(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2006-525686
(P2006-525686A)
(43)公表日　平成18年11月9日(2006.11.9)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	***(2006.01)***	H04L	9/00	675A	5J104

審査請求 有　予備審査請求 未請求　（全 28 頁）

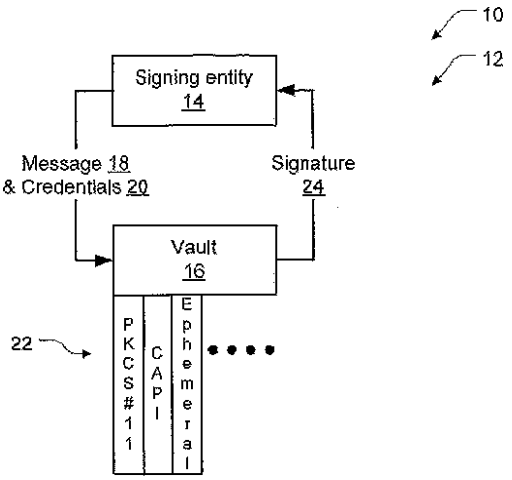
(21)出願番号	特願2004-571687 (P2004-571687)
(86)(22)出願日	平成15年6月25日 (2003.6.25)
(85)翻訳文提出日	平成17年11月1日 (2005.11.1)
(86)国際出願番号	PCT/US2003/019954
(87)国際公開番号	WO2004/100439
(87)国際公開日	平成16年11月18日 (2004.11.18)
(31)優先権主張番号	10/249,717
(32)優先日	平成15年5月2日 (2003.5.2)
(33)優先権主張国	米国 (US)

(71)出願人　503140344
セキュア　データ　イン　モーション，インコーポレイテッド
アメリカ合衆国　カリフォルニア州　９４４０２，サン　マテオ，テンス　フロアー，エス．グラント　ストリート　１８７５
1875 S. Grant Street, 10th Floor, San Mateo, CA 94402 USA
(74)代理人　100079980
弁理士　飯田　伸行
(72)発明者　オルキン，テリー，エム．
アメリカ合衆国　カリフォルニア州　９５０３２，ロス　ガトス，リージェント　ドライブ　１０４

最終頁に続く

(54)【発明の名称】会話型メッセージを対象とするデジタル式シグネーチャ／ベリファイシステム

(57)【要約】
【構成】デジタルシグネーチャベリファイシステムである。チャットダイアログ、ＩＭダイアログあるいはＥＩＭダイアログで使用されているようにシグネーチャシステムが会話型メッセージに署名する。次に、ベリファイシステムがこのシグネーチャをベリファイする。このシグネーチャシステムは署名エンティティ１４およびボールト１６をもつ。署名エンティティがメッセージおよびクレデンシャルを与え、ボールトがメッセージの第１ハッシュに基づいてシグネーチャ２４を生成し、これをシグネーチャキーで暗号化する。ベリファイシステムは、検証エンティティおよびベリファイヤをもつ。検証エンティティがメッセージ、シグネーチャおよびアサーションをベリファイヤに与え、次にこのベリファイヤがメッセージの第２ハッシュを生成し、シグネーチャキーに対応するベリファイキーを使用してシグネーチャを復号し、第１ハッシュを得てから、これら２つのハッシュを比較し、適正な検証レスポンスを求める。



【特許請求の範囲】
【請求項１】
会話型メッセージの通信方法において、
第１のコンピュータ化システムで、上記会話型メッセージに基づいて第１ハッシュ値を計算するステップ、
第２のコンピュータ化システムで、シグネーチャキーに基づいて上記第１ハッシュ値を暗号化することによってデジタルシグネーチャを生成するステップ、
ネットワークを介して、上記デジタルシグネーチャを第３のコンピュータ化システムに通信するとともに、上記会話型メッセージを第４のコンピュータ化システムに通信するステップ、
上記第３のコンピュータ化システムで、ベリファイキーに基づいて上記デジタルシグネーチャを復号して上記第１ハッシュ値を再生するステップ、
第４のコンピュータ化システムで、上記会話型メッセージに基づいて第２ハッシュ値を計算するステップ、および
第５のコンピュータ化システムで、上記第１ハッシュ値と上記第２ハッシュ値とを比較して検証レスポンスを求めるステップからなり、
上記検証レスポンスが、上記第１ハッシュ値と上記第２ハッシュ値とが一致したときに、検証すべき会話型メッセージを示し、および上記第１のコンピュータ化システムおよび上記第２のコンピュータ化システムとして同じか同一でないシステムを利用し、かつ上記第３のコンピュータ化システム、上記第４のコンピュータ化システムおよび上記第５のコンピュータ化システムとしてすべて同じシステムを利用するか、一部のシステムとして同じシステムを利用するか、あるいはすべて同一でないシステムを利用することを特徴とする会話型メッセージの通信方法。
【請求項２】
会話型メッセージを対象とするデジタルシグネーチャの生成方法において、
第１のコンピュータ化システムで、上記会話型メッセージに基づいてハッシュ値を計算するステップ、および
第２のコンピュータ化システムで、シグネーチャキーに基づいて上記ハッシュ値を暗号化することによって上記デジタルシグネーチャを生成するステップからなり、
上記第１のコンピュータ化システムおよび上記第２のコンピュータ化システムとして同じか同一でないシステムを利用することを特徴とする会話型メッセージを対象とするデジタルシグネーチャの生成方法。
【請求項３】
上記会話型メッセージを署名エンティティによって署名し、そしてさらにこの署名エンティティを認証するステップをもつ請求項２の方法。
【請求項４】
上記認証ステップで、上記署名エンティティの私的クレデンシャルを検証する請求項３の方法。
【請求項５】
さらに、上記署名エンティティから物理的に離間しているサーバから上記シグネーチャキーを生成するステップをもつ請求項３の方法。
【請求項６】
さらに、上記シグネーチャキーを発生するステップをもつ請求項３の方法。
【請求項７】
上記シグネーチャキーが、ＰＫＩ環境で発行されたＸ．５０９サーティフィケートから得られたものでない請求項２の方法。
【請求項８】
少なくとも、上記の暗号化ステップをボールトで行う請求項２の方法。
【請求項９】
上記ボールトで、上記ボールトから物理的に離間したサーバから上記シグネーチャキー

を取得する請求項８の方法。
【請求項１０】
会話型メッセージユニットを署名エンティティによって署名し、そして
上記暗号化ステップを実行する前に、上記ボールトが上記署名エンティティを認証する請求項８の方法。
【請求項１１】
上記ボールトが上記署名エンティティから物理的に離間し、そしてネットワークを介して上記署名エンティティおよび上記ボールトが通信する請求項８の方法。
【請求項１２】
上記会話型メッセージが複数の会話型メッセージユニットを有し、そして
上記計算ステップおよび上記暗号化ステップを上記複数の会話型メッセージユニットに基づいて一括的に行う請求項２の方法。
【請求項１３】
さらに、ダイアログにおける会話型メッセージ要素の中から上記複数の会話型メッセージユニットを選択する請求項１２の方法。
【請求項１４】
さらに、トランスクリプトを記憶するステップをもち、このトランスクリプトが上記会話型メッセージ要素を有する請求項１３の方法。
【請求項１５】
会話型メッセージを対象とするデジタルシグネーチャの検証方法において、
第１のコンピュータ化システムで、検証キーに基づいて上記デジタルシグネーチャを復号して第１ハッシュ値を再生するステップ、
第２のコンピュータ化システムで、上記会話型メッセージに基づいて第２ハッシュ値を計算するステップ、および
第３のコンピュータ化システムで、上記第１ハッシュ値と上記第２ハッシュ値とを比較して検証レスポンスを求めるステップからなり、
上記検証レスポンスが、上記第１ハッシュ値と上記第２ハッシュ値とが一致したときに、検証すべき会話型メッセージを示し、そして上記第１のコンピュータ化システム、上記第２のコンピュータ化システムおよび上記第３のコンピュータ化システムとしてすべて同じシステムを利用するか、一部のシステムとして同じシステムを利用するか、あるいはすべて同一でないシステムを利用することを特徴とするデジタルシグネーチャの検証方法。
【請求項１６】
上記会話型メッセージを検証エンティティによって検証し、そしてさらにこの検証エンティティを認証するステップをもつ請求項１５の方法。
【請求項１７】
上記認証ステップが、上記検証エンティティのアサーションを有する請求項１６の方法。
【請求項１８】
さらに、上記検証エンティティから物理的に離間しているサーバから上記アサーションを求めるステップをもつ請求項１７の方法。
【請求項１９】
さらに、上記検証エンティティから物理的に離間しているサーバから上記ベリファイキーを取得するステップをもつ請求項１６の方法。
【請求項２０】
上記検証キーが、ＰＫＩ環境で発行されたＸ．５０９サーティフィケートから得られたものでない請求項１５の方法。
【請求項２１】
少なくとも、上記復号ステップをベリファイヤで行う請求項１５の方法。
【請求項２２】
上記ベリファイヤが、このベリファイヤから物理的に離間しているサーバから上記ベリ

ファイヤキーを取得する請求項２１の方法。
【請求項２３】
上記デジタルシグネーチャを検証エンティティによって検証し、そして
上記復号ステップを実行する前に、上記ベリファイヤがこの検証エンティティを認証する請求項２１の方法。
【請求項２４】
上記ベリファイヤが上記検証エンティティから物理的に離間し、そしてネットワークを介して上記検証エンティティおよび上記ベリファイヤが通信する請求項２３の方法。
【請求項２５】
さらに上記検証レスポンスを第３者に通信するステップをもつ請求項１５の方法。
【請求項２６】
さらに上記第１ハッシュ値および上記第２ハッシュ値を第３者に通信するステップをもつ請求項１５の方法。
【請求項２７】
上記会話型メッセージがダイアログにおいて少なくとも一つの会話型メッセージ要素を有し、そしてさらに、上記会話型メッセージ要素を有するトランスクリプトを記憶するステップをもつ請求項１５の方法。
【請求項２８】
会話型メッセージを対象とするデジタルシグネーチャを生成するために、コンピュータ読み取り式記憶媒体で実行するコンピュータプログラムにおいて、
上記会話型メッセージに基づいてハッシュ値を計算するコードセグメント、および
シグネーチャキーに基づいてこのハッシュ値を暗号化するコードセグメントをもち、
上記計算セグメントおよび上記暗号化セグメントの両者が同じコンピュータ化システムを走るか、あるいは走らないことを特徴とするコンピュータプログラム。
【請求項２９】
上記会話型メッセージを署名エンティティによって署名し、そしてさらにこの署名エンティティを認証するコードセグメントをもつ請求項２８のコンピュータプログラム。
【請求項３０】
上記認証コードセグメントも、上記署名エンティティの私的クレデンシャルを検証する請求項２９のコンピュータプログラム。
【請求項３１】
さらに、上記署名エンティティから物理的に離間したサーバから上記シグネーチャキーを取得するコードセグメントをもつ請求項２９のコンピュータプログラム。
【請求項３２】
さらに、上記シグネーチャキーを発生するコードセグメントをもつ請求項２８のコンピュータプログラム。
【請求項３３】
さらに、ボールトを与えるコードセグメントをもち、少なくとも暗号化する上記コードセグメントがこのボールトで暗号化を行う請求項２８のコンピュータセグメント。
【請求項３４】
上記ボールトが、このボールトから物理的に離間したサーバから上記シグネーチャキーを取得する請求項３３のコンピュータプログラム。
【請求項３５】
上記会話型メッセージユニットを署名エンティティによって署名し、そして
上記暗号化コードセグメントが暗号化を行う前に、上記ボールトが上記署名エンティティを認証する請求項３３のコンピュータプログラム。
【請求項３６】
上記ボールトが上記署名エンティティから物理的に離間し、そして上記署名エンティティおよび上記ボールトがネットワークを介して通信する請求項３４のコンピュータプログラム。

