(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-534049
(P2005-534049A)
(43)公表日　平成17年11月10日(2005.11.10)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G09C 1/00	G09C 1/00	660E	5J104
G06F 13/00	G06F 13/00	610S	5K030
H04L 12/22	H04L 12/22		

審査請求 未請求　予備審査請求 未請求　（全 16 頁）

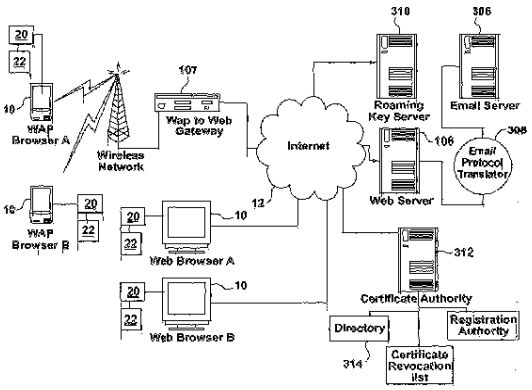
(21)出願番号　特願2004-522069 (P2004-522069)
(86)(22)出願日　平成15年7月23日 (2003.7.23)
(85)翻訳文提出日　平成17年3月18日 (2005.3.18)
(86)国際出願番号　PCT/CA2003/001102
(87)国際公開番号　WO2004/010661
(87)国際公開日　平成16年1月29日 (2004.1.29)
(31)優先権主張番号　2,394,451
(32)優先日　平成14年7月23日 (2002.7.23)
(33)優先権主張国　カナダ(CA)

(71)出願人　505026240
エコーワークス　コーポレイション
カナダ　エム３エム　２エイチ２　オンタリオ　トロント　キール　ストリート　２９５０　ユニット　シー
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100074228
弁理士　今城　俊夫
(74)代理人　100086771
弁理士　西島　孝喜

最終頁に続く

(54)【発明の名称】Ｓ／ＭＩＭＥ暗号化データの配信及び受信のためのシステム、方法、及びコンピュータ製品

(57)【要約】
本発明のシステム、コンピュータ製品、及び方法は、ユーザーが、eメールサーバー上の自分のeメールアカウントにアクセスし、クライアントベースのeメールソフトウェアをインストールする必要なく、任意のブラウザを通してS/MIMEメッセージを作成又は読むことを可能にする。ソフトウェア配信及びユーザーサポートの観点から、これは、一般的には、クライアントベースのeメールをサポートする必要性を取り除き、従って、ユーザー及びソフトウェアサポートのコストを減らし、加えて、ユーザーモビリティをサポートする必要性に応える。本発明のもう1つの側面として、ユーザーが、如何なるネットワーク接続デバイスからもインターネットにより、秘密鍵及びデジタル証明書に、リモートでアクセスすることを可能にする。これは、一般的には、秘密鍵及びデジタル証明書のロケーション固有のストレージの必要性を取り除く。



【特許請求の範囲】
【請求項１】
(a)通信ネットワークを介して、一又はそれ以上のリモートデバイスと通信するための少なくとも1つのネットワーク接続デバイス、
を備え、前記ネットワーク接続デバイスが、
(b)前記ネットワーク接続デバイスにリンクされたブラウザ、
(c)PKIトランザクションを前記ブラウザ内で行うことを可能にするように、前記ブラウザにリンクされた暗号化/復号化機能、及び、
(d)前記暗号化/復号化機能と協力して、前記ブラウザを介して、前記ネットワーク接続デバイスが、S/MIME準拠文書をリモートのネットワーク接続デバイスとやり取りすることを可能にする、前記ブラウザ及び前記暗号化/復号化機能にリンクされたS/MIME機能、
を含むことを特徴とする、S/MIME準拠文書を電子的にやり取りするためのシステム。
【請求項２】
前記システムがまた、
(e)データを暗号化及び復号化するために、各々が、公開鍵基盤内の関連ユーザーによって使用可能である複数の鍵、を格納するためのキーストレージ手段、及び、
(f)前記複数の鍵の中のある鍵の固有ユーザーが、前記鍵の前記関連ユーザーであるかどうかを判断するためのユーザー認証手段、
を備え、前記ユーザー認証手段が、前記ネットワーク接続デバイスのユーザーを認証したとき、前記暗号化/復号化機能が、前記複数の鍵を使ってデータを暗号化及び復号化するように、前記暗号化/復号化機能が、前記キーストレージ手段、及び前記ユーザー認証手段にリンクされた、
請求項1記載のS/MIME文書を電子的にやり取りするためのシステム。
【請求項３】
前記システムがさらに、Eメールサーバーを備え、かつ、前記暗号化/復号化機能及び前記S/MIME機能が、前記ネットワーク接続デバイスと前記eメールサーバーとの間でS/MIME準拠メッセージをやり取りすることを可能にする、
請求項2記載のシステム。
【請求項４】
前記固有ユーザーを認証するために、前記ユーザー認証手段が認証局と通信する、
請求項3記載のシステム。
【請求項５】
前記ユーザー認証手段が、S/MIME準拠文書の送信者を認証し、前記送信者の秘密鍵及び証明書を、前記リモートサーバーを介して前記ネットワーク接続デバイスに伝送するローミングキーサーバーを含む、
請求項4記載のシステム。
【請求項６】
(a)ブラウザ、
(b)PKIトランザクションを前記ブラウザ内で行うことを可能にするように、前記ブラウザにリンクされた暗号化/復号化機能、及び、
(c)ネットワーク接続デバイスが、前記暗号化/復号化機能と協力して、前記ブラウザを介して、S/MIME準拠文書をリモートデバイスとやり取りすることを可能にする、前記ブラウザ及び前記暗号化/復号化機能にリンクされたS/MIME機能、
を備えることを特徴とする、通信ネットワークを介して、前記ネットワーク接続デバイスと前記リモートデバイスの間のS/MIME準拠通信を可能にするために、前記ネットワーク接続デバイス上で動作可能なコンピュータ製品。
【請求項７】
(a)データを暗号化及び復号化するために、各々が、公開鍵基盤内の関連ユーザーによって使用可能である複数の鍵を格納するためのキーストレージ手段、及び、
(b)前記複数の鍵の中のある鍵の固有ユーザーが、前記鍵の前記関連ユーザーである

