

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2005-512425

(P2005-512425A)

(43) 公表日 平成17年4月28日(2005.4.28)

(51) Int.C1.⁷

H04M 1/725

F 1

H04M 1/725

テーマコード(参考)

5KO27

審査請求 未請求 予備審査請求 有 (全 23 頁)

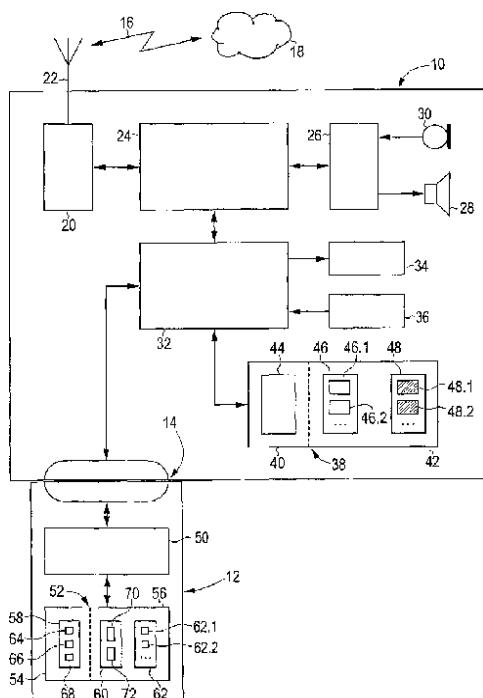
(21) 出願番号 特願2003-550529 (P2003-550529)
 (86) (22) 出願日 平成14年12月2日 (2002.12.2)
 (85) 翻訳文提出日 平成16年6月4日 (2004.6.4)
 (86) 國際出願番号 PCT/EP2002/013627
 (87) 國際公開番号 WO2003/049471
 (87) 國際公開日 平成15年6月12日 (2003.6.12)
 (31) 優先権主張番号 101 59 398.8
 (32) 優先日 平成13年12月4日 (2001.12.4)
 (33) 優先権主張国 ドイツ(DE)

(71) 出願人 596007511
 ギーゼッケ ウント デフリエント ゲー
 エムベーハー
 Giesecke & Devrient
 GmbH
 ドイツ連邦共和国 D-81677 ミュ
 ンヘン プリンツレーゲンテンシュトラッ
 セ 159
 (74) 代理人 100073184
 弁理士 柳田 征史
 100090468
 弁理士 佐久間 剛
 (72) 発明者 キルシュ, ヨッヘン
 ドイツ連邦共和国 80797 ミュンヘ
 ン クラウジングヴェーク 2
 最終頁に続く

(54) 【発明の名称】モバイル機器およびユーザー・モジュールへのデータの格納およびアクセス

(57) 【要約】

本発明はユーザー・モジュール(12)に接続されているモバイル機器(10)にユーザー・データ(48)および構成データ(62)を格納する方法、並びに格納されているこれらのデータにアクセスする方法に関するものである。本発明の第1の態様によれば、ユーザー・データ(48)が少なくとも一部が暗号化された形でモバイル機器(10)に格納され、アクセス操作において、ユーザー・モジュール(12)の復号化機能(66)によって復号される。本発明の第2の態様によれば、構成データ(62)がユーザー・モジュール(12)に格納される。構成データ(62)は、アプリケーション・プログラム(46)の実行をモバイル機器(10)許可するか否か、あるいは許可範囲を指示する。モバイル機器(10)のユーザー・データ(48)、およびアプリケーション・プログラム(46)に対する不正アクセス防止およびセキュリティが強化される。



【特許請求の範囲】

【請求項 1】

デバイス・メモリ(38)を有し、インターフェース(14)を介してユーザー・モジュール(12)に接続されているモバイル機器(10)、特に携帯電話または携帯情報端末にユーザー・データ(48)を格納し、該機器(10)の該データ(48)にアクセスする方法であって、

前記ユーザー・データ(48)を、少なくとも一部が暗号化された形で前記モバイル機器(10)のデバイス・メモリ(38)に格納し、

アクセス操作において、少なくとも前記ユーザー・データ(48)の復号を、前記ユーザー・モジュール(12)の復号化機能(66)によって実行する
ことを特徴とする方法。

【請求項 2】

格納操作において、前記ユーザー・データ(48)の暗号化を、前記ユーザー・モジュール(12)の暗号化機能(64)によって実行することを特徴とする請求項1記載の方法。

【請求項 3】

前記ユーザー・モジュール(12)が、該モジュール(12)の暗号化および復号化機能(64、66)、および該機能(64、66)によって使用されるキー・データ(60)を格納するモジュール・メモリ(52)を有し、該機能(64、66)の少なくとも一部を前記ユーザー・モジュール(12)のプロセッサー・ユニット(50)によって実行することを特徴とする請求項1または2記載の方法。

【請求項 4】

前記ユーザー・モジュール(12)が、前記キー・データ(60)の生成および前記モジュール・メモリ(52)への書き込みを行うための少なくとも1つの機能(68)を備えていることを特徴とする請求項3記載の方法。

【請求項 5】

少なくとも前記復号化機能(66)の実行が、パスワードおよび/または生体認証によって保護されていることを特徴とする請求項1～4いずれか1項記載の方法。

【請求項 6】

前記モバイル機器(10)が、通信機能もセットアップされている機器であることを特徴とする請求項1～5いずれか1項記載の方法。

【請求項 7】

前記ユーザー・モジュール(12)が、通信ネットワーク(18)にログインする機能も有する加入者識別モジュールであることを特徴とする請求項1～6いずれか1項記載の方法。

【請求項 8】

デバイス・メモリ(38)およびユーザー・モジュール(12)を接続するためのインターフェース(14)を備えるモバイル機器(10)、特に携帯電話または携帯情報端末であって、

前記ユーザー・モジュール(12)の暗号化および復号化機能(64、66)が、前記インターフェース(14)を介して呼出し可能であり、

前記デバイス・メモリ(38)が、暗号化されたユーザー・データ(48)を格納するための少なくとも1つの領域を有し、該領域に対し、前記ユーザー・モジュール(12)の暗号化および復号化機能(64、66)が書き込みおよび読み出しを行うようセットアップされていることを特徴とするモバイル機器(10)。

【請求項 9】

請求項8記載のモバイル機器(10)と連携し、請求項1～7いずれか1項記載の方法を実行するようセットアップされているユーザー・モジュール(12)、特に通信ネットワーク(18)の加入者識別モジュール。

