

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4845878号
(P4845878)

(45) 発行日 平成23年12月28日 (2011.12.28)

(24) 登録日 平成23年10月21日 (2011.10.21)

(51) Int. Cl.	F I
H04L 9/32 (2006.01)	H04L 9/00 675B
G09C 1/00 (2006.01)	G09C 1/00 640D

請求項の数 20 (全 21 頁)

(21) 出願番号	特願2007-512154 (P2007-512154)	(73) 特許権者	501263810
(86) (22) 出願日	平成17年4月22日 (2005.4.22)		トムソン ライセンシング
(65) 公表番号	特表2007-536847 (P2007-536847A)		Thomson Licensing
(43) 公表日	平成19年12月13日 (2007.12.13)		フランス国, 92130 イッシー レ
(86) 国際出願番号	PCT/EP2005/051798		ムーリノー, ル ジャンヌ ダルク,
(87) 国際公開番号	W02005/106616		1-5
(87) 国際公開日	平成17年11月10日 (2005.11.10)		1-5, rue Jeanne d' A
審査請求日	平成20年4月17日 (2008.4.17)		rc, 92130 ISSY LES
(31) 優先権主張番号	04291123.0		MOULINEAUX, France
(32) 優先日	平成16年5月3日 (2004.5.3)	(74) 代理人	100070150
(33) 優先権主張国	欧州特許庁 (EP)		弁理士 伊東 忠彦
		(74) 代理人	100091214
			弁理士 大貫 進介
		(74) 代理人	100107766
			弁理士 伊東 忠重

最終頁に続く

(54) 【発明の名称】 証明書の有効性の検査

(57) 【特許請求の範囲】

【請求項 1】

ネットワーク装置（601）に関連付けられた鍵を含む証明書（600）の有効性を検査する方法であって、前記ネットワーク装置は前記証明書を記憶し、前記方法は、前記ネットワーク装置において、

暗号化コンテンツ（611）と、該暗号化コンテンツに関連付けられた有効性指数（630）とを受信する工程と、

前記証明書内に含まれる時間指数（606）であって、前記証明書の発行の時点に相当する値を有する時間指数から、かつ、前記暗号化コンテンツに関連付けられた前記有効性指数から前記証明書の前記有効性を評価する工程とを備えることを特徴とする方法。

10

【請求項 2】

請求項 1 記載の方法であって、

前記有効性指数（630）は、前記関連付けられたコンテンツ（611）と一緒に受信されることを特徴とする方法。

【請求項 3】

請求項 1 又は 2 の何れかに記載の方法であって、

前記有効性指数が暗号化形式で受信され（ボックス 71）、

前記暗号化有効性指数を前記ネットワークで復号する工程（ボックス 72）を更に備えることを特徴とする方法。

【請求項 4】

20

請求項 1 乃至 3 の何れかに記載の方法であって、
前記有効性指数はインテグリティ保護されることを特徴とする方法。

【請求項 5】

請求項 1 乃至 4 の何れかに記載の方法であって、
前記有効性指数が前記時間指数よりも大きい場合に前記証明書を無効であるものとして
評価する工程（ボックス 7 3）を更に備えることを特徴とする方法。

【請求項 6】

請求項 1 乃至 4 の何れかに記載の方法であって、
前記時間指数から有効性間隔を得る工程（ボックス 8 2）と、前記有効性指数が、前記
得られた有効性間隔の外にある場合に前記証明書を無効であるものとして評価する工程（
ボックス 8 5）とを更に備えることを特徴とする方法。 10

【請求項 7】

請求項 1 乃至 4 の何れかに記載の方法であって、
前記受信された有効性指数を用いて、記憶された比較指数を更新する工程であって、前
記更新された比較指数が、前記ネットワークの、決定されたネットワーク装置内に記憶さ
れる工程（ボックス 9 2）と、

前記関連付けられた証明書の前記有効性を評価するよう前記更新された比較指数を前記
時間指数と比較する工程（ボックス 9 3）とを更に備えることを特徴とする方法。

【請求項 8】

請求項 7 記載の方法であって、 20
前記評価する工程は、新たなネットワーク装置（1021b）が前記ネットワーク内に設置
される際に行われることを特徴とする方法。

【請求項 9】

請求項 1 乃至 8 の何れかに記載の方法であって、
前記時間指数、及び前記暗号化コンテンツに関連付けられた前記有効性指数から前記証
明書が有効であるものとして評価された場合に、前記受信された暗号化コンテンツを前記
ネットワークの復号手段で復号する工程（ボックス 8 7 及び 9 6）を更に備えることを特
徴とする方法。

【請求項 10】

請求項 1 乃至 9 の何れかに記載の方法であって、 30
前記暗号化コンテンツ及び前記関連付けられた有効性指数を前記ネットワークのコンテ
ンツ受信器（1001）で受信する工程と、
前記ネットワークの少なくとも 1 つの端末装置（1021a、1021b）に、前記受信された暗
号化コンテンツ及び前記関連付けられた有効性指数を送信する工程とを更に備えることを
特徴とする方法。

【請求項 11】

請求項 10 記載の方法であって、
前記暗号化コンテンツに関連付けられたエンタイトルメント制御メッセージを前記コン
テンツ受信器（1001）で受信する工程であって、前記エンタイトルメント制御メッセージ
が、符号化された制御語を備え、該符号化された制御語が、前記暗号化コンテンツの復号
を可能にする工程と、 40

前記受信された制御語を前記コンテンツ受信器で復号化する工程と、
前記復号化された制御語を対称鍵（Kc）によって再符号化する工程と、
前記少なくとも 1 つの端末装置（1021a、1021b）に前記再符号化された制御語を送信す
る工程とを備えることを特徴とする方法。

【請求項 12】

請求項 11 記載の方法であって、
前記コンテンツ受信器（1001）で前記対称鍵（Kc）を定期的に更新する工程と、
前記更新された対称鍵（Kc）を公開鍵（PUB）によってスクランブルする工程と、
前記スクランブルされた対称鍵（Kc）を前記少なくとも 1 つの端末装置（1021a、1021 50

b) に送信する工程と、

前記公開鍵に対応する秘密鍵 (PRI) を用いて、前記スクランブルされた対称鍵 (Kc) を前記端末装置でスクランブル解除する工程と、

該スクランブル解除された対称鍵 (Kc) を対称ネットワーク鍵 (Kn) によってスクランブルする工程と、

該スクランブルされた対称鍵Kn (Kc) を前記コンテンツ受信器に送信する工程と、

前記スクランブルされた対称鍵Kn(Kc)を前記コンテンツ受信器に記憶する工程と、

前記コンテンツ受信器から少なくとも1つの端末装置に前記スクランブルされた対称鍵Kn(Kc)を前記再符号化された制御語とともに送信する工程と、

前記端末装置に関連付けられた前記証明書 (1002a、1002b) が有効であるものとして評価された場合、前記端末装置で前記対称鍵 (Kc) によって前記再符号化された制御語を復号化する工程と、

前記暗号化コンテンツを前記復号化された制御語によって復号する工程とを更に備えることを特徴とする方法。

【請求項13】

請求項1乃至12の何れかに記載の方法であって、前記暗号化コンテンツが、暗号化された有料テレビ番組であることを特徴とする方法。

【請求項14】

ネットワークのネットワーク装置に関連付けられた証明書 (600) の有効性を検査するシステムであって、

前記ネットワークの少なくとも1つのコンテンツ受信器 (601) であって、暗号化コンテンツ (611)、及び該コンテンツに関連付けられた有効性指数 (630) を少なくとも1つのコンテンツ・プロバイダから受信することを可能にするコンテンツ受信器と、

