

【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27年5月28日(2015.5.28)

【公表番号】特表2015-502701(P2015-502701A)

【公表日】平成27年1月22日(2015.1.22)

【年通号数】公開・登録公報2015-005

【出願番号】特願2014-541226(P2014-541226)

【国際特許分類】

H 04 W 12/06 (2009.01)

H 04 W 12/04 (2009.01)

H 04 L 9/32 (2006.01)

H 04 L 9/08 (2006.01)

【F I】

H 04 W 12/06

H 04 W 12/04

H 04 L 9/00 6 7 5 A

H 04 L 9/00 6 0 1 C

【手続補正書】

【提出日】平成27年4月6日(2015.4.6)

【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】

方法であつて、

アクセスポイントからモバイルデバイスで少なくとも1つのメッセージを受信することと、

前記少なくとも1つのメッセージを受信した後、第1の拡張可能認証プロトコル(EAP)認証を前記モバイルデバイスで実行することと、

前記第1のEAP認証を実行した後、前記第1のEAP認証に関連づけられたマスターセッション鍵(MSK)が満了する前に、第1のブーストラップされたEAP再認証プロトコル(ERP)再認証を前記モバイルデバイスで実行することと、

再認証ルート鍵(rRK)が経過したかどうかに基づいて、第2のEAP認証を実行するか、または第2のブーストラップされたERP再認証を実行するかを、前記モバイルデバイスで決定することを開始すると、ここで、rRKのライフタイムは、前記モバイルデバイスによってアクセスされる、

前記第2のブーストラップされたERP再認証が実行され、不成功である場合に前記rRKのライフタイムの値を減じることとを備える方法。

【請求項2】

前記アクセスポイントとのセッション中に前記モバイルデバイスから前記アクセスポイントに少なくとも1つの第2のメッセージを通信することをさらに備え、前記第1のブーストラップされたERP再認証は、前記セッションの終了前に実行される、請求項1に記載の方法。

【請求項3】

前記第1のブーストラップされたERP再認証中に、再認証MSK(rMSK)のライ

フタイムを受信することをさらに備える、請求項 1 に記載の方法。

【請求項 4】

前記第 2 の E A P 認証を実行するか、または前記第 2 のブーストランプされた E R P 再認証を実行するかを決定することを開始することは、前記モバイルデバイス内の不揮発性メモリから前記 r R K のライフタイムにアクセスすることを備える、請求項 3 に記載の方法。

【請求項 5】

前記 r R K のライフタイムは、前記モバイルデバイスの不揮発性メモリに記憶され、前記方法は、前記モバイルデバイスのプロビジョニング中に前記不揮発性メモリ内の前記 r R K のライフタイムにアクセスすることをさらに備える、請求項 1 に記載の方法。

【請求項 6】

方法であって、

アクセスポイントからモバイルデバイスで少なくとも 1 つのメッセージを受信することと、

前記少なくとも 1 つのメッセージを受信した後、第 1 の拡張可能認証プロトコル (E A P) 認証を前記モバイルデバイスで実行することと、

前記第 1 の E A P 認証を実行した後、前記第 1 の E A P 認証に関連づけられたマスターセッション鍵 (M S K) が満了する前に、第 1 のブーストランプされた E A P 再認証プロトコル (E R P) 再認証を前記モバイルデバイスで実行することと、

再認証ルート鍵 (r R K) のライフタイムが経過したかどうかに基づいて、第 2 の E A P 認証を実行するか、または第 2 のブーストランプされた E R P 再認証を実行するかを、モバイルデバイスで決定することと、ここで、

前記 r R K のライフタイムの値は、前記モバイルデバイス内の不揮発性メモリに記憶され、

前記第 2 の E A P 認証の代わりに前記第 2 のブーストランプされた E R P 再認証を開始することと、

前記第 2 のブーストランプされた E R P 再認証が不成功だったと決定することと、

前記第 2 のブーストランプされた E R P 再認証が不成功だったと決定することに応答して、前記 r R K のライフタイムの前記値を減じることと

を備える方法。

【請求項 7】

前記モバイルデバイスのプロビジョニング中に前記不揮発性メモリにアクセスすることをさらに備え、前記不揮発性メモリは、前記プロビジョニング中に前記 r R K のライフタイムを記憶する、請求項 6 に記載の方法。

