(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2004-503031
(P2004-503031A)
(43)公表日　平成16年1月29日(2004.1.29)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 17/60	G06F 17/60	410C	5B017
G06F 12/14	G06F 17/60	410E	5B058
G06F 15/00	G06F 17/60	414	5B085
G06K 17/00	G06F 12/14	320C	
	G06F 15/00	330B	

審査請求 未請求　予備審査請求 未請求　（全 60 頁）　最終頁に続く

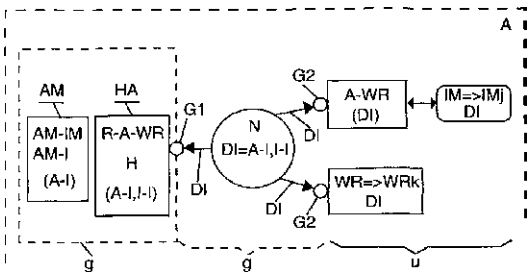
(21)出願番号　特願2002-508755(P2002-508755)
(86)(22)出願日　平成13年7月10日(2001.7.10)
(85)翻訳文提出日　平成14年3月8日(2002.3.8)
(86)国際出願番号　PCT/CH2001/000433
(87)国際公開番号　WO2002/005225
(87)国際公開日　平成14年1月17日(2002.1.17)
(31)優先権主張番号　1365/00
(32)優先日　平成12年7月11日(2000.7.11)
(33)優先権主張国　スイス(CH)
(81)指定国　EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),AU,BR,CA,CN,IL,IN,JP,MX,SG,US,ZA

(71)出願人　501477118
カバ・シュリースジステーメ・アー・ゲー
スイス、ツェー・ハー－８６２０　ヴェツィコン、ミューレブールシュトラーセ、２３
(74)代理人　100064746
弁理士　深見　久郎
(74)代理人　100085132
弁理士　森田　俊雄
(74)代理人　100083703
弁理士　仲村　義平
(74)代理人　100091409
弁理士　伊藤　英彦
(74)代理人　100096781
弁理士　堀井　豊

最終頁に続く

(54)【発明の名称】移動データ記憶媒体の初期化のための方法

(57)【要約】
この方法を用いて、移動データ記憶媒体（ＩＭ）は、認証システム（Ａ）のフレームワーク内で、割当てられ分散された読出および書込ステーション（ＷＲ）で初期化される。安全な環境（ｇ）の中の認証局（ＨＡ）で、初期化データ（ＤＩ，Ａ－Ｉ，Ｉ－Ｉ）が認証手段（ＡＭ）によって生成されかつ、認証システム（Ａ）に対応するセキュリティルールによっておよび安全な通信の中でネットワーク（Ｎ）を介して、分散され認証された読出および書込ステーション（Ａ－ＷＲ）に伝送される。ここで、移動データ記憶媒体（ＩＭ）は初期化データ（ＤＩ）で初期化されならびに／または、初期化データは分散された読出および書込ステーション（ＷＲ）へネットワークを介して伝送される。これにより、読出および書込ステーションが初期化される。この初期化方法は、この種類のシステムの適用および活用の新たな可能性を可能にする。



【特許請求の範囲】
【請求項１】
認証システム（Ａ）のフレームワーク内での、割当てられ分散された読出および書込ステーション（ＷＲ）を有する移動データ記憶媒体（ＩＭ）ならびに／または分散された読出および書込ステーション（ＷＲ）の初期化のための方法であって、安全な環境（ｇ）の中の認証局（ＨＡ）での認証手段（ＡＭ）による認証により、初期化データ（ＤＩ，Ａ－Ｉ，Ｉ－Ｉ）が生成されかつ、認証システムに対応するセキュリティルールによっておよび安全な通信の中でネットワーク（Ｎ）を介して、分散され認証された読出および書込ステーション（Ａ－ＷＲ）に伝送され、移動データ記憶媒体（ＩＭ）は、読出および書込ステーション（Ａ－ＷＲ）で初期化データ（ＤＩ）によって対応して初期化され（ＩＭｊ）ならびに／または、初期化データ（ＤＩ）は、ネットワーク（Ｎ）を介して、分散された読出および書込ステーション（ＷＲ）に伝送され、これにより、読出および書込ステーションが初期化される（ＷＲｋ）ことを特徴とする、方法。
【請求項２】
認証局（ＨＡ）は、ホストコンピュータ（Ｈ）またはリモート認証読出および書込ステーション（Ｒ－Ａ－ＷＲ）によって形成されることを特徴とする、請求項１に記載の方法。
【請求項３】
認証手段（ＡＭ）は、特別な認証識別媒体（ＡＭ－ＩＭ）または認証データ（ＡＭ－Ｉ）によって形成されることを特徴とする、請求項１または２に記載の方法。
【請求項４】
（認証されていない）分散された読出および書込ステーション（ＷＲ）は、まず、初期化データ（ＤＩ）に含まれる機能認証データ（Ａ－Ｉ－ＦＡ）により、認証された読出および書込ステーション（Ａ－ＷＲ）に変換され、これは後で、初期化データに対応して移動データ記憶媒体（ＩＭ）を初期化することができることを特徴とする、請求項１から３のいずれかに記載の方法。
【請求項５】
認証システム（Ａ）のフレームワーク内に、同じおよび／または異なる認証レベル（ＯＬｉ）を有するいくつかの認証局（ＨＡｉ）が設けられることを特徴とする、請求項１から４のいずれかに記載の方法。
【請求項６】
同じおよび／または異なる認証レベル（ＯＬｉ）を有するいくつかの認証手段（ＡＭｉ）が設けられることを特徴とする、請求項１から５のいずれかに記載の方法。
【請求項７】
初期化データ（ＤＩ，Ａ－Ｉ，Ｉ－Ｉ）は、１つよりも多くのネットワークレベル（Ｎ１，Ｎ２）を介しておよび／または１つよりも多くの認証局（ＨＡ１，ＨＡ２）を介して、認証された読出および書込ステーション（Ａ－ＷＲ）または分散された読出および書込ステーション（ＷＲ）へ伝送されることを特徴とする、請求項１から６のいずれかに記載の方法。
【請求項８】
初期化データ（ＤＩ）は安全なプライベートネットワーク（Ｎｐ）を介して伝送されることを特徴とする、請求項１から７のいずれかに記載の方法。
【請求項９】
初期化データは、両側に暗号化およびセキュリティゲート（Ｇ１，Ｇ２）を備えるオープン公衆ネットワーク（Ｎｏ）を介して伝送されることを特徴とする、請求項１から８のいずれかに記載の方法。
【請求項１０】
初期化データ（ＤＩ２．２）を用いて、アプリケーション拡張（Ａｐｐ２．２）が初期化されることを特徴とする、請求項１から９のいずれかに記載の方法。
【請求項１１】
初期化データ（ＤＩ３）を用いて、新たな独立したアプリケーション（Ａｐｐ３）が初期

化されることを特徴とする、請求項１から１０のいずれかに記載の方法。
【請求項１２】
システムデータフィールド（ＣＤＦ）を備えて準備されたブランクの移動データ記憶媒体の中で、アプリケーション（Ａｐｐ）は初期化データ（ＤＩ）で新たに初期化されることを特徴とする、請求項１から１１のいずれかに記載の方法。
【請求項１３】
ネットワーク（Ｎ）を介して、認証局（ＨＡ）と分散された読出および書込ステーション（Ａ－ＷＲ，ＷＲ）との間の永久的な接続が存在することを特徴とする、請求項１から１２のいずれかに記載の方法。
【請求項１４】
ネットワーク（Ｎ）を介した、認証局（ＨＡ）と分散された読出および書込ステーション（Ａ－ＷＲ，ＷＲ）との間の接続は、ときおりおよびデータの交換が発生するときだけ存在することを特徴とする、請求項１から１３のいずれかに記載の方法。
【請求項１５】
初期化のため、ユーザ認証（ａｗ）は、読出および書込ステーション（Ａ－ＷＲ，ＷＲ）もしくはその所有者（１２）によって行なわれならびに／または、識別認証手段（ＩＤ－ＡＭ）が必要であることを特徴とする、請求項１から１４のいずれかに記載の方法。
【請求項１６】
初期化のため、データ記憶媒体またはデータ記憶媒体の所有者（１３）を介したユーザ認証（ａｉ）が起こることを特徴とする、請求項１から１５のいずれかに記載の方法。
【請求項１７】
ネットワーク（Ｎ）を介した初期化の認証のためならびに読出および書込ステーション（Ａ－ＷＲ，ＷＲ）またはデータ記憶媒体（ＩＭ）でのアプリケーションの実行のために、読出および書込ステーションの所有者の個人データ（ａｗ）または、ＰＩＮコードもしくは生体測定的データなどの、データ記憶媒体の所有者の個人データ（ａｉ）が認証手段として利用されることを特徴とする、請求項１から１６のいずれかに記載の方法。
【請求項１８】
移動データ記憶媒体（ＩＭ）は、アプリケーションプログラムデータ（Ｉ－Ｉ－Ｃｏｄ）の処理のためにアプリケーションマイクロプロセッサ（ＡｐｐｕＰ）を含むことを特徴とする、請求項１から１７のいずれかに記載の方法。
【請求項１９】
データ記憶媒体（ＩＭ）は、非接触型の、能動型または受動型の識別媒体として設計されることを特徴とする、請求項１から１８のいずれかに記載の方法。
【請求項２０】
移動データ記憶媒体（ＩＭ）、認証識別媒体（ＡＭ－ＩＭ）および識別認証媒体（ＩＤ－ＡＭ）は同じ移動データ記憶媒体によって形成されることを特徴とする、請求項１から１９のいずれかに記載の方法。
【請求項２１】
認証されたもしくは分散された読出および書込ステーション（Ａ－ＷＲ，ＷＲ）ならびに／または移動データ記憶媒体（ＩＭ）でのイベントに関するステータス情報（Ｓ－Ｉ）は、ネットワーク（Ｎ）を介して、対応する認証局（ＨＡ）に告知されることを特徴とする、請求項１から２０のいずれかに記載の方法。
【請求項２２】
ステータス情報（Ｓ－Ｉ）は使用またはライセンス費用借方記入のために利用されることを特徴とする、請求項２１に記載の方法。
【請求項２３】
使用またはライセンス費用の借方記入の目的のための、データ記憶媒体（ＩＭ）のあらゆる新たな初期化は、ネットワーク（Ｎ）を介して認証局（ＨＡ）に告知されることを特徴とする、請求項１から２２のいずれかに記載の方法。
【請求項２４】

使用またはライセンス費用の借方記入の目的のための、読出および書込ステーション（ＷＲ）でのアプリケーションのあらゆる使用は、ネットワーク（Ｎ）を介して認証局（ＨＡ）に告知されることを特徴とする、請求項１から２３のいずれかに記載の方法。

【請求項２５】

ネットワーク（Ｎ）を介したデータ記憶媒体（ＩＭ）の多数のレベルでの初期化が提供され、これは、認証システム（Ａ）のフレームワーク内で、階層的に段階付けられたステップで行なわれることを特徴とする、請求項１から２４のいずれかに記載の方法。

【請求項２６】

ネットワーク（Ｎ）を介した認証により、請求項１に従って初期化されたアプリケーション（Ａｐｐ）を有する移動データ記憶媒体（ＩＭｊ）。

【請求項２７】

ネットワーク（Ｎ）を介した認証による、請求項１に記載の方法に従って初期化されたアプリケーション（ｋ）を有する読出および書込ステーション（ＷＲｋ）。

【請求項２８】

認証システム（Ａ）のフレームワーク内での、割当てられ分散された読出および書込ステーション（ＷＲ）を有する移動データ記憶媒体（ＩＭ）ならびに／または分散された読出および書込ステーション（ＷＲ）の初期化のためのインストールであって、初期化データ（ＤＩ，Ａ－Ｉ，Ｉ－Ｉ）は、安全な環境（ｇ）で認証局（ＨＡ）にある認証手段（ＡＭ）によって生成されかつ、認証システムに対応するセキュリティルールによっておよび安全な通信の中でネットワーク（Ｎ）を介して、分散され認証された読出および書込ステーション（Ａ－ＷＲ）に伝送され、読出および書込ステーション（Ａ－ＷＲ）にある移動データ記憶媒体（ＩＭ）は、初期化データ（ＤＩ）によって対応して初期化され（ＩＭｊ）ならびに／または、初期化データ（ＤＩ）は、ネットワーク（Ｎ）を介して、分散された読出および書込ステーション（ＷＲ）に伝送され、これにより、読出および書込ステーション（ＷＲ）が初期化される（ＷＲｋ）ことを特徴とする、インストール。