前記証明書の時間指数 (606) であって、前記証明書の発行の時間に相当する値を有する時間指数から、かつ、前記暗号化されたコンテンツに関連付けられた前記有効性指数から前記証明書の前記有効性を評価するための評価手段 (610) とを備えることを特徴とするシステム。

【請求項15】

請求項14記載のシステムであって、

前記有効性指数がインテグリティ保護されることを特徴とするシステム。

【請求項16】

請求項14又は15記載のシステムであって、

前記有効性指数 (630) が暗号化形式で受信され、

前記暗号化有効性指数を復号するための復号手段 (610) を更に備えることを特徴とするシステム。

【請求項17】

請求項14乃至16の何れかに記載のシステムであって、前記ネットワークの少なくとも1つの端末装置 (1021a、1021b) であって、各端末装置が一証明書 (1002a、1002b) に関連付けられる端末装置を更に備えることを特徴とするシステム。

【請求項18】

請求項17記載のシステムであって、

各端末装置はコンテンツ表示装置 (1016a、1016b) を含み、

各端末装置は、該コンテンツ表示装置に接続されたポータブル・セキュリティ・モジュール (1020a、1020b) を更に含み、

前記証明書 (1002a、1002b) は、前記ポータブル・セキュリティ・モジュール内に記憶された前記端末装置に関連付けられることを特徴とするシステム。

【請求項19】

請求項18記載のシステムであって、

前記コンテンツ受信器 (1001) は符号化制御語も受信し、

前記コンテンツ受信器は、

10

20

30

40

50

前記暗号化コンテンツを受信するための復号器（1017）と、
前記受信された符号化制御語を処理するよう前記復号器に接続された受信器ポータブル・セキュリティ・モジュール（1018）とを備えることを特徴とするシステム。

【請求項 20】

請求項18又は19の何れかに記載のシステムであって、
前記コンテンツ・プロバイダ（1106）は、有料テレビ番組の放送業者であり、
各コンテンツ表示装置はテレビ受像機（1116a、1116b、1116c、1116d、1116e、1116f）であることを特徴とするシステム。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明は一般にセキュア通信ネットワークの分野に関する。

【背景技術】

【0002】

ネットワークを介して交換されるデータは複製することができる。よって、ハードウェア製造業者は、交換されるデータを保護し、データ複製の許可又は禁止を管理しなければならない。通常、公開鍵インフラストラクチャ（PKI）が提供される。第3者機関（例えば、認証局）は秘密鍵・公開鍵の対を生成する。秘密鍵・公開鍵の対は、ネットワークのネットワーク装置間のデータ交換に関与する。

【0003】

20

第3者機関は、秘密・公開鍵の対の公開鍵を含む証明書に署名する。通常、ネットワークの各ネットワーク装置は、決定された証明書に関連付けられる。決定された証明書は、例えば、関連付けられたネットワーク装置のポータブル・セキュリティ・モジュール内に記憶することができる。上記証明書によって、ネットワークのネットワーク装置間のみでデータが確実に交換されることが可能になる。

【0004】

図1は、従来技術による証明書の例を示す。証明書100は、認証局によって生成される。証明書100は、情報部分101及び署名部分102を備える。

【0005】

情報部分101は、公開鍵フィールド103における少なくとも公開鍵PUB、及び関連付けられたネットワーク装置の識別フィールド104を備え、それによって、関連付けられたネットワーク装置に公開鍵PUBが確実に取り付けられることが可能になる。情報部分101は、証明書100の標準を示す標準フィールド105と、証明書100が有効な時間間隔を規定する第1の日付及び第2の日付を備える有効フィールド106とを更に備える。

30

【0006】

署名部分102は、情報部分101から生成される。認証局は、コンテンツのマークを供給することを可能にするハッシュ関数を情報部分101のコンテンツに施す。マークは認証局秘密鍵によって後に暗号化され、暗号化マークは署名部分102内に記憶される。

【0007】

40

認可された装置がネットワーク装置と通信したい場合、認可された装置は、証明書100の有効性及びインテグリティを検査する。

【0008】

証明書100の有効性は、有効性フィールド106の第1の日付及び第2の日付から検査される。

【0009】

証明書100が有効なものとして評価された場合、認可された装置は、ネットワーク装置の証明書100の情報部分101のコンテンツにハッシュ関数を施す。認可された装置は、認証局秘密鍵に関連付けられた認証局公開鍵によって署名部分102を復号する。

【0010】

50

ハッシングされたコンテンツ及び復号署名部分が類似している場合、ネットワーク装置の公開鍵は正規のものとみなされる。

【0011】

ハッカーは、ハッカー鍵によって、ネットワーク装置の正規の公開鍵を首尾良く置き換え得る。そうした場合、ネットワーク装置に関連付けられた証明書によって、ハッカー鍵が偽であるものとして識別することが可能になる。ネットワーク装置との如何なる通信も以降禁止し得る。

【0012】

Thomson Licensing SAによる西暦2002年10月30日付公開の欧州特許出願第1253762号明細書には、証明書を伴うセキュア通信ネットワークの例が開示されている。

10

【0013】

図2は、欧州特許出願第1253762号明細書に記載されているセキュア通信ネットワークの例を示す。図示した通信ネットワークはSmartRight（スマートライト）標準に準拠している。

【0014】

コンテンツ受信器201は、少なくとも1つの端末装置（221a、221b）にデータを送信する。単一のコンテンツ受信器201に対して複数の端末装置（221a、221b）が備えられる場合、端末装置（221a、221b）はローカル・ネットワーク222を形成する。

【0015】

ローカル・ネットワーク222の各端末装置（221a、221b）は、第3者機関（例えば、認証局（図示せず））によって認証された公開鍵PUBを備える。公開鍵PUBは、端末装置（221a、221b）に関連付けられた証明書（202a、202b）に記憶される。

20

【0016】

コンテンツ受信器201は、暗号化コンテンツCW(data)をコンテンツ・プロバイダから受信する。暗号化データCW(data)は後に、ローカル・ネットワーク222の端末装置（221a、221b）に送信される。

【0017】

受信コンテンツは有料テレビ番組であり得る。コンテンツ・プロバイダ206は、放送業者（例えば、衛星放送業者）であり得る。各端末装置（221a、221b）は通常、コンテンツ表示装置（216a、216b）（例えば、テレビ受像機）、及びポータブル・セキュリティ・モジュール（220a、220b）（例えば、スマートカード）を備える。

30

【0018】

暗号化コンテンツCW(data)はデータ・ストリームFにおいてブロードキャストされる。データ・ストリームFは、符号化された制御語K(CW)を含むエンタイトルメント制御メッセージ(ECM)を更に備える。制御語CWによって、暗号化コンテンツCW(data)の復号が可能になる。複数の鍵が暗号化コンテンツCW(data)のスクランブル解除に関係する。証明書（202a、202b）を用いてこれらの鍵の一部を取得する。

【0019】

通常、新たなネットワーク装置がローカル・ネットワークに設置されると、関連付けられた証明書によって、対称ネットワーク鍵Knのアクセスが可能になる。対称ネットワーク鍵は後に、新たに生成される対称鍵Kcの通信に用いられる。証明書がこの通信に関係する。更に、証明書の有効性を検査して、関連付けられた端末装置が暗号化コンテンツを復号することを可能にすることができる。

40

【0020】

図3は、欧州特許出願第1253762号明細書による、ローカル・ネットワーク内の新たな端末装置の設置時に原端末装置と新たな端末装置との間で対称ネットワーク鍵を通信することを示すタイム・チャートを含む。

