(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4695633号
(P4695633)
(45)発行日　平成23年6月8日(2011.6.8)　(24)登録日　平成23年3月4日(2011.3.4)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675B
G06Q 30/00	(2006.01)	G06F	17/60	312
H04W 74/08	(2009.01)	H04L	12/28	307
H04W 84/12	(2009.01)	G06F	17/60	302E
G06Q 10/00	(2006.01)	G06F	17/60	512

請求項の数 20　外国語出願　(全 33 頁)　最終頁に続く

(21)出願番号　特願2007-264576 (P2007-264576)
(22)出願日　平成19年10月10日 (2007.10.10)
(65)公開番号　特開2008-167406 (P2008-167406A)
(43)公開日　平成20年7月17日 (2008.7.17)
審査請求日　平成19年10月10日 (2007.10.10)
(31)優先権主張番号　06122033.1
(32)優先日　平成18年10月10日 (2006.10.10)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100099623
弁理士　奥山　尚一
(74)代理人　100096769
弁理士　有原　幸一
(74)代理人　100107319
弁理士　松島　鉄男
(72)発明者　ジーナ・コンガ
ドイツ連邦共和国，８１２４５　ミュンヘン，ヒルマーヴェーク　１０

最終頁に続く

(54)【発明の名称】ディジタルリソースを販売する方法および装置

(57)【特許請求の範囲】
【請求項１】
あるディジタルリソースｒをある売り手のノードＳからある買い手のノードＢへ販売する方法であって、
前記売り手のノードおよび前記買い手のノードの公開鍵が正当なオーナーによって使用されることを確認するために、固定ネットワークまたは信頼できる第三者へ接続することなく、前記売り手のノードと前記買い手のノードとを互いに認証するステップと、
前記売り手によって販売される前記ディジタルリソースに前記買い手がアクセスするのを可能にするために、前記売り手のノードがライセンスを生成するステップであって、前記ライセンスが鍵を含むものである、ステップと、
前記ライセンス内に含まれる前記鍵によって前記ディジタルリソースを暗号化するステップと、
前記暗号化されたディジタルリソースを含むメッセージを送信し、かつ、前記メッセージの署名または署名されたハッシュを送信するステップであって、前記署名が前記売り手の秘密鍵を用いて生成されるものである、ステップと、
前記買い手が前記ディジタルリソースを使用するのを可能にするために、前記ライセンスを前記売り手から前記買い手のノードへ転送するステップと
を含む方法。
【請求項２】
マルチメディアリソースを購入または販売することに参加できるように前記買い手のノ

ード及び前記売り手のノードの装置を設定するために、信頼できる課金機関から前記買い手のノード及び前記売り手のノードに設定データが送信されると、前記売り手の秘密鍵を用いて生成された前記メッセージの署名または前記メッセージの署名されたハッシュとともに、前記暗号化されたディジタルリソースを含む前記メッセージを、前記売り手が前記ディジタルリソースを販売した証拠として、前記買い手が前記信頼できる課金機関に対して使用するステップであって、前記設定データは、前記買い手のノード及び前記売り手のノードが前記マルチメディアリソースを販売および／または購入することが許されているかどうかを示す情報を含むものである、ステップと、

前記証拠に基づいて課金を実行するステップと

をさらに含む請求項１に記載の方法。

【請求項３】

前記暗号化されたディジタルリソースを含む前記メッセージが、現在の時刻をさらに含むものであり、前記署名を生成するのに使用された前記売り手の前記秘密鍵が、前記メッセージが送信されたときに有効であった秘密鍵である、請求項２に記載の方法。

【請求項４】

前記ライセンスが、前記買い手の前記秘密鍵を用いて生成された確認の署名または署名されたハッシュとともに、前記買い手が前記ディジタルリソースを購入したいことを確認する確認メッセージを前記買い手が送信した後にしか、前記売り手から前記買い手へ送信されないものである、請求項１から請求項３までのいずれか一項に記載の方法。

【請求項５】

前記確認メッセージが、前記暗号化されたディジタルリソースのハッシュと、前記確認メッセージ上の署名または署名されたハッシュとを備えるものである、請求項４に記載の方法。

【請求項６】

マルチメディアリソースを購入または販売することに参加できるように前記買い手のノード及び前記売り手のノードの装置を設定するために、信頼できる課金機関から前記買い手のノード及び前記売り手のノードに設定データが送信されると、前記買い手の前記秘密鍵を用いて生成された前記確認メッセージ上の署名または署名されたハッシュとともに、前記買い手からの前記確認メッセージを、前記買い手が前記ディジタルリソースを購入した証拠として、前記売り手が前記信頼できる課金機関に対して使用するステップであって、前記設定データは、前記買い手のノード及び前記売り手のノードが前記マルチメディアリソースを販売および／または購入することが許されているかどうかを示す情報を含むものである、ステップと、

前記証拠に基づいて課金を実行するステップと

をさらに含む請求項１から請求項５までのいずれか一項に記載の方法。

【請求項７】

前記確認メッセージが、

前記買い手が前記ディジタルリソースを購入したいという確認ステートメントと、

前記暗号化されたディジタルリソース、ハッシュ、またはディジタルリソースの署名されたハッシュと、

現在の時刻と、

前記確認メッセージが送信されたときに有効であった前記買い手の前記秘密鍵によって生成された、以前の元上の署名または署名されたハッシュと

の中の１つまたは複数を含むものである、請求項６に記載の方法。

【請求項８】

前記互いに認証するステップが、前記売り手のノードに対して前記買い手のノードを認証するステップを含み、前記買い手のノードを認証するステップが、

前記買い手のノードが秘密鍵ｓを選択し、そして、前記買い手のノードの証明データ内に含まれる固有のハッシュコード値を介して前記買い手のノードのアイデンティティに結合されるワンウェイ・ハッシュ・チェーンを生成するのに、前記秘密鍵ｓを使用すること

と、
前記買い手のノードが、前記買い手のノードの前記ワンウェイ・ハッシュ・チェーンを用いて、整数であるｍ個の公開鍵／秘密鍵のペアを導出し、前記公開鍵／秘密鍵のペアが、互いに結合され、かつ、前記買い手のノードの前記証明データ内に含まれるハッシュコード値に結合されることと、
前記買い手のノードが、前記導出した公開鍵の中の１つをそれの証明データとともに前記売り手のノードに送信することと、
前記売り手のノードが、開示された公開鍵が前記買い手のノードの前記証明データ内に含まれるハッシュコードに結合されていることを確認することによって、前記買い手のノードを認証することと、
前記買い手のノードが前記売り手のノードに対して認証されたのと同じようにして、前記売り手のノードを前記買い手のノードに対して認証することと
を含む、請求項１から請求項７までのいずれか一項に記載の方法。
【請求項９】
時間区間Ｔ$_{i}$、０≦ｉ＜ｍ、において、前記買い手のノードが、
【数１】

$$K_{m-1-i}=\prod_{j=0}^{m-i-1} f^{j}(s)$$

を秘密鍵として使用し、かつ、
【数２】

$$g^{K_{m-1-i}}$$

を対応する公開鍵として使用し、Ｇ＝（Ｇ，＊）が、位数ｑの有限巡回群であり、ｇ∈Ｇが、Ｇの生成元であるように、前記公開鍵が選択され、
ｇに対してＧにおける離散的対数を計算することが、計算処理的に不可能であると仮定され、
ｆが、集合｛０，１，．．．，ｑ－１｝をそれ自体の上に写像する暗号（ワンウェイ）ハッシュ関数である、請求項８に記載の方法。
【請求項１０】
信頼できる第三者により前記買い手のノードと前記売り手のノードとを初期化するステップをさらに含み、前記初期化するステップが、
Ｇ、ｆ、ｍ、信頼できる第三者の公開鍵Ｋ$_{TTP}$、および、ワンウェイハッシュ関数であるｈを、前記買い手のノードに配信することと、
前記買い手のノードおよび前記売り手のノードのクロックを、前記信頼できる第三者のクロックに同期させることと、
ノードのアイデンティティを証明したいノードに対して、
【数３】

$$v=h(g^{\prod_{j=0}^{m} f^{j}(s)})$$

に基づいて検査値を計算し、かつ、

【数４】

$$[ID, v, t_0, L]_{K_{TTP}^{-1}}$$

に基づいて前記証明データを計算し、ここで、ＩＤが前記ノードの識別子であり、ｔ$_0$が証明データの発行時刻であり、Ｌが公開鍵／秘密鍵のペアが有効である時間区間の長さを定義し、そして、

【数５】

$$[\ldots]_{K_{TTP}^{-1}}$$

が、ＴＴＰによって、前記証明データの体上におけるＴＴＰの秘密鍵

【数６】

$$K_{TTP}^{-1}$$

で生成された署名であることと
を含む、請求項８または請求項９に記載の方法。

【請求項１１】
前記買い手のノードを認証するステップが、
前記買い手のノードが、時間区間Ｔ$_i$、０≦ｉ＜ｍにおいて、

【数７】

$$K_{m-1-i} = \prod_{j=0}^{m-i-1} f^j(s)$$

を秘密鍵として使用し、かつ、

【数８】

$$g^{K_{m-1-i}}$$

を対応する公開鍵として使用することと、
前記売り手のノードが公開鍵

【数９】

$$g^{K_w}$$

の確認されたコピーを入手するのを可能にするために、前記買い手のノードから前記売り手のノードに、

【数１０】

$$g^{K_w}$$

と、ｆ$^{w+1}$（ｓ）とを送信することと
を備えており、

前記証明データがｖを含み、そして前記売り手のノードが、ｆ^{j}（ｓ）、ｗ＋１≦ｊ≦ｍを計算し、そしてこれらの値を用いて、前記売り手のノードが、

【数１１】

$$v^{*} = (g^{K_w})^{\prod_{j=w+1}^{m} f^{j}(s)}$$
$$= g^{\prod_{j=0}^{w} f^{j}(s) \prod_{j=w+1}^{m} f^{j}(s)}$$
$$= g^{\prod_{j=0}^{m} f^{j}(s)}.$$

を計算し、前記買い手のノードのアイデンティティを確認するために、ｖ＝ｈ（ｖ＊）であることを検査する、

請求項１０に記載の方法。

【請求項１２】

クロックドリフトが、同期したクロック間の最大クロックドリフトを定義することによって考慮され、さらに、前記クロックドリフトが、起こりうるクロックドリフトを考慮すべき認証中に、１つよりも多い鍵が開示されてもよいかどうかを定義することによって考慮される、請求項１０又は１１に記載の方法。

【請求項１３】

信頼できる第三者により前記買い手のノードと前記売り手のノードとを初期化するステップをさらに含み、前記初期化するステップにおいて、前記買い手のノードと前記売り手のノードが、前記信頼できる第三者から証明データを受信し、

前記証明データが、

ユーザ識別子と、

前記証明データを発行した前記プロバイダーまたは前記信頼できる第三者の識別子と、

前記証明データを発行した前記プロバイダーまたは前記信頼できる第三者のディジタル署名と、

前記証明データの発行時刻と、

ユーザ検査値と、

ユーザがマルチメディアリソースを販売／購入するのを許されているかどうかの指示と

からなる要素の中の１つまたは複数を備えるものである、請求項１から請求項１２までのいずれか一項に記載の方法。

【請求項１４】

信頼できる第三者により前記買い手のノードと前記売り手のノードとを初期化するステップをさらに含み、前記初期化するステップが、マルチメディアリソースを購入または販売することに参加できるように前記ユーザの装置を設定するために、ネットワーク事業者または信頼できる第三者から前記ユーザに設定データを送信することを含んでおり、前記設定データが、

