【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20年2月21日(2008.2.21)

【公表番号】特表2004-524779(P2004-524779A)
【公表日】平成16年8月12日(2004.8.12)
【年通号数】公開・登録公報2004-031
【出願番号】特願2002-584534(P2002-584534)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｚ

【誤訳訂正書】
【提出日】平成19年9月3日(2007.9.3)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
電子署名システムを利用した、小型携帯型の署名を行うデバイスを使用してデータに電子署名及び／又はディジタル署名する方法であって、
ａ）　第１の署名を使用するデバイスにおいて前記データの一部分を摘出するステップと、
ｃ）第１の署名を使用するデバイスにおいて前記データをハッシュ化して前記データをハッシュコードとするステップと、
ｄ）　単一のリクエストにおいて、前記データの一部及び前記ハッシュコードを、前記小型携帯型の署名を行うデバイスに転送するステップと、
ｅ）　前記電子署名システムに従って、小型携帯型の前記署名を行うデバイスにおいて前記リクエストに署名するステップと
を有し、
ステップａ）とステップｃ）との間に、
ｂ）　ユーザが読み取り可能な、前記小型携帯型の署名を行うデバイスに適応した形式に前記データの一部分を変換するステップを有することを特徴とする方法。
【請求項２】
小型携帯型の署名を行うデバイスから第１の署名を使用するデバイスに対して前記署名の結果としてその署名を返戻するステップをさらに含むことを特徴とする請求項１に記載の方法。
【請求項３】
第１の署名を使用するデバイスから第２の署名を使用するデバイスに対して前記データ、リクエスト及び署名を転送するステップをさらに含むことを特徴とする請求項２に記載の方法。
【請求項４】
小型携帯型の署名を行うデバイスは、特定のプロトコルを使用した暗号が使用可能な小型デバイスであり、第１の署名を使用するデバイスは、前記データの一部分を前記プロトコルに変換するように適応した署名を使用するシステムであることを特徴とする請求項１ないし３のいずれかに記載の方法。
【請求項５】

前記第２の署名を使用するデバイスは、少なくとも、署名データの処理、確認及び／又は格納を行う署名を受信するデバイスであることを特徴とする請求項３又は４に記載の方法。
【請求項６】
前記プロトコルは、ＷＡＰ（ワイヤレスアプリケーションプロトコル）であり、小型携帯型の署名を行うデバイスはＷＡＰが使用可能な携帯デバイスであることを特徴とする請求項４又は５に記載の方法。
【請求項７】
前記電子署名システムは、秘密鍵／公開鍵を使用していることを特徴とする請求項１ないし６のいずれかに記載の方法。
【請求項８】
前記データはドキュメントまたは、譲渡証、事業報告書もしくはその他様々な書式であることを特徴とする請求項１ないし７のいずれかに記載の方法。
【請求項９】
署名は、ＷＡＰ１．２ｓｉｇｎＴｅｘｔ（）機能を用いて実行されることを特徴とする請求項６ないし８のいずれかに記載の方法。
【請求項１０】
署名は、ＳＩＭアプリケーションツールキット（ＳＡＴ）を使用して実装された暗号署名アプリケーションを用いて実行されることを特徴とする請求項６ないし９のいずれかに記載の方法。
【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】０００２
【訂正方法】変更
【訂正の内容】
【０００２】
電子商取引（イーコマース）又は移動商取引（エムーコマース）等の多種の用途では、ある人が取引を行う権限を有しているという永久的な裏付けを提供する能力を必要とする。また、譲渡証、事業報告書及びその他様々な書式といった、電子資料の署名が近い将来に習慣的になると期待されている。
【誤訳訂正３】
【訂正対象書類名】明細書
【訂正対象項目名】００１４
【訂正方法】変更
【訂正の内容】
【００１４】
より具体的には、本発明は、署名を行うデバイスを使用してデータにディジタル署名する方法であって、署名を使用するシステムにおいてデータの一部を摘出することと、該データの一部を署名を行うデバイスが使用する適切なプロトコルに変換することと、データのハッシュコードと共に該データの一部を前記署名を行うデバイスに転送することとを含む方法を提供する。これにより、署名を行うデバイスのユーザには、署名を行うデバイスの制約に従って適応された、ユーザが認識可能なデータの変換された部分が提示される。次いで該ユーザは適切な署名アルゴリズムを使用した署名を行うデバイスを用いてデータに電子的に署名することができる。当該データの、認識可能で適応した部分だけがユーザに提示される場合も、正確なハッシュコードにより、ユーザが本当に対象データに署名することが実証される。その署名は署名を使用するシステムに返戻され、原データ、データの一部、ハッシュコード及び署名は、処理、確認、格納等を行う署名を受信するシステムに送信される。
【誤訳訂正４】
【訂正対象書類名】明細書

【訂正対象項目名】００２０
【訂正方法】変更
【訂正の内容】
【００２０】
署名を使用するシステムは、ユーザに提示及び理解されるように獲得された（１）メッセージを変換する（２）。該署名を使用するシステムは、獲得された署名されるべきデータ全体を所有する任意のデータシステム、ノード又はコンピュータであってよい。例えば、該署名を使用するシステムは、署名を必要とするドキュメントを受信したユーザＰＣであってもよい。
【誤訳訂正５】
【訂正対象書類名】明細書
【訂正対象項目名】００２１
【訂正方法】変更
【訂正の内容】
【００２１】
続いて、変換されたデータは、ＷＡＰ電話等のユーザの暗号が使用可能な小型デバイスに転送される（３）。ユーザは、適切な署名アルゴリズムを用いてこのメッセージに署名する。ユーザは、特定の署名ＰＩＮコードを入力することにより、署名を行うことができる。
【誤訳訂正６】
【訂正対象書類名】明細書
【訂正対象項目名】００２２
【訂正方法】変更
【訂正の内容】
【００２２】
その署名は、署名を使用するシステムに返戻されて（４）、少なくとも
１）OriginalData及びハッシュコードアルゴリズム識別子
２）ToBeSignedMessage及び署名アルゴリズム識別子並びに署名
を保存した署名を受信するシステムに送られる（５）メッセージに変換される（図２参照）。
【誤訳訂正７】
【訂正対象書類名】明細書
【訂正対象項目名】００２７
【訂正方法】変更
【訂正の内容】
【００２７】
最後に、図５は、（図２のToBeSignedMessage及び図３の変換されたデータとして引用された）変換された認識可能なデータが、暗号が使用可能なデバイスの表示装置上でのユーザ向けの表示例を図示している。