【0021】

原端末装置321aは、対称ネットワーク鍵Knを有する。新たな端末装置321bがローカル・ネットワーク内に設置されると、原端末装置321aは、新たな端末装置321bに関連付けられ

50

た証明書302bを読み取る。情報部分303bのコンテンツ及び署名部分304bのコンテンツを処理して、新たな端末装置321bに公開鍵PUBが適切に関連付けられているかを評価する。証明書の有効性も、証明書304bの有効性フィールド312bによって検査される。

【0022】

新たな端末装置321bは、証明書302bに記憶された公開鍵PUBを原装置321aに送信する。原装置321aは送信された公開鍵PUBを受信し、受信公開鍵PUBによって対称ネットワーク鍵Knを暗号化する。暗号化対称ネットワーク鍵PUB (Kn) は後に、新たな端末装置321bに送信される。新たな端末装置321bに記憶された秘密鍵PRIによって、暗号化対称ネットワーク鍵PUB (Kn) の復号が可能になる。

【0023】

対称ネットワーク鍵Knを、ローカル・ネットワークの端末装置 (321a、321b) とのデータ交換に用いる。

【0024】

次に図2を参照すれば、コンテンツ受信器201はデータ・ストリームFをコンテンツ・プロバイダ206から受信する。データ・ストリームFは、暗号化コンテンツCW(data)及びエンタイトルメント制御メッセージ (ECM) を備える。ECMは符号化制御語K(CW)自体を備え、制御語CWは鍵Kによって符号化される。

【0025】

コンテンツ受信器201は、復号器217、及び受信器ポータブル・セキュリティ・モジュール218 (例えば、スマートカード) を備える。コンテンツ受信器201によって、受信制御語CWの復号化及び再符号化が可能になり、制御語CWは対称鍵Kcによって再符号化される。暗号化データCW(data)及び再符号化制御語Kc(CW)は、少なくとも1つの端末装置 (221a、221b) に送信される。

【0026】

対称鍵Kcは好ましくは定期的に (例えば、各データ送信の開始時に) 更新される。

【0027】

図4は、従来技術による、スクランブルされた対称鍵Kn(Kc)の例を示す。コンテンツ受信器401は、端末装置421に関連付けられた公開鍵PUBが正規のものであることを証明書402が保証するかを確かめる。証明書の有効性402は、証明書402の有効性フィールド405によっても検査される。

【0028】

コンテンツ受信器401は後に、新たな対称鍵Kcを端末装置421に送信し、送信対称鍵Kcは公開鍵PUBによってスクランブルされる。端末装置421は、端末装置421に記憶された、関連付けられた秘密鍵PRIによって、スクランブルされた対称鍵Kcをスクランブル解除する。端末装置421は後に、対称ネットワーク鍵Knによって対称鍵Kcを再スクランブルする。コンテンツ受信器401は、再スクランブルされた対称鍵Kn (Kc) を端末装置421から受信する。対称鍵Kcが、そのスクランブル形式Kn(Kc)でコンテンツ受信器401内に記憶される。

【0029】

次に図2を参照すれば、コンテンツ受信器201は、獲得後に、そのスクランブル形式Kn (Kc) で対称鍵Kcを有する。

【0030】

コンテンツ受信器201は、スクランブルされた対称鍵Kn(Kc)及び処理済データ・ストリーム (すなわち、暗号化コンテンツCW(data)及び再符号化制御語Kc(CW)) を端末装置 (221a、221b) に送信する。

【0031】

各端末装置(221a、221b)は後に、対称ネットワーク鍵Knによって対称鍵Kn (Kc) をスクランブル解除することができる。対称鍵Kcによって、再符号化制御語Kc (CW) を復号化し、よって、暗号化コンテンツCW(data)を復号することが可能になる。各証明書 (202a、202b) の有効性が、受信コンテンツの復号を可能にする前に検査される。

10

20

30

40

50

【0032】

しかし、ハッカーは場合によっては、公開鍵を首尾良く取得し、認可されていない端末装置をローカル・ネットワークに挿入し得る。

【0033】

従来技術のシステムにおけるセキュリティを向上させるために、公開鍵は、暗号化を補強するように、より大きなサイズを有する鍵によって置き換えることができる。例えば、1024ビットのRSAアルゴリズムは、2048ビットのRSAアルゴリズムによって置き換えることができる。暗号化アルゴリズム、又は証明書の標準も更新することができる（例えば、RSAアルゴリズムを、よりセキュアな暗号アルゴリズムによって置き換える）。証明書はよって、定期的に（例えば、年1回）更新される。

10

【0034】

決定された証明書の有効性は、数回、検査することができる（例えば、新たな端末装置をセキュア通信ネットワーク内に設置する際に、又は、図4に示すように、新たな対称鍵Kcが生成され、端末装置に送信される際に）検査することができる。端末装置の所有者が受信コンテンツをアクセスすることを確実に可能にするように、有効性の連続した検査を行うこともできる。

【0035】

図5は、従来技術による、証明書の有効性を検査するシステムの例を示す。証明書500は、X509標準に準拠し得るものであり、どの開始日からどの終了日まで証明書500を有効なものとし得るかを規定する有効性フィールド506を備える。よって、有効性フィールド506は、証明書500を有効なものとし得る時間間隔を構成する第1の日付508及び第2の日付509を含む。

20

【0036】

関連付けられた端末装置521の処理手段510によって、証明書500の第1の日付508及び第2の日付509を、クロックが供給する現行日付と比較して証明書500の有効性を評価することが可能になる。

【0037】

現行日付が第1の日付及び第2の日付によって規定される時間間隔に属する場合、証明書500は有効なものとしなされる。証明書202の公開鍵PUBをアクセスし、よって、受信された暗号化コンテンツ511の復号を間接的に可能にすることができる。

30

【0038】

現行日付が時間間隔の外にある場合、証明書500が失効したか、又は証明書500がまだ有効でないとみなされる。

【0039】

有料テレビ・システムの場合、証明書500は定期的に更新する、又は置き換えることができる。加入者が賃借料の支払いを止めた場合、証明書500は置き換えられず、コンテンツ端末521は、受信された暗号化コンテンツ511を復号することがもうできない。

【0040】

特定の証明書の有効性は、失効した証明書、又は失効した証明書の識別子を備える証明書失効リスト（CRL）によって評価することもできる。端末装置の証明書は、CRL内に記載されていない限り、有効なものとしなされる。決定された証明書をハッカーが首尾良く取得した場合、決定された証明書を第3者機関は最新CRLに添付する。

40

【発明の開示】

【発明が解決しようとする課題】

【0041】

通常、証明書の有効性は、2つの工程の手順に従って評価される。証明書の有効性フィールドもCRLも評価に関係する。有効性フィールドは、証明書が有効であることが期待される時間間隔を構成する第1の日付及び第2の日付を備える。しかし、保護コンテンツをハッカーが首尾良くアクセスした場合、証明書は期待されたよりも早くディセーブルす

50

ることができる。新たなCRLが生成され、新たなCRLは、ディセーブルされた証明書の識別子を備える。よって、ディセーブルされた証明書は評価の第1の工程で有効なものとして評価され、第1の工程には有効性フィールドのみが関係する。評価の第2の工程では、ディセーブルされた証明書の識別子が、CRLの失効証明書識別子の中から探索され、ディセーブル証明書が無効なものとして明確に評価される。

【課題を解決するための手段】

【0042】

第1の局面では、本発明は、ネットワーク内のネットワーク装置に関連付けられた鍵を含む証明書の有効性を検査する方法を提供する。上記方法は、暗号化コンテンツと、このコンテンツに関連付けられた有効性指数とをネットワークで受信する工程を備える。証明書の有効性は、証明書内に含まれる時間指数と、暗号化コンテンツに関連付けられる有効性指数とを用いて評価される。時間指数は、証明書の発行の時点に相当する値である。