前記ネットワーク事業者または前記信頼できる第三者の公開鍵と、

別の信頼できるネットワーク事業者または信頼できる第三者の公開鍵と、

どの課金情報が収集されなければならないかの指示と、

ネットワーク事業者のＡＡＡサーバーまたは信頼できる第三者のＡＡＡサーバーのアドレスと、

前記ユーザがマルチメディアリソースを販売／購入するのを許されているかどうかの指示と、

リソースを購入する限度額と

からなる複数のデータの中の１つまたは複数を含むものである、請求項１から請求項１３までのいずれか一項に記載の方法。

【請求項１５】
前記売り手が前記ディジタルリソースを販売したことを証明するために、信頼できる課金機関に対してある買い手が使用する証拠が、
前記売り手の証明データと、
前記暗号化されたリソースが送信されたときに有効であった前記売り手の公開鍵、および前記売り手のワンウェイ・ハッシュ・チェーンの対応する元と、
現在時刻と前記暗号化されたリソースとを含むものであるＭＥＳ送信リソース・メッセージと、
前記リソースが送信されたときに有効であった前記売り手の秘密鍵によって署名された前記ＭＥＳ送信リソースのハッシュを含むものであるＭＥＳ送信ハッシュ・メッセージと
からなる要素の中の１つまたは複数を備えるものである、請求項１から請求項１４までのいずれか一項に記載の方法。
【請求項１６】
ある売り手が前記ディジタルリソースを販売したことを証明するために、信頼できる課金機関に対して前記売り手が使用する証拠が、
前記買い手の証明データと、
前記暗号化されたリソースｒのハッシュ、または前記ＭＥＳ送信ハッシュ・メッセージのコピーと、
前記暗号化されたリソースが送信されたときに有効であった前記買い手の公開鍵と、前記買い手の公開鍵の正当性を確認するのを可能にする前記買い手のワンウェイ・ハッシュ・チェーンの対応する元と、
現在時刻と、前記買い手が前記ディジタルリソースを購入したいことを確認する確認ステートメントと、前記暗号化されたリソースのハッシュと、前記現在時刻に基づいた前記買い手のディジタル署名とを含むものであるＭＥＳ購入要求メッセージと
からなる要素の中の１つまたは複数を備え、前記確認ステートメントと前記暗号化されたリソースの前記ハッシュとが、確認が送信されたときに有効であった秘密鍵によって生成されるものである、請求項１から請求項１５までのいずれか一項に記載の方法。
【請求項１７】
前記証拠が、前記暗号化されたディジタルリソースに対するライセンスをさらに備えるものである、請求項１６に記載の方法。
【請求項１８】
あるディジタルリソースｒをある売り手のノードＳからある買い手のノードＢへ販売する装置であって、
前記売り手のノードおよび前記買い手のノードの公開鍵が正当なオーナーによって使用されていることを確認するために、固定ネットワークまたは信頼できる第三者へ接続することなく、前記売り手および買い手のノードをお互いに認証するモジュールと、
前記売り手によって販売される前記ディジタルリソースに前記買い手がアクセスするのを可能にするために、前記売り手のノードがライセンスを生成するモジュールであって、前記ライセンスが鍵を含むものである、モジュールと、
前記ライセンス内に含まれる鍵によって前記ディジタルリソースを暗号化するモジュールと、
前記暗号化されたディジタルリソースを含むメッセージを送信し、かつ、前記メッセージの署名または署名されたハッシュを送信するモジュールであって、前記署名が前記売り手の秘密鍵を用いて生成されるものである、モジュールと、
前記買い手が前記ディジタルリソースを使用するのを可能にするために、前記ライセンスを前記売り手から前記買い手へ転送するモジュールと
を備えるものである装置。
【請求項１９】
請求項１から請求項１７までのいずれか一項に記載された方法を実行するためのモジュールをさらに備えている請求項１８に記載の装置。

【請求項２０】
コンピュータ上で実行する際に、前記コンピュータが請求項１から請求項１７までのいずれかに記載された方法を実行するのを可能にするコンピュータプログラムコードを含んでいるコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、特に、アドホックネットワークにおいて、ディジタルリソースを販売する方法および装置に関する。
【背景技術】
【０００２】
エンターテイメントの分野は、繁盛しているビジネス分野である。毎年、レコード会社は、何百万枚ものＣＤを販売している。さらに多くの枚数を販売するために、新しい配信システムが設計されている。今日、音楽は、モバイルネットワークにおいてダウンロードすることができる。これにより、レコード会社が何百万人もの潜在的な販売者（売り手）および購入者（買い手）とつながることができる。また、これは、モバイルネットワーク事業者がマルチメディアサービスを新たに提供することによって、より多くのユーザを「勧誘」するのを可能にする。エンターテイメントとモバイルネットワークビジネスとの関係は、音声会話を可能にするように設計されるだけでなく、写真を撮ること、ビデオを撮影すること、および、音楽およびビデオを再生することをも可能にするように設計された、携帯端末の発展によって知ることができる。現在、携帯電話は、たとえそれの所有者がどこにいようとも音楽およびビデオを入手するのを可能にする、マルチメディアプレーヤーである。マルチホップ通信によって、ユーザは、例えば、地下鉄、電車、などのような固定ネットワークが到達できない場所において、ビデオおよび音楽をダウンロードすることができる。しかしながら、マルチメディアリソースは、多くの場合、財産権によって保護されているので、アドホックネットワークにおいてそれらのリソースを交換することは制限されなければならず、財産権は守られなければならず、最終的に、マルチメディアリソースの販売は報酬を支払われなければならない。さらに、アドホックネットワークにおいてリソースを購入することは、ユーザにとって興味のあることである。なぜなら、それらのユーザはリソースを購入するとすぐに、そのリソースを使用することができるからである。このことは、あらかじめ知られていない可能性がある当事者と通信することによって生成された課金証拠が正当なものであることを、アドホックネットワークのノードが確信するのを可能にすることができる、認証（authentication）、許可（authorization）、課金（accounting）（ＡＡＡ）の必要性を高めている。また、このことは、アドホックネットワークにおいて販売されたリソースの監査およびチャージングの必要性を高めている。
【０００３】
アドホックネットワークは、誰かがＡＡＡを提供したいときにいくつかの制約をもたらすという特徴を有する。固定ネットワークと違って、アドホックネットワークは、適切なメッセージ配信を保証するために、あるいは、ネットワークメンバーシップを制御するために、中央管理機関（central administration authority）によって動作するものではなく、また、既存のインフラストラクチャーに依存するものでもない。その代わりに、ノードは、宛て先に到達するまで、それらに隣接するノードによって送信されたメッセージを転送することによって、協働しなければならない。しかしながら、様々な団体から到着する可能性があるノードは、未知のエンティティーと協働するインセンティブをまったく持たない場合がある。
【０００４】
協働を促すために、協力的なノードに報酬を支払ういくつかのアプローチが、定義されてきた（例えば、非特許文献１、非特許文献２、または非特許文献３を参照）。
【０００５】

これらのアプローチは、パケットごとの課金処理を提供する。これらは、固定ネットワークまたは中央機関が常に到達することのできる場所に接続された、アドホックネットワークのために設計されたものである。しかしながら、そのような接続性は、アドホックネットワークにおいて常に利用可能なものではない。なぜなら、ノードは自由に移動することができ、それによって、ソースノードと宛て先ノードとの間の接続性は、いつでも切断される可能性があるからである。これは、ネットワークを孤立させることがあり、かつ、ノードが、信頼できる第三者（ＴＴＰ）への保証されたアクセスを妨げられることがある。それは、ノードが、中央エンティティーと連絡することによって、不正なノードを検出するのを妨げる可能性がある。またそれは、ノードが、初期の認証段階中に協力的なノードとして識別されるのに使用することのできる、期限切れでない証明データを得るために、プロバイダーと連絡するのを妨げる可能性もある。

【０００６】

これらの問題を回避するために、報酬を与えるプロセスで何らかの第三者を使用するのではなく、公開鍵および秘密鍵を記憶しかつ信頼性を保証する、セキュリティーモジュールと呼ばれる不正操作しにくいハードウェアモジュール（tamper-resistant hardware module）に頼るアプローチが、提案されている（非特許文献４を参照）。

【０００７】

非特許文献５において説明されるもう１つのアプローチは、何らかの不正操作しにくいハードウェアモジュールを使用するのではなく、非特許文献６または非特許文献７に説明されるような、拡張性のある証明機関（ＣＡ）を使用することである。しかしながら、非特許文献６のＺｈｏｕらは、証明データ内に含まれるアイデンティティ（identity）が正当なものであることを保証しておらず、かつ、証明データが取り消されていないことを確認するのを可能にしていない。Ｌｕｏらは、それぞれのノードが固有の非ゼロＩＤ（nonzero ID）を有することを仮定しているが、Ｚｈｏｕらと同様に、ノードは、主張されたアイデンティティが、本当にあるノードによって所有されるものであることを確認する手段を有していない。これは、ノードが、異なるアイデンティティを備える多くの証明データを発行されるのを可能にするものであって、ここで、この証明データは送信するはずのない何らかのパケットに対する何らかの信用を受信するのに使用されうるものである。

【非特許文献１】Ｋｏｆｍａｎ ａｎｄ Ｍ．Ｍａｕｖｅ，「Ｌｉｇｈｔ－Ｗｅｉｇｈｔ Ｃｈａｒｇｉｎｇ ａｎｄ Ａｃｃｏｕｎｔｉｎｇ ｉｎ Ｍｏｂｉｌｅ ａｄ－Ｈｏｃ－Ｎｅｔｗｏｒｋｓ」ｉｎ ＡＣＭ ＳＩＧＭＯＢＩＬＥ ＭｏｂｉＣｏｍ ２００５ Ｐｏｓｔｅｒ Ｓｅｓｓｉｏｎ，Ｓｅｐｔｅｍｂｅｒ ２００５

【非特許文献２】Ａ．Ｗｅｙｌａｎｄ ａｎｄ Ｔ．Ｂｒａｕｎ，「Ｃｏｏｐｅｒａｔｉｏｎ ａｎｄ Ａｃｃｏｕｎｔｉｎｇ Ｓｔｒａｔｅｇｙ ｆｏｒ Ｍｕｌｔｉ－ｈｏｐ Ｃｅｌｌｕｌａｒ Ｎｅｔｗｏｒｋｓ」ｉｎ １３ｔｈ ＩＥＥＥ Ｗｏｒｋｓｈｏｐ ｏｎ Ｌｏｃａｌ ａｎｄ Ｍｅｔｒｏｐｏｌｉｔａｎ Ａｒｅａ Ｎｅｔｗｏｒｋｓ，Ａｐｒｉｌ ２００４

【非特許文献３】Ｐ．Ｈｏｆｍａｎｎ ａｎｄ Ｃ．Ｐｒｅｈｏｆｅｒ，「Ｇａｔｅｗａｙ－Ｃｏｎｔｒｏｌｌｅｄ Ａｃｃｏｕｎｔｉｎｇ ｆｏｒ Ｇｌｏｂａｌ Ｃｏｎｎｅｃｔｉｖｉｔｙ ｉｎ Ａｄ Ｈｏｃ Ｎｅｔｗｏｒｋｓ」ｉｎ Ｆｉｒｓｔ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｃｏｎｆｅｒｅｎｃｅ ｏｎ Ｍｏｂｉｌｅ Ｃｏｍｐｕｔｉｎｇ ａｎｄ Ｕｂｉｑｕｉｔｏｕｓ Ｎｅｔｗｏｒｋｉｎｇ（ＩＣＭＵ ２００４），Ｊａｎｕａｒｙ ２００４

【非特許文献４】Ｌ．Ｂｕｔｔｙａｎ ａｎｄ Ｊ．－Ｐ．Ｈｕｂａｕｘ，「Ｎｕｇｌｅｔｓ：ａ Ｖｉｒｔｕａｌ Ｃｕｒｒｅｎｃｙ ｔｏ Ｓｔｉｍｕｌａｔｅ Ｃｏｏｐｅｒａｔｉｏｎ ｉｎ Ｓｅｌｆ－Ｏｒｇａｎｉｚｅｄ Ｍｏｂｉｌｅ Ａｄ Ｈｏｃ Ｎｅｔｗｏｒｋｓ」Ｅｃｏｌｅ Ｐｏｌｙｔｅｃｈｎｉｑｕｅ ｄｅ Ｌａｕｓａｎｎｅ（ＥＰＦＬ），Ｔｅｃｈ．Ｒｅｐ．，２００１

【非特許文献５】「Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ａｄ－Ｈｏｃ Ｎｅｔｗｏｒｋｓ」ｉｎ Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ＩＥＥＥ ＩＮＦＯＣＯＭ’０３，Ｓａｎ