【請求項 10】

10

20

30

40

50

アプリケーション・プログラム(46)を格納するためのデバイス・メモリ(38)を有し、インターフェース(14)を介して、モジュール・メモリ(52)を有するユーザー・モジュール(12)に接続されているモバイル機器(10)、特に携帯電話または携帯情報端末に構成データ(62)を格納する方法、該機器(10)の該データ(62)にアクセスする方法、および少なくとも1つの該プログラム(46)を実行する方法であって、

前記構成データ(62)が、

少なくとも前記アプリケーション・プログラム(46)、または該プログラム(46)の個別機能のアベイラビリティに関わり、

該構成データ(62)を前記モジュール・メモリ(52)に格納し、前記アプリケーション・プログラム(46)の実行の可否または範囲を判定する際、該メモリ(52)から読み出す

ことを特徴とする方法。

【請求項11】

前記モジュール・メモリ(12)からの前記構成データの読み出しが、パスワードおよび/または生体認証によって保護されていることを特徴とする請求項10記載の方法。

【請求項12】

少なくとも前記アプリケーション・プログラム(46)のパートが、前記構成データ(62)に基づいて、前記デバイス・メモリ(38)にロードされることを特徴とする請求項10または11記載の方法。

【請求項13】

前記モバイル機器(10)が、通信機能もセットアップされている機器であることを特徴とする請求項10～12いずれか1項記載の方法。

【請求項14】

少なくとも前記アプリケーション・プログラム(46)のパートが、前記モバイル機器(10)の少なくとも1つの通信機能によって、前記デバイス・メモリ(38)に転送されることを特徴とする請求項12または13記載の方法。

【請求項15】

前記ユーザー・モジュール(12)が、通信ネットワーク(18)にログインする機能も有する加入者識別モジュールであることを特徴とする請求項10～14いずれか1項記載の方法。

【請求項16】

請求項1～5いずれか1項記載の方法の特徴を更に有して成ることを特徴とする請求項10～15いずれか1項記載の方法。

【請求項17】

アプリケーション・プログラム(46)を格納するためのデバイス・メモリ(38)を有し、インターフェース(14)を介して、モジュール・メモリ(52)を有するユーザー・モジュール(12)に接続されているモバイル機器(10)、特に携帯電話または携帯情報端末であって、

少なくとも前記アプリケーション・プログラム(46)、または該プログラム(46)の個別機能のアベイラビリティに関わる前記構成データ(62)が、前記インターフェース(14)を介して、前記モジュール・メモリ(52)から呼び出し可能であり、

該メモリ(52)から呼び出された前記構成データ(62)に基づき、前記アプリケーション・プログラム(46)の実行の可否および範囲を判定するようセットアップされている

ことを特徴とするモバイル機器(10)。

【請求項18】

ユーザー・モジュール(12)と連携し、請求項10～16いずれか1項記載の方法を実行するようセットアップされていることを特徴とする請求項17記載のモバイル機器(10)。

10

20

30

40

50

【請求項 19】

請求項 17 記載のモバイル機器(10)と連携し、請求項 10 ~ 16 いずれか 1 項記載の方法を実行するようセットアップされているユーザー・モジュール(12)、特に通信ネットワーク(18)の加入者識別モジュール。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、一般には、モバイル機器、およびこの種の機器に用いられるユーザー・モジュールに対するデータの格納およびアクセス技術に関するものである。通信機能(例えば、通信ネットワークを介した音声および/またはデータ伝送)およびアプリケーション・プログラム(例えば、アポイントメント・スケジューラー、またはテキスト・エディター)を備えるモバイル機器が本発明にとって 1 つの好ましい領域である。この種のモバイル機器は、取り分け高性能携帯電話または PDA(携帯情報端末)として構成されている。

10

【背景技術】**【0002】**

GSM 規格(GSM = 移動通信用グローバル・システム)に対応した携帯電話が特許文献 1 に開示されている。前記携帯電話は、コントロール・ユニット、デバイス・メモリ、および加入者識別モジュール(SIM)用インターフェースを備えている。例えば、コンピュータとライン接続することにより、住所録、売り上げデータ、あるいは価格表などのユーザー・データをデバイス・メモリにロードすることができる。また、ライン接続を介しプログラム(詳細な説明は省略)をデバイス・メモリにロードし、その後、携帯電話によって実行することもできる。データの完全性が保証された形態、即ち、暗号化されたデータを伝送することができる。

20

【0003】

GMS 対応の携帯電話のスイッチを投入すると、一般に、ユーザーが個人の秘密番号(PIN = 個人識別番号)を入力することが要求される認証チェックが行われる。携帯電話に格納されているユーザー・データにアクセスするオプションを含めた完全なユーザー・インターフェースは、前記秘密番号が正しく入力されて初めて可能となる。このようにして、最も機密性の高いユーザー・データがある程度保護されている。しかし、執拗な犯罪者は前記セキュリティーを回避することができる。例えば、携帯電話の記憶要素は、適切なデバイスを用いることにより、ハードウェア・レベルで直接読み出すことができる。モバイル機器がアプリケーション・プログラムを実行するようセットアップされている場合、当該アプリケーション・プログラムによって処理されるユーザー・データを格納することは特に有益である。最近の高性能 GSM 携帯電話および PDA はこの機能を有している。例えば、GPRS(汎用パケット無線システム)、EDGE、UMTS(ユニバーサル移動通信システム)および WCDMA(広帯域符号分割多元接続)ネットワーク対応機器のような 2.5 世代および第 3 世代のモバイル機器の伝送速度は高速であり、モバイル機器に対し、空中インターフェースを介してサービス・プロバイダーからアプリケーション・プログラムのロードおよび/またはアップデートが可能である。

30

【特許文献 1】 独国特許出願公開第 19724901 号明細書

40

【発明の開示】**【発明が解決しようとする課題】****【0004】**

前記モバイル機器は、改善すべき多くの問題を抱えている。第 1 に、アプリケーション・プログラムに対する不正アクセスの防止が可能でなければならない。従って、認定ユーザーのみがアプリケーション・プログラムを呼び出すことが可能であるか、またはアプリケーション・プログラムに対する個別保証機能を備える必要がある。第 2 に、ユーザー要件にできるだけ近い機能選択ができることが望ましい。第 3 に、提供機能ができるだけ機器に依存しないことが必要である。