かどうかを判断するためのユーザー認証手段、
をさらに備え、前記ユーザー認証手段が、前記ネットワーク接続デバイスのユーザーを認証したとき、前記暗号化/復号化機能が、前記複数の鍵を使ってデータを暗号化及び復号化するように、前記暗号化/復号化機能が、前記キーストレージ手段、及び前記ユーザー認証手段にリンクされた請求項6記載のコンピュータ製品。
【請求項８】
前記S/MIME機能がS/MIMEブラウザ拡張機能である、
請求項7記載のコンピュータ製品。
【請求項９】
前記S/MIME機能が、電子メッセージ及び添付ファイルの暗号化及び署名を可能にする、
請求項8記載のコンピュータ製品。
【請求項１０】
前記コンピュータ製品における暗号化動作のセキュリティが維持されるように、前記S/MIME機能を提供する、
請求項9記載のコンピュータ製品。
【請求項１１】
(a)ブラウザにリンクされ、送信者に関連付けられるネットワーク接続デバイス上でロードされる暗号化/復号化機能、及びS/MIME機能を提供し、
(b)前記ネットワーク接続デバイスにリンクされたユーザー認証手段により、リモートサーバーで、前記送信者を認証し、
(c)前記送信者が、前記リモートサーバーから、受信者とのS/MIME準拠通信を要求し、
(d)前記リモートサーバーが、前記受信者の秘密鍵及び証明書を、前記S/MIME機能に伝送し、
(e)前記ネットワーク接続デバイスが、前記受信者の公開鍵及び証明書を確認するために、前記暗号化/復号化機能によって認証局と交信し、及び、
(f)前記送信者の前記秘密鍵及び前記受信者の前記公開鍵を使って、前記ブラウザ内の文書を署名、及び暗号化することにより、前記暗号化/復号化機能、及び前記S/MIME機能によって、S/MIME準拠文書を作成する
ステップを含むことを特徴とする、S/MIME準拠文書を電子的に送信する方法。
【請求項１２】
(a)ブラウザにリンクされ、ネットワーク接続デバイス上でロードされる暗号化/復号化機能、及び、S/MIME機能を提供し、
(b)前記ネットワーク接続デバイスからのS/MIME準拠文書の検索を要求し、
(c)前記ネットワーク接続デバイスと関連付けられる受信者を、リモートサーバーで認証し、
(d)前記リモートサーバーが、送信者の秘密鍵及び証明書を、前記S/MIME機能に伝送し、
(e)前記リモートサーバーが、前記要求されたS/MIME準拠文書を、前記ネットワーク接続デバイスに送信し、
(f)前記暗号化/復号化機能が、前記受信者の秘密鍵及び証明書を、前記ネットワーク接続デバイスからアクセス可能な鍵/証明書記憶機構で格納された前記秘密鍵及び証明書と照らし合わせて認証し、その認証時に、前記秘密鍵及び証明書を前記S/MIME機能に解放し、それにより、前記S/MIME準拠文書を前記ブラウザ内で復号化することを可能にする、
ステップを含むことを特徴とする、S/MIME準拠文書を電子的に検索及び復号する方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的には、公開鍵暗号方式(PKI)でのデータのセキュアな配信及び受信に関するものである。本発明は、特に、インターネットに接続されたweb及びWAPブラウザを

使っての、(電子メールのような)S/MIME暗号化データのセキュアな配信及び受信に関するものである。

【背景技術】

【０００２】

過去10年間で、eメール(電子メール)が一般的に、当事者が労働成果を素早く、簡単に、かつ効率的に伝達することを可能にする非常に貴重なツールとなるにつれて、eメールは、比類のないほど使用されるようになった。eメールが非常に便利な一方で、企業通信が紙からデジタルの形に移行し、ハッカーがeメールシステムに進入することに、より習熟するにつれて、eメールを使って伝達されるデータのセキュリティは、一般的に、懸念を増してきている。(あるレポートの記述によると)会社の知的財産の60%は、そのeメールメッセージシステム内のどこかで、デジタルの形で見つけることができるので、セキュアなeメールメッセ-ジングに対する要求は、特に機密性の高いビジネス情報の場合には、妥当な事柄である。

【０００３】

このeメールセキュリティに対する要求に応えるため、だいたい1995年に、RSAデータセキュリティ及び他のソフトウェアベンダーにより、S/MIME(電子メールの暗号化と認証に関する標準仕様)プロトコルが確立された。S/MIMEの目標は、PKI(公開鍵基盤)暗号化、及び、デジタル署名技術の使用を通して、eメールメッセージのメッセージ整合性、認証、非否認、及び秘匿性を提供することであった。S/MIMEをサポートするeメールアプリケーションは、ネットワーク管理者及びISPのような第三者が、それらのメッセージを傍受する、読む、又は変更することができないことを、保証される。S/MIMEは、主に、普通のMIMEプロトコルの上にセキュリティを構築することにより機能し、これは、電子メッセージを組織化する方式、加えて、殆どのeメールアプリケーションで電子メッセージをサポートする方式を定める。

【０００４】

現在、S/MIMEの最も一般的なバージョンは、V3(バージョン3)であり、これは1999年7月に導入された。S/MIME標準化に関するさらなる情報、及び関連書類は、インターネットメールコンソーシアムのwebサイト(www.imc.org)、及び、IETFのS/MIMEワーキンググループのwebサイト(www.ietf.org/html.charters/smime-charter.html)で見つけることができる。

S/MIME V3標準は、一般的には、以下のプロトコルから構成される、すなわち、

- ●暗号化メッセージ構文(RFC2630)
- ●S/MIMEバージョン3　メッセージ仕様(RFC2633)
- ●S/MIMEバージョン3　認証処理(RFC2632)
- ●ディッフィー-ヘルマン鍵一致方法(RFC2631)

