティを形成し得る。

【００４６】

図２は、例示的な聴覚デバイス２を概略的に示す。聴覚デバイス２は、処理ユニット４と、メモリユニット６と、インターフェース８とを備える。聴覚デバイス２は、聴覚デバイス２のユーザの聴力損失を補うように構成された処理ユニット４を備える。インターフェース８は、例えば、２．４から２．５ＧＨｚの範囲内の周波数でワイヤレス通信するように構成された、ワイヤレストランシーバを備える。インターフェース８は、製造デバイス１２と、有線および／またはワイヤレス通信などの通信を行うように構成される。処理ユニット４は、製造中に受信されたデータに従って補聴器のユーザの聴力損失を補うように構成され得る。聴覚デバイス２は、音声信号を受信し、音声信号を変換済み音声信号に変換するためにマイクロフォン５または複数のマイクロフォンを備える。変換済み音声信号は、音声信号の電気的および／またはデジタルバージョンであってよい。処理ユニット４は、変換済み音声信号を受信し、聴覚デバイス２のユーザの聴力損失に応じて変換済み音声信号を処理済み音声信号に処理するように構成される。処理済み音声信号は、圧縮され、および／または増幅されるか、または同様の処理がなされ得る。聴覚デバイス２は、

レシーバと称される、出力トランスデューサ／ラウドスピーカ７を備える。レシーバ７は、処理済み音声信号を受信し、それをユーザの鼓膜で受信できるように出力音声信号に変換するように構成される。

【００４７】

聴覚デバイス２は、例えばインターフェース８を介して、聴覚デバイス証明書１００を受信するように構成され得る。聴覚デバイス２は、聴覚デバイス証明書を、例えばメモリユニット６に記憶するように構成され得る。聴覚デバイス２は、製造デバイス１２へのアクセスを認めることもでき、製造デバイス１２は次いで聴覚デバイス証明書をメモリユニット６に記憶するか、または書き込む。メモリユニット６は、限定はしないが、読出し専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、などを含む、取り外し可能および取り外し不可能データ記憶ユニットを含み得る。メモリユニット６は、そこに記憶される聴覚デバイス証明書を有するものとしてよい。聴覚デバイス証明書は、聴覚デバイス識別子、聴覚デバイス鍵を示す少なくとも１つの聴覚デバイス鍵識別子、および複数の聴覚デバイス鍵を備え得る。メモリユニット６は、メモリユニット６のメモリアドレスに記憶されている聴覚デバイス証明書１００を有するものとしてよい。メモリユニット６は、例えば、聴覚デバイス識別子、少なくとも１つの聴覚デバイス鍵識別子、複数の聴覚デバイス鍵、および／または聴覚デバイス証明書に含まれる任意のデータをメモリユニット６の明確に区別できるそれぞれのメモリアドレスに記憶しているものとしてよい。聴覚デバイス２は、聴覚デバイス識別子、少なくとも１つの聴覚デバイス鍵識別子、複数の聴覚デバイス鍵、および／または聴覚デバイス証明書に含まれる任意のデータをメモリユニット６の明確に区別できるそれぞれのメモリアドレスから取り出し得る。聴覚デバイス２は、聴覚デバイス証明書またはその少なくとも一部を使用して、クライアントデバイス、サーバデバイス、別の聴覚デバイスなどの、外部エンティティとの通信を保護することができる。

【００４８】

図３は、例示的な聴覚デバイス証明書１００を概略的に示す。聴覚デバイス証明書１００は、聴覚デバイス識別子１１２、聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子１１４を含む少なくとも１つの聴覚デバイス鍵識別子、および１つまたは複数の聴覚デバイス鍵を備える。聴覚デバイス識別子１１２は、一意のまたは疑似一意の識別子を指すものとしてよい。第１の聴覚デバイス鍵識別子１１４は、聴覚デバイス証明書の第１の聴覚デバイス鍵を示す。例えば、第１の聴覚デバイス鍵識別子１１４は、聴覚デバイス証明書の聴覚デバイス鍵の第１のセット１１５（１１５Ａ、１１５Ｂ、１１５Ｃ、１１５Ｄ）のうちの１つの聴覚デバイス鍵、例えば、第１の一次聴覚デバイス鍵１１５Ａを示すか、または指しているものとしてよい。

【００４９】

聴覚デバイス証明書１００は、適宜、対応する数の異なるクライアントデバイス／クライアントデバイスタイプとの安全な通信を可能にする聴覚デバイス鍵の２つ、３つ、または少なくとも４つのセットを備える。

【００５０】

聴覚デバイス証明書１００は、第１の一次聴覚デバイス鍵１１５Ａを含む聴覚デバイス鍵の第１のセット１１５を備える。少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵１１５Ａ、１１５Ｂ、１１５Ｃ、１１５Ｄの第１のセット１１５のうちの聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子１１４を含む。聴覚デバイス鍵の第１のセット１１５は、例えば、第１のクライアントデバイスまたは第１のクライアントデバイスタイプへの、および第１のクライアントデバイスまたは第１のクライアントデバイスタイプからの通信を保護することのみを目的とする第１の一次鍵１１５Ａ、第１の二次鍵１１５Ｂ、第１の三次鍵１１５Ｃ、および第１の四次鍵１１５Ｄを含む。例えば、聴覚デバイス鍵の第１のセット１１５は、第１のクライアントデバイスによる聴覚デバイスデータの通信を保護するための聴覚デバイス鍵１１５Ａ、１１５Ｂ、１１５Ｃ、１１５Ｄのセットであってよい。