【請求項３７】
さらに、複数の会話型メッセージユニットを有するように上記会話型メッセージを定義するコードセグメントをもち、
上記計算コードセグメントおよび上記暗号化コードセグメントがこれら複数の会話型メッセージユニット上で一括動作する請求項２８のコンピュータプログラム。
【請求項３８】
上記の会話型メッセージを定義するコードセグメントが、ダイアログにおいて会話型メッセージ要素の中から上記複数の会話型メッセージユニットを選択する請求項３７のコンピュータプログラム。
【請求項３９】
さらに、トランスクリプトを記憶するコードセグメントをもち、このトランスクリプトが上記会話型メッセージ要素を有する請求項３８のコンピュータプログラム。
【請求項４０】
会話型メッセージを対象とするデジタルシグネーチャを検証するコンピュータプログラムにおいて、
ベリファイキーに基づいて上記デジタルシグネーチャを復号して第１ハッシュ値を再生するコードセグメント、
上記会話型メッセージに基づいて第２ハッシュ値を計算するコードセグメント、および
上記第１ハッシュ値と上記第２ハッシュ値とを比較して検証レスポンスを求めるコードセグメントからなり、
上記検証レスポンスが、上記第１ハッシュ値と上記第２ハッシュ値とが一致したときに、検証すべき会話型メッセージを示し、そして上記復号コードセグメント、上記計算セグメントおよび上記比較コードセグメントのすべて、あるいは一部が同じコンピュータ化システムを走るか、あるいはいずれもが走らないことを特徴とするコンピュータプログラム。

【請求項４１】
上記会話型メッセージを検証エンティティによって検証し、そしてさらにこの検証エンティティを認証するコードセグメントをもつ請求項４０のコンピュータプログラム。
【請求項４２】
上記認証コードセグメントが上記検証エンティティのアサーションを検証する請求項４１のコンピュータプログラム。
【請求項４３】
上記検証エンティティから物理的に離間しているサーバから上記アサーションを求めるコードセグメントをもつ請求項４２のコンピュータプログラム。
【請求項４４】
上記検証エンティティから物理的に離間しているサーバから上記ベリファイキーを取得するコードセグメントをもつ請求項４１のコンピュータプログラム。
【請求項４５】
さらにベリファイヤを与えるコードセグメントをもち、このベリファイヤで少なくとも上記復号コードセグメントが復号を行う請求項４０のコンピュータプログラム。
【請求項４６】
上記ベリファイヤが、このベリファイヤから物理的に離間しているサーバから上記ベリファイキーを取得する請求項４５のコンピュータプログラム。
【請求項４７】
上記デジタルシグネーチャを検証エンティティによって検証し、そして
上記復号コードセグメントを実行する前に、上記ベリファイヤがこの検証エンティティを認証する請求項４５のコンピュータプログラム。
【請求項４８】
上記ベリファイヤが上記検証エンティティから物理的に離間し、そしてネットワーク

を介して上記検証エンティティおよび上記ベリファイヤが通信する請求項４７のコンピュータプログラム。
【請求項４９】
さらに上記検証レスポンスを第３者に通信するコードセグメントをもつ請求項４０のコンピュータプログラム。
【請求項５０】
さらに上記第１ハッシュ値および上記第２ハッシュ値を第３者に通信するコードセグメントをもつ請求項４０のコンピュータプログラム。
【請求項５１】
上記会話型メッセージがダイアログにおいて少なくとも一つの会話型メッセージ要素を有し、そしてさらに上記会話型メッセージ要素を有するトランスクリプトを記憶するコードセグメントをもつ請求項４０のコンピュータプログラム。
【請求項５２】
会話型メッセージを対象とするデジタルシグネーチャの生成装置において、
この会話型メッセージに基づいてハッシュ値を計算できるロジックをもつ第１のコンピュータ化システム、および
シグネーチャキーに基づいてこのハッシュ値を暗号化することによって上記デジタルシグネーチャを生成できるロジックをもつ第２のコンピュータ化システムからなり、
上記第１のコンピュータ化システムおよび上記第２のコンピュータ化システムの両者を同じシステムとして構成するか、同一でないシステムとして構成したことを特徴とする生成装置。

【請求項５３】
上記会話型メッセージを署名エンティティによって署名し、そしてさらに上記第２のコンピュータ化システムがネットワークを介してサーバで上記署名エンティティを認証できるロジックを有する請求項５２の生成装置。
【請求項５４】
上記の認証ロジックも上記署名エンティティの私的クレデンシャルを検証する請求項５２の生成装置。
【請求項５５】
上記第２のコンピュータ化システムが、さらにネットワークを介してサーバから上記シグネーチャキーを取得できるロジックをもつ請求項５２の生成装置。
【請求項５６】
上記第２のコンピュータ化システムが、さらに上記シグネーチャキーを生成できるロジックをもつ請求項５２の生成装置。
【請求項５７】
上記第２のコンピュータ化システムがボールトで上記ハッシュ値を暗号化する請求項５２の生成装置。
【請求項５８】
上記ボールトが、このボールトから物理的に離間しているサーバから上記シグネーチャキーを取得する請求項５２の生成装置。
【請求項５９】
上記会話型メッセージユニットを署名エンティティによって署名し、そして上記第２のコンピュータ化システムが、さらにネットワークを介してサーバで上記ボールトの上記署名エンティティを認証できるロジックをもつ請求項５８の生成装置。
【請求項６０】
上記第２のコンピュータ化システムが、さらにネットワークを介してサーバーから上記ボールトの上記署名キーを取得できるロジックをもつ請求項５７の生成装置。
【請求項６１】
上記第１のコンピュータ化システムが、さらに複数の会話型メッセージユニットを含む

ように上記会話型メッセージを構成できるロジックをもつ請求項５２の生成装置。
【請求項６２】
上記第１のコンピュータ化システムが、さらにダイアログの会話型メッセージ要素の中から上記複数の会話型メッセージユニットを選択できるロジックを有する請求項６１生成装置。
【請求項６３】
上記第１のコンピュータ化システムが、さらに上記会話型メッセージ要素を有するトランスクリプトを記憶できるロジックを有する請求項６２の生成装置。
【請求項６４】
会話型メッセージを対象とするデジタルシグネーチャの検証装置において、
ベリファイキーに基づいてこのデジタルシグネーチャを復号して第１ハッシュ値を再生できるロジックをもつ第１のコンピュータ化システム、
上記会話型メッセージに基づいて第２ハッシュ値を計算できるロジックをもつ第２のコンピュータ化システム、および
上記第１ハッシュ値と上記第２ハッシュ値とを比較して検証レスポンスを求めることができるロジックをもつ第３のコンピュータ化システムからなり、
上記検証レスポンスが、上記第１ハッシュ値と上記第２ハッシュ値とが一致したときに、検証すべき会話型メッセージを示し、そして上記第１のコンピュータ化システム、上記第２のコンピュータ化システムおよび上記第３のコンピュータ化システムのすべてあるいは一部を同じシステムとするか、あるいはすべてを同じシステムとしないことを特徴とする検証装置。
【請求項６５】
上記第１のコンピュータ化システムが、さらにネットワークを介してサーバで上記検証エンティティを認証できるロジックを有する請求項６４の検証装置。
【請求項６６】
上記第１のコンピュータ化システムが、さらにネットワークを介してサーバから上記ベリファイキーを取得できるロジックを有する請求項６４の検証装置。
【請求項６７】
上記第１のコンピュータ化システムがベリファイヤにおいて上記デジタルシグネーチャを復号する請求項６４の検証装置。
【請求項６８】
上記第１のコンピュータ化システムが、さらにネットワークを介してサーバから上記ベリファイヤの上記ベリファイキーを取得する請求項６７の検証装置。
【請求項６９】
上記デジタルシグネーチャを検証エンティティによって検証し、そして上記第１のコンピュータ化システムが、さらにネットワークを介してサーバで上記ベリファイヤの上記検証エンティティを認証できるロジックを有する請求項６７の検証装置。
【請求項７０】
上記第３のコンピュータ化システムが、さらにネットワークを介して上記検証レスポンスを第３者に通信できるロジックを有する請求項６４の検証装置。
【請求項７１】
上記会話型メッセージがダイアログに少なくとも一つの会話型メッセージ要素を有し、そして上記第１のコンピュータ化システム、上記第２のコンピュータ化システムおよび上記第３のコンピュータ化システムの一つが、さらに上記会話型メッセージ要素を有するトランスクリプトを記憶できるロジックを有する請求項６４の検証装置。
【請求項７２】
上記第３のコンピュータ化システムが上記第１のコンピュータ化システムでもなくまた上記第２のコンピュータ化システムでもなく、
上記第１のコンピュータ化システムが、さらにネットワークを介して上記第１ハッシュ値を上記第３のコンピュータ化システムに通信できるロジックを有し、そして

上記第２のコンピュータ化システムが、さらに上記ネットワークを介して上記第２ハッシュ値を上記第３のコンピュータ化システムに通信できるロジックを有する請求項６４の検証装置。

【請求項７３】

会話型メッセージを対象とするデジタルシグネーチャの生成装置において、

この会話型メッセージに基づいてハッシュ値を計算する手段、および

シグネーチャキーに基づいて上記ハッシュ値を暗号化することによってデジタルシグネーチャを生成する手段からなり、

上記計算手段および上記暗号化手段の両者を同じコンピュータ化システムとするか、あるいはいずれも同じコンピュータ化システムとしないことを特徴とする生成装置。

【請求項７４】

会話型メッセージを対象とするデジタルシグネーチャの検証装置において、

ベリファイキーに基づいてこのデジタルシグネーチャを復号して第１ハッシュ値を再生する手段、

上記会話型メッセージに基づいて第２ハッシュ値を計算する手段、および

上記第１ハッシュ値と上記第２ハッシュ値とを比較して検証レスポンスを求める手段からなり、

上記検証レスポンスが、上記第１ハッシュ値と上記第２ハッシュ値とが一致したときに、検証すべき会話型メッセージを示し、そして上記復号手段、上記計算手段および上記比較手段のすべてかあるいは一部を同じコンピュータ化システムとするか、あるいはいずれも同じコンピュータ化システムとしないことを特徴とする検証装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、全体としては、コンピュータネットワーク通信のセキュリティ確保、具体的には、チャットおよびインスタント・メッセージング（ＩＭ）システムのセキュリティを効率よく確保することに関する。なお、本発明の主な目的の一つは、インターネットを含む、ローカルエリアネットワークおよびワイドエリアネットワークの両者におけるエンタープライズインスタントメッセージングにある。

