(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4668619号
(P4668619)
(45)発行日　平成23年4月13日(2011.4.13)　(24)登録日　平成23年1月21日(2011.1.21)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601A
H04L 9/00 601E

請求項の数 16　(全 13 頁)

(21)出願番号　特願2004-546219(P2004-546219)
(86)(22)出願日　平成14年10月28日(2002.10.28)
(65)公表番号　特表2006-504309(P2006-504309A)
(43)公表日　平成18年2月2日(2006.2.2)
(86)国際出願番号　PCT/IB2002/004450
(87)国際公開番号　WO2004/038995
(87)国際公開日　平成16年5月6日(2004.5.6)
審査請求日　平成17年6月28日(2005.6.28)

前置審査

(73)特許権者　398012616
ノキア　コーポレイション
フィンランド　エフイーエンー０２１５０
エスプー　ケイララーデンティエ　４
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100108383
弁理士　下道　晶久
(74)代理人　100141162
弁理士　森　啓

最終頁に続く

(54)【発明の名称】装置鍵

(57)【特許請求の範囲】
【請求項１】
パーソナル装置（１００）固有の暗号鍵を管理するための方法において、前記方法は、前記パーソナル装置と通信するようになっている安全処理点（１５０）において実行され、
前記安全処理点は、
前記パーソナル装置（１００）内に含まれる集積回路チップ（１１０）の読み出し専用記憶装置（１２０）から一意のチップ識別子を取り出す段階と、
少なくとも１つの通信用暗号鍵を含むデータ・パッケージを前記パーソナル装置内に記憶する段階と、
前記データ・パッケージを記憶する段階に反応して、前記集積回路チップ（１１０）の改ざん防止機能のある秘密記憶装置（１２５）内に記憶された一意の秘密チップ鍵を用いて暗号化された前記データ・パッケージであるバックアップ・データ・パッケージを前記パーソナル装置（１００）から受信する段階と、
前記一意のチップ識別子を受信されたバックアップ・データ・パッケージに関連付ける段階と、
前記バックアップ・データ・パッケージ及び関連付けられた一意のチップ識別子を常設公開データベース（１７０）内に記憶する段階と、
を実行し、更に
一意の装置ＩＤを前記一意のチップ識別子に関連付ける段階と、

前記パーソナル装置の読み出し専用記憶装置内に記憶された製造者の公開署名鍵に対応する製造者の個人署名鍵を用いて前記関連付ける段階の結果に署名して、それにより、前記一意の装置ＩＤに対する証明書を生成する段階と、
前記証明書を前記パーソナル装置内に記憶する段階と、
前記バックアップ・データ・パッケージ及び前記一意のチップ識別子に関連して前記一意の装置ＩＤ及び前記証明書を前記常設公開データベース内に記憶する段階と、
を実行することを特徴とする方法。
【請求項２】
前記少なくとも１つの通信用暗号鍵は、パーソナル装置製造者と前記パーソナル装置との間の通信用暗号鍵を用いる安全な通信チャンネルに対して用いられる少なくとも１つの鍵を含む請求項１に記載の方法。
【請求項３】
前記通信用暗号鍵を用いる安全な通信チャンネルに対して用いられる少なくとも１つの鍵は、対称鍵を含む請求項２に記載の方法。
【請求項４】
前記対称鍵は、マスター鍵及び前記一意の装置ＩＤの関数として生成される請求項３に記載の方法。
【請求項５】
前記通信用暗号鍵を用いる安全な通信チャンネルに対して用いられる少なくとも１つの鍵は、個人／公開鍵対を含む請求項２乃至４のいずれか一項に記載の方法。
【請求項６】
前記個人／公開鍵対は、
前記パーソナル装置の組み立て過程で前記安全処理点によって生成されるか、又は、
前記パーソナル装置の組み立て以前に安全データベース（１４０）内にあらかじめ生成され記憶されるか、のいずれかであり、
後者の場合において、組み立て以前に記憶された前記個人／公開鍵対は、前記バックアップ・データ・パッケージの受信後に前記安全データベースから除去される請求項５に記載の方法。
【請求項７】
前記パーソナル装置は無線通信端末であり、前記一意の装置ＩＤは、無線通信ネットワーク内で前記無線通信端末を識別する識別子である請求項１乃至６のいずれか一項に記載の方法。
【請求項８】
パーソナル装置固有の暗号鍵を管理するためのシステムにおいて、前記システムは、少なくとも１つのパーソナル装置（１００）及び前記パーソナル装置と通信するようになっている安全処理点（１５０）を含み、
前記パーソナル装置は、読み出し専用記憶装置（１２０）内の一意のチップ識別子及び改ざん防止機能のある記憶装置（１２５）内の一意の秘密チップ鍵を有する集積回路チップ（１１０）を含み、
前記安全処理点は、前記一意のチップ識別子を取り出して、少なくとも１つの通信用暗号鍵を含むデータ・パッケージを前記パーソナル装置内に記憶するための処理手段（１５５）を含み、
前記パーソナル装置は、前記一意の秘密チップ鍵を用いて受信されたデータ・パッケージを暗号化して、その結果得られるバックアップ・データ・パッケージを前記安全処理点に返送するための処理手段（１２７）を含み、
前記安全処理点の処理手段（１５５）は、常設公開データベース（１７０）内の前記一意のチップ識別子に関連して前記受信されたバックアップ・データ・パッケージを記憶するようになっており、
前記安全処理点の処理手段は更に、
一意の装置ＩＤを前記一意のチップ識別子に関連付け、