【００５１】
複数の聴覚デバイス鍵は、第２の一次聴覚デバイス鍵１１７Ａ、第２の二次聴覚デバイス鍵１１７Ｂ、第２の三次聴覚デバイス鍵１１７Ｃ、および／または第２の四次聴覚デバイス鍵１１７Ｄを含む聴覚デバイス鍵の第２のセット１１７を含み得る。少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵１１７Ａ、１１７Ｂ、１１７Ｃ、１１７Ｄの第２のセット１１７のうちの聴覚デバイス鍵を示す第２の聴覚デバイス鍵識別子１１６を含む。聴覚デバイスは、第１のクライアントデバイスおよび／または第２のクライアントデバイスなどの、１つまたは複数のクライアントデバイスと通信するように構成される。聴覚デバイスが通信するように構成されている各クライアントデバイスまたはクライアントデバイスタイプについて、聴覚デバイス証明書は、特定のクライアントデバイスまたはクライアントデバイスタイプとの安全な通信を可能にするように構成された聴覚デバイス鍵のセット、およびどの聴覚デバイス鍵が聴覚デバイス証明書の一部であるかを示す聴覚デバイス鍵識別子を備える。聴覚デバイス証明書は、第３の一次聴覚デバイス鍵１１９Ａ、第３の二次聴覚デバイス鍵１１９Ｂ、第３の三次聴覚デバイス鍵１１９Ｃ、および／または第３の四次聴覚デバイス鍵１１９Ｄを含む聴覚デバイス鍵の第３のセット１１９を含み得る。少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の第３のセット１１９のうちの聴覚デバイス鍵を示す第３の聴覚デバイス鍵識別子１１８を含む。聴覚デバイス証明書１００は、第４の一次聴覚デバイス鍵（図示せず）を含む聴覚デバイス鍵の第４のセットを備え得る。少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の第４のセットのうちの聴覚デバイス鍵を示す第４の聴覚デバイス鍵識別子を含む。聴覚デバイス２は、聴覚デバイスに接続されているクライアントデバイスまたはクライアントデバイスタイプに基づいて聴覚デバイス鍵のセットを選択し、聴覚デバイスの選択されたセットに関連付けられている聴覚デバイス鍵識別子に基づいて聴覚デバイス鍵のセットから聴覚デバイス鍵を１つ選択するように構成され得る。

【００５２】
聴覚デバイス証明書１００は、証明書タイプ識別子１３０を備える。証明書タイプ識別子１３０は、例えば、聴覚デバイスファミリ証明書タイプ、聴覚デバイス証明書タイプ、ファームウェア証明書タイプ、研究開発証明書タイプ、およびクライアントデバイス証明書タイプなどの、さまざまな証明書タイプのうちから選択された聴覚デバイス証明書であることを示す。証明書タイプ識別子１３０は、どのようなタイプの証明書を受信し、記憶し、認証し、および／または取り出すかを聴覚デバイス２が識別できるようにするために使用され得る。聴覚デバイス証明書１００は、聴覚デバイス証明書のデータフォーマットバージョンを示すバージョン識別子を含むものとしてよい。聴覚デバイス２は、証明書タイプ識別子１３０および／またはバージョン識別子を使用して、聴覚デバイス証明書１００がどのようなタイプのデータを含むか、どのようなタイプのデータが聴覚デバイス証明書１００のフィールドに入っているかを決定することができる。例えば、聴覚デバイス２は、証明書タイプ識別子１３０および／またはバージョン識別子に基づいて、証明書のどのようなフィールドがデジタル署名１１３を含むか、およびデジタル署名１１３を検証するためにどの公開鍵が必要かを決定し得る。証明書タイプ識別子１３０と公開／秘密鍵ペアとの間に、デジタル署名１１３を生成するために使用される一対一マッピングがあることが想定され得る。聴覚デバイス証明書１００は、聴覚デバイス証明書１００の長さを、例えば、ビット、バイト単位で示す長さ識別子を含むものとしてよい。

【００５３】
聴覚デバイス証明書１００は、適宜、署名デバイス識別子１３６を備える。署名デバイス識別子１３６は、聴覚デバイス証明書１００に署名したデバイス（製造デバイス１２、例えば、製造デバイス１２に含まれる集積回路カード、スマートカード、ハードウェアセキュリティモジュールなど）を識別する一意の識別子を指す。署名デバイス識別子１３６は、例えば、媒体アクセス制御（ＭＡＣ）、署名デバイスのアドレス、シリアル番号を含み得る。署名デバイス識別子１３６は、例えば、聴覚デバイス２が、署名デバイスが例えばブラックリストに載っているかどうかを決定すること、したがってブラックリストに載