【背景技術】

【０００２】

チャットシステムでは、ユーザーグループ間でオンライン会話をリアルタイムで実施できる。このようなシステムの初期の二つのシステムはＵＮＩＸトークおよびインターネットリレーチャット（ＩＲＣ）である。ＩＲＣは、すでにかなりの割合で持続的に普及し、ここでの有用な実例である。簡単に説明すると、ＩＲＣは、ＩＲＣサーバの個別的な各種のネットワークまたはネットからなる。ユーザーがクライアントプログラムを実行して、ＩＲＣサーバに接続し、このＩＲＣサーバが次にユーザーのメッセージを同じネット上において、従ってユーザー間において他のＩＲＣサーバに、あるいはこのサーバからリレーする。ＩＲＣサーバにいったん接続すると、通常、ユーザーは、チャット“ルーム”に参加、あるいは一つかそれ以上の“チャンネル”に加わり、他のユーザーと会話できる。例えば、これらルームまたはチャンネルは、異なるトピックに割り当てられるため、チャットの会話は、オープンの場合には、“その時点の”すべてのユーザーがメッセージを閲覧でき、かつ会話に参加することができ、またプライベートな場合には、特定のユーザー間でのみメッセージを交換でき、かつ会話に参加できる。

【０００３】

チャットシステムの普及につれて、多数の改良が行われ、特にＩＭシステム（ｉｎｓｔａｎｔ　ｍｅｓｓａｇｉｎｇ　ｓｙｓｔｅｍｓ）として知られている新しいクラスのシステムが出現している。ＩＭシステムの場合、ユーザーが、他の特定のユーザーがネットワークにいつログオンしたかを知ることができ、また私的メッセージを送信することができる。一般に会話は公開ルームまたはチャンネルで始まり、それから“プライベートに設定

”できるチャットシステムとは異なり、ＩＭの場合は、一般に、プライベートとして始まり、そのままプライベートを維持する。また、会話に参加している人が誰であるかを確認するためにごく限られた手段しかもたない大半のチャットシステムとは違って、ＩＭシステムのユーザーは中央データベースに登録され、このデータベースでアイデンティティを確認できる。

【０００４】

チャットシステムやＩＭシステムの場合、ダイアログメタファーや会話メタファーを利用しているが、動作はメッセージの交換に基づく。その他にも多くのメッセージングももちろん存在するが、最もよく利用されているのはｅ－メールである。ところが、このような他のシステムは、リアルタイムで他のユーザーと会話できる能力はない。ここで、他のメッセージングシステムとの混乱、およびこれらから区別するために、一般的に、チャット、ＩＭ、および今後出現する可能性のある応用型を指す用語“会話型メッセージングシステム”を採用する。

【０００５】

具体的に対象とするのは、現在“エンタープライズ・インスタント・メッセージング”（ＥＩＭ）と呼ばれている応用型である。従来の会話型メッセージングシステムとは異なり、ＥＩＭシステムを利用する多くの企業は、送受信するメッセージの機密が保持されていることが望ましく、あるいは決定的に重要であると考えている。

【０００６】

本明細書の文脈に関する限り、機密保持会話には、６つの重要な属性がある。第１は、参加者すべてを認証することが好ましいという属性である。第２は、参加者すべてが会話への参加許可を得ることが好ましいという属性である。第３は、トランジット時および記憶時の両者において、会話におけるすべてのメッセージの秘密を保護することが好ましいという属性である。第４は、トランジット時および記憶時の両者において、会話におけるすべてのメッセージの完全性を保護することが好ましいという属性である。第５は、会話におけるメッセージを任意の数の参加者によってデジタル署名できることが好ましく、またこれらデジタル署名（シグネーチャ）を任意の時点でベリファイすることが好ましいという属性である。第６は、セキュリティ属性をそのまま保持した（即ち機密保持状態およびデジタル署名状態）状態で会話のトランスクリプトを記録できることが好ましいという属性である。特にこのリストの属性５および属性６については、実施しがたいことがわかっている。

【０００７】

会話の一部をオリジネータおよびターゲットの両者が署名できるデジタルシグネーチャ（以下単にシグネーチャという）生成／ベリファイシステムが必要である。これは、拒否できないメッセージを送信するオリジネータおよびその正確なメッセージの受信を確認するレシピエントのビジネスセマンティクスを実行するものである。

【０００８】

また、このようなシステムの場合、ある署名者が会話の任意の部分を署名確認できることが好ましく、会話の異なる部分を異なる署名者（各個別の署名者、多重署名者のいずれの場合もある）が署名できることが好ましい。通常の会話過程では、すべての交換について、非拒否特性をもつ必要はないが、ある種の行為に結果するメッセージ、例えばある量の株を購入せよというメッセージの場合には、オリジネータが署名できるようにし、また後でベリファイできるようにする必要がある。

【０００９】

さらに、上記属性５に対処するさいには、望ましいシステムの場合、シグネーチャキーの期限切れの後に、シグネーチャをベリファイできるようにしておく必要がある。これは、シグネーチャキーを発行したシステムがなくなったかなり後に、会話の妥当性をベリファイする必要が生じた場合に特に有効である。

【００１０】

また、望ましいシステムの場合、メッセージシグネーチャをトランスクリプトとして記

録できなければならない。即ち、会話メッセージを記録する通常の過程で、会話の署名部分を区切り、この特定の部分にシグネーチャを付ける必要がある。このようにすれば、トランスクリプトは、署名が明瞭なメッセージの拒否できない特徴を始めとする最初の会話の特徴をすべてもつことになる。これは、上記の属性６に対応する。

【００１１】

シグネーチャ生成／ベリファイシステムの場合、その基礎となるデジタルシグネーチャ技術とは独立していることが好ましい。唯一の必要条件は、署名する当事者がシグネーチャキーをもち、かつベリファイする当事者が対応するベリファイキーをもつことである。すなわち、公開鍵基盤（ＰＫＩ）サーティフィケートにおいて、シグネーチャ／ベリファイキーは、同一でもよく、あるいは異なっていてもよく、また短命でもよく、あるいは長命でもよい。

【００１２】

広く利用されている従来のセキュリティシステムの大半は、その基礎はＰＫＩであるが、問題も多くある。例えば、ＰＫＩを使用したシグネーチャ生成／ベリファイシステムの場合、署名する参加者のすべてが、デジタル署名を生成するために好適なキーをもつ長命のデジタルサーティフィケートをもつ必要がある。また、各署名者のサーティフィケートがすべてのベリファイヤにとって利用できるものでなければならない。さらに、サーティフィケートを発行したサーティフィケート当局がその機能を止めた後長い期間を経過したベリファイ時点ですべてのベリファイヤにとって署名者のサーティフィケートの取り消し状態が利用できなければならない。

【００１３】

従って、シグネーチャ生成／ベリファイを行うためにＰＫＩサーティフィケートを利用できるが、これを必要としないシステムが望まれている。即ち、一般的には、サーティフィケートにおけるＰＫＩベリファイキー、署名者およびベリファイヤに知られている対称キー、エフェメラルアサーションにおける、対応する私的キーが署名者に知られている短命公開キーを始めとする任意のタイプのキーが使用できなければならない。

【００１４】

ＰＫＩシステムと異なり、望ましいシグネーチャ生成／ベリファイシステムの場合には、シグネーチャの生成時に署名者のキーの妥当性状態を記録できるものでもなければならない。このためには、上記キー、このキーをもつ任意のサーティフィケートまたはアサーション、トラスト・ルートにつながるすべてのサーティフィケートまたはアサーション、およびサーティフィケートそれぞれの取り消し状態（一般的に、アサーションは短命で、取り消し不可能である）を記録する必要がある。

【発明の開示】

【発明が解決しようとする課題】

【００１５】

従って、本発明の一つの目的は、会話型メッセージを対象とするデジタルシグネーチャ／ベリファイシステム（ｄｉｇｉｔａｌ　ｓｉｇｎａｔｕｒｅ　ａｎｄ　ｖｅｉｆｉｃａｔｉｏｎ　ｓｙｓｔｅｍ）を提供することである。

【課題を解決するための手段】

【００１６】

本発明の一つの好適な実施態様は、会話型メッセージの通信システムである。このシステムは、会話型メッセージに基づいて第１ハッシュ値を計算する。次にシグネーチャキーに基づいてこの第１ハッシュ値を暗号化してデジタルシグネーチャを生成する。ネットワークを介してこのデジタルシグネーチャと会話型メッセージを通信する。次に、ベリファイキー（ｖｅｒｉｆｉｃａｔｉｏｎ　ｋｅｙ）に基づいてデジタルキーを復号して第１ハッシュ値を再生する。会話型メッセージに基づいて第２ハッシュ値を計算する。第１ハッシュ値と第２ハッシュ値とを比較して検証レスポンスを求める。第１ハッシュ値と第２ハッシュ値が一致したときに、この検証レスポンスは、会話型メッセージが検証されたこと示す。

