【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18年8月3日(2006.8.3)

【公表番号】特表2006-514478(P2006-514478A)
【公表日】平成18年4月27日(2006.4.27)
【年通号数】公開・登録公報2006-017
【出願番号】特願2004-568844(P2004-568844)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ

【手続補正書】
【提出日】平成18年6月13日(2006.6.13)
【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】
センダからレシピエントへメッセージを機密保持通信する方法において、
レシピエントの機密に基づくベラファイヤに基づくメッセージキーを暗号化することによってこのメッセージキーを含むエンベロープを生成する段階、
このメッセージキーを上記センダに与える段階、
上記センダにおいて、上記メッセージキーに基づき上記メッセージを暗号化する段階、
上記センダから上記レシピエントにこのメッセージを送る段階、
上記エンベロープを上記レシピエントに与える段階、および
上記レシピエントにおいて、上記レシピエントの機密に基づくエンベロープを開き、上記エンベロープから上記メッセージキーを検索し、かつこのメッセージキーに基づいて上記メッセージを復号する段階を有することを特徴とする機密保持通信方法。
【請求項２】
センダからレシピエントへメッセージを機密保持通信する方法において、
（ａ）メッセージキーを準備する段階、
（ｂ）レシピエントの機密に基づくベラファイヤに基づくメッセージキーを暗号化することによってこのメッセージキーを含むエンベロープを生成する段階、および
（ｃ）このメッセージキーに基づいて上記メッセージを暗号化することによって、上記エンベロープで機密を保持された状態で、上記メッセージを上記センダから上記レシピエントに送るとともに、上記レシピエントにこのエンベロープを与え、上記機密を使用して上記エンベロープを開き、上記メッセージキーを検索するとともに、上記メッセージを復号する段階を有することを特徴とする機密保持通信方法。
【請求項３】
上記段階（ａ）は、上記センダそれ自体において上記メッセージキーを生成する段階を含む請求項２記載の方法。
【請求項４】
上記段階（ａ）は、キーサーバで上記メッセージキーを得るとともに、上記センダがこのキーサーバから上記メッセージキーを受け取る段階を含む請求項２記載の方法。
【請求項５】
上記キーサーバは、上記メッセージキーのコピーを保存する請求項４記載の方法。

【請求項６】
上記段階（ａ）は、上記メッセージキーがセンダそれ自体以外の当事者に解除されているかどうか、またどんな条件下でこれが行われているかに関して上記キーサーバに命令する段階を含む請求項５記載の方法。
【請求項７】
上記段階（ａ）は、上記センダが上記キーサーバにレシピエントリストを与えるとともに、上記キーサーバがこのレシピエントリストのコピーを記憶する段階を含む請求項５記載の方法。
【請求項８】
上記段階（ａ）は、上記メッセージキーを与える上記キーサーバの条件として上記センダを認証する段階を含み、又は、上記センダが上記キーサーバに認証サーバから生成されるセンダアサーションを与える段階を含む請求項４記載の方法。
【請求項９】
上記段階（ｂ）は、直接に上記ベラファイヤを用いてエンベロープキーを暗号化することによって直接に上記機密を用いて上記エンベロープを復号する段階を含む請求項２記載の方法。
【請求項１０】
上記段階（ｂ）は、キーサーバで上記エンベロープを生成し、そして上記センダがこのエンベロープを上記キーサーバから受け取る段階を含む請求項２記載の方法。
【請求項１１】
上記レシピエントは上記メッセージの複数のレシピエントの一つであり、そして
上記段階（ｂ）は、上記複数のレシピエントのうちどのレシピエントに関して上記エンベロープを生成するかについて上記センダが上記キーサーバに命令し、これによって、上記複数のレシピエントのうち少なくとも一部が上記メッセージキーをオンラインで受け取り、そして他のレシピエントは上記メッセージをオフラインで読み取る段階を含む請求項１０記載の方法。
【請求項１２】
上記段階（ｂ）は、上記センダが上記ベラファイヤまたは上記機密のいずれかを上記キーサーバに与え、これによってこのキーサーバが上記ベラファイヤを生成する段階を含む請求項１０記載の方法。
【請求項１３】
上記段階（ｂ）は、上記キーサーバが認証サーバに上記ベラファイヤまたは上記機密を要求し、これによってこのキーサーバが上記ベラファイヤを生成する段階を含み、そして上記認証サーバは、既に上記ベラファイヤを有するメンバー、既に機密をもち上記ベラファイヤを生成するメンバー、上記機密と等価なデータをもち上記ベラファイヤを生成するメンバー、および上記機密のハッシュをもち上記ベラファイヤを生成するメンバーからなるセットのうちの一つのメンバーである請求項１０記載の方法。
【請求項１４】
上記機密は、パスワードまたはパスワード以外の上記レシピエントの少なくとも一つのパブリックまたはプライベートな属性に基づいている請求項２記載の方法。
【請求項１５】
上記ベラファイヤはレシピエントベラファイヤであり、そして上記センダは上記メッセージをもつセンダベラファイヤを含み、それによって、上記レシピエントが上記メッセージに対して機密を保持した状態で簡単に返答できるようにした請求項２記載の方法。
【請求項１６】
メッセージキーで機密を保護したメッセージをレシピエントが復号する方法において、
（ａ）上記レシピエントの、エンベロープを生成するために使用するベラファイヤに対応する機密に基づくエンベロープを受け取る段階、
（ｂ）上記エンベロープを開いて上記メッセージキーを検索する段階、および
（ｃ）上記メッセージキーに基づいて上記メッセージを復号する段階からなることを特