【発明の詳細な説明】

【０００１】

この発明は、請求項１の包括項目に従う認証システムのフレームワーク内での割当てられ分散された読出および書込ステーションによる移動データ記憶媒体の初期化のための方法に関する。移動データ記憶媒体（たとえば、接触型もしくは非接触型の識別媒体、チップカードまたは価値保有カードなど）は、サービス（ＰＣ－アクセス）および商品（飲料販売機、レストラン）へのアクセスまたは、保護区域、建物、スポーツ競技場などへのアクセスなどの、対応するアプリケーションを、割当てられた読出および書込ステーションでユーザが実行するのを可能にする。これらのアクセスまたはアプリケーションの実行を可能にするには、対応する初期化情報を用いた、認証システムのフレームワーク内での割当てられた読出および書込ステーションならびにデータ記憶媒体の初期化が必要である。

【０００２】

この初期化は、（たとえば、データ記憶媒体への貨幣価値の登録などの）特定用途向けデータと、（たとえば、カード発行者の数、アプリケーションが多数である場合のデータ構成、データ記憶媒体のアクセスルールなどの）システム特有のデータとに関し得る。また、これらの初期化データまたはアプリケーションは、時間とともに、段階的におよび異なる時点で、初期化されたり変更されたりし得る。

【０００３】

この初期化は、セキュリティにとって極めて重要なプロセスでありかつ非常に精巧なものであり、これはまた、地理的に非常に制限されかつ、安全な環境内の場所でのみ起こり得る。この例はＷＯ９７／３４２６５に記載されている。これは、認証システムＡのフレームワーク内に、割当てられた読出および書込ステーションＷＲを有する、識別媒体ＩＭとして非接触型受動型電子データ記憶媒体を有するシステムを記載している。データ記憶媒体はいくつかの独立したアプリケーションを含み得る。ここでは、あらゆる識別媒体およびあらゆるアプリケーションを、階層的認証システムのルールに従って初期化しなければ

ならない。データ記憶媒体のこの初期化のため、特別なプログラミング読出および書込ステーションならびに安全な環境の中の特別な認証媒体が必要であり、すべての分散された読出および書込ステーションも、それらの機能を果たし得るために、特別な認証手段で「洗礼」（ｂａｐｔｉｓｅｄ）または初期化され得る。

【０００４】

大体において安全ではない環境の中のこれらの分散された読出および書込ステーションでのデータ記憶媒体ＩＭの分散された初期化はここでは不可能である。初期化はこの理由のために非常に精巧でありかつ限定され、認証媒体の初期化および管理も、セキュリティという点で極めて重要でありかつ精巧でありかつ費用がかかる。

【０００５】

安全な環境の中での、特別な認証手段による各個別データ記憶媒体のこれらの公知の中央での初期化は、この理由のために、非常に精巧かつ高価であり、あまり柔軟性がなく非常に制限されている。それらを安全ではない環境で用いて、新たなアプリケーションおよび新たなデータ記憶媒体を初期化しかつ動作させることは不可能である。

【０００６】

異なる用途のために非接触型識別媒体がスキーパスとして発行される、たとえばスキー場の山間のレストランがたとえばお得意様用アプリケーションとしてその用途および顧客のために用途の拡大を加えたい場合、この目的のために、各個別のデータ記憶媒体、すなわちすべてのスキーパスを、初期化装置および対応の初期化媒体を用いて安全な環境の中で、すなわち、山間のレストランではなく、このスキー場の谷の中央ステーションに降りて、初期化しなければならない。当然ながらこの手順はそのような場合には実際的ではない。

【０００７】

構成全体およびすべての認証が単一のシステムセンターから来るものでなければならない接触型カードシステムの場合、ネットワークを介した全く異なる種類のデータ伝送が公知である。したがって、ＤＥ１９７　２０　４３１からの、たとえば、中央のチップカード管理システムからの、チップカードの電子的個別化および初期化のためのプロセスが公知である。これらの初期化は、物理的にチップカードと接触しかつチップカードにデータを直接に転送するチップカードコントロールシステムまたは読取装置への通信チャネルを通して行なわれる。この種類のシステムを用いても、以下に述べられる問題を解決することはできない。

【０００８】

したがって、本明細書に述べられるこの発明の目的は、データ記憶媒体ならびに分散された読出および書込ステーションの初期化、用途の拡大ならびに新たなデータ記憶媒体の発行に対する、これまでに該当するこれらの限定を克服しかつ、大幅に単純で、より用途が広く安全な初期化方法を形成し、これを用いて新たな用途の可能性も作り出しかつ、非接触型データ記憶媒体も特に利用可能にする、方法またはシステムを作成することである。

【０００９】

この問題は、請求項１に従う移動データ記憶媒体の初期化のための方法および請求項２８に従うインストールにより、この発明に従って解決される。安全な通信を用いたネットワークを介した初期化によっておよび、安全な環境のリモート認証局にある認証手段を用いた認証によって、移動データ記憶媒体と分散された読出および書込ステーションとを有するこのようなシステムの、述べられたさらなる適用および活用可能性が拡張されるのは明らかである。

【００１０】

従属する請求項は、新たなデータ記憶媒体の適用および導入に対するならびに新たな種類の活用、適用および使用に対する、地理的な面での可能性の拡張による、この発明のさらなる発展例に関する。ネットワークを介した安全な通信と、安全な環境の中の、認証手段を有するリモート認証局とのリンクとによってセキュリティが保証される限り、安全ではない環境の中のすべての分散された読出および書込ステーションも、それにより原則的に

、初期化に利用可能であることが明らかである。これは全く新しいタイプの用途を可能にする。たとえば、分散された読出および書込ステーションを介したライセンス支払の記録およびコントロールである。データ記憶媒体の所有者または読出および書込ステーションの所有者の個人データのさらなる照会も、分散された認証のセキュリティをさらに高めることができる。

【００１１】

以下、図面および例に基づいてこの発明がさらに詳細に説明される。

【００１２】

【詳細な説明】

図１－図３は、認証システムＡのフレームワーク内での割当てられ分散された読出および書込ステーションＷＲでの移動データ記憶媒体ＩＭの初期化のための、この発明に従う方法を図示する。これは、たとえば、ＷＯ９７／３４２６５中の非接触型識別媒体を有するシステムに基づいて記載されたものなどの、読出および書込ステーション、データ記憶媒体、認証局ならびに認証手段からなる完全なシステムに適用可能な階層的ルールを規定する。しかしながら、この公知のシステムは、この発明の適用例の可能な例としての役割しか果たさない。

【００１３】

この発明に従う方法が図３に図示される。割当てられ分散された読出および書込ステーションＡ－ＷＲによるならびに／または分散された読出および書込ステーションＷＲによる、移動データ記憶媒体ＩＭの初期化は、安全な環境ｇ中の認証局ＨＡにある認証手段ＡＭによる認証によって、すべてのシステム要素に適用可能な階層的認証システムＡのフレームワーク内で実現される。ここで、初期化データＤＩ＝Ａ－Ｉ，Ｉ－Ｉが生成されかつ、認証システムに対応するセキュリティルールを用いておよび安全な通信中でネットワークＮを介して、認証され分散された読出および書込ステーションＡ－ＷＲへまたは分散された読出および書込ステーションＷＲへ伝送される。このときの初期化データＤＩは認証情報Ａ－Ｉを含むが、これは、認証手段ＡＭおよび初期化情報Ｉ－Ｉによって認証局に入力され、これもまた、認証局ＨＡに入力されるかまたはそれから呼出される。

【００１４】

分散された読出および書込ステーションＡ－ＷＲでは、移動データ記憶媒体ＩＭが、初期化データＤＩで対応して初期化され、これにより初期化データ記憶媒体ＩＭｊに変換されるかまたは、初期化データＤＩにより、分散された読出および書込ステーションＷＲが初期化されて、初期化済読出および書込ステーションＷＲｋに変換される。

【００１５】

図１および図２は、安全でない環境ｕの中の分散された読出および書込ステーションＡ－ＷＲまでの、ネットワークＮを介した安全な通信を図示する。

【００１６】

図１の例ではこのとき、初期化は安全なプライベートネットワークＮｐを介して実現される。これにより、ちょうど読出および書込ステーションまで、安全な環境が保証される。

【００１７】

図２は、オープン公衆ネットワークを介した必要な安全な通信を確実にするため、両側で暗号化ならびにセキュリティゲートＧ１およびＧ２を用いたオープンネットワークＮｏを介した、この発明に従う初期化の例を図示する。

【００１８】

ネットワークＮを介した安全な接続により、安全でない環境に通常は位置する分散された読出および書込ステーションＷＲまたはＡ－ＷＲは、初期化のため、認証局ＨＡの安全な環境に結合される。これにより、初期化は安全な環境で行なわれる。初期化が実行された後、アプリケーションの実行を、これまでのように、安全でない環境の中の読出および書込ステーションＷＲで識別媒体ＩＭによって行なうことができる。したがって、ネットワークを介した安全な環境ｇを、初期化のために一時的に作り出すだけでよい。

【００１９】

図４－図６を用いて、異なる初期化プロセスがより詳細に図示される。図４では、まず、認証局ＨＡおよびＡＭの可能な実施例が図示される。

【００２０】

すべての初期化を実行しかつ管理しなければならない単一の中央認証および構成ステーション（システムセンター）を有する、たとえばＤＥ１９７　２０　４３１に従う、公知の接触型カードシステムに対して、この発明に従うシステムでは、認証システムＡのそのようなセンターは必要ではない。認証システムａはむしろ階層的認証ルールを順守することによってさらに規定される。これらの認証ルールは、たとえばチップ上にまたはプログラムとして、地理的に分散されたさまざまな認証局ＨＡｉのメモリに植込まれるかまたは記憶される。これらの認証ルールまたは認証手段ＡＭは、原則的に、地理的に分散された“バーチャル認証システムセンター”Ａを形成する。すべての読出および書込ステーションならびにすべての識別媒体の、システムＡへの加入（ａｆｆｉｌｉａｔｉｏｎ）が、基本的なシステム準備または基本的な初期化によって確実になる。

【００２１】

初期化情報Ｉ－Ｉ（Ａｐｐｉ）による新たなアプリケーションＡｐｐｉの初期化のため、認証情報Ａ－Ｉを用いた、構成レベルに対応する認証が必要である。認証手段ＡＭにより、認証システムＡに対応するこの認証情報Ａ－Ｉが認証局ＨＡに伝送される。

【００２２】

ここで、図４に従う認証局ＨＡは、たとえば、システムＡの対応する認証ルールを有するホストコンピュータＨからまたはリモート認証読出および書込ステーションＲ－Ａ－ＷＲから成り得る。たとえば、認証手段ＡＭは認証識別媒体ＡＭ－ＩＭを含み得るが、これは、たとえば、ソフトウェア（プログラム）としてホストＨでポーリング可能なまたは実行可能な、認証情報Ａ－Ｉまたは認証データＡＭ－Ｉを含むものである。物理的な認証媒体ＡＭ－ＩＭの場合、セキュリティ要件に対応する処理は、認証媒体の保持者（所有者）によって実行される。ホストＨ中のソフトウェアプログラムＡＭ－Ｉの場合、セキュリティは、たとえば、ＰＩＮコードもしくは生物測定的データによるまたは割当てられた特別な識別媒体（ＩＤ－ＡＭ）による、ユーザの識別によって確実になる。

【００２３】

図４にはデータ記憶媒体ＩＭの初期化が図示される。ここで、認証情報Ａ－Ｉ（ｊ）は、データ記憶媒体ＩＭの初期化ｊのための認証に関する。新たなアプリケーションＡｐｐｉのための初期化情報Ｉ－Ｉ（Ａｐｐｉ）は、認証局ＨＡに入力され、生成されまたはそれによって呼出されかつ、記載のように、ネットワークおよび分散された読出および書込ステーションＡ－ＷＲを介してデータ記憶媒体の中で初期化される。すなわち（Ａｐｐｉを有する）ＩＭｊである。

