【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成29年11月16日(2017.11.16)

【公表番号】特表2016-533055(P2016-533055A)
【公表日】平成28年10月20日(2016.10.20)
【年通号数】公開・登録公報2016-060
【出願番号】特願2016-521582(P2016-521582)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｗ　84/10　(2009.01)
Ｈ０４Ｗ　12/06　(2009.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６０１Ｆ
Ｈ０４Ｗ　84/10　１１０
Ｈ０４Ｗ　12/06

【手続補正書】
【提出日】平成29年10月6日(2017.10.6)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
第１のデバイスが、ニアフィールド通信を使用することによって、前記第１のデバイスに関連する公開鍵が、アクセスネットワークに関連するアクセスポイントに送られるべきであることを示すコマンドを受信することと、ここにおいて、前記第１のデバイスおよび前記アクセスポイントは、公開秘密鍵ペアに関連する、
前記第１のデバイスが、ニアフィールド通信を使用することによって、前記アクセスポイントに、前記第１のデバイスに関連する前記公開鍵を送ることと、
前記第１のデバイスが、ニアフィールド通信を使用することによって、前記アクセスポイントに関連する公開鍵および前記アクセスネットワークに関連する暗号化された認証データを受信することと、
前記アクセスポイントに関連する前記公開鍵および前記アクセスネットワークに関連する前記暗号化された認証データを受信することに少なくとも部分的に基づいて、前記アクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記第１のデバイスを構成することとを備える方法。
【請求項２】
前記アクセスネットワークに関連する前記暗号化された認証データは、前記第１のデバイスに関連する前記公開鍵を使用して暗号化される、請求項１に記載の方法。
【請求項３】
前記アクセスネットワークに関連する前記暗号化された認証データは、前記第１のデバイスに関連する少なくとも前記公開鍵から導出された共有秘密鍵を使用して暗号化される、請求項１に記載の方法。
【請求項４】
前記暗号化された認証データは、ユーザ名、またはパスワード、または暗号化鍵、または事前共有鍵、またはそれらの組合せのうちの少なくとも１つを備える、請求項２に記載

の方法。
【請求項５】
前記暗号化された認証データに少なくとも部分的に基づいて前記アクセスネットワークにワイヤレスに接続するように前記第１のデバイスを構成することは、
前記第１のデバイスが、前記アクセスネットワークに関連する前記暗号化された認証データを解読することと、前記暗号化された認証データが、前記第１のデバイスに関連する秘密鍵を使用して解読される、
前記第１のデバイスが、前記アクセスポイントに関連する前記公開鍵を使用してメッセージを暗号化することと、
前記第１のデバイスから、前記暗号化されたメッセージを送ることとを備える、請求項２に記載の方法。
【請求項６】
前記暗号化された認証データに少なくとも部分的に基づいて前記アクセスネットワークにワイヤレスに接続するように前記第１のデバイスを構成することは、
前記第１のデバイスが、前記アクセスネットワークに関連する前記暗号化された認証データを解読することと、前記暗号化された認証データは共有秘密鍵を使用して解読され、ここにおいて、前記共有秘密鍵が、前記アクセスポイントに関連する少なくとも前記公開鍵から導出される、
前記第１のデバイスが、前記アクセスポイントに関連する前記共有秘密鍵を使用してメッセージを暗号化することと、前記メッセージは、前記第１のデバイスが、前記アクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続することを可能にするためのデータを含む、
前記第１のデバイスから、前記暗号化されたメッセージを送ることとを備える、請求項２に記載の方法。
【請求項７】
前記アクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記第１のデバイスを構成することは、
前記第１のデバイスが、前記アクセスネットワークに関連する第１の認証データを生成すること、前記第１の認証データが、前記アクセスポイントに関連する前記公開鍵に少なくとも部分的に基づいて前記第１のデバイスによって生成され、前記第１の認証データが、前記アクセスネットワークに関連する前記暗号化された認証データとは異なる、を備える、請求項１に記載の方法。
【請求項８】
前記アクセスポイントに関連する前記アクセスネットワークに接続するように前記第１のデバイスを構成することは、
前記第１のデバイスが、第３のデバイスに関連する構成データを受信することと、
前記第３のデバイスに接続するように前記第１のデバイスを構成することと、
前記第１のデバイスが、前記アクセスポイントに関連する構成データを受信することと、
前記アクセスポイントに関連する前記構成データに少なくとも部分的に基づいて、前記アクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記第１のデバイスを構成することとを備える、請求項１に記載の方法。
【請求項９】
前記第１のデバイスが、少なくとも部分的に、前記アクセスポイントによって送信された無線周波数信号によって電力供給され、前記アクセスポイントに関連する前記アクセスネットワークに接続するように前記第１のデバイスを構成することは、
前記アクセスポイントによって送信された前記無線周波数信号とは異なる前記第１のデバイスに電力供給することに少なくとも部分的に基づいて、前記アクセスポイントに関連する前記アクセスネットワークに接続するように前記第１のデバイスを前記構成することを開始することをさらに備える、請求項１に記載の方法。