【００１７】
次に、本発明の別な好ましい実施態様は、会話型メッセージを対象とするデジタルシグネーチャの生成システムである。このシステムは、会話型メッセージに基づいてハッシュ値を計算する。次に、シグネーチャキーに基づいてこのハッシュ値を暗号化してデジタルシグネーチャを生成する。
【００１８】
本発明のさらに別な好ましい実施態様は、会話型メッセージを対象とするデジタルシグネーチャの検証システムである。このシステムの場合は、ベリファイキーに基づいてデジタルシグネーチャを復号して第１ハッシュ値を再生する。次に、会話型メッセージに基づいて第２ハッシュ値を計算してから、第１ハッシュ値と第２ハッシュ値とを比較して検証レスポンスを求める。この場合、第１ハッシュ値と第２ハッシュ値が一致したときに、この検証レスポンスは、会話型メッセージが検証されたこと示す。
【発明の効果】
【００１９】
本発明の第１の作用効果によれば、会話の一部をオリジネータとターゲットの両者によって署名でき、オリジネータが拒否できないメッセージを送り、その正確なメッセージの受信に関してレシピエントが拒否できない確認を返信するビジネスセマンティクスを実行できる。
【００２０】
また、本発明の第２の作用効果によれば、署名者が会話の任意の部分に署名でき、かつ会話の任意の他の異なる部分に異なる署名者（単独の署名者、複数の署名者）が署名できる。
【００２１】
本発明の第３の作用効果によれば、機密保持会話の重要な６つの属性のうち任意の属性またはすべての属性を満足できる。即ち、すべての参加者が会話に参加できるように認証することができる；トランジット時および記憶時の両者において、すべてのメッセージの秘密性および完全性を保護することができる；メッセージは、参加者のうち任意の人数によってデジタル署名することができ、これらシグネーチャは任意の時点でベリファイすることができる；そしてセキュリティ属性をそのまま保持した状態で会話のトランスクリプトを記録することができる。
【００２２】
本発明の第４の作用効果によれば、上記属性と調和した状態で、いくつかの実施態様は、シグネーチャキーの期限が切れ、既に存在しなくなってからかなり経過した後でも、シグネーチャをベリファイできるものである。
【００２３】
本発明の第５の作用効果によれば、上記属性と調和した状態で、いくつかの実施態様は、メッセージシグネーチャをトランスクリプトに載せることができ、かつ署名された会話の部分を区切るとともにシグネーチャをこれら特定部分に付けることができるものである。
【００２４】
本発明の第６の作用効果によれば、本発明はその基礎となるデジタルシグネーチャ技術とは独立して実施でき、唯一の要件は、署名する当事者がシグネーチャキーをもち、かつベリファイする当事者が対応するベリファイキーをもつことである。これらキーが異なるかあるいは同一のキーであるか、短命かあるいは長命かには制限がなく、また公開鍵基盤（ＰＫＩ）に使用するかにも制限はない。
【００２５】
本発明の第７の作用効果によれば、以上と調和した状態で、本発明はＰＫＩに依存せず、従って署名する参加者が、潜在的かつ最終的なベリファイヤについて取り消し可能な状態で利用できる長命デジタルサーティフィケートを用意する必要はない。
【００２６】

本発明の第８の作用効果によれば、シグネーチャ生成時に署名者のキーがどのような妥当性状態にあるかを求めることも可能である。

以上の、およびこれら以外の本発明の目的、作用効果については、当業者ならば本明細書で説明し、かつ添付図面に示した現在までに知られている本発明の最良の実施態様および好適な実施態様の産業上の利用可能性に関する記載から理解できるはずである。

【発明を実施するための最良の形態】

【００２７】

本発明の好適な実施態様は、会話型メッセージングを対象としたデジタルシグネーチャ／検証（ＤＳＶ）システムである。添付の図面においては、特に図１、図２および図６では、本発明の好適な実施態様は参照符号１０で示す。

【００２８】

なお、以下のＤＳＶシステム１０に関する説明では、本発明は会話型メッセージングを対象とする。すなわち、チャット、インスタント・メッセージング（ＩＭ）およびエンタープライズ・インスタント・メッセージング（ＥＩＭ）である。他のメッセージングスキーム、例えば、シグネーチャおよびベリファイを目的としてダイアログ全体、ダイアログの一方の側あるいはクリティカルな部分を一括処理できないｅ－メールとは異なり、ＤＳＶシステム１０は、ダイナミックで自由度の高いことが必要な会話型メッセージング、特に現状では十分なセキュリティ機構がないことが採用への重大な障害になっているＥＩＭに好適である。

【００２９】

図１は、本発明のシグネーチャシステム１２を示す概略ブロック線図である。このシグネーチャシステム１２は、署名エンティティ１４およびボールト１６の２つの主構成要素からなる。署名エンティティ１４が署名すべきメッセージ１８および私的クレデンシャル２０を送り出す。ボールト１６はこれらを受け取り、これがもつシグネーチャキー２２を使用して、署名エンティティ１４に戻されるメッセージ１８のシグネーチャ２４を生成する。

【００３０】

図２は、本発明のベリファイシステム３２を示す概略ブロック線図である。ベリファイシステム３２もまた検証エンティティ３４およびベリファイヤ３６の２つの主構成要素からなる。この検証エンティティ３４はメッセージ１８、シグネーチャ２４、ベリファイキー３８およびアサーション４０を送り出す。ベリファイヤ３６はこれらを受け取り、これらを使用して、検証エンティティ３４に戻されるメッセージ１８の検証レスポンス４２を生成する。

【００３１】

シグネーチャシステム１２およびベリファイシステム３２が一体的になって、シグネーチャ２４を生成し、ベリファイするための既存の通常の式を使用することができるＤＳＶシステム１０の好適な実施態様を構成する。このＤＳＶシステム１０では、２つの（同じものでもよいが、代表例では異なる）暗号化キー、シグネーチャキー２２およびベリファイキー３８を使用する。（例えばデジタルシグネーチャ・アルゴリズムを使用する場合）これらは通常異なり、かつ非対称的であるが、（例えばハッシュド・メッセージ認証コードを使用する場合には）同一かつ対称的であってもよい。

【００３２】

概念的には、シグネーチャ２４を生成する構成成分はボールト１６である。本発明の現状の好適な実施態様では、ボールト１６がシグネーチャキー２２を記憶するが、これを出力することはない。ボールト１６のデザインまたは構成にもよるが、シグネーチャキー２２については、永久的に記憶してもよく、あるいはエフェメラルに記憶してもよい。実際には、このボールト１６は、図１に示すように、複数のシグネーチャキー２２を記憶することができ、また複数の暗号プロトコルを利用することができる。

【００３３】

ボールト１６がシグネーチャ２４を生成するためには、署名エンティティ１４がこれに

署名すべきメッセージ１８を与える。より詳しく説明するように、現在では、このメッセージ１８には、会話型メッセージングセッションにおけるダイアログのすべて、あるいは所定部分、あるいは単に一部からなる多数のメッセージユニットを含むことができる。また、署名エンティティ１４の場合には、ボールト１６に私的クレデンシャル２０を与えることができる。これらは、何を知っているかに、何をもっているかに、あるいは何であるかに基づけばよい。例えば、パスワードは何を知っているかの一つの例であり、ハードウェアセキュリティモジュールは何をもっているかの一つの例であり、生体測定は何であるかの一つの例である。私的クレデンシャル２０はオプションとすることができるが、ＤＳＶシステム１０の多くは、これを必要とし、利用するものである。理由は、セキュリティが増し、信頼性が増すからである。同一のコンピュータシステムを使用する一つかそれ以上の署名エンティティ１４についてボールト１６が複数のシグネーチャキー２２を記憶する場合には、署名エンティティ１４がどのシグネーチャキー２２を使用するかを指定することもできる。あるいは、ボールト１６は私的クレデンシャル２０を単に使用して、適正なシグネーチャキー２２を“開き”かつ選択することもできる。この場合には、適正なアルゴリズムに従ってメッセージ１８のシグネーチャ２４を生成する。

【００３４】

具体的に図２について説明すると、主構成要素は検証エンティティ３４およびベリファイヤ３６である。検証エンティティ３４は、メッセージ１８の妥当性を求める当事者である。多くの場合、検証エンティティ３４は、署名エンティティ１４、即ち直接的なレシピエントである署名エンティティ１４からのメッセージ１８を直接受け取るものであるが、これは必要条件ではなく、レシピエントがメッセージ１８を検証エンティティ３４に送り、ベリファイすることもできる。

【００３５】

ベリファイシステム３２のシグネーチャシステム１２のカウンターパートであると同様に、ベリファイヤ３６はボールト１６のカウンターパートである。検証エンティティ３４がベリファイヤ３６にメッセージ１８、シグネーチャ２４、ベリファイキー３８およびアサーション４０を与える。シグネーチャキー２２を記憶するボールト１６とは異なり、図２に示す実施態様の検証キー３８は、検証エンティティ３４によってベリファイヤ３６に送られる。このため、例えば、検証エンティティ３４がメッセージの最初のレシピエント以外の当事者になることができる。検証キー３８については、検証エンティティ３４によって特定されたベリファイ時に有効でなければならない（例えば、期限切れになってはならず、あるいは取り消されたり、没収されたり、あるいは禁止されたりしてはならない）。アサーション４０が、検証エンティティ３４によってベリファイヤ３６に与えられたオプションのタイム・スタンプ４４とともに、これを許す。また、アサーション４０により、ベリファイヤ３６がベリファイキー３８および検証エンティティ３４の権利を確認し、これを利用して検証を行うだけでなく、署名エンティティ１４の権利を確認し、これを利用して検証を行うことができる。このように、アサーション４０は、公開クレデンシャルと類似したものであり、ベリファイキーが署名キーに対応し、署名者の所有になるものである“証拠”になる。また、アサーション４０は、本発明のＤＳＶシステム１０のより簡単で、よりセキュリティが低い実施態様では、オプションとすることができる。

【００３６】

上記でついでに触れたタイム・スタンプ４４について説明する。これは検証エンティティ３４によってベリファイヤ３６に与えられ、ベリファイヤ３４が次にこれを使用して、タイム・スタンプ４４における特定の時期においてシグネーチャキー２２が有効であるかどうかについて答える。従って、検証エンティティ３４が、“このシグネーチャキー２４はそのような時期に有効であったか？”という質問にダイナミックに答えることができる。これは、特に、従来技術の深刻な問題、キーの期限切れ時に一時的な検証が不可能になる問題を解決するものである。タイム・スタンプ４４それ自体はメッセージ１８からくるが、これは必要ない。例えばある時点Ｔで書類が署名されたという申し立てがあった場合には、検証エンティティ３４がベリファイヤ３６に“このシグネーチャは時点Ｔにおいて

有効であったのか？”という質問を発することになる。ここでの利点は、検証エンティティ３４が、信頼されているタイム・スタンプサービスの存在に依存しないことである。

【００３７】

次に、全体的なシグネーチャ／ベリファイプロセスの輪郭について説明する。使用する記号は次の通りである。

Ｍ＝署名ベリファイすべきメッセージ
Ｓ＝メッセージのシグネーチャ
Ｈ＝一方向性ハッシュ関数；ここではＨ１およびＨ２を使用する（例えばセキュア・ハッシュアルゴリズム、ａ．ｋ．ａ．ＳＨＡ－１）
Ｋ１＝シグネーチャキー
Ｋ２＝ベリファイキー
Ｅ＝暗号関数
Ｄ＝復号関数

【００３８】

図３は、シグネーチャシステム１２がシグネーチャ２４を生成し、このシグネーチャ２４をベリファイシステム３２がベリファイするプロセス５０を示すフローチャートである。このプロセス５０は、署名エンティティ２４を署名すべきメッセージ１８で構成するか、あるいは署名エンティティ２４が署名すべきメッセージ１８を与えるステップ５２で開始する。ステップ５４で、メッセージ１８の第１の一方向性ハッシュＨ１（Ｍ）を生成する。ステップ５６で、第１の一方向性ハッシュをシグネーチャキー２２で暗号化し、シグネーチャ２４、Ｅ（Ｈ１（Ｍ））Ｋ１あるいは単にＳを生成する。

【００３９】

ステップ５２～５６については、シグネーチャシステム１２によって、あるいはその制御下で行う。ステップ５８で、メッセージ１８およびそのシグネーチャ２４をベリファイシステム３２に通信し、そこで以下の後続ステップを行う。