【００２４】

図５は、読出および書込ステーションＷＲの初期化ｋを図示する。認証情報は、認証手段ＡＭにより認証局ＨＡによって入力され、作成されまたは呼出される。初期化情報Ｉ－Ｉ（ｋ）も入力認証局の中に入力される。読出および書込ステーションＷＲの初期化のためすなわちネットワークを介したＷＲｋへの変換のために、まず、認証情報Ａ－Ｉ（ｋ）が認証局ＨＡから読出および書込ステーションＷＲに伝送される。ここで、その後に、初期化情報Ｉ－Ｉ（ｋ）の伝送が実現される。データ記憶媒体上での新たなアプリケーションの初期化に類似して、読出および書込ステーションＷＲの初期化も、対応する初期化データＩ－Ｉ（ｋ）によって実行され得る。これにより、たとえば、さらなる機能を読出および書込ステーションに導入することができる。

【００２５】

図６は、分散された読出および書込ステーションＷＲを、認証された読出および書込ステーションＡ－ＷＲに変換または初期化し、それによりここで移動データ記憶媒体ＩＭの初期化を実行可能であるのを図示する。これを達成するため、読出および書込ステーションＷＲを認証機能ＦＡで予め初期化しなければならない。まず、認証情報Ａ－Ｉ－ＦＡを認証手段ＡＭによって認証局ＨＡの中に入力しなければならない。ここで、認証機能ＦＡに

よる、認証された読出および書込ステーションＡ－ＷＲへの分散された読出および書込ステーションＷＲの初期化または変換が実行される。その後、あるアプリケーションＡｐｐｉのための認証情報Ａ－Ｉ（ｊ）および対応する初期化情報Ｉ－Ｉ（Ａｐｐｉ）によって、移動データ記憶媒体ＩＭ中で、ネットワークならびに認証され分散された読出および書込ステーションＡ－ＷＲを介して、これまでのように（図４）アプリケーションの初期化が実現され得る。すなわち、Ｉ－Ｉ（Ａｐｐｉ）を有するＩＭｊである。

【００２６】

この認証機能ＦＡを永久的に活性化する必要はなく、それを、再び取消したりまたは、ネットワークリンクともしくはある期間の後もしくはある数の初期化の後で、中断したりすることができる。その結果、認証された読出および書込ステーションＡ－ＷＲは、通常の分散された読出および書込ステーションＷＲに変換されて戻る。

【００２７】

図４－図６には、ネットワークＮを介して初期化または実行可能なさらなる可能な機能が図示される。

【００２８】

認証されたもしくは分散された読出および書込ステーションＡ－ＷＲ、ＷＲでのならびに／または移動データ記憶媒体ＩＭでのイベントに関するステータス情報Ｓ－Ｉは、ネットワークを介して、対応する認証局に通知され得る。そこでは、たとえば、使用およびライセンスの費用のインボイス作成または決済のために利用される。この例は後に説明される。

【００２９】

識別認証手段ＩＤ－ＡＭによる初期化のための、合法的なユーザの認証のさらなるオプションとして、その人の識別ＩＤ－Ｉ（図４、図５、図１４）を検出することが可能である。

【００３０】

絶対的に必須なのは、ネットワークを介した初期化データＤＩの安全な通信である。それにより、移動データ記憶媒体を有する完全なシステムのセキュリティが、ネットワークを介したデータ伝送によって損なわれることはない。

【００３１】

プライベートネットワークＮｐ、たとえば企業の専用ネットワークを介した通信の場合は、この必要なセキュリティが与えられている。

【００３２】

公衆ネットワークＮｏを介した初期化データの伝送の場合、この目的のため、そのような公知の手段（暗号化およびさらなるセキュリティファクタ）による安全な通信が保証されなければならない。これは、公衆ネットワークとプライベートネットワークとの組合せを介した通信にも当てはまる。これにより、原則的に、（ＬＡＮ、ＷＡＮ、インターネット、イントラネットおよびエクストラネットなどの）いずれのネットワークも初期化データの伝送に利用可能である。この発明に従う初期化は、たとえば企業ネットワークとして公衆電気通信ネットワークを利用する仮想プライベートネットワークすなわちプライベートデータネットワークを介しても行なわれ得る。暗号化およびトンネリングメカニズムにより、認証済ユーザだけが、たとえばインターネットＩＰ（インターネットプロトコル）、ＶＰＮ（仮想プライベートネットワーク）を介してアクセスを得るのが確実になる。

【００３３】

必須であるのは、この通信のセキュリティ度が初期化または初期化データの重要性に対応して保証されることである。ネットワークを介した通信については、原則的に、ネットワークに対する外部セキュリティおよび認証システム中の内部セキュリティのこの両者が、階層的規定およびアプリケーションの重要性に対応する異なる階層レベルＯＬｉを区別する。全体的に、アプリケーションまたは初期化の重要性に対応するセキュリティが、外部および内部セキュリティの両者として保証されなければならない。当然ながら、ネットワークに対する外部セキュリティは、必要な内部セキュリティよりも低いものであってはな

らない。
【００３４】
たとえば、重要性または認証の異なるレベルとは以下のものであろう。
スーパーマーケットの顧客カードへの、お客様用ボーナスなどの付加アプリケーションのローディングは比較的低いセキュリティレベルしか求めない。なぜなら、未認証の行為による潜在的な損害はわずかだからである。一方で、たとえば、ＥＤＰデータシステムまたは全く新しいデータ記憶媒体の初期化および何よりも貨幣量の記入において、秘密性が最も高い利用レベルに対するアクセス認証には高いセキュリティレベルが求められる。
【００３５】
図７は、認証システムＡのフレームワーク内に、各々がそれぞれ対応する認証手段ＡＭ１、ＡＭ２、ＡＭ３を有するいくつかの認証局ＨＡ１、ＨＡ２、ＨＡ３を有する例を図示する。これは、ネットワークＮ１、Ｎ２、Ｎ３を介して、対応する割当てられ認証された読出および書込ステーションＡ－ＷＲに、それらの初期化データＤＩ１、ＤＩ２、ＤＩ３を有するそれら自身の独立したアプリケーションＡｐｐ１、Ａｐｐ２、Ａｐｐ３を伝送する。ここで、移動データ記憶媒体ＩＭがそれぞれ初期化される。このときネットワークは異なってもよく、たとえばＮ１はオープン公衆ネットワークであり、Ｎ２はプライベートネットワークであり、または、２つもしくはそれ以上の認証局が、同じネットワークを、しかしそれら自身のセキュリティルールによって利用してもよい。当然ながら、読出および書込ステーションは認証局に対応しなければならない。すなわち、この例では、読出ステーションＡ－ＷＲ２は認証局ＨＡ３にのみアクセス可能である。すなわち、対応するアプリケーションＡｐｐ３をもってそれに割当てられる。一方、この例の読出および書込ステーションＡ－ＷＲ１は、それらのそれぞれのアプリケーションＡｐｐ１、Ａｐｐ２、Ａｐｐ３を備えてすべての３つの認証局ＨＡ１、ＨＡ２、ＨＡ３に割当てられかつアクセス可能である。同じことは、それらのアプリケーションの初期化の対応する可能性を有する１つまたはそれ以上の認証局にも割当てられる、移動データ記憶媒体ＩＭの割当にも当てはまる。
【００３６】
図８－図１１は、いくつかの認証局ＨＡおよび認証手段ＡＭならびにいくつかのまたは異なる認証レベルＯＬｉを有する、いくつかのネットワークまたは（同じネットワーク内の）いくつかのネットワークレベルを介した初期化のさらなる例を図示する。
【００３７】
図８は、いくつかの認証局ＨＡ１、ＨＡ２と、認証手段ＡＭ１、ＡＭ２と、異なるアプリケーションＡｐｐ１、Ａｐｐ２とを有する例を図示する。対応する初期化データＤＩ１、ＤＩ２は、データ記憶媒体ＩＭｊ中の２つのアプリケーションＡｐｐ１、Ａｐｐ２の初期化のため、１つのレベルで同じネットワークを介して、分散され認証された読出および書込ステーションＡ－ＷＲに伝送される。これは、認証レベルＯＬｉとは独立して（認証局ＨＡｉ、認証手段ＡＭｉ、アプリケーションＡｐｐｉの異なるＯＬｉに対しても）起こり得る。
【００３８】
図８と類似の図９は、アプリケーションＡｐｐｉのためのいくつかの認証局ＨＡおよび認証手段ＡＭを図示する。しかしながらここでは、認証された読出および書込ステーションＡ－ＷＲに対する初期化はいくつかのネットワークレベルＮ１、Ｎ２を介して起こる。ネットワークレベルＮ１およびＮ２は、同じまたは異なるネットワークでも形成され得る。認証局ＨＡ１の、Ｉ－Ｉ１を有するアプリケーションＡｐｐ１はここで、ネットワークレベルＮ１を通って認証局ＨＡ２の中へ向かい、さらにネットワークレベルＮ２を通って、認証された読出および書込ステーションの中まで不変である。認証局ＨＡ２でのアプリケーションＡｐｐ２は、ネットワークレベルＮ２を通ってのみ導かれる。これもまた、認証レベルＯＬｉから独立している。
【００３９】
図１０は、いくつかの認証局、アプリケーションおよびネットワークレベルを有する、図

９と同様のさらなる例を示す。ここで、たとえば、ＯＬｎ上のアプリケーションＡｐｐ１およびＯＬｎ＋１上のアプリケーションＡｐｐ２などの異なる認証レベル上の２つのアプリケーションが図示される。認証局ＨＡ１のアプリケーションＡｐｐ１を有するこの例は、認証局ＨＡ２の中のＩ－Ｉ１＋にそれを補足可能であり、それにより、データ記憶媒体ＩＭｊ中の対応するアプリケーションがこのアプリケーションＡｐｐ１＋に対応することを図示する。

【００４０】

認証局中のアプリケーションのこの変更または補足に類似して、読出および書込ステーションＡ－ＷＲ中の、図４に従うＩ－Ｉ＋に初期化情報を変更するかまたは補足することも可能である。

【００４１】

図１１は、たとえばＯＬｉ＝ＯＬ０からＯＬ５などのいくつかの認証または構成レベルを有し、異なる認証レベル上にいくつかの認証局ＨＡを有しかつ独立したアプリケーションＡｐｐ１、Ａｐｐ２、Ａｐｐ３を有するいくつかの独立したユーザＨＡ１、ＨＡ２、ＨＡ３を有する、認証システムＡ内の構成を概略的に図示する。最も高い構成レベルＯＬ０は、（たとえばシステムデータフィールドＣＤＦを介した）すべての読出および書込ステーションならびにすべてのデータ記憶媒体ＩＭの基本的初期化が、異なる認証局ＨＡｉ０またはこれらに割当てられた認証局ＨＡｉ０．１を介して、認証システムＡへの加入という意味で行なわれるレベルに対応する。システムの認証ルールは、構成レベルＯＬ１上の対応する独立したユーザの独立したアプリケーションＡｐｐ１、Ａｐｐ２、Ａｐｐ３の独立性および相互の無影響性を保証する。次の認証レベルＯＬ２からＯＬ５のように、たとえば、独立したユーザは、その人自身、二次的なサブ認証システムＡＳを有する認証システムＡのフレームワーク内で自分のアプリケーションを構成しかつ規定することができる。ＯＬ２からのようなこれらのレベル上でも、認証局ＨＡを対応する認証手段ＡＭによって形成可能であり、地理的に分散されたさまざまな認証局ＨＡの間で、対応するネットワーク接続および初期化をネットワークレベルを介して実現することができる。これは、説明されたルールに従う。

【００４２】

認証システムＡを用いると、このとき、さまざまな認証局のアプリケーションが互いから独立しかつ相互に影響しないことが確実になる。データ記憶媒体の中にいくつかの独立したアプリケーションを有する例が図１３にさらに図示される。その中では何よりも、非接触型でかつ受動型の識別媒体またはデータ記憶媒体も利用可能であり、これらは距離をおいて、たとえば入口ゲートで、読出および書込ステーションと通信することもできる。

