(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2025-507264
(P2025-507264A)
(43)公表日　令和7年3月18日(2025.3.18)

(51)国際特許分類　F I
H04L 9/16 (2006.01)　H04L 9/16

審査請求　未請求　予備審査請求　未請求　（全31頁）

(21)出願番号　特願2024-544634(P2024-544634)
(86)(22)出願日　令和5年2月6日(2023.2.6)
(85)翻訳文提出日　令和6年7月26日(2024.7.26)
(86)国際出願番号　PCT/EP2023/052749
(87)国際公開番号　WO2023/152059
(87)国際公開日　令和5年8月17日(2023.8.17)
(31)優先権主張番号　22156570.8
(32)優先日　令和4年2月14日(2022.2.14)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)
(81)指定国・地域　AP(BW,CV,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV
最終頁に続く

(71)出願人　590000248
コーニンクレッカ フィリップス エヌヴェ
Koninklijke Philips N.V.
オランダ国 5656 アーヘー アインドーフェン ハイテック キャンパス 52
High Tech Campus 52, 5656 AG Eindhoven, Netherlands
(74)代理人　100122769
弁理士　笛田 秀仙
(74)代理人　100163809
弁理士　五十嵐 貴裕
(74)代理人　100145654
最終頁に続く

(54)【発明の名称】　設定中に暗号強度を変更するための初期の指標

(57)【要約】
方法、コミッショニング装置およびエンローリー装置ならびにそれらのシステムが提供される。この方法は、無線ネットワークにおける通信のためにエンローリー装置を設定するためのものであり、この方法は、コミッショニング装置9およびエンローリー装置4,5による実行のために構成される。コミッショニング装置およびエンローリー装置は、無線通信プロトコルを使用して通信し、設定プロトコルに参加するように構成され、設定プロトコルは、エンローリー装置が無線ネットワークにおいて通信するように設定するように構成される。この方法は、設定プロトコルを実行することを含み、設定プロトコルはコミッショニング装置によって、公開鍵のタイプの選択の指標を含むメッセージを送信することを含み、公開鍵のタイプはエンローリー装置から取得された複数の公開鍵のタイプのから選択され、選択された公開鍵のタイプの鍵は設定プロトコル後のフェイズのために使用されるべきであり、選択された公開鍵のタイプはブートストラップのためにエンローリーから取得された公開鍵のタイプとは異なる。

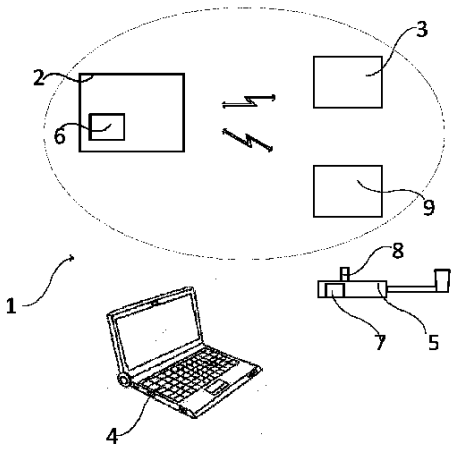

Fig 1

【特許請求の範囲】
【請求項１】
設定プロトコルの実行により無線ネットワークにおける通信のためにエンローリー装置を設定する方法であって、当該方法は、コミッショニング装置およびエンローリー装置により実行されるように構成され、前記コミッショニング装置および前記エンローリー装置は、無線通信プロトコルを用いて通信し、前記設定プロトコルに参加するように構成され、前記設定プロトコルは、
前記エンローリー装置により前記コミッショニング装置へと、帯域外（ＯＯＢ）通信を用いて、第1の公開鍵と、第2の公開鍵のタイプの少なくとも１つの指標とを提供し、
前記コミッショニング装置により、第2の公開鍵のタイプの前記少なくとも１つの指標が、前記第1の公開鍵のタイプと異なる鍵のタイプを示す場合、
前記少なくとも１つの指標から鍵の少なくとも１つのタイプの選択であって、当該選択における全てのタイプが前記第1の公開鍵のタイプと異なる、選択を行い、
前記無線通信プロトコルを用いて第1のメッセージを送信し、前記第1のメッセージは、前記選択におけるいずれかの鍵のタイプに対応するタイプの第2の公開鍵を要求し、前記第2の公開鍵は、前記エンローリー装置が前記無線ネットワークに接続することを可能にするために前記コミッショニング装置により用いられ、
前記エンローリー装置により、前記第1のメッセージにおいて要求された鍵のタイプの第2の公開鍵を含む第2のメッセージを送信し、
前記エンローリー装置および前記コミッショニング装置により、前記選択に対応するタイプの鍵を用いて前記設定プロトコルを完了して、前記エンローリー装置により、前記無線ネットワークへの接続を試行する、方法。
【請求項２】
設定プロトコルの実行により無線ネットワークにおける通信のためにエンローリー装置を設定する方法であって、当該方法は、コミッショニング装置およびエンローリー装置により実行されるように構成され、前記コミッショニング装置および前記エンローリー装置は、無線通信プロトコルを用いて通信し、前記設定プロトコルに参加するように構成され、前記設定プロトコルは、
前記エンローリー装置により前記コミッショニング装置へと、帯域外（ＯＯＢ）通信を用いて、第1の公開鍵と、第2の公開鍵のタイプの少なくとも１つの指標とを提供し、
前記コミッショニング装置により、第2の公開鍵のタイプの前記少なくとも１つの指標が、前記第1の公開鍵のタイプと異なる鍵のタイプを示す場合、
前記少なくとも１つの指標から鍵の少なくとも１つのタイプの選択であって、当該選択における全てのタイプが前記第1の公開鍵のタイプと異なる、選択を行い、
データオブジェクトに署名するために前記選択におけるいずれかの鍵のタイプに対応するタイプの第3の鍵を使用し、前記データオブジェクトは、前記エンローリー装置に送信されるように構成され、前記無線ネットワークへの接続を試行するために前記エンローリー装置により用いられるように構成され、
前記エンローリー装置および前記コミッショニング装置により、前記選択に対応するタイプの鍵を用いて前記設定プロトコルを完了し、前記データオブジェクトを用いて前記無線ネットワークへの接続を試行し、
前記選択の実行および前記データオブジェクトへの署名が、前記エンローリー装置により前記コミッショニング装置へと、前記ＯＯＢ通信を用いて、前記第1の公開鍵と、第2の公開鍵のタイプの前記少なくとも１つの指標とを提供して以降、最初に前記無線ネットワークへの接続の試行が行われる前に行われる、方法。
【請求項３】
第2の公開鍵のタイプの前記少なくとも１つの指標が前記第1の公開鍵のタイプと同じ鍵のタイプを示す場合、前記少なくとも１つの指標は、第2の公開鍵のタイプの前記少なくとも１つの指標が前記第1の公開鍵のタイプと異なる鍵のタイプを示す場合に用いられるデータ要素より小さいデータ要素を使用する、請求項１または２に記載の方法。

【請求項４】
第2の公開鍵のタイプの前記少なくとも１つの指標が前記第１の公開鍵のタイプの同じタイプのみを示す場合、前記コミッショニング装置により、前記設定プロトコルの完了前に、前記設定プロトコルの実行を終了する、請求項１から３のいずれか一項に記載の方法。
【請求項５】
第2の公開鍵のタイプの前記少なくとも１つの指標が前記コミッショニング装置が使用できる公開鍵のタイプを含まない場合、前記コミッショニング装置により、前記設定プロトコルの完了前に、前記設定プロトコルの実行を終了する、請求項１から４のいずれか一項に記載の方法。
【請求項６】
前記エンローリー装置が単純な装置である、請求項１から５のいずれか一項に記載の方法。
【請求項７】
前記設定プロトコルがデバイスプロビジョニングプロトコル（Device Provisioning Protocol ：DPP)である、請求項１から６のいずれか一項に記載の方法。
【請求項８】
第2の公開鍵のタイプの前記少なくとも１つの指標がＤＰＰブートストラップＵＲＬのビットマスク部分に含まれる、請求項７に記載の方法。
【請求項９】
鍵の前記少なくとも１つのタイプの前記選択の実行および前記第１のメッセージの前記送信が、前記エンローリー装置により前記コミッショニング装置へと、前記OOB通信を用いて、前記第1の公開鍵と、第2の公開鍵のタイプの前記少なくとも１つの指標とを提供して以降、最初に前記エンローリー装置により前記無線ネットワークへの接続が試行される前に行われる、請求項１に直接または間接的に従属する請求項３から８のいずれか一項に記載の方法。
【請求項１０】
無線通信プロトコルを用いて通信するように構成され、無線ネットワークにおける通信のためにコミッショニング装置により設定されるように構成されたエンローリー装置であって、
前記エンローリー装置は、前記無線ネットワークにおける通信のために構成されたトランシーバを有し、
前記エンローリー装置は、
前記エンローリー装置を設定するように構成された設定プロトコルに参加し、
帯域外（OOB）通信を用いて、前記設定プロトコルの第１フェイズにおいて用いるための第１の公開鍵と、第２の公開鍵のタイプの少なくとも１つの指標とを提供し、
前記トランシーバを介して、前記無線通信プロトコルを用いて、コミッショニング装置から第１メッセージを受信するように構成され、
前記第１メッセージは、第２の公開鍵の１つまたは複数のタイプを示す要求を含み、第２の公開鍵の前記タイプは前記第１の公開鍵のタイプと異なり、
前記エンローリー装置はさらに、
前記トランシーバを介して、前記無線通信プロトコルを用いて、前記第１メッセージにおいて要求されたタイプの第２の公開鍵を含む第２メッセージを前記コミッショニング装置に送信し、
設定された結果として前記無線ネットワークへの接続を試行する、
ように構成される、エンローリー装置。
【請求項１１】
無線通信プロトコルを用いて通信するように構成され、無線ネットワークにおける通信のためにコミッショニング装置により設定されるように構成されたエンローリー装置であって、

前記エンローリー装置は、前記無線ネットワークにおける通信のために構成されたトランシーバを有し、
前記エンローリー装置は、
前記エンローリー装置を設定するように構成された設定プロトコルに参加し、
帯域外（ＯＯＢ）通信を用いて、前記設定プロトコルの第１フェイズにおいて用いるための第１の公開鍵と、第２の公開鍵のタイプの少なくとも１つの指標とを提供し、
前記少なくとも１つの指標から前記コミッショニング装置により選択された、前記第１の公開鍵と異なるタイプである第３の鍵を用いて前記コミッショニング装置により署名されたデータオブジェクトを復号し、
設定された結果として前記無線ネットワークへの接続を試行するように構成され、
前記データオブジェクトの前記復号が、前記エンローリー装置により前記コミッショニング装置へと、前記ＯＯＢ通信を用いて、前記第1の公開鍵と、第2の公開鍵のタイプの前記少なくとも１つの指標とを提供して以降、最初に前記無線ネットワークへの接続の試行が行われる前に行われる、エンローリー装置。
【請求項１２】
前記要求が公開鍵の複数のタイプを示す場合、最大の暗号化強度を持つタイプの第２の公開鍵を提供するように構成される、請求項１０または１１に記載のエンローリー装置。
【請求項１３】
単純な装置である、請求項１０から１２のいずれか一項に記載のエンローリー装置。
【請求項１４】
第２の公開鍵のタイプの前記少なくとも１つの指標が、ＤＰＰブートストラップＵＲＬのビットマスク部分に含まれる、請求項１０から１３のいずれか一項に記載のエンローリー装置。
【請求項１５】
前記第１メッセージの受信および前記第２メッセージの送信が、前記エンローリー装置により前記コミッショニング装置へと、ＯＯＢ通信を使用して、前記第1の公開鍵、および、第2の公開鍵のタイプの前記少なくとも1つの指標を提供して以降、最初に前記エンローリー装置が前記無線ネットワークへの接続を試行する前に実行される、請求項１０および請求項１０に直接または間接的に従属する請求項１２から１４のいずれか一項に記載のエンローリー装置。
【請求項１６】
コミッショニング装置として動作するように構成され、無線ネットワークにおける通信のためにエンローリー装置を設定するように構成された装置であって、
前記装置は、無線通信プロトコルに従って送受信するように構成されたトランシーバを有し、
前記装置は、
設定プロトコルに参加し、
前記エンローリー装置から、帯域外（ＯＯＢ）通信を介して、第１の公開鍵と、前記設定プロトコルの一部として使用されるべき公開鍵の第２のタイプの少なくとも１つの指標とを取得し、
前記少なくとも１つの指標が前記第１の公開鍵のタイプと異なる鍵のタイプを示す場合、前記少なくとも１つの指標に基づいて鍵の少なくとも１つのタイプの選択を行うように構成され、当該選択における全てのタイプは前記第１の公開鍵のタイプと異なり、
前記装置はさらに、
前記トランシーバおよび前記無線通信プロトコルを用いて、前記選択におけるいずれかの鍵のタイプに対応する鍵のタイプの第２の公開鍵を要求する第１メッセージを前記エンローリー装置に送信するように構成される、装置。
【請求項１７】
コミッショニング装置として動作するように構成され、無線ネットワークにおける通信のためにエンローリー装置を設定するように構成された装置であって、

