(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6071520号
(P6071520)

(45)発行日　平成29年2月1日(2017.2.1)　(24)登録日　平成29年1月13日(2017.1.13)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675B
G09C	1/00	(2006.01)	G09C	1/00	640D
H04L	9/10	(2006.01)	H04L	9/00	621A

請求項の数 12　外国語出願　(全 10 頁)

(21)出願番号　特願2012-274587 (P2012-274587)
(22)出願日　平成24年12月17日 (2012.12.17)
(65)公開番号　特開2013-128280 (P2013-128280A)
(43)公開日　平成25年6月27日 (2013.6.27)
審査請求日　平成27年12月16日 (2015.12.16)
(31)優先権主張番号　11306683.1
(32)優先日　平成23年12月16日 (2011.12.16)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　Ｆｒａｎｃｅ
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(74)代理人　100117189
弁理士　江口　昭彦

最終頁に続く

(54)【発明の名称】署名検証のための装置および方法

(57)【特許請求の範囲】

【請求項１】

デジタルデータのデジタル署名を検証するための装置であって、

複数の異なる署名エンティティの各々の署名鍵に対応する複数の異なる検証鍵を格納するように構成された第１のメモリと、

前記デジタルデータ及び前記デジタル署名を格納するように構成された第２のメモリであって、前記デジタルデータは、前記装置のブートコードまたは別のデジタルデータを認証するために使用されることになる第２段階の認証鍵を含み、前記デジタル署名は、任意の署名エンティティの署名鍵を用いて提供される、第２のメモリと、

前記装置の電源を入れた、または前記装置をリセットしたとき、前記デジタルデータおよび前記デジタル署名を受信し、前記複数の異なる検証鍵のうちの第１の検証鍵を用いて前記デジタル署名を検証するように構成された処理手段と

を備え、

前記処理手段がさらに、前記第１の検証鍵を用いた検証が不成功である場合、前記複数の異なる検証鍵のうちの第２の検証鍵を用いて前記デジタル署名を検証するように構成される、前記装置。

【請求項２】

前記処理手段は、前記デジタル署名の検証に成功するまで、または前記デジタル署名の検証がすべての格納された検証鍵を使用して不成功になるまで、前記デジタル署名および前記格納された検証鍵のそれぞれを使用して、前記デジタル署名を検証するように構成さ

れる、請求項１に記載の装置。
【請求項３】
前記処理手段は、前記第１の検証鍵を用いて前記デジタル署名の検証に成功しない場合、前記第２の検証鍵を用いて前記デジタル署名を処理することによって前記デジタル署名を検証するように構成される、請求項１に記載の装置。
【請求項４】
前記処理手段は、前記第１の検証鍵および前記第２の検証鍵を並行して使用して前記デジタル署名を検証するように構成される、請求項１に記載の装置。
【請求項５】
前記ブートコードが組み込まれる、請求項１に記載の装置。
【請求項６】
前記デジタル署名の検証に成功した場合に前記ブートコードを実行するように構成された第２の処理手段をさらに備える、請求項５に記載の装置。
【請求項７】
前記処理手段はさらに、前記デジタル署名の検証に成功すると、現在の限定受信システムを識別し、限定受信特定機能を起動するように構成される、請求項１に記載の装置。
【請求項８】
前記第１のメモリは書込み不可能である、請求項１に記載の装置。
【請求項９】
前記装置は、限定受信の受信機であり、前記署名エンティティは、限定受信プロバイダである、請求項１に記載の装置。
【請求項１０】
装置のブートコードまたは別のデジタルデータを認証するために使用されることになる第２段階の認証鍵を含むデジタルデータのデジタル署名を検証するための方法であって、処理手段において、前記装置に電源を入れた、または前記装置をリセットしたとき、
前記装置の第１のメモリから前記デジタルデータおよび前記デジタル署名を受信するステップであって、前記デジタル署名は、任意の署名エンティティの署名鍵を用いて提供される、ステップと、
複数の異なる署名エンティティの各々の署名鍵に対応する複数の異なる検証鍵を格納するように構成された、前記装置の第２のメモリから、前記複数の異なる検証鍵のうちの第１の検証鍵を取得することと、
前記取得した第１の検証鍵を用いて前記デジタル署名を検証することと、
前記検証が不成功であって、前記複数の異なる検証鍵のうちで試していない検証鍵がある場合、前記検証が成功するまで異なる検証鍵を用いて前記デジタル署名を検証することと、
によって前記デジタル署名を検証するステップと
を含む、前記方法。
【請求項１１】
前記取得することおよび前記検証することは、並行して行われる、請求項１０に記載の方法。
【請求項１２】
前記取得することおよび前記検証することは、前記デジタル署名の検証に成功するまで、または前記デジタル署名の検証が利用可能なすべての検証鍵を使用して不成功になるまで、繰り返して行われる、請求項１０に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般にセキュリティに関し、詳細にはデジタル署名の検証に関する。
【背景技術】
【０００２】