Ｆｒａｎｃｅｓｃｏ，ＣＡ，Ａｐｒｉｌ　２００３
【非特許文献６】Ｌ．Ｚｈｏｕ　ａｎｄ　Ｚ．Ｊ．Ｈａａｓ，「Ｓｅｃｕｒｉｎｇ　Ａｄ　Ｈｏｃ　Ｎｅｔｗｏｒｋｓ」ＩＥＥＥ　Ｎｅｔｗｏｒｋ，ｖｏｌ．１３，ｎｏ．６，ｐｐ．２４－３０，１９９９
【非特許文献７】Ｈ．Ｌｕｏ，Ｐ．Ｚｅｆｒｏｓ，Ｊ．Ｋｏｎｇ，Ｓ．Ｌｕ，ａｎｄ　Ｌ．Ｚｈａｎｇ，「Ｓｅｌｆ－ｓｅｃｕｒｉｎｇ　Ａｄ　Ｈｏｃ　Ｗｉｒｅｌｅｓｓ　Ｎｅｔｗｏｒｋｓ」ｉｎ　Ｓｅｖｅｎｔｈ　ＩＥＥＥ　Ｓｙｍｐｏｓｉｕｍ　ｏｎ　Ｃｏｍｐｕｔｅｒｓ　ａｎｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ（ＩＳＣＣ’０２），２００２

【発明の開示】

【発明が解決しようとする課題】

【０００８】

既知であるこれらのアプローチは、どれも、孤立したアドホックネットワーク、すなわち、固定ネットワークとのどのような接続性も有していないアドホックネットワークにおいて、どのようにして認証が提供されるかを開示していない。したがって、本発明の目的は、アドホックネットワークにおいてディジタルリソースを販売するための改善された方法を提供することである。

【課題を解決するための手段】

【０００９】

一実施形態によれば、アドホックネットワークにおいて、あるディジタルリソースｒをある売り手のノードＳからある買い手のノードＢへ販売するための方法が提供され、当該方法は、

第１および第２のノードの公開鍵が正当なオーナーによって使用されることを確認するために、固定ネットワークまたは信頼できる第三者へ接続することなく、前記売り手のノードと前記買い手のノードとを互いに認証するステップと、

前記売り手によって販売される前記ディジタルリソースに前記買い手がアクセスするのを可能にするために、前記売り手のノードがライセンスを生成するステップであって、前記ライセンスが鍵を含むものである、ステップと、

前記ライセンス内に含まれる前記鍵によって前記ディジタルリソースを暗号化するステップと、

前記暗号化されたディジタルリソースを含むメッセージを送信し、かつ、前記メッセージの署名または署名されたハッシュを送信するステップであって、前記署名が前記売り手の秘密鍵を用いて生成されるものである、ステップと、

前記買い手が前記ディジタルリソースを使用するのを可能にするために、前記ライセンスを前記売り手から前記買い手へ転送するステップと、

を含む。

【００１０】

アドホックネットワークのノードにおけるライセンスの生成と、トランザクションに対する拒否できない証拠（non-repudiable evidence）として使用されうるメッセージの送信（および、記憶）とは、アドホックネットワークにおいてさえもディジタルリソースを販売するのを可能にする。暗号化されたディジタルリソースを含むメッセージおよび署名は、一緒に単一メッセージとして送信されてもよく、あるいは、別々のメッセージとして送信されてもよい。

【００１１】

一実施形態によれば、前記方法は、

信頼できる課金機関への接続が利用できるようになると、前記売り手の前記秘密鍵を用いて生成された前記メッセージ上の署名または前記メッセージの署名されたハッシュとともに、前記暗号化されたディジタルリソースを含む前記メッセージを、前記売り手が前記ディジタルリソースを販売した証拠として、前記買い手が、前記信頼できる課金機関に対して使用するステップと、

前記証拠に基づいて課金を実行するステップと

を含む。

【００１２】

これは、売り手がディジタルリソースを買い手に販売した拒否できない証拠を、買い手が信頼できる第三者に対して発行するのを可能にし、そして信頼できる第三者または何らかの課金エンティティーは、前記証拠に基づいて課金処理を実行しうる。

【００１３】

一実施形態によれば、前記暗号化されたディジタルリソースを含む前記メッセージは、現在時刻をさらに含み、前記署名または前記署名されたハッシュを生成するのに使用された前記売り手の前記秘密鍵は、前記メッセージが送信されたときに有効であった秘密鍵である。

【００１４】

時刻に依存した秘密鍵（time dependent private key）の使用は、セキュリティーを向上させる。

【００１５】

一実施形態によれば、前記ライセンスが、前記買い手の秘密鍵を用いて生成された確認の署名または確認の署名されたハッシュとともに、前記買い手が前記ディジタルリソースを購入したいことを確認する確認メッセージを前記買い手が送信した後にしか、前記売り手から前記買い手へ送信されないものである。

【００１６】

確認メッセージは、買い手が前記ディジタルリソースを購入する意思があったことの信頼できる第三者に対する証拠として、売り手によって使用されうる。

【００１７】

一実施形態によれば、前記確認メッセージは、前記暗号化されたリソースのハッシュと前記確認メッセージ上の署名とを備えるものである。

【００１８】

これは、買い手が実際にディジタルリソースを入手したという、信頼できる第三者に対する証拠として、売り手によって使用されてもよく、それによって、買い手がそれを購入したことを意味する。

【００１９】

一実施形態によれば、前記方法は、

前記信頼できる課金機関への接続を利用できるようになると、前記買い手の前記秘密鍵を用いて生成された前記確認メッセージの署名または署名されたハッシュとともに、前記買い手からの前記確認メッセージを、前記買い手が前記ディジタルリソースを購入した証拠として、前記売り手が、前記信頼できる課金機関に対して使用するステップと、

前記証拠に基づいて課金を実行するステップと、

を含む。

【００２０】

信頼できる課金機関は、課金処理を実行することのできる、信頼できるどのような第三者であってもよい。

【００２１】

これは、売り手が拒否できない証拠を信頼できる第三者に対して発行するのを可能にする。

【００２２】

一実施形態によれば、確認メッセージは、

前記買い手が前記ディジタルリソースを購入したいという確認ステートメントと、

前記暗号化されたディジタルリソース、ハッシュ、またはディジタルリソースの署名されたハッシュと、

前記確認メッセージが送信された現在の時刻と、

の中の１つまたは複数を含み、

前記署名を生成するのに使用された前記買い手の前記秘密鍵が、前記確認が送信された

ときに有効であった秘密鍵である。

【００２３】

確認は、ディジタルリソースを購入しようとする買い手の意思を指示（証明）して行ってもよい。暗号化されたディジタルリソースの署名、ハッシュ、または、署名されたハッシュは、買い手が実際にディジタルリソースを受信した証拠として使用されうる。現在の時刻の使用と、確認メッセージが送信されたとき（すなわち、確認メッセージに含まれる時刻）に有効であった秘密鍵の使用とは、時刻に依存した鍵（time independent key）を使用することを可能にし、セキュリティーを向上させる。

【００２４】

一実施形態によれば、前記方法は、

前記買い手のノードを前記売り手のノードに対して認証するステップを含み、前記認証するステップは、

前記買い手のノードが秘密鍵ｓを選択し、そして、前記買い手のノードの証明データ内に含まれる固有のハッシュコード値を介して前記買い手のノードのアイデンティティ（identity）に結合されるワンウェイ・ハッシュ・チェーンを生成するのに、前記秘密鍵ｓを使用することと、

前記買い手のノードが、前記買い手のノードの前記ワンウェイ・ハッシュ・チェーンを用いて、整数であるｍ個の公開鍵／秘密鍵対を導出し、前記公開鍵／秘密鍵対が、互いに結合され、かつ、前記買い手のノードの証明データ内に含まれるハッシュコード値に結合されることと、

前記買い手のノードが、前記導出した公開鍵の中の１つをそれの証明データとともに前記第２のノードに送信することと、

前記売り手のノードが、開示された公開鍵が前記第１のノードの証明データ内に含まれるハッシュコードに結合されていることを確認することによって、前記買い手のノードを認証することと、

前記買い手のノードが前記売り手のノードに対して認証されたのと同じようにして、前記売り手のノードを前記買い手のノードに対して認証することと

を含む。

【００２５】

これは、認証するときに信頼できる第三者への接続を利用できない場合でさえも、アドホックネットワークにおいて認証が実行されるのを可能にする認証スキームを提供する。したがって、このスキームは、本発明の実施形態に基づいてディジタルリソースを販売するための販売メカニズムに関連して使用されてもよい。

【００２６】

一実施形態によれば、時間区間T_i、$0 \leqq i < m$、において、前記第１のノードが、

【数１】

$$K_{m-1-i} = \prod_{j=0}^{m-i-1} f^j(s)$$

を秘密鍵として使用し、かつ、

【数２】

$$g^{K_{m-1-i}}$$

を対応する公開鍵として使用し、Ｇ＝（Ｇ，＊）が位数（order）ｑの有限巡回群（finite cyclic group）であり、ｇ∈ＧがＧの生成元（generator）であるように、公開鍵が選択され、ｇに対してＧにおける離散的対数（discrete logarithm）を計算することが、計算処理的に不可能であると仮定され、そしてｆは、集合｛０，１，．．．，ｑ－１｝をそ

れ自体の上に写像する暗号（ワンウェイ）ハッシュ関数である。

【００２７】

これは、時刻に依存し、かつ、お互いに結合された公開鍵／秘密鍵のペアを生成するのを可能にし、それによって、時刻に依存した鍵が認証に使用されてもよく、また拒否できない証拠の生成に使用されてもよい。

【００２８】

一実施形態によれば、本方法は、信頼できる第三者により前記買い手のノードと前記売り手のノードとを初期化するステップをさらに備え、前記初期化するステップが、

Ｇ、ｆ、ｍ、信頼できる第三者の公開鍵K_{TTP}、ワンウェイハッシュ関数であるｈを、前記買い手のノードに配信することと、

前記買い手のノードおよび前記売り手のノードのクロックを、前記信頼できる第三者のクロックに同期させることと、

ノードのアイデンティティを証明したいノードに対して、

【数３】

$$v = h(g^{\prod_{j=0}^{m} f^{j}(s)})$$

に基づいて検査値を計算し、かつ、

【数４】

$$[ID, v, t_0, L]_{K_{TTP}^{-1}}$$

に基づいて証明データを計算し、ここで、ＩＤは前記ノードの識別子であり、t_0は証明データの発行時刻であり、Ｌは公開鍵／秘密鍵対が有効である時間区間長を定義し、そして、

【数５】

$$[...]_{K_{TTP}^{-1}}$$

は、ＴＴＰによって、証明データの体上におけるＴＴＰの秘密鍵

【数６】

$$K_{TTP}^{-1}$$

で生成された署名であることと

を備える。

【００２９】

これは、時刻に依存した認証スキームを提供し、検査値は、時刻に依存した鍵と、時刻に依存した鍵をお互いに結合するハッシュ・チェーンとを用いて、検査されうる。

【００３０】

一実施形態によれば、前記買い手のノードを認証するステップは、

前記売り手のノードが公開鍵

【数７】

$$K_{m-1-i} = \prod_{j=0}^{m-i-1} f^{j}(s)$$

の確認されたコピーを入手するのを可能にするために、前記第１のノードが、時間区間T_i、０≦ｉ＜ｍ、において、
【数８】

$$g^{K_{m-1-i}}$$

を秘密鍵として使用し、かつ、
【数９】

$$g^{K_w}$$

を対応する公開鍵として使用することと、
前記第１のノードから前記第２のノードに、
【数１０】

$$g^{K_w}$$

と、f^{w+1}（ｓ）とを送信することと
を備えており、
証明データがｖを含み、そして前記売り手のノードが、f^j（ｓ）、ｗ＋１≦ｊ≦ｍを計算し、そしてこれらの値を用いて、前記売り手のノードが、
【数１１】

$$\begin{aligned} v^* &= (g^{K_w})^{\prod_{j=w+1}^{m} f^j(s)} \\ &= g^{\prod_{j=0}^{w} f^j(s) \prod_{j=w+1}^{m} f^j(s)} \\ &= g^{\prod_{j=0}^{m} f^j(s)}. \end{aligned}$$

を計算し、前記買い手のノードのアイデンティティを確認するために、ｖ＝ｈ（v^*）であることを検査する。
【００３１】
このようにして、検査値が時刻に依存した鍵に対して検査されることができ、それによって、その鍵が証明データ内に指示される当事者から送信されたという証拠を提供してもよい。
【００３２】
一実施形態によれば、クロックドリフト（clock drift）が、同期したクロック間の最大クロックドリフトを定義することによって考慮され、さらに、前記クロックドリフトが、起こりうるクロックドリフトを考慮すべき認証中に、１つよりも多い鍵が開示されてもよいかどうかを定義することによって考慮される。
【００３３】
このようにして、関係する当事者において起こりうるクロックのドリフト（drift）または不完全な同期を考慮に入れることができる。
【００３４】
一実施形態によれば、初期化ステップにおいて、ノードは、そのノードを別のノードに対して識別すべき信頼できる第三者またはプロバイダーから証明データを受信し、前記証