10

【0043】

第1の好ましい実施例では、有効性指数は、関連付けられたコンテンツと一緒に受信される。

【0044】

第2の好ましい実施例では、有効性指数は暗号化形式で受信される。暗号化された有効性指数は、ネットワークで復号される。

【0045】

第3の好ましい実施例では、有効性指数は、インテグリティ保護される。

20

【0046】

第4の好ましい実施例では、有効性指数が時間指数より大きい場合に、証明書は無効であるものとして評価される。

【0047】

第5の好ましい実施例では、有効性間隔が時間指数から得られる。証明書は、得られた有効性間隔の外に有効性指数がある場合に、無効であるものとして評価される。

【0048】

第6の好ましい実施例では、方法は、受信有効性指数を用いて比較指数を更新する工程を更に備える。比較指数は、ネットワークの、決定されたネットワーク装置内に記憶される。更新された比較指数を時間指数と比較して、関連付けられた証明書の有効性を評価する。

30

【0049】

第7の好ましい実施例では、新たなネットワーク装置がネットワーク内に設置される際に評価が行われる。

【0050】

第8の好ましい実施例では、時間指数、及び暗号化コンテンツに関連付けられた有効性指数によって有効であるものとして証明書が評価された場合に、受信された暗号化コンテンツがネットワークで復号される。

【0051】

第9の好ましい実施例では、方法は、暗号化コンテンツ及び関連付けられた有効性指数をネットワークのコンテンツ受信器で受信する工程を更に備える。受信された暗号化コンテンツと、関連付けられた有効性指数は、ネットワークの少なくとも1つの端末装置に送信される。

40

【0052】

第10の好ましい実施例では、方法は、暗号化コンテンツに関連したエンタイトルメント制御メッセージをコンテンツ受信器で受信する工程を更に備える。エンタイトルメント制御メッセージは、暗号化された制御語を備え、この制御語によって、暗号化コンテンツの復号が可能になる。受信された制御語はコンテンツ受信器で復号化され、後に、対称鍵によって再符号化される。再符号化された制御語は、少なくとも1つの端末装置に送信される。

50

【0053】

第11の好ましい実施例では、対称鍵は、コンテンツ受信器で定期的に更新される。新たな対称鍵は、公開鍵によってスクランブルされ、少なくとも1つの端末装置に送信される。スクランブルされた対称鍵は、公開鍵に相当する秘密鍵を用いて少なくとも1つの端末装置でスクランブル解除される。スクランブル解除された対称鍵は、対称ネットワーク鍵によってスクランブルされ、後に、コンテンツ受信器に送信される。スクランブルされた対称鍵は、コンテンツ受信器内に記憶される。上記方法は、コンテンツ受信器から少なくとも1つの端末装置に、再符号化された制御語とともに、スクランブルされた対称鍵を送信する工程を更に備える。端末装置に関連付けられた証明書が有効であるものとして評価された場合、再符号化された制御語は、端末装置で対称鍵によって復号化される。暗号化コンテンツは、復号化制御語とともに復号される。

10

【0054】

好ましくは、暗号化コンテンツは、暗号化された有料テレビ番組である。

【0055】

第2の局面では、本発明は、ネットワークのネットワーク装置に関連付けられた証明書の有効性を検査するシステムを提供する。上記システムは、ネットワークの少なくとも1つのコンテンツ受信器を備え、このコンテンツ受信器によって、暗号化コンテンツと、このコンテンツに関連付けられた有効性指数とを少なくとも1つのコンテンツ・プロバイダから受信することが可能になる。評価手段によって、証明書の時間指数（この時間指数は、証明書の発行の時点に相当する値を有する）から、かつ、暗号化コンテンツに関連付けられた有効性指数から証明書の有効性を評価することが可能になる。

20

【0056】

第12の好ましい実施例では、有効性指数は暗号化形式で受信される。上記システムは、暗号化された有効性指数を復号するための復号手段を更に備える。

【0057】

第13の好ましい実施例では、上記システムは、ネットワークの少なくとも1つの端末装置を更に備える。各端末装置は、1つの証明書に関連付けられる。

【0058】

第14の好ましい実施例では、各端末装置は、コンテンツ表示装置と、このコンテンツ表示装置に接続されたポータブル・セキュリティ・モジュールとを備える。端末装置に関連付けられた証明書は、ポータブル・セキュリティ・モジュール内に記憶される。

30

【0059】

第15の好ましい実施例では、コンテンツ受信器は、符号化された制御語も受信する。コンテンツ受信器は、暗号化コンテンツを受信するための復号器と、受信された符号化制御語を処理するよう復号器に接続された受信器ポータブル・セキュリティ・モジュールとを備える。

【0060】

第16の好ましい実施例では、SmartRight（スマートライト）環境が用いられる。

【0061】

好ましくは、コンテンツ・プロバイダは、有料テレビ番組の放送業者である。

40

【0062】

好ましくは、各コンテンツ表示装置は、テレビ受像機である。

【発明を実施するための最良の形態】

【0063】

本発明の他の局面及び特徴は、以下の明細書及び特許請求の範囲から明らかであろう。

【実施例】

【0064】

セキュア通信ネットワークを介して交換されるデータは、秘密鍵・公開鍵の対を伴うセキュア・システムによって、複製から保護することができる。公開鍵は通常、受信コンテンツを端末装置がアクセスすることを可能にするように端末装置に関連付けられた証明書

50

内に格納されている。

【0065】

証明書は定期的に更新されるか、又は置き換えられる。特定の証明書の有効性は、クロックによって供給される現行日付を証明書の有効性フィールドの第1の日付及び第2の日付と比較することによって検査することができる。

【0066】

しかし、一部の端末装置（特に、消費者向電子装置）はクロックを備えていない。対応策として、第1の方法及び第2の方法によって、以下のように証明書の有効性を検査することが可能になる。

【0067】

第1の方法では、現行日付は、ネットワーク・クロックを備える別個のネットワークによって与えられる。

【0068】

第2の方法では、外部ソースをクロックとして用いる。

【0069】

第1の方法も第2の方法も、現行日付の送信時の攻撃を妨げるための強固な認証機構を必要とする。前述の認証機構は比較的に費用がかかり得る。

【0070】

更に、クロックを備える端末装置の場合、ハッカーは、現行時間のエラー値を（例えば、端末装置の電源を削減することによって）供給するようクロックを処理し得る。ユーザ・インタフェースを有する端末装置の場合、ハッカーは、失効した証明書を有効であるものとみなすように非常に容易に、クロックによって供給される現行時間の値を変更することができる。

【0071】

よって、証明書の有効性の評価に関係するクロックを保護する必要がある。このことも、比較的に費用がかかるものであり得る。

【0072】

クロック管理が一切なしで証明書の有効性の検査を可能にするシステムに対する必要性が存在している。

【0073】

図6は、本発明による、証明書の有効性を検査するシステムの例を示す。上記システムによって、証明書600の有効性の検査が可能になる。証明書600は、ネットワークのネットワーク装置601に関連付けられる。

【0074】

上記システムは、暗号化コンテンツ611と、暗号化コンテンツ611に関連付けられた有効性指数630とを少なくとも1つのコンテンツ・プロバイダ（図示せず）から受信するための少なくとも1つのコンテンツ受信器601を備える。

【0075】

上記システムは、評価手段610を更に備える。評価手段610によって、証明書600の時間指数606から、かつ受信された有効性指数630から証明書600の有効性を評価することが可能になる。時間指数606は、証明書600の発行の時点に相当する値を有する。