っている署名デバイスによって署名された聴覚デバイス証明書１００を拒絶することを可能にする。

【００５４】

聴覚デバイス証明書１００は、適宜、第１のハードウェア識別子１４８および／または第２のハードウェア識別子（図示せず）を含む１つまたは複数のハードウェア識別子を備える。ハードウェア識別子１４８は、処理ユニット４、聴覚デバイス２に備えられている無線チップ、聴覚デバイス２のデジタルシグナルプロセッサなどの、聴覚デバイス２に備えられているハードウェアを識別することができる。第１のハードウェア識別子１４８は、ハードウェアの製造時に聴覚デバイス２に備えられているハードウェアのレジスタに記憶され得る。第１のハードウェア識別子１４８は、シリアル番号、媒体アクセス制御（ＭＡＣ）アドレス、チップ識別子、またはこれらの任意の組合せを含み得る。聴覚デバイス証明書１００は、第１のハードウェア識別子１４８、第２のハードウェア識別子、および／または第３のハードウェア識別子を含み得る。例えば、第１のハードウェア識別子１４８は、聴覚デバイス２のハードウェアモジュール（例えば、処理ユニットまたは無線チップ）のレジスタ内に存在する第１の聴覚デバイスに特有の値を与えることができ、第２のハードウェア識別子は、聴覚デバイス２のハードウェアモジュールのレジスタ内に存在する第２の聴覚デバイスに特有の値を与えることができ、第３のハードウェア識別子は、第３のハードウェアモジュール識別子（例えば、処理ユニット識別子、ＤＳＰ識別子）を与えることができる。聴覚デバイス２は、第１のハードウェア識別子１４８を含む聴覚デバイス証明書１００を受信した後に、次いで、記憶されているハードウェア識別子と受信された聴覚デバイス証明書１００に含まれる第１のハードウェア識別子１４８とを比較することによって聴覚デバイス証明書１００を検証し得る。このようにして、聴覚デバイス２は、受信された聴覚デバイス証明書が聴覚デバイス２を意図したものであるかどうかを判定し、記憶され、受信されたハードウェア識別子が一致しない場合に受信された聴覚デバイス証明書を拒絶し得る。

【００５５】

聴覚デバイス証明書１００は、適宜、クライアントデバイスタイプ認証識別子１４４を備える。クライアントデバイスタイプは、タブレット製品モデル、カテゴリ、またはタイプ、ＵＳＢドングル製品モデル、カテゴリ、またはタイプなどの、クライアントデバイスのモデル、カテゴリ、またはタイプを含み得る。クライアントデバイスタイプ認証識別子１４４は、フィッティング、保守、および／または運用などのために、聴覚デバイス２が通信に認証し得るクライアントデバイスタイプの識別子などの、認証されたクライアントデバイスタイプの識別子である。クライアントデバイスタイプ認証識別子１４４は、例えば、フィッティングのために聴覚デバイス２が許容すべきであるクライアントデバイスのタイプを示すビットフィールドである。

【００５６】

聴覚デバイス証明書１００は、適宜、トークンパラメータ１４６を備える。トークンパラメータ１４６は、トークンベースの認証が有効化されているかどうかを示す。例えば、トークンパラメータ１４６が、０に設定されている場合、クライアントデバイスのトークンベースの認証は、聴覚デバイス２によって有効化されることはなく、聴覚デバイス２は、例えば、クライアントデバイスタイプ識別子および／またはクライアントデバイス識別子（シリアル番号など）の組合せを使用してクライアントデバイス１０の認証を実行することになる。例えば、トークンパラメータ１４６が、１に設定されている場合、クライアントデバイスのトークンベースの認証は、聴覚デバイス２によって有効化されることになる、すなわち、聴覚デバイス２は、クライアントデバイス１０を認証する（クライアントデバイス１０から受信されたトークンに基づくなどして）。聴覚デバイス２は、例えばユーザの介入なくクライアントデバイス１０への接続を受け入れるために使用される受信されたトークンパラメータ１４６に基づいてセッション特有のトークンも導出し得る。

【００５７】

聴覚デバイス証明書１００は、ハードウェアプラットフォーム識別子１３８、ソフトウ

ェアプラットフォーム識別子１４０、および／または証明書タイムスタンプ１４２のうちの１つまたは複数を備える。ハードウェアプラットフォーム識別子１３８は、動作している聴覚デバイスハードウェアプラットフォーム、すなわち、聴覚デバイス証明書が使用され得るハードウェアプラットフォームなどの、ハードウェアプラットフォームを識別し得る。ソフトウェアプラットフォーム識別子１４０は、聴覚デバイス証明書が動作するように構成されているソフトウェアプラットフォームのファミリを識別し得る。証明書タイムスタンプ１４２は、聴覚デバイス証明書１００が生成されるときに時刻を示す製造デバイス１２のタイムスタンプなどの、聴覚デバイス証明書１００の生産または製造のタイムスタンプを指す。証明書タイプスタンプ１４２は、例えば、時、分、日、月、年の形態であるものとしてよい。

【００５８】

聴覚デバイス証明書は、デジタル署名１１３および／またはＭＡＣを備える。デジタル署名１１３は、署名者の正当性（例えば、署名者が正当な製造デバイスであるかどうか）の検証などの、聴覚デバイス証明書１００の真正性の立証または検証を可能にする。デジタル署名１１３は、聴覚デバイスの製造時にデバイスファミリ秘密鍵を使用して製造デバイス１２によって生成される。次いで、聴覚デバイス２または処理ユニット４は、デジタル署名１１３を含む聴覚デバイス証明書１００を受信したとき、デジタル署名１１３を検証することができる。デジタル署名１１３は、対応するデバイスファミリ公開鍵を使用して聴覚デバイス２によって検証可能である。デジタル署名１１３が、申し立てられた公開鍵を使用して検証に成功しなかった場合、聴覚デバイスは、聴覚デバイス証明書１００を破棄し、および／または通常動作を中断することができる。