前記装置は、無線通信プロトコルに従って送受信するように構成されたトランシーバを有し、
前記装置は、
設定プロトコルに参加し、
前記エンローリー装置から、帯域外（OOB）通信を介して、第１の公開鍵と、前記設定プロトコルの一部として使用されるべき第２の公開鍵のタイプの少なくとも１つの指標とを取得し、
前記少なくとも１つの指標が前記第１の公開鍵のタイプと異なる鍵のタイプを示す場合、前記少なくとも１つの指標に基づいて鍵の少なくとも１つのタイプの選択を行うように構成され、当該選択における全てのタイプは前記第１の公開鍵のタイプと異なり、
前記装置はさらに、
データオブジェクトに署名するために前記選択における鍵のタイプに対応するタイプの第３の鍵を使用し、前記トランシーバを介して、前記無線通信プロトコルを用いて、署名された前記データオブジェクトを前記エンローリー装置に送信するように構成され、前記データオブジェクトは、前記無線ネットワークへの接続を試行するために前記エンローリー装置により使用されるように構成され、
前記選択の実行および前記第３の鍵の使用は、前記第１の公開鍵と、前記第２の公開鍵のタイプの前記少なくとも１つの指標とを、前記OBB通信を介して、前記エンローリー装置から取得して以降、最初に前記エンローリー装置が前記無線ネットワークへの接続を試行する前に行われる、装置。

【請求項１８】

前記第１の公開鍵のタイプと同じ鍵のタイプのみを前記指標が示す場合、前記エンローリー装置の設定の完了前に終了するように構成される、請求項１６または１７に記載の装置。

【請求項１９】

前記装置が使用することができる鍵のタイプを前記少なくとも１つの指標が示さない場合、前記エンローリー装置の設定の完了前に終了するように構成される、請求項１６または１７に記載の装置。

【請求項２０】

鍵の前記少なくとも１つのタイプの選択の前記実行および前記第１のメッセージの前記送信が、前記エンローリー装置により前記コミッショニング装置へと、前記OOB通信を用いて、前記第1の公開鍵と、第2の公開鍵のタイプの前記少なくとも１つの指標とを提供して以降、最初に前記エンローリー装置により前記無線ネットワークへの接続が試行される前に行われる、請求項１６ならびに請求項１６に従属する請求項１８および１９のいずれか一項に記載の装置。

【請求項２１】

エンローリー装置のプロセッサにより実行され、請求項１から９のいずれか一項に記載の方法を前記エンローリー装置に実行させる、コンピュータプログラム。

【請求項２２】

コミッショニング装置のプロセッサにより実行され、請求項１から９のいずれか一項に記載の方法を前記コミッショニング装置に実行させる、コンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、無線ネットワーク、特に、IEEE 802.11規格ファミリーに準拠する無線ネットワークにおいて使用するための装置及び方法に関する。

【背景技術】

【０００２】

図1は、第1装置2と別の装置3とを含む無線ネットワーク1を示す。第1装置2は中央機能を有し、アクセスポイント(AP)、ハブまたはゲートウェイ装置のようなものであるこ

とができる。第1装置2は、以下では簡略化のためにAPと呼ばれるが、他のタイプの装置も実際に可能である。ユーザ(図示せず)は、ネットワーク1にさらに2つの装置、すなわち複雑な装置4(ここではコンピュータとして表される)および単純な装置5(ここでは歯ブラシとして表される)を追加することを望む。単純な装置5のような装置は、多くの場合、恐らくライト以外の実際のユーザインタフェース(UI)を有しておらず、したがって、しばしば「ヘッドレス」装置と呼ばれる。AP 2はプロセッサ6を有し、単純な装置5は、マイクロコントローラと、小型の不揮発性メモリ7と、単純な装置5をリセットするために使用することができるボタン8とを有する。第3の装置9もある。単純な装置5は、特定のリセットボタンを有していなくてもよい。無線ネットワークはIEEE 802.11に基づくものなどの無線通信技術を使用するが、他の技術も適切であり得る。

【０００３】

一部の無線ネットワーク規格では、接続を確立して通信するために、或る装置が別の装置を設定できる。これは、ユーザがもはや手動入力を行う必要がないという点で、ネットワークに新しい装置を追加または登録するタスクの負担を軽くする。ネットワークに参加するために設定を必要とする装置は「エンローリー（enrollee）」と呼ばれることがあり、設定を実行する装置は、「コミッショニング装置(commissioning device)」または「コミッショナー（commissioner）」と呼ばれることがある。「Wi-Fi Easy Connect」とも呼ばれるデバイスプロビジョニングプロトコル（DPP）の場合、コミッショニング装置は「コンフィギュレータ」と呼ばれ、登録デバイスは「エンローリー」と呼ばれる。

【０００４】

コミッショニング装置と、エンローリー及び、最終的にはエンローリーが接続されることになるネットワークとの間で信頼が確立されることが望ましい。この文脈における「信頼」は、設定されている装置が意図された装置であり、他の悪意のある装置が接続に介入できないことを意味すると理解されることができる。この目的のために、通信はしばしば暗号化される。

【０００５】

Diffie-Hellman(参考文献[DH])は、秘密鍵を確立するための当事者間の通信が、確立された秘密鍵に関するいかなる情報も第三者に開示しない、2者間で秘密鍵を確立するための公知の技術である。2つの当事者はそれぞれ、自身の公開/秘密鍵ペアを使用し、公開鍵を互いに交換する。各当事者は、自身の秘密鍵と相手の公開鍵、および場合によっては、各当事者からのナンス(乱数)などの他の情報を使用して、秘密鍵を計算することができる。各当事者は、Diffie-Hellmanを実行するたびに新しい鍵ペアを生成するか、あるいは古い鍵ペアを再利用することができる。

【０００６】

Wi-Fi Allianceのデバイスプロビジョニングプロトコル（ Device Provisioning Protocol：DPP）は（文献［DPP］を参照）、Diffie-Hellmanを使用して、2つのデバイス、すなわち、設定されることを望むDPPエンローリーと、DPPエンローリーを設定することができるDPPコンフィギュレータ（すなわち、コミッショニング装置）との間に秘密鍵を確立し、そしてこれらは、DPP対応ネットワークへのアクセスを得ることができるか、またはDPP対応ネットワークをアクセスポイント（AP）として設定することができる（文献［802.11］を参照）。

【０００７】

ネットワーク上でDiffie-Hellmanを実行するとき、Diffie-Hellmanを実行するための公開鍵を受信する装置は、この公開鍵がどの装置からであるかを知らない。これは、いわゆる中間者攻撃において、攻撃者によって悪用される可能性がある。攻撃者Eは、装置Aが接続したい実際の装置Bを装う可能性がある。攻撃者Eは装置AとDiffie-Hellmanを実行し、装置Aと秘密鍵Kaeを確立する。同様に、攻撃者は、装置Bに対して装置Aになりすまし、装置Bと秘密鍵Kbeを確立する。装置AまたはBのうちの1つからメッセージが到来すると、攻撃者は一方の秘密鍵でメッセージを解読し、それを他方の秘密鍵で暗号

化し、それをもう1つの装置に転送する。このようにして、装置A及びBは、何らかの余分な遅延を除いて、それらの通信において何らかの不思議なことに気付かない。別の通信方法で同じ情報を送信し、その結果を比較することによって通信をチェックする場合、彼らは、彼らの通信のいかなる改竄にも気付かない。しかし、攻撃者は、何を通信するかについて完全な知識を持っている。

` 中間者攻撃を防止し、信頼性を確保するための1つの方法は、公開鍵または公開鍵のハッシュを交換するために、追加のプロトコル、いわゆる帯域外(OOB)通信を使用することである。OOB通信は、Wi-Fi[802.11]、Bluetooth[BT]、802.15.4[802.15.4]、ZigBee[ZIGBEE]、近距離無線通信[NFC]などの近距離無線通信プロトコルであることができる。あるいは、OOB通信は、エンローリー装置に関連するQRコードをスキャンするなどの技法によって、コミッショニング装置が公開鍵を取得することを伴うことができ、エンローリー装置はQRコードから（1つまたは複数の）公開鍵を復号する。

【０００８】

このようにして、装置のユーザは、QRコードとエンローリーとの関連付けを検証することができるので、またはエンローリーがOOB通信プロトコルの動作範囲内にあるので、OOBで受信された公開鍵が意図された装置からであることが分かる。公開鍵のハッシュがOOBで交換されると、装置は、暗号化が必要な通信プロトコルを介して受信された公開鍵が、OOB受信されたハッシュと同じハッシュをもたらすかどうかを確認することができる。本明細書における通信プロトコルという用語の使用は、送受信のための物理層を含むISO-OSIモデルの複数の層を包含することに注意されたい。

【０００９】

具体的には、DPP(装置プロビジョニングプロトコル)(https://www.wi-fi.org/downloads-public/wi-fi_Easy_Connect_Specification_v2.0.pdf/35330))を用いて設定されたエンローリーのケースを考える。このプロトコルは、Wi-Fi Easy Connectの名称でも知られている。

【００１０】

DPPでは、楕円曲線暗号［RFC 6090］がすべての非対称暗号、特に公開プロトコル鍵（ネットワークアクセス鍵（NAK）とも呼ばれる）とコミッショニング装置署名鍵に使用される。ECC曲線をサポートするための必須条件はP-256である。他の設定または設定プロトコルでは、他の形態の暗号化が使用されることができる。

【００１１】

エンローリー(APまたはAPに関連付けることができるWi-Fi装置）が、ネットワークアクセス鍵(netAccessKeyまたはNAK）についてECC曲線P-256 を使用してWi-Fi Easy Connect Release 2のコンフィギュレータによって設定されているとする。これは、エンローリーがP-256ブートストラップ鍵を使用したことを意味する。これは、これら2つの曲線がDPP R2において同じである必要があるためである。コミッショニング装置は、その署名鍵にP-256とは異なる曲線を使用していた可能性がある。

【００１２】

ユーザは、P-256がもはや使用されず、代わりにより強い曲線が使用されるように、ネットワークのセキュリティをアップグレードすることを望む。つまり、APとそのネットワーク上で許可されているすべての装置が新しく設定される必要がある。またはユーザは、P-384などの、P-256を実装するために必須であるよりも好ましくはより強い他の曲線を使用して、DPPネットワークを作成することを望む。曲線（P-256または他のもの）は、鍵の「タイプ」であると考えることができる。