【0076】

従来技術によるシステムと違って、本発明のシステムによって、クロックなしで証明書の有効性を検査することが可能になる。

【0077】

更に、従来技術によるシステムは、どの開始日からどの終了日まで証明書が有効であるとみなし得るかを示す有効性フィールドを備えた証明書を備える。前述のシステムは、終了日が満了すると証明書を置き換える必要がある。本発明の方法では、証明書は、受信コンテンツに対して相対的な有効性を有する。受信コンテンツをハッカーが首尾良くアクセ

10

20

30

40

50

スしない限り、有効性指数は同じ値を保ち、それによって、証明書の置き換え、及び関連した費用発生を延期することを可能にすることができる。

【0078】

一方、コンテンツ暗号化の強度が期待されたものよりも低くなった場合、より高い値を有する新たな有効性指数によって有効性指数を置き換えることができる。証明書はよって、無効であるものとして評価される（すなわち、システムは、受信された暗号化コンテンツを復号することがもう可能でない）。証明書の所有者はよって、自らの証明書の置き換えを促される。前述のケースは特に、有料テレビ・システムにおいてうまく適合できる。従来技術によるシステムは、証明書の所有者が終了日の満了前に証明書を置き換えることを奨励することができない。それは、証明書の所有者が受信コンテンツを既にアクセスしているからである。

10

【0079】

評価手段610は、図6に表すように、コンテンツ受信器601の一部であり得る。あるいは、評価手段は、コンテンツ受信器と通信する端末装置の一部である。

【0080】

図7は、本発明の第1の実施例による、証明書の有効性を検査する方法の例を示す図である。証明書は、ネットワーク内のネットワーク装置に関連付けられる。

【0081】

暗号化コンテンツがネットワークで受信される。暗号化コンテンツに関連付けられた暗号化有効性指数がネットワークで受信される（ボックス71）。受信有効性指数が、ネットワークの復号手段で復号される（ボックス72）。

20

【0082】

あるいは、有効性指数VIは、目に見える結果なしで有効性指数VIの値をハッカーが変えることが可能でないようにインテグリティ保護される。例えば、指数署名が、有効性指数と関連付けられる。指数署名は、有効性指数の値から、かつネットワークのセキュア装置に記憶された秘密鍵から計算される値を有する。セキュア装置（例えば、コンテンツ受信器）は、指数署名によって有効性指数のインテグリティを検査することを可能にする検査手段（例えば、ポータブル・セキュリティ・モジュール）を備える。受信有効性指数の値は、秘密鍵によってスクランブルされ、関連付けられた指数署名と後に比較される。これによって、有効性指数の値の改変を検出することが可能になる。

30

【0083】

あるいは、有効性指数は、ハッカーの試行を（非効果的なものであっても）検出することが可能になるように暗号化し、インテグリティ保護することができる。

【0084】

証明書の有効性は、復号された有効性指数VIから評価され、証明書内に含まれた時間係数TIから評価される。時間指数TIは、証明書の発行の時点に相当する値を有する。より厳密には、有効性指数VIが時間指数TIと比較される（ボックス74）。有効性係数VIが時間係数TL以下の場合、証明書は有効なものとして評価される（ボックス75）。

【0085】

有効性指数VIが時間指数TIよりも大きい場合、証明書が失効したものとみなされる。証明書は無効であるものとして評価される（ボックス73）。

40

【0086】

あるいは、証明書は、有効性指数VIが時間指数TLに等しい場合にのみ、有効であるものとして評価される。有効性指数VIが時間指数TIよりも小さい場合、証明書はまだ有効でないものとみなされるか、又は、有効性指数VIに関連付けられた暗号化コンテンツは、古い証明書を有するユーザのみを対象とするものとみなされる。前述のケースでは、関連付けられたコンテンツは、例えば、新たな証明書をユーザが購入することを奨励する視聴覚メッセージであり得る。証明書はよって、時間指数及び有効性指数が異なる場合、無効であるものとして評価される。

【0087】

50

図8は、本発明の第2の実施例による、証明書の有効性を検査する方法の例を示す。

【0088】

証明書は、証明書の発行の時点（例えば、証明書のハードウェア・サポートの製造日付）に相当する値を有する時間指数TIを備える。時間指数TIが読み取られる（ボックス81）。

【0089】

有効性間隔Iが、時間指数TIの、読み取られた値から得られる（ボックス82）。

【0090】

時間係数TIは、証明書内に暗号化形式で含まれている場合がある。前述のケース（図示せず）の場合、時間係数TIは、有効性間隔Iを得る前に復号される。

10

【0091】

暗号化コンテンツ、及び関連した有効性指数VIがネットワークで受信されると（ボックス83）、証明書の有効性が評価される。受信された有効性指数VIが時間間隔Iに属する場合、証明書は有効であるものとして評価される（ボックス86）。受信有効性指数VIが時間間隔Iの外にある場合、証明書は無効であるものとして評価される（ボックス85）。

【0092】

証明書が有効であるものとして評価された場合、受信暗号化コンテンツが復号される（ボックス87）。

【0093】

20

時間間隔は、半無限であり得る。時間間隔Iは例えば、時間指数の値以下の何れかの値を備え得る。

【0094】

あるいは、時間間隔は、有限の範囲を包含する。100に等しい値を有する時間指数例の場合、時間間隔Iは、80と120との間の何れかの値を備え得る。証明書に関連付けられたネットワーク装置によって、この場合、80を上回り、かつ120未満の有効性指数に関連付けられた暗号化コンテンツを復号することが可能になる。

【0095】

図9は、本発明の第3の実施例による、証明書の有効性を検査する方法の例を示す図である。証明書は、ネットワークのネットワーク装置に関連付けられる。

30

【0096】

暗号化コンテンツ、及び関連付けられた有効性指数VIが、ネットワークで受信される（ボックス91）。受信された有効性指数を用いて、比較指数CIを更新する（ボックス92）。比較指数は、ネットワークの、決定されたネットワーク装置（例えば、証明書が関連付けられたネットワーク装置）内に記憶される。

【0097】

更新された比較指数が、証明書内に含まれている時間指数TIと比較される（ボックス93）。時間指数は、証明書の発行の時点に相当する値を有する。証明書の有効性はよって、時間指数TIから、かつ有効性指数VIから評価される。有効性指数VIによって、比較指数CIの更新のみが可能になる。

40

【0098】

更新された比較指数よりも時間指数TIが小さい場合、証明書は無効であるものとして評価される（ボックス94）。一方、時間指数TIが、更新された比較指数以上の場合、証明書は有効であるものとして評価される（ボックス95）。この前述のケースでは、受信された暗号化コンテンツが復号される（ボックス96）。

【0099】

図10は、本発明の第4の実施例による、セキュア通信ネットワークの例を示す。セキュア通信ネットワークは、コンテンツ受信器1001及び少なくとも1つの端末装置（1021a、1021b）を備える。各端末装置（1021a、1021b）は、証明書（1002a、1002b）と関連付けられる。

50

【0100】

コンテンツ受信器1001によって、暗号化コンテンツCW(data)（例えば、暗号化された有料テレビ番組）をコンテンツ・プロバイダ1006（例えば、有料テレビ番組の放送業者）から受信することが可能になる。

【0101】

複数の端末装置（1021a、1021b）を、単一のコンテンツ受信器1001に備え、よってローカル・ネットワーク1022を構成することを可能にすることができる。ローカル・ネットワーク1022の端末装置（1021a、1021b）は通常、コンテンツ表示装置（1016a、1016b）と、コンテンツ表示装置（1016a、1016b）に接続されたポータブル・セキュリティ・モジュール（1020a、1020b）とを備える。