【００５９】

図４は、聴覚デバイス２と製造デバイス１２との間の例示的な信号図を概略的に示している。聴覚デバイス１０１は、場合によっては製造デバイス１２から識別子要求を受信した後に、聴覚デバイス証明書要求またはメッセージ４０１を製造デバイス１２に送信し得る。聴覚デバイス証明書要求４０１は、第１のハードウェア識別子１４８を備え得る。次いで、製造デバイス１２は、例えば乱数または疑似乱数に基づいて、聴覚デバイス２を識別して聴覚デバイス識別子１１２を生成することができる。次いで、製造デバイス１２は、聴覚デバイス識別子１１２に基づいて、１つまたは複数の聴覚デバイス鍵を生成し得る。製造デバイス１２は、聴覚デバイス識別子１１２と生成された聴覚デバイス鍵のうちの少なくとも１つとを含む聴覚デバイス証明書１００を生成するように構成される。製造デバイス１２は、聴覚デバイス鍵を示す少なくとも１つの鍵識別子を決定するものとしてよく、聴覚デバイス証明書中で示す少なくとも１つの鍵識別子を含み得る。次いで、製造デバイス１２は、デジタル署名なしで聴覚デバイス証明書１００のハッシュ値を生成し、デジタル署名なしでハッシュされた聴覚デバイス証明書に基づいてデジタル署名を生成し得る。次いで、製造デバイス１２は、デジタル署名を聴覚デバイス証明書１００に入れることができる。製造デバイス１２は、聴覚デバイス証明書１００を含む聴覚デバイス証明書応答４０２を聴覚デバイス２に送信し得る。製造デバイス１２は、聴覚デバイス証明書１００を、直接、メモリユニット６に書き込むようにも構成され得る。聴覚デバイス証明書を受信する聴覚デバイス２は、デジタル署名１１３、証明書タイプ識別子１３０、バージョン識別子、ハードウェアプラットフォーム識別子１３８、ソフトウェアプラットフォーム識別子１４０、署名デバイス識別子１３６、および／またはハードウェア識別子１４８を検証することによって受信された聴覚デバイス証明書１００を検証するように構成され得る。聴覚デバイス２は、例えば検証が成功した場合に、受信された聴覚デバイス証明書１００をメモリユニット６に記憶するように構成され得る。聴覚デバイス２は、メモリユニットから聴覚デバイス証明書を取り出し、デジタル署名１１３、証明書タイプ識別子１３０、バージョン識別子、ハードウェアプラットフォーム識別子１３８、ソフトウェアプラットフォーム識別子１４０、署名デバイス識別子１３６、および／またはハードウェア識別子１４８を検証することによって聴覚デバイス証明書を検証するように構成され得る。検証のどれかが失敗した場合、聴覚デバイス２は、メモリユニットから聴覚デバイス証

明書を削除するか、または聴覚デバイス証明書を無視し得る。

【００６０】

図５は、聴覚デバイス２を製造する例示的な方法５００のフローチャートを概略的に示す。方法５００は、製造デバイスにおいて実行され得る。聴覚デバイス２は、聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニット４と、メモリユニット６と、インターフェース８とを備える。方法５００は、聴覚デバイス識別子１１２を生成すること（Ｓ１）を含む。聴覚デバイス識別子を生成することは、例えば処理ユニットおよび／またはインターフェースの１つまたは複数のハードウェア識別子を取得すること含み得る。聴覚デバイス識別子を生成すること（Ｓ１）は、聴覚デバイスハードウェア構成要素のハードウェア識別子に基づいてもよい。聴覚デバイス識別子を生成すること（Ｓ１）は、乱数または疑似乱数を生成することを含み得る。方法５００は、聴覚デバイス識別子１１２に基づいて１つまたは複数の聴覚デバイス鍵を生成すること（Ｓ２）を含み得る。方法は、聴覚デバイス識別子１１２と生成された聴覚デバイス鍵のうちの少なくとも１つとを含む聴覚デバイス証明書１００を生成すること（Ｓ３）と、聴覚デバイス証明書１００を聴覚デバイス２に送信すること（Ｓ４）とを含む。次いで、聴覚デバイス２は、聴覚デバイス証明書１００をメモリユニット６に記憶し得る。

【００６１】

方法５００は、第１のクライアントデバイス鍵を含む１つまたは複数のクライアントデバイス鍵を取得すること（Ｓ１１）を含み、１つまたは複数の聴覚デバイス鍵を生成すること（Ｓ２）は、第１のクライアントデバイス鍵に基づく。第１のクライアントデバイス鍵は、第１のクライアントデバイスまたはデバイスタイプとの通信を保護することのみを目的とするＡＥＳの基本鍵などの第１のクライアントデバイスの基本鍵であってよい。製造デバイス１２は、第１のクライアントデバイス鍵を生成し、適宜、第１のクライアントデバイス鍵をデータ記憶装置に記憶し得る。製造デバイス１２は、第１のクライアントデバイス鍵に基づいて１つまたは複数の聴覚デバイス鍵を生成し得る。例えば、第１のクライアントデバイスとの通信のための第１の聴覚デバイス鍵｛ＨＤ＿ＫＥＹ＿１｝は、以下の式