この節は、以下に説明するおよび／または特許請求されている本発明の様々な態様に関連する可能性がある当技術分野の様々な態様を読者に紹介することを目的としている。この説明は、本発明の様々な態様をより良く理解する助けとなるように、読者に背景情報を提供するのに役立つと考えられる。したがって、これらの記述は、従来の技術の承認としてではなく、このような観点で読まれるべきであることを理解されたい。

【０００３】

例えば高い価値のあるテレビ番組などの、デジタルコンテンツを保護するために、いわゆる限定受信（Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ、ＣＡ）技術を使用することが、当技術分野ではよく知られている。このような技術は、様々な暗号プロトコルを使用してデジタルコンテンツを暗号化し、後に復号化し、さらに無許可の使用から端末を守る。

【０００４】

ＣＡ技術は、ＣＡプロバイダによってユーザに直接または間接的に提供された何らかの（通常、取り外し可能な）セキュリティ要素を使用して、例えばテレビおよびいわゆるセットトップボックス（ＳＴＢ）などの受信機に実装される。このようなセキュリティ要素の好ましい実装がスマートカードであり、これは当技術分野でよく知られているものである。

【０００５】

ＣＡ保護されたデジタルコンテンツを受信するためには一般に料金を支払う必要があること、および代金を支払わずにＣＡ保護されたデジタルコンテンツを受信するために、著作権侵害者がＣＡシステムを「ハッキング」しようとすることは非常によく起こることであると理解されるであろう。スマートカードがますます安全になる、すなわちますますハッキングしづらくなるにつれて、著作権侵害者は受信機を直接攻撃する傾向にある。

【０００６】

当然ながら、受信機製造業者は、サポートするＣＡプロバイダによって要求され、指定される一定のセキュリティ機能を実装すること、および特に以下を実装するメインＩＣのＣＡ専用版を使用することによって、その受信機のセキュリティを向上させることに取り組んできた。すなわち、

・　１２８ビットの対称鍵として実装することができる、秘密ルート鍵（ＳＲＫ）。

・　有利には非対称の１０２４または２０４８ビットＲＳＡ鍵として実装することができる、公開認証鍵（ＰＵＡＫ）。

【０００７】

チッププロバイダによって実装することができるこうしたセキュリティ機能は、提供される特定のＣＡのセキュリティ要件を満たさなければならない。第１のＣＡプロバイダＡが第２のＣＡプロバイダＢとは異なるセキュリティ要件を有する可能性は非常に高い。これは、Ａのためにカスタマイズされたコンポーネントが、Ｂには役に立たない、またはＢには受け入れられない可能性があることを意味する可能性があり、さらに、ＣＡプロバイダは通常その解決策を他のＣＡプロバイダに伝えない。

【０００８】

さらに、ＣＡプロバイダは商業上の競争相手であることが多いので、ＣＡプロバイダが共通のセキュリティ要件のセットに同意することは難しい可能性がある。この商業上の対抗意識にこのように後押しされてＣＡプロバイダはそのセキュリティ要件を向上させ、それを非公開にしている。