10

【0102】

各ポータブル・セキュリティ・モジュール（1020a、1020b）によって、端末装置（1021a、1021b）に関連付けられた証明書（1002a、1002b）を記憶することが可能になる。ポータブル・セキュリティ・モジュール（1020a、1020b）は例えば、スマートカードであり得る。

【0103】

コンテンツ表示装置（1016a、1016b）はテレビ受像機であり得る。ローカル・ネットワーク1022はよって、単一の所有者のテレビ受像機を備える。暗号化された有料テレビ番組はコンテンツ受信器1001で受信され、上記所有者のテレビ受像機に更に送信される。

【0104】

20

新たなテレビ受像機1016bが設置される場合、新たなスマートカード1020bが新たなテレビ受像機1016bに接続される。スマートカード1020bによって、関連付けられた証明書1002bを記憶することが可能になる。適切な条件下では、証明書1002bによって、新たな端末装置1021bが設置時に対称ネットワーク鍵Knを獲得することが可能になる。対称ネットワーク鍵Knによって、コンテンツ受信器1001と端末装置（1021a、1021b）との間のデータ交換を保護することが可能になる。

【0105】

新たなテレビ受像機1016bに接続される新たな証明書1002bの有効性は、設置時に検査することができる。評価手段1010bによって、ブロードキャスト有効性指数VIから、かつ、新たな証明書1002bの時間指数1012bから新たな証明書1002bの有効性を評価することが可能になる。時間指数1012bは、新たな証明書1002bの発行の時点に相当する値を有する。有効性指数VIは、コンテンツ受信器1001で受信される暗号化コンテンツCW(data)に関連付けられる。

30

【0106】

有効性指数VIは、コンテンツ受信器1001で、暗号化形式で受信することができる。コンテンツ受信器1001は後に、有効性指数を復号する。

【0107】

有効性指数VIによって、コンテンツ受信器1001に記憶された比較指数CIの更新が可能になる。例えば、更新は比較指数CIを有効性指数の値、増やすことからなる。有効性指数がゼロよりも低い値を有する場合、比較指数の値を減らす。

40

【0108】

更新された比較指数CIは後に、端末装置（1021a、1021b）に送信される。

【0109】

更新された比較指数CIは、コンテンツ受信器でスクランブルし、スクランブル形式で送信し（図10に図示せず）、端末装置でスクランブル解除することができる。

【0110】

従来技術において行われるように証明書の開始日及び終了日を、クロックによって供給される現行時間と比較する代わりに、本発明の方法は、時間指数1012bを比較指数CLと比較する工程を備える。

【0111】

50

時間指数TIが比較指数CI以上の場合、新たな証明書1002bが有効なものとして評価される。

【0112】

時間係数TIが比較指数CIよりも小さい場合、証明書は無効であるものとして評価され、新たなテレビ受像機1016bを、ローカル・ネットワーク1022内に設置することができない。

【0113】

あるいは、無効の証明書を備えたスマートカードを有する新たなテレビ受像機を、ローカル・ネットワーク内に受け入れ得る。受信された有料テレビ番組の更なる復号時に、新たなテレビ受像機が、有料テレビ番組の大半にアクセスできない場合がある。無料テレビ番組、及び十分低い値を有する比較指数CIに関連付けられた有料テレビ番組（すなわち、多数の人々に到達することが意図された有料テレビ番組）のみをテレビ受像機でアクセスすることができる。

【0114】

コンテンツ受信器1001と端末装置（1021a、1021b）との間で交換されるデータは、コンテンツ受信器1001で生成される対称鍵Kcによって保護することができる。

【0115】

対称鍵Kcは好ましくは定期的に（例えば、各データ送信の開始時に）更新される。コンテンツ受信器1001は、新たな対称鍵Kcそれぞれを少なくとも1つの端末装置（1021a、1021b）に送信し、送信された対称鍵Kcは、コンテンツ受信器1001の受信器ポータブル・セキュリティ・モジュール1018に記憶された端末装置の公開鍵PUBによってスクランブルされる。

【0116】

端末装置（1021a、1021b）は、ポータブル・セキュリティ・モジュール（1020a、1020b）に記憶された、関連付けられた秘密鍵PRIによって、スクランブルされた対称鍵Kcをスクランブル解除する。

【0117】

第4の実施例では、証明書（1002a、1002b）の有効性が、対称鍵Kcのスクランブル解除を可能にする前に評価される。

【0118】

ポータブル・セキュリティ・モジュール（1020a、1020b）の評価手段が、（スクランブルされた鍵Kcとともにコンテンツ受信器によって送信された）受信有効指数VIから、かつ端末装置に挿入された時間指数（1012a、1012b）から、受信コンテンツに対する、証明書（1002a、1002b）の有効性を評価する。

【0119】

証明書（1002a、1002b）が有効なものとなされた場合、端末装置によって、秘密鍵PRIによって対称鍵Kcをスクランブル解除することが可能になる。端末装置（1021a、1021b）は後に、新たな端末装置の設置時に、新たな端末装置それぞれによって獲得された対称ネットワーク鍵Knによって、対称鍵Kcを再スクランブルする。コンテンツ受信器1001は、再スクランブルされた対称鍵Kn（Kc）を端末装置（1021a、1021b）から受信する。対称鍵Kcが、スクランブル形式Kn(Kc)でコンテンツ受信器内に記憶される。

【0120】

よって、受信器ポータブル・セキュリティ・モジュール1018によって、端末装置の公開鍵PUB、対称鍵Kc、スクランブルされた対称鍵Kn（Kc）及び比較指数CIを記憶することが可能になる。

【0121】

図示した実施例では、暗号化コンテンツはコンテンツ・プロバイダ1006（例えば、衛星放送業者）からコンテンツ受信器1001にブロードキャストされる。コンテンツ受信器1001は、暗号化コンテンツCW(data)、エンタイトルメント制御メッセージ（ECM）を備えるデータ・ストリームを受信する。ECMは、符号化制御語K（CW）、及びブロードキャ

10

20

30

40

50

ストされたコンテンツに関連付けられた有効性指数VIを備える。制御語によって、暗号化コンテンツCW(data)の復号が可能になる。

【0122】

あるいは、有効性指数は、符号化制御語を含むECMとは別個の第2のECMにおいて送信される。

【0123】

ECMは復号器1017で受信され、受信器ポータブル・セキュリティ・モジュール1018で処理される。受信された符号化制御語は、対称鍵Kcによって復号化され、後に再符号化される。コンテンツ受信器1001は、再符号化制御語Kc(CW)を少なくとも1つの端末装置(1021a、1021b)に送信する。再符号化制御語は、局所エンタイトルメント制御メッセージ(LECM)内に含まれている場合がある。

10

【0124】

コンテンツ受信器1001は又、暗号化コンテンツCW(data)及びスクランブルされた対称鍵Kn(Kc)を少なくとも1つの端末装置(1021a、1021b)に送信する。図10に示すように、スクランブルされた対称鍵Kn(Kc)はLECM内で送信することができる。

【0125】

コンテンツ受信器は、暗号化コンテンツCW(data)、再符号化制御語Kc(CW)、スクランブルされた対称鍵Kn(Kc)及び比較指数CIを、ローカル・ネットワークの他の端末装置と後に通信する単一の端末装置に送信することができる。ローカル・ネットワークの端末装置間の通信には、対称ネットワーク鍵Knが関係し得る。