【００４０】

ステップ６０では、ステップ５４で使用したのと同じ結果を与えるハッシュアルゴリズムを使用して、受信メッセージ１８に基づいて第２の一方向性ハッシュを生成する。ここでのメッセージ１８は、署名されたメッセージ１８の正確なコピーである。ステップ６２で、受信シグネーチャ２４を式Ｄ（Ｓ）Ｋ２またはＤ（Ｅ（Ｈ１（Ｍ））Ｋ１）Ｋ２に従ってベリファイキー３８によって復号し、第１の一方向性ハッシュを再生する必要がある。

【００４１】

ステップ６４では、第１の一方向性ハッシュおよび第２の一方向性ハッシュを比較する。もし同じならば、シグネーチャ２４はベリファイされたと考える。あるいは、ハッシュが同一でない場合には、シグネーチャ２４はベリファイされない。ステップ６６で、プロセス５０は終了する。なお、必要ならば、ステップ６８で、失敗したベリファイの結果に基づいて適正な処置を行う。

【００４２】

一般的に、次の５つの条件になると、結果的に、シグネーチャ２４がベリファイされないことになる。第１の条件では、受信メッセージ１８を変更できない。第２の条件では、受信シグネーチャ２４を変更できない。第３の条件では、ベリファイキー３８が間違ったキーになる。即ち、シグネーチャキー２２と使用するには不適当なキーになる。第４の条件では、ステップ５４および６０で使用した一方向性ハッシュアルゴリズムが合わなくなる。即ち、同じメッセージに使用したときに、結果が異なる。第５の条件では、使用した暗号および復号アルゴリズムが合わなくなる場合が生じる。

【００４３】

これらのケースのうち第１と第２のケースは、プロセス５０を検出することを意図したケースであり、一方第３、第４および第５のケースは、単にユーザーエラーを原因とし、直ちに修復可能である。例えば、異なるハッシュまたは暗号アルゴリズムが許される実施

態様では、ステップ５８でアルゴリズム識別子に通信できる。

【００４４】

ここで再度図１～３について説明すると、プロセス５０の場合は、シグネーチャシステム１２の署名エンティティ１４およびボールト１６、あるいはベリファイシステム３２の検証エンティティ３４およびベリファイヤ３６のいずれにも密接な関係をもたない。シグネーチャシステム１２およびベリファイシステム３２の物理的構成要素において上記のようにプロセス５０のステップを行うことは、本発明の好ましい実施態様であるが、本発明の概念はこの構成以上の構成を含むもので、他の実施態様についても等しく、あるいは場合によってはより好適に応用できるものである。

【００４５】

図４ａ～図４ｇは、ＤＳＶシステム１０の構成要素の考えられる多数の配置を示すブロック線図であるが、本発明はこれらに制限を受けるものではない。図４ｂは、署名エンティティ７２が検証エンティティ７４にメッセージ１８およびシグネーチャ２４を与える基本的な実施態様を示す図である。ここでの署名エンティティ７２は、図１のシグネーチャシステム１２において検証エンティティ１４およびボールト１６が行ったタスクを実行し、そして検証エンティティ７４は、図２のベリファイシステム３２において検証エンティティ３４およびベリファイヤ３６が行ったタスクを実行する。なお、メッセージ１８およびシグネーチャ２４は一緒に、あるいは個別に与えることができ、図４ａにこれら応用例の２つを示す。

【００４６】

図４ｂに、シグネーチャ２４を与える一つの応用例を示す。ここで署名エンティティ７６はメッセージ１８をエージェント７８に与える。このエージェント７８はメッセージ１８の第１の一方向性ハッシュＨ１（Ｍ）を生成し、これをシグネーチャキー２２で暗号化し、シグネーチャ２４、Ｅ（Ｈ１（Ｍ））Ｋ１またはＳを生成する。ここでの署名エンティティ７６として署名エンティティ１４と同様なものを使用し、そしてエージェント７８として図１のボールト１６と同様なものを使用するのが有効である。署名エンティティ７６およびエージェント７８は、一つのコンピュータに格納することができる。あるいは、別々なコンピュータに格納してもよい。すなわち、代表的にはファイアーウオールの後方にあるローカルエリアネットワークに設けることができる。あるいは、ワイドエリアネットワークによって分離間隔を広げてもよく、この場合には、他のセキュリティ保護を講じることができる。図４ｂに示すように、シグネーチャ２４を署名エンティティ７６に戻し、ここからメッセージ１８およびシグネーチャ２４を送り出す場合にも、エージェント７８が署名エンティティ７６の名においてこれらを送り出すことができる。図４ａ～図４ｇに、主な応用例を示すが、本発明の原理を理解できなければ理解できないような副次的な応用例ではない。

【００４７】

図４ｃに、シグネーチャ２４を与える別な応用例を示す。ここでは、署名エンティティ８０がメッセージ１８の第１の一方向性ハッシュＨ１（Ｍ）を作り、これをエージェント８２に送る。次に、エージェント８２がシグネーチャキー２２で第１の一方向性ハッシュを暗号化し、シグネーチャ２４Ｅ（Ｈ１（Ｍ））Ｋ１またはＳを生成する．ここで考える点は、第１の一方向性ハッシュが最初のメッセージ１８よりかなり小さく、従って通信がより簡単な点、およびここではエージェント８２には最初のメッセージ１８が見えない点である。

【００４８】

図４ｄに、メッセージ１８およびシグネーチャ２４を検証する応用例を示す。ここでは、検証エンティティ８４がメッセージ１８およびシグネーチャ２４を受信し、これら両者をエージェント８６に送る。あるいは、検証エンティティ８４がメッセージを受信し、これをエージェント８６に送る一方で、エージェント８６が別なルートからシグネーチャ２４を受信する。次に、エージェント８６がメッセージ１８の第２の一方向性ハッシュＨ２（Ｍ）を生成し、式Ｄ（Ｓ）Ｋ２またはＤ（Ｅ（Ｈ１（Ｍ））Ｋ１）Ｋ２に従ってシグネ

ーチャ２４を復号し、第１の一方向性ハッシュＨ２（Ｍ）を再生し、第１の一方向性ハッシュと第２の一方向性ハッシュとを比較し、検証エンティティ８４に検証レスポンスを与える。このためには、エージェント８６は検証キー３８を必要とするが、これは検証エンティティ８４によって与えることができる（あるいは、エージェント８６が既に保持しているか別な手段で得ることができる。例えば、図４ｅを参照）。この応用例では、図１に示した、検証エンティティ３４およびベリファイヤ３７からなるベリファイシステム３２と同じシステムを利用するのが有効である。

【００４９】

図４ｅに、メッセージ１８およびシグネーチャ２４を検証する別な応用例を示す。ここでは、受信エンティティ８８（潜在的には、メッセージおよびシグネーチャを受信し、これらを送り出す任意の当事者）がメッセージ１８を受信し、このメッセージ１８およびシグネーチャ２４を、潜在的には図４ｄで使用した同じエージェント８６であるエージェント８６（ここでは実際の“検証”エンティティ）に送る。ここで、エージェント８６はベリファイキー３８をもっている（あるいは、受信エンティティ８８がこれを与えてもよい。例えば、図４ｄを参照）が、図４ｄの場合と異なり、検証レスポンス４２を第３者９０に与えるのはエージェント８６である。第３者９０には、メッセージ１８の内容は見えない。

【００５０】

図４ｆに、メッセージ１８およびシグネーチャ２４を検証するさらに別な応用例を示す。ここでは、検証エンティティ９２がメッセージ１８およびシグネーチャ２４を受信するが、シグネーチャ２４のみエージェント９４に送る（なお、これ以外にエージェント９４がベリファイキー３８にアクセスできない場合には、ベリファイキー３８にも送る）。次に、エージェント９４が、式Ｄ（Ｓ）Ｋ２またはＤ（Ｅ（Ｈ１（Ｍ））Ｋ１）Ｋ２に従ってシグネーチャ２４を復号し、第１の一方向性ハッシュＨ１（Ｍ）を再生し、この第１の一方向性ハッシュを検証エンティティ９２に送り戻す。この検証エンティティ９２が第２のメッセージ１８の一方向性ハッシュＨ２（Ｍ）を生成し、これと第１の一方向性ハッシュとを比較し、メッセージ１８を検証するかどうかを確認する。エージェント９４にはメッセージ１８の内容が見えず、またここで通信されるシグネーチャ２４および第２の一方向性ハッシュは、例えば、小さく、従って管理が容易である。

【００５１】

図４ｇに、図４ｆに示した応用例をいくぶん展開したさらに別な応用例を示す。ここでは、検証エンティティ９６がメッセージ１８およびシグネーチャ２４を受信し、潜在的には図４ｆに示した同じエージェント９４であるエージェント９４にシグネーチャ２４だけを送る。この検証エンティティ９６もメッセージ１８の第２の一方向性ハッシュＨ２（Ｍ）を生成するが、ここではこのハッシュを第３者９８に送る。エージェント９４が、式Ｄ（Ｓ）Ｋ２またはＤ（Ｅ（Ｈ１（Ｍ））Ｋ１）Ｋ２に従ってシグネーチャ２４を復号し、第１の一方向性ハッシュＨ１（Ｍ）を再生するが、この例では、これを第３者９８に送る。従って、第３者９８は、別々に受信された第１の一方向性ハッシュと第２の一方向性ハッシュとを比較して、メッセージ１８を検証するかどうかを確認できる。ここでは、エージェント９４にも、また第３者９８にもメッセージ１８の内容が見えず、検証エンティティ９６を超えて通信される構成要素が、例えば小さく、従って管理が容易である。

【００５２】

図５は、メッセージユニットに署名しこれを検証するためにどのように本発明ＤＳＶシステム１０を使用するかを示すためのセールスの実例において使用される会話型メッセージングダイアログ、即ちＥＩＭダイアログを示す図である。既に説明したように、メッセージ１８には、ダイアログのすべて、所定の部分または単なる一部からなる多数のメッセージユニットが含まれる。従って、シグネーチャ２４用のメッセージ１８は、図５ではダイアログ１８ａ全体であればよい。あるいは、売買契約の細部を煮詰めた後の雑談を除く、部分的なダイアログ１８ｂをメッセージ１８として使用してもよい。あるいは、メッセージ１８は、買い手側の文１８ｃのみ、あるいは売り手側の文１８ｄからなっていてもよく

、あるいは買い手側の文１８ｃは第１の署名されたベリファイ可能なメッセージ１８から構成できるとともに、売り手側の文１８ｄは第２の署名されたベリファイ可能なメッセージ１８から構成できる。さらに、メッセージ１８を単文１８ｅから構成することも可能である。当業者ならば、最後の場合を除いて、ｅ－メールなどのメッセージングシステムの場合、上記のやり方では機密を有効に保持できないことを理解できるはずである。ここでのセールスの実例は、通常どのようにして最も効率的に通信を行うかの代表例である。即ち、対話型の“リアルタイム”会話の代表例である。このようなトランザクションなどにおいては、ＥＩＭは、長期にわたってメッセージを交換するｅ－メール、ボイスメール、郵便、テレグラフなどのシステムよりも好ましい。本発明のＤＳＶシステム１０の場合、必要に応じて、かつ当事者の好みに応じて、ダイナミックかつ自由度をもって、会話型メッセージング（例えば、チャット、ＩＭ、ＥＩＭ）の機密を保持することができる。