【０００９】

このために、あるＣＡプロバイダは、チッププロバイダの「標準的」セキュリティ機能の代わりに使用するようにチッププロバイダに独自のセキュリティブロックを提供する。

【００１０】

このように様々なＣＡプロバイダが様々なセキュリティ機能を提供することがわかる。

【００１１】

またペイＴＶオペレータのようなＣＡプロバイダの顧客は、複数のＣＡプロバイダからの製品を利用できることに関心があることが理解されるであろう。しかしながらこれまで

のところ、オペレータがＣＡプロバイダを選択すると、次の理由により新しいＣＡプロバイダに切り替えることは困難である。すなわち、
・　導入した受信機を交換するには費用がかかる。古い受信機と新しい受信機の両方が同じように機能できることを保証するようにこれを行うべきである。
・　セキュリティを低下させる危険を冒すことなく、要求されるセキュリティ機能を有効にするプラットフォームを新しいＣＡプロバイダに提供することは困難である。
【００１２】
このために、ペイＴＶオペレータは、同じ受信機ハードウェアが異なるＣＡシステムで使用できるように、ＣＡプロバイダからできるだけ独立していることができることを希望し、したがって、様々なセキュリティ要件が個々にサポートされる。
【００１３】
各ＣＡプロバイダのセキュリティ機能、すなわちセキュリティブロックが、チップ製造業者によって提供されるチップに統合される場合、受信機が複数のＣＡプロバイダに対応しているという要件を満たすことができる。
【００１４】
ＳＷ認証チェーン
例えば受信機に組み込まれたソフトウェア（または第２段階の認証鍵）が有効であることを、電源を入れたときに検証することによって、許可されたソフトウェアのみが受信機にインストールされることを保証するために、有利にはＣＡプロバイダによって保持されるプライベート非対称鍵（ＰＲＡＫ）を使用してソフトウェア（または第２段階の認証鍵）をデジタル署名することが知られている。電源を入れると、受信機は、当技術分野でよく知られているように、ＰＲＡＫに対応するその公開認証鍵（ＰＵＡＫ）を使用して、受信機に組み込まれたソフトウェア（または第２段階の認証鍵）の署名を確認する。
【００１５】
ＣＡプロバイダにとってのＰＵＡＫは、ＣＡプロバイダのセキュリティ要件を満たすためのチップのカスタマイズの一部である。
【発明の概要】
【発明が解決しようとする課題】
【００１６】
これまでのところ、単一ＣＡプロバイダのＰＵＡＫはチップに格納される。これは、別のＣＡプロバイダの他のすべてのセキュリティ機能がチップに実装されても、チップが複数のＣＡシステムに対応することはできないことを意味する。
【００１７】
したがって、受信機が複数のＰＵＡＫを格納および使用できるようにする解決策の必要がある。本発明は、このような解決策を提供する。
【課題を解決するための手段】
【００１８】
第１の態様では、本発明は、デジタルデータのデジタル署名を検証するための装置を対象とする。この装置は、第１の検証鍵を格納するように構成された第１のメモリと、デジタルデータを格納するように構成された第２のメモリであって、デジタルデータは、装置のブートコードまたは別のデジタルデータを認証するために使用されることになる第２段階の認証鍵を含む、第２のメモリと、装置の電源を入れた、または装置をリセットしたとき、デジタルデータおよびデジタル署名を受信して、第１の検証鍵を用いてデジタル署名を処理することによってデジタル署名を検証するように構成された処理手段とを備える。さらに第１のメモリは、第２の検証鍵もまた格納するように構成され、第１の検証鍵および第２の検証鍵は、それぞれ第１の署名エンティティおよび第２の署名エンティティの署名鍵に対応し、さらに処理手段は、第２の検証鍵を用いてデジタルデータを処理することによってデジタル署名を検証するように構成される。
【００１９】
第１の好ましい実施形態では、第１のメモリは、複数の検証鍵を格納するように構成さ