20

【0126】

あるいは、図10に示すように、コンテンツ受信器1001は、ローカル・ネットワーク1022の端末装置(1021a、1021b)全てと直接通信することができる。

【0127】

対称ネットワーク鍵Knがポータブル・セキュリティ・モジュール(1020a、1020b)内に記憶されるので、端末装置(1021a、1021b)によって、対称鍵Kcをスクランブル解除することが可能になる。符号化された制御語は後に復号化され、それによって、暗号化コンテンツCW(data)の復号が可能になる。

【0128】

受信コンテンツ毎に、関連付けられた比較指数VIによって、端末装置(1021a、1021b)の証明書(1002a、1002b)の時間指数TIと後に比較される比較指数CIを更新することが可能になり、よって、受信コンテンツに対する、証明書(1002a、1002b)の有効性を推定することが可能になる。決定された端末装置(1021a、1021b)の証明書(1002a、1002b)が失効したものと推定された場合、決定された端末装置は、受信コンテンツの復号を可能にすることができない。

30

【0129】

復号は好ましくは、端末装置(1021a、1021b)で行われる。

【0130】

好ましくは、セキュア通信ネットワークは、SmartRight(スマートライト)標準に準拠している。

40

【0131】

セキュア通信ネットワークで受信されたコンテンツは、MPEG-2標準又は何れかの他の標準に従って暗号化することができる。

【0132】

証明書(1002a、1002b)は認証局1008によって署名される。通常、証明書(1002a、1002b)は、添付されたスマートカード(1020a、1020b)の製造時に署名される。

【0133】

第4の実施例では、有効性指数は、符号化制御語を備えるECM内で受信される。前述のECMは通常、10秒毎にブロードキャストされる。よって、有効性指数は、10秒間の視聴覚情報を表すコンテンツに関連付けられる。

50

【0134】

別の実施例（図示せず）では、コンテンツ受信器は、符号化制御語のみを含むECMを受信する。有効性指数は、エンタイトルメント管理メッセージ（EMM）で受信される。有効性指数によって、比較指数CIの更新が可能になる。評価手段は後に、更新された比較指数を証明書の時間指数と比較する。通常、EMMは月に一度ブロードキャストされる。しかし、EMMは、より高い頻度で（特に、ハッカーがコンテンツを首尾良くアクセスした場合）ブロードキャストされ得る。

【0135】

図11A及び図11Bは、本発明の第5の実施例による、テレビ番組のブロードキャストを示す。

10

【0136】

コンテンツ・プロバイダ1106（例えば、衛星放送業者）は、暗号化テレビ番組CW(data)を複数のコンテンツ受信器（1101a、1101b、1101c）にブロードキャストする。適切な条件下では、各コンテンツ受信器（1101a、1101b、1101c）は加入者に属する。

【0137】

各コンテンツ受信器（1101a、1101b、1101c）は、少なくとも1つのテレビ受像機（1116a、1116b、1116c、1116d、1116e、1116f）と通信する。単一の加入者は、複数のテレビ受像機を有し得る。例えば、テレビ受像機1116a及び1116bは単一の加入者に属する。

【0138】

証明書（1102a、1102b、1102c、1102d、1102e、1102f）は、各テレビ受像機（1116a、1116b、1116c、1116d、1116e、1116f）に関連付けられる。証明書（1102a、1102b、1102c、1102d、1102e、1102f）は、証明書（1102a、1102b、1102c、1102d、1102e、1102f）の発行の時間に相当する時間指数TIを備える。図11A及び図11Bに示す例では、時間指数の値は、関連付けられたスマートカードの製造年（例えば、2003）に等しい。

20

【0139】

図11Aに示すように、ブロードキャストされた暗号化テレビ番組が、2000に等しい値を有する有効性指数に関連付けられた場合、2000よりも小さい値を有する時間指数を有する証明書（1102b、1102f）は無効であるものとして評価される。関連付けられたテレビ受像機（1116b、1116f）は、暗号化テレビ番組を復号することができない。相当する加入者は、テレビ番組をアクセスするようスマートカード（1102b、1102f）を置き換える必要がある。

30

【0140】

本発明の方法によって、図11Bに示すように、期待よりも低い値を有する、関連付けられた有効性指数を備えた暗号化テレビ番組をブロードキャストすることが可能になる。ブロードキャストされた有効性指数が1998に等しい値を有する場合、1998よりも高い値を有する時間指数を含む証明書（1102a、1102b、1102c、1102d、1102e）は、有効であるものとして評価される。関連付けられたテレビ受像機（1116a、1116b、1116c、1116d、1116e）によって、ブロードキャストされたテレビ番組にアクセスすることが可能になる。

【0141】

よって、本発明の方法によって、（比較的低い値を有する有効性指数のブロードキャストによって）多数の人々（例えば、古いスマートカードを有する以前の加入者）に到達することが可能になる。決定されたテレビ番組に関連付けられる有効性指数は、テレビ番組が対象とするテレビ受像機によって予め選択される。

40

【0142】

本発明のシステムは、古いスマートカードのみを保有する以前の加入者が古い記録コンテンツを視聴することを可能にするものでもある。

【0143】

証明書の「有効性」は、証明書の時間的な有効性を意味する。有効であるものとして評価される証明書は、他のネットワーク装置との如何なる通信も可能にしない公開鍵を含み得る。

50

【0144】

本発明は、本明細書記載の実施例の如何なる組み合わせも備える。

【0145】

本発明は、限定数の実施例に関して説明したが、本明細書及び特許請求の範囲記載の本発明の範囲から逸脱することなく他の実施例を考え出すことが可能であることが、当業者が本明細書及び特許請求の範囲記載を利用することによって認識されよう。よって、本発明の範囲は、特許請求の範囲によってのみ限定されるものとする。

【図面の簡単な説明】

【0146】

【図1】従来技術による証明書の例を示す図である。

10

【図2】欧州特許出願第1253762号明細書に記載されたセキュア通信ネットワークの例を示す図である。

【図3】欧州特許出願第1253762号明細書による、ローカル・ネットワーク内の新たな端末装置の設置時に原端末装置と新たな端末装置との間で対称ネットワーク鍵を通信することを示すタイム・チャートである。

【図4】従来技術による、スクランブルされた対称鍵Kn (Kc) の例を略示する図である。

【図5】従来技術による、証明書の有効性を検査するシステムの例を示す図である。

【図6】本発明による、証明書の有効性を検査するシステムの例を示す図である。

【図7】本発明の第1の実施例による、証明書の有効性を検査する方法の例を示す図である。

20

【図8】本発明の第2の実施例による、証明書の有効性を検査する方法の例を示す図である。

【図9】本発明の第3の実施例による、証明書の有効性を検査する方法の例を示す図である。

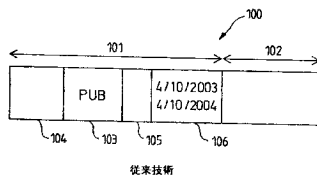
【図10】本発明の第4の実施例による、セキュア通信ネットワークの例を示す図である。

【図11A】本発明の第5の実施例による、テレビ番組のブロードキャストを示す図である。

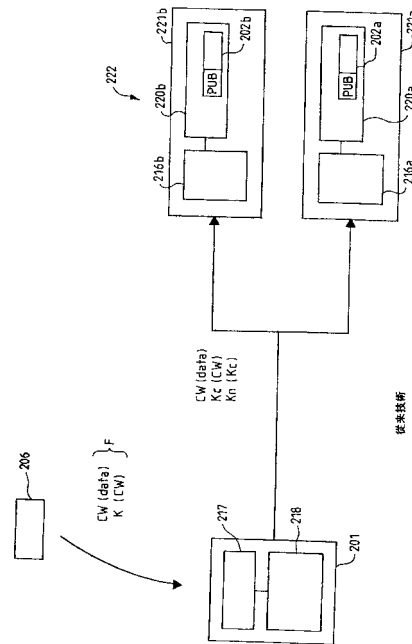
【図11B】本発明の第5の実施例による、テレビ番組のブロードキャストを示す図である。