【０００５】

高度セキュリティサービス(RFC2634)が、S/MIMEのもう1つのプロトコルであり、これは、署名付き受信、セキュリティラベル、及びセキュアなメーリングリストを可能にする拡張機能のセットである。署名付き受信、及びセキュリティラベルの拡張機能が、S/MIME V2又はS/MIME V3のいずれかで機能するのに対して、セキュアなメーリングリストの拡張機能は、S/MIME V3で機能するだけである。eメールソフトウェアがS/MIME仕様によってS/MIMEファイルを作成することを必要とすることにより、S/MIMEメッセージをユーザー間でやり取りする。S/MIMEファイルは、eメールメッセージの添付ファイルとして送られる。このメッセージが受信者に到達すると、受信者が、匹敵するバージョンのS/MIME eメールリーダーを所有している場合に、それを処理することができるだけである。

【０００６】

現在のS/MIME標準を用いてeメールメッセージをやり取りすることにおいて、以下のことを含む多数の課題が存在する。受信者が、S/MIMEソフトウェア機能を持たない場合には、S/MIMEメッセージにアクセスできず、そのS/MIMEメッセージは、受信者のコンピューター上で開かれずに格納される。送信者又は受信者のいずれかが、認証局に登録されていな

かった場合も、S/MIME暗号化メッセージは、同様に読むことができない。送信者が使用するS/MIMEのバージョンと、受信者が使用するS/MIMEのバージョンとの間に互換性がない場合にも、同じ結果が起こるであろう。S/MIME標準が、万一セキュリティの穴が検出された場合には、現在のS/MIMEバージョンから変更されたS/MIMEバージョンへの一般的な程度の更新を意図しているという点で、これは特に重要な問題である。送信者又は受信者の各々が使用するeメールソフトウェア間に互換性が無い場合にも、S/MIME eメール交換はまた、妨げられるであろう。S/MIME準拠のeメールソフトウェアが壊れた、又は、送信者又は受信者の鍵の期限が切れた場合にもまた、S/MIME暗号化eメール交換は、効果的に妨げられるであろう。

【０００７】

これらの問題の多くを改善するために、受信者は通常、自分のS/MIMEeメールリーダーを更新又は取得して、S/MIMEプロトコルの最新の標準化バージョンのを利用する。この解決法での問題は、システムリソースを食うことに加えて、常時更新を必要とするかなり大きい追加ソフトウェアパッケージをユーザーがダウンロードすることを必要とする、という事実である。

【０００８】

ブラウザを使ったセキュアなeメールメッセ-ジングのためのS/MIME暗号化の導入は、前述の問題に対して考えられる1つの解決策である。web又はWAPブラウザ技術を用いた従来技術の多数の解決策が、知られている。

【０００９】

例えば、発明者がTumbleweed Communications社のDmitry Dolinsky及びJean-Christophe Bandiniの、2000年7月20日に公開された、特許出願第WO00/42748号(「Tumbleweed」参考文献)は、ユーザー及び受信者が、eメールソフトウェアアプリケーションとは離れた介在のホストサーバーの使用を通して、S/MIMEソフトウェアパッケージをダウンロードする必要を取り除くことを示した、セキュアなwebベースのeメールのための以前の解決策を開示する。この解決策では、介在のホストサーバーが、送信者が送ったeメールを止め、次に、セキュアなeメールが待機中であることを知らせるメッセージを、受信者のeメールアカウントに伝える。このメッセージはまた、介在のホストサーバー上に置かれた復号化されたメッセージへのリンクも含む。その復号化されたメッセージは、SSLセッションで受信者に提示される。

【００１０】

この従来技術の解決策は、多数の短所を持つ。相対的に言えば、介在のホストサーバーの使用は、一般的には、セキュアなトランザクション全体を複雑にし、セキュアなeメールメッセ-ジングを提供するインフラのコストを増大させる。Tumbleweed技術のもう1つの短所は、送信者のコンピューターが暗号化機能を持っていないために、その解決策全体が、かなり侵入しやすいネットワーク環境と関連付けられる関連リスクを負うことである。また、Tumbleerrd参考文献全体で提案された解決策の性質は、有線及び無線ネットワークわたる導入に簡単に備えるものでもない。

【００１１】

それゆえ、必要とされるものは、web及びWAPブラウザを使用して導入するのが容易なS/MIMEを使って、セキュアベースでデータ(eメールを含む)を伝達するためのwebベースのシステム、コンピュータ製品、及び方法である。さらに必要とされるものは、容易に導入され、かつ、S/MIME暗号化メッセ-ジングに必要な暗号化リソースがネットワーク接続デバイス自身において提供されるという点でかなり低コストで導入される前述のシステム、コンピュータ製品、及び方法である。また必要とされるものは、データの通信全体にわたってS/MIME暗号化が持続するwebベースのシステム、コンピュータ製品、及び方法である。

【００１２】

(本発明の要約)

本発明のシステム、コンピュータ製品、及び方法は、ユーザーが、eメールサーバー上の自分のeメールアカウントにアクセスし、クライアントベースのeメールソフトウェアを

インストールする必要なく、任意のブラウザを通してS/MIMEメッセージを作成又は読むことを可能にする。ソフトウェア配信及びユーザーサポートの観点から、これは、一般的には、クライアントベースのeメールをサポートする必要性を取り除き、従って、ユーザー及びソフトウェアサポートのコストを減らし、加えて、ユーザーモビリティをサポートする必要性に応える。

【００１３】

本発明のもう1つの側面として、ユーザーが、如何なるネットワーク接続デバイスからもインターネットにより、秘密鍵及びデジタル証明書に、リモートでアクセスすることを可能にする。これは、一般的には、秘密鍵及びデジタル証明書のロケーション固有のストレージの必要性を取り除く。

【００１４】

次の図面を参照して、例を介してのみ、より好ましい実施形態の詳細な説明を以下に提供する。

【００１５】

本図面では、本発明のより好ましい実施形態を、例を介して示す。本説明及び図面は、例証の目的のためだけのものであり、理解の手助けであるに過ぎず、本発明の限定の解釈を意図するものではないことを明確に理解すべきである。