【請求項１０】
前記アクセスポイントに、前記第１のデバイスに関連する前記公開鍵を前記送ることは、前記第１のデバイスが、ニアフィールド通信を使用することによって、前記アクセスポイントと通信する第３のデバイスに前記第１のデバイスに関連する前記公開鍵を送ることを備え、前記第１のデバイスは、ニアフィールド通信タグを備え、前記ニアフィールド通信タグは、前記第３のデバイスによって送信された無線周波数信号によって電力供給される、
前記アクセスポイントに関連する前記公開鍵および前記アクセスネットワークに関連する前記暗号化された認証データを前記受信することは、前記第１のデバイスが、ニアフィールド通信を使用することによって、前記第３のデバイスから、前記アクセスポイントに関連する前記公開鍵および前記アクセスネットワークに関連する前記暗号化された認証データを受信することを備える、請求項１に記載の方法。
【請求項１１】
前記第１のデバイスがニアフィールド通信タグとワイヤレス制御ユニットとを備える、請求項１に記載の方法。
【請求項１２】
前記第１のデバイスが、ニアフィールド通信を使用することによって、前記第１のデバイスに関連する前記公開鍵を送ることは、前記ニアフィールド通信タグによって、前記第１のデバイスに関連する前記公開鍵を送信することを備え、ここにおいて、前記ニアフィールド通信タグが前記アクセスポイントによって送信された無線周波数信号によって電力供給される、請求項１１に記載の方法。
【請求項１３】
前記第１のデバイスが、ニアフィールド通信を使用することによって、前記アクセスポイントに関連する前記公開鍵を受信することは、前記アクセスポイントに関連する前記公開鍵を前記ニアフィールド通信タグ上のメモリに書き込むことを備える、請求項１１に記載の方法。
【請求項１４】
デバイスであって、
ニアフィールド通信を使用して、前記デバイスに関連する公開鍵が、アクセスネットワークに関連するワイヤレスアクセスポイントに送られるべきであることを示すコマンドを受信することと、ここにおいて、前記デバイスおよび前記ワイヤレスアクセスポイントは、公開秘密鍵ペアに関連する、
ニアフィールド通信を使用して、前記デバイスに関連する前記公開鍵を前記ワイヤレスアクセスポイントに送ることと、
ニアフィールド通信を使用して、前記ワイヤレスアクセスポイントに関連する公開鍵および前記アクセスネットワークに関連する暗号化された認証データを受信することと
を行うためのニアフィールド通信タグと、
前記ワイヤレスアクセスポイントに関連する前記公開鍵および前記アクセスネットワークに関連する前記暗号化された認証データを受信することに少なくとも部分的に基づいて、前記ワイヤレスアクセスポイントに関連するフライル前記アクセスネットワークにワイヤレスに接続するように前記デバイスを構成すること
を行うためのワイヤレス制御ユニットと、ここにおいて、前記ワイヤレス制御ユニットが前記ニアフィールド通信タグに結合された、を備えるデバイス。
【請求項１５】
前記アクセスネットワークに関連する前記暗号化された認証データは、前記デバイスに関連する前記公開鍵を使用して暗号化される、請求項１４に記載のデバイス。
【請求項１６】
前記アクセスネットワークに関連する前記暗号化された認証データは、前記デバイスに関連する少なくとも前記公開鍵から導出された共有秘密鍵を使用して暗号化される、請求項１４に記載のデバイス。