【0005】

50

本発明の目的は、前記問題を完全または部分的に解決することである。特に、モバイル機器内のユーザー・データおよびアプリケーション・プログラムのセキュリティおよび不正アクセス防止が本発明によって強化される。また、好ましい構成において、高いユーザーの利便性が実現されると共に、本発明がコスト効率よく導入される。

【課題を解決するための手段】

【0006】

本発明によれば、前記目的は、請求項1および10の特徴を有する方法、請求項8および17の特徴を有するモバイル機器、および請求項9および19の特徴を有するユーザー・モジュールによって完全または部分的に達成される。従属請求項は、本発明の好ましい構成に関連している。

10

【0007】

本発明は、ユーザー・データおよび構成データを適切な方法によって格納することにより、前記セキュリティ要件を満足するという基本概念から発している。

【0008】

本発明の第1の態様は、ユーザー・データの格納に関連している。本発明によれば、前記データは、暗号化された形でモバイル機器のデバイス・メモリに格納される。ユーザー・モジュールが提供する対応機能を用いて、少なくとも前記ユーザー・データが復号化される（好ましい構成では、暗号化も行われる）。

20

【0009】

無認可ユーザーが、モバイル機器の正規のユーザー・インターフェースをバイパスしてデバイス・メモリにアクセスしても、モバイル機器のメモリに格納されているユーザー・データはすべて暗号化されているため覗き見することはできない。一般に容量が大きいデバイス・メモリを用いて、セキュリティを気にせずユーザー・データを格納することができるため、比較的大量のデータおよび複雑な構造のデータをモバイル機器によって持ち運ぶことができる。

【0010】

本発明に基づいて格納されるユーザー・データは、ユーザーが希望するどのようなデータであってもよい。前記データは、モバイル機器上で動作するアプリケーション・プログラムによって処理されるデータであることが好ましい。前記のデータには、例えば、電話帳機能を有するアポイントメント・スケジューラーによって処理される予定リストおよび住所録、スプレッドシート・プログラムによって処理されるビジネス表、口述録音プログラムによって生成される音声データ、あるいはテキスト・エディターによって処理される一般的なテキストが含まれる。モバイル機器が適切なアプリケーション・プログラムを持たないユーザー・データを格納することも好ましい。この場合、モバイル機器は、例えば、職場と家庭との間におけるデータ交換のための安全なデータ記憶媒体となる。

30

【0011】

好ましい構成において、前記暗号化および復号化機能は、モジュール・メモリに記憶されているキー・データにアクセスする、ユーザー・モジュールのプロセッサー・ユニットによって全面的または部分的に実行される。前記好ましい構成において、前記キー・データをユーザー・モジュールから転送する必要がないため、特に高度なセキュリティが確保される。前記キー・データがユーザー・モジュール内で生成され、モジュール・メモリに書き込まれる場合、特にこのことが言える。しかし、ユーザー・モジュールの暗号化および/または復号化機能が、モバイル機器に転送され、少なくとも暗号化、および隨意的に復号化が、モバイル機器のプロセッサー・ユニットによって全面的または部分的に実行される本発明の構成も可能である。

40

【0012】

例えば、RSAのような非対称暗号化方式を用いることが好ましい。この場合、前記キー・データは、公開キーと秘密キーとから成る。しかし、対称暗号化方式を用いる構成も可能である。“暗号化および復号化機能”は同じ計算ステップを実行するが、概念的な用語として前記構成に引用されている。

50

【 0 0 1 3 】

本発明によれば、少なくとも復号化ステップを実行する上で、ユーザー・モジュールが必要である。このこと自体により、ユーザー・モジュールとモバイル機器とが分離されるため一定の保護が得られる。しかし、好ましい実施の形態において、パスワード（パスフレーズ）が入力されると共に/または、例えば、指紋検査あるいは音声分析のような生体認証が実施されるまで、少なくとも復号化機能を有効にしない措置が講じられている。前記措置により、モバイル機器およびユーザー・モジュールが置き忘れられた場合でも、データのセキュリティーが保証される。

【 0 0 1 4 】

本発明の第2の態様は、モバイル機器のアプリケーション・プログラムの実行に際し、構成データを利用するに關連している。この態様は、すべてのアプリケーション・プログラム、またはアプリケーション・プログラムの個別機能のアベイラビリティを構成データによって指示するという基本概念に基づいている。前記構成データは、ユーザー・モジュールに格納され、アプリケーション・プログラムはモバイル機器に格納される。前記アプリケーション・プログラムは、構成データによって指示されたとき、または指示された範囲のみが実行される。

【 0 0 1 5 】

本発明の教示により、アプリケーション・プログラム、または個別プログラム機能が無断で実行されるのを防止することができる。この理由は、モバイル機器の他に、プログラムの実行を可能にする構成データを備えるユーザー・モジュールが必ず必要とされるからである。また、本発明は、ユーザー要件に的確に対応したプログラム構成を提供するための技術基盤を創出する。このことは、例えば、ASP料金（ASP = アプリケーション・サービス・プロバイティング）のように、提供されている機能に依存し、プログラムの利用に対し使用料を支払う必要がある場合特に重要である。本発明によれば、構成データがユーザー・モジュールに格納されるため、互換性を有するモバイル機器にユーザー・モジュールをプラグ接続するのみで、希望するプログラム構成をセットアップすることができる。

【 0 0 1 6 】

“アプリケーション・プログラム”という用語は、本明細書においては、特に、前記ユーザー・データに対し、データ処理機能を実行するプログラムを意味する。モバイル機器が通信機能を備えている場合には、前記アプリケーション・プログラムは、通信機能から独立しているか、または少なくとも通信機能とは別の目的に兼用されるものであることが好ましい。標準的なアプリケーション・プログラムの例には、アポイントメント・スケジューラー、電話帳、テキスト・エディター、スプレッドシート・プログラム、データベース、口述録音プログラム等が含まれる。また、“アプリケーション・プログラム”という用語は、本明細書においては、前記アプリケーション・プログラム、または（ASPプロバイダーのサーバーを通して実際にデータ処理が行われている間の）同様のアプリケーションに対するユーザー・インターフェースのみを提供するプログラムも含んでいる。一部の構成においては、アプリケーション・プログラムとしてフォーマット化されたドキュメントを表示するためのブラウザーおよびビューアも提供される。しかし、アプリケーション・プログラムは、例えば、MP3形式のマルチメディア・コンテンツを再生するプログラムであってもよい。