【発明の概要】

【発明が解決しようとする課題】

【００１３】

セキュリティアップグレードを管理するという要件は、単純な装置が新しい要求を処理する方法に加えて、新しい鍵/鍵タイプを処理する方法が必要であることを意味する。

【課題を解決するための手段】

【００１４】
したがって、設定プロトコルの実行によって無線ネットワークにおける通信のためにエンローリー装置を設定する方法が提供され、この方法は、コミッショニング装置およびエンローリー装置によって実行されるように構成され、コミッショニング装置およびエンローリー装置は、無線通信プロトコルを使用して通信し、設定プロトコルに参加するように構成され、設定プロトコルは、
- エンローリー装置によって、第1の公開鍵、および、第2の公開鍵のタイプの少なくとも1つの指標を、アウトオブバンド（ＯＯＢ）通信を使用して、コミッショニング装置へと提供するステップと、
- コミッショニング装置によって、第2の公開鍵のタイプの前記少なくとも1つの指標が、第1の公開鍵のタイプとは異なる鍵のタイプを示す場合、前記少なくとも1つの指標から少なくとも1つの鍵のタイプを選択するステップであって、前記選択における全てのタイプが、前記第1の公開鍵のタイプとは異なる、ステップと、
- 無線通信プロトコルを使用して第1のメッセージを送信するステップであって、第1のメッセージは、前記選択における任意の鍵タイプに対応するタイプの第2の公開鍵を要求し、第2の鍵は、エンローリー装置が無線ネットワークに接続することを可能にするためにコミッショニング装置によって使用される、ステップと、
-エンローリー装置によって、第1のメッセージ内で要求された鍵のタイプの第2の公開鍵を含む第2のメッセージを送信するステップと、
- エンローリー装置およびコミッショニング装置によって、前記選択に対応するタイプの鍵を使用して設定プロトコルを完了し、エンローリー装置によって、無線ネットワークに接続しようと試みるステップとを有する。
【００１５】
設定プロトコルの実行によって無線ネットワークにおける通信のためにエンローリー装置を設定する方法も提供され、前記方法は、コミッショニング装置（9）およびエンローリー装置によって実行されるように構成され、前記コミッショニング装置およびエンローリー装置は、無線通信プロトコルを使用して通信し、前記設定プロトコルに参加するように構成され、前記設定プロトコルは、
- エンローリー装置によって、アウトオブバンド（ＯＯＢ）通信を使用して、第1の公開鍵、および、第2の公開鍵のタイプの少なくとも1つの指標を、コミッショニング装置へと提供するステップと;
- コミッショニング装置によって、第2の公開鍵のタイプの少なくとも1つの指標が第1の公開鍵のタイプとは異なる鍵のタイプを示す場合、前記少なくとも1つの指標から少なくとも1つの鍵のタイプの選択を行うステップであって、前記選択におけるすべてのタイプが第1の公開鍵のタイプとは異なる、ステップと、
- 前記選択における任意の鍵タイプに対応するタイプの第3の鍵を使用してデータオブジェクトに署名するステップであって、前記データオブジェクトは、エンローリーに送信されるように構成され、無線ネットワークに接続しようと試みるためにエンローリー装置によって使用されるように構成される、ステップと;
- エンローリー装置およびコミッショニング装置によって、前記選択に対応するタイプの鍵を使用して設定プロトコルを完了し、前記データオブジェクトを使用して無線ネットワークに接続することを試みるステップとを有し、前記選択の実行およびデータオブジェクトの署名は、エンローリー装置によって、ＯＯＢ通信を使用して、第1の公開鍵、および、第2の公開鍵のタイプの少なくとも1つの指標を、コミッショニング装置に提供して以降、ネットワークへの接続の試行が最初に行われる前に行われる。
【００１６】
一態様では、第2の公開鍵のタイプの少なくとも1つの指標が第1の公開鍵と同じ鍵のタイプを示すとき、前記少なくとも1つの指標は、第2の公開鍵のタイプの少なくとも1つの指標が第1の公開鍵のタイプとは異なる鍵のタイプを示すときに使用されるデータ要素よりも小さいデータ要素を使用する。

【００１７】
このようにして、符号化されるデータの量が低減されることができる。誤り訂正機構のオーバーヘッドを考慮すると、節約はさらに大きくなることが明らかになる。これは、ＯＯＢ通信がＱＲコードを使用するときに特に有利である。ＱＲコードでは、空間は重要視され、符号化されるデータを増加させることはコードにより必要とされる面積を増加させる。これにより、製品またはパッケージ上に拡張されたＱＲコードを適合させることが困難になる場合がある。
【００１８】
一態様では、本方法は、第２の公開鍵のタイプの少なくとも１つの指標が第１の公開鍵のタイプと同じタイプのみを示す場合、設定プロトコルの実行をコミッショニング装置によって完了する前に、終了することを含むことができる。
【００１９】
一態様では、本方法は、第２の公開鍵のタイプの少なくとも１つの指標がコミッショニング装置が使用することが可能である公開鍵のタイプを含まない場合、設定プロトコルの実行をコミッショニング装置により完了する前に終了することを含むことができる。
【００２０】
したがって、コミッショニング装置は、エンローリーがサポートすることができる暗号化の最高強度を決定することができる。そのような暗号化の強度は、問題のネットワークにとって不十分であることが生じる可能性がある。ＯＯＢ通信フェイズにおいて、またはエンローリーが提案された新しい公開鍵で応答したときに、この最高暗号強度を決定することによって、コミッショニング装置は、早期に失敗することによって（ユーザ側での）手間を省くことができる。これをユーザに報告することもできる。
【００２１】
一態様では、エンローリー装置は単純な装置である。
【００２２】
一態様では、設定プロトコルはデバイスプロビジョニングプロトコル（ＤＰＰ）に従う。
【００２３】
一態様では、第２の公開鍵のタイプの少なくとも１つの指標は、ＤＰＰブートストラップＵＲＩのビットマスク部分に含まれる。
【００２４】
一態様では、少なくとも１つの公開鍵のタイプの選択の実行と、第１のメッセージの送信は、エンローリー装置によりコミッショニング装置へと、ＯＯＢ通信を使用して、第１の公開鍵、および第２の公開鍵のタイプの少なくとも１つの指標が提供されてから、エンローリー装置による初めてのネットワークへの接続の試行の前に行われる。
【００２５】
無線通信プロトコルを使用して通信するように構成され、無線ネットワークにおける通信のためのコミッショニング装置によって設定されるように構成されるエンローリーが提供され、エンローリー装置は無線ネットワークにおける通信のために構成されるトランシーバを有し、エンローリー装置は、
- エンローリー装置を設定するように構成される設定プロトコルに参加し;
- 帯域外（ＯＯＢ）通信を使用して、設定プロトコルの第１のフェイズで使用するための第１の公開鍵と、第２の公開鍵のタイプの少なくとも１つの指標とを提供し;
-前記トランシーバを介して、および無線通信プロトコルを使用して、コミッショニング装置から第１のメッセージを受信し、第１のメッセージは第２の公開鍵の１つまたは複数のタイプを示す要求を含み、第２の公開鍵のタイプは第１の公開鍵のタイプとは異なり;
-前記トランシーバを介して、および無線通信プロトコルを使用して、コミッショナー装置に第２のメッセージを送信し、第２のメッセージは、第１のメッセージにおいて要求されたタイプの第２の公開鍵を含み;
- 無線通信プロトコルを使用して、コミッショニング装置と共に、第１の公開鍵および前記少なくとも１つの指標によって示されるタイプの鍵を使用してコミッショニングプロト

コルに参加し;
- 設定された結果としてネットワークへの接続を試みる、ように構成される。
【００２６】
このように構成されたエンローリー装置は、OOB通信フェイズにおいて、すなわち設定プロセスのスタート付近において、自身の公開ブートストラップ鍵のレベルまたは強度を超えてサポートすることができる暗号化のレベルまたは強度を示すことができる。これは、次に、このファシリティを使用するように構成されたコミッショニング装置が、a）エンローリーが十分な暗号化強度をサポートすることができることを決定し、b）エンローリーがサポートすることができる暗号化強度を（1つまたは複数の鍵のタイプを選択する形で）選択することを可能にする。
【００２７】
追加的にまたは代替として、エンローリー装置はデータオブジェクトを検証するように構成され、データオブジェクトは前記少なくとも1つの指標に対応するタイプの鍵を使用してコミッショニング装置によって署名されている。
【００２８】
したがって、エンローリーは、初期設定の暗号化、すなわち、エンローリーの公開ブートストラップ鍵よりも高い強度の暗号化を有する鍵を提供し、使用することができる。
【００２９】
一態様では、エンローリー装置は、前記要求が2つ以上の公開鍵のタイプを示すときに、最大の暗号強度を有するタイプの第2の公開鍵を提供するように構成される。
【００３０】
コミッショニング装置が新しい鍵タイプのオプションを含む要求を行うことが有利である。例えば、コミッショニング装置は、多くのタイプのエンローリーに対処しなければならない場合があり、そのうちのいくつかは、厳密に必要とされるよりもエンローリーにとってより負担の大きい暗号化のレベルに対するサポートを通知する場合がある。選択の一部をエンローリーに任せることで、プロセスにいくらかの柔軟性を導入することができる。要求により、エンローリーが新しい（アップグレードされた）公開鍵にどの鍵タイプを使用するかを選択することが可能になり、エンローリーが最も強力な暗号化を提供するオプションを選択することにより、ネットワークがこれから恩恵を受けることが可能になる。
【００３１】
一態様では、エンローリー装置は単純な装置である。
【００３２】
コミッショニング装置として機能するように構成され、無線ネットワークにおける通信のためにエンローリー装置を設定するように構成される装置が提供される。
- この装置は、無線通信プロトコルに従って送受信するように構成されたトランシーバを有し、この装置は以下のように構成される：
- 設定プロトコルに参加し、
- 第1の公開鍵、および、設定プロトコルの一部として使用されるべき公開鍵の第2のタイプの少なくとも1つの指標を、アウトオブバンド（OOB）通信を介して、エンローリー装置から取得し;
- 前記少なくとも1つの指標が、第1の公開鍵のタイプとは異なる鍵のタイプを示す場合、前記少なくとも1つの指標に基づいて少なくとも1つのタイプの鍵の選択を実行し、前記選択におけるすべてのタイプは第1の公開鍵のタイプとは異なり、
- トランシーバと無線通信プロトコルを使用して、前記選択における鍵タイプのいずれかに対応する鍵のタイプの第2の公開鍵を要求する第1のメッセージをエンローリー装置に送信し、および/または、
- 前記選択における鍵タイプのいずれかに対応するタイプの第3の鍵を使用してデータオブジェクトに署名し、トランシーバを介して、無線通信プロトコルを使用して、署名されたデータオブジェクトをエンローリーに送信し、データオブジェクトは、無線ネットワー