【００４３】

この発明に従うと、異なる種類の初期化および対応して異なるセキュリティ要件を有するものが認証システムＡの中で実現可能である。この文脈において図１２は、高い階層レベルおよびセキュリティ要件の例を図示する。この場合、システムに対応して準備された空の移動データ記憶媒体がアプリケーションとともに新たに初期化される。このデータ記憶媒体ＩＭはこのとき、システムデータフィールドＣＤＦ中の認証システムＡのシステムデータを介して準備され、これがシステムＡへの加入を規定しかつ保証するが、しかしながら、この目的のために準備されたアプリケーションデータフィールドにはまだ一切のアプリケーションを含まない。このアプリケーションデータフィールド中のアプリケーションＡｐｐの新たな初期化情報Ｉ－Ｉによる新たな初期化ＤＩは、第１の上位初期化レベルを表わす。

【００４４】

図１３は、認証局ＨＡ３の初期化データＤＩ３による、さらなる新たなアプリケーション、ここではたとえばアプリケーションＡｐｐ３の初期化を図示する。

【００４５】

さらなる例として、図１３は、対応する初期化データＤＩ２．２による、既存のアプリケーションＡｐｐ２に加えた、認証局ＨＡ２のアプリケーション拡張Ａｐｐ２．２に対する

初期化を図示する。これは、以下の例の山間のレストランに基づき、いくつかの独立したアプリケーションＡｐｐ１、Ａｐｐ２、Ａｐｐ３を有しかつ認証システムＡに対応する固定データ部分ＣＤＦを有する、データ記憶媒体ＩＭの中にデータ構成を有する、図１３のデータ記憶媒体について図示される。アプリケーションＡｐｐ１はたとえばスキーのリフトであり、アプリケーションＡｐｐ２は山間のレストランである。これは、そのアプリケーションＡｐｐ２．２のさらなる拡張を導入する希望がありかつ、対応する初期化ＤＩ２．２を用いて、ネットワークを介してその読出および書込ステーションＡ－ＷＲを介して山間のレストランのその場で直接に、ゲストの既存のスキーパスまたはデータ記憶媒体ＩＭにこれを記すことができる。ゲストは、この目的のため、これまでそうであったように、認証媒体をもって（アプリケーションＡｐｐ１としてのスキーパス発行者の）認証された読出および書込ステーションへ谷を降りて行く必要はない。

【００４６】

さらなる例として、スキーパスを持って夕方谷を降りる同じゲストは、これがその人のデータ記憶媒体に設定済でなければ、たとえばスポーツ施設へのアクセスなどの、認証局ＨＡ３の初期化データＤＩ３で新たに初期化されるさらなる独立したアプリケーションＡｐｐ３を有し得る。

【００４７】

実施例のさらなる変形としての図１２は、アプリケーションプログラムデータＩ－Ｉ－Ｃｏｄを含むアプリケーションマイクロプロセッサＡｐｐｕＰを含む移動データ記憶媒体を図示する。集積化されたインテリジェンスを有するこの種類のデータ記憶媒体の場合、アプリケーションの組合せを実現可能であるが、これらは、一部は読出および書込ステーションＷＲに含まれ、一部はデータ記憶媒体ＩＭに含まれる。それらはユーザ認証ａｉ（図１４）の処理を可能にする。

【００４８】

この発明に従う初期化は、好適な安全なネットワークを介して、新たな用途およびビジネスモデルを可能にすることができる。たとえば、以下のようなものなどのステータス情報Ｓ－Ｉの利用による、初期化リンクされたビジネスモデルなどである。すなわち、

１．新たに初期化されるデータ記憶媒体および新たに初期化されるアプリケーションのライセンス費用の借方記入（ｄｅｂｉｔｉｎｇ）。データ記憶媒体ＩＭ中の新たなアプリケーションまたは新たなデータ記憶媒体のすべての初期化のたびに、対応して合意されたライセンス費用が、認証局ＨＡにおいてネットワークを介して借方記入される。

【００４９】

２．あらゆる使用に対するライセンス費用借方記入。読出および書込ステーションでデータ記憶媒体がアプリケーションを利用すれば、この使用について、ライセンス費用が認証局ＨＡ（たとえばホストＨ）によって課され得る。これは、読出および書込ステーションＷＲがネットワークを介してオンラインで認証局ＨＡと永久的に接続されたままである場合に連続して決済されてもよくまたは、ネットワークを介した接続は周期的に起こってもよい。このとき使用データＳ－Ｉは、読出および書込ステーションＷＲのメモリに記憶されかつ認証局ＨＡと周期的に交換され決済され得る。

【００５０】

したがって、この発明に従う、ネットワークを介した初期化およびそれと関連の通信は、アプリケーションに依存して、永久的なネットワーク接続によってまたは周期的にのみ起こり得る。このとき、たとえば、時間が限られた有効性を有するアプリケーションは、再び、対応する周期的初期化（たとえば月ごと）によって、時間を更新され得る。

【００５１】

図１４はネットワークを介した可能な初期化の異なる変形例を図示する。ここで、初期化は、初期化通信もしくは利用通信ならびに／または、認証局ＨＡと、認証読出および書込ステーションＡ－ＷＲと、識別媒体もしくはデータ記憶媒体ＩＭとの間の識別通信も含む。初期化は認証局ＨＡによって始まってもよくまたは、それは読出および書込ステーションＡ－ＷＲによってもしくはデータ記憶媒体ＩＭの所有者によって要求されてもよい。そ

のために、新たな初期化またはアプリケーションのタイプに依存して、読出および書込ステーションの所有者１２またはデータ記憶媒体の所有者１３のユーザ認証すなわち合致が必要である。これは、認証手段としての、たとえば、読出および書込ステーションの所有者１２の個人データ（ａｗ）または、ＰＩＮコード、生体測定的データなどの、データ記憶媒体の所有者１３の個人データ（ａｉ）であり得る。同じことが、データ記憶媒体による読出および書込ステーションでのアプリケーションの実行にも当てはまる。したがって、認証およびその利用のタイプに依存して、

読出および書込ステーションによるもしくはその所有者１２による初期化のためのユーザ認証ａｗ、

または、データ記憶媒体の所有者１３による初期化のためのユーザ認証ａｉが行なわれてもよく、

またはさらなる識別認証手段ＩＤ－ＡＭによる初期化のための認証も行なわれてもよい。

【００５２】

実施例の例は、たとえば、カード読取装置としての読出および書込ステーションでのキャッシュカードのローディングである。ここでは、データ記憶媒体としてのキャッシュカードの所有者が自分の認証すなわちユーザ認証ａｉ（たとえばクレジットカード番号およびＰＩＮコード）を用いて、ＰＣおよびインターネットを介してお金をロードすることも可能である。

【００５３】

この発明に従う方法を用いると、たとえば、認証Ａに対応して階層的に段階分けされたいくつかのステップで、多数の段階の初期化をネットワークを介して実行することも可能である。これは、図１１を参照して、データ記憶媒体としてのチップカードの分散された製造および流通の例によって図示される。この例での認証システムＡの所有者は、たとえば、データフィールドＣＤＦを有する基本システム構成を含むブランクカードまたはデータ記憶媒体ＩＭを作成する本拠地およびセンターをヨーロッパに有する製造者ＨＡ０である。これらのブランクカードは、ネットワークを介して、たとえば合衆国内の企業駐在事務所としての子会社ＨＡ０．１に送られ、ここで、最も高い認証局としての製造者のセンターＨＡ０によってカードのさらなる基本的初期化を実行することができる。子会社ＨＡ０．１は、認証局ＨＡ１、ＨＡ２、ＨＡ３を表わす、独立したアプリケーションを有するこれらのカードを独立したユーザに配布し、そのカードはユーザコードによって区別される。これは、子ＨＡ０．１がそうする権限を与えられていなければ、センターＨＡ０により、子会社ＨＡ０．１でネットワークを介して初期化可能である。ＨＡ０およびＨＡ０．１はＯＬ０のレベルにある。これは以下の初期化レベルを生じる。

【００５４】

ＨＡ０　－＞　ＨＡ０．１　－＞　ＨＡ１

階層の次のレベルでは、ここではこれらのカードＦＭは、分散された読出および書込ステーションＡ－ＷＲで再び、さらなる構成レベルを介して、必要なアプリケーションＡｐｐ１、Ａｐｐ２、Ａｐｐ３とともに認証局ＨＡ１、ＨＡ２、ＨＡ３（すなわち独立したユーザ）によって初期化される。システムＡの初期化および認証ルールならびに階層的段階付けにより、認証システムＡの所有者ＨＡ０はカードのシステム互換性に対するコントロールを維持することができかつ、独立したユーザＨＡ１、ＨＡ２などについては、割当てられた構成レベル（たとえばＯＬ１）のように、その認証局のフレームワーク内のそのアプリケーションを有するカードに対するコントロールを保つことが保証される。これは、構成レベルＯＬ１からＯＬｎまでの上に、さらなる初期化レベルを生じる。たとえば、

ＨＡ１　－＞　ＨＡ１．１　－＞　ＨＡ１．１１　－＞　Ａ－ＷＲ／ＩＭである。

【００５５】

独立したアプリケーションを有する独立したユーザＨＡ１、ＨＡ２、ＨＡ３なども構成レベルＯＬ１上にある。

【００５６】

示された例および説明により、非接触型システムおよび識別媒体について、この発明に従

う新たな方法の普遍的な適用可能性が何よりも図示されるであろう。

【図面の簡単な説明】

【図１】プライベートネットワークを介したデータ記憶媒体の初期化のための、この発明に従う方法の概略図である。

【図２】オープン公衆ネットワークを介したデータ記憶媒体の初期化のための方法の図である。

【図３】認証手段を有する認証局での認証による、ネットワークを介した、データ記憶媒体ならびに分散された読出および書込ステーションの初期化のための、この発明に従う方法の図である。

【図４】認証および初期化情報による、移動データ記憶媒体の初期化の図である。

【図５】認証および初期化情報による、分散された読出および書込ステーションの初期化の図である。

【図６】分散された読出および書込ステーションでの認証機能の初期化の図である。

【図７】いくつかの認証局によるネットワークを介したアプリケーションの初期化の図である。

【図８】ネットワークを介したいくつかの認証局による初期化の図である。

【図９】いくつかのネットワークレベルを介したいくつかの認証局による初期化の図である。

【図１０】いくつかの認証レベルを有するいくつかのネットワークレベルを介した、いくつかの認証局による初期化の図である。

【図１１】異なる認証レベル上の、いくつかの認証または構成レベル、いくつかの認証局と、いくつかの独立したユーザとを有する、認証システムの中の構成を概略的に示す図である。

【図１２】新たなデータ記憶媒体の中のアプリケーションの初期化の図である。

【図１３】データ記憶媒体の中のさらなるアプリケーションの初期化の図である。

【図１４】ネットワークを介したデータ記憶媒体の初期化のための認証の図である。

【国際公開パンフレット】

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
17. Januar 2002 (17.01.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/05225 A1

(51) Internationale Patentklassifikation⁷: G07F 7/10

(21) Internationales Aktenzeichen: PCT/CH01/00433

(22) Internationales Anmeldedatum:
10. Juli 2001 (10.07.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
1365/00 11. Juli 2000 (11.07.2000) CH

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: KABA SCHLIESSSYSTEME AG [CH/CH]; Mühlebühlstrasse 23, CH-8620 Wetzikon (CH).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: KLOSA, Klaus, Ulrich [DE/CH]; Dürnterstrasse 50, CH-8627 Grüningen (CH); EPPENBERGER, Roman [CH/CH]; Hinterhofstrasse 5, CH-8635 Dürnten (CH).

(74) Anwalt: FREI PATENTANWALTSBÜRO; Postfach 768, CH-8029 Zürich (CH).

(81) Bestimmungsstaaten *(national)*: AE, BR, CA, CN, ID, IN, JP, MX, SG, US, ZA.