【請求項 8】

前記不揮発性メモリはサブスクライバアイデンティティモジュール (S I M) を備え、前記不揮発性メモリにアクセスすることは、前記プロビジョニング中に前記 S I M から前記 r R K のライフタイムの値を読み取ることを備える、請求項 7 に記載の方法。

【請求項 9】

第 3 のブーストランプされた E R P 再認証を開始することと、

前記第 3 のブーストランプされた E R P 再認証が不成功だったと決定することと、

前記第 3 のブーストランプされた E R P 再認証が不成功だったと決定することに応答して、前記 r R K のライフタイムの値を変えることと

をさらに備える、請求項 6 に記載の方法。

【請求項 10】

前記第 3 のブーストランプされた E R P 再認証が不成功だったと決定することに応答して、前記 r R K のライフタイムの前記値を変えることは、前記 r R K のライフタイムの前記値を減じることを備える、請求項 9 に記載の方法。

【請求項 11】

命令を備えた非一時的プロセッサ可読媒体であって、前記命令は、モバイルデバイスの

プロセッサによって実行されると、前記プロセッサに、

アクセスポイントから少なくとも1つのメッセージを受信させ、

前記少なくとも1つのメッセージを受信した後、第1の拡張可能認証プロトコル(EAP)認証を実行させ、

前記第1のEAP認証を実行した後、前記第1のEAP認証に関連づけられたマスターセッション鍵(MSK)が満了する前に、第1のブーストラップされたEAP再認証プロトコル(ERP)再認証を実行させ、

再認証ルート鍵(rRK)が経過したかどうかに基づいて、第2のEAP認証を実行するか、または第2のブーストラップされたERP再認証を実行するかについての決定を開始させ、ここで、rRKのライフタイムは、前記プロセッサによってアクセスされ、前記第2のブーストラップされたERP再認証が実行され、不成功である場合に前記rRKのライフタイムの値を減じさせる、非一時的プロセッサ可読媒体。

【請求項12】

前記モバイルデバイスは、不揮発性メモリを備え、前記命令の実行はさらに、前記プロセッサに、前記モバイルデバイスのプロビジョニング中に前記不揮発性メモリから前記rRKのライフタイムにアクセスさせる、請求項11に記載の非一時的プロセッサ可読媒体。

【請求項13】

モバイルデバイスであって、

プロセッサと、

命令を記憶したメモリと

を備え、前記命令は、

アクセスポイントから少なくとも1つのメッセージを受信し、

前記少なくとも1つのメッセージを受信した後、第1の拡張可能認証プロトコル(EAP)認証を実行し

前記第1のEAP認証を実行した後、前記第1のEAP認証に関連づけられたマスターセッション鍵(MSK)が満了する前に、第1のブーストラップされたEAP再認証プロトコル(ERP)再認証を実行し、

再認証ルート鍵(rRK)が経過したかどうかに基づいて、第2のEAP認証を実行するか、または第2のブーストラップされたERP再認証を実行するかについての決定を開始し、ここで、前記rRKのライフタイムは、前記プロセッサによってアクセスされ、前記第2のブーストラップされたERP再認証が実行され、不成功である場合に前記rRKのライフタイムの値を減じる

ようにプロセッサによって実行可能である、モバイルデバイス。

【請求項14】

前記モバイルデバイスは、不揮発性メモリを備え、前記プロセッサによる前記命令の実行は、前記rRKのライフタイムが、前記モバイルデバイスのプロビジョニング中に、前記不揮発性メモリからアクセスされることを引き起こす、請求項13に記載のモバイルデバイス。