クに接続を試みるためにエンローリー装置によって使用される。
【００３３】
こうして、コミッショニング装置は、エンローリーブートストラップ鍵のタイプ以外のどのタイプの鍵をエンローリーがサポートすることができるかを決定することができる。その情報を用いて、それは、エンローリーから新しい公開鍵を要求することができる。追加的にまたは代替として、（エンローリーブートストラップ鍵のタイプとは異なる）どの鍵タイプを使用して、接続情報パケットを含むデータオブジェクト（例えば、ＤＰＰコネクタ）に署名することができるかを決定することができる。コミッショニング装置は、使用できるものを決定することによって、試行錯誤に頼ることを必要とせずに、暗号化レベルを変更することができる。
【００３４】
一態様では、装置は、指標が第1の公開鍵の鍵タイプと同じタイプの鍵のみを示す場合、エンローリー装置の設定を完了する前に終了するように構成される。
【００３５】
一態様では、装置は、前記少なくとも1つの指標が装置が使用可能にされている鍵のタイプを示していない場合、エンローリー装置の設定を完了する前に終了するように構成される。
【００３６】
エンローリー装置内のプロセッサ上で動作するとき、エンローリー装置に本明細書で説明する方法を実行させるコンピュータプログラム製品、およびコミッショニング装置内のプロセッサ上で動作するとき、コミッショニング装置に本明細書で説明する方法を実行させるコンピュータプログラム製品も提供される。
【図面の簡単な説明】
【００３７】
開示された装置、システムおよび方法の上記ならびに追加の目的、特徴および利点は、添付の図面を参照して、装置及び方法の実施形態の以下の例示的かつ非限定的な詳細な説明を通して、より良く理解されるであろう。
【図１】追加のために装置を設定したい無線ネットワークを表す図。
【図２】設定プロセスのフロー。
【図３】実施形態に係る再設定プロセスのフロー。
【図４】ＱＲコードの表現を示す図。
【図５ａ】コンピュータ可読媒体を示す図。
【図５ｂ】プロセッサシステムの概略図。
【００３８】
図面は概略的であり、一定の縮尺で描かれていない。図面において、既に説明された要素に対応する要素は、同じ参照番号を有する場合がある。
【発明を実施するための形態】
【００３９】
以下の説明では、同じ参照符号は同様の要素を指す。
【００４０】
図2は、図1の第3の装置9などの1つの装置が、図1の複雑なまたは単純な装置4，5などの別の装置を設定し、それに接続し得る、装置で制御される設定のフローを表す。
【００４１】
図2のプロセスは、コミッショニングプロトコルまたは設定プロトコルと呼ばれることがある。一例として、単純な装置5の場合について説明する。この説明の多くは、ＡＰ２のような装置を持つネットワークを含む例を提供しているが、このプロセスはピアツーピアの状況で機能する可能性があることを理解しておく必要がある。この設定フローは、設定されていない状態にあるか、またはまだ接続できない装置を設定するために使用され得る。
【００４２】

装置制御設定方法の一例として、Wi-FiまたはIEEE 802.11 を使用するネットワークで使用される装置プロビジョニングプロトコル(DPP) がある。装置プロビジョニングプロトコル(DPP)では、DPPコンフィギュレータとして機能する装置が、Wi-Fi APに接続するために、任意のWi-Fi対応装置を安全に設定できる。

【００４３】

S1(Start)において、プロセスは、2つの装置9および5が接続されていない状態で開始し、装置5は設定されていない。説明のために、装置9は、無線ネットワーク1に参加するために装置5を設定するために使用され、したがって、装置9は、コミッショニング装置（たとえば、DPPコンフィギュレータ）と呼ばれ、装置5は、（無線ネットワーク1に「エンロール（登録）される」ので）エンローリーと呼ばれることがある。

【００４４】

しばしば「ブートストラップ」と呼ばれるS2（Bootstrapping）において、一方の装置、イニシエータは、他方の装置、レスポンダのブートストラップ公開鍵（B_R）を取得する。レスポンダ装置が相互認証を望む場合、イニシエータのブートストラップ公開鍵（B_I）も取得する。これは、無線通信技術とは別の方法によって達成され、いわゆる「帯域外」通信(OOB)と呼ばれる。たとえば、ユーザが或る装置にレスポンダ上のQRコードを読み取らせること、2つの装置間のNFC通信、または別の無線技術（例えばBluetooth)の場合がある。ブートストラッププロセスは、ユーザの介入によって開始される。ブートストラップが成功した場合、プロセスはS3(Bootstrapped)に達し、装置9，5は「ブートストラップ」され、そうでない場合、S1において「start」状態に戻る。いずれの場合も、エンローリー装置(この場合は単純装置5)は、ブートストラップ処理の結果を、例えばメモリ内のレジスタ内のフラグとして、適切な記憶装置に記録することができる。しばしば、単純な装置は、製造後またはリセット後に起動し、設定のためにQRコードに示されるチャネル上で無線をオンにし、認証要求メッセージをリスンすることを開始するようにプログラムされる

【００４５】

S4(Authentication)において、装置9，5は、認証手順を実行し、それによって、装置は「信頼」を確立し、すなわち、ユーザは、それらの装置が信じるものであり、問題の装置のうちの1つまたは他のものである「ふりをする」他の未知の(および潜在的に悪意のある)装置ではないことを確信することができる。認証の開始を要求するメッセージが1つの装置から送信される。このメッセージは、設定を行う装置（コミッショニング装置もしくはコンフィギュレータ（DPPの場合））または設定されるべき装置（エンローリー）のいずれかによって送信されることができる。この例では、第3のデバイス9は、コミッショニング装置として機能し、単純な装置5はエンローリーとして機能する。第3の装置9はネットワーク1に接続されているように示されているが、これは実施形態が機能するために必ずしも必要ではないことに留意されたい。無線通信を開始する装置をイニシエータ、応答する装置をレスポンダと呼ぶ。特に、DPPプロトコルは、コミッショニング装置及びエンローリー装置の両方がDPPプロトコルのイニシエータとして動作することを可能にし、そして他の装置は自動的にレスポンダになる。単純な装置またはヘッドレス装置は、通常、レスポンダの役割を担う。

【００４６】

他の装置がこのメッセージに応答する。認証要求メッセージが正しく復号され、イニシエータがレスポンダ装置が信じる装置であり、必要な機能を持っていることを示す情報が含まれる場合、応答メッセージはメッセージが「受け入れられた」ことを示し、イニシエータがレスポンダの資格情報を検証するために必要な情報を含み、必要な機能も持っていることを示す。2つの装置が他の装置から必要な情報を受信しない場合、プロセスは中断し、装置はS3におけるブートストラップされた状態または開始状態S1に戻る。イニシエータがエンローリーの場合、認証要求メッセージには、エンローリーを設定するための以前の試行の結果を示す追加部分も含まれる場合がある。レスポンダがエンローリーの場合、認証応答メッセージは、前回の試行の結果を示す追加部分を含む場合がある。指標はま

た、以前の試行があったか否かを示してもよいことを理解されたい。これらの認証メッセージにおいて、両方の装置は、自身の公開鍵に属する秘密鍵を所有していることを証明する情報を提供し、その公開鍵は他の装置によって取得されている。秘密鍵の所有を証明することは、Diffie-Hellman手順において同じ対称鍵を首尾よく導出することによって、または、両方の装置がDPPにおけるI-AuthおよびR-Authなどの同じ認証値を計算することによって、実行されることができる。

【００４７】

DPPプロトコルの場合、第1のメッセージは認証要求（Authentication Request）であり、応答メッセージはDPP認証応答（ DPP Authentication Response）である。レスポンダは、DPP認証要求メッセージが、正しく生成されたレスポンダ公開ブートストラップ鍵の暗号化ハッシュと、イニシエータの公開ブートストラップ鍵のコピーを有するかどうかをチェックする。レスポンダは、認証を継続できるかどうかを示すDPP認証応答メッセージを送信する。そうでない場合、例えば、DPP認証要求メッセージ中の暗号化されたナンスの復号化の試行が失敗するため、プロセスは中止される。DPP認証応答は、レスポンダ公開ブートストラップ鍵の暗号化ハッシュを含み、イニシエータ公開ブートストラップ鍵のハッシュを含む場合がある。同様に、イニシエータについては、エンローリーがOOB通信によってこの公開鍵を取得することができる。その後、イニシエータの公開ブートストラップ鍵を相互認証に使用できる。イニシエータの公開ブートストラップ鍵がない場合、イニシエータのみがエンローリー5を認証することができるが、その逆はできない。

【００４８】

認証応答メッセージが、レスポンダが認証要求メッセージを受け入れたことを示し、応答がイニシエータのセットアップによって課された基準を満たす場合、イニシエータは認証確認メッセージを発行する。認証応答および確認メッセージ内の認証値が関連する装置によって正しいことが判明した場合、プロトコルのこのパート、認証パートは成功し、プロセスはS5(Authenticated)に達し、設定を開始することができる。確認メッセージには、エンローリーがイニシエータでもある以前の設定試行の結果の指標も含まれる場合がある。

【００４９】

DPPプロトコルの場合、認証確認メッセージはDPP 認証確認(Authentication Confirm)メッセージである。

【００５０】

S6(Configuration)において、エンローリーは、エンローリーがどのタイプの設定を望むかに関する情報を有する設定要求メッセージを送信する。コミッショニング装置は、その要求を許可することができる場合、ネットワーク鍵等の、エンローリーが必要とする情報を含むメッセージを送信する。変形例では、設定要求は、以前の設定試行の結果の指標を含むこともできる。

【００５１】

DPPの場合、要求メッセージはDPP 設定要求（Configuration Request）であり、コミッショニング装置応答はDPP設定応答（ Configuration Response）メッセージである。コミッショニング装置からの応答（例えば、DPP設定応答）は、エンローリーが接続すべきネットワークのサービスセット識別子（SSID）を含むことができ、「接続情報パッケージ」として機能することができるデータオブジェクトを含むことができる。DPPの場合、これはDPPコネクタと呼ばれる。便宜上、この接続情報パッケージを「コネクタ」と呼ぶ。これは、本明細書に記載のシステムおよび方法をDPPに限定するものではなく、実際には、他のコミッショニングプロトコルがコネクタを使用することができることを理解されたい。コネクタは、少なくともDPPの場合、コミッショニング装置によって鍵（C-署名鍵）を使用してデジタル的に署名され、とりわけ、エンローリーの公開ネットワークアクセス鍵（NAK）を含む。そして、エンローリーは、継続するために、署名鍵を使用して、接続情報パッケージの内容を検証することができる。

【００５２】
コミッショニング装置は、認証の終了時にエンローリーによって送信されたメッセージ（DPPの場合はDPP認証応答メッセージ）からエンローリーの公開ネットワークアクセス鍵を取得することができ、この鍵はレスポンダの公開プロトコル鍵と呼ばれる。本出願では、プロトコル鍵という用語は、DPPプロトコルにおけるプロトコル鍵だけでなく、任意のコミッショニングプロトコルおよび/またはエンローリーのコミッショニングの成功に基づいてネットワークに接続するための任意のプロトコルにおいて使用される任意の他のエンローリー公開鍵に対しても使用されることに留意されたい。DPP認証が成功すると、レスポンダの公開プロトコル鍵は、プロトコルにおける新しい目的を示すために、エンローリーの公開ネットワークアクセス鍵に名前が変更される。DPP 設定応答メッセージは、設定の公開署名鍵も含む。同じコミッショニング装置9（例えば、DPPコンフィギュレータ）によって設定された他の装置は、それにより、それらが他の装置の公開ネットワークアクセス鍵を信頼できるかどうかをチェックすることができる。したがって、ネットワークへの接続を試みるエンローリーは、そのNAKを含むそのコネクタの署名を使用して、ネットワークまたはネットワーク内の他の装置により承認されることができる。DPP設定応答メッセージは、また、ネットワークのWi-Fiパスフレーズまたは事前共有鍵（PSK）を含むことができる。エンローリーは、コミッショニング装置（例えば、DPPコンフィギュレータ）にメッセージ（例えば、DPPのバージョンに応じて、DPP設定結果（Configuration Result））を送信して、設定を受け入れるか否かを知らせる。コミッショニング装置によってこのメッセージを受信しないことは、コミッショニング装置とエンローリーとの間にWi-Fi問題があったことをコミッショニング装置に示すことができる。そして、「設定されていると思われる」エンローリーは、そのコネクタをDPP設定AP 2に送信することができる。コネクタ署名が正しいことが検出され、AP 2に一致するコネクタ(同じコミッショニング装置によって署名された、同じネットワークのコネクタ)がある場合、AP 2は自身のコネクタをエンローリー（例えば、DPPエンローリー）に送信する。エンローリーとAP 2は、コネクタ中の互いのネットワークアクセス鍵と、Diffie-Hellman方式の独自の秘密ネットワークアクセス鍵に基づいて、対称鍵を計算できる。

【００５３】
S7(Connection)において、エンローリー4または5はネットワークへの接続を試みる。Wi-Fiの場合、エンローリーは、Wi-FiパスワードまたはWi-Fi事前共有鍵(Pre Shared key:PSK)を受信しており、エンローリーは[802.11]で規定されているように、4ウェイハンドシェイクを通じた通常の方法でAP 2との関連付けを試みる。接続試行が成功した場合、フローはS8(Complete)に進み、そこで完了する。