ＨＤ＿ＫＥＹ＿１＝ｈａｓｈ（ＨＤ＿ＩＤ，ＣＤ＿ＫＥＹ＿１）

で生成されるものとしてよい。

ここで、ｈａｓｈはハッシュ関数であり、ＨＤ＿ＩＤは聴覚デバイス識別子１１２であり、ＣＤ＿ＫＥＹ＿１は第１のクライアントデバイス鍵である。これは、第２のクライアントデバイス鍵に基づく聴覚デバイス鍵の第２のセットに、および／または第１の二次クライアントデバイス鍵に基づく第１の二次聴覚デバイス鍵にも適用可能であるものとしてよい。

【００６２】

１つまたは複数の例示的な方法において、１つまたは複数の聴覚デバイス鍵を生成すること（Ｓ２）は、第１の一次聴覚デバイス鍵１１５Ａを含む聴覚デバイス鍵の第１のセット１１５を生成することを含む。聴覚デバイス鍵のセットは、一次聴覚デバイス鍵１１５Ａ、二次聴覚デバイス鍵１１５Ｂなどの、１つまたは複数の聴覚デバイス鍵を含み得る。単一の鍵で、聴覚デバイス鍵の１つのセットを構成し得る。聴覚デバイス鍵の第１のセット１１５は、例えば、第１のクライアントデバイスタイプなどの、第１のクライアントデバイスとの間の安全な通信を可能にすることのみを目的とする第１の聴覚デバイス鍵のセットを含む。例えば、聴覚デバイス鍵の第１のセット１１５　ＨＤ＿ＫＥＹ＿Ａ＝｛ＨＤ＿ＫＥＹ＿１＿１，ＨＤ＿ＫＥＹ＿１＿２，ＨＤ＿ＫＥＹ＿１＿３，ＨＤ＿ＫＥＹ＿１＿４｝は、以下の式

Ｈ＿ＫＥＹ＿Ｘ＝ｈａｓｈ（ＨＤ＿ＩＤ，ＣＤ＿ＫＥＹ＿Ｘ）

で生成される。

ここで、ｈａｓｈはハッシュ関数であり、Ｘは第１のセットに対して生成されるべきそれぞれの聴覚デバイス鍵を識別するインデックスであり（例えば、第１の一次聴覚デバイス鍵１１５Ａ、第１の二次聴覚デバイス鍵１１５Ｂ、第１の三次聴覚デバイス鍵１１５Ｃ

、第１の四次聴覚デバイス鍵１１５Ｄに対してＸ＝｛１，２，３，４｝）、ＨＤ＿ＩＤは聴覚デバイス識別子１１２であり、ＣＤ＿ＫＥＹ＿ＸはＸ番目の第１のクライアントデバイス鍵である。これは、第２のクライアントデバイス鍵に基づく聴覚デバイス鍵の第２のセット１１７に、および／または第３のクライアントデバイス鍵に基づく聴覚デバイス鍵の第３のセット１１９にも適用可能である。

【００６３】

方法５００は、聴覚デバイス鍵の第１のセット１１５の聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子１１４を取得すること（Ｓ２１）を含み得る。第１の聴覚デバイス鍵識別子を取得すること（Ｓ２１）は、第１の聴覚デバイス鍵識別子１１４を、どの聴覚デバイス鍵が聴覚デバイス証明書（聴覚デバイス鍵の第１のセット１１５）に含まれるかを示す値に設定することなど、第１の聴覚デバイス鍵識別子１１４を生成することを含み得る。聴覚デバイス証明書を生成すること（Ｓ３）は、聴覚デバイス鍵の第１のセット１１５と第１の聴覚デバイス鍵識別子１１４とを聴覚デバイス証明書１００に入れることを含む。

【００６４】

１つまたは複数の例示的な方法において、１つまたは複数の聴覚デバイス鍵を生成すること（Ｓ２）は、第２の一次聴覚デバイス鍵１１７Ａを含む聴覚デバイス鍵の第２のセット１１７を生成することを含む。方法５００は、聴覚デバイス鍵の第２のセット１１７の聴覚デバイス鍵を示す第２の聴覚デバイス鍵識別子１１６を取得すること（Ｓ２２）を含み得る。聴覚デバイス証明書を生成すること（Ｓ３）は、聴覚デバイス鍵の第２のセット１１７と第２の聴覚デバイス鍵識別子１１６とを聴覚デバイス証明書１００に入れることを含み得る。１つまたは複数の例示的な方法において、１つまたは複数の聴覚デバイス鍵を生成すること（Ｓ２）は、第３の一次聴覚デバイス鍵１１９Ａを含む聴覚デバイス鍵の第３のセット１１９を生成することを含む。方法５００は、聴覚デバイス鍵の第３のセット１１９の聴覚デバイス鍵を示す第３の聴覚デバイス鍵識別子１１８を取得することを含み得る。聴覚デバイス証明書を生成すること（Ｓ３）は、聴覚デバイス鍵の第３のセット１１９と第３の聴覚デバイス鍵識別子１１８とを聴覚デバイス証明書１００に入れることを含み得る。

【００６５】

１つまたは複数の例示的な方法において、聴覚デバイス証明書を生成すること（Ｓ３）は、デジタル署名１１３を生成することと、デジタル署名１１３を聴覚デバイス証明書１００中に入れることとを含む。デジタル署名１１３を生成することは、例えば秘密／公開鍵ペアおよび署名生成関数を伴う。署名生成および検証システムの例として、ＲＳＡ暗号システム（上で説明されている）が挙げられる。