【 0 0 1 7 】

アプリケーション・プログラムが無断で実行されるのを更に防止するため、パスワードおよび/または、例えば、音声または指紋分析のような生体認証によって前記構成データの読み出しを保護することが好ましい。この場合、ユーザー・モジュールは単に構成データをリリースするだけであるため、ユーザーは、パスワードおよび/または生体認証データを通して身元を証明する充分な証拠を提示することにより、対応するアプリケーション・プログラムまたはプログラム機能を実行することができる。

【 0 0 1 8 】

10

20

30

40

50

また、本発明による機能は、1つ以上のアプリケーション・プログラムを固定的に格納しているモバイル機器に使用することもできる。しかし、構成データは、アプリケーション・プログラム、または少なくともその一部をモバイル機器にロードする際の制御にも用いられることが好ましい。特に、高度な無線データ通信機能を備えたモバイル機器の場合には、空中インターフェースを介して外部のサービス・プロバイダーからアプリケーション・プログラム、あるいは必要なプログラム・モジュールをロードすることできる。この選択肢はASP料金との関連において特に有利である。ユーザー・モジュールを互換性のあるモバイル機器に接続するだけで、ユーザーのプログラム構成に対応するアプリケーション・プログラムを自動的にローディング開始することができれば、更に大幅に利便性が増す。コンピュータ・プラットフォームに依存しないプログラミング言語、例えば、Java（登録商標）を使用することによって、アプリケーション・プログラムの非専有ローディングがサポートされる。10

【0019】

前記本発明の2つの態様を組み合わせることにより、ユーザー・データに対する不正アクセスおよびアプリケーション・プログラムの無断実行が防止されるため特に効果的である。

【0020】

前記2つの態様の好ましい構成において、モバイル機器は通信機器、特に携帯電話または電話機能を有する携帯情報端末（PDA）である。通信ネットワークにログインする際に必要となるユーザー・モジュールは、加入者識別モジュール（SIM）であることが好ましい。特に、前記ユーザー・モジュールは、所謂トラステッド・デバイス、またはタンパレジスタント・デバイスと呼ばれているような不正改竄防止機能を備えることができ、暗号化および復号化機能、暗号化データ、あるいは機密構成データが盗み見されることがない。モバイル機器が電話機能を備えていない場合、または電話サービス会社に登録されていない場合であっても、加入者識別モジュールを備えることができる。というのは、この種のモジュールは大量生産されており比較的安価に入手できるからである。20

【0021】

前記モバイル機器およびユーザー・モジュールは、前記機能に対応する機能および/または方法に関する従属請求項に記載の機能を更に備えていることが好ましい。

【0022】

本発明の更なる機能、効果および目的は、以下に述べる本発明の実施の形態および複数の代替構成に関する詳細な説明によって明らかになる。30

【発明を実施するための最良の形態】

【0023】

図1は、インターフェース14を介して相互接続されているモバイル機器10およびユーザー・モジュール12を示す図である。本実施の形態において、モバイル機器10は、GSM規格の電話サービス、およびGPRS規格のデータ伝送サービスに必要な通信機能を備える高性能携帯電話として構成されている。従って、ユーザー・モジュール12は、前記携帯電話に挿入されるか、または固定的に配されているSIMカードとして構成されている。モバイル機器10は、空中インターフェース16を介し、対応する通信ネットワーク18にアクセスすることができる。別の構成において、モバイル機器10は、UMTSのような拡張移動電話規格に基づく携帯電話および/またはマルチメディア機能も備える携帯情報端末として構成される。40

【0024】

周知のモバイル機器同様、モバイル機器10は、アンテナ22を介して電波を送受信する高周波コンポーネント20を備えている。デジタル信号プロセッサー（DSP）24によって送信または受信信号が処理される。また、デジタル信号プロセッサー24は、低周波コンポーネント26を介し、ラウドスピーカー28に送られる低周波信号、あるいはマイクロフォン30から低周波コンポーネント26を介してデジタル信号プロセッサー24に送られる低周波信号も処理する。プロセッサー・ユニット32は、モバイル機器10内

50

部のすべての動作を調整する。プロセッサー・ユニット32は、インターフェース14、デジタル信号プロセッサー24、グラフィック・ケーブルLCDディスプレイとして構成されているディスプレイ34、キーボード36、およびデバイス・メモリ38に接続されている。デバイス・メモリ38は、固定的に設置するか、または、例えば、メモリカードのように取外し可能とすることができます。

【0025】

デバイス・メモリ38は、各種メモリ技術による複数の半導体チップによって構成することができる。図1の概念的描写において、デバイス・メモリ38は読み取り専用領域40(例えば、マスクプログラムROMによって実現)および、例えば、RAM、EEPROM、あるいはフラッシュ・メモリによって実現される書き込み可能領域42を備えている。特に、デバイス・メモリ38の読み取り専用領域40は、通信機能の実行に加え、モバイル機器10の基本オペレーティング・システムとしてプロセッサー・ユニット32によって実行されるオペレーティング・プログラム44を格納している。アプリケーション・プログラム46およびユーザー・データ48は、書き込み可能領域42にロードされる。

10

【0026】

図1において、アプリケーション・プログラム46の例として、(電話帳機能を有する)アポイントメント・スケジューラー46.1、およびテキスト・エディター46.2が示されている。アポイントメント・スケジューラー46.1によって処理される予定リストと住所録48.1、およびテキスト・エディター46.2によって処理される書簡48.2がユーザー・データとして図1に示されている。アプリケーション・プログラムは、プロセッサー・ユニット32によって実行され、その際ユーザー・データ48にアクセスする。ユーザー・データ48は、図1に斜線で示してあるように、デバイス・メモリ38に暗号化された形で格納されている。

20

【0027】

ユーザー・モジュール12は通信ネットワーク18のSIM(加入者識別モジュール)として構成され、インターフェース14も機械的および電気的に通信ネットワーク18の規格に対応している。ユーザー・モジュール12は、マイクロコントローラとして構成されモジュール・メモリ52と共に1つのチップ上に一体成形されているプロセッサー・ユニット50を備えている。モジュール・メモリ52は、各種メモリ技術によって、読み取り専用領域54と書き込み可能領域56とに分割されている。