【００１６】

(より好ましい実施形態の詳細な説明)

図1に示すように、少なくとも1つの既知のネットワーク接続デバイス10が提供される。ネットワーク接続デバイス10は、コンピュータネットワークへの接続性を提供する多数のデジタルデバイスを含むことができる。例えば、ネットワーク接続デバイス10は、既知のパーソナルコンピュータ、又は既知のWAPデバイス、セル電話、PDA等を含むことができる。

【００１７】

ネットワーク接続デバイス10は、既知の手法でインターネット12に接続される。特に図1に関しては、既知のWAPデバイスであるネットワーク接続デバイス10のインターネットへの接続が示されており、それにより、これもまた既知の手法で、既知のWAPからWEBへのゲートウェイ107が提供される。

【００１８】

ネットワーク接続デバイス10の各々はまた、ブラウザ20を含む。ブラウザは、ネットスケープナビゲーター、又は、マイクロソフトのインターネットエクスプローラ、又は、セル電話又はPDAのような無線製品の既知のミニブラウザ、のような標準のインターネットベースのブラウザとすることができる。

【００１９】

ネットワーク接続デバイス10の各々はまた、本発明のアプリケーション22を含む。このアプリケーションの詳細、及び、それが有線及び無線ネットワークによるPKIイネーブルの通信を可能にする手法は、係属中の出願である米国特許出願第10/178,224号(「係属中の出願」)で開示される。

【００２０】

アプリケーション22の特定の一実施形態では、ブラウザ拡張機能、又はプラグインが、既知の手法で提供される。特に、アプリケーション22及びブラウザ20は、例えばカスタマイズされたHTMLタグにより、相互作用する。介在のホストサーバー、又はかなり大きなコンピュータプログラムを使用するのに対し、アプリケーション22が、以下で詳細に説明するように、例えば、ENTRUST、MICROSOFT、BALTIMORE、RSA等を含む如何なるサードパーティPKIシステムでも機能するのに必要なリソースを提供することが望ましい。ここで説明するアプリケーション22の機能はまた、既知の手法で「ACTIVE Xオブジェクト」として提供される、又はブラウザ内に組み込まれることができることもまた、理解すべきである。

【００２１】

ネットワーク接続デバイス10の各々はまた、ブラウザ20を含む。ブラウザは、ネットス

ケープナビゲーター、又は、マイクロソフトのインターネットエクスプローラ、又は、セル電話又はPDAのような無線製品の既知のミニブラウザ、のような標準のインターネットベースのブラウザとすることができる。

【００２２】

ネットワーク接続デバイス10の各々はまた、本発明のアプリケーション22を含む。本発明の特定の一実施形態では、アプリケーション22は、既知の手法で提供されるブラウザ拡張機能、又はプラグインとして最もよく理解される。特に、アプリケーション22及びブラウザ20は、例えばカスタマイズされたHTMLタグにより、相互作用する。

【００２３】

しかしながら、独立型アプリケーションに対して、アプリケーション22のリソースはまた、ブラウザ又はミニブラウザ内のアプリケーション22の機能の統合により提供することができるであろうということもまた、理解すべきである。

【００２４】

アプリケーション22が、以下に詳述するように、例えばENTRUST、MICROSOFT、BALTIMORE、RSA等を含む如何なるサードパーティPKIシステムでも機能するのに必要なリソースを提供することが、望ましい。

【００２５】

アプリケーション22は、既知の手法で提供される暗号化ユーティリティ24を含み、これは、ネットワーク接続デバイス10において一連の暗号化動作を実行するようにされ、以下のものを含むが、これに限られるわけではない。

・書式フィールド内のデータのデジタル署名
・書式フィールド内のデータの暗号化
・書式フィールド内のデータの復号化
・書式フィールド内のデータの署名の確認
・書式フィールド内のデータのデジタル署名及び暗号化
・書式フィールド内のデータのデジタル署名及び復号化の確認
・全ページのデジタル署名
・全ページのデジタル署名の確認
・全ページの暗号化、及び、
・ファイル添付の暗号化及び署名

【００２６】

特に、アプリケーション22は、既知の手法で提供される暗号ライブラリ300を含む。本発明の特定の一実施形態では、アプリケーション22はまた、本発明で意図するデータ文書(eメールを含む)に含まれるデータを暗号化する、及び/又はデジタル署名するのに必要な暗号化データを収容するユーザー証明書及び秘密鍵記憶機構302を含む。例えば、本発明の特定の一実装、すなわち、Entrustが認証局の働きをする実装では、送信者及び受信者の両方を認証するのに必要な.EPFファイルを、ネットワーク接続デバイス10にダウンロードする。.EPFファイルは、暗号化動作を処理するのに必要なユーザー証明書及び秘密鍵にアクセスするために使用される暗号化されたファイルである。

【００２７】

本発明のアプリケーション22はまた、PKIブラウザ拡張機能、特にS/MIMEブラウザ拡張機能304を含む。S/MIMEブラウザ拡張機能は、ここで詳述するように、ブラウザ内のデータ文書(eメールを含む)の暗号化及び復号化を可能にする。ブラウザ技術はありふれたものであるので、これは、広いベースの導入という利点を持つ。図1に示すように、S/MIMEブラウザ拡張機能を含む本発明のアプリケーション22は、webブラウザ又はWAPブラウザと関連付けることができるので、これはまた、無線及び有線ネットワーク全体にわたる導入、という利点も持つ。さらに、各ネットワーク接続デバイス10においてブラウザ及び関連アプリケーション22のみを必要とする、ここで開示された発明では、ネットワーク接続デバイス10上で完全S/MIME暗号化プログラム/eメールのリーダーを実行するのために通常必要とされるリソースを用いることなく、S/MIME暗号化通信が可能である。