【００６６】

方法５００は、聴覚デバイス２の第１のハードウェア識別子１４８を取得すること（Ｓ２３）を含み得る。聴覚デバイス２の第１のハードウェア識別子１４８を取得すること（Ｓ２３）は、聴覚デバイス２の第１のハードウェア識別子１４８を受信すること、および／またはデータ記憶装置から聴覚デバイス２の第１のハードウェア識別子１４８を取り出すことを含み得る。聴覚デバイス２は、レジスタなど、メモリユニットからハードウェア識別子１４８を取り出すか、または読み出すことができ、ハードウェア識別子１４８を製造デバイス１２に送信することができる。第１のハードウェア識別子１４８は、シリアル番号、媒体アクセス制御（ＭＡＣ）アドレス、チップ識別子、またはこれらの任意の組合せを含み得る。聴覚デバイス証明書１００を生成すること（Ｓ３）は、第１のハードウェア識別子１４８を聴覚デバイス証明書１００に入れることを含み得る。第１のハードウェア識別子１４８を含む聴覚デバイス証明書１００を受信する聴覚デバイス２は、次いで、記憶されている第１のハードウェア識別子と受信された聴覚デバイス証明書１００に含まれる第１のハードウェア識別子１４８とを比較することによって聴覚デバイス証明書１００を検証し得る。

【００６７】

１つまたは複数の例示的な方法において、聴覚デバイス証明書を生成すること（Ｓ３）は、証明書タイプ識別子１３０、署名デバイス識別子１３６、第１のハードウェア識別子１４８を含む１つまたは複数のハードウェア識別子、クライアントデバイスタイプ認証識別子１４４、および／またはトークンパラメータ１４６のうちの１つまたは複数を聴覚デバイス証明書１００に入れることを含み得る。聴覚デバイス２は、聴覚デバイス証明書の中の証明書タイプ識別子１３０、クライアントデバイスタイプ認証識別子１４４、および／またはトークンパラメータ１４６を使用して、聴覚デバイスにアクセスするクライアントデバイスを制御し、認証する。聴覚デバイス２は、署名デバイス識別子１３６を使用して聴覚デバイス証明書１００を認証し得る。聴覚デバイス２は、第１のハードウェア識別子１４８を含む、１つまたは複数のハードウェア識別子を使用して、聴覚デバイス証明書１００が実際にその聴覚デバイス２を対象としていることを検証し得る。

【００６８】

１つまたは複数の例示的な方法において、聴覚デバイス証明書を生成すること（Ｓ３）は、ハードウェアプラットフォーム識別子１３８、ソフトウェアプラットフォーム識別子１４０、および／または証明書タイムスタンプ１４２を聴覚デバイス証明書１００に入れることを含む。聴覚デバイス２は、適宜、聴覚デバイス証明書１００の中のハードウェアプラットフォーム識別子１３８、ソフトウェアプラットフォーム識別子１４０、および／または証明書タイムスタンプ１４２を使用して、聴覚デバイス２のハードウェア、またはファームウェアとの互換性を検証し、適宜取り消しを実行することができる。

【００６９】

「第１の」、「第２の」、「一次」、「二次」、「三次」、「四次」、および同様の言い回しの使用は、特定の順序を意味しないが、それらは、個別の要素を識別するために含まれている。さらに、第１の、第２の、などの言い回しの使用は、順序、または重要度を表さず、むしろ、第１の、第２の、などは、要素を互いに区別するために使用される。第１および第２という単語は、ここで、および別のところで、ラベルを付けることのみを目的として使用されており、特定の空間的または時間的順序付けを表すことを意図されていないことに留意されたい。さらに、第１の要素のラベル付けは、第２の要素の存在を意味しない。

【００７０】

特定の特徴について図示して説明したが、それらは特許請求の範囲に記載された発明を限定することを意図するものではないことが理解され、また特許請求の範囲に記載された発明の趣旨および範囲から逸脱することなく、様々な変更および修正を行うことができることが、当業者には明らかであろう。本明細書および図面は、したがって、限定的な意味ではなく、説明的なものと見なされるべきものである。特許請求の範囲に記載された発明は、すべての代替形態、修正形態および均等形態を含めることを意図している。

以下の項目は、本出願時の特許請求の範囲に記載の要素である。

［項目１］

聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットと、

メモリユニットと、

インターフェースとを備え、

前記メモリユニットは、そこに記憶される聴覚デバイス証明書を有し、前記聴覚デバイス証明書は

聴覚デバイス識別子と、

聴覚デバイス鍵を示す少なくとも１つの聴覚デバイス鍵識別子と、

複数の聴覚デバイス鍵とを備える聴覚デバイス。

［項目２］

前記複数の聴覚デバイス鍵は、第１の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第１のセットを含み、前記少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の前記第１のセットのうちの聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子を含む項目１に記載の聴覚デバイス。