30

【0028】

モジュール・メモリ52は、第1にユーザー・モジュール12の基本オペレーティング・システム機能を提供し、第2に通信ネットワーク18にログインし、モバイル機器10の通信操作を可能とする制御プログラムおよびデータを格納している。図1においては、図面の複雑化を避けるため、前記制御プログラムとデータは一体的に示されている。モジュール・メモリ52の読み取り専用領域54の暗号化/復号化機能58、および書き込み可能領域56のキー・データ60と構成データ62は、本発明の実施の形態による態様に密接に関連しているため図1に示す。

【0029】

暗号化/復号化機能58は、暗号化機能64、復号化機能66、およびキー生成機能64を備えている。キー・データ60は、公開キー70と秘密キー72とに分類されている。構成データ62は、モバイル機器10が備えている各々のアプリケーション・プログラム46に対応する構成データ・レコード、即ち、本実施の形態においては、アポイント・スケジューラー46.1に対応する構成データ・レコード62.1およびテキスト・エディター46.2に対応する構成データ・レコード62.2から成っている。

40

【0030】

動作において、図1のシステムは、それぞれの規格(本実施の形態ではGSMおよびGPRS規格)に対応した従来の通信機能を提供する。前記に加え、ユーザーは、アプリケーション・プログラムをスタートさせて、ユーザー・データ48、またはその他のデータを処理することができます。

50

【0031】

モバイル機器10のスイッチが投入されるか、または遅くとも、ユーザーがアプリケーション・プログラム46の開始を希望したとき、モバイル機器10はユーザー・モジュール12の構成データ62にアクセスし、アプリケーション・プログラム46を準備する。前記アクセスは、ユーザー・モジュールのプロセッサー・ユニット50を介して行われ、プロセッサー・ユニット50はアクセスを許可する前にパスワードの入力を要求する。前記パスワードの入力要求は、モバイル機器10のディスプレイ34に表示され、ユーザーはキーボード36によってパスワードを入力する。プロセッサー・ユニット50は入力されたパスワードが正しいか否かチェックする。

【0032】

正しいパスワードが入力されると、ユーザー・モジュール12が、要求された構成データ62（すべての構成データ62、またはアプリケーション・プログラム46.1および46.2に対応するデータ・レコード62.1および62.2のみ）をモバイル機器10に転送する。次いで、プロセッサー・ユニット32が、転送されてきた構成データ62、62.1、62.2に基づいて、アプリケーション・プログラム46、または具体的に要求されたアプリケーション・プログラム46.1および46.2が実行可能であるか否かチェックし、可能であれば実行を許可する。

【0033】

希望するアプリケーション・プログラム46.1、46.2が、デバイス・メモリ38に既に存在している場合には、直ちに実行開始することができる。存在していない場合には、課金される可能性がある必要なプログラムまたはユーザー・データが、空中インターフェース16および通信ネットワーク18を介して、ASPプロバイダーのサーバーからデバイス・メモリ38にロードされる。前記ダウンロード・プロセスも、所謂ゲートキーパーとして機能するユーザー・モジュール12の認可を受ける必要がある。希望するアプリケーション・プログラム46.1、46.2が、デバイス・メモリ38に既に存在している場合であっても、第1に課金データを伝送するため、第2に入手可能なアップデート・プログラムをモバイル機器10にインポートするため、空中インターフェース16を介し、ASPプロバイダーに要求を出すことができる。

【0034】

本実施の形態においては、構成データ62は、基本的なユーザー認証に関わるのみならず、例えば、所定のファイル・パス、言語設定、メニュー構成、およびその他のユーザー嗜好など、アプリケーション・プログラム46の好みのセッティングにも関わっている。これらのセッティングは、開始したアプリケーション・プログラムによってアクセス可能であるため、ユーザーは常に希望するプログラム構成の下で作業をすることができる。このことは、新しいモバイル機器、または別のモバイル機器にユーザー・モジュールを接続した場合でも当てはまる。

【0035】

例えば、中期展望として実現が期待されている、プログラミング言語Javaを用いた標準化のように、アプリケーション・プログラミング・インターフェース(API)が充分標準化された暁には、個々のユーザーに対応し、且つ使用モバイル機器10に依存しないアプリケーション・プログラム・サービスが、ASPプロバイダーによって提供されるようになる。また、すべてのアプリケーション・プログラム46は、ユーザー・モジュールが提示され、パスワードが入力されて初めて呼び出すことができるため、高度なセキュリティも確保される。モバイル機器10のスイッチが投入された状態で（ユーザーがパスワードを入力した後）盗難に遭った場合、悪用を防止するため、例えば、使用されていないオフィス・コンピュータのスクリーン・セイバーのように、所定の時間モバイル機器10が非活動状態になると、パスワードの再入力を要求するようにすることができる。

【0036】

本実施の形態の説明において、アプリケーション・プログラム46を認証メカニズムおよび空中インターフェース16を介した随意のローディング・プロセスの最小単位と見なし

10

20

30

40

50

てきた。しかし、プログラミング技術にもよるが、更に細かい単位を採用することもできる。従って、例えば、個別プログラム機能またはプログラム・モジュールを実行する際のユーザー認証に構成データ62を関連付けると共に、必要があれば、空中インタフェース16を介して、これらのプログラム機能またはプログラム・モジュールを個別にロードすることができる。前記方法により、第1に、ローディングに要する時間を短縮することができ、第2に、ユーザーの嗜好により正確に対応することができる。また、空中インタフェース16を介してアプリケーション・プログラム46をアップデートする際、モバイル機器10に存在しているバージョンの実際に変更されたプログラム・モジュールのみを転送することが好ましい。

【0037】

アプリケーション・プログラム46によって処理されたユーザー・データ48は、完全または少なくとも一部が暗号化されデバイス・メモリ38に格納される。例えば、ユーザーに対し、個別フォルダーまたは個別ドライブを選択的にセットして暗号化データおよび非暗号化データを格納する、ユーザー・データ48を格納するためのファイル・システムを提供することができる。ユーザー・モジュールを使用しない固定オフィス・コンピュータに対する同様の機能が、Network Associates社の製品、PGPdisk（登録商標）によって既に知られている。