明データは、
ユーザ識別子と、
検査値と、
前記証明データの発行時刻と、
前記証明データを発行したプロバイダーまたは信頼できる第三者の識別子と、
前記証明データを発行した前記プロバイダーまたは前記信頼できる第三者のディジタル署名と、
ユーザがマルチメディアリソースを販売／購入するのを許されているかどうかの指示と、
からなる要素の中の１つまたは複数を備えるものである。

【００３５】
これは、初期化中に信頼できる第三者によって証明されたデータと、ノードがリソースを販売または購入するのを少なくとも許されているかどうかというような初期化中に定義された境界条件とに基づいて、システムが販売手順を実行するのを可能にする。

【００３６】
一実施形態によれば、初期化ステップにおいて、前記方法は、マルチメディアリソースを購入または販売することに参加できるように前記ユーザの装置を設定するために、プロバイダーまたは信頼できる第三者から前記ユーザに設定データを送信することを備え、前記設定データは、
プロバイダーまたは信頼できる第三者の公開鍵と、
別の信頼できるプロバイダーの公開鍵と、
どの課金情報が収集されなければならないかの指示と、
ネットワーク事業者のＡＡＡサーバーのアドレスと、
ユーザがマルチメディアリソースを販売／購入するのを許されているかどうかの指示と、
リソースを購入する限度額と、
からなる要素の中の１つまたは複数を備えるものである。

【００３７】
このようにして、販売／購入手順に参加するノードが設定されてもよい。

【００３８】
一実施形態によれば、前記売り手が前記ディジタルリソースを販売したことを証明するために、信頼できる課金機関に対してある買い手が使用する証拠が、
前記売り手の証明データと、
前記暗号化されたリソースが送信されたときに有効であった前記売り手の公開鍵、および前記売り手の公開鍵の正当性を確認するのを可能にする前記売り手のワンウェイ・ハッシュ・チェーンの対応する元と、
現在時刻と前記暗号化されたリソースとを含むものであるＭＥＳ送信リソース・メッセージと、
前記リソースが送信されたときに有効であった前記売り手の秘密鍵によって署名された前記ＭＥＳ送信リソース・メッセージのハッシュを含むものであるＭＥＳ送信ハッシュ・メッセージと
からなる要素の中の１つまたは複数を備えるものである。

【００３９】
このようにして、拒否できない証明または証拠が、買い手によって、ネットワーク事業者またはそれに類似するエンティティーのような信頼できる第三者または課金機関に対して提供されてもよい。信頼できる課金機関は、例えば、ネットワーク事業者または何らかの信頼できる第三者であってもよい。

【００４０】
一実施形態によれば、ある売り手が前記ディジタルリソースを販売したことを証明するために、信頼できる課金機関に対して前記売り手が使用する証拠が、

前記買い手の証明データと、
前記暗号化されたリソースが送信されたときに有効であった前記買い手の公開鍵と、前記買い手の公開鍵の正当性を確認するのを可能にする前記買い手のワンウェイ・ハッシュ・チェーンの対応する元と、
現在時刻と、前記買い手が前記ディジタルリソースを購入したいことを確認する確認ステートメントと、前記暗号化されたリソースのハッシュと、前記現在時刻における前記買い手のディジタル署名とを含むものであるＭＥＳ購入要求メッセージと、
前記売り手が前記買い手に送信した前記ＭＥＳ送信ハッシュ・メッセージのコピー、および／または前記売り手によって前記買い手に送信された暗号化されたディジタルリソースのハッシュと
からなる要素の中の１つまたは複数を備え、前記確認ステートメントおよび前記暗号化されたリソースの前記ハッシュは、前記ＭＥＳ購入要求メッセージが送信されたときに有効であった買い手の秘密鍵によって生成された前記ＭＥＳ購入要求メッセージを構成している。

【００４１】
このようにして、拒否できない証明または証拠が、売り手によって、ネットワーク事業者またはそれに類似するエンティティーのような信頼できる第三者または課金機関に対して提供されてもよい。

【００４２】
一実施形態によれば、前記証拠は、暗号化されたディジタルリソースに対するライセンスをさらに備えるものである。

【００４３】
これは、買い手がライセンスを正しく受信していないことをその買い手が主張し、しかしその買い手は、彼がライセンスを購入したという証拠を提供することができる場合に、その後に、課金機関または信頼できる第三者によって、再度ライセンスを交付するのに使用されてもよい。

【００４４】
一実施形態によれば、アドホックネットワークにおいてあるディジタルリソースｒをある売り手のノードＳからある買い手のノードＢへ販売するための装置が提供され、当該装置は、
第１および第２のノードの公開鍵が正当なオーナーによって使用されていることを確認するために、固定ネットワークまたは信頼できる第三者へ接続することなく、前記第１のノードと第２のノードとを互いに認証するモジュールと、
前記売り手によって販売される前記ディジタルリソースに前記買い手がアクセスするのを可能にするために、前記売り手のノードがライセンスを生成するモジュールであって、前記ライセンスが鍵を含むものである、モジュールと、
前記ライセンス内に含まれる前記鍵によって、前記ディジタルリソースを暗号化するモジュールと、
前記暗号化されたディジタルリソースを含むメッセージを送信し、かつ、前記メッセージの署名または署名されたハッシュを送信するためのモジュールであって、前記署名が売り手の秘密鍵を用いて生成されるものである、モジュールと、
前記買い手が前記ディジタルリソースを使用するのを可能にするために、前記ライセンスを前記売り手から前記買い手へ転送するモジュールと
を備えるものである。

【００４５】
一実施形態によれば、本発明の実施形態のいずれかに基づいた方法を実行するための１つまたは複数のモジュールを備える装置が、提供される。

【００４６】
一実施形態によれば、アドホックネットワークにおいて認証を実行するためのコンピュータプログラムが提供され、前記コンピュータプログラムは、コンピュータ上で実行され

る際に、本発明の実施形態のいずれかに基づいた方法を前記コンピュータが実行するのを可能にするコンピュータプログラムコードを備えている。

【発明を実施するための最良の形態】

【００４７】

以下、アドホックネットワークにおいてマルチメディアリソースが販売されるときにＡＡＡを提供する実施形態を説明する。提案される解決法は、アドホックネットワークのために少しだけ拡張された既存のＡＡＡアーキテクチャーに基づくものである。より詳細には、何らかのＴＴＰまたは固定ネットワーク（fixed network）にアクセスしなくても、ノードがそれらが通信する当事者を認証することを可能にする、エンティティー認証ソリューションが提供される。これは、請求およびチャージングのためにその後にネットワーク事業者によって実施形態に基づいて使用されうる拒否ができない課金証拠（non-repudiable accounting evidence）を、ノードが生成するのを可能にする。しかしながら、チャージングが実施形態に基づいて固定ネットワークにおいてなされたとしても、買い手（buyer）は従来通り、彼らがマルチメディアリソースをアドホックネットワークにおいて購入するとすぐに、それらのマルチメディアリソースを再生することができる。このことは、売り手(seller)がライセンスを買い手に発行することができるため可能となる。

【００４８】

本発明の実施形態を説明する前に、以下で使用されるいくつかの用語を簡単に説明する。

ＡＡＡ：認証（Authentication）、許可（Authorization）、および、課金（Accounting）

ＴＴＰ：信頼できる第三者

ＤＲＭ：ディジタル著作権管理（Digital Right Management）

ＭＥＳ：マルチメディアリソース交換システム

ＭＮＯｓ：モバイルネットワーク事業者

Ａ４Ｃ：認証、許可、課金、監査（Auditing）、および、チャージング（Charging）

ＳＥ：サービス機器

ＡＶＰｓ：属性値のペア(Attributes Value Pairs)

ＣＲＬ：証明データ失効リスト（Certificate Revocation List）

ＯＣＳＰ：オンライン証明データ状態プロトコル（Online Certificate Status Protocol）

【００４９】

一実施形態による基本的シナリオは、ユーザが、歌曲のようなマルチメディアリソースをアドホックネットワークにおいて販売するのを可能にされるべきことである。３つのエンティティー、すなわち、ユーザ、（モバイル）ネットワーク事業者、およびコンテンツプロバイダーが、シナリオに関与する。ユーザの（モバイル）ネットワーク事業者は、チャージングおよび請求（billing）に対して責任のあるエンティティーである。ユーザは、何らかのコンテンツを別のユーザに販売する。コンテンツプロバイダーは、コンテンツをユーザに最初に販売しており、コンテンツに対する権利を所有している。ユーザが、例えばｍｐ３ファイルを販売する場合、３つのエンティティーのすべてが関与する。ユーザはファイルを配信し、実施形態に基づいて、その配信に対する手数料を得ることになる。そして、ユーザの次回の請求書はその手数料を含んでおり、そのために、彼が（モバイル）ネットワーク事業者に支払わなければならない金額は減少することになる。（モバイル）ネットワーク事業者は、ユーザから受信した課金データによって、チャージングおよび請求に対する責任を有し、そしてこのサービスの料金をコンテンツプロバイダーにチャージングする。コンテンツプロバイダーは、ユーザの手数料分と事業者のサービスに対するチャージング分とだけ減らした、販売されたコンテンツに対する金銭を、コンテンツ購入者の請求書にその金額をチャージングした（モバイル）ネットワーク事業者から得ることになる。また、役割ユーザ（売り手および買い手）と、コンテンツプロバイダー（ここでは同様に、チャージングおよび請求を行う）とだけを有することも可能である。

【００５０】
図１および図２に示されるアドホックネットワークのいずれかにおいて使用されてもよい、上述したシナリオに適用できるソリューションを説明する。したがって、図１に示されるように、ユーザは、何らかのやり方で固定ネットワークに接続されていてもよく、あるいは、図２に示されるように、ユーザは、固定ネットワークとの接続性を有していなくてもよい。一般性を損なうことなく、何らかの固定ネットワークとの接続性を有していなくてもよいアドホックネットワーク内にユーザが存在すると仮定してもよい。その場合、それらのユーザはマルチメディアリソースを販売することができ、そしてユーザ自身が課金データを生成しなくてはならず、それらの課金データは、ユーザが再度（事業者のネットワークへの接続を提供する）固定ネットワークに接続されたときに、ユーザの（モバイル）ネットワーク事業者に転送される。課金データが生成され、そしてユーザのワンタイム公開鍵／秘密鍵のペアによって確認されるが、それぞれのユーザは、異なるトランザクションごとに異なる公開鍵／秘密鍵のペアを使用する。一実施形態によるシナリオは、ユーザがネットワーク事業者に登録するとき、それらのユーザは、固定ネットワーク内に存在する信頼できる第三者（ＴＴＰ）によって署名された証明データを発行されるという仮定に基づくものである。その後は、ユーザらはＴＴＰにアクセスしなくてもよい。さらにまた、一実施形態によれば、ユーザは、ユーザ自身の装置上にインストールされたマルチメディアリソース交換システム（ＭＥＳ）を用いて、ファイルを別のユーザに転送しようとすることが仮定され、このマルチメディアリソース交換システム（ＭＥＳ）は、ファイルが確実に転送され、かつ買い手は、買い手が完全なファイルを受信した場合にしかチャージングされないことを保証する。そのようなＭＥＳに関する詳細な説明が、後に本発明の実施形態に関連してなされる。しかしながら、そのようなＭＥＳのインストールは、随意的なものであり、かつ、本発明の実施形態を実施するのに少しだけ有益であることに留意されたい。

【００５１】
一実施形態によるＭＥＳは、正当な権利を有するユーザしかマルチメディアリソースを使用できないことを保証する、ディジタル著作権管理（ＤＲＭ）システムを使用する。ＤＲＭシステムは、リソースの価格がいくらであるかに関する情報を含むライセンスを使用し、それによって、ユーザはリソースを別のユーザに販売し、そのリソースに対する正しい価格を要求することができる。ライセンス内に存在するマルチメディアリソースへのアクセスキーは保護されるが、ライセンスの保護に関する詳細はＤＲＭシステムによって定義される。さらに、ライセンスは、ユーザがコピーを別のユーザに販売することが許容されているかどうかを指定している。これに加えて、ＤＲＭシステムは、既存のライセンスから新しいライセンスを生成することができ、かつ、マルチメディアリソースのための新しいラッパー（wrapper）を生成することができ、それによってユーザは、そのリソースを販売し、かつ正しいライセンスをそのリソースとともに送信することができる。さらにまた、マルチメディアリソースはコンテンツ所有者によってサイン（sign）されており、それによってユーザは、そのマルチメディアリソースが本当にそのユーザが入手したいリソースであることを確認することができる。