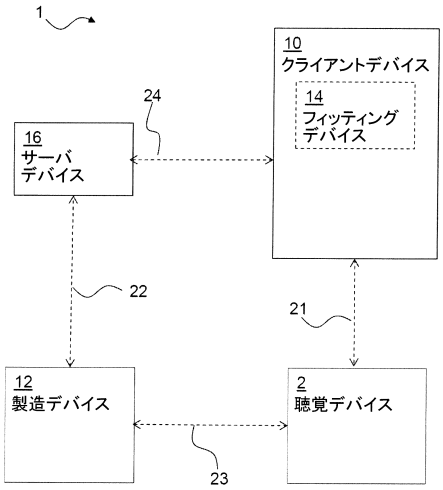
［項目３］
前記複数の聴覚デバイス鍵は、第２の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第２のセットを含み、前記少なくとも１つの聴覚デバイス鍵識別子は、聴覚デバイス鍵の前記第２のセットのうちの聴覚デバイス鍵を示す第２の聴覚デバイス鍵識別子を含む項目１または２に記載の聴覚デバイス。
［項目４］
前記聴覚デバイス証明書は、証明書タイプ識別子、署名デバイス識別子、１つまたは複数のハードウェア識別子、クライアントデバイスタイプ認証識別子、および／またはトークンパラメータのうちの１つまたは複数を備える項目１から３のいずれか一項に記載の聴覚デバイス。
［項目５］
前記聴覚デバイス証明書は、ハードウェアプラットフォーム識別子、ソフトウェアプラットフォーム識別子、および／または証明書タイムスタンプを備える項目１から４のいずれか一項に記載の聴覚デバイス。
［項目６］
前記聴覚デバイス証明書は、デジタル署名および／またはメッセージ認証コードを備える項目１から５のいずれか一項に記載の聴覚デバイス。
［項目７］
聴覚デバイスのユーザの聴力損失を補うように構成された処理ユニットと、メモリユニットと、インターフェースとを備える前記聴覚デバイスを製造する方法であって、
聴覚デバイス識別子を生成するステップと、
前記聴覚デバイス識別子に基づいて１つまたは複数の聴覚デバイス鍵を生成するステップと、
前記聴覚デバイス識別子と前記生成された聴覚デバイス鍵のうちの少なくとも１つとを含む聴覚デバイス証明書を生成するステップと、
前記聴覚デバイス証明書を前記聴覚デバイスに送信するステップとを含む方法。
［項目８］
第１のクライアントデバイス鍵を含む１つまたは複数のクライアントデバイス鍵を取得するステップを含み、１つまたは複数の聴覚デバイス鍵を生成するステップは、前記第１のクライアントデバイス鍵に基づく項目７に記載の方法。
［項目９］
１つまたは複数の聴覚デバイス鍵を生成するステップは、第１の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第１のセットを生成するステップを含み、前記方法は聴覚デバイス鍵の前記第１のセットの聴覚デバイス鍵を示す第１の聴覚デバイス鍵識別子を取得するステップを含み、前記聴覚デバイス証明書を生成するステップは、聴覚デバイス鍵の前記第１のセットと前記第１の聴覚デバイス鍵識別子とを前記聴覚デバイス証明書に入れるステップを含む項目７から８のいずれか一項に記載の方法。
［項目１０］
１つまたは複数の聴覚デバイス鍵を生成するステップは、第２の一次聴覚デバイス鍵を含む聴覚デバイス鍵の第２のセットを生成するステップを含み、前記方法は聴覚デバイス鍵の前記第２のセットの聴覚デバイス鍵を示す第２の聴覚デバイス鍵識別子を取得するステップを含み、前記聴覚デバイス証明書を生成するステップは、聴覚デバイス鍵の前記第２のセットと前記第２の聴覚デバイス鍵識別子とを前記聴覚デバイス証明書に入れるステップを含む項目７から９のいずれか一項に記載の方法。
［項目１１］
前記聴覚デバイス証明書を生成するステップは、デジタル署名を生成するステップと、前記デジタル署名を前記聴覚デバイス証明書中に入れるステップとを含む項目７から１０のいずれか一項に記載の方法。
［項目１２］
前記聴覚デバイス識別子を生成するステップは、乱数または疑似乱数を生成するステッ

プを含む項目７から１１のいずれか一項に記載の方法。
［項目１３］
前記聴覚デバイスの第１のハードウェア識別子を取得するステップを含み、前記聴覚デバイス証明書を生成するステップは、前記第１のハードウェア識別子を前記聴覚デバイス証明書に入れるステップを含む項目７から１２のいずれか一項に記載の方法。
［項目１４］
前記聴覚デバイス証明書を生成するステップは、証明書タイプ識別子、署名デバイス識別子、１つまたは複数のハードウェア識別子、クライアントデバイスタイプ認証識別子、および／またはトークンパラメータのうちの１つまたは複数を前記聴覚デバイス証明書に入れるステップを含む項目７から１３のいずれか一項に記載の方法。
［項目１５］
前記聴覚デバイス証明書を生成するステップは、ハードウェアプラットフォーム識別子、ソフトウェアプラットフォーム識別子、および／または証明書タイムスタンプを前記聴覚デバイス証明書に入れるステップを含む項目７から１４のいずれか一項に記載の方法。