徴とする方法。
【請求項１７】
上記レシピエントが上記メッセージを受け取った後に、上記エンベロープを生成する請求項１６記載の方法。
【請求項１８】
上記機密が、上記レシピエントが上記メッセージを受け取った後に、新しい機密になる請求項１７記載の方法。
【請求項１９】
上記段階（ａ）は、上記エンベロープを上記メッセージとともに上記レシピエントに与える段階を含む請求項１６記載の方法。
【請求項２０】
上記段階（ａ）は、上記エンベロープをキーサーバから上記レシピエントに与える段階を含む請求項１６記載の方法。
【請求項２１】
上記段階（ａ）は、上記エンベロープを与える上記キーサーバの条件として上記レシピエントを認証する段階を含む請求項２０記載の方法。
【請求項２２】
上記キーサーバはレシピエントリストをもち、そして
上記段階（ａ）は、上記レシピエントが、上記エンベロープを与える上記キーサーバの条件として、上記レシピエントリストに載っていることを確認する段階を含む請求項２１記載の方法。
【請求項２３】
上記認証する段階は、認証サーバによって発行されるレシピエントの信用証明を上記キーサーバに与える段階を含む請求項２１記載の方法。
【請求項２４】
上記認証サーバは上記ベラファイヤを保存することによって、このベラファイヤのリポジトリを与え、そして
上記キーサーバは上記認証サーバからこのベラファイヤを得る請求項２３記載の方法。
【請求項２５】
上記認証サーバは上記ベラファイヤを生成し、そして
上記キーサーバは上記認証サーバから上記ベラファイヤを得る請求項２３記載の方法。
【請求項２６】
アサーションを生成する上記要求以外のレシピエントとのトランザクションに基づいて上記認証サーバは上記ベラファイヤを生成する請求項２５記載の方法。
【請求項２７】
上記機密は、パスワードまたはパスワード以外の上記レシピエントの少なくとも一つのパブリックまたはプライベートな属性に基づいている請求項２６記載の方法。
【請求項２８】
上記エンベロープキーはキーアグリーメントプロトコルに基づいて誘導され、そして、
上記復号は対称復号アルゴリズムを使用する請求項１６記載の方法。
【請求項２９】
上記エンベロープキーは上記ベラファイヤで直接に暗号化され、そして上記段階（ｂ）は、上記機密で直接に上記エンベロープを復号またはパブリックキー復号アルゴリズムに基づいて上記エンベロープを復号することによって上記メッセージキーを検索する段階を含む請求項１６記載の方法。
【請求項３０】
センダがレシピエントと対象とするメッセージを暗号化するシステムにおいて、
このレシピエントの機密に基づくベラファイヤに基づいてメッセージキーを暗号化することによってこのメッセージキーを有するエンベロープを生成する第１コンピュータ化システムであって、少なくとも上記エンベロープを第２コンピュータ化システムに与える第

１コンピュータ化システムを有し、
この第２コンピュータ化システムは上記センダによって使用され、そして
上記第２コンピュータ化システムは上記メッセージキーに基づいて上記メッセージを暗号化し、これによって上記センダから上記レシピエントへ機密を保持した状態で上記メッセージを送り、かつ上記レシピエントに上記エンベロープを与え、上記機密を使用して上記エンベロープを開き、上記メッセージキーを検索するとともに上記メッセージを復号することを特徴とするシステム。
【請求項３１】
上記第１コンピュータ化システムはキーサーバであり、そして
上記第２コンピュータ化システムは別個で、このキーサーバから上記メッセージキーを受け取る請求項３０記載のシステム。
【請求項３２】
上記キーサーバは上記メッセージキーのコピーを保存するデータベースを有し、
上記第２コンピュータ化システムは上記キーサーバにレシピエントリストを与え、そして上記キーサーバは上記データベース内にこのレシピエントリストのコピーを保存する請求項３１記載のシステム。
【請求項３３】
認証サーバをさらに有し、そして上記第２コンピュータ化システムは、上記第２コンピュータ化システムに上記メッセージを与える上記キーサーバの条件として、上記認証サーバによって発行されたアサーションに基づく上記キーサーバに上記センダを認証するか、または上記ベラファイヤまたは上記機密のいずれかに関して上記キーサーバが上記認証サーバに要求し、これによって上記キーサーバが上記ベラファイヤを生成する請求項３１記載のシステム。
【請求項３４】
レシピエントが、メッセージキーで機密保護されたメッセージを復号するシステムにおいて、
エンベロープを受け取ることができるコンピュータ化システムを有し、
上記エンベロープは上記レシピエントの機密に基づき、上記機密が上記エンベロープを生成するために使用したベラファイヤに対応し、
上記コンピュータ化システムはさらに上記エンベロープを開き、上記メッセージキーを検索でき、かつ
上記コンピュータ化システムがさらに上記メッセージキーに基づいて上記メッセージを復号できることを特徴とするシステム。
【請求項３５】
上記コンピュータ化システムは、上記メッセージの上記センダから上記エンベロープを受け取る請求項３４記載のシステム。
【請求項３６】
上記コンピュータ化システムは、キーサーバから上記エンベロープを受け取る請求項３４記載のシステム。
【請求項３７】
上記コンピュータ化システムは、上記エンベロープを与える上記キーサーバの条件として、上記レシピエントを認証する請求項３６記載のシステム。
【請求項３８】
上記コンピュータ化システムは、上記キーサーバに認証サーバによって発行される上記レシピエントのアサーションを与える請求項３７記載のシステム。
【請求項３９】
上記認証システムは、上記ベラファイヤを生成し、そして
上記キーサーバは、上記認証サーバから上記ベラファイヤを取得する請求項３８記載のシステム。