れる。処理手段は、デジタル署名が検証に成功するまで、またはデジタル署名が格納されたすべての検証鍵を使用して不成功になるまで、デジタル署名および格納された検証鍵のそれぞれを使用してデジタル署名を検証するように構成されることが有利である。

【００２０】

第２の好ましい実施形態では、処理手段は、第１の検証鍵を使用してデジタル署名が検証に成功しない場合、第２の検証鍵を用いてデジタル署名を処理することによって、デジタル署名を検証するように構成される。

【００２１】

第３の好ましい実施形態では、処理手段は、第１の検証鍵および第２の検証鍵を並行して使用して署名を検証するように構成される。

【００２２】

第４の好ましい実施形態では、ブートコードが組み込まれる。装置はさらに、デジタル署名が認証に成功した場合にブートコードを実行するように構成された第２のプロセッサを備えることが有利である。

【００２３】

第５の好ましい実施形態では、プロセッサはさらに、デジタルデータの検証に成功すると、現在のＣＡシステムを識別して、ＣＡ特定機能を起動するように構成される。

【００２４】

第６の好ましい実施形態では、第１のメモリは書込み不可能である。

【００２５】

第２の態様では、本発明は、装置のブートコードを含むデジタルデータのデジタル署名、または別のデジタルデータを認証するために使用される第２段階の認証鍵を検証するための方法を対象とする。装置の電源を入れた、または装置をリセットしたとき、処理手段がデジタルデータおよびデジタル署名を受信し、検証鍵を取得すること、および取得した検証鍵を用いてデジタル署名を処理することによりデジタル署名を検証することによって、複数回、デジタル署名を検証する。複数回のそれぞれには、異なる検証鍵が取得され、使用される。

【００２６】

第１の好ましい実施形態では、取得するステップおよび検証するステップは、並行して行われる。

【００２７】

第２の好ましい実施形態では、取得するステップおよび検証するステップは、デジタル署名の検証に成功するまで、またはプロセッサが利用可能なすべての検証鍵を試して失敗するまで、繰り返して行われる。

【００２８】

次に、本発明の好ましい特徴について、非限定的な例として、添付の図面を参照して説明する。

【図面の簡単な説明】

【００２９】

【図１】本発明の好ましい実施形態に係る受信機を示す図である。

【図２】本発明の好ましい実施形態により、ソフトウェアまたは第２段階の認証鍵の署名の検証のための方法を示す図である。

【発明を実施するための形態】

【００３０】

本発明の主要な発明の概念は、複数の限定受信（ＣＡ）プロバイダから発信される署名を検証することができるように複数の認証鍵（ＰＵＡＫ）を格納するＣＡシステムの受信機を提供することである。この受信機は、好ましくはセットトップボックス（ＳＴＢ）であるが、テレビなど、他のいかなる好適な装置であることも可能である。

【００３１】

図１は、本発明の好ましい実施形態による受信機を示している。受信機１００は、セキ

ュアチップ（ｓｅｃｕｒｅｄ　ｃｈｉｐ）１０２と、第１の（好ましくは不揮発性）メモリ１０６とを備えている。図には本発明に必要とされる特徴のみを示していることを理解されたい。

【００３２】

第１のメモリ１０６は、好ましい実施形態ではソフトウェア（以下、一例として使用する）であり、有利には受信機がオンにされるときに、または受信機がリセットされるときに使用されるいわゆるブートコードである、デジタルデータ１０７と、ソフトウェアのデジタル署名１０８とを格納する。ソフトウェア１０７および署名１０８は、単一ファイルの一部であることが好ましい。またデジタルデータ１０７は、第２段階の認証鍵である場合もある。

【００３３】

効率の理由から、セキュアチップ１０２は、セキュリティプロセッサ１０３と、メインプロセッサ１０４とを備えることが好ましい。セキュリティプロセッサ１０３は、以下に説明するように、ソフトウェアの署名１０８を検証するように構成される。セキュアチップ１０２はさらに、第２のメモリ１０５、好ましくは複数の認証鍵（ＰＵＡＫ）を保持する書込み不可能な、すなわちリードオンリメモリ（ＲＯＭ）を備える。図１では、２つのＰＵＡＫ、すなわちＰＵＡＫ　ＡおよびＰＵＡＫ　Ｂのみがある。しかしながら、少なくともセキュアチップを使用することができるＣＡプロバイダと同数のＰＵＡＫを格納することが有利であることは理解されるであろう。一部のＣＡプロバイダは、そのソフトウェアに複数の署名を提供するために、複数の鍵を使用することができる。