前記パーソナル装置の読み出し専用記憶装置内に記憶された製造者の公開署名鍵に対応する製造者の個人署名鍵を用いて関連付けの結果に署名して、それにより、前記一意の装置ＩＤに対する証明書を生成し、
前記パーソナル装置内に前記証明書を記憶し、
前記バックアップ・データ・パッケージ及び前記一意のチップ識別子に関連して前記一意の装置ＩＤ及び前記証明書を前記常設公開データベース内に記憶する
ようになっていることを特徴とするシステム。
【請求項９】
前記少なくとも１つの通信用暗号鍵は、パーソナル装置製造者と前記パーソナル装置との間の通信用暗号鍵を用いる安全な通信チャンネルに対して用いられる少なくとも１つの鍵を含む請求項８に記載のシステム。
【請求項１０】
前記通信用暗号鍵を用いる安全な通信チャンネルに対して用いられる少なくとも１つの鍵は、対称鍵を含む請求項９に記載のシステム。
【請求項１１】
前記対称鍵は、マスター鍵及び前記一意の装置ＩＤの関数として生成される請求項１０に記載のシステム。
【請求項１２】
前記通信用暗号鍵を用いる安全な通信チャンネルに対して用いられる少なくとも１つの鍵は、個人／公開鍵対を含む請求項９乃至１１のいずれか一項に記載のシステム。
【請求項１３】
前記安全処理点の処理手段は、
前記パーソナル装置の組み立て過程で前記個人／公開鍵対を生成するようになっているか、又は、
前記鍵対が前記パーソナル装置の組み立て以前にあらかじめ記憶されている安全データベース（１４０）から前記個人／公開鍵対を取り出すようになっているか、のいずれかであり、
後者の場合において、前記安全処理点は更に、前記バックアップ・データ・パッケージの受信後に前記安全データベースから前記個人／公開鍵対を除去するためにようになっている請求項１２に記載のシステム。
【請求項１４】
前記パーソナル装置は無線通信端末であり、前記一意の装置ＩＤは、無線通信ネットワーク内で前記無線通信端末を識別する識別子である請求項８乃至１３のいずれか一項に記載のシステム。
【請求項１５】
請求項１乃至７のいずれか一項に従って組み立てられ記憶された、パーソナル装置（１００）のバックアップ・データ・パッケージを復元する方法であって、
前記パーソナル装置（１００）の読み出し専用記憶装置（１２０）から一意のチップ識別子を読み出す段階と、
前記チップ識別子を公開データベース（１７０）に送信する段階と、
送信されたチップ識別子に対応する前記バックアップ・データ・パッケージを前記公開データベースから受信する段階と、
受信されたバックアップ・データ・パッケージを前記パーソナル装置内に記憶する段階と、
を含む方法。
【請求項１６】
パーソナル装置（１００）固有の暗号鍵を管理するための、該パーソナル装置（１００）と通信することができる安全処理点（１５０）であって、
前記パーソナル装置（１００）に含まれる集積回路チップ（１１０）の読み出し専用記憶装置（１２０）から一意のチップ識別子を取り出し、

少なくとも１つの通信用暗号鍵を含むデータ・パッケージを前記パーソナル装置内に記憶し、
記憶されたデータ・パッケージに反応して、バックアップ・データ・パッケージの形態での前記データ・パッケージの暗号化版を、前記パーソナル装置から受信し、
前記一意のチップ識別子に関連して受信されたバックアップ・データ・パッケージを常設公開データベース（１７０）内に記憶し、更に、
一意の装置ＩＤを前記一意のチップ識別子に関連付け、
前記パーソナル装置の読み出し専用記憶装置内に記憶された製造者の公開署名鍵に対応する製造者の個人署名鍵を用いて関連付けの結果に署名して、それにより、前記一意の装置ＩＤに対する証明書を生成し、
前記パーソナル装置内に前記証明書を記憶し、
前記バックアップ・データ・パッケージ及び前記一意のチップ識別子に関連して前記一意の装置ＩＤ及び前記証明書を前記常設公開データベース内に記憶するようになっている処理手段（１５５）を含むことを特徴とする安全処理点。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、パーソナル装置内に含まれるアプリケーションによって用いられるように意図された、暗号鍵の鍵管理に関する。

【背景技術】

【０００２】

携帯電話及び携帯型ＰＤＡ（携帯情報端末）のようなパーソナル装置の利用は、次第に普及しつつある。何らかの形でエンド・ユーザＩＤと関連するか、又は無名のユーザを有する、端末ＩＤを有するあらゆる移動体通信端末を含む、別の種類のパーソナル装置は、容易に考えられる。パーソナル装置のエンド・ユーザ及びこの装置を用いて通信する団体の間には、暗号化通信、デジタル署名、及びデジタル証明書を用いることができるための要請が存在する。この種の暗号技術を用いると、通信される情報データのセキュリティ及び完全性を保証すること、情報の発信元を認証すること、並びに意図された情報の受信者を認証することが可能となる。