【0038】

アプリケーション・プログラム46が、ユーザー・データ48を前記ファイル・システムの暗号領域に格納する場合、当該データはインタフェース14を介して、プロセッサー・ユニット32からユーザー・モジュール12に転送される。ユーザー・モジュール12のプロセッサー・ユニット50が、キー・データ60の公開キー70を使用する暗号化機能64を実行する。暗号化されたユーザー・データ48は、インタフェース14およびプロセッサー・ユニット32を介してデバイス・メモリ38に書き込まれる。

【0039】

暗号化された形で格納されているユーザー・データは、それに対応する方法によってアクセスされる。ここでも、ユーザー・モジュール12のプロセッサー・ユニット50が、復号化機能66および秘密キー72を用いて実際の復号化処理を行う。しかし、プロセッサー・ユニット50は、復号化処理を実行する前に、ユーザーに対しパスフレーズを入力するよう要求する。正しいパスフレーズがキーボード36から入力されたとき（または、別の方針として、ユーザーが生体的に正しく識別されたとき）に限り、復号化プロセスが有効になる。

【0040】

本実施の形態においては、非対称RSA方式に基づいて暗号化および復号化が行われている。これに対し、別の構成においては、別の非対称または対称暗号化/復号化方式、あるいは非対称に暗号化したキーを用いた対称暗号化のような混合方式が用いられる。対称方式においては、公開キー70と秘密キー72とを区別する必要はない。

【0041】

要約すれば、提案技術により、正当なユーザーのユーザー・モジュール12がインタフェース14に接続され、ユーザーが、例えば、パスフレーズを用いて、正しく身元を証明したときに限り、暗号化されたデータ48を読み出すことができる、即ち、使用することができる。

【0042】

本実施の形態においては、暗号化および復号化処理はすべてユーザー・モジュール12のプロセッサー・モジュール50によって実行され、キー・データ60がユーザー・モジュール12から離れることはない。しかし、暗号化機能64および秘密にしておく必要がない公開キー70をモバイル機器10に転送し、モバイル機器10の一般により強力なプロセッサー・ユニット32によって暗号化プロセスを実行することができる別の構成も可能である。一部の別の構成において、秘密キー72のセキュリティが確保されることを条件に、プロセッサー・ユニット32が復号化処理にも利用される。

10

20

30

40

50

【0043】

本実施の形態において、ユーザー・モジュール12のプロセッサー・ユニット50によって実行されるキー生成機能68によってキー・データ60が生成される。このプログラムは、周知の方法によって公開キー70および秘密キー72のペアを算出する。秘密キー72が生成中においてもユーザー・モジュール12から離れることがないため、前記方法により特に高度なデータのセキュリティーが確保される。

【0044】

本実施の形態においては、ユーザー・データ48に対し、1つの暗号化領域、および1つの暗号化方式に限定されるものではない。パスフレーズによって適切に身元が証明されていることを条件に、例えば、いつでも暗号化領域を解除して自由にアクセスできるようになることができる。前記領域は、同一または別のユーザー・モジュール12によって再度暗号化することができる。異なるキー・ペアによるか否かは任意であると共に/または異なるサイズの複数の暗号化領域を設定し管理することもできる。

10

【0045】

本構成においては、特に、暗号化されたユーザー・データ48をモバイル機器10に格納すると共に、空中インターフェース16を介し、ASPプロバイダーのサーバーに転送し、その場に格納することもできる。両サイドに格納されているユーザー・データ48は、アプリケーション・プログラムの書き込みアクセスの都度、ユーザー・セッションが終了した都度、あるいはユーザーから明示的に要求されたときに同期化することができる。これにより、ユーザーは、一方において、ローカル的に格納されているユーザー・データ48に迅速にアクセスすることができ、他方において、使用するモバイル機器10とは無関係にASPプロバイダーに格納されているユーザー・データ48を読み出すことができる。

20

【0046】

一部の構成において、キーのコンポーネントをネットワーク・オペレータまたはASPプロバイダーに預託することができる。モバイル機器が通信ネットワーク18にログインした後、空中インターフェースを介し、前記キーのコンポーネントが転送される。これにより、ネットワーク・オペレータ、またはASPプロバイダーが、モバイル機器10に格納されている一定のユーザー・データ48の制御をユーザーと共有することができる。

30

【図面の簡単な説明】

【0047】

【図1】本発明の実施の形態によるシステムの基本機能ユニットを示すブロック図。

【符号の説明】

【0048】

1 0	モバイル機器
1 2	ユーザー・モジュール
3 2	プロセッサー・ユニット(モバイル機器)
3 8	デバイス・メモリ
4 4	オペレーティング・プログラム
4 6	アプリケーション・プログラム
4 8	ユーザー・データ
5 0	プロセッサー・ユニット(ユーザー・モジュール)
5 2	モジュール・メモリ
5 8	暗号化/復号化機能
6 0	キー・データ
6 2	構成データ
6 4	暗号化機能
6 6	復号化機能
6 8	キー生成機能

40

【 図 1 】

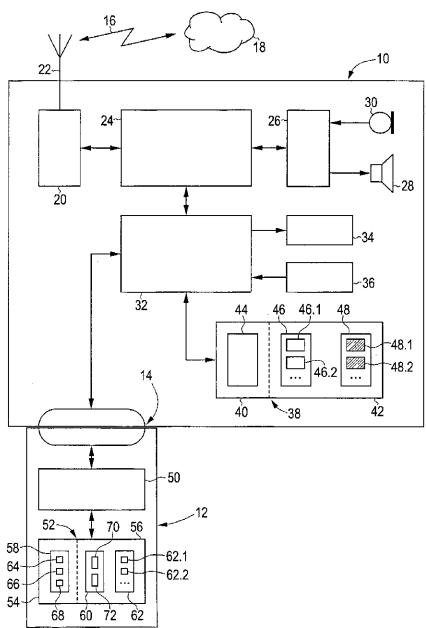


Fig. 1

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/13627

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 107 627 A (SIEMENS AG) 13 June 2001 (2001-06-13) column 1, line 5 - line 25 column 1, line 45 -column 2, line 5 column 3, line 19 -column 4, line 25 figure 1 ---	1-9
Y	WO 00 59244 A (SONERA SMARTTRUST OY ;VATANEN HARRI (GB)) 5 October 2000 (2000-10-05) page 1, line 11 - line 25 page 2, line 26 -page 3, line 11 page 5, line 7 - line 37 figure 1 ---	1-9 -/-

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *S* document member of the same patent family