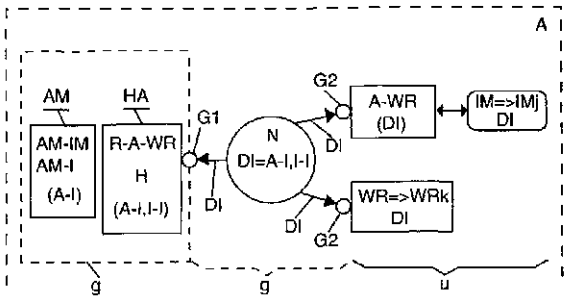
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD FOR THE INITIALISATION OF MOBILE DATA SUPPORTS

(54) **Bezeichnung:** VERFAHREN ZUR INITIALISIERUNG VON MOBILEN DATENTRÄGERN



(57) **Abstract:** The invention relates to a method for the initialisation of mobile data supports (IM) on dedicated decentralised read/write stations (WR), within the frame of an authorisation system (A). Initialisation data (DI, A-I, I-I) are created in an authorisation process (HA) in a secure environment (g) by means of authorisation means (AM) and sent to a decentralised authorised read/write station (A-WR) over a network (N) in a secure communication, according to security rules corresponding to the authorisation system (A). The mobile data support (IM) is initialised with the initialisation data (DI) and/or the initialisation data is sent over the network to a decentralised read/write station (WR), whereupon the read/write station is initialised. The above initialisation method permits new application and use possibilities for said systems.

[Fortsetzung auf der nächsten Seite]

WO 02/05225 A1

WO 02/05225 A1

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Mit dem Verfahren werden mobile Datenträger (IM) an zugeordneten dezentralen Schreib- und Lesestationen (WR) im Rahmen eines Autorisierungssystems (A) initialisiert. An einer Autorisierungsinstanz (HA) in einer gesicherten Umgebung (g) werden durch Autorisierungsmittel (AM) Initialisierungsdaten (DI, A-I, I-I) erzeugt und über ein Netzwerk (N) in einer gesicherten Kommunikation und mit dem Autorisierungssystem (A) entsprechenden Sicherheitsregeln an eine dezentrale autorisierte Schreib- und Lesestation (A WR) gesendet, wo die mobilen Datenträger (IM) mit den Initialisierungsdaten (DI) initialisiert werden, und/oder wobei die Initialisierungsdaten über das Netzwerk an eine dezentrale Schreib- und Lesestation (WR) gesendet werden, womit die Schreib- und Lesestation initialisiert wird. Dieses Initialisierungsverfahren ermöglicht neue Anwendungs- und Nutzungsmöglichkeiten solcher Systeme.

VERFAHREN ZUR INITIALISIERUNG VON MOBILEN DATENTRÄGERN

Die Erfindung betrifft ein Verfahren zur Initialisierung von mobilen Datenträgern mit zugeordneten dezentralen Schreib- und Lesestationen im Rahmen eines Autorisierungssystems gemäss Oberbegriff von Patentanspruch 1. Mobile Datenträger (z.B. kontaktlose oder kontaktbehaftete Identifikationsmedien, Chipkarten oder Wertkarten usw.) ermöglichen dem Benutzer an zugeordneten Schreib- und Lesestationen die Ausübung von entsprechenden Applikationen wie den Zugriff auf Dienstleistungen (PC-Zugang) und Waren (Getränkeautomat, Restaurant) bzw. den Zugang zu geschützten Bereichen, Gebäuden, Sportstadien usw. Um diese Zugriffe bzw. die Ausübung von Applikationen zu ermöglichen ist die Initialisierung der Datenträger und der zugeordneten Schreib- und Lesestationen im Rahmen eines Autorisierungssystems mit entsprechenden Initialisierungsinformationen notwendig.

Diese Initialisierung kann sich auf anwendungsspezifische Daten (z.B. Aufbuchen eines Geldwerts auf den Datenträger) und auf systemspezifische Daten (z.B. Nummer des Kartenherausgebers, Datenorganisation bei Multi-Applikationen, Zugriffsregeln auf Datenträger etc.) beziehen. Diese Initialisierungsdaten bzw. Applikationen können auch nach und nach, stufenweise und zu unterschiedlichen Zeitpunkten initialisiert und auch geändert werden.

Diese Initialisierung ist ein sicherheitskritischer und sehr aufwändiger Prozess, der auch örtlich stark eingeschränkt ist und nur an Orten in gesicherter Umgebung stattfinden kann. Ein Beispiel dazu ist in der WO 97/34265 beschrieben. Diese beschreibt ein System mit berührungslosen passiven elektronischen Datenträgern als Identifikationsmedien IM mit zugeordneten Schreib- und Lesestationen WR im Rahmen eines Autorisierungssystems A, wobei die Datenträger mehrere unabhängige Applikationen enthalten können. Hier muss jedes Identifikationsmedium und jede Anwendung gemäss den Regeln des hierarchischen Autorisierungssystem initialisiert werden. Für diese Initialisierung der Datenträger werden spezielle Programmier-Schreib- und Lesestationen sowie spezielle Autorisierungsmedien in gesicherter Umgebung benötigt und alle dezentralen Schreib- und Lesestationen können ebenfalls mit einem speziellen Autorisierungsmittel getauft bzw. initialisiert werden, um ihre Funktionen aufnehmen zu können.

Eine dezentrale Initialisierung von Datenträgern IM an diesen dezentralen Schreib- und Lesestationen meist in ungesicherter Umgebung ist hier nicht möglich. Die Initialisierung ist deshalb sehr aufwändig und eingeschränkt und die Initialisierung und Verwaltung der Autorisierungsmedien ist ebenfalls sicherheitskritisch und aufwändig.

Diese bekannten zentralen Initialisierungen eines jeden einzelnen Datenträgers mit speziellen Autorisierungsmitteln in gesicherter Umgebung ist deshalb sehr aufwändig, wenig flexibel und sehr eingeschränkt. Es können damit nicht dezentral in ungesicherter Umgebung neue Anwendungen und neue Datenträger initialisiert und in Gebrauch genommen werden.

Wenn beispielsweise ein Bergrestaurant in einem Skigebiet, in dem für verschiedene Applikationen berührungslose Identifikationsmedien als Skikarten ausgegeben sind, für seine Applikation und für seine Kunden eine Anwendungserweiterung, beispielsweise eine Loyality-Anwendung, in seiner Applikation hinzufügen möchte, so muss dazu jeder einzelne Datenträger, d.h. jede Skikarte, mit einem Initialisierungsgerät in einer gesicherten Umgebung und mit einem entsprechenden Initialisierungsmedium initialisiert werden, d.h. nicht im Bergrestaurant sondern im Tal unten an der Zentrale in diesem Skigebiet. Diese Vorgehensweise ist hier natürlich nicht praktikabel.

Eine ganz andere Art von Datenübertragung über ein Netz ist bei Kontaktkarten-Systemen bekannt, wo die ganze Organisation und alle Autorisierungen von einer einzigen Systemzentrale ausgehen müssen. So ist aus der DE 197 20 431 z.B. ein Verfahren zur elektronischen Personalisierung und Initialisierung von Chipkarten von einem zentralen Chipkarten-Administrationssystem aus bekannt. Diese Initialisierungen erfolgen über einen Kommunikationskanal an ein Chipkarten-Kontrollsystem bzw. Lesegerät, welches die Chipkarte physikalisch kontaktiert und die Daten direkt an die Chipkarte weiterleitet. Auch mit solchen Systemen ist die nachstehende Aufgabe nicht lösbar.

Es ist daher Aufgabe der vorliegenden Erfindung, ein Verfahren bzw. ein System zu schaffen, welches diese bisherigen Beschränkungen bezüglich der Initialisierung von Datenträgern und dezentralen Schreib- und Lesestationen, der Erweiterung von Applikationen und der Ausgabe von neuen Datenträgern überwindet, welches eine wesentlich einfachere, vielseitigere und sichere Initialisierungsmethode bildet und damit auch neue Einsatzmöglichkeiten schafft, und welches insbesondere auch die Anwendung von berührungslosen Datenträgern ermöglicht.

Diese Aufgabe wird erfindungsgemäss gelöst durch ein Verfahren zur Initialisierung von mobilen Datenträgern gemäss Patentanspruch 1 und eine Anlage nach Patentanspruch 28. Durch die Initialisierung über ein Netz mit gesicherter Kommunikation und mit Autorisierungen durch Autorisierungsmittel an entfernten Autorisierungsinstanzen in gesicherter Umgebung werden die erwähnten weiteren Anwendungs- und Nutzungsmöglichkeiten solcher Systeme mit mobilen Datenträgern und dezentralen Schreib- und Lesestationen ganz entscheidend erweitert.

Die abhängigen Patentansprüche betreffen Weiterentwicklungen der Erfindung mit Erweiterung der Möglichkeiten in örtlicher Hinsicht, bezüglich Applikationen und Einführung neuer Datenträger und bezüglich neuer Arten von Nutzung, Einsatz und Anwendung. Entscheidend ist, dass damit im Prinzip auch alle dezentralen Schreib- und Lesestationen in ungeschützter Umgebung für Initialisierungen einsetzbar sind, indem die Sicherheit durch die gesicherte Kommunikation über das Netz und durch die Anbindung an die entfernte Autorisierungsinstanz mit Autorisierungsmitteln in geschützter Umgebung gewährleistet wird. Dies ermöglicht auch ganz neue Anwendungsarten, beispielsweise eine Erfassung und Kontrolle von Lizenzzahlungen über dezentrale Schreib- und Lesestationen, die zusätzliche Abfrage persönlicher Daten vom Inhaber des Datenträgers oder des Inhabers der Schreib- und Lesestation kann die Sicherheit dezentraler Autorisierungen weiter erhöhen.

Im folgenden wird die Erfindung anhand von Figuren und Beispielen weiter erläutert. Es zeigen:

Fig. 1 ein Schema eines erfindungsgemässen Verfahrens zur Initialisierung von Datenträgern über ein privates Netzwerk,

Fig. 2 ein Verfahren zur Initialisierung von Datenträgern über ein offenes Netzwerk,

Fig. 3 das erfindungsgemässe Verfahren zur Initialisierung von Datenträgern und von dezentralen Schreib- und Lesestationen über ein Netzwerk durch Autorisierung an einer Autorisierungsinstanz mit Autorisierungsmitteln,

Fig. 4 die Initialisierung eines mobilen Datenträgers mit Autorisierungs- und Initialisierungsinformationen,

Fig. 5 eine Initialisierung einer dezentralen Schreib- und Lesestation mit Autorisierungs- und Initialisierungsinformationen,

Fig. 6 die Initialisierung einer Autorisierungsfunktion an einer dezentralen Schreib- und Lesestation,

Fig. 7 Initialisierungen von Applikationen über Netzwerke durch mehrere Autorisierungsinstanzen,

Fig. 8 Initialisierungen durch mehrere Autorisierungsinstanzen über ein Netzwerk,

Fig. 9 Initialisierungen durch mehrere Autorisierungsinstanzen über mehrere Netzstufen,

Fig. 10 Initialisierungen durch mehrere Autorisierungsinstanzen über mehrere Netzstufen mit mehreren Autorisierungsstufen,

Fig. 11 schematisch die Organisation in einem Autorisierungssystem mit mehreren Autorisierungs- bzw. Organisationsstufen, mehreren Autorisierungsinstanzen auf verschiedenen Autorisierungsstufen und mit mehreren unabhängigen Anwendern,

Fig. 12 die Initialisierung von Applikationen in einem neuen Datenträger,

Fig. 13 die Initialisierung von zusätzlichen Applikationen in einem Datenträger,

Fig. 14 Autorisierungen zur Initialisierung von Datenträgern über ein Netzwerk.

Die Fig. 1 - 3 illustrieren das erfindungsgemässe Verfahren zur Initialisierung von mobilen Datenträgern IM an zugeordneten dezentralen Schreib- und Lesestationen WR im Rahmen eines Autorisierungssystems A, das für das ganze System von Schreib- und Lesestationen, Datenträgern, Autorisierungsinstanzen und Autorisierungsmitteln gültige hierarchische Regeln festlegt, wie dies beispielsweise an einem System mit berührungslosen Identifikationsmedien in der WO 97/34265 beschrieben ist. Dieses bekannte System dient jedoch nur als ein mögliches Anwendungsbeispiel der Erfindung.