【００５４】
DPPの場合、実際の公開鍵、例えば、特定のP-256鍵は、それらがメッセージ内で転送されるとき、通常、公開鍵を含む構造内に公開鍵のタイプを含む。[RFC 5280]のセクション4.1で規定されているSubjectPublicKeyInfoと呼ばれるASN.1構造として表される楕円曲線公開鍵の例は、ASN.1の表記において次の通りである:

```
SEQUENCE {
   SEQUENCE {
      OBJECTIDENTIFIER 1.2.840.10045.2.1 (ecPublicKey)
      OBJECTIDENTIFIER 1.2.840.10045.3.1.7 (P-256)
   }
   BITSTRING 0x0343A6A094A9BC6C9B92CBA3164849F0DB0B91350270
ABE80DC554B1E6B3897F30 : 0 unused bit(s)
}
```

【００５５】
両方のOBJECTIDENTIFIERは共に公開鍵のタイプを定義する一方で、BITSTRINGはこの特定の公開鍵の値を含む。

【００５６】
現在、特にDPPにおいて、エンローリー装置の公開鍵に関する情報に関して、ブートストラップURIは、DPP R2におけるブートストラップ鍵のみを含む。このブートストラップ鍵は、ブートストラップURI中の最後の属性である。それは次の形式である:
"K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADM2206avxHJaHXgLMkq/24e0rsrfMP9K1Tm8gx+ovP0I=;",
ここで、":"と";"の間のシンボルは、[RFC 5280]からのbase64で符号化されたASN.1 SEQUENCE SubjectPublicKeyInfoである。上の例のブートストラップ鍵表現を復号し、きれいに表示すると、次のようになる:

```
SEQUENCE {
    SEQUENCE {
        OBJECTIDENTIFIER 1.2.840.10045.2.1 (ecPublicKey)
        OBJECTIDENTIFIER 1.2.840.10045.3.1.7 (P-256)
    }
    BITSTRING 0x03336db4e9abf11c96875e02cc92aff6e1ed2bb2b7cc3fd2b54e6f20c7ea2f3f42 : 0 unused bit(s)
}
```

【００５７】
DPPでは楕円曲線暗号［RFC 6090］がすべての非対称暗号、特にネットワークアクセス鍵（NAK）およびコミッショニング装置（コンフィギュレータ）署名鍵のために使用されるが、[DH]で説明されているようなqを法とする整数の乗法群のような他の形式の非対称暗号も可能である。ここで qは素数（[DH]では「素数qの要素を持つ有限体GF(q)」と呼ばれている）であり 、αはqを法とする原始根（[DH]では「GF(q)の固定原始要素」と呼ばれる）である。qおよびαの同じ値で生成されたすべての公開鍵は本明細書の目的のために、同じタイプの公開鍵と見なされる。同様に、同じ楕円曲線上の点であるすべての公開鍵も、同じタイプであると見なされる。異なる暗号化アルゴリズム、例えばECCおよびqを法とする整数の乗法群を使用する公開鍵は、異なるタイプの公開鍵と見なされる。同じ暗号化アルゴリズムを使用するが、定義パラメータのうちの少なくとも1つが異なる値を有する公開鍵は本明細書の目的では異なるタイプの公開鍵と見なされる。例えば、定義パラメータはqを法とする整数の乗法群に対してqおよびαであり、楕円曲線はECCアルゴリズムに対する定義パラメータである。上記の例に示されているOBJECTIDENTIFIERを使用することに加えて、楕円曲線の表示は、IETF RFC 2409 [RFC 2409]および[IKE]の"group Description"属性としてIANAによって維持されているレジストリを使用して、[DPP]の8.1.1.12節"Finite Cyclic group attribute"に規定されているFinite Cyclic group属性を含む要素グループを使用して、与えられ、または取得されることもできる。例えば、曲線P-256の［IKE］におけるIANA表現は1300である。例えば、DPP再設定アナウンス (Reconfiguration Announcement)メッセージにおいて、要素グループは、エンローリーのコネクタにおけるネットワークアクセス鍵の公開鍵のタイプを示す。

【００５８】
上記の段落は、DPPにおける状況を説明していることを理解されたい。しかしながら、他のコミッショニングプロトコルが同様の態様および類似の要素（ネットワークアクセス鍵など）を有し得る。

【００５９】
本開示の目的のために、公開鍵のタイプを選択、比較、提供、取得、受信などすることは、公開鍵とその公開鍵のタイプを含む構造体、またはデータのブロブを選択、比較、提供、取得、受信などするときにも達成されることに留意されたい。そのような構造またはデータのブロブの例を本明細書に示す。

【００６０】
現在、特に現在のバージョンのDPPでは、ブートストラップURIはブートストラップ

鍵を１つのみを含むことができる。このブートストラップ鍵は、ブートストラップURIの最後の属性である。それは次の形式である:
"K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADM2206avxHJaHXgLMkq/24e0rsrfMP9K1Tm8gx+ovP0I=;",
ここで、":"と";"の間のシンボルは、[RFC 5280]からのbase64で符号化されたASN.1 SEQUENCE SubjectPublicKeyInfoである。上の例のブートストラップ鍵表現を復号し、きれいに表示すると、次のようになる:

```
SEQUENCE {
   SEQUENCE {
     OBJECTIDENTIFIER 1.2.840.10045.2.1 (ecPublicKey)
     OBJECTIDENTIFIER 1.2.840.10045.3.1.7 (P-256)
}
BITSTRING 0x03336db4e9abf11c96875e02cc92aff6e1ed2bb2b7cc3fd2b54e6f20c7ea2f3f42 : 0 unused bit(s)
}
```

【００６１】
本発明者はこれが、設定プロトコルの効率的な動作に対する欠点を有することを認識した。
【００６２】
プライバシーとサイバー攻撃からの保護の問題に多くの注意が払われている。このような攻撃に対する防御の主要な部分は暗号の強度であり、暗号の強度を高める傾向がある。したがって、エンローリーからの初期情報（例えば、ブートストラップURIおよび初期の交換）から、コミッショニング装置が使用することを「望む」（すなわち、プログラムされているか、または有効にされている）強度よりも低い強度の暗号を使用するようにエンローリー装置が構成されていることをコミッショニング装置が発見する状況が生じる場合がある。実際、多くの古い潜在的なエンローリー装置が、古くて脆弱な暗号を有しており、いわばサプライチェーンに残されているので、そのような事態が発生する可能性が高く、この問題は、理解されているよりも差し迫ったものであるかもしれない。
【００６３】
さらに、本発明者は、追加の問題があることに気付いた。設定プロトコルは、設定プロトコルの後のフェイズ及びエンローリーの無線ネットワークへの接続のために、コミッショニング装置がより高い強度の暗号化に変更することを可能にし、実際にDPPはそれを規定している。DPPの場合、S6aにおいて、DPPコンフィギュレータ（すなわち、コミッショニング装置）は特定の（おそらく）より強い曲線上の新しい公開プロトコル鍵(NEWK REQ)を要求するために、DPP設定応答メッセージを使用することができる。S6bにおいて、エンローリーが提案された曲線を使用することができる場合、エンローリーは新しい公開プロトコル鍵を含むメッセージ（例えば、DPPの場合、DPP設定要求）で応答する。そしてフローは、上述のようにS7に続く。しかしながら、エンローリーが準拠することができない場合、エンローリーは応答に失敗し、最終的に、設定プロセスはタイムアウトの後に終了し、S6c（FAIL）において設定失敗となる。コミッショニング装置は、いわばハングアップされたままとなり、最終的に、設定を完了することができないことをユーザに知らせることになる。ユーザに残された唯一のオプションは、プロシージャを再開することである。このイベントの流れは時間を浪費する。さらに好ましくないことに、コミッショニング装置は「ブラインド」で再スタートしなければならず、先ほど要求したのとは異なるタイプの鍵を要求する新しい鍵の要求を試したとしても、それが成功するかどうかは前もってわからない。要するに、唯一のオプションは試行錯誤であり、すなわち、上手くいくまで設定手順を繰り返し実行することである。
【００６４】
同様の状況は、コミッショニング装置が、エンローリーによって提供されるブートストラップ鍵の鍵タイプ以外のタイプ、例えばよりセキュアなタイプの秘密鍵を使用すること

を望むときに生じ得る。コミッショニング装置は設定応答を送信することができ、その情報（の一部）、例えばDPPコネクタは、エンローリーによって提供されるブートストラップ鍵の鍵タイプとは異なるタイプの秘密鍵で署名される。しかしながら、エンローリーが対応することができない場合、エンローリーは応答に失敗し、最終的に、設定プロセスはステップ6において終了し、コミッショニング装置は以前のように、ハングアップしたままとなる。

【００６５】

実施形態によれば、ブートストラップURIは、追加の楕円曲線が後方互換性のある様式で追加され得るように拡張されることができる。これは、DPPブートストラップURIにおいて「K」によって示される既存の属性に全て類似した、既存の前のどこかに現れる一連の1つまたは複数の属性により行われることができるが、ここでは別の未使用の文字によって示される。

【００６６】

いくつかの変形例が可能である。

【００６７】

1つの変形例では、1つのリストに、ブートストラップURIにおけるブートストラップ鍵のタイプ以外の、コミッショニング装置が署名鍵として使用するため、およびプロトコル鍵（ネットワークアクセス鍵）として使用するために、ブートストラップURIが属する装置がサポートするすべてのタイプの鍵（すなわち、DPPの場合は楕円曲線）の指標が含まれる。

【００６８】

別の変形例では、ブートストラップURI内のブートストラップ鍵のタイプ以外の、コミッショニング装置（コンフィギュレータ）署名およびネットワークアクセス鍵としての使用のためにブートストラップURIが属する装置サポートするすべての鍵タイプ（たとえば、楕円曲線）の指標が、2つの別個のリスト中にある。

【００６９】

ASN.1 を用いると、符号化は

```
  SEQUENCE {
      OBJECTIDENTIFIER 1.2.840.10045.2.1 (ecPublicKey)
      OBJECTIDENTIFIER 1.3.132.0.34 (P-384)
   }
```

}であり、これは、BASE64符号化において、MBAGByqGSM49AgEGBSuBBAAiである。

【００７０】

署名鍵とプロトコル鍵/ネットワークアクセス鍵の両方に対するP-384のサポートは以下のように示されることができ、ここで、「B」は、「両方」を意味することができる:

B:MBAGByqGSM49AgEGBSuBBAAi;

そして、DPPの場合、ブートストラップURIは次のようになる:

DPP:B:MBAGByqGSM49AgEGBSuBBAAi;K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADM2206avxHJaHXgLMkq/24e0rsrfMP9K1Tm8gx+ovP0I=;;

【００７１】

他の情報、例えば、エンローリーがリスンするチャネルもブートストラップURIに追加することができる。

【００７２】

上記のASN.1表記は非常に長い。これは、ブートストラップURIを含むQRコードのサイズを、製品上にQRコードを印刷するのに十分なスペースが残っていない程度まで増大させる可能性があるという欠点を有する。有利な方法は、上述のIANAが維持するレジストリにおいて符号化を使用することであり得る。そして、P-521 NAKについてのサポートを示すことから独立してP-384署名鍵についてのサポートを示すことは、以下のように行うことができ、ここで、「S」は署名鍵タイプを示すことができ、「N」はNAK鍵タ

イプを示すことができる:
DPP:S:1400;N:1500;K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADM2206avxHJaHXgLMkq/24e0rsrfMP9K1Tm8gx+ovP0I=;;
署名およびNAK使用の両方のための2つの曲線のサポートは、以下のように行うことができる:
DPP:B:14001500;K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADM2206avxHJaHXgLMkq/24e0rsrfMP9K1Tm8gx+ovP0I=;;
または
DPP:B:1400;B:1500;K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADM2206avxHJaHXgLMkq/24e0rsrfMP9K1Tm8gx+ovP0I=;;