Date of the actual completion of the international search

1 April 2003

Date of mailing of the international search report

11.04.03

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl
Fax: (+31-70) 340-3016

Authorized officer

Rabe, M

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/EP 02/13627

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 802 175 A (KARA SALIM G) 1 September 1998 (1998-09-01) abstract column 2, line 42 - line 67 column 5, line 12 - line 25 column 5, line 56 - line 65 figure 2 ----	1-9
A	WO 00 48416 A (HILTUNEN MATTI ;LIUKKONEN JUKKA (FI); SONERA SMARTTRUST OY (FI); V) 17 August 2000 (2000-08-17) abstract page 3, line 12 -page 4, line 16 page 5, line 28 -page 6, line 5 page 10, line 13 -page 11, line 12 figures 1,2 ----	1-9
X	EP 0 730 387 A (IBM) 4 September 1996 (1996-09-04)	10,17-19
Y	column 1, line 6 - line 35 column 2, line 25 - line 47 column 4, line 1 - line 29 column 6, line 2 - line 31 column 8, line 32 - line 50 figure 5 ----	11-16
X	US 5 814 798 A (ZANCHO WILLIAM F) 29 September 1998 (1998-09-29)	10,17-19
Y	abstract column 3, line 6 - line 35 column 5, line 6 -column 6, line 15 figure 8 ----	11-16
A	EP 0 969 644 A (NOKIA MOBILE PHONES LTD) 5 January 2000 (2000-01-05) abstract column 1, line 36 - line 45 column 3, line 14 - line 50 figure 1 ----	10,11, 17-19
A	EP 0 891 111 A (MANNESMANN AG) 13 January 1999 (1999-01-13) abstract column 1, line 48 -column 2, line 35 column 5, line 58 -column 8, line 3 figure 1A -----	10,17-19

INTERNATIONAL SEARCH REPORT

International application No. _____

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

SEE SUPPLEMENTAL SHEET

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest.
 No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP02/13627

The International Searching Authority has determined that this international application contains multiple (groups of) inventions, namely:

1. Claims: 1-9

Method for storing and accessing useful data in a mobile device, said useful data being stored at least in part in encrypted form in the memory of the mobile device and being decrypted during access processes by using a decryption function provided by a user module connected via an interface; corresponding mobile device and user module.

2. Claims: 10-19

Method for storing and accessing configuration data and for carrying out at least one application program in a mobile device, said configuration data being stored in the module memory of a user module connected via an interface and being read therefrom so as to determine whether and to what extent the application program is being executed; corresponding mobile device and user module.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 02/13627

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
EP 1107627	A	13-06-2001	EP	1107627 A1	13-06-2001
WO 0059244	A	05-10-2000	AU WO	3437000 A 0059244 A1	16-10-2000 05-10-2000
US 5802175	A	01-09-1998	NONE		
WO 0048416	A	17-08-2000	FI AU EP WO	990256 A 2551500 A 1151625 A1 0048416 A1	10-08-2000 29-08-2000 07-11-2001 17-08-2000
EP 0730387	A	04-09-1996	US EP JP JP	5675630 A 0730387 A2 3352582 B2 8279842 A	07-10-1997 04-09-1996 03-12-2002 22-10-1996
US 5814798	A	29-09-1998	US CA CN DE ES FR GB IT JP	5633484 A 2165278 A1 1132874 A ,B 19548393 A1 2112198 A1 2729038 A1 2296584 A ,B RM950854 A1 8255033 A	27-05-1997 30-06-1996 09-10-1996 11-07-1996 16-03-1998 05-07-1996 03-07-1996 01-07-1996 01-10-1996
EP 0969644	A	05-01-2000	EP	0969644 A1	05-01-2000
EP 0891111	A	13-01-1999	DE EP	19729933 A1 0891111 A2	04-02-1999 13-01-1999

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 02/13627

A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04Q7/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie ^a	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 1 107 627 A (SIEMENS AG) 13. Juni 2001 (2001-06-13) Spalte 1, Zeile 5 - Zeile 25 Spalte 1, Zeile 45 - Spalte 2, Zeile 5 Spalte 3, Zeile 19 - Spalte 4, Zeile 25 Abbildung 1 ---	1-9
Y	WO 00 59244 A (SONERA SMARTTRUST OY ; VATANEN HARRI (GB)) 5. Oktober 2000 (2000-10-05) Seite 1, Zeile 11 - Zeile 25 Seite 2, Zeile 26 - Seite 3, Zeile 11 Seite 5, Zeile 7 - Zeile 37 Abbildung 1 --- -/-	1-9

 Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen Siehe Anhang Patentfamilie^a Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert,

aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen

Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweitheitlich er-

scheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung,

eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahelegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

Absendedatum des internationalen Recherchenberichts

1. April 2003

11.04.03

Name und Postanschrift der Internationalen Recherchenbehörde

Bevollmächtigter Bediensteter

Europäisches Patentamt, P.O. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel: (+31-70) 340-2040, Fax: 31 651 epo nl.
Fax: (+31-70) 340-3016

Rabe, M

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen PCT/EP 02/13627

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 5 802 175 A (KARA SALIM G) 1. September 1998 (1998-09-01) Zusammenfassung Spalte 2, Zeile 42 - Zeile 67 Spalte 5, Zeile 12 - Zeile 25 Spalte 5, Zeile 56 - Zeile 65 Abbildung 2 ---	1-9
A	WO 00 48416 A (HILTUNEN MATTI ; LIUKKONEN JUKKA (FI); SONERA SMARTTRUST OY (FI); V) 17. August 2000 (2000-08-17) Zusammenfassung Seite 3, Zeile 12 -Seite 4, Zeile 16 Seite 5, Zeile 28 -Seite 6, Zeile 5 Seite 10, Zeile 13 -Seite 11, Zeile 12 Abbildungen 1,2 ---	1-9
X	EP 0 730 387 A (IBM) 4. September 1996 (1996-09-04)	10,17-19
Y	Spalte 1, Zeile 6 - Zeile 35 Spalte 2, Zeile 25 - Zeile 47 Spalte 4, Zeile 1 - Zeile 29 Spalte 6, Zeile 2 - Zeile 31 Spalte 8, Zeile 32 - Zeile 50 Abbildung 5 ---	11-16
X	US 5 814 798 A (ZANCHO WILLIAM F) 29. September 1998 (1998-09-29)	10,17-19
Y	Zusammenfassung Spalte 3, Zeile 6 - Zeile 35 Spalte 5, Zeile 6 -Spalte 6, Zeile 15 Abbildung 8 ---	11-16
A	EP 0 969 644 A (NOKIA MOBILE PHONES LTD) 5. Januar 2000 (2000-01-05) Zusammenfassung Spalte 1, Zeile 36 - Zeile 45 Spalte 3, Zeile 14 - Zeile 50 Abbildung 1 ---	10,11, 17-19
A	EP 0 891 111 A (MANNESMANN AG) 13. Januar 1999 (1999-01-13) Zusammenfassung Spalte 1, Zeile 48 -Spalte 2, Zeile 35 Spalte 5, Zeile 58 -Spalte 8, Zeile 3 Abbildung 1A -----	10,17-19

