

【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 24 年 10 月 18 日 (2012.10.18)

【公表番号】特表 2012-517185 (P2012-517185A)
 【公表日】平成 24 年 7 月 26 日 (2012.7.26)
 【年通号数】公開・登録公報 2012-029
 【出願番号】特願 2011-549117 (P2011-549117)
 【国際特許分類】

H 0 4 L 9/08 (2006.01)

H 0 4 W 12/08 (2009.01)

H 0 4 L 9/32 (2006.01)

【 F I 】

H 0 4 L 9/00 6 0 1 B

H 0 4 Q 7/00 1 8 4

H 0 4 L 9/00 6 7 3 B

H 0 4 L 9/00 6 7 3 A

【手続補正書】
 【提出日】平成 24 年 8 月 30 日 (2012.8.30)
 【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】

ブートストラップ・メッセージの保護を可能にするデバイス管理 D M ネットワーク・システムの第 1 のネットワーク・ユニット (5 0 0) であって、

デバイス (6 0 0) をブートストラップする要求を含む第 1 のメッセージであって、前記デバイス (6 0 0) を識別する情報及び加入者を識別する情報を含む前記第 1 のメッセージを受信する受信機 (5 1 0) と、

前記加入者を識別する前記情報を含む第 2 のメッセージであって、前記加入者を識別する前記情報に基づくブートストラップ・キーを前記第 1 のネットワーク・ユニット (5 0 0) へ提供するように、第 2 のネットワーク・ユニットへ要求する前記第 2 のメッセージを、前記第 2 のネットワーク・ユニットへ送信する送信機 (5 2 0) とを備え、

前記受信機 (5 1 0) は、さらに、前記第 2 のネットワーク・ユニットから、前記ブートストラップ・メッセージの保護を可能にするための、前記ブートストラップ・キーと、トリガ情報とを含む第 3 のメッセージを受信するように構成され、

前記送信機 (5 2 0) は、さらに、前記デバイス (6 0 0) において前記ブートストラップ・キーの生成を開始させるために、該デバイス (6 0 0) へ前記トリガ情報を送信するように構成されることを特徴とする第 1 のネットワーク・ユニット (5 0 0) 。

【請求項 2】

前記ブートストラップ・キーを記憶する記憶手段 (5 3 0) をさらに備え、

前記第 1 のネットワーク・ユニット (5 0 0) は、さらに、

前記ブートストラップ・キーに基づいて、前記送信機 (5 2 0) が保護されたブートストラップ・メッセージを前記デバイス (6 0 0) へ送信する前に、前記ブートストラップ・メッセージを保護するように構成されることを特徴とする請求項 1 に記載の第 1 のネットワーク・ユニット (5 0 0) 。

【請求項 3】

前記送信機（520）は、ジェネリック・ブートストラップ・アーキテクチャ・ブッシュ情報 G P I の前記トリガ情報を送信するように構成され、

前記受信機（510）は、G P I レスポンス・メッセージの前記ブートストラップ・キーを含む前記第 3 のメッセージを受信するように構成されることを特徴とする請求項 1 又は 2 に記載の第 1 のネットワーク・ユニット（500）。

【請求項 4】

前記ブートストラップ・メッセージの検証後に、前記デバイス（600）と前記 D M ネットワーク・システムとの間の少なくとも 1 つの D M セッション中に少なくとも 1 つのメッセージの保護のための追加のキーを生成するために、マスタキーとして前記ブートストラップ・キーを使用するようにさらに構成されることを特徴とする請求項 1 乃至 3 の何れか 1 項に記載の第 1 のネットワーク・ユニット（500）。

【請求項 5】

ブートストラップ・メッセージの保護を可能にするためのデバイス管理 D M ネットワーク・システムの第 1 のネットワーク・ユニット（500）と通信可能なデバイス（600）であって、

前記デバイスを識別する情報及び加入者を識別する情報を、前記第 1 のネットワーク・ユニット（500）へ通知する手段（610）と、

前記第 1 のネットワーク・ユニット（500）から、前記デバイスのブートストラップ・キーの生成を開始させるトリガ情報を受信する受信機（610）であって、前記ブートストラップ・キーに基づいて保護される、保護されたブートストラップ・メッセージを受信するように構成される前記受信機（610）と、

前記保護されたブートストラップ・キーを検証するか、復号化するか、の少なくとも一方を行う手段（630）と

を備えることを特徴とするデバイス（600）。

【請求項 6】

前記受信機（610）は、ジェネリック・ブートストラップ・アーキテクチャ G B A ブッシュ情報 G P I メッセージの前記トリガ情報を受信するように構成されることを特徴とする請求項 5 に記載のデバイス（600）。

【請求項 7】

前記ブートストラップ・キーを記憶する記憶手段（640）をさらに備えることを特徴とする請求項 5 又は 6 に記載のデバイス（600）。

【請求項 8】

ブートストラップ・メッセージの保護を可能にするデバイス管理 D M ネットワーク・システムの第 1 のネットワーク・ユニット（500）における方法であって、

デバイスをブートストラップする要求を含む第 1 のメッセージであって、前記デバイスを識別する情報及び加入者を識別する情報を含む前記第 1 のメッセージを前記第 1 のネットワーク・ユニットで受信するステップ（401）と、

前記加入者を識別する前記情報を含む第 2 のメッセージであって、前記加入者を識別する前記情報に基づくブートストラップ・キーを前記第 1 のネットワーク・ユニットへ提供するように、第 2 のネットワーク・ユニットへ要求する前記第 2 のメッセージを、前記第 2 のネットワーク・ユニットへ送信するステップ（402）と、

前記第 2 のネットワーク・ユニットから、前記ブートストラップ・メッセージの保護を可能にするための、前記ブートストラップ・キーと、トリガ情報とを含む第 3 のメッセージを受信するステップ（403）と、

前記デバイスにおいて前記ブートストラップ・キーの生成を開始させるために、該デバイスへ前記トリガ情報を送信するステップ（404）とを含むことを特徴とする方法。

【請求項 9】

前記ブートストラップ・キーを前記第 1 のネットワーク・ユニットで記憶するステップ

と、

前記ブートストラップ・キーに基づいて、前記ブートストラップ・メッセージを前記デバイスへ送信する前に、前記ブートストラップ・メッセージを保護するステップとをさらに含むことを特徴とする請求項 8 に記載の方法。

【請求項 10】

前記トリガ情報を送信する前記ステップ(404)は、ジェネリック・ブートストラップ・アーキテクチャ・プッシュ情報 G P I メッセージの前記トリガ情報を送信するステップを含み、

前記第 3 のメッセージを受信する前記ステップ(403)は、G P I レスポンス・メッセージの前記第 3 のメッセージを受信するステップを含むことを特徴とする請求項 8 又は 9 に記載の方法。

【請求項 11】

前記ブートストラップ・メッセージの検証後に、前記デバイスと前記 D M ネットワーク・システムとの間の少なくとも 1 つの D M セッション中に少なくとも 1 つのメッセージを保護するための追加のキーを生成するために、マスタキーとして前記ブートストラップ・キーを使用するステップをさらに含むことを特徴とする請求項 8 乃至 10 の何れか 1 項に記載の方法。

【請求項 12】

請求項 8 乃至 11 の何れか 1 項に記載の第 1 のネットワーク・ユニット(500)における方法の各ステップをコンピュータに実行させるためのプログラム命令を含むコンピュータで実行可能なコンピュータプログラム。