【００５２】
ＭＥＳは、リソースを転送するためのｐｌａｉｎＦＴＰまたはＨＴＴＰに基づくものにすることができる。ＭＥＳは、マルチメディアリソースおよびハッシュを受信し、そのハッシュによって、ＭＥＳは、リソースが正しく転送されたかどうかを自動的に検査する。さらにＭＥＳは、装置上のＡＡＡシステムのための課金データを収集し、そして収集された課金データをＡＡＡサーバーに転送する。ＡＡＡサーバーは、課金データを記憶し、それらを、例えばネットワーク事業者のネットワーク内の別のＡＡＡサーバーに転送する責任がある。ＡＡＡシステムは、ＡＡＡシステムおよびＭＥＳがどのように設定されなければならないかを記述した設定プロフィール（configuration profile）を記憶する。この設定プロフィールは、それがネットワーク事業者によってだけ変更され、かつ、それが装置上のＡＡＡシステムにだけ可読でなければならないような形で、ＡＡＡによって保護さ

れる。

【００５３】

一実施形態によれば、ＡＡＡおよびＭＥＳシステムは、システムによって記憶されたデータを、またはシステムがどのように動作するかを、ユーザが改ざんできないようなやり方で実施される。スマートカード上でＡＡＡシステムおよび／またはＭＥＳシステムのいくつかの部分を実施することは、それらのシステムの不正操作に対する抵抗性（tamper resistance）を増大させうる。

【００５４】

一実施形態によれば、ユーザは、もしそれらのユーザがマルチメディアリソースを販売／購入したいならば、チャージングおよび請求のために、ネットワーク事業者との加入契約を有していなければならない。したがって、以下の説明の場合、ユーザは、（モバイル）ネットワーク事業者との加入契約を有すると仮定される。さらにまた、一実施形態によれば、その契約は、ユーザがマルチメディアリソースを販売および／または購入することが許されるかどうかを規定している。

【００５５】

ここで、以下において、一実施形態に基づいてマルチメディアリソースを販売しかつそれに対して課金およびチャージングを行うプロセスの全体について説明する。プロセスは、以下でより詳細に説明される３つのステップに分割されてもよい。１回だけ実行されなければならない第１のステップにおいて、ユーザは、彼がディジタルリソースまたはマルチメディアリソースを販売／購入することが許され、かつ必要なすべての情報が提供されるかどうかが明記された契約を締結しなければならない。第２のステップは、マルチメディアリソースを実際に販売／購入することを記載する。最後のステップにおいて、マルチメディアリソースの販売に対する課金およびチャージングがどのようになされるかが記述される。

【００５６】

以下においては、一実施形態に基づいて（モバイル）ノードを登録するステップについて説明する。ユーザＵが、アドホックネットワークにおいて、何らかのマルチメディアリソースを購入または販売したい場合、そのユーザが固定ネットワーク内に存在する限り、ユーザＵがマルチメディアリソースを販売および／または購入することが許されようが許されまいが、そのユーザは最初に、そのユーザのネットワーク事業者と契約を締結しなければならない。また、マルチメディアリソースの購入限度額が規定される。この情報は、ネットワーク事業者のＡＡＡシステムのための設定プロフィール内に記憶され、またユーザＵの（モバイル）装置にも転送され、そこに記憶される。契約はまた、関与するそれぞれの当事者（ユーザ、事業者、コンテンツ所有者）の分け前をパーセンテージで規定する。

【００５７】

マルチメディアリソースの買い手および売り手は、彼らがネットワーク事業者に登録されたエンティティーとやりとりしようとしていることを識別することができなければならない。さらに、ネットワーク事業者が、リソースの売り手に報酬を支払うのを可能にするために、また買い手にチャージングするのを可能にするために、買い手および売り手は、アドホックネットワークにおいて彼らが生成した証拠が事業者のデータベースに記憶されたユーザの識別情報に固有に関連づけられるようなやり方で、ネットワーク事業者によって固有に特定されることが重要である。チャージングおよび請求が正しく実行されることを保証するために、この識別情報は、Ｕが登録したとき、ネットワーク事業者によって確認されなければならない。Ｕのアイデンティティ（identity）が確認されると、ネットワーク事業者は、顧客番号を固有識別子$ＩＤ_u$として含む証明データ（certificate）をＵに発行することができる。さらに、発行された証明データは、また、Ｕがアドホックネットワークにおいてリソースを販売および／または購入することが許されているかどうかを指示する情報を含まなければならない。

【００５８】

図３は、Ｕが契約を締結した後に、および／またはマルチメディアリソースを購入するためのサービスに加入した後に、固定ネットワークにおいて、ノードを登録するプロセスを示している。

【００５９】

ユーザＵが事業者のネットワークに接続するとき、そのユーザＵは、そのユーザＵの事業者（または、何らかの信頼できる第三者）のＡＡＡシステムによって許可される。許可された後に、Ｕは、彼の装置上でＡＡＡシステムを設定するのに必要な設定データを、そのユーザＵの事業者（Ｏ）のＡＡＡサーバーに要求する。それに応答して事業者（Ｏ）は、安全なやり方でその装置に設定データを送信し、その設定データはＵの証明データも含む。一実施形態による設定データの内容の例が、表１に示されている。一実施形態によれば、プロバイダーはまた、Ｕの信頼性を保証するために、プロバイダーの公開鍵をＵに安全なやり方で送信する。これは例えば、Ｆ．Ｓｔａｊａｎｏ，「Ｔｈｅ Ｒｅｓｕｒｒｅｃｔｉｎｇ Ｄｕｃｋｌｉｎｇ － Ｗｈａｔ Ｎｅｘｔ？」ｉｎ Ｒｅｖｉｓｅｄ Ｐａｐｅｒｓ ｆｒｏｍ ｔｈｅ ８ｔｈ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｗｏｒｋｓｈｏｐ ｏｎ Ｓｅｃｕｒｉｔｙ Ｐｒｏｔｏｃｏｌｓに定義されるインプリンティング（imprinting）によって、あるいは、それらの設定データをモバイル装置のスマートカードに記憶することによってなされうる。プロバイダーはまた、そのプロバイダーが契約したその他のプロバイダーの公開鍵を安全なやり方でＵに送信する。これらの公開鍵は、アドホックネットワークにおいて、Ｕが、既存の信頼できるネットワーク事業者に登録されたユーザを確認するのを可能にする。

【表１】

表１：ユーザに発行される証明データおよびプロバイダーから登録されたユーザに送信される設定データを構成するデータ

構成	ユーザ証明書	環境設定データ
	・ユーザ識別子 ・ユーザ検査値 ・証明データの発行時刻 ・ユーザが加入しているプロバイダーの識別子 ・ユーザが加入しているプロバイダーのディジタル署名 ・ユーザはマルチメディア資源の販売/購入を許されているか	・ユーザが加入しているプロバイダーの公開鍵 ・その他の信頼できるプロバイダーの公開鍵 ・どの課金情報を収集する必要があるか ・ネットワーク事業者の AAA サーバーのアドレス ・ユーザはマルチメディア資源の販売/購入を許されているか ・資源を購入する限度額

【００６０】

以下においては、一実施形態に基づいてマルチメディアリソースを販売するステップを説明する。ノードがアドホックネットワークに入ると、そのノードは、マルチメディアリソースを交換するようにあらかじめ設定された装置を探索する。したがって、一実施形態によれば、対応する装置は、仮定において説明されたようにインストールされた互換性のあるＭＥＳ、およびＡＡＡシステムを有していなければならない。

【００６１】

上述した要件が満たされると、マルチメディアリソースの交換を開始することができる。一実施形態においては、マルチメディアリソースの売り手（Ｓ）は、プロセスに積極的には関与しない。なぜなら売り手のＭＥＳは、売り手が販売するのを許された別のユーザにマルチメディアリソースを自動的に提供するからである。買い手（Ｂ）は、どのマルチメディアリソースを購入したいかを選択しなければならず、そしてファイルが転送された後に、買い手が本当にそれを購入したいことを確認する。

【００６２】

図４は、そのような環境において一実施形態に基づいてマルチメディアリソースを販売するためのプロセスの例を示している。Ｂの装置は別のＭＥＳを探索しており（「ＭＥＳ利用要求（MES-Available-Request）」を送信することによって）、Ｂの装置が応答を受信すれば、ＭＥＳバージョンは互換性があるかどうかを検査する。これに加えて、入手可能なリソースのリストが、互換性のあるそれぞれのＭＥＳからさらに送信され、そのリストはまた、マルチメディアリソースの価格情報を含んでいる。そしてＢは、互換性のあるＡＡＡシステムがその別の装置上にインストールされているかどうかを検査する。要件が満たされ、かつマルチメディアリソースのリストを入手できれば、Ｂは、ＢのＭＥＳ上において、Ｂが購入したいマルチメディアリソースを探索してもよい。Ｂがリソースを探し出した後、Ｂは、入手することを希望し、かつＢが購入プロセスを開始したＳから購入することを希望しうる。最初に、Ｂは後により詳細に説明される認証システムを用いて、ＳとともにＢ自身を認証する。そして、ＢのＭＥＳが装置上のＡＡＡシステムによって設定される（例えば、「ＭＥＳ設定要求（Configure-MES-request）」によって）。Ｓの装置上において、同じプロセスが逆に発生しており、それによって、後に説明される相互認証プロセスにおいて説明されるように、Ｓもまた認証される。

【００６３】

設定の後、Ｂは、ＢのＭＥＳ上において、ダウンロードするマルチメディアリソースを選択し、そのマルチメディアリソースが、購入限度額にまだ達していないかどうかをＡＡＡシステムによって検査された後（例えば、「購入限度額検査要求（Check-Purchase-Limit request）」によって）、ＢのＭＥＳは、ＭＥＳリソースダウンロード要求（MES-Download-Resource-Request）をＳに送信する。Ｂは、ＤＲＭシステムによって保護されたマルチメディアリソース（「ＭＥＳ送信リソース（MES-Send-Resource）」）およびマルチメディアリソースのハッシュ（「ＭＥＳ送信ハッシュ（MES-Send-Hash）」）を受信し、それによって、マルチメディア交換システムは、リソースが完全にダウンロードされたかどうかを検査することができる。さらにまた、リソースはディジタル署名され、それによってＢは、そのリソースがＳからのものであることを確信することができる。リソースが完全にダウンロードされた後、Ｂは、Ｂが本当にそのリソースを購入したいかどうかを質問される（「ＭＥＳ購入確認ユーザ質問（MES-Ask-User-for-Buy-Confirmation）」）。Ｂが同意すれば、メッセージ（「ＭＥＳ購入要求（MES-Buy-Request）」）が送り返され、リソースが受信されたことおよびＢがそのリソースを購入したいことが確認される。一実施形態によるこのメッセージは、何らかのリソースが販売されたというＳの事業者に対するＳのための証拠として使用され、この証拠は、買い手のアイデンティティのデータおよび送信されたリソースのハッシュとともに、ＡＡＡシステム内に記憶される（「課金データ記憶（Store-Accounting-Data）」）。購入確認を受信した後、Ｓは、リソースに対するライセンスをＢに送信する（「ＭＥＳライセンス送信（MES-Send-License）」）。ライセンスは、Ｓの装置のＡＡＡシステム内に記憶される（「課金データ記憶」）。

【００６４】

データがこのようにして販売された後、課金データは、適切な課金処理を実施できるように事業者に転送されなければならない。以下、これについて説明する。

【００６５】

売り手Ｓが彼の事業者のネットワークに接続されると、収集されたすべての課金データは、彼のネットワーク事業者に転送されることが可能である。図５は、課金データを事業者に転送するためのプロセスを示している。事業者のネットワークへの接続が確立された後、Ｓは、Ｓ自身を認証しなければならず（「認証要求／応答（Authentication-Request/Answer）」）、そして事業者は、Ｓに対して事業者自身を認証する。次のステップにおいて、ＳのＡＡＡシステムは、Ｓの事業者のネットワーク内に存在するＡＡＡサーバーに課金データを送信する（「課金データ送信」）。データの受信は、「課金データ受信（Accounting-Data-Received）」によって、ＡＡＡサーバーによって確認される。一実施形態による課金データは、何が誰に販売されたか、およびその証拠（これは、一実施形態によれば、「ＭＥＳ購入要求」メッセージと、Ｂに送信されたマルチメディアリソースに対す