【００２８】
S/MIMEブラウザ拡張機能304は、熟練したプログラマーに知られた手法で提供される。しかしながら、本発明のS/MIMEブラウザ拡張機能304が、多数の特性を持つことが望ましい。第一に、以下に説明する本発明の方法の結果として、S/MIMEブラウザ拡張機能304が、eメールメッセージに添付ファイルを添付し、かつ、eメールメッセージ全体がS/MIMEメッセージとなるようにeメールメッセージ及び添付ファイルの両方を署名及び暗号化できることが望ましい。第二に、ここで説明するS/MIME標準によるデータの暗号化及び復号化は、S/MIMEブラウザ拡張機能304が正しく設計されない場合には、潜在的なセキュリティリスクを含む。特に、セキュリティが甘くならないように、暗号化動作の過程でブラウザメモリを利用することを確実にすることが、必須である。本発明の特定の一実施形態では、熟練したプログラマに知られた手法でブラウザ20の「TEMP」メモリ空間を使用することにより、これを実現する。第三に、S/MIMEブラウザ拡張機能304はさらに、秘密性を維持するために、ブラウザと関連付けられたメモリからユーザー証明書及び秘密鍵記憶機構302の一部であるメッセージ、又は、ユーザー証明書又は秘密鍵のいずれかの如何なる残物も取り除く、又は、ネットワーク接続デバイス10を用いた別のやり方で取り除く、既知の手法でのクリーンアップルーチンを含む。

【００２９】
さらに、S/MIMEブラウザ拡張機能304が、本発明のアプリケーションのベンダーとは関連のない実体で発行されたデジタル証明書の承認を助け、かつ、これはまた既知の手法で「相互認証」されるものではないことを、本発明は意図している。特に、S/MIMEブラウザ拡張機能304は、本発明のアプリケーション22のユーザーが、このアプリケーション22のベンダーと関連のないユーザーの人々のデジタル証明書及び公開鍵を格納することを可能にするようにされる。

【００３０】
また、既知の手法でネットワーク接続デバイス10の供給を可能にするように、既知のハードウェア及びソフトウェアユーティリティを使用して提供されるwebサーバー106が、インターネット12に接続される。Webサーバー106は、webアプリケーション16を含む。webアプリケーション16は、以下で参照するPKI動作を含む動作を実行するようにされる。

【００３１】
本発明の2つの側面は、
1. S/MIME準拠eメールメッセージを作成し、eメールサーバーに配信する、及び、
2. S/MIME準拠eメールメッセージをeメールサーバーから検索し、復号する
ためのシステム、コンピュータ製品、及び方法を含む。

【００３２】
前述の事項を実現するために、本発明のシステム、コンピュータ製品、及び方法は、PKIイネーブルのトランザクションをするための係続中の出願の側面に依存する。特に、eメールメッセージは、係続中の出願で説明する「セキュアベースのデータのポスティング」と類似の手法で、本発明により、作成及び配信される。eメールメッセージは、これもまた係続中の特許出願で説明する「セキュアベースのデータの検索」と類似の手法で、検索及び復号される。本発明のアプリケーション22で暗号化動作を処理する手法の詳細に関しては、その係続中の特許出願を参照する。

【００３３】
図1に示すように、本発明のシステムの一側面はまた、既知のeメールサーバー306も含む。eメールサーバー306は、良く知られた手法で、eメールを送信及び受信する。Eメールサーバー306は、既知のハードウェア及びソフトウェアユーティリティによって提供される。また図1に示すように、本発明のシステムの一側面は、eメールプロトコル変換機構308を含む。eメールプロトコル変換機構308は、webサーバー106及びeメールサーバー306が、webサーバー106で送信されたメッセージを、例えばPOP3又はIMAP4のような、eメールサーバー306で理解される特定のeメールプロトコルに変換することによって通信することを可能にする既知のユーティリティである。

【００３４】
S/MIME準拠Eメールメッセージを作成し、Eメールサーバーに配信する
図3は、本発明による、S/MIME準拠eメールメッセージの作成、及びeメールサーバーへの配信を示している。
【００３５】
セキュアベースでeメールを作成及び送信することを望む、ネットワーク接続デバイス10と関連付けられるユーザー(「送信者」)は、ネットワーク接続デバイス10上でロードされたブラウザ20を使って、webサーバー106上のページを要求する。
【００３６】
webサーバー106は、詳細にはwebサーバー106でロードされたwebアプリケーション16と協力して、webアプリケーション16、特にwebアプリケーション16内に含まれるweb eメールアプリケーション(示されていない)へのアクセスを獲得するために、ネットワークデバイス10と関連付けられたユーザーが認証を提供することを必要とするwebフォームであるwebページを表示することにより、ネットワーク接続デバイス10に答える。
【００３７】
送信者は、webページ上の(ユーザー名及びパスワードのような)認証フォームフィールド内の情報を提供し、典型的には「送信」ボタン又はそれと等価なものを押すことにより、そのフォームを送信することで締めくくる。
【００３８】
認証証明書が、webサーバー106に送られる。次に、webサーバー106は、eメールプロトコル変換機構308を介して、その認証証明書をeメールサーバー306に配信する。
【００３９】
特に、ユーザー証明書及び秘密鍵記憶機構302にアクセスするためにローミングキーサーバー310を使用する本発明の側面により、webサーバー106はまた、ユーザー証明書をローミングキーサーバー310に転送する。
【００４０】
eメールサーバー306は送信者を認証し、次に、送信者のブラウザ20内での伝達表示のため、メッセージ待ちリスト、及び、送信者のeメールアカウントについての他の関連情報を、eメールプロトコル変換機構308を通してwebサーバー106に送り返し、既知の手法で、典型的にはクッキーを使ってeメールセッションを確立する。
【００４１】
再び、ローミングキーサーバー310を利用する本発明の側面により、ローミングキーサーバー310は送信者を認証し、webサーバー106を通して、送信者の秘密鍵及び証明書をS/MIMEブラウザ拡張機能304に伝送する。ユーザー証明書及び秘密鍵記憶機構がネットワーク接続デバイス10にある本発明の側面により、S/MIMEブラウザ拡張機能304が、その秘密鍵及び証明書にアクセスする。
【００４２】
送信者は、例えばメッセージの題名、本文、及び、意図する受信者フィールドを含む、参照したwebフォームの適切なフィールドを完成させることにより、eメールメッセージを用意する。本発明の特定の一実施形態では、アプリケーション22はまた、受信者パスワードも提供する。
【００４３】
認証局312と交信し、それにより、受信者の公開鍵及び証明書を確認し、関連ディレクトリ314から検索する。
【００４４】
送信者の秘密鍵、及び、受信者の公開鍵を使って、メッセージ及び如何なる添付ファイルも署名及び暗号化するために、及び、S/MIME準拠eメールメッセージを形成するように、メッセージフォームのデータが、S/MIMEブラウザ拡張機能304を含むアプリケーション22に送られる。
【００４５】