【０００３】

２つの団体の間の暗号化通信は、通常、共有秘密鍵又は公開／個人鍵対のいずれかに基づいている。鍵ベースの暗号化通信及び／又はデジタル署名の利用を実施するためには、いかにしてどこで要求される鍵を生成するか、及び関連する団体に生成された鍵を配信する方法を決定するための方法が必要である。鍵の生成、記憶、及び配信に関する課題を含み、この文献において用いられる、より一般的な用語は、鍵管理である。

【０００４】

秘密鍵は、明らかに、参加する団体の間で、管理され、何らかの形で配信される必要がある。秘密鍵又は個人鍵を或る団体に送信する必要がある場合には、第３者が鍵にアクセスしようと最大限の努力を払ったとしても、鍵が第３者に暴露されないように安全な方法でこれを実行することが重要である。公開／個人鍵対は、或る団体内で生成することができ、公開鍵のみを団体外に配信する必要があるということが要請される。しかしながら、公開／個人鍵対が特定の団体外で生成される場合には、個人鍵を団体に送信する必要がある。秘密鍵又は個人鍵を送信する場合はいつでも、鍵の完全性を保証することができることも重要である。

【０００５】

将来のパーソナル装置は、１つ以上の装置固有の暗号鍵を含むことになろう。これらの鍵の個数及び種類は、装置に含まれる様々なアプリケーションに依存し、アプリケーションは、異なるユーザ間及びユーザそれぞれの装置の使用法の間で異なることになろう。従って、装置に含むべき鍵の個数及び種類を予測することは困難である。この理由から、装置を初期化する際に、装置の記憶領域に様々な鍵を記憶できる必要がある。通常、これら

の鍵の大半は、或る堅牢でないメモリ、すなわち、情報を書くことができ、メモリ内に情報を保持するために用いられる機構の故障により、任意のかかる情報を失う潜在的な危険性を有するあらゆるメモリ、に記憶されることになろう。結果として、元々記憶されていた鍵の紛失につながる装置の故障の場合には、装置内のこの元の鍵を復元できることが望ましい。装置内に再記憶するためにあらゆる秘密鍵又は個人鍵を送信する際には、先に述べたように、送信される鍵のセキュリティ及び完全性を保持することが、通常、要請される。

【０００６】

インタートラストに付与された米国特許第５，８９２，９００号は、特に、暗号鍵管理に対してセキュリティを与えるための暗号鍵の利用を開示している。この文献には、処理タスクを実行し、安全な方法で外部団体と通信するように設計された「保護処理環境」（ＰＰＥ）を有する「安全処理装置」（ＳＰＵ）が記載されている。ＰＰＥは、製造者及びＰＰＥ自身によって生成された鍵を用いて初期化される鍵の記憶装置を含む。公開鍵ベースであるか又は共有鍵に基づく製造鍵は、安全な方法で別の鍵を通信するためのいわゆるマスター鍵として用いられる。製造鍵は、製造時にＰＰＥに配線接続されるか、又はその第１の鍵としてＰＰＥに送信されるかのいずれかである。製造鍵は、公開／個人鍵対及び／又は秘密共有鍵のような、ＰＰＥ内にダウンロードされる様々な別の鍵を保護するために用いられる。それとは別に、ＰＰＥは、内部にそれ自身の鍵対を生成する機能を有し、この場合には、製造鍵は、必要とされなくてもよい。

【０００７】

ダウンロード認証鍵の利用も、米国特許第５，８９２，９００号に開示されている。ダウンロード認証鍵は、初期化ダウンロード過程においてＰＰＥによって受信される。それは、ＰＰＥが機能しなくなった場合にＰＰＥの管理者による復元を可能とすべく、ＰＰＥ鍵の更新を認証するために、及びＰＰＥ外部の安全なデータベース・バックアップを保護するために、用いられる。この文献は、バックアップ鍵の利用も開示している。バックアップ鍵は、ＰＰＥ内で生成され記憶される。ＰＰＥ外部の安全なデータベースは、バックアップ鍵を用いて暗号化されたバックアップ記録を記憶している。バックアップ鍵は、ダウンロード認証鍵を用いて暗号化され、ＰＰＥの障害の際に管理者がバックアップを復号化して復元することができるようにバックアップ自信内に記憶されてもよい。

【発明の開示】

【０００８】

本発明の要約

本発明の目的は、パーソナル装置固有の暗号鍵を管理するための、オーバーヘッドの少ない、方法及びシステムを提供することである。

【０００９】

本発明の別の目的は、管理に対する米国特許第５，８９２，９００号の教示と比較して、より簡略的でかつ改善されたセキュリティを有する、装置固有の暗号鍵の管理に対する技術を提供することである。

【００１０】

本発明によれば、これらの目的は、独立請求項１に従う方法、独立請求項９に従うシステム、及び請求項１８に従うパーソナル装置によって達成される。望ましい実施形態は、従属請求項において規定される。

【００１１】

本発明によれば、装置固有の暗号鍵をパーソナル装置内に記憶するために、装置の組み立てラインの安全処理点からパーソナル装置に、１つ以上の暗号鍵を含むデータ・パッケージを送信する。送信されたデータ・パッケージに反応して、安全処理点は、パーソナル装置からバックアップ・データ・パッケージを受信する。このバックアップ・データ・パッケージは、パーソナル装置内に含まれる、改ざん防止機能のあるチップの秘密記憶装置内に記憶された独自の秘密チップ鍵を用いて暗号化されたデータ・パッケージである。安全処理点は、独自のチップ識別子をチップから取り出し、その識別子をバックアップ・デ