【００５３】

図６は、多数のオプションをもつ本発明ＤＳＶシステム１０を示す概略ブロック線図である。ここでも同様に、署名エンティティ１４および検証エンティティ３４がメッセージ１８を交換し、シグネーチャ２４での検証を受ける。メッセージ１８、シグネーチャ２４およびその他のオプションである他の要素に関する通信は、ネットワーク１００を介して行う。

【００５４】

適宜、キーサーバ１０２を設けて、ネットワーク１００を介してアクセスできるようにする。キーサーバ１０２は、シグネーチャキー２２およびベリファイキー３８のいずれ一方、あるいは両方を与えるか、記憶保存することができる。キーサーバ１０２は、メッセージ１８の秘密性および完全性を保護する機能をもつ。ボールト１６をもつＤＳＶシステム１０の多くの実施態様では、これはプライベートであり、また通常はシグネーチャキー２２を記憶保存するために好ましい。ベリファイキー３８はキーサーバ１０２に記憶保存することができるが、より一般的には、公開クレデンシャル（例えば、アサーション、サーティフィケートなど）に記憶保存する。従って、キーサーバ１０２は、広くは利用されてはいないが、ＤＳＶシステム１０における一つの考えられるオプションである。

【００５５】

同様に適宜、認証サーバ１０４を設けて、ネットワーク１００を介してアクセスできるようにしてもよい。認証サーバ１０４は、私的クレデンシャル２０およびアサーション４０のいずれか一方かあるいは両方を発行できるか、あるいは保障できる。これらオプション両者は、ＤＳＶシステム１０を利用する団体にとって、特に既に説明したＥＩＭとして望ましいものである。

【００５６】

所望ならば、ネットワーク１００を介して検証レスポンス４２を第３者９０に通信するか、あるいはネットワーク１００を介してハッシュ値Ｈ１（Ｍ）およびＨ２（Ｍ）を第３者に通信して、そこでの検証レスポンス４２を求めることができる。これらオプションを利用すると、ＥＩＭをさらに促進できる。

【００５７】

ネットワーク１００は、ローカルエリア形ネットワークか、あるいはインターネットなどのワイドエリア形ネットワークであればよい。署名エンティティ１４、検証エンティティ３４、キーサーバ１０２、認証サーバ１０４および第３者９０、９８はいずれもコンピュータ化システムか、あるいはこれらを含むものである。例えば、制限するものではないが、署名エンティティ１４、検証エンティティ３４および第３者９０、９８のすぐれた候補としてはパソコン（ＰＣ）および通信が可能な携帯情報端末（ＰＡＤ）がある。高度なスマートカードでさえ、署名エンティティ１４および検証エンティティ３４のすべての、あるいは一つの構成要素として使用できる好適な“コンピュータ化システム”である。既存のシングルプロセッサシステムおよびマルチプロセッサシステムは、キーサーバ１０２および認証サーバ１０４のすぐれた候補である。

【００５８】

本明細書全体を通して、暗黙の前提として検証エンティティを会話型メッセージング交換における文の意図するターゲットの一つとしているが、これは必ずしも必要ない。シグネーチャ検証サービスの場合、メッセージのシグネーチャを検証し、検証結果を要求する当事者（例えば、第３者９０、９８）に通信できるように展開できる。この能力は、メッセージのレシピエントが特定のシグネーチャを検証するリソースをもたない、あるいはもつことを望まない場合に特に有用である。これは、既に説明したエージェント８６、９４の役割に一致する。

【００５９】

図７は、シグネーチャ検証サービス１１０をもってさらに展開できるように具体化した本発明のＤＳＶシステム１０を示す概略展開図である。このシグネーチャ検証サービス１１０は、トランザクションの期限切れ後長く経過したときに特に有用である。例えば、訴訟のさいに、妥当なシグネーチャがあると、トランザクションをその最初の署名者まで辿るために役立つ。

【００６０】

長命の検証は、概念的にはリアルタイムな認証とはやや異なるものである。この違いは、それぞれが外部データおよびサービスに依存する量である。リアルタイムな認証サービスは、他のデータまたはサービス（例えば、エルダップ（ＬＤＡＰ）ディレクトリまたはオンライン・サーティフィケート・ステータス・プロトコル（ＯＣＳＰ）サーバにおけるサーティフィケート・リソースリスト（ＣＲＬ）に依存できるが、長命の認証サービスの場合には、できるだけ自給自足的であることが好ましい。すなわち、最初のメッセージや検証するシグネーチャをもつメッセージの集合を別にすると、他のいかなるデータまたはサービスに頼らないほうが好ましい。従って、長命の検証サービスの場合、２つのオペレーション、生成および検証をサポートする必要がある。

【００６１】

シグネーチャ検証サービスの本発明の好適な実施態様の場合、メッセージ１８毎に生成オペレーションによりデータベース１１２に記録１１４を割り当てる（すなわち、各メッセージ１８を定義署名し、単文または文の集合に署名する）。メッセージ１８の暗号ハッシュに基づいてデータベース１１２のプライマリキー１１６を使用し、かつ各記録１１４はさらにメッセージ１８のシグネーチャ２４だけでなく、ベリファイキー３８をもち、これをメッセージ１８の署名エンティティ１４にリンクする公開クレデンシャル１１８（例えば、サーティフィケートまたはアサーション）および公開クレデンシャル１１８の取り消しステータス１２０を含む。

【００６２】

シグネーチャ検証サービス１１０は情報を受信し、署名エンティティ１４から直接記録１１４を生成するか（即ち、追加レシピエント）、この情報を前のレシピエントから間接的に受信する。使用するプライマリキー１１６がメッセージ１８のハッシュであるため、メッセージ１８をシグネーチャ検証サービス１１０に送ることはできず、通信量が減り、セキュリティが増す。公開クレデンシャル１１８はメッセージ１８を伴うことができる。即ち、署名エンティティ１４によって与えることができる。あるいは、シグネーチャ検証サービス１１０はこれらを任意の場所（例えば、認証サーバ１０４または通常のサーティフィケートサービス）から得ることができる。公開クレデンシャル１１８は、署名エンティティをコントロールするが、それ以外では完全な公開からＤＳＶシステム１０のコンテキスト外では知られていない範囲にわたるという意味で“公開”である（例えば、公開クレデンシャル１１８は、シグネーチャ２４を生成するさいに使用した私的クレデンシャル２０と潜在的には同じ場合があってもよいが、これは明らかに欠点の一つである）。

【００６３】

妥当性オペレーションはプライマリキー１１６（メッセージ１８の暗号ハッシュ）を入力とし、そのデータベース１１２のコンテンツに基づいてメッセージ１８の妥当性状態に関する情報を与える。本発明の現状での好ましい実施態様では、これは、最初の署名エンティティ１４の公開クレデンシャル１１８（エフェメラルアサーションまたはＰＫＩサー

ティフィケート）における名前によって決定する場合に、シグネーチャ２４が妥当であるかどうかを示すブールを与えるとともに、誰がメッセージ１８に署名したかを示す。また、妥当性オペレーションは、署名エンティティ１４の公開クレデンシャル１１８からトラストパスのルートにいたる経路に関する一組の情報（信頼性の増した一連のクレデンシャル、即ち何が公開クレデンシャル１１８を保障するのか、またこれを何が保障するのか、など）だけでなく、これらすべてのクレデンシャルの妥当性をサポートする取り消しデータ（例えば、妥当なＣＲＬに関するサーティフィケートの不在）を与えるものでもある。

【００６４】

長命の検証のプロバイダとして、シグネーチャ検証サービス１１０は、特にタイム・スタンプ４４（図２）を利用できる。既に説明したように、署名に使用したキーが期限切れの場合に“このシグネーチャ２４はこのような時点で妥当であったのか？”という質問に答えることは、従来システムでは対処できない問題であるが、本発明のＤＳＶシステム１０では対処できる。

【００６５】

本発明の実施態様をいくつか説明してきたが、いずれもｐ例示であり、制限的なものではない。換言すれば、本発明の範囲は、これら例示的な実施態様には制限されず、特許請求の範囲およびこれと等価な範囲によってのみ定義されるものである。

【産業上の利用可能性】

【００６６】

本発明のＤＳＶシステム１０は、チャットやＩＭなどの会話型メッセージングコンテクスト、特にＥＩＭなどの普及しつつある応用型に好適に使用できる。

【００６７】

明細書冒頭で説明したように、機密保持会話には多くの重要な属性があり、本発明のＤＳＶシステム１０は会話型メッセージのこれら属性のうち任意の属性、あるいはすべての属性を与えることができる。すべての参加者が会話に参加できるように認証することができる。この場合、会話型メッセージのオリジネータおよびターゲットの両者が参加することができ、署名者が会話の任意の部分に署名でき、かつ会話の任意の他の異なる部分に異なる署名者（単独の署名者、複数の署名者）が署名できる。トランジット時及び記憶時の両者において、すべてのメッセージの秘密性および完全性を保護することができる。メッセージは、デジタル署名することができ、シグネーチャキーの期限が切れ、既に存在しなくなってからかなり経過した後でも、デジタルシグネーチャのすべてをベリファイできる。また、セキュリティ属性（即ち、秘密デジタル署名）をそのまま維持した状態で会話型メッセージのトランスクリプトを記録することができ、かつ署名された会話の部分を区切るとともにシグネーチャをこれら特定部分に付けることができる。

【００６８】

本発明のＤＳＶシステム１０はその基礎となるデジタルシグネーチャ技術とは独立して実施でき、唯一の要件は、署名する当事者がシグネーチャキーをもち、かつベリファイする当事者が対応するベリファイキーをもつことである。これらキーが異なるかあるいは同一のキーであるか、短命かあるいは長命かには制限がなく、また公開鍵基盤（ＰＫＩ）サーティフィケートを使用するかにも制限はない。この後者の点では、ＤＳＶシステム１０は、すべての署名参加者が現在利用でき、現存している妥当性サーティフィケート当局によってベリファイ可能であるとともに、シグネーチャがベリファイ可能な場合には、現状で決定できる取り消し状態をもつデジタルサーティフィケートをもっていなければならない。ＤＳＶシステム１０はシグネチャー生成及びベリフィケイションを行うためにＰＫＩサーティフィケートを利用できるが、これを必要としない。

【００６９】

以上の理由、およびこれら以外の理由から、本発明のＤＳＶシステム１０は、産業上広範な利用可能性をもつことが予想され、従って、本発明の産業上の実用性は広範にわたるとともに持続的であることが考えられる。