30

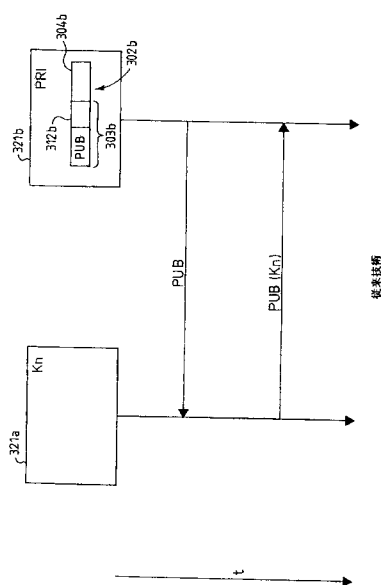
【図 1】



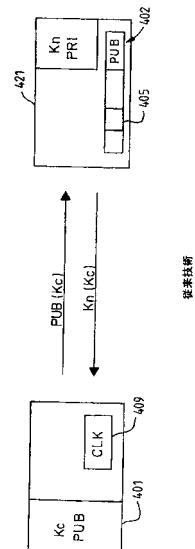
【図 2】



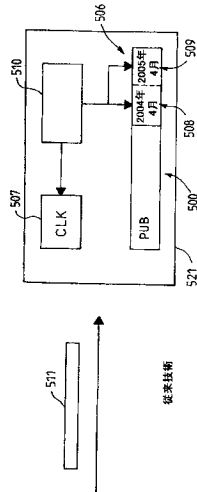
【図 3】



【図 4】



【図 5】



【図 6】

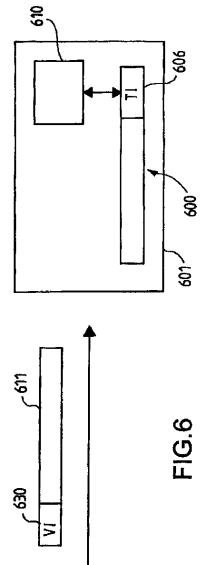
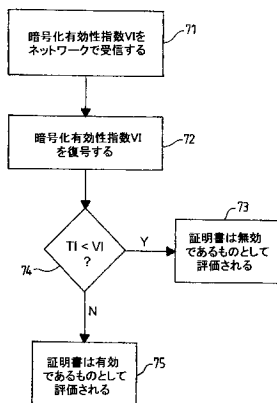
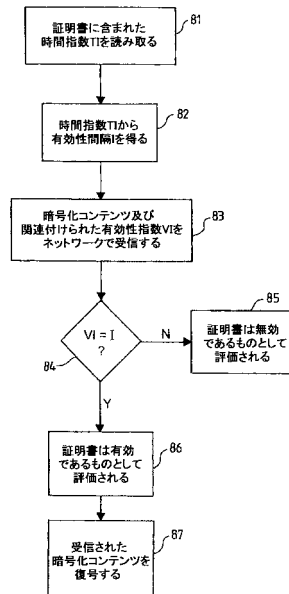


FIG. 6

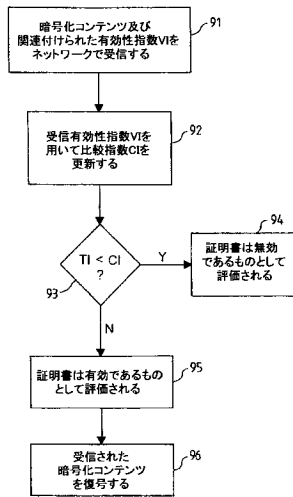
【図 7】



【図 8】



【図 9】



【図 10】

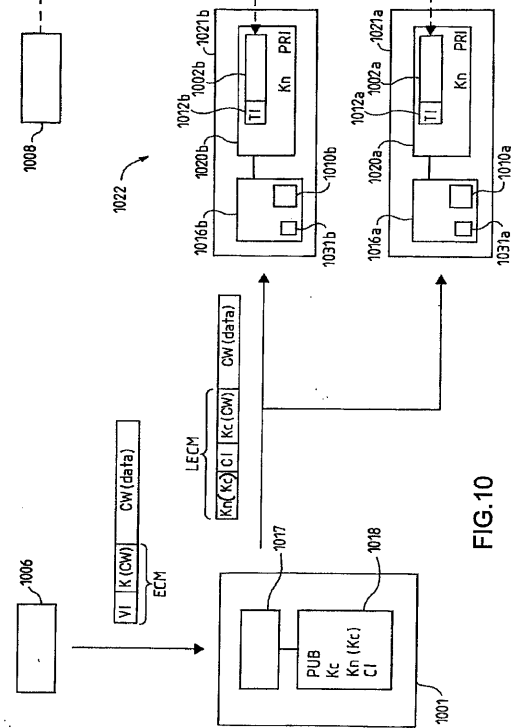


FIG. 10

【図 1 1 A】

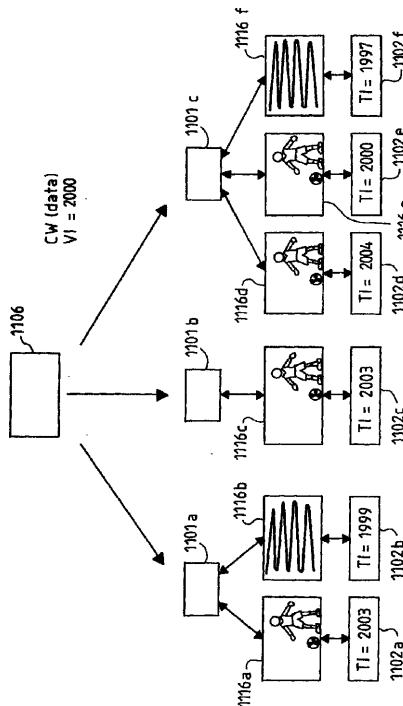


FIG. 11A

【図 1 1 B】

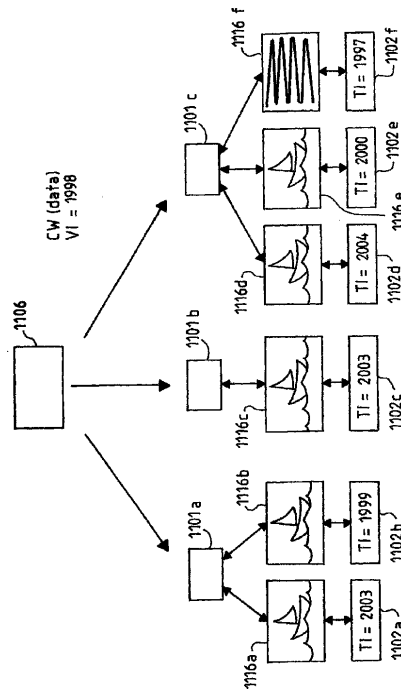


FIG. 11B

フロントページの続き

(72)発明者 デュラン, アラン
フランス国, 3 5 0 0 0 レンヌ, リュ・ド・ディナン 7 9

審査官 新田 亮

(56)参考文献 特表2 0 0 4－5 0 4 6 4 8 (J P, A)
特開2 0 0 3－0 0 8 5 6 6 (J P, A)

(58)調査した分野(Int.Cl., D B名)
H04L 9/32
G09C 1/00