ータ・パッケージに関連付ける。その後、例えばインターネットに接続された常設の大域的公開データベース内に、関連付けられた独自のチップ識別子と共に、バックアップ・データ・パッケージを記憶する。

【００１２】

背景の節で前に説明したように、暗号鍵は、通常、装置の、例えばフラッシュ・メモリ等の、書替え可能な堅牢でないメモリ内に、記憶される。このメモリ内の情報が失われるか又は破損した場合には、その内容は、バックアップ・データ・パッケージを用いて復元する必要がある。本発明を用いると、バックアップ・データ・パッケージを復号化するのに用いられる鍵を記憶する、いかなる秘密データベースも保持する必要がなくなる。その代わり、チップ識別子によってバックアップ・データ・パッケージが関連付けられている特定の装置は、暗号鍵を復元するために独自の秘密チップ鍵を用いて、受信されたバックアップ・データ・パッケージを復号化することができる。

【００１３】

装置製造者もあらゆる装置管理者も、バックアップ・データ・パッケージを復号化するための鍵を記憶する秘密データベースを保持する必要はない。実際には、セキュリティの理由から、チップ製造において、独自の秘密チップ鍵のいかなるコピーも記憶又は配信しないことが望ましい。この独自の秘密チップ鍵は、改ざん防止機能のある記憶装置から決して出てこない。装置製造者を含む、いかなる他の団体も、この鍵を修得しない。改善されたセキュリティを可能とすることと並んで、これはまた、鍵の管理を非常に簡略化する。

【００１４】

公開データベース内にバックアップ・データ・パッケージを記憶することによって、鍵の管理は、更に簡略化され、高価ではなくなる。更に、これによって、装置製造者だけではなく、装置所有者又は装置管理者のような、装置を管理するあらゆる者は、完全に自分自身で、装置の元の暗号鍵を復元することができる。

【００１５】

装置内に記憶された配信されない独自の秘密チップ鍵を用いる、装置内のバックアップ・データ・パッケージの暗号化及び復号化は、送信中及び公開データベースにおける記憶中の両方の場合に、バックアップ・データ・パッケージの内容の保護及び完全性を提供する。理解されるように、データ・パッケージは、例えば、ＤＲＭ（デジタル権利管理）、無線端末を実現するパーソナル装置のＳＩＭ（加入者識別モジュール）ロッキングに関連する鍵、パーソナル装置と装置製造者との間における安全な鍵ベースの通信チャンネルの準備等の、様々な目的に対するあらゆる種類の暗号鍵を含むことができる。更に、あらゆる他の種類の秘密の、装置固有の情報は、データ・パッケージ内に含めて、それにより、暗号鍵と同じ方法で独自の秘密チップ鍵によって保護することもできる。従って、公開データベース内に記憶されたバックアップ・データ・パッケージ内に含まれる情報は、暗号鍵並びにその他の秘密の、装置固有のデータに関連することができる。

【００１６】

有利なことに、バックアップ・データ・パッケージは、装置製造者と装置との間における安全な鍵ベースの通信に対する１つ以上の通信鍵を含む。このことは、かかる安全な通信チャンネルの確立と復元が保護されて完全性を備えることを意味する。すなわち、例えば、装置が盗まれるか、又は装置の悪意のある所有者によって別の消費市場で再販売されることになる場合等に、組み立て過程で規定された、この安全なチャンネルの暗号化／復号化を逃れるように、装置に対する安全なチャンネルの通信鍵を、外部の団体は、改ざんできないことになる。このことは、製造者とパーソナル装置との間における通信に対する安全なチャンネルを保証し、この通信は、装置の組み立て過程及びパーソナル装置が顧客へ出荷された後のいずれの場合においても、いかなる装置所有者又は第３者によっても改ざんされ得ない。

【００１７】

望ましくは、特定の装置に関連付けられた独自の装置ＩＤに対する証明書は、対応する

バックアップ・データ・パッケージに関連して、記憶される。このことが有する利点として、独自の装置ＩＤは、パーソナル装置の復元過程において真の装置ＩＤとして、装置のＲＯＭメモリ内に記憶される公開署名検証鍵によって、検証することができる点が挙げられる。

【００１８】

有利なことに、データ・パッケージ内の１つ以上の暗号鍵は、装置とその製造者との間におけるあらゆる後続の安全な通信に必要な対称鍵及び／又は公開／個人鍵を含み、暗号鍵対及び署名鍵対のような別の通信目的に対するその他の暗号鍵を除外しない。

【００１９】

データ・パッケージ内の鍵は、外部の源から安全処理点に提供されるか又は安全処理点自身によって生成されるかのいずれかである。これは、製造者との通信に対して用いられる暗号鍵の装置内に決定論的生成が存在しないことを意味する。このことは、暗号鍵及びアルゴリズムの種類に関して、例えば安全な通信チャンネルに対して選択すべき実行を決定するに際して、柔軟性を与える。更に、かかる安全な通信チャンネルに対する鍵及びアルゴリズムは、必要な場合には、基本的製造／組み立て工程を変更する必要なく、変更することができる。