Das erfindungsgemässe Verfahren wird in Fig. 3 illustriert: Die Initialisierung von mobilen Datenträgern IM mit zugeordneten dezentralen Schreib- und Lesestationen A-WR und/oder von dezentralen Schreib- und Lesestationen WR erfolgt im Rahmen

eines für alle Systemelemente gültigen hierarchischen Autorisierungssystem A durch eine Autorisierung mit Autorisierungsmitteln AM an einer Autorisierungsinstanz HA in einer gesicherten Umgebung g, wo Initialisierungsdaten DI = A-I, I-I erzeugt und über ein Netzwerk N in einer gesicherten Kommunikation und mit dem Autorisierungssystem entsprechenden Sicherheitsregeln an eine dezentrale autorisierte Schreib- und Lesestation A-WR oder an eine dezentrale Schreib- und Lesestation WR gesendet werden. Die Initialisierungsdaten DI enthalten dabei Autorisierungsinformationen A-I, die von den Autorisierungsmitteln AM in die Autorisierungsinstanz eingegeben werden und Initialisierungsinformationen I-I, die auch in die Autorisierungsinstanz HA eingegeben oder aus dieser abgerufen werden.

An der dezentralen Schreib- und Lesestation A-WR werden die mobilen Datenträger IM mit den Initialisierungsdaten DI entsprechend initialisiert und damit in initialisierte Datenträger IMj übergeführt,
oder mit den Initialisierungsdaten DI wird die dezentrale Schreib- und Lesestation WR initialisiert und in eine initialisierte Schreib- und Lesestation übergeführt: WRk.

Die Fig. 1 und 2 illustrierten die gesicherte Kommunikation über ein Netzwerk N bis zu den dezentralen Schreib- und Lesestationen A-WR in ungesicherter Umgebung u.

Im Beispiel von Fig. 1 erfolgt dabei die Initialisierung über ein gesichertes privates Netzwerk Np, womit die gesicherte Umgebung bis an die Schreib- und Lesestationen gewährleistet wird.

Fig. 2 zeigt ein Beispiel der erfindungsgemässen Initialisierung über ein offenes Netz No mit einer Verschlüsselung und beidseitigen Sicherheitspforten G1 und G2, um die notwendige gesicherte Kommunikation über das offene Netz zu gewährleisten.

Durch die gesicherte Verbindung über das Netzwerk N werden die dezentralen Schreib- und Lesestationen WR bzw. A-WR, die sich normalerweise in ungesicherter Umgebung u befinden, in die gesicherte Umgebung der Autorisierungsinstanz HA eingebunden für die Initialisierungen und damit findet die Initialisierung in gesicherter Umgebung g statt. Nachdem die Initialisierung ausgeführt ist, kann die Ausführung von Applikationen mit den Identifikationsmedien IM an den Schreib- und Lesestationen WR wieder wie bisher in ungesicherter Umgebung stattfinden. Die gesicherte Umgebung g über das Netz muss also nur temporär für die Initialisierung hergestellt werden.

Mit den Fig. 4 – 6 werden verschiedene Initialisierungsvorgänge genauer dargestellt. In Fig. 4 werden zuerst mögliche Ausführung von Autorisierungsinstanzen HA und Autorisierungsmitteln AM illustriert.

Im Unterschied zu bekannten Kontaktkartensystemen, z.B. gemäss DE 197 20 431 mit einer einzigen zentralen Autorisierungs- und Organisationsstelle (Systemzentrale), von der aus alle Initialisierungen ausgeführt und verwaltet werden müssen, ist im erfindungsgemässen System keine solche Zentrale des Autorisierungssystems A notwendig. Das Autorisierungssystem A wird vielmehr durch die Einhaltung von hierarchischen Autorisierungsregeln bestimmt, wobei diese Autorisierungsregeln in verschiedenen örtlich verteilten Autorisierungsinstanzen HAi z.B. auf einem Chip oder als Programm implantiert und gespeichert sind. Diese Autorisierungsregeln bzw. die Autorisierungsmittel AM bilden im Prinzip eine

örtlich verteilte "virtuelle Autorisierungssystem-Zentrale" A. Die Zugehörigkeit zum System A für alle Schreib- und Lesestationen und alle Identifikationsmedien wird durch eine System-Grundvorbereitung oder Grundinitialisierung sichergestellt.

Zur Initialisierung einer neuen Applikation Appi mit den Initialisierungsinformationen I-I(Appi) ist eine der Organisationsstufe entsprechende Autorisierung mit den Autorisierungsinformationen A-I erforderlich. Mit den Autorisierungsmitteln AM werden diese dem Autorisierungssystem A entsprechenden Autorisierungsinformationen A-I an die Autorisierungsinstanz HA übermittelt.

Die Autorisierungsinstanzen HA können dabei gemäss Fig. 4 z.B. aus einem Hostcomputer H mit den entsprechenden Autorisierungsregeln des Systems A oder auch aus einer entfernten Autorisierungs- Schreib- und Lesestation R-A-WR bestehen. Die Autorisierungsmittel AM können beispielsweise bestehen aus einem Autorisierungs-Identifikationsmedium AM-IM, das die Autorisierungsinformationen A-I enthält oder aus Autorisierungsdaten AM-I, die z.B. als Software (Programm) in einem Host H abgerufen bzw. ausgeführt werden kann. Bei einem physikalischen Autorisierungsmedium AM-IM erfolgt die den Sicherheitsanforderungen entsprechende Handhabung durch den Träger (Inhaber) des Autorisierungsmediums. Im Falle von Softwareprogrammen AM-I in einem Host H wird die Sicherheit gewährleistet durch eine Identifikation des Benützers, z.B. mittels PIN Code oder biometrischen Daten oder durch ein zugeordnetes spezielles Identifikationsmedium (ID-AM).

In Fig. 4 ist die Initialisierung eines Datenträgers IM dargestellt. Dabei bezieht sich die Autorisierungsinformation A-I(j) auf die Autorisierung für die Initialisierung j eines Datenträgers IM. Die Initialisierungsinformationen I-I(Appi) für eine neue Applikation Appi werden in die Autorisierungsinstanz HA eingegeben, erzeugt oder

abgerufen und wie beschrieben über das Netz und die dezentralen autorisierten Schreib- und Lesestation A-WR im Datenträger IM initialisiert: IMj (mit Appi).

Fig. 5 zeigt die Initialisierung k einer Schreib- und Lesestation WR. Die Autorisierungsinformationen A-I(k) werden vom Autorisierungsmittel AM der Autorisierungsinstanz HA eingegeben, erzeugt oder abgerufen. Die Initialisierungsinformation I-I(k) wird ebenfalls in die Autorisierungsinstanz eingegeben. Zur Initialisierung der Schreib- und Lesestation WR, d.h. zur Überführung in eine WRk über ein Netzwerk wird zuerst die Autorisierungsinformation A-I(k) von der Autorisierungsinstanz HA auf die Schreib- und Lesestation WR übertragen, worauf anschliessend die Übertragung der Initialisierungsinformation I-I(k) erfolgt. In Analogie zur Initialisierung von neuen Applikationen auf einem Datenträger kann auch eine Initialisierung der Schreib- und Lesestation WR durch entsprechende Initialisierungsdaten I-I(k) erfolgen, mit denen beispielsweise zusätzliche Funktionen in der Schreib- und Lesestation eingeführt werden können.

Fig. 6 zeigt die Überführung bzw. Initialisierung einer dezentralen Schreib- und Lesestation WR in eine autorisierte Schreib- und Lesestation A-WR, um damit Initialisierungen von mobilen Datenträgern IM ausführen zu können. Dazu muss die Schreib- und Lesestation WR zuerst mit der Autorisierungsfunktion FA initialisiert werden. Zuerst muss die Autorisierungsinformation A-I-FA von einem Autorisierungsmittel AM in die Autorisierungsinstanz HA eingegeben werden, worauf die Initialisierung bzw. die Überführung der dezentralen Schreib- und Lesestation WR in eine autorisierte Schreib- und Lesestation A-WR mit Autorisierungsfunktion FA ausgeführt wird. Anschliessend kann die Initialisierung von Applikationen wie bisher (Fig. 4) durch die Autorisierungsinformation A-I(j) für eine bestimmte

Applikation Appi und die entsprechende Initialisierungsinformation I-I(Appi) über das Netzwerk und die dezentrale autorisierte Schreib- und Lesestation A-WR im mobilen Datenträger IM vorgenommen werden: IMj mit I-I(Appi).

Diese Autorisierungsfunktion FA muss nicht permanent aktiviert sein, sie kann auch wieder gelöscht werden, bzw. mit der Netzverbindung unterbrochen oder nach einer bestimmten Zeit oder einer bestimmten Anzahl von Initialisierungen gelöscht werden, wodurch die autorisierte Schreib- und Lesestation A-WR wieder in eine gewöhnliche dezentrale Schreib- und Lesestation WR zurückgeführt wird.

In den Fig. 4 – 6 sind weitere mögliche Funktionen dargestellt, die über das Netzwerk N initialisiert bzw. ausgeführt werden können.

Statusinformationen S-I über Ereignisse an den autorisierten bzw. an den dezentralen Schreib- und Lesestationen A-WR, WR und/oder an den mobilen Datenträgern IM können über das Netzwerk an entsprechende Autorisierungsinstanzen gemeldet und dort beispielsweise für Nutzungs- und Lizenzverrechnungen eingesetzt werden. Beispiele dazu werden später erläutert.

Als weitere Option ist es möglich, als Autorisierung eines rechtmässigen Benutzers für eine Initialisierung mit einem Identifikations-Autorisierungsmittel ID-AM dessen Identifikation ID-I zu überprüfen (Fig. 4, 5, 14).

Ganz wesentlich ist die gesicherte Kommunikation der Initialisierungsdaten DI über das Netzwerk, so dass die Sicherheit des gesamten Systems mit den mobilen

Datenträgern nicht durch die Daten-Übertragung über das Netzwerk beeinträchtigt wird.

Bei einer Kommunikation über private Netzwerke Np, z.B. über Firmennetzwerke, ist diese gewünschte Sicherheit gegeben.

Bei Übertragung der Initialisierungsdaten über öffentliche Netze No muss dafür eine gesicherte Kommunikation mit an sich bekannten Mitteln (Verschlüsselung und weiteren Sicherheitsfaktoren), gewährleistet werden. Dies gilt auch für eine Kommunikation über eine Kombination von offenen und privaten Netzwerken. Damit können im Prinzip beliebige Netze zur Übertragung der Initialisierungsdaten verwendet werden (wie LAN, WAN, Internet, Intranet und Extranet etc.).
Die erfindungsgemässe Initialisierung kann auch über ein virtuelles privates Netzwerk erfolgen, d.h. ein privates Datennetzwerk, das öffentliche Telecommunikationsnetze benützt, z.B. als Firmennetzwerk, wobei Verschlüsselungs- und Tunneling-Mechanismen sicherstellen, dass nur autorisierte Anwender Zugang erhalten, z.B. über das Internet IP (Internetprotokoll), VPM (Virtual Private Networks).

Wesentlich ist, dass der Sicherheitsgrad dieser Kommunikation der Wichtigkeit der Initialisierung bzw. der Initialisierungsdaten entsprechend gewährleistet wird.
Dies sowohl bezüglich der Kommunikation über das Netz, im Prinzip die äussere Sicherheit bezüglich dem Netz, wie auch bezüglich der inneren Sicherheit im Autorisierungssystem A, welches verschiedene hierarchische Stufen OLi entsprechend der hierarchischen Definition und der Wichtigkeit der Anwendungen unterscheidet. Insgesamt muss eine der Wichtigkeit der Applikationen bzw. der Initialisierungen entsprechende Sicherheit sowohl als äussere wie auch als innere

Sicherheit gewährt werden. Wobei natürlich die äussere Sicherheit bezüglich dem Netz nicht kleiner sein sollte als die gewünschte innere Sicherheit.