【請求項１７】
前記暗号化された認証データが、ユーザ名、またはパスワード、または暗号化鍵、または事前共有鍵、またはそれらの組合せのうちの少なくとも１つを備える、請求項１５に記載のデバイス。
【請求項１８】
前記ワイヤレスアクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記デバイスを構成するための前記ワイヤレス制御ユニットは、
前記アクセスネットワークに関連する前記暗号化された認証データを解読することと、前記暗号化された認証データは、前記デバイスに関連する秘密鍵を使用して解読される、
前記ワイヤレスアクセスポイントに関連する前記公開鍵を使用してメッセージを暗号化することと、
前記暗号化されたメッセージを送ることと、を行うための前記ワイヤレス制御ユニットを備える、請求項１５に記載のデバイス。
【請求項１９】
前記ワイヤレスアクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記デバイスを構成するための前記ワイヤレス制御ユニットは、
前記アクセスネットワークに関連する前記暗号化された認証データを解読することと、前記暗号化された認証データが共有秘密鍵を使用して解読され、前記共有秘密鍵が、前記ワイヤレスアクセスポイントに関連する少なくとも前記公開鍵から導出される、
前記ワイヤレスアクセスポイントに関連する前記公開鍵を使用してメッセージを暗号化することと、前記メッセージは、前記デバイスが、前記ワイヤレスアクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続することを可能にするためのデータを含む、
前記暗号化されたメッセージを送ることと、を行うための前記ワイヤレス制御ユニットを備える、請求項１５に記載のデバイス。
【請求項２０】
前記ワイヤレスアクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記デバイスを構成するための前記ワイヤレス制御ユニットは、
前記アクセスネットワークに関連する第１の認証データを生成するための前記ワイヤレス制御ユニットを備え、前記第１の認証データは、前記ワイヤレスアクセスポイントに関連する前記公開鍵に少なくとも部分的に基づいて生成され、前記第１の認証データは、前記アクセスネットワークに関連する前記暗号化された認証データとは異なる、請求項１４に記載のデバイス。
【請求項２１】
前記ワイヤレスアクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記デバイスを構成するための前記ワイヤレス制御ユニットは、
第３のデバイスに関連する構成データを受信することと、
前記第３のデバイスに接続するように前記デバイスを構成することと、
前記ワイヤレスアクセスポイントに関連する構成データを受信することと、
前記ワイヤレスアクセスポイントに関連する前記構成データに少なくとも部分的に基づいて、前記ワイヤレスアクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記デバイスを構成するための前記ワイヤレス制御ユニットを備える、請求項１４に記載のデバイス。
【請求項２２】
前記ニアフィールド通信タグが前記ワイヤレスアクセスポイントによって送信された無線周波数信号によって電力供給される、請求項１４に記載のデバイス。
【請求項２３】
前記ニアフィールド通信タグは、前記ワイヤレスアクセスポイントに関連する前記公開鍵を前記ニアフィールド通信タグ上のメモリに書き込むようにさらに構成される、請求項１４に記載のデバイス。

【請求項２４】
前記ワイヤレス制御ユニットは、前記ニアフィールド通信タグから前記ワイヤレスアクセスポイントに関連する前記公開鍵を読み取るようにさらに構成される、請求項１４に記載のデバイス。
【請求項２５】
前記ワイヤレス制御ユニットは、前記デバイスに関連する前記公開鍵を前記ニアフィールド通信タグに書き込むようにさらに構成される、請求項１４に記載のデバイス。
【請求項２６】
デバイスであって、
ニアフィールド通信を使用して、前記デバイスに関連する公開鍵がアクセスネットワークに関連するワイヤレスアクセスポイントに送られるべきであることを示すコマンドを受信するための手段と、ここにおいて、前記デバイスおよび前記ワイヤレスアクセスポイントは、公開秘密鍵ペアに関連する、
ニアフィールド通信を使用して、前記デバイスに関連する前記公開鍵を前記ワイヤレスアクセスポイントに送るための手段と、
ニアフィールド通信を使用して、前記ワイヤレスアクセスポイントに関連する公開鍵および前記アクセスネットワークに関連する暗号化された認証データを受信するための手段と、
前記ワイヤレスアクセスポイントに関連する前記公開鍵および前記アクセスネットワークに関連する前記暗号化された認証データを前記受信することに少なくとも部分的に基づいて、前記ワイヤレスアクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記デバイスを構成するための手段とを備えるデバイス。
【請求項２７】
前記アクセスネットワークに関連する前記暗号化された認証データは、前記デバイスに関連する前記公開鍵を使用して暗号化される、請求項２６に記載のデバイス。
【請求項２８】
前記ワイヤレスアクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記デバイスを構成するための前記手段は、
前記アクセスネットワークに関連する前記暗号化された認証データを解読するための手段と、前記暗号化された認証データが、前記デバイスに関連する秘密鍵を使用して解読される、
前記ワイヤレスアクセスポイントに関連する前記公開鍵を使用してメッセージを暗号化するための手段と、
前記暗号化されたメッセージを送るための手段とを備える、請求項２７に記載のデバイス。
【請求項２９】
ニアフィールド通信技術を使用して、第１のデバイスに関連する公開鍵が、アクセスネットワークに関連するアクセスポイントに送られるべきであることを示すコマンドを受信することと、ここにおいて、前記第１のデバイスおよび前記アクセスポイントは、公開秘密鍵ペアに関連する、
ニアフィールド通信を使用して、前記第１のデバイスに関連する前記公開鍵を前記アクセスポイントに送ることと、
ニアフィールド通信を使用して、前記アクセスポイントに関連する公開鍵および前記アクセスネットワークに関連する暗号化された認証データを受信することと、
前記アクセスポイントに関連する前記公開鍵および前記アクセスネットワークに関連する前記暗号化された認証データを受信することに少なくとも部分的に基づいて、前記アクセスポイントに関連する前記アクセスネットワークにワイヤレスに接続するように前記第１のデバイスを構成することとを行うためにプロセッサによって実行可能な命令を記憶する非一時的コンピュータ可読媒体。
【請求項３０】

前記アクセスネットワークに関連する前記暗号化された認証データは、前記第１のデバイスに関連する前記公開鍵を使用して暗号化される、請求項２９に記載の非一時的コンピュータ可読媒体。