【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】令和1年11月21日(2019.11.21)

【公表番号】特表2019-500798(P2019-500798A)
【公表日】平成31年1月10日(2019.1.10)
【年通号数】公開・登録公報2019-001
【出願番号】特願2018-532423(P2018-532423)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｇ０６Ｆ　21/60　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｈ０４Ｌ　9/00　６７５Ａ
Ｇ０９Ｃ　1/00　６４０Ｄ
Ｇ０６Ｆ　21/60　３２０

【手続補正書】
【提出日】令和1年10月8日(2019.10.8)
【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】
電子エンティティ（２）がデータ（Ｄｉ；ＤＡＴＡＳＥＮＤ）を受信する方法であって、
第１の暗号キー（ＳＫ－ＥＮＣ）を用いた暗号化によってセキュアされた第１のセキュアチャネルを、前記電子エンティティ（２）と外部電子機器との間に確立するステップ（Ｅ２、Ｅ４、Ｅ６、Ｅ８、Ｅ１０）と、
前記第１のセキュアチャネルを介して、第１のコマンド（ＣＨＭ）を受信するステップ（Ｅ１４）と、
前記第１のセキュアチャネルを介して、少なくとも一つの第２の暗号キー（ＢＫ－ＥＮＣ）を受信するステップと、
前記第１のコマンド（ＣＨＭ）を実行することにより、前記第２の暗号キー（ＢＫ－ＥＮＣ）を用いた暗号化によってセキュアされた第２のセキュアチャネルを設定するステップ（Ｅ２０）と、
前記第２のセキュアチャネルにおいて前記データ（Ｄｉ；ＤＡＴＡＳＥＮＤ）を受信するステップ（Ｅ２２）と、を有する、ことを特徴とする方法。
【請求項２】
前記第１のコマンドを受信するステップの後で、前記第２のセキュアチャネルを設定するステップの前に、前記電子エンティティ（２）のメモリ（８）の中に前記第１の暗号キー（ＳＫ－ＥＮＣ）をセーブするステップ（Ｅ１８）を有する、請求項１に記載の方法。
【請求項３】
前記データおよび第２のコマンド（ＣＨＭ）を受信するステップの後、前記第１のセキュアチャネルへ変更するステップ（Ｅ３０）を有する、請求項１または２に記載の方法。

【請求項４】
前記データおよび第２のコマンド（ＣＨＭ）を受信するステップの後、前記第１のセキュアチャネルへ変更するステップ（Ｅ３０）を有し、
前記変更するステップは、前記メモリ（８）の中にセーブされた前記第１の暗号キーを読み取るサブステップを有する、請求項２に記載の方法。
【請求項５】
前記変更するステップの後、前記第１のセキュアチャネルに関するリストアデータを無効化するステップを有する、請求項３または４に記載の方法。
【請求項６】
前記変更するステップの後、前記第１のセキュアチャネルにおいて認証コマンドを待機するステップを有する、請求項３～５のいずれか一項に記載の方法。
【請求項７】
前記第１のセキュアチャネルにおいて完全性検証コード（ＭＡＣ）を検査するステップを有する、請求項６に記載の方法。
【請求項８】
前記第１の暗号キー（ＳＫ－ＥＮＣ）は、前記電子エンティティ（２）の中に記憶される静的キー（Ｋ）から導出されるセッションキーである、請求項１～７のいずれか一項に記載の方法。
【請求項９】
前記第２の暗号キー（ＢＫ－ＥＮＣ）は、他の電子エンティティによって確立されたセキュアチャネルを暗号化するのに用いられるブロードキャストキーである、請求項１～８のいずれか一項に記載の方法。
【請求項１０】
前記データ（ＤＡＴＡＳＥＮＤ）は、前記電子エンティティ（２）のオペレーティングシステムの一部、または前記電子エンティティによって後で用いられることができるアプリケーションもしくはデータの少なくとも一部を表す、請求項１～９のいずれか一項に記載の方法。
【請求項１１】
前記受信されたデータは、前記電子エンティティ（２）の不揮発性メモリ（６）の中に記憶される、請求項１～１０のいずれか一項に記載の方法。
【請求項１２】
前記電子エンティティは、セキュアエレメント（２）である、請求項１～１１のいずれか一項に記載の方法。
【請求項１３】
前記外部電子機器は、携帯端末、エネルギ供給メータ、接続されたオブジェクトまたは携帯オブジェクトである、請求項１～１２のいずれか一項に記載の方法。
【請求項１４】
第１の暗号キー（ＳＫ－ＥＮＣ）を用いた暗号化によってセキュアされた第１のセキュアチャネルを、電子エンティティと外部電子機器との間に確立するモジュールと、
前記第１のセキュアチャネルを介して、第１のコマンド（ＣＨＭ）および第２の暗号キー（ＢＫ－ＥＮＣ）を受信するモジュールと、
前記第１のコマンド（ＣＨＭ）を実行することにより、前記第２の暗号キー（ＢＫ－ＥＮＣ）を用いた暗号化によってセキュアされた第２のセキュアチャネルを設定するモジュールと、
前記第２のセキュアチャネルにおいてデータ（Ｄｉ；ＤＡＴＡＳＥＮＤ）を受信するモジュールと、を有する、ことを特徴とする電子エンティティ（２）。