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 02/13627

Feld I Bemerkungen zu den Ansprüchen, die sich als nicht recherchierbar erwiesen haben (Fortsetzung von Punkt 2 auf Blatt 1)

Gemäß Artikel 17(2a) wurde aus folgenden Gründen für bestimmte Ansprüche kein Recherchenbericht erstellt:

1. Ansprüche Nr. weil sie sich auf Gegenstände beziehen, zu deren Recherche die Behörde nicht verpflichtet ist, nämlich
2. Ansprüche Nr. weil sie sich auf Teile der internationalen Anmeldung beziehen, die den vorgeschriebenen Anforderungen so wenig entsprechen, daß eine sinnvolle internationale Recherche nicht durchgeführt werden kann, nämlich
3. Ansprüche Nr. weil es sich dabei um abhängige Ansprüche handelt, die nicht entsprechend Satz 2 und 3 der Regel 6.4 a) abgefaßt sind.

Feld II Bemerkungen bei mangelnder Einheitlichkeit der Erfindung (Fortsetzung von Punkt 3 auf Blatt 1)

Die internationale Recherchenbehörde hat festgestellt, daß diese internationale Anmeldung mehrere Erfindungen enthält:

siehe Zusatzblatt

1. Da der Anmelder alle erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht auf alle recherchierbaren Ansprüche.
2. Da für alle recherchierbaren Ansprüche die Recherche ohne einen Arbeitsaufwand durchgeführt werden konnte, der eine zusätzliche Recherchengebühr gerechtfertigt hätte, hat die Behörde nicht zur Zahlung einer solchen Gebühr aufgefordert.
3. Da der Anmelder nur einige der erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht nur auf die Ansprüche, für die Gebühren entrichtet worden sind, nämlich auf die Ansprüche Nr.
4. Der Anmelder hat die erforderlichen zusätzlichen Recherchengebühren nicht rechtzeitig entrichtet. Der internationale Recherchenbericht beschränkt sich daher auf die in den Ansprüchen zuerst erwähnte Erfindung; diese ist in folgenden Ansprüchen erfaßt:

Bemerkungen hinsichtlich eines Widerspruchs

 Die zusätzlichen Gebühren wurden vom Anmelder unter Widerspruch gezahlt. Die Zahlung zusätzlicher Recherchengebühren erfolgte ohne Widerspruch.

Internationales Aktenzeichen PCT/EP 02/13627

WEITERE ANGABEN	PCT/ISA/ 210
<p>Die internationale Recherchenbehörde hat festgestellt, daß diese internationale Anmeldung mehrere (Gruppen von) Erfindungen enthält, nämlich:</p> <p>1. Ansprüche: 1-9</p> <p>Verfahren zum Speichern von und Zugreifen auf Nutzdaten in einem Mobilgerät, wobei Nutzdaten im Gerätespeicher des Mobilgeräts zumindest teilweise in verschlüsselter Form gespeichert werden, und wobei das Entschlüsseln der Nutzdaten bei Zugriffsvorgängen unter Verwendung einer durch ein über eine Schnittstelle verbundenes Benutzermodul bereitgestellten Entschlüsselungsfunktion erfolgt; entsprechendes Mobilgerät und Benutzermodul</p> <p>2. Ansprüche: 10-19</p> <p>Verfahren zum Speichern von und Zugreifen auf Konfigurationsdaten sowie zum Ausführen mindestens eines Anwendungsprogramms in einem Mobilgerät, wobei die Konfigurationsdaten in dem Modulspeicher eines durch eine Schnittstelle verbundenen Benutzermoduls gespeichert sind, und aus diesem ausgelesen werden, um zu bestimmen, ob bzw. in welchem Umfang das Anwendungsprogramm ausgeführt wird; entsprechendes Mobilgerät und Benutzermodul</p>	

INTERNATIONALE RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 02/13627

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung		Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 1107627	A	13-06-2001	EP	1107627 A1		13-06-2001
WO 0059244	A	05-10-2000	AU	3437000 A		16-10-2000
			WO	0059244 A1		05-10-2000
US 5802175	A	01-09-1998	KEINE			
WO 0048416	A	17-08-2000	FI	990256 A		10-08-2000
			AU	2551500 A		29-08-2000
			EP	1151625 A1		07-11-2001
			WO	0048416 A1		17-08-2000
EP 0730387	A	04-09-1996	US	5675630 A		07-10-1997
			EP	0730387 A2		04-09-1996
			JP	3352582 B2		03-12-2002
			JP	8279842 A		22-10-1996
US 5814798	A	29-09-1998	US	5633484 A		27-05-1997
			CA	2165278 A1		30-06-1996
			CN	1132874 A ,B		09-10-1996
			DE	19548393 A1		11-07-1996
			ES	2112198 A1		16-03-1998
			FR	2729038 A1		05-07-1996
			GB	2296584 A ,B		03-07-1996
			IT	RM950854 A1		01-07-1996
			JP	8255033 A		01-10-1996
EP 0969644	A	05-01-2000	EP	0969644 A1		05-01-2000
EP 0891111	A	13-01-1999	DE	19729933 A1		04-02-1999
			EP	0891111 A2		13-01-1999

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT, BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ, GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DK,DM,DZ,EC,EE,ES, FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,N O,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 クラーセン , ラルフ

ドイツ連邦共和国 8 1 8 2 5 ミュンヘン シュピールヨッハシュトラーセ 8

(72)発明者 エッカルト , シュテファン

ドイツ連邦共和国 8 1 7 3 9 ミュンヘン グスタフ - ハイネマン - シュトラーセ 8 5

F ターム(参考) 5K027 AA11 BB04 BB09 KK07 MM03