【図面の簡単な説明】

【００７０】
【図１】本発明シグネーチャシステムを示す概略ブロック線図である。
【図２】本発明ベリファイシステムを示す概略線図である。
【図３】シグネーチャシステムがシグネーチャを生成し、そしてベリファイシステムがこのシグネーチャをベリファイするプロセスを示すフローチャートである。
【図４ａ】本発明の実施態様を構成する構成要素の多数の考えられる配置を示す一連の図である。具体的には、図４ａは、署名エンティティがメッセージおよびシグネーチャを検証エンティティに与える実施態様を示す図である。
【図４ｂ】本発明の実施態様を構成する構成要素の多数の考えられる配置を示す一連の図である。具体的には、図４ｂは、エージェントを使用してシグネーチャを与える応用例を示す図である。
【図４ｃ】本発明の実施態様を構成する構成要素の多数の考えられる配置を示す一連の図である。図４ｃは、エージェントを使用してシグネーチャを与える別な応用例を示す図である。
【図４ｄ】本発明の実施態様を構成する構成要素の多数の考えられる配置を示す一連の図である。具体的には、図４ｄは、エージェントを使用してメッセージおよびシグネーチャを検証する応用例を示す図である。
【図４ｅ】本発明の実施態様を構成する構成要素の多数の考えられる配置を示す一連の図である。具体的には、図４ｅは、エージェントを使用してメッセージおよびシグネーチャを検証する別な応用例を示す図である。
【図４ｆ】本発明の実施態様を構成する構成要素の多数の考えられる配置を示す一連の図である。具体的には、図４ｆは、エージェントを使用してメッセージおよびシグネーチャを検証するさらに別な応用例を示す図である。
【図４ｇ】本発明の実施態様を構成する構成要素の多数の考えられる配置を示す一連の図である。具体的には、図４ｇは、エージェントを使用してメッセージおよびシグネーチャを検証するさらに別な応用例を示す図である。
【図５】セールスの実例として、メッセージユニットを署名ベリファイするために本発明をどのように使用するかを示すＥＩＭ会話型メッセージングダイアログ図である。
【図６】多数のオプションを備えた本発明を示す概略ブロック線図である。
【図７】シグネーチャ検証サービスを含むように具体化した本発明を示す概略ブロック線図である。　なお、図中、同じ符号は同じ構成要素およびステップを示す。
【符号の説明】
【００７１】
１０：ＤＳＶシステム、
１２：シグネーチャシステム、
１４：署名エンティティ、
１６、２６：ボールト、
１８：メッセージ、
２０：私的クレデンシャル、
２２：シグネーチャキー、
２４：シグネーチャ、
３２：ベリファイシステム、
３４：検証エンティティ、
３６：ベリファイヤ、
３８：ベリファイキー、
４０：アサーション、
４２：検証レスポンス、
４４：タイム・スタンプ、
５０：プロセス、
５２～５６、６０、６２、６４、６６、６８：ステップ。

【図１】

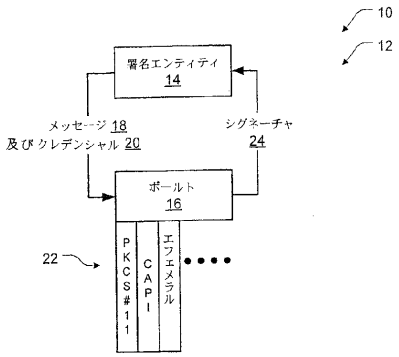


FIG. 1

【図２】

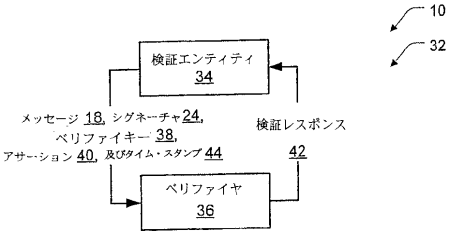


FIG. 2

【図３】

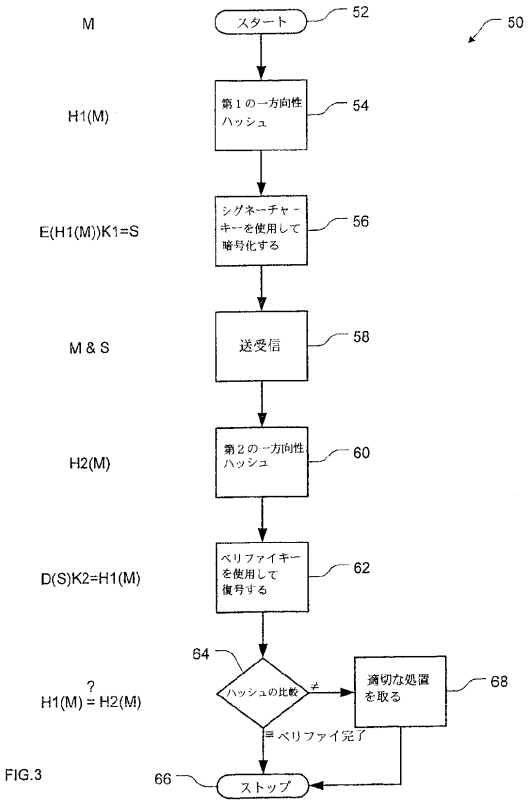


FIG.3

【図４ａ】

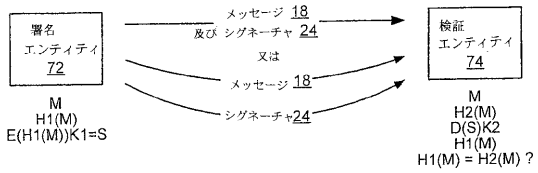


FIG. 4a

【図４ｂ】

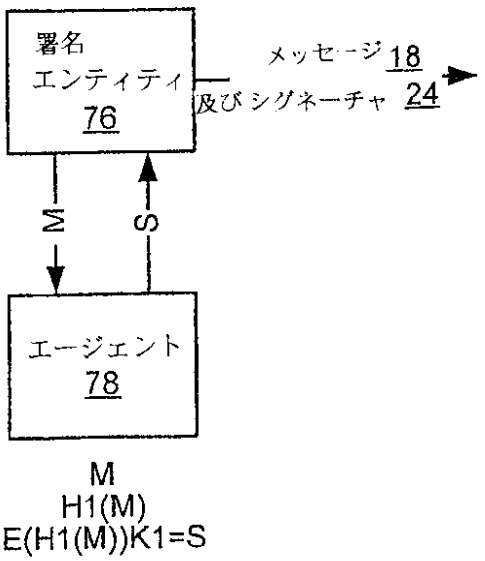


FIG. 4b

【図４ｃ】

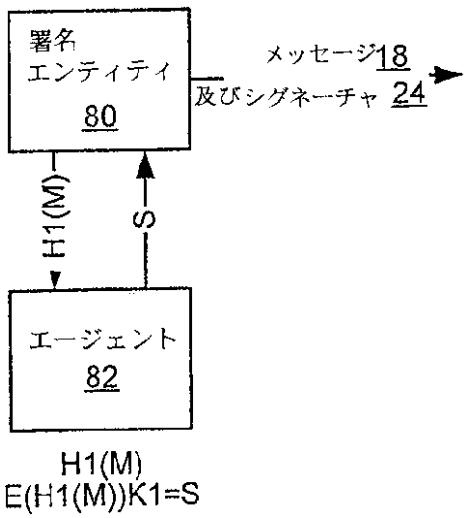
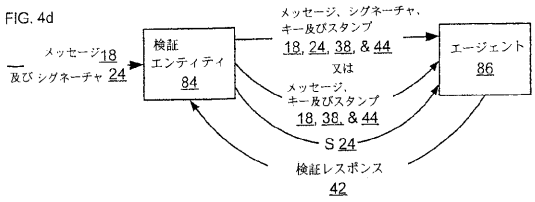
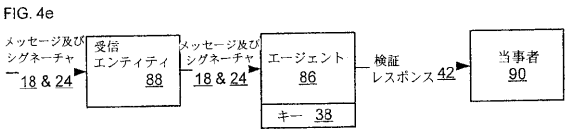


FIG. 4c

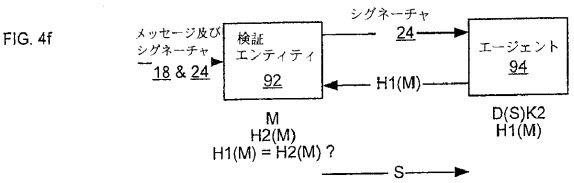
【図４ｄ】



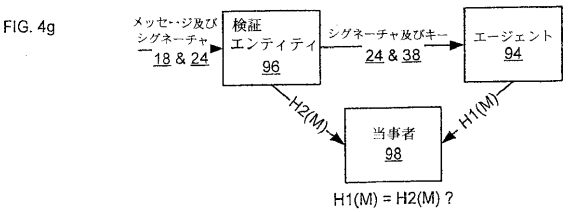
【図４ｅ】



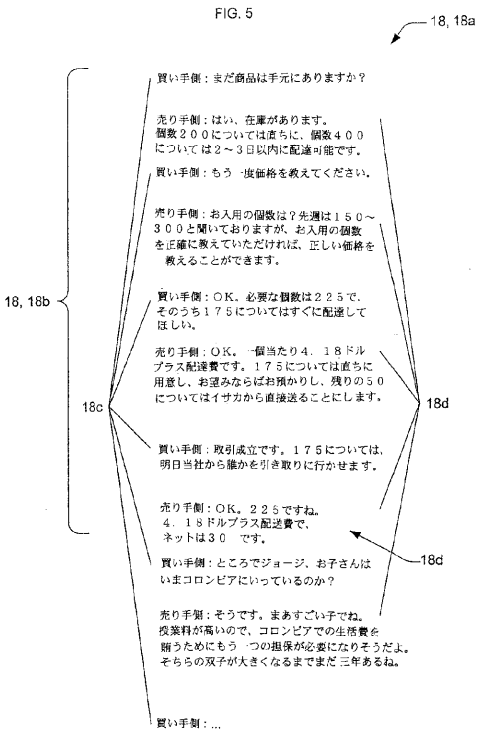
【図４ｆ】



【図４ｇ】



【図５】



【図６】

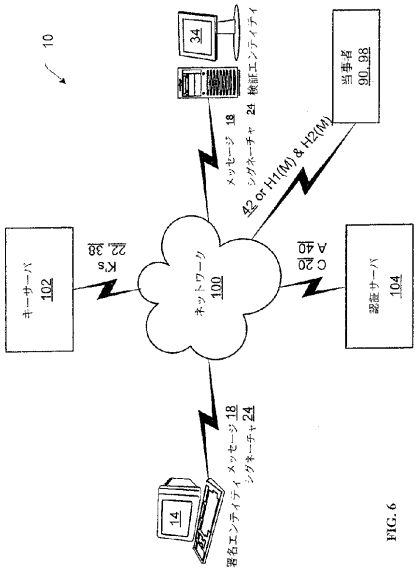


FIG. 6

【図７】

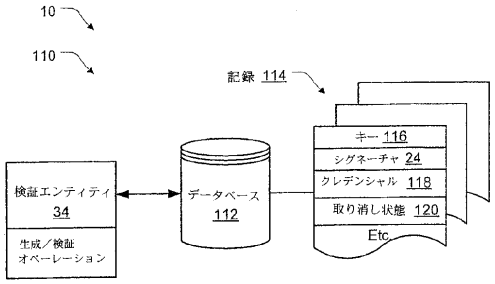


FIG. 7

【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】
会話型メッセージの通信方法において、
第１のコンピュータ化システムで、上記会話型メッセージに基づいて第１ハッシュ値を計算するステップ、
第２のコンピュータ化システムで、シグネーチャキーに基づいて上記第１ハッシュ値を暗号化することによってデジタルシグネーチャを生成するステップ、
ネットワークを介して、上記デジタルシグネーチャを第３のコンピュータ化システムに通信するとともに、上記会話型メッセージを第４のコンピュータ化システムに通信するステップ、
上記第３のコンピュータ化システムで、検証キーに基づいて上記デジタルシグネーチャを復号して上記第１ハッシュ値を再生するステップ、
上記第４のコンピュータ化システムで、上記会話型メッセージに基づいて第２ハッシュ値を計算するステップ、および
第５のコンピュータ化システムで、上記第１ハッシュ値と上記第２ハッシュ値とを比較して検証レスポンスを決めるステップからなり、
上記検証レスポンスは、上記第１ハッシュ値と上記第２ハッシュ値とが一致したときに検証すべき会話型メッセージを示し、および上記第１のコンピュータ化システムおよび上