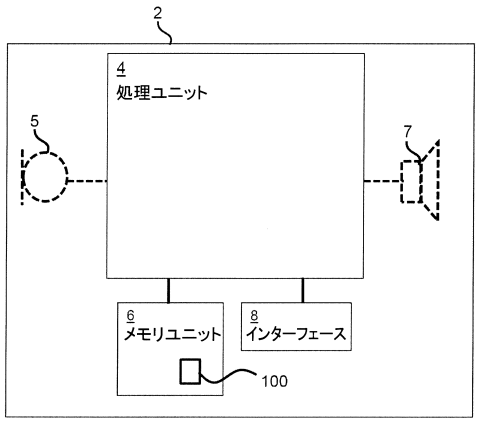
１　：システム
２　：聴覚デバイス
４　：処理ユニット
５　：マイクロフォン
６　：メモリユニット
７　：レシーバ
８　：インターフェース
１０　：クライアントデバイス
１２　：製造デバイス
１４　：フィッティングデバイス
１６　：サーバデバイス
２１　：クライアントデバイスと聴覚デバイスの間の通信リンク
２２　：サーバデバイスと製造デバイスの間の通信リンク
２３　：聴覚デバイスと製造デバイスの間の通信リンク
２４　：サーバデバイスとクライアントデバイス／フィッティングデバイスの間の通信リンク
１００　：聴覚デバイス証明書
１１２　：聴覚デバイス識別子
１１３　：デジタル署名
１１４　：第１の聴覚デバイス鍵識別子
１１５　：聴覚デバイス鍵の第１のセット
１１５Ａ　：第１の一次聴覚デバイス鍵
１１５Ｂ　：第１の二次聴覚デバイス鍵
１１５Ｃ　：第１の三次聴覚デバイス鍵
１１５Ｄ　：第１の四次聴覚デバイス鍵
１１６　：第２の聴覚デバイス鍵識別子
１１７　：聴覚デバイス鍵の第２のセット
１１７Ａ　：第２の一次聴覚デバイス鍵
１１７Ｂ　：第２の二次聴覚デバイス鍵
１１７Ｃ　：第２の三次聴覚デバイス鍵
１１７Ｄ　：第２の四次聴覚デバイス鍵
１１８　：第３の聴覚デバイス鍵識別子
１１９　：聴覚デバイス鍵の第３のセット
１１９Ａ　：第３の一次聴覚デバイス鍵
１１９Ｂ　：第３の二次聴覚デバイス鍵

１１９Ｃ　：第３の三次聴覚デバイス鍵
１１９Ｄ　：第３の四次聴覚デバイス鍵
１３０　：証明書タイプ識別子
１３６　：署名デバイス識別子
１３８　：ハードウェアプラットフォーム識別子
１４０　：ソフトウェアプラットフォーム識別子
１４２　：証明書タイプスタンプ
１４４　：クライアントデバイスタイプ認証識別子
１４６　：トークンパラメータ
１４８　：第１のハードウェア識別子
４００　：信号図
４０１　：聴覚デバイス証明書要求
４０２　：聴覚デバイス証明書応答
５００　：方法

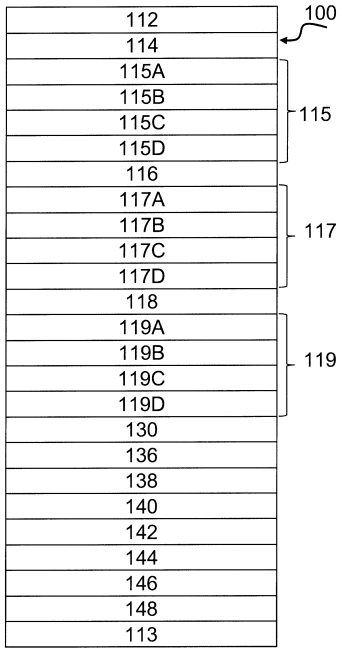
【図１】



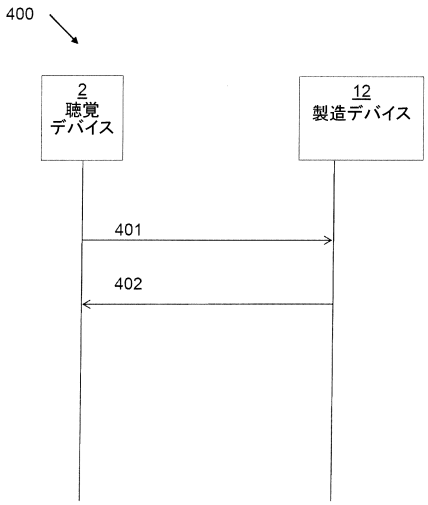
【図２】



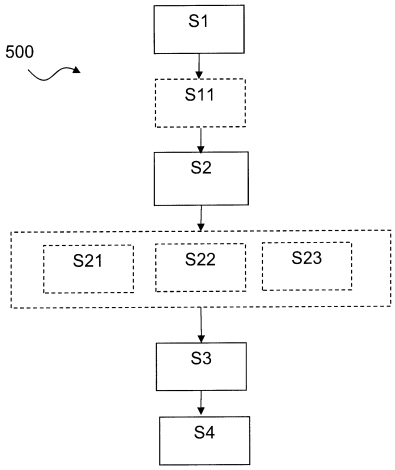
【図３】


100
112
114
115A
115B
115C
115D
115
116
117A
117B
117C
117D
117
118
119A
119B
119C
119D
119
130
136
138
140
142
144
146
148
113

【図４】


400
2
聴覚
デバイス
12
製造デバイス
401
402

【図５】


500
S1
S11
S2
S21
S22
S23
S3
S4

フロントページの続き

審査官　宮司　卓佳

(56)参考文献　特開２０１３－１６２４３３（ＪＰ，Ａ）
特表２０１２－５２９８４３（ＪＰ，Ａ）
特開２００９－０３８６０３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１４
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｒ　２５／００