【００７３】

図3は、一実施形態による、暗号化をアップグレードする（すなわち、暗号強度を高める）ためのプロトコルのフローを表す。S1、S2、S3、S4、S5、S7、S7aおよびS8におけるプロセスは図2を参照して説明した通りであり、したがって、これ以上説明しない。図3のプロセスは、コミッショニングまたは設定プロトコルと呼ばれる場合もある。

【００７４】

S20において、コミッショニング装置は、例えばブートストラップURIにおいて、S2においてエンローリーから受信した情報を検査する。コミッショニング装置は、ブートストラップのタイプの鍵（例えば、曲線）を、コネクタ署名およびネットワークアクセスのためのNAKのためにも使用することを「望む」場合、プロセスをS3に進める。

【００７５】

しかしながら、コミッショニング装置は、ブートストラップURIにおけるブートストラップ鍵のものとは別のタイプの鍵（例えば、曲線）を後の段階のプロトコル（例えば、署名DPPコネクタ、またはNAKなどのプロトコル鍵）のために使用することを望む場合、エンローリーが署名のためにどの曲線をサポートするかについての情報を探すことを試みる。上記の例では、これは、"B:"、"N:"、または"S:" の後、かつ、次のセミコロンの前の情報になる。コミッショニング装置がそれが受け入れることができる鍵のタイプ（例えば、曲線）を見つけた場合、プロセスはS3に進む。そして、コミッショニング装置は、例えば、再設定が必要とされる場合など、後で使用するためにブートストラップURIの記録を保持することができる。

【００７６】

しかしながら、コミッショニング装置が使用することを受け入れることができる曲線（すなわち、鍵のタイプ）をエンローリーがサポートしない場合、コミッショニング装置はこのエンローリーを設定するプロセスを停止し、プロセスは、S20aにおいて中止される。そして、コミッショニング装置は、許容可能な鍵のタイプをエンローリーがサポートしていないようであるという事実をユーザに通知することができる。

【００７７】

S61において、コミッショニング装置は、ブートストラップURI内の情報から1つまたは複数の鍵タイプ（例えば、曲線）を選択し、選択されたタイプのいずれかの公開プロトコル鍵を提供するようにエンローリーに要求することができる。そして、エンローリーは、S62において、要求された（1つまたは複数の）タイプの（1つの）新しいプロトコル鍵（たとえば、NAK）で応答することができる。公開鍵の2つ以上のタイプを許可する要求が提示されたときに、最も強いタイプの鍵を使用するようにエンローリーが設定されることが有利であり得る。そして、コミッショニング装置は、エンローリーがネットワークに接続するときに許容可能なレベルの暗号化を使用していることを知る。コミッショニング装置は、理論的には、エンローリーがサポートするリストから選択を行っているので、エンローリーが接続情報パッケージを検証するために署名鍵を使用することができずに応答に失敗する（プロセスをハングアップさせ、次いで中止させる）リスクは大幅に低減される。これは、署名および公開プロトコル鍵のための適切な鍵タイプをコミッショニング装置が「推測」しようとする無駄な試行錯誤が排除され、接続できないエンローリーは早

期に排除されることにより、コミッショニングプロセスの効率の大幅な改善を提供する。

【００７８】

コミッショニング装置が、新しい鍵タイプのオプションを含む要求を行うことが有利であり得る。例えば、コミッショニング装置は,多くのタイプのエンローリーに対処しなければならない場合があり、そのうちのいくつかは、所与の状況において厳密に必要とされるよりもエンローリーにとってより負担となる暗号化のレベルに対するサポートを通知する場合がある。選択の一部をエンローリーに任せることで、プロセスにいくらかの柔軟性を導入することができる。要求により、エンローリーが新しい（アップグレードされた）公開プロトコル鍵にどの鍵タイプを使用するかを選択することが可能になり、エンローリーが最も強力な暗号化を提供するオプションを選択することにより、ネットワークがこれから恩恵を受けることが可能になる。

【００７９】

S60において、ブートストラップURI内の情報からの鍵タイプ（例えば曲線）の公開プロトコル鍵を提供するようにS61でエンローリーに要求することに加えてまたはその代わりとして、コミッショニング装置は、ブートストラップURI内の情報から、ブートストラップURI内の鍵タイプ以外の鍵タイプ（例えば曲線）を選択して、接続情報パケット（例えば、DPPコネクタ）に署名することができる。コミッショニング装置は、サポートされている鍵タイプで接続情報パケット（例えば、DPPコネクタ）に署名できることを知っている。そして、エンローリーは、接続情報パッケージの署名を使用して、ネットワークへの接続を試みるときに、ネットワークから受諾を得ることができる。コミッショニング装置が新しい公開プロトコル鍵も要求した場合、接続情報パケットに署名するための鍵のタイプは、要求された公開プロトコル鍵のうちの1つと同じであっても、異なっていてもよい。エンローリーがサポートするリストからコミッショニング装置が選択を行っているので、理論的には、エンローリーが応答しない（プロセスがハングアップし、中断する）リスクは大幅に低減される。これは、署名および公開プロトコル鍵のための適切な鍵タイプをコミッショニング装置が「推測」しようとする無駄な試行錯誤が排除され、接続できないエンローリーは早期に排除されることにより、コミッショニングプロセスの効率の大幅な改善を提供する。

【００８０】

エンローリーは、ネットワークに接続されている場合でも、再設定を必要とする場合がある。例えば、この動作は、ネットワークの暗号セキュリティをアップグレードするために実行されることができ、したがって、鍵タイプの変更を必要とする。別の状況は、S7aによって表されるように、エンローリーがネットワークへの接続を試み、失敗した場合である。本発明者は、どの鍵タイプ（例えば曲線）が当該エンローリーによってサポートされているかをコミッショニング装置が知らないとき、そのような再設定が同じ問題を被る可能性があることを認識した。

【００８１】

一実施形態によれば、エンローリーの再設定が実行されることができる。有利な実施態様では、コミッショニング装置は、各エンローリーを設定したNAKと組み合わせて、設定したすべてのエンローリーのブートストラップURIを記憶する。S9において、エンローリーは再設定を必要とし、DPP再設定通知（DPP Reconfiguration Announcement）メッセージのような要求メッセージの送信を開始する。DPP再設定通知メッセージ内のその署名鍵のハッシュを認識するDPP コンフィギュレータなどのコミッショニング装置は、DPP 再設定認証要求（Reconfiguration Authentication Request）メッセージでエンローリーに応答する。DPPの場合、コミッショニング装置は、エンローリーからDPP再設定認証応答メッセージを受信したときに、DPP再設定認証プロトコル中にエンローリーのIDを学習することができ、このメッセージは、エンローリーコネクタおよびエンローリーNAKを含む。このエンローリーのIDの確立は、以下のように行われ得る：

【００８２】

S10において、エンローリーは、（DPP再設定認証応答メッセージのような）応答で返信し、その（エンローリー）コネクタを含める。コミッショニング装置は、受信された(DPP再設定認証応答)メッセージ内のエンローリーコネクタ内のNAKを見つける。そして、コミッショニング装置は、以前にエンローリーを設定するためにコネクタにおいて使用したNAKのリストにおいて、このNAKを見つけようと試みることができる。そのリストにおいてNAKを見つけると、そのNAKを使用してコネクタ で設定されたときにエンローリーが使用したブートストラップURIを見つける。そしてS63において、コミッショニング装置は、上述のように、このエンローリーによってサポートされる鍵タイプ（例えば曲線）を評価することができる。コミッショニング装置は、S63aにおいて再設定手順を中止するか、または、S63bにおいて、コミッショニング装置が使用することを望む曲線をサポートするのでこのエンローリーを再設定することを進めるかのいずれかを決定することができる。いくつかのコミッショニングプロトコルでは、S63bは、S60、S61、S62およびS7を含むものとして示されることができる。再設定が成功した後、プロセスは、前述のようにS8で終了する。

【００８３】

したがって、設定プロトコルの実行によって無線ネットワークにおける通信のためにエンローリー装置を設定する本方法は、以下のように説明され得る。本方法は、コミッショニング装置およびエンローリー装置によって実行されるように構成され、コミッショニング装置およびエンローリー装置は、無線通信プロトコルを使用して通信し、設定プロトコルに参加するように構成される。設定プロトコルは、以下の要素を含む。エンローリー装置が、帯域外（OOB）通信を使用して、第1の公開鍵と、第2の公開鍵のタイプの少なくとも1つの指標とをコミッショニング装置に提供する。コミッショニング装置は、第2の公開鍵のタイプの少なくとも1つの指標が第1の公開鍵のタイプとは異なる鍵のタイプを示すと決定した場合、以下のことを行う。

【００８４】

コミッショニング装置は、少なくとも1つの指標から少なくとも1つの鍵のタイプの選択を行い（この選択におけるすべてのタイプは、第1の公開鍵のタイプとは異なる）、無線通信プロトコルを使用して第1のメッセージを送信し、第1のメッセージは、前記選択における任意の鍵タイプに対応するタイプの第2の公開鍵を要求し、第2の鍵は、エンローリー装置がワイヤレスネットワークに接続することを可能にするためにコミッショニング装置によって使用される。

【００８５】

追加的にまたは代替的に、コミッショニング装置は、選択における任意の鍵タイプに対応するタイプの第3の鍵を使用してデータオブジェクトに署名し、データオブジェクトは、エンローリーに送信されるように構成され、エンローリー装置によって、ワイヤレスネットワークへの接続を試みるために使用されるように構成される。

【００８６】

エンローリー装置は、要求された場合、第1のメッセージにおいて要求された鍵のタイプの第2の公開鍵を含む第2のメッセージを送信する。そして、エンローリーおよびコミッショニング装置は、エンローリーの公開鍵およびコミッショニング装置の署名鍵のうちの1つまたは複数を使用することによって、選択に対応するタイプの1つまたは複数の鍵を使用して設定プロトコルを完了する。

【００８７】

第2の公開鍵のタイプの指標が第1の公開鍵のタイプと同じ鍵のタイプを示す場合、この指標は、第2の公開鍵のタイプの指標が第1の公開鍵のタイプとは異なる鍵のタイプを示す場合に使用されるデータ要素よりも小さいデータ要素を使用することができる。

【００８８】

このようにして、符号化されるデータの量が低減され得る。誤り訂正機構のオーバーヘッドを考慮すると、節約はさらに大きくなることが明らかになる。これは、OOB通信がQRコードを使用するときに特に有利である。QRコードでは空間が限られており、符号化

されるべきデータが増加すると、コードによって必要とされる面積も増加するだろう。これにより、製品またはパッケージに大きくなったQRコードをフィットさせることが困難になる場合がある。

【００８９】

したがって、本方法は、第2の公開鍵のタイプの少なくとも1つの指標が第1の公開鍵のタイプと同じタイプを示す場合にのみ、設定プロトコルの完了前に、設定プロトコルの実行を、コミッショニング装置によって、終了することを含むことができる。本方法は、第2の公開鍵のタイプの少なくとも1つの指標が、コミッショニング装置が使用することができる公開鍵のタイプを含まない場合に、設定プロトコルの実行を、コミッショニング装置によって、設定プロトコルの完了前に終了することを含むことができる。

【００９０】

したがって、コミッショニング装置は、エンローリーがサポートすることができる暗号化の最高強度を決定することができる。そのような暗号化の強度は、問題のネットワークにとって不十分であることが生じる可能性がある。OOB通信フェイズにおいて、またはエンローリーが提案された新しい公開鍵で応答したときに、この最高暗号強度を決定することによって、コミッショニング装置は、早期に失敗することによって（ユーザの側での）手間を省くことができる。これをユーザに報告することもできる。

【００９１】

一実施形態によるエンローリーは、無線通信プロトコルを使用して通信するように構成され、無線ネットワークにおける通信のためにコミッショニング装置によって設定されるように構成される。エンローリー装置は、以下のように構成される:

- エンローリー装置を設定するように構成された設定プロトコルに参加する;
- 帯域外（OOB）通信を使用して、設定プロトコルの第1のフェイズで使用するための第1の公開鍵と、第2の公開鍵のタイプの少なくとも1つの指標とを提供する;
- 無線通信プロトコルを使用して、コミッショニング装置と共に、第1の公開鍵と、少なくとも1つの指標によって示されるタイプの鍵とを使用してコミッショニングプロトコルに参加する;
- 設定された結果としてネットワークへの接続を試行する。

【００９２】

このように構成されたエンローリー装置は、OOB通信フェイズにおいて、すなわち、設定プロセスの開始付近において、それがその公開ブートストラップ鍵のレベルまたは強度を超えてサポートすることができる暗号化のレベルまたは強度を示すことができる。これは、次に、このファシリティを使用するように構成されたコミッショニング装置が、a）エンローリーが十分な暗号化の強度をサポートすることができることを決定し、b）エンローリーがサポートすることができる暗号化の強度を（1つまたは複数のタイプの鍵を選択する形で）選択することを可能にする。

【００９３】

一実施形態によれば、エンローリー装置は、少なくとも1つの指標に対応するタイプの鍵を使用してコミッショニング装置によって署名されているデータオブジェクトを検証するように構成される。

【００９４】

エンローリーはトランシーバを有することができ、このトランシーバを介して、無線通信プロトコルを使用して、コミッショニング装置からの第1のメッセージを受信し（第1のメッセージは第2の公開鍵の1つまたは複数のタイプを示す要求を含み、第2の公開鍵のタイプは第1の公開鍵のタイプとは異なる）、トランシーバを介して、無線通信プロトコルを使用して、コミッショナー装置へ第2のメッセージを送信するように構成される。この第2のメッセージは、メッセージ内で要求されたタイプの第2の公開鍵を含むことができる。

【００９５】

したがって、エンローリーは、初期設定の鍵、すなわち、エンローリーの公開ブートス

トラップ鍵よりも高い強度の暗号化を有する鍵を提供し、使用することができる。

【００９６】

一実施形態では、エンローリー装置は、要求が公開鍵の2つ以上のタイプを示す場合に、最大の暗号強度を有するタイプの第2の公開鍵を提供するように構成される。コミッショニング装置が、新しい鍵タイプの選択肢を含む要求を行うことが有利である。例えば、コミッショニング装置は、多くのタイプのエンローリーに対処しなければならない場合があり、そのうちのいくつかは、厳密に必要とされるよりもエンローリーにとってより負担の大きい暗号化のレベルに対するサポートを通知する場合がある。選択の一部をエンローリーに任せることで、プロセスにいくらかの柔軟性を導入することができる。要求により、エンローリーが新しい（アップグレードされた）公開鍵にどの鍵タイプを使用するかを選択することが可能になり、エンローリーが最も強力な暗号化を提供するオプションを選択することにより、ネットワークがこれから恩恵を受けることが可能になる。

【００９７】

一実施形態によるコミッショニング装置は、無線ネットワークにおける通信のためにエンローリー装置を設定するように構成される。

- 装置は、無線通信プロトコルに従って送受信するように構成されたトランシーバを有し、装置は以下のように構成される：
- 設定プロトコルに参加し；
- 第1の公開鍵と、設定プロトコルの一部として使用されるべき公開鍵の第2のタイプの少なくとも1つの指標とを、帯域外（ＯＯＢ）通信を介して、エンローリー装置から取得し；
- 前記少なくとも1つの指標が、第1の公開鍵のタイプとは異なる鍵のタイプを示す場合、前記少なくとも1つの指標に基づいて鍵の少なくとも1つのタイプを選択し（この選択における全てのタイプは第1の公開鍵のタイプとは異なる）、
- 第1のメッセージを、トランシーバおよび無線通信プロトコルを使用して、エンローリー装置に送信し、エンローリー装置は、前記選択における任意の鍵タイプに対応する鍵のタイプの第2の公開鍵を要求し；および/または、
- 前記選択における任意の鍵タイプに対応するタイプの第3の鍵を使用して、データオブジェクトに署名し、トランシーバを介して、無線通信プロトコルを使用して、署名されたデータオブジェクトをエンローリーに送信する（データオブジェクトは、無線ネットワークへの接続を試行するためにエンローリー装置によって使用されるように構成される）。

【００９８】

したがって、コミッショニング装置は、エンローリーブートストラップ鍵のタイプ以外のどのタイプの鍵をエンローリーがサポートすることができるかを決定することができる。その情報を用いて、それは、エンローリーから新しい公開鍵を要求することができる。追加的にまたは代替として、（エンローリーブートストラップ鍵のタイプとは異なる）どの鍵タイプを使用して、接続情報パケットを含むデータオブジェクト（例えば、ＤＰＰコネクタ）に署名することができるかを決定することができる。コミッショニング装置は、使用できるものを決定することによって、試行錯誤に頼る必要なく、暗号化レベルを変更することができる。

【００９９】

装置は、指標が第1の公開鍵の鍵タイプと同じ鍵のタイプのみを示す場合、エンローリー装置の設定を完了する前に、終了するように構成されることができる。追加的にまたは代替として、装置は、少なくとも1つの指標が装置が使用可能にされている鍵のタイプを示さない場合、エンローリー装置の設定を完了する前に終了するように構成されることができる。

【０１００】

エンローリー装置内のプロセッサ上で動作するとき、エンローリー装置に本明細書で説明する方法を実行させるコンピュータプログラム、およびコミッショニング装置内のプロセッサ上で動作するとき、コミッショニング装置に本明細書で説明する方法を実行させるコンピュータプログラムも提供される。

【０１０１】
図４は、上述のS２のブートストラップ段階で使用され得るQRコードを表す。国際標準化機構（ISO）は、標準化されたシンボル構造を定義する "Information technology - Automatic identification and data capture techniques - QR code bar code symbology specification"という名称のQRコードのための規格ISO/IEC18004:２０１５を確立した。異なる情報容量を持つ４０個のバージョンがある。QRコード１００は、ファインダパターン１０１、データ及び誤り訂正領域１０２などの様々な構成要素領域を有する。データは、８ビットコードワードに分割されるビットストリームとして符号化される。印刷されたコードに記憶される符号化データの実際の量をさらに増加させる誤り訂正機構が使用される。QRコード内の情報量を増加させると、印刷されたQRコードのサイズが著しく増加する可能性があり、これは装置またはパッケージ上の利用可能なスペースにQRコードを実際にフィットさせる際に問題を生じさせる可能性がある。したがって、空間を節約することには利点がある。一実施形態では、エンローリーがその公開ブートストラップ鍵の鍵タイプ（例えば、曲線）のみをサポートする場合、署名および/または公開プロトコル鍵（すなわち、NAK）のためにサポートされる鍵タイプの指標が削除される。したがって
DPP:B:１３００;K:MDkwEwYHKoZIzj０CAQYIKoZIzj０DAQcDIgADM２２０６avxHJaHXgLMkq/２４e０rsrfMP９K１Tm８gx+ovP０I=;;
は、
DPP:B:;K:MDkwEwYHKoZIzj０CAQYIKoZIzj０DAQcDIgADM２２０６avxHJaHXgLMkq/２４e０rsrfMP９K１Tm８gx+ovP０I=;;
となり、
DPP:S:１４００;N:１５００;K:MDkwEwYHKoZIzj０CAQYIKoZIzj０DAQcDIgADM２２０６avxHJaHXgLMkq/２４e０rsrfMP９K１Tm８gx+ovP０I=;;
は
DPP:S:;K:MDkwEwYHKoZIzj０CAQYIKoZIzj０DAQcDIgADM２２０６avxHJaHXgLMkq/２４e０rsrfMP９K１Tm８gx+ovP０I=;;
となる。
【０１０２】
これは、（署名鍵およびプロトコル鍵の一方または両方に対する指標が関係しているかどうかに応じて）４つまたは８つのオクテットを節約し、したがって、QRコードにおける潜在的な面積減少またはそれらのオクテットが別の目的のために使用されることを可能にする。この実施形態によるコミッショニング装置は、署名鍵および/またはNAKがURI内の公開ブートストラップ鍵と同じタイプでなければならないというフラグとして「欠落した」指標を読み取る。
【０１０３】
オクテットを節約する別の方法は、いくつかの曲線の１つまたは複数のセットのための特別な指標を使用することであり、そのセットは、例えば、インターネットドラフト、RFC、またはIEEE、Wi-Fiアライアンス、NIST、ETSI、IECなどの標準化団体によって公開された規格において指定される。一例として、文字Aが、全てのNIST曲線P-２５６、P-３８４及びP-５２１を、Brainpool曲線BP-２５６、BP-３８４及びBP-５１２と共に示すように規定されることができる。この例を使用すると、URIは次のようになる ：
DPP:S:A;K:MDkwEwYHKoZIzj０CAQYIKoZIzj０DAQcDIgADM２２０６avxHJaHXgLMkq/２４e０rsrfMP９K１Tm８gx+ovP０I=;;
これは、装置が、すべてのNIST曲線P-２５６P-３８、およびP-５２１ をBrainpool曲線BP-２５６、BP-３８４、およびBP-５１２ とともに、署名およびNAKのためにサポートしていることを示す。
【０１０４】
図５aはコンピュータプログラム１０２０を含む書き込み可能部分１０１０を有するコンピュータ可読媒体１０００を示し、コンピュータプログラム１０２０は図１を参照して説明したよ

うに、プロセッサシステムに上記の方法およびプロセスのうちの1-3つ以上を実行させるための命令を含む。コンピュータプログラム1020は、物理マークとして、またはコンピュータ可読媒体1000の磁気化によって、コンピュータ可読媒体1000上に実現されてもよい。しかしながら、任意の他の適切な実施形態も考えられる。さらに、コンピュータ可読媒体1000は、ここでは光ディスクとして示されているが、コンピュータ可読媒体1000はハードディスク、固体メモリ、フラッシュメモリなどの任意の適切なコンピュータ可読媒体であってもよく、記録不可能または記録可能であってもよいことが理解されるのであろう。代替として、コンピュータ可読媒体は、クラウドストレージなどの遠隔サーバストレージ1200上に配置され得る。コンピュータプログラム1020は、プロセッサシステムに上記方法を実行させるための命令を含む。

【０１０５】

図5bは、図1～図3を参照して説明した装置または方法の一実施形態によるプロセッサシステム1100の概略図を示す。プロセッサシステムは回路1110、例えば、1つまたは複数の集積回路を備えることができる。回路1110のアーキテクチャを図に概略的に示す。回路1110は、一実施形態による方法を実行し、かつ/またはそのモジュールもしくはユニットを実装するためにコンピュータプログラムコンポーネントを実行するための処理ユニット1120、例えばCPUを備える。回路1110は、プログラムコード、データなどを記憶するためのメモリ1122を備える。メモリ1122の一部は、読み出し専用であってもよい。回路1110は、通信要素1126、例えば、アンテナ、トランシーバ、コネクタまたはその両方などを含んでもよい。回路1110は、方法で定義された処理の一部または全部を実行するための専用集積回路1124を含んでもよい。プロセッサ1120、メモリ1122、専用IC 1124、および通信要素1126は、相互接続1130、たとえばバスを介して互いに接続することができる。プロセッサシステム1110は、それぞれコネクタおよび/またはアンテナを使用して、有線および/または無線通信のために構成され得る。

【０１０６】

コミッショニング装置およびエンローリー装置の両方は適合されたメッセージを処理することができなければならないので、それらはメッセージを正しく解析するように適宜プログラムされなければならない。これにより、設定装置の複雑さが増し、実行時間が長くなることを理解されたい。また、より複雑なファームウェアとより大きな不揮発性メモリが必要になるという点で、エンローリー側での複雑さが増加する。このような装置には価格の大幅な下落圧力があり、明らかにわずかな追加であっても正当化が要求されることに留意すべきである。さらに、多くのそのような装置はバッテリ駆動であり、情報を取得すること、より複雑なメッセージを構成すること、およびそれらのより複雑でより長いメッセージを送信することなどの、如何なる余分なエネルギー消費も、特にバッテリが小さく、長期間持続することが意図される場合、積極的に推奨されない。最後に、プロトコルを変更することは、レガシー装置の処理を可能にするために他の修正を伴うことが多い。