メッセージはブラウザ20に返され、ブラウザ20からwebサーバー106に送られ、かつ、識別された受信者に転送するために、eメールプロトコル変換機構308を使ってeメールサーバー306に送られる。

【００４６】

S/MIME準拠eメールメッセージを、eメールサーバーから検索し、復号する

図2は、本発明による、eメールサーバーからのS/MIME準拠メッセージの受信、確認、復号、及び表示を示している。

【００４７】

セキュアベースで受信したセキュアなS/MIME準拠メッセージを表示することを望む、ネットワーク接続デバイス10と関連付けられるユーザー(「受信者」)は、ネットワーク接続デバイス10上でロードされたブラウザ20を使用して、webサーバー106上のページを要求する。

【００４８】

webサーバー106は、具体的にはそのwebサーバー106上でロードされたwebアプリケーション16と協力して、webアプリケーション16、特に、webアプリケーション16内に含まれるweb eメールアプリケーション(示されていない)へのアクセスを獲得するために、受信者が認証を提供することを必要とするwebフォームであるwebページを表示することによって、ネットワーク接続デバイス10に答える。

【００４９】

受信者は、webページ上の(ユーザー名及びパスワードのような)認証フォームフィールド内の情報を提供し、典型的には「送信」ボタン又はそれと等価なものを押すことにより、そのフォームを送信することで締めくくる。

【００５０】

認証証明書が、webサーバー106に送られる。次にwebサーバー106は、その認証証明書を、eメールプロトコル変換機構308を介してeメールサーバー306に配信する。

【００５１】

特に、ユーザー証明書及び秘密鍵記憶機構302にアクセスするためにローミングキーサーバー310を使用する本発明の側面により、webサーバー106はまた、ユーザー証明書をローミングキーサーバー310に転送する。

【００５２】

eメールサーバー306は受信者を認証し、次に、受信者のブラウザ20内での伝達表示のために、eメールプロトコル変換機構308を通して、メッセージ待ちリスト、及び、受信者のeメールアカウントについての他の関連情報をwebサーバー106に送り返し、既知の手法で、典型的にはクッキーを使ってeメールセッションを確立する。

【００５３】

eメールサーバーは受信者を認証し、次に、受信者のブラウザ20内での伝達表示のために、eメールプロトコル変換機構308を通して、メッセージ待ちリスト、及び、受信者のeメールアカウントについての他の関連情報をwebサーバー106に送り返し、典型的にはクッキーを使って、eメールセッションを確立する。

【００５４】

再び、ローミングキーサーバー310を利用する本発明の側面により、ローミングキーサーバー310は受信者を認証し、受信者の秘密鍵及び証明書を、webサーバー106を通してS/MIMEブラウザ拡張機能304に伝送する。ユーザー証明書及び秘密鍵記憶機構がネットワーク接続デバイス10にある本発明の側面により、S/MIMEブラウザ拡張機能304が、秘密鍵及び証明書にアクセスする。

【００５５】

受信者は、そのメッセージ要求と共に、どの要求がwebサーバー106に送られ、eメールプロトコル変換機構308を通してeメールサーバー306に送られたかを読み取るためのメッセージを要求する。

【００５６】

eメールサーバー306はメッセージを検索し、受信者へのメッセージを、eメールプロトコル変換機構308を使って、webサーバー106を通して受信者のブラウザ20に伝送する。

【００５７】

アプリケーション22は、そのユーザー証明書及び秘密鍵記憶機構302と対照して認証し、それにより、鍵を、メッセージ署名を確認できた時に、受信者のブラウザ20で表示するためにメッセージを復号化するそのS/MIMEブラウザ拡張機能304コンポーネントに解放する。代わりに、ローミングキーサーバー310を利用する本発明の側面により、メッセージ署名を確認でき、S/MIMEブラウザ拡張機能304でメッセージを復号化できるローミングキーサーバー310で提供されたデータと対照して、認証が生じる。

【００５８】

本発明のもう1つの側面として、係続中の出願で開示された永続的なフィールドレベルの暗号化を、本発明の目的のため、関連データを暗号化し、webサーバー106と関連付けられたデータベース(示されていない)においてデータを暗号化された形で格納することにより、ユーザーの身元情報(例えば、本発明により、セキュアベースでユーザーが通信するクライアント)、及び他の個人情報の秘密性を維持するために使用する。

【００５９】

本発明のシステムは、ネットワーク接続デバイス10及びそのリソースを含み、アプリケーション22、webサーバー106、eメールサーバー306、及びこれらのリソースも同様に含むシステム全体として最もよく理解される。本発明のコンピュータ製品は、一方ではアプリケーション22であり、また他方ではwebアプリケーション16でもある。本発明のもう1つの側面は、リモートキーサーバー310を含む。