るライセンスとを備えている）を含む。ネットワーク事業者は、その証拠が正しいかどうか検査する。ネットワーク事業者は、買い手がその事業者のデータベース内に登録されていることを確認し、あるいは、買い手が契約している事業者に照会する。これらの検査が正しければ、Ｓのネットワーク事業者は、彼がライセンスのコピーを受信したかどうかを検査する。好ましくは、彼はまた、確認メッセージの正当性および対応する署名の正当性を検査する（これは、一実施形態によれば、後により詳細に説明する認証スキームに基づくものである）。課金データが正しければ、Ｓは、Ｓの請求額分を減らした手数料を得る。ネットワーク事業者は、Ｂが事業者との加入契約を有していれば、マルチメディアリソースについてＢにチャージングすることになり、そして、ネットワーク事業者のサービス料分だけ減らした金銭を、コンテンツ所有者に渡す。ＢがＳの事業者に加入していなければ、Ｓのネットワーク事業者は、課金データをＢのネットワーク事業者に送信する。そして、Ｂのネットワーク事業者は、リソースに対する金銭をコンテンツ所有者にチャージングし、かつ、渡すことになる。

【００６６】

以下において、提案されたプロセスへの考えられるいくつかの脅威について説明する。買い手は、彼がマルチメディアコンテンツを使用するライセンスを受け取っていないこと、したがって、コンテンツに対する料金を支払いたくないことを、悪意的に主張する可能性がある。ネットワーク事業者は、コンテンツを販売した証拠の一部としてライセンスのコピーを入手するので、ネットワーク事業者は、この主張が真実かどうかを判定することができる。もしネットワーク事業者がライセンスのコピーを有していれば、主張は真実ではなく、買い手はライセンスのコピーを入手し、それによって、彼はコンテンツを使用することができ、そして購入に対する料金がチャージングされる。もしネットワーク事業者がライセンスのコピーを有していなければ、買い手は支払わなくてもよく、そして買い手は、買い手の装置に転送されたマルチメディアリソースを使用することはできない。また、ライセンスが売り手によって送信されたのに、例えばネットワーク問題のために買い手によって受信されなかった場合も、このように取り扱われる。

【００６７】

売り手は、その売り手がすべての証拠（ライセンスを含めて）を事業者に転送した場合にしか金銭を得られないので、売り手がライセンスを買い手に送信しない動機は存在しない。ネットワーク事業者がライセンスのコピーを有するという事実は、また、買い手が本当にマルチメディアリソースを使用できる場合にしか買い手にチャージングされないことを保証する。必要であれば、買い手はライセンスを最後に事業者から入手してもよい（例えば、売り手から買い手への送信が、何らかの理由で、例えばネットワーク問題のために失敗した場合）。

【００６８】

以下において、中央インフラストラクチャーを備えてないアドホックネットワークにおける認証のための、本発明の一実施形態によるソリューションについて説明する。そして、この認証スキームは、これまでに説明されたマルチメディアリソースの販売／購入プロセスに関連して使用されうる。

【００６９】

一実施形態によれば、そのソリューションは、認証を与えるための１回（ｏｎｅ－ｔｉｍｅ）限り有効な公開鍵を利用する。

【００７０】

提案されるスキームを詳細に説明する前に、そのスキームに対する認証との関連性について、もう一度簡単に考察する。認証および課金が提供されなければならない場合、認証は、サービスの消費に対する料金をチャージングされなければならない主債務者（principal）を識別するのを可能にする。これは、認証が、チャージングされるべき相手方（主債務者）のアイデンティティを確認するのを可能にすることを意味する。固定ネットワークにおいては、主債務者を認証するのを可能にするソリューションが存在する。しかしながら、それらのソリューションは主として、中央エンティティーに頼るものである。アド

ホックネットワークにおいては、インフラストラクチャーが欠如していると、ノードが最新の証明データ失効リスト（ＣＲＬ：certificate revocation list）を入手することができ、オンライン証明データ状態プロトコル（ＯＣＳＰ：online certificate status protocol）レスポンダーにアクセスすることができ、かつ、エンティティー認証のために公開鍵証明データ（public key certificate）の正当性を評価しあるいは秘密鍵を配信するのを可能にするＴＴＰにアクセスすることができるという保証が、ノードに与えられない。これらの理由から、従来の証明データに基づいたあるいは秘密鍵に基づいたエンティティー認証ソリューションは、それらの現在のやり方では、マルチメディアリソースを購入したい主債務者をアドホックネットワーク内のノードが認証するのを可能にするのに使用することはできない。このことは、何らかの中央エンティティーに頼ることのないエンティティー認証ソリューションの必要性を高めることになる。

【００７１】

本ソリューションにおいて、一実施形態によれば、あらかじめ秘密鍵を共有しておらずかつ初めて出会った任意の売り手のノードＳと買い手のノードＢとは、公開鍵証明データを使用するのではなくワンウェイ・ハッシュ・チェーン（one-way hash chain）を使用して、お互いに認証し、そしてワンタイム公開鍵を生成することができる。Ｓによって認証されるために、Ｂは秘密鍵ｓを選択し、そしてワンウェイ・ハッシュ・チェーンを生成するのにその鍵ｓを使用する。このチェーンは、証明データに含まれる固有のハッシュコード値を介して、Ｂのアイデンティティに結合される。証明データの有効期間は、ユーザであるＢが、アドホックネットワークにおいて、リソースを販売し、リソースを購入または販売し、またリソースを購入するのを、ユーザＢのネットワークプロバイダーから許される時間である。Ｂは、多数の公開鍵／秘密鍵のペアを導出するのにそれのチェーンを使用する。これらの公開鍵／秘密鍵のペアは、お互いに結合され、かつ、Ｂの証明データに含まれるハッシュコード値に結合される。そして、Ｓによって認証されるためには、Ｂは、それの公開鍵の中の１つをそれの証明データとともにＳに送信するだけでよい。Ｓは、開示された公開鍵がＢの証明データに含まれるハッシュコードに結合されていることを確認することによって、Ｂを認証してもよい。Ｓが、これまでに説明されたように生成された公開鍵をＢに送信すれば、お互いの認証が提供される。これらの公開鍵は、交換が実施される現在の時間区間中にのみ有効であり、また、交換された証明データの本物の所有者しか生成することができない。

【００７２】

以下において、一実施形態に基づいて本スキームに参加するノードの初期化について説明する。

【００７３】

初期化は、エンティティーＢおよびＳが固定ネットワークに接続されている間に一回だけ実施されるが、必ずしも同時に実施されるとは限らない。例えばそれは、個人がネットワーク事業者に登録するときに実施されることが可能である。登録するとき、ユーザは加入する必要があるサービスを選択する。これは例えば、リソースを購入するのを可能にするサービス、リソースを販売するのを可能にするサービス、または、リソースを購入および販売するのを可能にするサービスでありうる。ＢおよびＳは、それのクロックを同期させるために、また以下のパラメータを得るために、ＴＴＰに連絡する。

・Ｇ＝（Ｇ，*）は、位数（order）ｑ（何らかの大きなｑ）の有限巡回群（finite cyclic group）であり、ｇ∈Ｇは、Ｇの生成元（generator）であり、そして、ｇに対してＧにおける離散的対数（discrete logarithm）を計算することは、計算処理的に不可能であると仮定する。例えばＧは、何らかの大きな素数ｐに対するＺ’$_{p}$の大きな乗法的部分群（multiplicative subgroup）であってもよく、ここでｑは、ｐ－１を除算する大きな素数であり、あるいはＧは、楕円曲線上の点の群であってもよい（通常、加法的に記述される）。

・ｈは、任意の長さの２進列を固定長ｌの列に写像する暗号（ワンウェイ）ハッシュ関数である（例えば、ｌの典型的な値は、２２４である）。

・ｆは、集合｛０，１，．．．，ｑ－１｝をそれ自体の上に写像する暗号（ワンウェイ）ハッシュ関数である。実際には、ｆは、例えばｈから導出されてもよい。
・ｍ≧１は、ノードが利用できる鍵対の数を決定する正の整数である。
・K_{TTP}：ＴＴＰの公開鍵。
【００７４】
ＴＴＰは、パラメータを要求したすべてのエンティティーに同じパラメータを送信する。Ｂがこれらのパラメータを受信すると、Ｂは、Ｂが安全に維持する秘密鍵ｓを選択する。これは、例えば、その秘密鍵が使用されなければならないほんの短い期間だけ秘密鍵へのアクセスを可能にする、パスフレーズに基づくものであってもよい。これはまた、個人の要求されるアイデンティティを識別または確認するのに使用することのできる生体特徴、すなわち何らかの測定可能なロバストな独特の物理的特徴、または個人的特徴に基づくものであってもよく（例えば、Ｅ．Ｍ．Ｎｅｗｔｏｎ ａｎｄ Ｊ．Ｄ．Ｗｏｏｄｗａｒｄ，「Ｂｉｏｍｅｔｒｉｃｓ：Ａ ｔｅｃｈｎｉｃａｌ ｐｒｉｍｅｒ」ＲＡＮＤ，２００１を参照）、それらの特徴は、その秘密鍵を生成しかつほんの短い期間だけその鍵を有効にするために、捕捉されなければならない。そしてＢは、検査値：
【数１２】

$$v = h(g^{\prod_{j=0}^{m} f^{j}(s)})$$

を生成する。
【００７５】
これがなされると、Ｂは、これらの２つの値に結合する証明データを入手するために、Ｂのアイデンティティ$ＩＤ_{B}$およびｖをＴＴＰに送信する。ＴＴＰが$ＩＤ_{B}$およびｖを受信した後、ＴＴＰは、Ｂが本当に$ＩＤ_{B}$を所有すること、およびｖを含む証明データがまだ発行されていないことを確認する。すべての確認が正しければ、ＴＴＰは、証明データ$Ｃｅｒｔ_{B}$：
【数１３】

$$[ID_B, v, t_0, L]_{K_{TTP}^{-1}}$$

をＢに送信する。ここで$ｔ_{0}$は、証明データの発行時刻であり、Ｌは、整数であり、
【数１４】

$$[...]_{K_{TTP}^{-1}}$$

は、ＴＴＰによって、$Ｃｅｒｔ_{B}$の体（field）上におけるＴＴＰの秘密鍵
【数１５】

$$K_{TTP}^{-1}$$

で生成された署名である。Ｂが、それの証明データを受信した後、Ｂはもはやｔｔｐにアクセスしなくてもよい。Ｂは、時間を等しい長さＬを有する区間に分割する。それぞれの区間は、ｆをｓに反復的に適用することによって得られるＢのワンウェイ・ハッシュ・チェーンからの元（element）によって生成された鍵に割り当てられる（図６を参照）。証明データの時刻を発行する代わりに、公開鍵／秘密鍵のペアが有効な時間区間を規定する

ための開始時刻または基準開始点として使用されてもよい何らかの時刻が、ｔ$_0$として使用されてもよい。

【００７６】

ここで、初期化の後に実施されてもよい実際の認証について説明する。

【００７７】

０≦ｉ＜ｍである時間区間Ｔ$_i$において、Ｂは、

【数１６】

$$K_{m-1-i} = \prod_{j=0}^{m-i-1} f^j(s)$$

を秘密鍵として使用し、かつ、

【数１７】

$$g^{K_{m-1-i}}$$

を対応する公開鍵として使用する。Ｓが、公開鍵、

【数１８】

$$g^{K_w}$$

の確認されたコピーを入手するのを可能にするために、Ｂは、

【数１９】

$$g^{K_w}$$

・ｆ$^{w+1}$（ｓ）

・ｖを含む証明データ

をＳに送信する。ここでｗは、ｍ－１－ｉによって、したがって実際には、それが生成された時間区間によって定義される。

【００７８】

そのメッセージを受信すると、Ｓはそれを記憶する。Ｓは（時間依存のため）ｗを知っていると仮定され、そしてｆ^j（ｓ）を計算することができ、ここで、ｗ＋１≦ｊ≦ｍである。そしてこれらの値を使用して、Ｓは、

