【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10月19日(2017.10.19)

【公表番号】特表2016-533048(P2016-533048A)
【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2016-517299(P2016-517299)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｑ　20/32　(2012.01)
Ｇ０６Ｑ　20/38　(2012.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｇ０６Ｑ　20/32　３００
Ｇ０６Ｑ　20/38　３１８
Ｇ０６Ｑ　20/38　３１６

【手続補正書】
【提出日】平成29年9月5日(2017.9.5)
【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】
モバイルデバイス内のモバイルアプリケーションとゲートウェイの間を通過する取引メッセージを安全化する方法であって、取引が開始されるとき、
モバイルアプリケーションの取引カウンタを増加させるステップと、
セッション暗号化鍵ＥＮＣを取引カウンタ値およびゲートウェイ暗号化鍵ＫＥＮＣから導出するステップであって、前記ゲートウェイ暗号化鍵が第１のマスタゲートウェイ鍵から導出される、導出するステップと、
機密データをセッション暗号化鍵ＥＮＣで暗号化するステップと、
暗号化された機密データ、取引カウンタ値、およびモバイルアプリケーションのアプリケーション識別子を含む取引要求メッセージを作り出すステップと、
取引要求メッセージをモバイルアプリケーションからモバイルデバイスを介してゲートウェイに送るステップであって、ゲートウェイが、受け取った取引要求メッセージからセッション暗号化鍵を計算するように構成されている、送るステップと、
受け取った暗号化されたデータを計算されたセッション暗号化鍵ＥＮＣで復号するステップと
を含む、方法。
【請求項２】
セッション完全性鍵ＭＡＣを取引カウンタ値およびゲートウェイ完全性鍵ＫＭＡＣから導出するステップであって、前記ゲートウェイ完全性鍵が第２のマスタゲートウェイ鍵から導出される、導出するステップと、
ＭＡＣ署名値を、セッション完全性鍵ＭＡＣおよび取引要求メッセージの内容の少なくとも一部から計算するステップと、
前記ＭＡＣ値を、その作成中、取引要求メッセージに追加するステップと

を含み、
ゲートウェイが、受け取った取引要求メッセージからセッション完全性鍵を計算し、受け取った取引要求メッセージのＭＡＣ署名値を確認するように構成されている、請求項１に記載の方法。
【請求項３】
ゲートウェイ暗号化鍵ＫＥＮＣおよびゲートウェイ完全性鍵ＫＭＡＣの導出が、
第１および第２のマスタゲートウェイ鍵を生成するステップと、
モバイルアプリケーション用のアプリケーション識別子を生成するステップと、
ゲートウェイ暗号化鍵ＫＥＮＣを、前記アプリケーション識別子、第１のマスタ鍵および第１の導出アルゴリズムから導出するステップと、
ゲートウェイ完全性鍵ＫＭＡＣを、前記アプリケーション識別子、第２のマスタ鍵および第２の導出アルゴリズムから導出するステップと、
モバイルアプリケーションに、生成されたアプリケーション識別子、導出されたゲートウェイ暗号化鍵ＫＥＮＣおよび導出されたゲートウェイ完全性鍵ＫＭＡＣをロードするステップと
を含む、請求項２に記載の方法。
【請求項４】
ゲートウェイが、
ゲートウェイ暗号化鍵ＫＥＮＣとゲートウェイ完全性鍵ＫＭＡＣを、受け取ったアプリケーション識別子から、およびそれぞれ、格納された第１と第２のマスタゲートウェイ鍵および第１と第２の導出アルゴリズムから導出するステップと、
セッション暗号化鍵ＥＮＣとセッション完全性鍵ＭＡＣを、受け取った取引カウンタ値から、およびそれぞれ、導出されたゲートウェイ暗号化鍵ＫＥＮＣと導出されたゲートウェイ完全性鍵ＫＭＡＣから導出するステップと
に従ってセッション鍵を計算する、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１と第２の導出アルゴリズムが同一である、請求項３または４に記載の方法。
【請求項６】
第１と第２のマスタゲートウェイ鍵が同一である、請求項２から５のいずれか一項に記載の方法。
【請求項７】
生成されたアプリケーション識別子、ゲートウェイ暗号化鍵ＫＥＮＣおよびゲートウェイ完全性鍵ＫＭＡＣを含むモバイルアプリケーションが、モバイルデバイスのセキュア要素に格納される、請求項１から６のいずれか一項に記載の方法。
【請求項８】
ゲートウェイが、復号された機密データを含む取引要求メッセージを、処理のためにモバイルアプリケーションのイシュアに転送する、請求項１から７のいずれか一項に記載の方法。
【請求項９】
取引が、モバイルデバイスのユーザによって、モバイルデバイス自体によって、またはプッシュメッセージがモバイルアプリケーションによって受け取られたときに開始される、請求項１から８のいずれか一項に記載の方法。
【請求項１０】
モバイルアプリケーションがモバイル決済アプリケーションであり、取引カウンタがアプリケーション取引カウンタ（ＡＴＣ）であり、取引要求メッセージが、
アプリケーション識別子と、
その時点のアプリケーション取引カウンタＡＴＣと、
磁気ストライプデータトラックの内容を全体的または部分的（トラック１、トラック２、トラック３）に含む機密データと、
イシュアがモバイル決済アプリケーションを認証できるようにする動的取引データおよ

び静的アプリケーションデータと
を含む、請求項１から９のいずれか一項に記載の方法。
【請求項１１】
開始される取引が、
モバイル決済アプリケーションのパラメータを更新すること、
モバイルデバイスの決済アプリケーションをブロックすること、
モバイル決済アプリケーションのブロックを解除すること、
モバイル決済アプリケーションのＰＩＮのブロックを解除すること、および／または
モバイル決済アプリケーションのＰＩＮを変更すること
を含む無線イシュア更新である、請求項１０に記載の方法。
【請求項１２】
開始される取引が、イシュアによるモバイル通信デバイスの認証である、請求項１から１０のいずれか一項に記載の方法。
【請求項１３】
開始される取引が、モバイル通信デバイスを介した決済取引である、請求項１から１０のいずれか一項に記載の方法。
【請求項１４】
ゲートウェイが、安全化された処理ネットワークを介してイシュアと通信する、請求項１から１３のいずれか一項に記載の方法。
【請求項１５】
モバイルデバイスに格納されたモバイルアプリケーションを含む取引処理システムであって、前記モバイルアプリケーションが、モバイル通信デバイスを経由し、ゲートウェイを介してイシュアと通信するように構成されており、この通信の間、モバイルアプリケーションとゲートウェイの間を通過する取引メッセージが、請求項１から１４のいずれか一項に従って安全化される、取引処理システム。