【００２０】

更に、装置における内部での公開鍵の生成を最小化するか又は完全に回避することによって、装置内における計算を最小化する。この減少されたオーバーヘッドは、より小さい遅延及び組み立てラインにおける装置のより速い組み立てを与える。

【００２１】

このように、本発明は、装置固有の暗号鍵をパーソナル装置に割り当てること並びに装置の組み立て及び出荷後にこの暗号鍵を管理することの両者に対するオーバーヘッドを簡略化し減少させる。

【００２２】

更に、本発明の特徴及び利点は、以下の詳細な説明から、より容易に明らかとなろう。

【００２３】

添付の図面を参照して、非常に詳細に本発明の実施形態の例示を記載する。ここで、いくつかの図面に現れる同じ機能は、同じ参照符号を用いて表示される。

【００２４】

望ましい実施形態の詳細な説明

図１を参照して、非常に詳細に本発明の実施形態の例示をここに記載する。装置製造者における組み立てによって決まるパーソナル装置１００を同図に示す。製造者は、装置と通信するように準備された安全処理点１５０によって、装置の組み立てを制御する。装置と通信するための方法及び手段は、当業者には公知であって、問題の種類の装置に適した、あらゆる技術に基づくことができる。当業者には理解できることであるが、装置の組み立ては、Ｉ／Ｏドライバ及び通信ポート（図示せず）を導入するための装置のインターフェース回路によって用いられる通信プロトコルのような、様々な基本的ソフトウェア・モジュールを装置のメモリにロードすることを含む。それとは別に、かかるＩ／Ｏドライバは、装置に含まれるＲＯＭメモリ（図示せず）に、あらかじめ記憶しておくこともできる。安全処理点１５０は、装置の通信ポートによって用いられる通信プロトコルと互換性のある対応する通信ソフトウェアを含み、それにより、安全処理点１５０とパーソナル装置１００との間における通信を容易にする。

【００２５】

パーソナル装置１００の実現は、メモリ回路、処理回路、インターフェース回路等のような、パーソナル装置が動作可能となるのに必要な全ての種類の回路を含むハードウェア・プラットフォームに基づいている。本発明に関して重要なことであるが、装置１００は、集積チップ１１０を含み、このチップは、読み出し専用記憶領域１２０及び改ざん防止機能のある秘密記憶装置１２５を含む。このチップは、これらの２つの記憶領域がチップ内に備わるという条件に従う、あらゆる技術の状態を用いて、設計することができる。こ

の装置は、例えば情報を書くことができるフラッシュ・メモリで実現される、通常の安全でないメモリを提供するメモリ回路１３０も含む。更に、この装置は、データ・パッケージ、すなわち、改ざん防止機能のある秘密記憶１２５に記憶された独自の秘密チップ鍵を用いた、安全処理点からのデータの収集を規定するパッケージ、において受信されるデータを暗号化するための手段１２７を含む。受信したデータ・パッケージを暗号化するためのこの手段は、装置のメモリ内にロードされてあったプログラム命令を実行する、マイクロプロセッサ又は１つ以上の特定用途向け集積回路のような、あらゆる適切な処理ハードウェア手段によって実現される。この実行によって、処理ハードウェアは、公知の技術に従ってデータの対称暗号化を実行することができる。結果として、このプログラム命令の設計を、プログラミング技術に熟練した人は、理解することになろう。

【００２６】

安全処理点１５０は、例えば、装置との通信を制御するための及び装置に関する或る機能を実行するための汎用コンピュータの実装による、処理手段１５５を含む。処理手段１５５はまた、様々なデータベース１４０、１６０、及び１７０との通信を容易にし、これらのデータベースに安全処理点１５０は、動作可能に接続される。処理手段１５５は、適切なプログラム命令を実行することにより、本発明に従って動作すべく、安全処理点１５０を制御する。このプログラム命令の設計を、プログラミング技術に熟練した人は、以下で説明する本発明の動作に関する記載を学習した後で、理解することになろう。

【００２７】

一時的安全データベース１４０は、本発明の第１の実施形態において用いられる独自の装置ＩＤのための記憶装置として、与えられる。記憶されるＩＤの種類は、組み立てによって決まる装置の種類に依存する。装置が、例えば、ＧＳＭ（グローバル・システム・フォー・モバイル・コミュニケーションズ）ネットワークにおける移動局として、又はＵＭＴＳ（ユニバーサル・モバイル・テレコミュニケーション・システム）ネットワークにおけるユーザ機器として、無線通信ネットワークにおいて用いられる無線通信端末である場合には、独自の装置ＩＤは、携帯電話の機体識別番号（ＩＭＥＩ）に対応することになる。安全データベース１４０は、前もって、すなわち、対称鍵又は個人／公開鍵対がデータ・パッケージによって記憶されることになる装置を組み立てる前に、導き出された対称鍵又は個人／公開鍵対に対する記憶装置としても、与えられる。上述のように、データベース１４０は、一時的である。装置に関してこのデータベースから情報が取り出された後は、この情報は、データベースから消去される。

【００２８】

図１に示したシステムは、安全処理点から受信したバックアップ・データ・パッケージを記憶するための常設公開データベース１７０も含む。このバックアップ・データ・パッケージは、各装置が暗号化したデータ・パッケージを構成する。更に、このシステムは、随意的な秘密データベース１６０も含む。秘密データベース１６０は、製造者に属しており、秘密データベース１６０内に、製造者は、組み立てられた装置の或る装置固有データを記憶することができる。