【００３４】

セキュリティプロセッサ１０３には、署名１０８の検証にどのＰＵＡＫを使用すべきかがわからないので、これまでの説明の受信機１００は、複数のＣＡプロバイダに対応するには十分ではない。

【００３５】

図２は、本発明の好ましい実施形態によるソフトウェアの署名１０８の検証の方法を示している。

【００３６】

ステップＳ２１では、受信機は、オンにされ、またはリセットされ、受信機は、第１のメモリ１０６に格納された、認証されることになるソフトウェア１０７に注意を向けることを要求される。この時点の受信機は、どのエンティティがソフトウェアの署名１０８を提供したかがわからず、そのためどのＰＵＡＫを使用すべきかがわからないことを理解されるであろう。

【００３７】

セキュリティプロセッサ１０３は、セキュアチップ１０２の制御を行う（ステップＳ２２）。ソフトウェア１０７および署名１０８は、次に第１のメモリ１０６からセキュアチップ１０２へロードされる（ステップＳ２３）。

【００３８】

セキュリティプロセッサ１０３は次に、第２のメモリ１０５からＰＵＡＫをロードし（ステップＳ２４）、これを使用して署名１０８を検証する（ステップＳ２５）。

【００３９】

ステップＳ２６において検証が成功する、すなわち「Ｙ」の場合、次にソフトウェアコードはステップＳ２７において使用され、検証方法は終了する。

【００４０】

一方、ステップＳ２６において検証が成功しない、すなわち「Ｎ」の場合、さらなるＰＵＡＫ、すなわち署名１０８の検証に使用されていないＰＵＡＫがあるかどうかが検証される。

【００４１】

ステップＳ２８においてそれ以上署名がない、すなわち「Ｎ」の場合、検証は失敗し（ステップＳ２９）、このソフトウェアを検証することができないのでこれを使用すべきで

はなく、検証方法は終了する。ステップＳ２８において試されていない署名がある、すなわち「Ｙ」の場合、ステップＳ２５において第２のメモリから次のＰＵＡＫがロードされる。

【００４２】

検証方法が終了すると、セキュリティプロセッサ１０３は、セキュアチップの制御をメインプロセッサ１０４に戻すことができる。データが第２段階の認証鍵である場合、セキュアチップは、認証された第２段階の認証鍵を使用して、第２段階の認証を行うことができる。

【００４３】

言い換えれば、この方法は、格納されたＰＵＡＫ鍵を続けて（繰り返して）試して、ソフトウェアの署名を検証する。ＰＵＡＫが署名を検証する場合、ソフトウェアは検証に成功し、署名を検証するＰＵＡＫがない場合、ソフトウェアは検証に成功しない。

【００４４】

当業者は理解するであろうが、少なくとも２つのＰＵＡＫを並行して試すことも可能であり、重要な点は、１つのＰＵＡＫがソフトウェアの署名を検証する場合、ソフトウェアは検証に成功するということである。

【００４５】

したがって、本発明は、ソフトウェアの署名が複数の署名者のいずれかによって提供された可能性があるとき、受信機がソフトウェアの署名を検証する方法を提供することができるということが理解されるであろう。どの鍵を使用すべきかを知る方法はないと考えられていたので、これまでのシステムではこれは可能ではなかったこともまた理解されるであろう。したがって本発明は、これまで未解決の重要な技術的問題に斬新で驚くべき解決策を提供する。さらに、本発明は、使用されるＣＡシステムを識別できるようにすることもでき、次に受信機１００においてＣＡ特定機能の起動を可能にする。