【請求項15】

命令を備えた非一時的プロセッサ可読媒体であって、前記命令は、モバイルデバイスのプロセッサによって実行されると、前記プロセッサに、

アクセスポイントから少なくとも1つのメッセージを受信させ、

前記少なくとも1つのメッセージを受信した後、第1の拡張可能認証プロトコル(EAP)認証を実行させ、

前記第1のEAP認証を実行した後、前記第1のEAP認証に関連づけられたマスターセッション鍵(MSK)が満了する前に、第1のブーストラップされたEAP再認証プロトコル(ERP)再認証を実行させ、

再認証ルート鍵(rRK)のライフタイムが経過したかどうかに基づいて、第2のEAP認証を実行するか、または第2のブーストラップされたERP再認証を実行するかを決

定させ、ここで、前記 r R K のライフタイムは、前記モバイルデバイス内の不揮発性メモリに記憶され、

前記第 2 の E A P 認証の代わりに前記第 2 のブーストラップされた E R P 再認証を開始させ、

前記第 2 のブーストラップされた E R P 再認証が不成功だったと決定させ、前記第 2 のブーストラップされた E R P 再認証が不成功だったと決定することに応答して、前記 r R K のライフタイムの値を減じさせる、非一時的プロセッサ可読媒体。

【請求項 16】

前記命令の実行はさらに、前記プロセッサに、前記モバイルデバイスのプロビジョニング中に前記不揮発性メモリ内の前記 r R K のライフタイムにアクセスさせる、請求項 15 に記載の非一時的プロセッサ可読媒体。

【請求項 17】

前記プロセッサはさらに、

第 3 のブーストラップされた E R P 再認証を開始させられ、

前記第 3 のブーストラップされた E R P 再認証が不成功だったと決定させられ、

前記第 3 のブーストラップされた E R P 再認証が不成功だったと決定することに応答して、前記 r R K のライフタイムの前記値を変えさせられる、

請求項 15 に記載の非一時的プロセッサ可読媒体。

【請求項 18】

モバイルデバイスであって、

再認証ルート鍵 (r R K) のライフタイムを記憶した不揮発性メモリと、

プロセッサと、

命令を記憶した第 2 のメモリと

を備え、前記命令は、

アクセスポイントから少なくとも 1 つのメッセージを受信し、

前記少なくとも 1 つのメッセージを受信した後、第 1 の拡張可能認証プロトコル (E A P) 認証を実行し、

前記第 1 の E A P 認証を実行した後、前記第 1 の E A P 認証に関連づけられたマスターセッション鍵 (M S K) が満了する前に、第 1 のブーストラップされた E A P 再認証プロトコル (E R P) 再認証を実行し、

前記 r R K が経過したかどうかに基づいて、第 2 の E A P 認証を実行するか、または第 2 のブーストラップされた E R P 再認証を実行するかを決定し、

前記第 2 の E A P 認証の代わりに前記第 2 のブーストラップされた E R P 再認証を開始し、前記第 2 のブーストラップされた E R P 再認証が不成功だったと決定し、

前記第 2 のブーストラップされた E R P 再認証が不成功だったと決定することに応答して、前記 r R K のライフタイムの値を減じる

ように前記プロセッサによって実行可能である、モバイルデバイス。

【請求項 19】

前記プロセッサによる前記命令の実行は、前記 r R K のライフタイムが、前記モバイルデバイスのプロビジョニング中に前記不揮発性メモリからアクセラされることを引き起こす、請求項 18 に記載のモバイルデバイス。

【請求項 20】

前記命令はさらに、

第 3 のブーストラップされた E R P 再認証を開始し、

前記第 3 のブーストラップされた E R P 再認証が不成功だったと決定し、

前記第 3 のブーストラップされた E R P 再認証が不成功だったと決定することに応答して、前記 r R K のライフタイムの前記値を変える

ように前記プロセッサによって実行可能である、請求項 18 に記載のモバイルデバイス。