【００２９】

再び、図１を参照し、このシステムの動作の例示形態及びそれに含まれる本発明の実施形態をここで記載する。この記載は、特に、記載された実施形態に従って暗号鍵を管理するために実行される動作を強調し、この動作を、段階的に記載する。様々な段階に含まれる要素の相互作用及びデータ・フローを説明するために、段階に対応する数字を有する矢印を図に含めた。

【００３０】

最初に段階１において、矢印１で示したように、装置製造者は、パーソナル装置が基づいているハードウェアを、かかるハードウェアを生産する工場から受け取る。先に説明したように、このハードウェアは、その読み出し専用記憶領域１２０及び改ざん防止機能のある秘密記憶装置１２５を有する集積チップ１１０、及びメモリ回路１３０を含む。装置の組み立ては、矢印２で示したように、装置内の様々な基本的実行可能ソフトウェア・モ

ジュールを、安全処理点１５０からダウンロードすることによって、段階２において開始する。それとは別に、或いはそれに加えて、或る基本的ソフトウェア・モジュールを、装置に含まれるＲＯＭメモリ内にあらかじめ記憶しておいてもよい。特に、データ・パッケージを暗号化するための手段を実現すべく動作する装置の処理手段１２７を制御するためのプログラム命令を、メモリ回路１３０内に記憶する。記憶された命令は、受信したバックアップ・データ・パッケージを復号化するための命令も含む。

【００３１】

段階３において、独自の装置ＩＤを、安全処理点１５０は、多数の独自の装置ＩＤを記憶しているデータベース１４０から読み出すことができる。更なる選択肢として、この段階は、前もって生成されるか又は計算された対称鍵又は１つ以上の個人／公開鍵対を読み出すことを含むこともできる。

【００３２】

段階４において、安全処理点１５０は、そのときは組み立ての段階にある、装置１００に含まれる集積チップ１１０の読み出し専用記憶領域１２０から、独自のチップ識別子を読み出す。次いで、安全処理点は、問題の装置１００内に記憶することになるデータ・パッケージを組み立てる。例えば、パーソナル装置１００とパーソナル装置製造者との間で、それらの間に目的として適切に確立された通信チャンネルを介した、将来の安全な鍵ベースの通信を可能とすべく、このデータ・パッケージは、少なくとも１つの暗号鍵を含む必要がある。

【００３３】

例えば、将来の安全な通信チャンネルと関連する、少なくとも１つの暗号鍵は、対称鍵又は公開／個人鍵対のいずれかとすることができる。前述したように、鍵又は鍵対は、安全データベース１４０によって実現される外部の源から与えられるか、又は随意的に安全処理点自身によって生成されるか、のいずれかとすることができる。

【００３４】

対称鍵を用いる場合には、安全処理点は、単一の秘密マスター鍵及び独自の装置ＩＤの関数としてこの鍵を生成することができる。対称鍵を各独自の装置ＩＤから導出することによって、組立工程中においても、安全な通信チャンネルを介して組み立てられた装置と通信する間に対称鍵が用いられた後においても、秘密データベースにおける全ての装置に対して全ての対称鍵を記憶する必要はなくなる。秘密に記憶する必要の或る唯一の鍵は、全ての対称鍵に対して共通なマスター鍵である。

【００３５】

公開／個人鍵対を用いる場合には、前述したように、装置の外部でのこの対の生成は、組立工程を速める。安全処理点における鍵対の任意の生成は、公知の技術に従って実行されることになる。この鍵対及び鍵対の公開鍵に対する証明書が、前もって計算され、安全データベース１４０として実現される外部の源によって与えられる場合には、装置組み立ての速度は、更に速くなるであろう。当業者には明らかとなるように、証明書のための個人鍵及び公開鍵は、データ・パッケージ内にそれらを組み込むことによって、装置内に記憶される。次いで、個人鍵に対応する公開鍵及びその証明書は、なんら特定のセキュリティ対策を取ることなしに、データベース１７０のようなデータベース内に記憶することができる。この記憶操作の後で、生成された鍵及び証明書情報は、データベース１４０から除去される。このように、公開／個人鍵対に対するあらゆるオンライン秘密データベースの必要性は、回避されることになる。安全処理点によって生成される対称鍵を用いることと比較して、鍵対の利用は、対称鍵を導出するマスター鍵を秘密に記憶する必要性を回避することになる。

【００３６】

段階５において、少なくとも対称鍵又は公開／個人鍵対を含むデータ・パッケージは、装置による暗号化によって決まり、装置１００のメモリ回路１３０内にロードされる。データ・パッケージを受信すると、装置の処理手段１２７は、受信したデータ・パッケージの一部又は全内容を暗号化するために、秘密記憶装置１２５からの独自の秘密チップ鍵を

用いることになる。暗号化は、公知の技術に従って設計された適切なプログラム命令を実行することによって、行われる。このプログラム命令は、（段階２において）装置内にあらかじめロードされている。