【００４６】

この方法は、ソフトウェアコードの検証、または実際には内部メモリからダウンロードされるデジタルデータに、決して限定されないことを理解されるであろう。

【００４７】

この説明および（必要に応じて）特許請求の範囲および図面に開示する各特徴は、個々に、または任意の適切な組合せで提供されることが可能である。ハードウェアに実装されるように記載した特徴は、ソフトウェアに実装されることも可能であり、逆もまた同様である。特許請求の範囲に表示する参照符号は、説明のためにすぎず、特許請求の範囲への制限的効果はないものとする。

＜付記１＞

デジタルデータのデジタル署名を検証するための装置であって、

第１の検証鍵を格納するように構成された第１のメモリと、

デジタルデータを格納するように構成された第２のメモリであって、前記デジタルデータは、装置のブートコードまたは別のデジタルデータを認証するために使用されることになる第２段階の認証鍵を含む、第２のメモリと、

装置の電源を入れた、または装置をリセットしたとき、前記デジタルデータおよび前記デジタル署名を受信し、前記第１の検証鍵を用いて前記デジタル署名を処理することによって、前記デジタル署名を検証するように構成された処理手段と

を備え、

前記第１のメモリがさらに、第２の検証鍵も格納するように構成され、前記第１の検証鍵および前記第２の検証鍵はそれぞれ第１の署名エンティティの署名鍵および第２の署名エンティティの署名鍵に対応し、

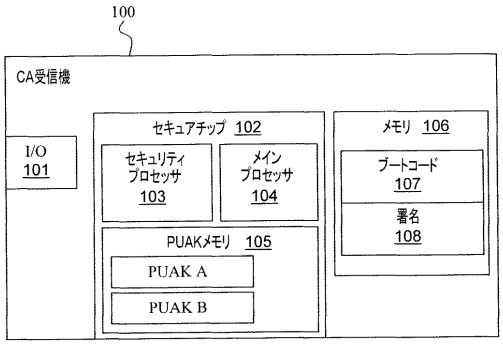
前記処理手段がさらに、前記第２の検証鍵を用いて前記デジタルデータを処理することによって前記デジタル署名を検証するように構成される