【数２０】

$$\begin{aligned} v^* &= (g^{K_w})^{\prod_{j=w+1}^{m} f^j(s)} \\ &= g^{\prod_{j=0}^{w} f^j(s) \prod_{j=w+1}^{m} f^j(s)} \\ &= g^{\prod_{j=0}^{m} f^j(s)}. \end{aligned}$$

を計算する。最後にＳは、ｖ＝ｈ（ｖ*）であるかどうかを検査する。等しいことが確認されると、Ｓは、

【数２１】

$$g^{K_w}$$

が、受信された証明データ内にアイデンティティが含まれるＢによって生成されたことを知る。Ｓが、以前にＢによって使用された方法と同じ方法を使用するならば、Ｓは鍵
【数２２】

$$g^{K_y}$$

を開示することによって、それのアイデンティティをＢに証明することができる。
【００７９】
以下において、一実施形態に基づいてどのようにクロックドリフト（clock drift（同期のずれ））が取り扱われるかを説明する。
【００８０】
説明されるソリューションにおいては、Ｂ、Ｓ、およびＴＴＰは、クロックを同期させたはずである。多くのソリューションが、ネットワーク時間プロトコル（例えば、Ｄ．Ｍｉｌｌｓ．Ｎｅｔｗｏｒｋ Ｔｉｍｅ Ｐｒｏｔｏｃｏｌ（Ｖｅｒｓｉｏｎ ３）Ｓｐｅｃｉｆｉｃａｔｉｏｎ，Ｉｍｐｌｅｍｅｎｔａｔｉｏｎ ａｎｄ Ａｎａｌｙｓｉｓ．ＲＦＣ １３０５，Ｍａｒｃｈ １９９２を参照）の使用を含めて、そのような同期を達成するのに使用されることが可能であり、ＢとＳとをＴＴＰのクロックなどに同期させる。これは初期化段階においてなされてもよく、それと同時に、ＢおよびＳが固定ネットワークに接続される。しかしながらその後は、それらのＢおよびＳは、ＴＴＰおよび固定ネットワークとは無関係に動作してもよい。同期は、認証プロセス中に発行された鍵の鮮度および正当性を確認するのを可能にするために実行される。しかしながらエンティティーは、完璧に同期したクロックを有する必要はない。例えば、図７に示されるように、２つの鍵が１つの時間期間中に有効であれば、数秒のクロックドリフトは問題とならない可能性がある。ｄが、ＴＴＰに同期した２つのエンティティー間で許容される最大クロックドリフトであれば、ｄは、この２つの鍵の有効期間の開始を同じ時間区間中において分離する時間期間であってもよい。これは、少なくとも１つの鍵がそれぞれの時間区間中に認証を実行するのを可能にすることを保証する。これを説明するために、図７を考察する。区間T_0において、K_{m-1}およびK'_{m-1}が有効であり、かつ、たとえＢのクロックとＳのクロックとの間にｄ以下のクロックドリフトが存在するとしても、鍵の少なくとも１つは、ｖ＝ｈ（ｖ*）という関係を確認するのを可能にする。１つよりも多い鍵が、時間区間中に開示されなければならないならば、ＴＴＰはそれを証明データに明記してもよい。ｄの値は初期化段階においてＴＴＰによって指定され、そしてエンティティーに送信されてもよい。
【００８１】
以下においては、提案されたソリューションによって提供されるセキュリティーを説明する。
【００８２】
説明されるソリューションにおいて、エンティティーは、更新された失効状態情報を得ることによって、証明データの正当性を確認しなくてもよい。実際に、値ｓが良好に保護されていれば、これは例えば、パスワードまたはパスフレーズに基づくものであり、かつ、何らかのｉに対するK_iを生成するのに必要な短い期間だけそのマシンにのみ記憶されていてもよいが、ｓを知るＢだけが、区間T_iにおいて有効な鍵K_{m-i-1}およびそれに対応する公開鍵

【数２３】

$$g^{K_{m-1-i}}$$

を生成することができる。K_{m-i-1}は、別の時間期間においては発行されていないクライアントのワンウェイ・ハッシュ・チェーンの元（element）によって生成されるので、また、ワンウェイ・ハッシュ・チェーンは、逆変換（reverse）するのが計算処理的に難しいので、アタッカーは、クライアントが過去に使用した鍵からK_{m-i-1}を見つけ出すことはできない。また、アタッカーが、

【数２４】

$$g^{K_{m-1-i}}$$

からK_{m-i-1}を見つけ出すのは計算処理的に難しい（例えば、Ｗ．Ｄｉｆｆｉｅ ａｎｄ Ｍ．Ｅ．Ｈｅｌｌｍａｎ，「Ｎｅｗ Ｄｉｒｅｃｔｉｏｎｓ ｉｎ Ｃｒｙｐｔｏｇｒａｐｈｙ」ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ，ｖｏｌ．ＩＴ－２２，ｎｏ．６，ｐｐ．６４４－６５４，１９７６を参照）。

【００８３】

最後に、例えばＳが、Ｂに対する過去の公開鍵の信頼できるコピーをキャッシュに格納する（cache）ならば、公開鍵確認プロセスにおけるある種の最適化が実施されうることに注目してもよい。

【００８４】

ここで、説明された認証スキームの課金処理との関連性を説明する。

【００８５】

本シナリオは、ユーザにとって興味のあることである。なぜなら、ユーザがアドホックネットワーク内に存在するときに、それらのユーザが新しいマルチメディアリソースにアクセスするのを可能にすることができるからである。したがって、アドホックネットワークにおいて何らかのファイルを購入したユーザが、彼らがまだアドホックネットワーク内に存在するときにそれらのファイルを使用するのを可能にすることは、重要なことである。これは、正当なプロバイダー、すなわち、実在し、信頼できるものであり、かつ、売り手のノードのネットワーク事業者と契約しているプロバイダーによって登録された買い手のノードに、売り手のノードがリソースを販売することになることを、それらの売り手のノードに対して保証するメカニズムを定義することを必要とする。これが保証されると、売り手のノードは、それが実際にリソースｒを正当なプロバイダーに登録されたノードに販売したという何らかの証拠を有することが必要となる。これらの証拠は、その後に、チャージングのためにネットワーク事業者に提供されてもよい。交換が実施される前に、売り手Ｓおよび買い手Ｂは、これまでに説明された認証プロセスを実行する。交換されたプローブ（prove）が正当なものであれば、両方のノードは、意図するエンティティーと対話していることを確信することになる。それらはまた、受信した公開鍵は有効であり、かつそれらの本物の所有者によって現時点で使用されていることを知る。これらの公開鍵は、マルチメディアリソースｒがＢに送信された、またはＢによって購入されたという拒否できないプローブ（non-repudiable prove）を確認するのに使用されうる。証拠を確認するために交換されるメッセージが、図８に示されている。

【００８６】

相互認証が実行された後、Ｓは、Ｂがマルチメディアリソースｒを閲覧するのを可能にするライセンスを生成し、そして、そのライセンス内に含まれる対応する鍵によってｒを暗号化する。そしてＳは、それの現在時刻と暗号化されたマルチメディアリソースｒとを含むメッセージ「ＭＥＳ送信リソース（MES-Send-Resource）」を生成する。これが実行されるとすぐに、Ｓは、「ＭＥＳ送信リソース」と、それの現在の有効な秘密鍵によって署名された「ＭＥＳ送信リソース」のハッシュを含む「ＭＥＳ送信ハッシュ（MES-Send-H

ash）」とをＢに送信する。「ＭＥＳ送信リソース」が、相互認証が実行されたときの時間区間と同じ時間区間中に送信されたならば、ハッシュは、認証のためにＳがＢに送信した公開鍵に対応する秘密鍵によって署名される。

【００８７】

もしそうでなければ、Ｓは、現在の時間区間中に有効な秘密鍵によってハッシュを署名しなければならず、また、対応する公開鍵を「ＭＥＳ送信リソース」および「ＭＥＳ送信ハッシュ」とともにＢに送信しなければならない。またＳは、公開鍵の正当性をＢが確認するのを可能にするために、それのワンウェイ・ハッシュ・チェーンの対応する元（element）を送信しなければならない。ノードが新しい公開鍵を送信しなければならないときにはいつでも、そのノードは、対応するヘルパーを送信しなければならない。これは、以下の説明においては暗黙的なものである。Ｂがメッセージを受信した後、Ｂは、Ｓの現時点で有効な公開鍵によって署名されたハッシュの正当性を検査することによって、暗号化されたマルチメディアリソースがＳから送信されたことを確認することができる。Ｓから受信された受信メッセージが新しい公開鍵を含むならば、Ｂは、署名を確認するのにそれを使用する前に、それの正当性を検査しなければならない。またＳは、それが新しい公開鍵をＢから受信したときにはいつでも、同じことを実行しなければならない。署名が正当であれば、Ｂは、「ＭＥＳ送信リソース」、「ＭＥＳ送信ハッシュ」、および、現時点で有効な公開鍵（もしそれが以前に受信したものと異なっていれば）を、Ｓのワンウェイ・ハッシュ・チェーンの対応する元とともに記憶する。記憶されたデータは、ＢがｒをＳから受信したことを証明するために、Ｂがネットワーク事業者に提供しうる拒否できない証明（non-repudiable proof）である。もしＢが、受信したマルチメディアリソースを購入したいならば、Ｂは、彼のクロックにおける現在時刻に基づいて、彼の現時点で有効な秘密鍵によるディジタル署名、彼がｒを購入したいという確認ステートメント、および、暗号化されたマルチメディアリソースのハッシュを生成する。これらの値は、署名とともに、ＢがＳに送信するメッセージ「ＭＥＳ購入要求（MES-Buy-Request）」を構成する。もし現時点で有効な秘密鍵が、相互認証中に有効であった秘密鍵と異なるならば、Ｂは、「ＭＥＳ購入要求」とともに彼の現時点で有効な公開鍵をＳに送信しなければならない。Ｓが「ＭＥＳ購入要求」を受信した後、彼は、Ｂの現時点で有効な公開鍵によって、Ｂの署名を確認してもよい。署名が正当なものであれば、Ｓは「ＭＥＳ購入要求」を記憶し、そして、Ｂがｒを復号化するのを可能にするライセンスを含むメッセージ「ＭＥＳライセンス送信（MES-Send-License）」をＢに送信する。記憶されたデータは、Ｂがマルチメディアリソースｒを購入したいことをＢが確認したことを証明するために、Ｓがネットワーク事業者に提供しうる拒否できない証明である。

【００８８】

表２は、ＳおよびＢによって記憶される証拠を示している。

【表２】

表２　販売者および購入者によって記憶される証拠

	販売者Ｓ	購入者Ｂ
記憶される証拠	・Ｂの証明書 ・確認が送信されたときに有効であったＢの公開鍵（および、Ｂのワンウェイ・ハッシュ・チェーンの対応する元） ・暗号化された資源ｒのハッシュまたは Ｂ に送信されたメッセージ「MES ハッシュ送信」 ・メッセージ「MES 購入要求」、これは、 ・現在時刻 ・Ｂがｒを購入したいことの確認ステートメント ・暗号化された資源ｒのハッシュ ・確認が送信されたときに有効であった秘密鍵によって以前の値に基づいて生成された Ｂ のディジタル署名を備える。 ・暗号化された資源ｒに対するライセンス	・Ｓの証明書 ・暗号化された資源ｒが送信されたときに有効であったＳの公開鍵（および、Ｓのワンウェイ・ハッシュ・チェーンの対応する元） ・メッセージ「MES 送信資源」、これは、 ・現在時刻 ・暗号化された資源ｒを備える。 ・暗号化された資源ｒが送信されたときに有効であった Ｓ の秘密鍵によって署名された「MES 送信資源」のハッシュを含むメッセージ「MES 送信ハッシュ」

【００８９】

売り手が固定ネットワーク内に存在する場合、売り手は、表２に記載された証拠を送信することによって、Ｂがリソースｒを購入したことをネットワーク事業者に証明することができる。ネットワーク事業者は、それのデータベースにＢが登録されていることを検査し、あるいは、Ｂが契約している事業者に照会する。すべてのことが正しければ、事業者は、Ｂの公開鍵が「ＭＥＳ購入要求」が送信されたときに有効であった公開鍵であることを確認するために、Ｂの証明データを使用する。有効な公開鍵は、確認ステートメントの正当性を確認するために、事業者によって使用される。それが正当なものであれば、事業者はＢの公開鍵によって、Ｂの署名（「ＭＥＳ購入要求」に含まれる）を確認する。署名が正当性であることは、売り手Ｓによって送信されたマルチメディアリソースｒをＢが購入したいことをＢが確認したことを事業者に証明することになる。