【００３７】

段階６において、安全処理点は、装置からバックアップ・データ・パッケージを受信する。このバックアップ・データ・パッケージは、装置の独自の秘密チップ鍵を用いて暗号化されたデータ・パッケージの内容に等しい。装置が将来において受信時にバックアップ・データ・パッケージを通常のデータ・パッケージと区別することができるようにするために、安全処理点は、ここで、バックアップ・データ・パッケージにバックアップ・コードを加えることができる。それとは別に、かかるコードは、装置自身によってバックアップ・データ・パッケージに加えることができる。もちろん、この区別機構を実現する別の方法は、当業者によって理解されよう。安全処理点は、段階４で取り出された独自のチップ識別子を受信したバックアップ・データ・パッケージに関連付ける。

【００３８】

本発明の実施形態によれば、各装置は、対応する独自の装置ＩＤを有する。更に、この独自の装置ＩＤは、独自の装置ＩＤに対する証明書と共に装置内に記憶する必要がある。先に述べたように、安全処理点１５０は、この場合には、（段階３において）安全データベース１４０から独自の装置ＩＤを取り出す。更に、上記段階４は、例えば取り出された独自の装置ＩＤと取り出された独自のチップ識別子の連結を実行することによって、これら２つを関連付けることを含むことになる。この場合、連結の結果は、製造者の個人署名鍵を用いて、署名される。この個人署名鍵は、製造者の公開署名鍵に対応する。この公開鍵は、例えば上記段階２において、装置の読み出し専用メモリ内に記憶されている。結果として生じる独自の装置ＩＤに対する証明書は、上記段階５において、装置のフラッシュ・メモリ内に記憶される。段階６において、独自のチップ識別子の受信したバックアップ・パッケージへの関連付けは、独自の装置ＩＤとその生成された証明書の関連付けも含む。

【００３９】

段階７において、様々な装置固有のデータは、製造者によって管理されるデータベース１６０内に記憶することができる。このデータベース１６０のセキュリティ・レベルは、そこに記憶されるデータの種類に依存する。通常、そこに含まれるデータは、装置に関して第３者に様々なサービスを提供する際に用いられるデータであり、このデータは、セキュリティの中程度のレベルしか要求しない。しかしながら、このデータベースは、例えば、対称鍵の生成のために対称鍵又はマスター秘密鍵を記憶するために、高度なセキュリティのデータベースが要求される場合には、高度なセキュリティを有するオンライン秘密データベースを構成することになる。

【００４０】

段階８において、バックアップ・データ・パッケージ及び関連付けられた独自のチップ識別子、及び証明書を伴うあらゆる関連付けられた独自の装置ＩＤは、常設公開データベース１７０内に、安全処理点１５０によって記憶される。このデータベースは、例えばインターネットを介して第３者にアクセス可能である。従って、装置が組み立てられて出荷された後で、第３者は、例えば装置の独自のチップ識別子を用いて、装置のバックアップ・データ・パッケージを取り出すことができる。バックアップ・データ・パッケージは、装置に関連付けられた特定のデータを復元するために用いられるので、バックアップ・データ・パッケージは、装置の正当な所有者でない第３者には、有用とはならないことになる。安全な通信チャンネルに関連する公開／個人鍵対の公開鍵は、第３者にアクセス可能となるように、公開データベース内に記憶することができるということに着目されたい。この場合には、安全通信チャンネルは、装置と製造者との間だけでなく、あらゆる団体と装置との間のチャンネルとすることになる。