【０１０７】

本実施形態の態様はコンピュータによって実行されることができるコンピュータ可読記憶装置上に記憶されたコンピュータプログラム命令の集合であってもよく、コンピュータプログラム製品において実施されてもよい。命令は、スクリプト、解釈可能プログラム、ダイナミックリンクライブラリ(DLL)またはJavaクラスを含む(但しこれらに限定されない)、任意の解釈可能または実行可能コードメカニズムあってもよい。命令は、完全な実行可能プログラム、部分的な実行可能プログラム、既存のプログラムに対する修正(例えば、更新)または既存のプログラムに対する拡張(例えば、プラグイン)として提供されることができる。さらに、本発明の処理の一部は、複数のコンピュータまたはプロセッサに分散させることができる。

【０１０８】

コンピュータプログラム命令を記憶するのに適した記憶媒体には、EPROM、EEPROMおよびフラッシュメモリ装置、内部および外付けハードディスクドライブなどの磁気ディスク、リムーバブルディスクおよびCD-ROMディスクを含むが、これらに限定されな

い、すべての形態の不揮発性メモリが含まれる。コンピュータプログラム製品はこのような記憶媒体上に配布されてもよいし、HTTP、FTP、電子メールを介して、またはインターネットのようなネットワークに接続されたサーバを介したダウンロードのために、提供されてもよい。

【０１０９】

参考文献としては、以下のものを用いることができる:

[802.11] IEEE Computer Society, "IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," (IEEE Std. 802.11-2016), December 2016

[DH] Diffie, W.; Hellman, M. (1976), "New directions in cryptography", IEEE Transactions on Information Theory, 22 (6): 644-654

[DPP] Device Provisioning Protocol - Technical Specification - Version 1.0, Wi-Fi Alliance, 2018, https://www.wi-fi.org/file-member/device-provisioning-protocol-specification.

[FIPS180-4] FIPS180-4, "Secure Hash Standard", United States of America, National Institute of Standards and Technology, Federal Information Processing Standard (FIPS) 180-4

[IKE] Internet Key Exchange (IKE) Attributes, Group Description (Value 4), https://www.iana.org/assignments/ipsec-registry/ipsec-registry.xhtml#ipsec-registry-10

[RFC 2409] RFC 2409, The Internet Key Exchange, November 1998, https://datatracker.ietf.org/doc/rfc2409/.

[RFC 5280] RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://datatracker.ietf.org/doc/rfc5280/

[RFC 5297] Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES), October 2008, https://datatracker.ietf.org/doc/rfc5297/

[RFC 6090] RFC 6090, Fundamental Elliptic Curve Cryptography Algorithms, February 2011 https://datatracker.ietf.org/doc/rfc6090/

【図面】

【図１】

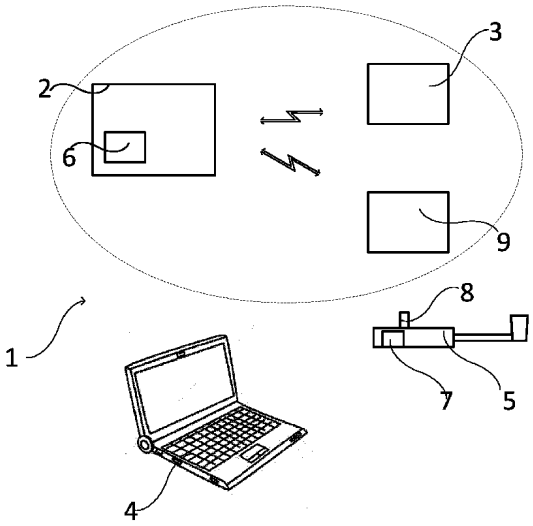

Fig 1

【図２】

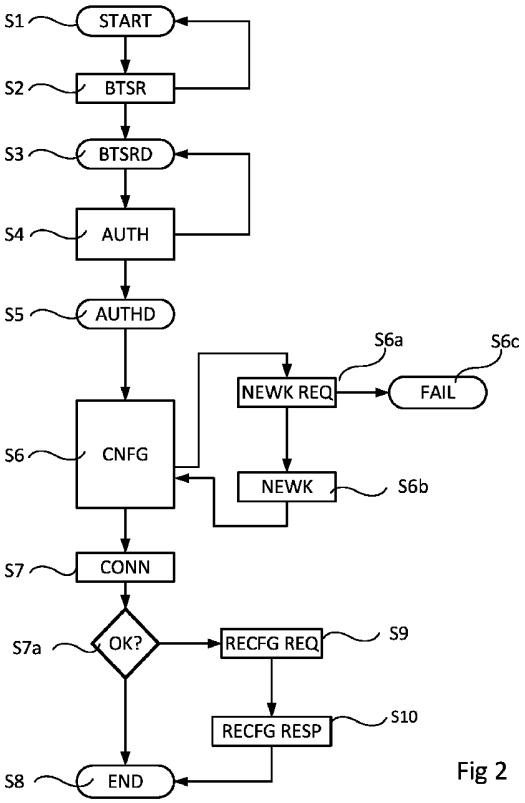

Fig 2

【図３】

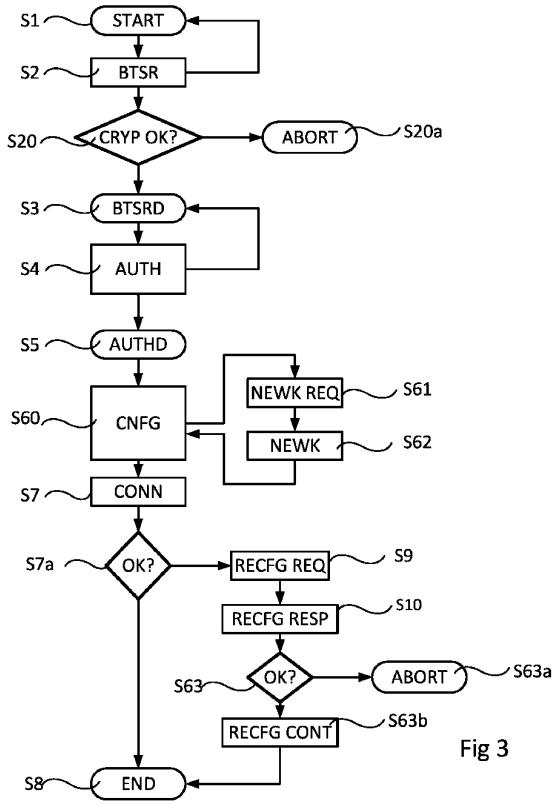

Fig 3

【図４】

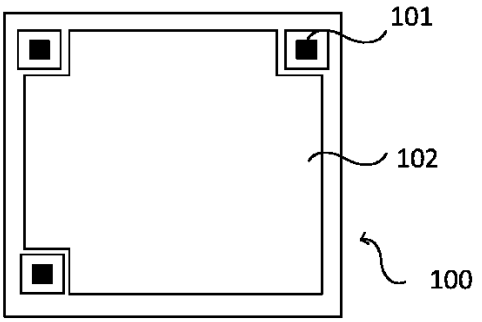

Fig 4

【図５ａ】

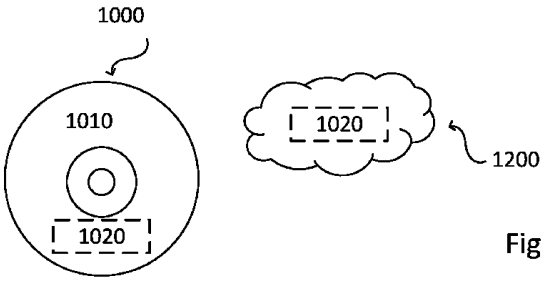

Fig 5a

【図５ｂ】

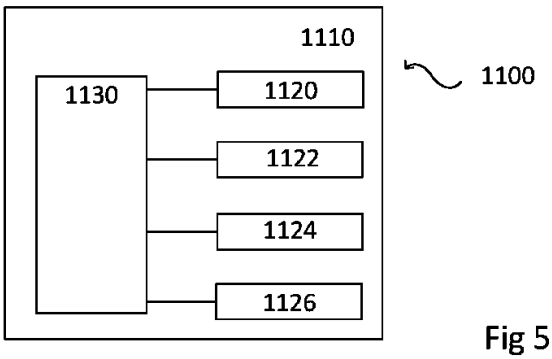

Fig 5b

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2023/052749

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/50
ADD. H04W12/069 H04W12/67 H04W12/77 H04L9/40 H04W84/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2021/219674 A1 (KONINKLIJKE PHILIPS NV [NL]) 4 November 2021 (2021-11-04) page 7, line 9 - page 25, line 23 figures 1-4b	1-22
A	US 2018/375870 A1 (BERNSEN JOHANNES ARNOLDUS CORNELIS [NL]) 27 December 2018 (2018-12-27) paragraph [0005] - paragraph [0225] figures 1-9	1-22

-/--

[x] Further documents are listed in the continuation of Box C. [x] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 March 2023	31/03/2023

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ghomrasseni, Z

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2023/052749

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Anonymous: "DRAFT Device Provisioning Protocol Specification Version 1.2", wi-fi alliance, 3 March 2020 (2020-03-03), pages 1-174, XP055787796, Retrieved from the Internet: URL:https://www.wi-fi.org/download.php?file=/sites/default/files/private/DRAFT%20Device_Provisioning_Protocol_Specification_v_1.2_0.pdf [retrieved on 2021-03-19] the whole document -----	1-22
A	Wi-Fi Alliance: "Wi-Fi Easy Connect(TM) Specification Version 2.0 WI-FI ALLIANCE PROPRIETARY - SUBJECT TO CHANGE WITHOUT NOTICE", , 1 January 2020 (2020-01-01), pages 1-226, XP055873009, Retrieved from the Internet: URL:https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Easy_Connect_Specification_v2.0.pdf [retrieved on 2021-12-14] the whole document -----	1-22
A	EP 3 618 475 A1 (KONINKLIJKE PHILIPS NV [NL]) 4 March 2020 (2020-03-04) paragraph [0017] - paragraph [0058] figure 1 -----	1-22

2

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2023/052749

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2021219674 A1	04-11-2021	BR 112022021971 A2	13-12-2022
		CN 115516892 A	23-12-2022
		EP 4144061 A1	08-03-2023
		WO 2021219674 A1	04-11-2021
US 2018375870 A1	27-12-2018	BR 112018012417 A2	18-12-2018
		CN 108476205 A	31-08-2018
		EP 3395034 A1	31-10-2018
		JP 6517444 B2	22-05-2019
		JP 2018538758 A	27-12-2018
		KR 20180098589 A	04-09-2018
		MY 190785 A	12-05-2022
		RU 2018126780 A	23-01-2020
		TW 201725921 A	16-07-2017
		US 2018375870 A1	27-12-2018
		US 2021067514 A1	04-03-2021
		US 2022329598 A1	13-10-2022
		WO 2017108412 A1	29-06-2017
EP 3618475 A1	04-03-2020	CN 112640510 A	09-04-2021
		EP 3618475 A1	04-03-2020
		EP 3844990 A1	07-07-2021
		JP 2021536157 A	23-12-2021
		US 2021329462 A1	21-10-2021
		WO 2020043634 A1	05-03-2020

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

,MC,ME,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）

１．ＢＬＵＥＴＯＯＴＨ

２．ＺＩＧＢＥＥ

３．ＱＲコード

４．ＪＡＶＡ

弁理士　矢ヶ部 喜行

(72)発明者　ベルンセン ヨハネス アーノルドゥス コルネリス

オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ５ フィリップス インターナショナル ベー ヴェ インテレクチュアル プロパティ アンド スタンダーズ