【００６０】

本発明の方法は、webブラウザ又はWAPブラウザのいずれかのブラウザを通して、PKI S/MIMEメッセージをやり取りするための処理として、最も良く理解される。また、本発明の方法は、S/MIMEを使ってインターネットセキュアメッセ-ジングと無線デバイスを融合させる方法として理解されるべきである。本発明の方法のもう1つの側面は、インターネット又は無線ネットワークを通して、秘密鍵及び証明書を配信する方法である。本発明のさらにもう1つの側面は、S/MIMEを使って永続的セキュアなデータ通信を提供することにより、インターネットと無線ネットワークの間のプロキシベースのゲートウェイの「中間人」セキュリティホールを取り除く方法である。本発明のさらに他の側面は、webサーバーと無線デバイスの間で、永続的ベースでS/MIME暗号化を提供するように、PKIを無線デバイスに提供するように、データリソースを割り当てる方法である。

【００６１】

本発明はまた、インターネットベースのデータ処理全体にわたって、選択的ベースで、S/MIMEを使う永続的フィールドレベルの暗号化に備えるものである。これは、セキュリティ/認証を最も必要とするインターネットベースのデータ処理の特定の要素について、PKI動作を起動することにより、リソースの有効利用を促進する。

【００６２】

本発明はまた、効率的な手法でPKI S/MIME機能をブラウザに追加するツールのセットを提供する。

【００６３】

本発明はまた、S/MIMEを組み込んだwebメールシステムを使用する無線デバイスに関連することを含む、正規のデジタル署名要求に適合するためのツールのセットとして理解すべきである。

【００６４】

本発明のさらに他の側面は、S/MIMEを使って、無線ネットワークと、インターネットベースのネットワーク又はその他のネットワークとの間のセキュアなeメールメッセ-ジングを可能にする方法である。

【図面の簡単な説明】

【００６５】

【図１】S/MIMEブラウザベースのeメールシステムの、システムアーキテクチャのコンポーネントの概略図である。
【図１ａ】本発明のアプリケーションのリソースを示すプログラムリソースのチャートである。
【図２】ブラウザ内で表示するために、eメールサーバーからS/MIMEメッセージを受信し、確認し、復号化するステップを示すフローチャートである。
【図３】eメールサーバーへ向かうwebサーバーへ伝達するために、ブラウザ内のS/MIMEメッセージを作成し、署名し、暗号化するステップを示すフローチャートである。
【図４】暗号化されていないメッセージを作成、署名、及び暗号化することに関連する詳細なステップの概略図である。
【図５】暗号化されたメッセージを検索、及び復号することに関連する詳細なステップの概略図である。