【００４１】

組立工程の段階８の後で、装置は、矢印９で示される出荷のために準備される。

【００４２】
図２を参照し、出荷後の組み立てられた装置に関して実行することのできる可能な装置管理活動のいくつかの例を記載する。
【００４３】
図２は、図１を参照して前述したデータベース１６０及び１７０を含む。データベース１７０は、バックアップ・データ・パッケージを記憶する公開データベースであり、データベース１６０は、様々な装置固有の秘密データを記憶する随意的な秘密データベースである。装置１００は、出荷後に、所有者の制御下にある、図１で組み立てられた装置に相当する。公開データベース１７０に動作可能に接続された第３者のアプリケーション・サーバ１８０、及び装置製造者によって操作され、装置固有のデータを有するデータベース１６０及び１７０に動作可能に接続された装置サービス・サーバ１９０も、同図は示す。
【００４４】
ここで、装置のメモリ回路１３０が、何らかの理由で、その内容を失うと仮定する。これは、組み立ての過程で装置内に記憶された全ての暗号鍵が失われることを意味する。例えばインターネット等を介して公開データベース１７０と相互作用する第３者のアプリケーション・サーバによって、パーソナル装置の所有者は、サービス点及び／又は秘密データベースといかなる相互作用もせずに、失われたデータの或るものをフラッシュ・メモリ内に復元することができる。
【００４５】
不可欠なフラッシュ・メモリのデータの復元は、まず、独自のチップ識別子をパーソナル装置１００の読み出し専用記憶装置１２０から読み出すことによって達成される。次いで、チップ識別子は、公開データベース１７０を内蔵するオンライン・システムに送信される。オンライン・システムは、いかなる秘密情報にアクセスする必要もなく、対応するバックアップ・データ・パッケージ及び独自の装置ＩＤに対する証明書を返送する。次いで、所有者は、バックアップ・データ・パッケージ及び証明書の受信したコピーを用いて、新しいフラッシュ・イメージを生成することができる。次に装置１００が起動されると、装置は、受信したバックアップ・データ・パッケージに付随するバックアップ・コードを認識し、製造者が装置の組み立て過程でフラッシュ・メモリ内に元々記憶させたデータ・パッケージに等しいデータ・パッケージへと、バックアップ・データ・パッケージを復号化し始める。更に、フラッシュの内容の復元は、装置に割り当てられた独自の装置ＩＤの復元も含む。誰しも復元中にこの装置ＩＤを変更可能であってはならず、製造者が元々記憶させたＩＤと同じである必要がある。このことを確実にするために、装置は、証明書を検証し装置ＩＤの信憑性を検証すべく、装置のＲＯＭメモリ内に記憶された製造者の公開署名鍵を用いる。このように、この操作は、製造者からのいかなる相互作用もなく実行される。この検証が成功する場合には、暗号鍵及び独自の装置ＩＤ、場合によっては、製造者が組み立て過程で装置に関連付けた何らかの別のデータが、メモリ回路１３０内に完全に復元されることになる。
【００４６】
装置の所有者が、例えば新しいソフトウェア・モジュールのダウンロード等の、製造者からのサービスを要求する場合には、所有者は、製造者の提供する装置サービス・サーバ１９０にアクセスする。このアクセスは、装置の独自の装置ＩＤをサーバに送信することを含む。このとき、製造者のサーバ１９０は、受信した装置ＩＤに対応し、かつ、装置との安全な通信のために用いられることになる、適切な暗号鍵を取り出すか又は生成する。このように、かかる鍵は、データベース１６０から取り出される対称鍵、装置ＩＤ及びマスター秘密鍵から生成される対称鍵、又は装置内に記憶された対応する個人鍵を有するデータベース１７０から取り出される証明書から解凍される公開鍵とすることができる。この場合、適用可能な暗号鍵は、あらゆる適切な作動中の接続を用いて、製造者の通信を暗号化するために、用いられる。通常、これは、長距離接続、インターネット、無線接続等を用いるようにして、遠隔的に実行される。これらのどれもが、適切であり、パーソナル装置のインターフェース回路によってサポートされる。このように、パーソナル装置との

安全な通信チャンネルによって、製造者は、ソフトウェア・モジュールのダウンロード、設定データのダウンロード等を含む様々なサービスを、装置に対して提供することができる。

【図面の簡単な説明】

【００４７】

【図１】概略的に、要素を含む例示のシステムを示し、本発明の望ましい実施形態の動作を説明する図である。

【図２】図１で組み立てられた装置の出荷後に実行することのできる、可能な装置管理活動を概略的に説明する図である。

【図１】

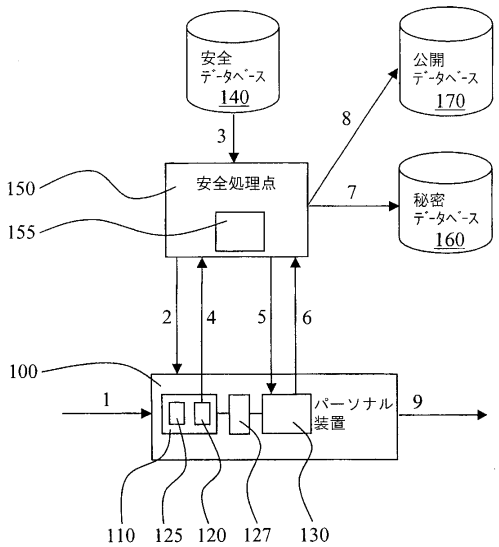

FIG. 1

【図２】

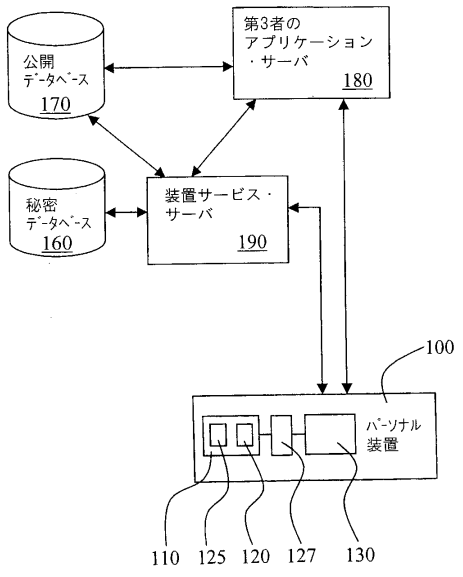

FIG. 2

フロントページの続き

(72)発明者　アソカン，ナダラジャ
フィンランド国，エフイーエン－０２３２０　エスプー，アンクリンバーシ　６　コー
(72)発明者　ニーミ，バルテリ
フィンランド国，エフイーエン－００１８０　ヘルシンキ，タルベルギンカツ　３　アス　４３

審査官　新田　亮

(56)参考文献　国際公開第０２／００３２７１（WO，Ａ１）
特開２００１－１０３０４５（ＪＰ，Ａ）
国際公開第０１／０７３５３９（WO，Ａ１）
米国特許出願公開第２００２／０１０７７９８（ＵＳ，Ａ１）
特開２０００－３３１４２０（ＪＰ，Ａ）
特開２００２－２９１０４３（ＪＰ，Ａ）
国際公開第０２／０４３０１６（WO，Ａ１）
特開２００２－２４５４２７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/08