【００９０】

Ｂがライセンスを受信しなかった場合、Ｂは、ネットワーク事業者に連絡することができ（彼が固定ネットワークに接続されたときに）、そして、ライセンスを要求するために、ネットワーク事業者に証拠（表２に示されるような）を送信することができる。事業者は、その事業者のデータベースに、またはＳが加入している事業者のデータベースに、Ｓが登録されていることを確認する。Ｓが登録されていれば、事業者は、暗号化されたマルチメディアリソースが送信されたとき、Ｓの公開鍵は有効であったことを確認する。公開鍵が有効であったならば、事業者は、「ＭＥＳ購入ハッシュ」を、Ｓによって送信された署名されたハッシュと比較することによって、その「ＭＥＳ購入ハッシュ」もまた有効なものであることを確認する。それらが等しければ、ネットワーク事業者は、アドホックネットワークにおいてＢによって購入されたマルチメディアリソースは、本当にＳによって送信されたことを知ることになる。ネットワーク事業者は、Ｓが生成したライセンスをその事業者のデータベースから探索し、そのライセンスをＢに送信する。

【００９１】

ここで、以下のことに留意すべきである。

このソリューションは、売り手がリソースを販売したこと、およびそのリソースのコン

テンツ所有者（レコード会社など）が報酬を支払われることを、売り手がネットワーク事業者に報告することを必要とする。ユーザはＡＡＡシステムに影響を及ぼすことができないと仮定しているので、トランザクションは自動的に報告される。しかしながら、売り手は正直ではない可能性があり、そして例えば、その売り手の装置を固定ネットワークに接続しないで、その売り手がマルチメディアリソースを配信したことをネットワークプロバイダーに通知することなく、マルチメディアリソースを配信する可能性がある。この事例は、システム全体の複雑さを増大させずに防止することはできない。しかしながら考えられるソリューションとしては、買い手は、トランザクションが報告されたかどうかを、彼の事業者に照会しなければならないこと、そして買い手が永久的なライセンスを入手することである（売り手は、一時的なライセンスを発行するのを許されるだけである）。提案されたソリューションによれば、売り手に報酬を支払うことによってその不誠実な行動を最小限に抑制することが試みられている。売り手は、売り手がトランザクションをネットワークプロバイダーに報告した場合にしか報酬を支払われないので、売り手はトランザクションを報告しないことに経済的利益を有さない。

【００９２】

以下において、本発明の実施形態とともに使用されてもよいＡＡＡアーキテクチャーの構成要素について簡単に説明する。

【００９３】

ＡＡＡアーキテクチャーは、サーバーおよびクライアントからなる。サーバーは、すべての課金データおよび設定データを記憶し、クライアントは、計量された課金データをサーバーに報告する。さらにまた、クライアントは、何がどのように計量されるべきかをサーバーが指定できるように、サーバーによって設定されることが可能である。

【００９４】

一実施形態によるユーザのクライアント装置は、クライアント側で部分的に課金処理を実行できるように、何らかのＡＡＡサーバー機能を有していなければならない。クライアント上のＡＡＡサーバーは、速度およびサイズに関して最適化されたバージョンであってもよく、したがって、本格的なＡＡＡサーバーのすべての機能はなくてもよい。さらにまた、このＡＡＡサーバーは、事業者のネットワーク内に存在するＡＡＡサーバーに課金データを報告できるように、クライアントとしても動作することができなければならない。課金データが事業者に報告されるまでその課金データを記憶することに加えて、サーバーはまた、マルチメディアリソースの販売プロセスに関する情報が規定される設定プロフィールを記憶するものである。

【００９５】

設定プロフィールは、どのデータが計量されなければならないかを記述しており、またユーザが、データを事業者の課金サーバーに再度送信する可能性があるときに、どのデータがユーザの事業者の課金サーバーに送信されなければならないかを記述している。それに加えて、設定プロフィールは、設定プロフィールが正しいことをプロバイダーがどれだけの期間にわたり保証するかに関する情報と、ユーザがマルチメディアリソースを購入／販売するのを許されているかどうかに関する情報とを含むものである。

【００９６】

ＡＡＡクライアント機能は、ＭＥＳ内に統合されているので、サーバーは、それの設定プロフィールを用いてＭＥＳを設定することができ、クライアントは、計量された課金データを装置上のＡＡＡサーバーに報告するようになっている。

【００９７】

当業者には、これまでに説明された実施形態は、ハードウェアによって、ソフトウェアによって、または、ソフトウェアとハードウェアとを組み合わせたものによって実施されうることが理解されるべきである。本発明の実施形態に関連して説明されたモジュールおよび機能は、本発明の実施形態に関連して説明された方法に基づいて動作するように適切にプログラムされた、マイクロプロセッサまたはコンピュータによって、全体的にまたは部分的に実施されてもよい。本発明の実施形態を実施する装置は、例えば、適切にプログ

ラムされたノードまたは構成要素をネットワーク内に備えてもよく、それによって、その装置は、本発明の実施形態において説明されたように認証を実行することができる。これまでの説明に基づいて、当業者は、コンピュータまたはマイクロプロセッサをプログラムする当業者自身のルーチン・プログラマ・スキルを使用することによって、そのような装置またはそのようなモジュールを実施することができ、それによって、それらの装置またはモジュールは、本発明の実施形態に関連して説明された方法のステップを実行することができる。そのためには、従来の何らかのコンピュータまたはマイクロプロセッサが、従来の何らかのプログラミング言語に関連して使用されることが可能である。

【００９８】

本発明の実施形態によれば、データ記憶媒体に記憶されるか、または、記録媒体または伝送リンクのような何らかの物理的手段によって実施されるその他の何らかのやり方で記憶された、コンピュータプログラムが提供され、そのコンピュータプログラムは、コンピュータ上で実行されると、そのコンピュータがこれまでに説明された本発明の実施形態に基づいて動作するのを可能にする。

【００９９】

本発明の実施形態は、例えば、これまでに説明された認証メカニズムに基づいて動作するようにプログラムされた、ネットワーク内のノードまたはネットワーク内の何らかのエンティティーによって実施されてもよい。

【図面の簡単な説明】

【０１００】

【図１】アドホックネットワークによって固定ネットワークのカバレージを拡張することを概略的に示している図である。

【図２】孤立したアドホックネットワークを概略的に示している図である。

【図３】固定ネットワーク内に存在するノードの登録プロセスを概略的に示している図である。

【図４】本発明の一実施形態に基づいてマルチメディアリソースを販売するプロセスを示している図である。

【図５】本発明の一実施形態に基づいて課金データを事業者へ転送するプロセスを示している図である。

【図６】本発明の一実施形態に基づいてワンウェイ・ハッシュ・チェーンの元によって生成された異なる鍵を、異なる時間に割り当てることを示している図である。

【図７】本発明の一実施形態に基づいてどのようにしてクロックドリフトを考慮するかを示している図である。

【図８】本発明の一実施形態に基づいて証拠を使用する動作を示している図である。

【図１】

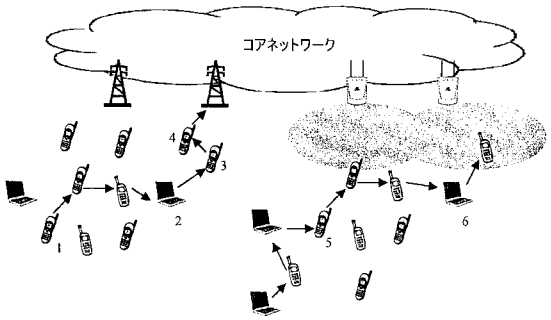

Fig. 1

【図２】

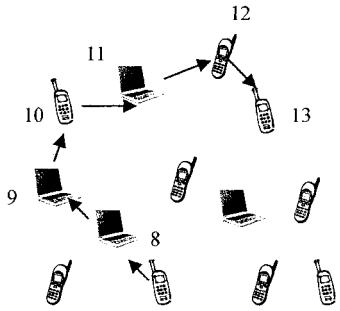

Fig. 2

【図３】

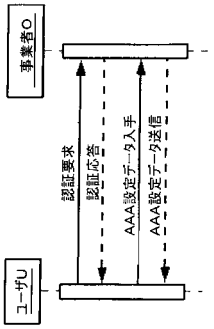

Fig. 3

【図４】

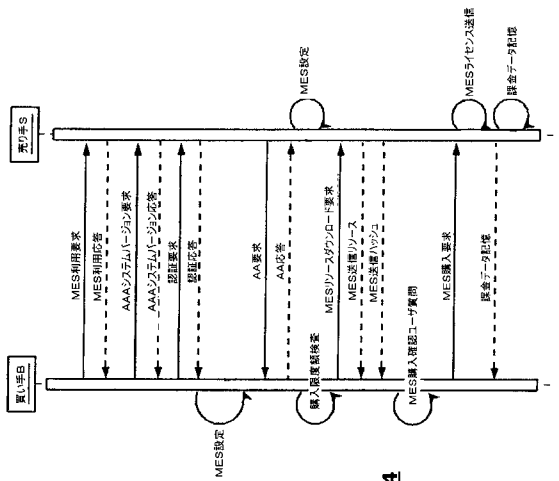

Fig. 4

【図５】

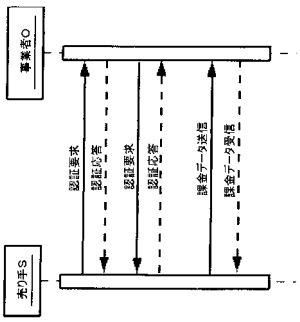

Fig. 5

【図６】

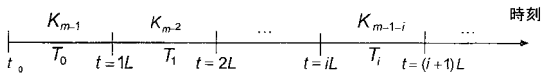

Fig. 6

【図７】

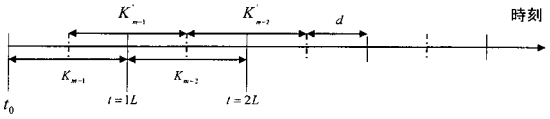

Fig. 7

【図８】

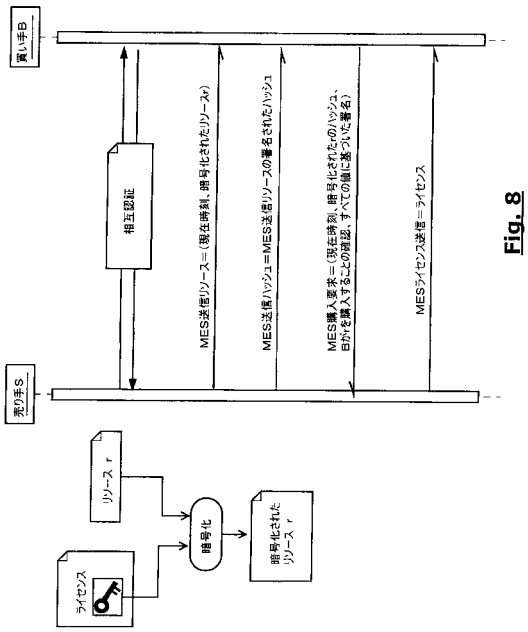
買い手B
売り手S
相互認証
MES送信リソース＝(現在時刻, 暗号化されたリソースr)
MES送信ハッシュ＝MES送信リソースの署名されたハッシュ
MES購入要求＝(現在時刻, 暗号化されたrのハッシュ, Bから支払うことの確認, すべての値に基づいた署名)
MESライセンス送信＝ライセンス
リソース r
ライセンス
暗号化
暗号化された リソース r

Fig. 8

フロントページの続き

(51)Int.Cl. F I
H04L 12/56 (2006.01) H04L 12/56 Z

(72)発明者 クリスティアン・シェーファー
ドイツ連邦共和国，８５７６４ オーバーシュリースハイム，アム・フォーレンガルテン ６エル

審査官 西田 聡子

(56)参考文献 特開２００２－０８４２７４（ＪＰ，Ａ）
特開２００４－０４８４９３（ＪＰ，Ａ）
特開２００５－３１６８３７（ＪＰ，Ａ）
特開２０００－２９５２０８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｑ １０／００
Ｇ０６Ｑ ３０／００
Ｈ０４Ｌ １２／５６
Ｈ０４Ｗ ７４／０８
Ｈ０４Ｗ ８４／１２
ＣｉＮｉｉ