【図１】

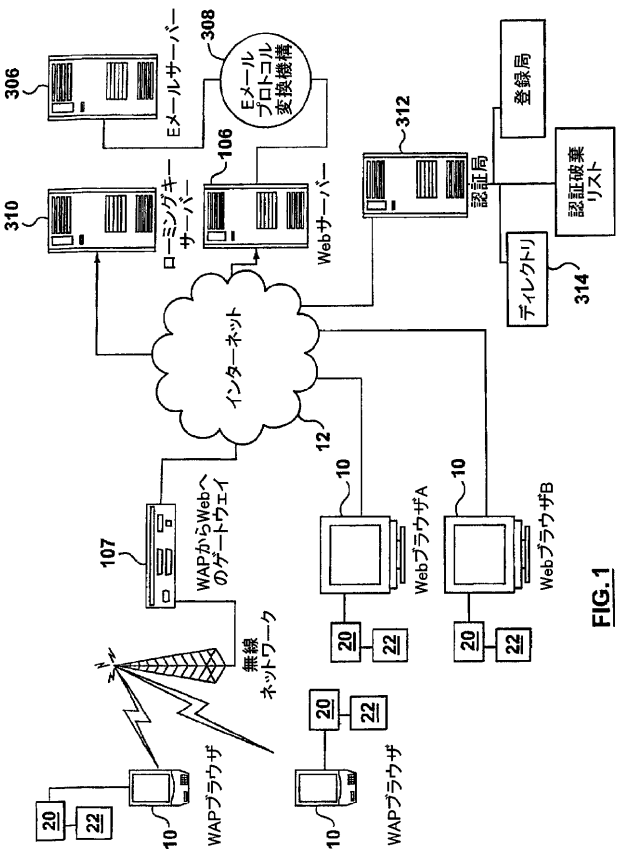


FIG. 1

【図１ａ】

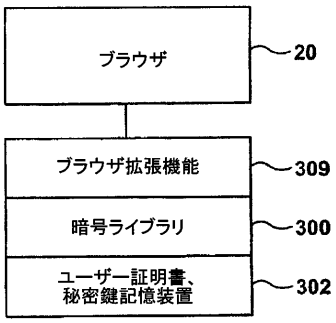


FIG. 1A

【図２】

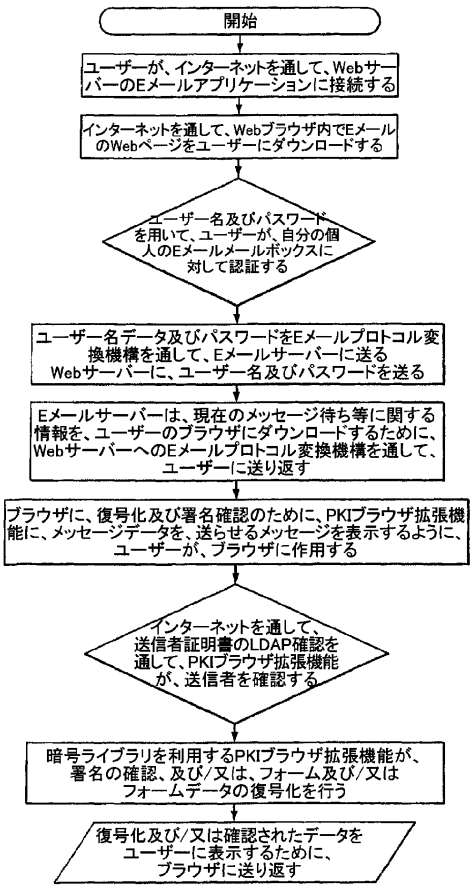


FIG. 2

【図３】

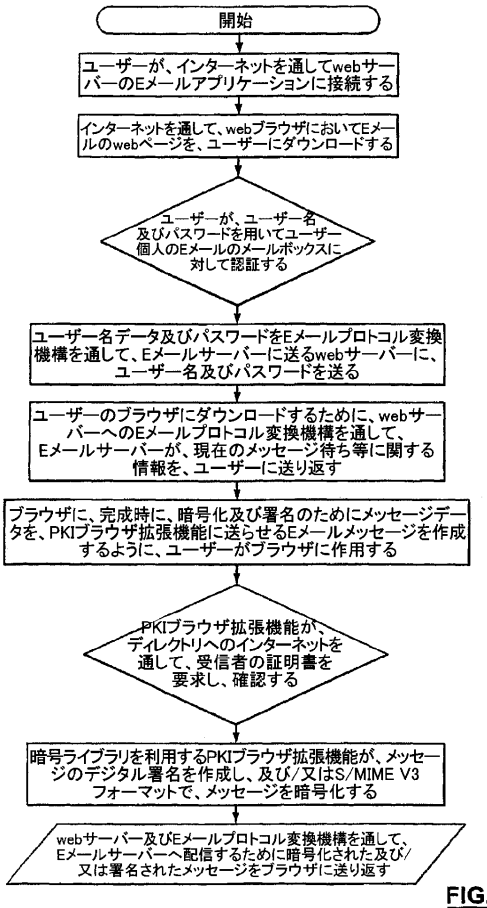


FIG. 3

【図４】

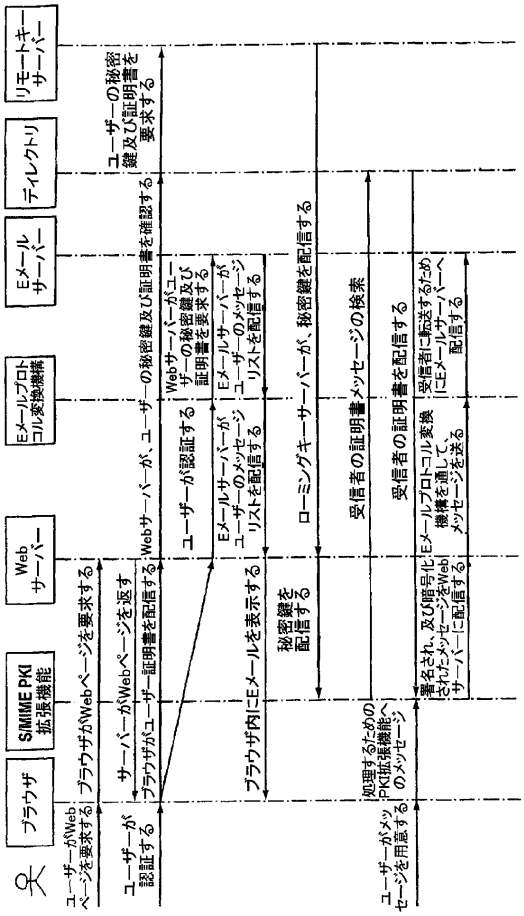


FIG. 4

【図５】

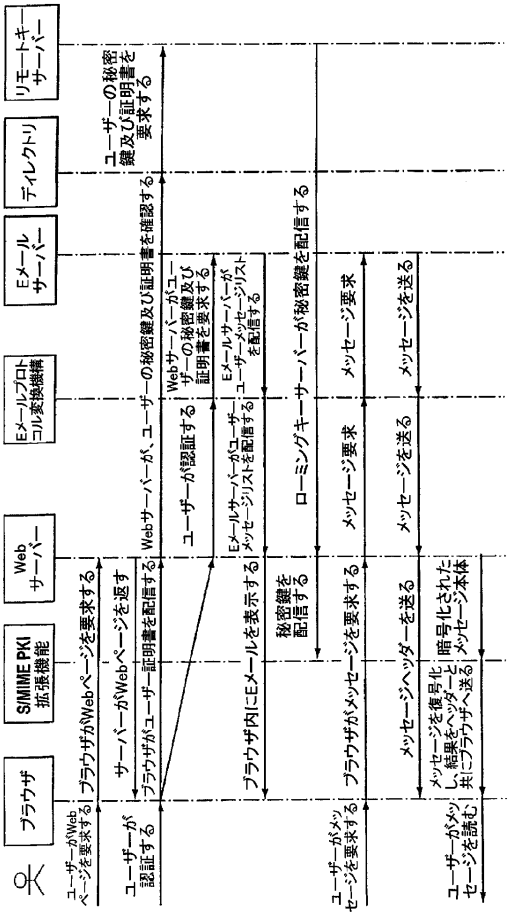


FIG. 5

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 03/01102

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/58 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 97089 A (COOK DAVID P ;ZIXIT CORP (US)) 20 December 2001 (2001-12-20) page 2, line 2 -page 3, line 19 page 17, line 25 -page 20	1-12
A	STALLINGS W: "S/MIME: E-MAIL GETS SECURE" BYTE, MCGRAW-HILL INC. ST PETERBOROUGH, US, vol. 23, no. 7, 1 July 1998 (1998-07-01), pages 41-42, XP000774260 ISSN: 0360-5280 /* the whole article */	1-12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 November 2003	02/12/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Veen, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 03/01102

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0197089 A	20-12-2001	AU 6697101 A	24-12-2001
		EP 1311984 A1	21-05-2003
		WO 0197089 A1	20-12-2001

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 ウォー ドナルド
カナダ エル６ジェイ ５ケイ８ オンタリオ オークヴィル キャンタベリー クレッセント ４３３
(72)発明者 ロバーツ マイケル
カナダ エル４ジェイ ７イー６ オンタリオ ソーンヒル マウントフィールド クレッセント ５６
(72)発明者 ヴィアチェスラヴ イヴァノフ
カナダ エル４ジェイ ５ジー１ オンタリオ ソーンヒル ジョアンナ クレッセント １０１

Ｆターム(参考) 5J104 AA07 AA16 EA04 EA15 JA21 KA01 KA05 LA03 MA01 MA05
NA02 NA37 PA08
5K030 GA15 HA08 HC01 HD03 HD06 KA05