Unterschiedliche Wichtigkeits- bzw. Autorisierungsstufen können beispielsweise sein:

Das Laden einer zusätzlichen Applikation wie eine Treueprämie auf einer Kundenkarte eines Supermarkts erfordert nur eine relativ geringe Sicherheitsstufe, da der potentielle Schaden durch unautorisierte Handlungen gering ist. Anderseits erfordert z.B. die Zugangsberechtigung für Nutzungsstufen höchster Geheimhaltung in einem EDV-Datensystem oder die Initialisierung ganz neuer Datenträger und vor allem das Aufbuchen von Geldbeträgen eine hohe Sicherheitsstufe.

Fig. 7 illustriert nun ein Beispiel mit mehreren Autorisierungsinstanzen HA1, HA2, HA3 mit je den entsprechenden Autorisierungsmitteln AM1, AM2, AM3 im Rahmen des Autorisierungssystems A, welche ihre eigenen unabhängigen Applikationen App1, App2, App3 mit ihren Initialisierungsdaten DI1, DI2, DI3 über Netzwerke N1, N2, N3 an entsprechende zugeordnete autorisierte Schreib- und Lesestationen A-WR senden, bei denen die mobilen Datenträger IM entsprechend initialisiert werden. Dabei können die Netzwerke unterschiedlich sein, z.B. N1 ein offenes Netz und N2 ein privates Netz, oder es können auch zwei oder mehr Autorisierungsinstanzen das selbe Netzwerk, jedoch mit ihren eigenen Sicherheitsregeln, verwenden. Natürlich müssen die Schreib- und Lesestationen der Autorisierungsinstanz entsprechen, d.h. in diesem Beispiel ist die Lesestation A-WR2 nur der Autorisierungsinstanz HA3 zugänglich, d.h. dieser zugeordnet mit entsprechenden Applikationen App3, während die Schreib- und Lesestation A-WR1 in diesem Beispiel allen drei Autorisierungsinstanzen HA1, HA2, HA3 mit ihren entsprechenden Applikationen App1, App2, App3 zugeordnet und zugänglich ist. Analoges gilt für die Zuordnung der mobilen Datenträger IM, die auch einer oder mehreren Autorisierungsinstanzen mit entsprechender Möglichkeit zur Initialisierung von deren Applikationen zugeordnet sind.

Die Fig. 8 – 11 illustrieren weitere Beispiele von Initialisierungen über mehrere Netzwerke bzw. über mehrere Netzstufen (auch im gleichen Netz) mit mehreren Autorisierungsinstanzen HA und Autorisierungsmitteln AM sowie mit mehreren bzw. verschiedenen Autorisierungsstufen OLi.

Fig. 8 zeigt ein Beispiel mit mehreren Autorisierungsinstanzen HA1, HA2 mit Autorisierungsmitteln AM1, AM2 und mit verschiedenen Applikationen App1, App2. Die entsprechenden Initialisierungsdaten DI1, DI2 werden über das gleiche Netzwerk in einer Stufe an die dezentralen autorisierten Schreib- und Lesestationen A-WR übermittelt zur Initialisierung von beiden Applikationen App1, App2 in den Datenträgern IMj. Dies kann unabhängig von der Autorisierungsstufe OLi (auch für verschiedene OLi der Autorisierungsinstanzen HAi, der Autorisierungsmittel AMi, der Applikationen Appi) erfolgen.

Fig. 9 zeigt analog zu Fig. 8 mehrere Autorisierungsinstanzen HA und Autorisierungsmittel AM für Applikationen Appi, wobei jedoch die Initialisierung über mehrere Netzstufen N1, N2 auf die autorisierten Schreib- und Lesestationen A-WR erfolgt. Die Netzstufen N1 und N2 können im gleichen oder auch in verschiedenen Netzen gebildet werden. Die Applikation App1 mit I-I1 der Autorisierungsinstanz HA1 geht hier über die Netzstufe N1 in die Autorisierungsinstanz HA2 und unverändert weiter über die Netzstufe N2 in die autorisierte Schreib- und Lesestation. Die Applikation App2 an der Autorisierungsinstanz HA2 wird nur über die Netzstufe N2 geleitet. Auch dies ist unabhängig von der Autorisierungsstufe OLi.

Fig. 10 zeigt ein weiteres Beispiel ähnlich Fig. 9 mit mehreren Autorisierungsinstanzen, Applikationen und Netzstufen, wobei hier zwei Applikationen auf unter-

schiedlicher Autorisierungsstufe dargestellt sind, wie z.B. die Applikation App1 auf OLn und die Applikation App2 auf OLn+1. Dieses Beispiel zeigt an der Applikation App1 der Autorisierungsinstanz HA1, dass diese in der Autorisierungsinstanz HA2 auch ergänzt werden kann in I-I1+, so dass die entsprechende Applikation im Datenträger IMj dieser Applikation App1+ entspricht.

In Analogie zu dieser Veränderung oder Ergänzung einer Applikation in der Autorisierungsinstanz kann auch in einer Schreib- und Lesestation z.B. nach Fig. 4 in der autorisierten Schreib- und Lesestation A-WR eine Initialisierungsinformation verändert oder ergänzt werden in I-I+.

Fig. 11 zeigt schematisch die Organisation in einem Autorisierungssystem A mit mehreren Autorisierungs- bzw. Organisationsstufen z.B. OLi = OL0 bis OL5, mit mehreren Autorisierungsinstanzen HA auf verschiedenen Autorisierungsstufen und mit mehreren unabhängigen Anwendern HA1, HA2, HA3 mit den unabhängigen Applikationen App1, App2, App3. Die oberste Organisationsstufe OL0 entspricht der Stufe auf welcher eine Grundinitialisierung aller Schreib- und Lesestationen und aller Datenträger IM (z.B. über das Systemdatenfeld CDF) im Sinne einer Zugehörigkeit zum Autorisierungssystem A durch verschiedene Autorisierungsinstanzen HAi0 oder diesen zugeordnete Autorisierungsinstanzen HAi0.1 erfolgt. Die Autorisierungsregeln des Systems sichern die Unabhängigkeit und gegenseitige Nicht-Beeinflussbarkeit der unabhängigen Anwendungen App1, App2, App3 der entsprechenden unabhängigen Anwender auf Organisationsstufe OL1. Ab der nächsten Autorisierungsstufe OL2 bis OL5 z.B. kann ein unabhängiger Anwender seine Applikationen im Rahmen des Autorisierungssystems A mit einem sekundären Unterautorisierungssystem AS selber organisieren und festlegen. Auch auf diesen Stufen ab OL2 können Autorisierungsinstanzen HA mit den entsprechenden Autorisierungsmitteln AM gebildet werden und zwischen den

verschiedenen, örtlich verteilten Autorisierungsinstanzen HA können entsprechende Netzverbindungen und Initialisierungen über Netzstufen realisiert werden, gemäss den erläuterten Regeln.

Mit dem Autorisierungssystem A wird dabei gesichert, dass die Applikationen der verschiedenen Autorisierungsinstanzen unabhängig voneinander und gegenseitig nicht beeinflussbar sind. Ein Beispiel mit mehreren unabhängigen Applikationen in einem Datenträger wird in Fig. 13 weiter illustriert. Dabei sind vor allem auch berührungslose und passive Identifikationsmedien bzw. Datenträger einsetzbar, die auch auf Distanz mit einer Schreib- und Lesestation kommunizieren können, z.B. an Eintrittspforten.

Es können erfindungsgemäss verschiedene Arten von Initialisierungen über Netzwerke durchgeführt werden mit unterschiedlichen hierarchischen Stufen im Autorisierungssystem A und entsprechend unterschiedlicher Sicherheitsanforderung. Fig. 12 zeigt dazu ein Beispiel hoher hierarchischer Stufe und Sicherheitsanforderung, bei dem ein systementsprechend vorbereiteter leerer mobiler Datenträger neu mit Applikationen initialisiert wird. Dieser Datenträger IM ist dabei durch Systemdaten des Autorisierungssystems A in einem Systemdatenfeld CDF vorbereitet, welcher die Zugehörigkeit zum System A festlegt und sicherstellt, der jedoch noch keine Applikationen in einem dafür vorbereiteten Applikationsdatenfeld ADF enthält. Die Neuinitialisierung DI mit den Initialisierungsinformationen I-I von Applikationen App in diesem Applikationsdatenfeld ADF stellt eine erste obere Initialisierungsstufe dar.

Fig. 13 illustriert die Initialisierung von zusätzlichen neuen Applikationen, hier z.B. der Applikation App3, mit Initialisierungsdaten DI3 einer Autorisierungsinstanz HA3.

Als weiteres Beispiel zeigt Fig. 13 die Initialisierung einer Applikationserweiterung App2.2 einer Autorisierungsinstanz HA2 zusätzlich zur bestehenden Applikation App2 mittels entsprechender Initialisierungsdaten DI2.2. Dies wird am folgenden Beispiel Bergrestaurant für den Datenträger von Fig. 13 illustriert mit einer Datenorganisation in einem Datenträger IM mit mehreren unabhängigen Applikationen App1, App2, App3 und mit einem dem Autorisierungssystem A entsprechenden festen Datenteil CDF. Die Applikation App1 seien z.B. Skilifte, die Applikation App2 das Bergrestaurant, das eine zusätzliche Erweiterung seiner Applikation App2.2 einführen möchte und das diese mit einer entsprechenden Initialisierung DI2.2 über das Netz direkt an Ort, im Bergrestaurant über seine Schreib- und Lesestation A-WR auf eine schon bestehende Skikarte bzw. Datenträger IM eines Gastes einschreiben kann - ohne dass dieser dazu ins Tal an eine autorisierte Schreib- und Lesestation (des Herausgebers der Skikarte als Applikation App1) mit Autorisierungsmedium fahren muss, wie dies bisher notwendig war.

Als weiteres Beispiel könnte derselbe Gast mit seiner Skikarte am Abend im Tal unten eine weitere unabhängige Applikation App3, z.B. Zutritt zu Sportanlagen, neu initialisieren lassen mit Initialisierungsdaten DI3 der Autorisierungsinstanz HA3, wenn diese auf seinem Datenträger noch nicht eingerichtet ist.

Fig. 12 zeigt als weitere Ausführungsvariante einen mobilen Datenträger, der einen Applikationsmicroprozessor AppuP aufweist, welcher Applikationsprogramm-Daten I-I-Cod enthält. Mit solchen Datenträgern mit integrierter Intelligenz können kombinierte Applikationen realisiert werden, welche teilweise in der Schreib- und

Lesestation WR und teilweise im Datenträger IM enthalten sind und sie erlauben die Handhabung von Nutzerautorisierungen ai (Fig. 14).

Die erfindungsgemässe Initialisierung über ein passendes gesichertes Netz kann ganz neue Anwendungen und Business-Modelle ermöglichen, z.B. initialisierungsgebundene Businessmodelle durch Verwendung von Status-Informationen S-I, z.B.:

1. Lizenzverrechnung für neu initialisierte Datenträger und neu initialisierte Applikationen: Bei jeder Initialisierung eines neuen Datenträgers oder einer neuen Applikation in einem Datenträger IM wird über das Netz bei der Autorisierungsinstanz HA eine entsprechende vereinbarte Lizenzgebühr verrechnet.

2. Lizenzverrechnung für jede Nutzung: Wenn eine Applikation von einem Datenträger an einer Schreib- und Lesestation genutzt wird, so kann für diese Nutzung von der Autorisierungsinstanz HA (z.B. einem Host H) eine Lizenzgebühr erhoben werden.
Dies kann entweder laufend abgerechnet werden, falls die Schreib- und Lesestation WR online über das Netz mit der Autorisierungsinstanz HA verbunden bleibt, oder die Verbindung über das Netz kann periodisch erfolgen. Dann können die Nutzungsdaten S-I in der Schreib- und Lesestation WR gespeichert und periodisch mit der Autorisierungsinstanz HA ausgetauscht und abgerechnet werden.

Die erfindungsgemässe Initialisierung über das Netz und die damit verbundene Kommunikation kann also je nach Anwendung sowohl mit einer dauernden Netzverbindung oder auch nur periodisch erfolgen. Dabei könnten beispielsweise

zeitlich begrenzte Applikationen durch entsprechende periodische Initialisierungen immer wieder erneuert werden (z.B. monatlich).