ことを特徴とする装置。

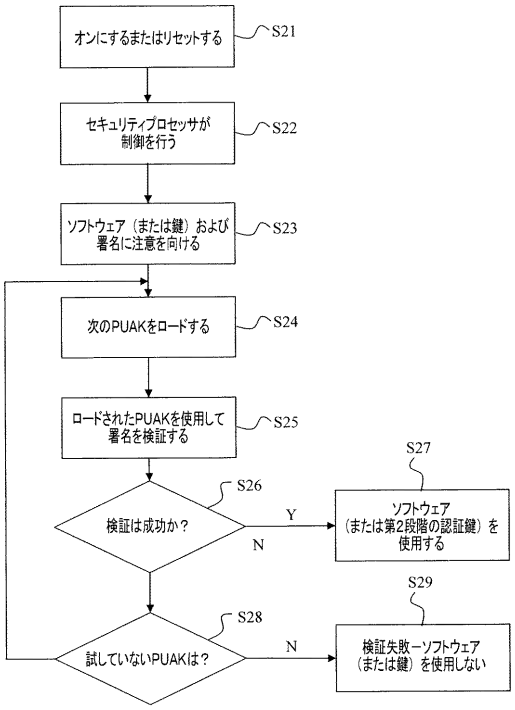
＜付記２＞

前記第１のメモリは、複数の検証鍵を格納するように構成されることを特徴とする付記１に記載の装置。
＜付記３＞
前記処理手段は、前記デジタル署名が検証に成功するまで、またはデジタル署名が格納されたすべての検証鍵を使用して不成功になるまで、前記デジタル署名および前記格納された検証鍵のそれぞれを使用して、前記デジタル署名を検証するように構成されることを特徴とする付記２に記載の装置。
＜付記４＞
前記処理手段は、前記第１の検証鍵を用いて前記デジタル署名が検証に成功しない場合、前記第２の検証鍵を用いて前記デジタル署名を処理することによって前記デジタル署名を検証するように構成されることを特徴とする付記１に記載の装置。
＜付記５＞
前記処理手段は、前記第１の検証鍵および前記第２の検証鍵を並行して使用して前記署名を検証するように構成されることを特徴とする付記１に記載の装置。
＜付記６＞
前記ブートコードが組み込まれることを特徴とする付記１に記載の装置。
＜付記７＞
前記デジタル署名が認証に成功した場合に前記ブートコードを実行するように構成された第２の処理手段をさらに備えることを特徴とする付記６に記載の装置。
＜付記８＞
前記処理手段はさらに、前記デジタルデータの検証に成功すると、現在のＣＡシステムを識別し、ＣＡ特定機能を起動するように構成されることを特徴とする付記１に記載の装置。
＜付記９＞
前記第１のメモリは書込み不可能であることを特徴とする付記１に記載の装置。
＜付記１０＞
装置のブートコードまたは別のデジタルデータを認証するために使用されることになる第２段階の認証鍵を含むデジタルデータのデジタル署名を検証するための方法であって、処理手段において、前記装置に電源を入れた、または前記装置をリセットしたとき、
前記デジタルデータおよび前記デジタル署名を受信するステップと、
検証鍵を取得し、
前記取得した検証鍵を用いて前記デジタル署名を処理することによって前記デジタル署名を検証すること
によって前記デジタル署名を複数回検証するステップと
を含み、
前記複数回のそれぞれに、異なる検証鍵が取得され、使用されることを特徴とする方法。
＜付記１１＞
前記取得するステップおよび前記検証するステップは、並行して行われることを特徴とする付記１０に記載の方法。
＜付記１２＞
前記取得するステップおよび前記検証するステップは、前記デジタル署名が検証に成功するまで、または前記プロセッサが利用可能なすべての検証鍵を試して不成功になるまで、繰り返して行われることを特徴とする付記１０に記載の方法。

【図１】


100
CA受信機
I/O
101
セキュアチップ 102
セキュリティ
プロセッサ
103
メイン
プロセッサ
104
PUAKメモリ 105
PUAK A
PUAK B
メモリ 106
ブートコード
107
署名
108

【図２】


オンにするまたはリセットする
S21
セキュリティプロセッサが
制御を行う
S22
ソフトウェア（または鍵）および
署名に注意を向ける
S23
次のPUAKをロードする
S24
ロードされたPUAKを使用して
署名を検証する
S25
S26
検証は成功か？
Y
N
S27
ソフトウェア
（または第2段階の認証鍵）を
使用する
S28
試していないPUAKは？
N
S29
検証失敗－ソフトウェア
（または鍵）を使用しない

フロントページの続き

(74)代理人 100134120
弁理士 内藤 和彦
(74)代理人 100108213
弁理士 阿部 豊隆
(72)発明者 ジャン－マリー シュタイヤー
フランス ３５５７６ セソン セヴィニェ シーエス １７６ １６ ゼットエーシー デ シャン ブラン アベニュー デ シャン ブラン ９７５ テクニカラー アールアンドディー フランス内
(72)発明者 ディディエ ルースタイド
フランス ３５５７６ セソン セヴィニェ シーエス １７６ １６ ゼットエーシー デ シャン ブラン アベニュー デ シャン ブラン ９７５ テクニカラー アールアンドディー フランス内

審査官 脇岡 剛

(56)参考文献 特開２００８－１７５６４８（ＪＰ，Ａ）
特表２００１－５１６５３２（ＪＰ，Ａ）
特開平０９－１２１３４０（ＪＰ，Ａ）
米国特許第０５６２５６９３（ＵＳ，Ａ）
特開２００９－２６７６０５（ＪＰ，Ａ）
特開２００４－３４３２７２（ＪＰ，Ａ）
特開２００５－１３６４７０（ＪＰ，Ａ）
特開２００１－０８４１４５（ＪＰ，Ａ）
米国特許出願公開第２００８／０１８９５３９（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／１０