記第２のコンピュータ化システムとして同じか同一でないシステムを利用し、かつ上記第３のコンピュータ化システム、上記第４のコンピュータ化システムおよび上記第５のコンピュータ化システムとしてすべて同じシステムを利用するか、一部のシステムとして同じシステムを利用するか、あるいはすべて同一でないシステムを利用することを特徴とする会話型メッセージの通信方法。

【請求項２】

会話型メッセージを対象とするデジタルシグネーチャの生成方法において、

第１のコンピュータ化システムで、上記会話型メッセージに基づいてハッシュ値を計算するステップ、および

第２のコンピュータ化システムで、シグネーチャキーに基づいて上記ハッシュ値を暗号化することによって上記デジタルシグネーチャを生成するステップからなり、

上記第１のコンピュータ化システムおよび上記第２のコンピュータ化システムとして同じか同一でないシステムを利用することを特徴とする会話型メッセージを対象とするデジタルシグネーチャの生成方法。

【請求項３】

上記会話型メッセージを署名エンティティによって署名し、そしてさらにこの署名エンティティを認証するステップを有する請求項２記載の方法。

【請求項４】

上記認証ステップで、上記署名エンティティの私的クレデンシャルを検証する請求項３記載の方法。

【請求項５】

上記シグネーチャキーは、ＰＫＩ環境で発行されたＸ．５０９サーティフィケートから得られたものでない請求項２記載の方法。

【請求項６】

少なくとも、上記の暗号化ステップをボールトで行う請求項２記載の方法。

【請求項７】

会話型メッセージユニットを署名エンティティによって署名し、そして

上記暗号化ステップを実行する前に、上記ボールトが上記署名エンティティを認証する請求項６記載の方法。

【請求項８】

上記会話型メッセージは複数の会話型メッセージユニットを有し、そして

上記計算するステップおよび上記暗号化ステップは上記複数の会話型メッセージユニットに基づいて一括的に行われる請求項２記載の方法。

【請求項９】

会話型メッセージを対象とするデジタルシグネーチャの検証方法において、

第１のコンピュータ化システムで、検証キーに基づいて上記デジタルシグネーチャを復号して第１ハッシュ値を再生するステップ、

第２のコンピュータ化システムで、上記会話型メッセージに基づいて第２ハッシュ値を計算するステップ、および

第３のコンピュータ化システムで、上記第１ハッシュ値と上記第２ハッシュ値とを比較して検証レスポンスを決めるステップからなり、

上記検証レスポンスは、上記第１ハッシュ値と上記第２ハッシュ値とが一致したときに検証すべき会話型メッセージを示し、そして上記第１のコンピュータ化システム、上記第２のコンピュータ化システムおよび上記第３のコンピュータ化システムとしてすべて同じシステムを利用するか、一部のシステムとして同じシステムを利用するか、あるいはすべて同一でないシステムを利用することを特徴とするデジタルシグネーチャの検証方法。

【請求項１０】

上記会話型メッセージを検証エンティティによって検証し、そしてさらにこの検証エンティティを認証するステップを有する請求項９記載の方法。

【請求項１１】

上記認証するステップは、上記検証エンティティのアサーションを検証する請求項１０の方法。
【請求項１２】
上記検証キーが、ＰＫＩ環境で発行されたＸ．５０９サーティフィケートから得られたものでない請求項１５の方法。
【請求項１３】
少なくとも、上記復号するステップは、ベリファイヤで行われる請求項９記載の方法。
【請求項１４】
上記デジタルシグネーチャを検証エンティティによって検証し、そして
上記復号するステップを実行する前に、上記ベリファイヤが上記検証エンティティを認証する請求項１３記載の方法。
【請求項１５】
上記検証レスポンスを第３者に通信するステップをさらに有する請求項９記載の方法。
【請求項１６】
上記第１ハッシュ値および上記第２ハッシュ値を第３者に通信するステップをさらに有する請求項９記載の方法。
【請求項１７】
会話型メッセージを対象とするデジタルシグネーチャの生成装置において、
上記会話型メッセージに基づいてハッシュ値を計算できるロジックを有する第１のコンピュータ化システム、および
上記ハッシュ値をシグネーチャキーに基づいて暗号化できるロジックを有することによって上記デジタルシグネーチャを生成する第２のコンピュータ化システムからなり、
上記第１のコンピュータ化システムおよび上記第２のコンピュータ化システムの両者を同じシステムとして構成するか、同一でないシステムとして構成したことを特徴とする生成装置。
【請求項１８】
上記会話型メッセージを署名エンティティによって署名し、そして上記第２のコンピュータ化システムはネットワークを介してサーバで上記署名エンティティを認証できるロジックをさらに有する請求項１７記載の生成装置。
【請求項１９】
上記の認証できるロジックは上記署名エンティティの私的クレデンシャルも検証する請求項１７記載の生成装置。
【請求項２０】
上記第２のコンピュータ化システムは、上記ハッシュ値をボールトで暗号化する請求項１７記載の生成装置。
【請求項２１】
上記ボールトは、このボールトから物理的に離間しているサーバから上記シグネーチャキーを取得し、上記会話型メッセージユニットを署名エンティティによって署名し、そして上記第２のコンピュータ化システムは、ネットワークを介してサーバで上記ボールトの上記署名エンティティを認証できるロジックをさらに有する請求項１７記載の生成装置。
【請求項２２】
上記第１のコンピュータ化システムは、複数の会話型メッセージユニットを含むように上記会話型メッセージを構成できるロジックをさらに有する請求項１７記載の生成装置。
【請求項２３】
会話型メッセージを対象とするデジタルシグネーチャの検証装置において、
検証キーに基づいて上記デジタルシグネーチャを復号して第１ハッシュ値を再生できるロジックを有する第１のコンピュータ化システム、
上記会話型メッセージに基づいて第２ハッシュ値を計算できるロジックを有する第２のコンピュータ化システム、および
上記第１ハッシュ値と上記第２ハッシュ値とを比較して検証レスポンスを決めることが

できるロジックを有する第３のコンピュータ化システムからなり、
上記検証レスポンスは、上記第１ハッシュ値と上記第２ハッシュ値とが一致したときに検証すべき会話型メッセージを示し、そして上記第１のコンピュータ化システム、上記第２のコンピュータ化システムおよび上記第３のコンピュータ化システムのすべてあるいは一部を同じシステムとするか、あるいはすべてを同じシステムとしないことを特徴とする検証装置。
【請求項２４】
上記第１のコンピュータ化システムは、ネットワークを介してサーバで上記検証エンティティを認証できるロジックをさらに有する請求項２３記載の検証装置。
【請求項２５】
上記第１のコンピュータ化システムは、上記デジタルシグネーチャをベリファイヤにおいて復号する請求項２３記載の検証装置。
【請求項２６】
上記第１のコンピュータ化システムは、ネットワークを介してサーバから上記ベリファイヤの上記検証キーを取得できるロジックをさらに有し、上記デジタルシグネーチャを検証エンティティによって検証し、そして上記第１のコンピュータ化システムは、ネットワークを介してサーバで上記ベリファイヤの上記検証エンティティを認証できるロジックをさらに有する請求項２５記載の検証装置。
【請求項２７】
上記会話型メッセージはダイアログに少なくとも一つの会話型メッセージ要素を有し、そして上記第１のコンピュータ化システム、上記第２のコンピュータ化システムおよび上記第３のコンピュータ化システムの一つは、上記会話型メッセージ要素を有するトランスクリプトを記憶できるロジックをさらに有する請求項２３記載の検証装置。
【請求項２８】
上記第３のコンピュータ化システムは上記第１のコンピュータ化システムでもなくまた上記第２のコンピュータ化システムでもなく、
上記第１のコンピュータ化システムは、ネットワークを介して上記第１ハッシュ値を上記第３のコンピュータ化システムに通信できるロジックをさらに有し、そして
上記第２のコンピュータ化システムは、上記ネットワークを介して上記第２ハッシュ値を上記第３のコンピュータ化システムに通信できるロジックをさらに有する請求項２３記載の検証装置。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/19954

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :H04L 9/00
US CL : 713/176, 201
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)
U.S. : 713/176, 201

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 practicable, search terms used)
Internet, Inspect, WEST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,787,175 A (CARTER) 28 Jul 1998, Figures 1, 3 Abstract, Columns 9-16	1-74
Y	US 5,915,024 A (KITAORI et. al.) 22 June 1999 Abstract, Figure 4	1-74
A	US 2002/0053021 A1 (RICE et. al.) 02 May 2002 Abstract, Figure 1, 3	1-74
A	US 6,418,457 B1 (SCHMIDT et. al.) 09 July 2002	1-74
A	US 5,659,616 A (SUDIA) 19 August 1997	1-74

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"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
"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)	"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
"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	"&"	document member of the same patent family

Date of the actual completion of the international search 11 SEPTEMBER 2003	Date of mailing of the international search report 26 SEP 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Ayaz Sheikh Telephone No. (703) 308-4562

Form PCT/ISA/210 (second sheet) (July 1998)★

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,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
ＵＮＩＸ

(72)発明者 モレイ，ジャハーンシャー
アメリカ合衆国 カリフォルニア州 ９００６７，ロサンゼルス，アパートメント ４１７，センチュリー パーク レーン ２１２２
(72)発明者 オルキン，ジェフリイ シー.
アメリカ合衆国 カリフォルニア州 ９４０６２，ウッドサイド，マウンテン ホーム ロード １０１５

Ｆターム(参考) 5J104 LA01 PA07