Fig. 14 illustriert verschiedene Varianten möglicher Initialisierungen über ein Netzwerk, wobei die Initialisierungen auch eine Initialisierungskommunikation, bzw. eine Nutzungskommunikation und / oder eine Identifikationskommunikation zwischen Autorisierungsinstanz HA, autorisierter Schreib- und Lesestation A-WR und Identifikationsmedium bzw. Datenträger IM enthalten. Eine Initialisierung kann von der Autorisierungsinstanz HA ausgehen oder sie kann auch von der Schreib- und Lesestation A-WR oder vom Inhaber des Datenträgers IM angefordert werden. Dazu ist je nach Art der neuen Initialisierung bzw. der Applikation auch eine Nutzerautorisierung, d.h. das Einverständnis des Inhabers 12 der Schreib- und Lesestation bzw. des Inhabers 13 des Datenträgers notwendig, welche als Autorisierungsmittel beispielsweise persönliche Daten des Inhabers 12 der Schreib- und Lesestation (aw) bzw. persönliche Daten (ai) des Inhabers 13 des Datenträgers sein können wie PIN-Codes, biometrische Daten usw. Analoges gilt auch für die Ausübung von Applikationen an der Schreib- und Lesestation durch den Datenträger. Je nach Art der Autorisierung und von deren Nutzung kann somit

eine Nutzerautorisierung aw zur Initialisierung durch die Schreib- und Lesestation bzw. deren Inhaber 12 erfolgen

oder es kann eine Nutzerautorisierung ai zur Initialisierung durch den Inhaber 13 des Datenträgers erfolgen

oder es kann auch eine Autorisierung zur Initialisierung durch ein zusätzliches Identifikations-Autorisierungsmittel ID-AM erfolgen.

Ein Ausführungsbeispiel sei z.B. das Aufladen von Geldkarten an einer Schreib- und Lesestation als Karten-Lesegerät. Hier kann vom Inhaber einer Geldkarte als Datenträger mit seiner Berechtigung, d.h. Nutzerautorisierung ai (z.B. Kreditkartennummer und PIN-Code) über einen PC und das Internet auch Geld aufgeladen werden.

Mit dem erfindungsgemässen Verfahren können auch mehrstufige Initialisierungen über Netzwerke ausgeführt werden, z.B. in mehreren dem Autorisierungssystem A entsprechend hierarchisch abgestuften Schritten. Dies illustriert ein Beispiel dezentraler Herstellung und Distribution von Chip-Karten als Datenträger mit Bezug auf Fig. 11. Der Inhaber des Autorisierungs-Systems A sei ein Hersteller HA0 mit Hauptsitz und Zentrale in Europa, wo leere Karten bzw. Datenträger IM produziert werden, welche beispielsweise die Systemgrundorganisation mit dem Datenfeld CDF enthalten. Diese leeren Karten werden über ein Netzwerk an Tochterfirmen HA0.1 als Ländervertretungen, z.B. in den USA, geschickt, wo eine weitere Grundinitialisierung der Karten auch von der Herstellerzentrale HA0 aus als oberster Instanz ausgeführt werden kann. Die Tochterfirma HA0.1 vertreibt diese Karten mit unabhängigen Applikationen an unabhängige Anwender, welche die Autorisierungsinstanzen HA1, HA2, HA3 darstellen und deren Karten durch einen Anwendercode unterschieden werden, welcher über das Netz bei der Tochterfirma HA0.1 durch die Zentrale HA0 initialisiert werden kann, falls die Tochter HA0.1 dazu nicht berechtigt ist. HA0 und HA0.1 sind auf Stufe OL0. Dies ergibt folgende Initialisierungsstufen

HA0 -> HA0.1 -> HA1

Auf einer nächsten Hierarchiestufe werden dann diese Karten IM durch die Autorisierungsinstanzen HA1, HA2, HA3 (d.h. die unabhängigen Anwender) mit ihren gewünschten Applikationen App1, App2, App3 über weitere Organisationsstufen wiederum an dezentralen autorisierten Schreib- und Lesestationen A-WR initialisiert. Durch Initialisierungs- und Autorisierungsregeln und hierarchische Abstufungen des Systems A wird sichergestellt, dass der Inhaber HA0 des Autorisierungssystems A die Kontrolle über die Systemkompatibilität der Karten behalten kann und gleichzeitig für einen unabhängigen Anwender HA1, HA2 usw., dass er die Kontrolle über Karten mit seinen Applikationen im Rahmen seiner Befugnisse ab dem zugeordneten Organisationslevel (z.B. OL1) behält. Dies ergibt weitere Initialisierungsstufen, z.B.

HA1 -> HA1.1 -> HA1.11 -> A-WR/IM

auf Organisationsstufen OL1 bis OLn.

Die unabhängigen Anwender HA1, HA2, HA3 usw. mit den unabhängigen Applikationen sind auch auf dem Organisationslevel OL1.

Mit den angegebenen Beispielen und Ausführungen soll die universelle Einsetzbarkeit des erfindungsgemässen neuen Verfahrens vor allem auch für berührungslose Systeme und Identifkationsmedien illustriert werden.

Im Rahmen dieser Beschreibung werden die folgenden Bezeichnungen verwendet:

N	Netzwerk
No	öffentliches Netzwerk

Np	privates Netzwerk
G1, G2	Sicherheitspforten für gesicherte Kommunikation über das Netz
g	gesicherte Umgebung
u	ungesicherte Umgebung
IM	mobiler Datenträger, Identifikationsmedium
IMj	initialisierter IM
WR	dezentrale Schreib- und Lesestation
WRk	initialisierte WR
j	bezieht sich auf IM
k	bezieht sich auf WR
A-WR	dezentrale autorisierte Schreib- und Lesestation
A	Autorisierungssystem
AS	sekundäres Unterautorisierungssystem
AM	Autorisierungsmittel
AM-IM	Autorisierungs-Identifikationsmedien
AM-I	Autorisierungsdaten
HA	Autorisierungsinstanz, entfernte
H	Hostcomputer
R-A-WR	entfernte Autorisierungs-Schreib- und Lesestation
DI	Initialisierungsdaten
A-I	Autorisierungsinformationen
A-I-FA	Autorisierungsdaten für die Funktion A-WR
I-I	Initialisierungsinformationen
I-I-Cod	Applikationsprogramm-Daten
ID-AM	Identifikations-Autorisierungsmittel
ID-I	Identifikations-Informationen
S-I	Status-Informationen
OLi	Autorisierungsstufe, Organisationslevel
App	Applikationen

AppuP	Applikationsmicroprozessor
CDF	Grunddatenfeld, Grundorganisation von A
ADF	Applikationsdatenfeld
I2	Inhaber von WR
I3	Inhaber von IM
aw	Nutzerautorisierung von WR
ai	Nutzerautorisierung von IM
H0	Systeminhaber
H0.1	Tochtergesellschaft von H0

PATENTANSPRÜCHE

1. Verfahren zur Initialisierung von mobilen Datenträgern (IM) mit zugeordneten dezentralen Schreib- und Lesestationen (WR) und/oder von dezentralen Schreib- und Lesestationen (WR) im Rahmen eines Autorisierungssystems (A), dadurch gekennzeichnet, dass durch eine Autorisierung mit Autorisierungsmitteln (AM) an einer Autorisierungsinstanz (HA) in einer gesicherten Umgebung (g) Initialisierungsdaten (DI, A-I, I-I) erzeugt und über ein Netzwerk (N) in einer gesicherten Kommunikation und mit dem Autorisierungssystem entsprechenden Sicherheitsregeln an eine dezentrale autorisierte Schreib- und Lesestation (A-WR) gesendet werden
und wobei die mobilen Datenträger (IM) an der Schreib- und Lesestation (A-WR) mit den Initialisierungsdaten (DI) entsprechend initialisiert werden (IMj)
und/oder dass die Initialisierungsdaten (DI) über das Netzwerk (N) an eine dezentrale Schreib- und Lesestation (WR) gesendet werden, womit die Schreib- und Lesestation initialisiert wird (WRk).

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Autorisierungsinstanz (HA) durch einen Hostcomputer (H) oder durch eine entfernte Autorisierungs-Schreib- und Lesestation (R-A-WR) gebildet wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Autorisierungsmittel (AM) durch spezielle Autorisierungs- Identifikationsmedien (AM-IM) oder durch Autorisierungsdaten (AM-I) gebildet werden.

4. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass eine (nicht autorisierte) dezentrale Schreib- und Lesestation (WR) durch in den Initialisierungsdaten (DI) enthaltene Funktions-Autorisierungsdaten (A-I-FA) zuerst in eine autorisierte Schreib- und Lesestation (A-WR) übergeführt wird, welche anschliessend mobile Datenträger (IM) entsprechend den Initialisierungsdaten initialisieren kann.

5. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass im Rahmen des Autorisierungssystems (A) mehrere Autorisierungsinstanzen (HAi) mit gleichen und/oder unterschiedlichen Autorisierungsstufen (OLi) vorgesehen sind.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass mehrere Autorisierungsmittel (AMi) mit gleichen und/oder unterschiedlichen Autorisierungsstufen (OLi) vorgesehen sind.

7. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass Initialisierungsdaten (DI, A-I, I-I) über mehr als eine Netzstufe (N1, N2) und/oder über mehr als eine Autorisierungsinstanz (HA1, HA2) an die autorisierten Schreib- und Lesestationen (A-WR) bzw. die dezentralen Schreib- und Lesestationen (WR) übermittelt werden.

8. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Inititalisierungsdaten (DI) über ein gesichertes privates Netzwerk (Np) übermittelt werden.

9. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Initialisierungsdaten über ein offenes Netzwerk

(No) mit einer Verschlüsselung und beidseitigen Sicherheitspforten (G1, G2) übermittelt werden.

10. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass mit den Initialisierungsdaten (DI2.2) Applikationserweiterungen (App2.2) initialisiert werden.

11. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass mit den Initialisierungsdaten (DI3) neue unabhängige Applikationen (App3) initialisiert werden.

12. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass in einem, mit einem Systemdatenfeld (CDF) vorbereiteten leeren mobilen Datenträger mit den Initialisierungsdaten (DI) Applikationen (App) neu initialisiert werden.

13. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass über das Netzwerk (N) eine dauernde Verbindung zwischen Autorisierungsinstanz (HA) und dezentralen Schreib- und Lesestation (A-WR, WR) besteht.

14. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Verbindung zwischen Autorisierungsinstanz (HA) und dezentralen Schreib- und Lesestationen (A-WR, WR) über das Netzwerk (N) nur zeitweise besteht und dabei ein Datenaustausch stattfindet.

15. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass für die Initialisierung eine Nutzer-Autorisierung (aw) durch die Schreib- und Lesestation (A-WR, WR) bzw. deren Inhaber (12)

erfolgt und/oder ein Identifikations-Autorisierungsmittel (ID-AM) notwendig ist.

16. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass für eine Initialisierung eine Nutzer-Autorisierung (ai) durch den Datenträger bzw. den Inhaber (13) des Datenträgers erfolgt.

17. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass zur Autorisierung von Initialisierungen über das Netzwerk (N), wie auch zur Ausübung von Applikationen an der Schreib- und Lesestation (A-WR, WR) bzw. am Datenträger (IM) persönliche Daten (aw) des Inhabers der Schreib- und Lesestation bzw. persönliche Daten (ai) des Inhabers des Datenträgers, wie PIN-Code oder biometrische Daten, als Autorisierungsmittel eingesetzt werden.

18. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die mobilen Datenträger (IM) einen Applikations-Mikroprozessor (AppuP) zur Verarbeitung von Applikations-Programmdaten (I-I-Cod) enthalten.

19. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Datenträge (IM) als berührungslose, aktive oder passive Identifikationsmedien ausgebildet sind.

20. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die mobilen Datenträger (IM), die Autorisierungs-Identifikationsmedien (AM-IM) und die Identifikations-Autorisierungsmedien (ID-AM) aus den gleichen mobilen Datenträgern gebildet werden.

21. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass Statusinformationen (S-I) über Ereignisse an den autorisierten bzw. an den dezentralen Schreib- und Lesestationen (A-WR, WR) und/oder an den mobilen Datenträgern (IM) über das Netzwerk (N) an eine entsprechende Autorisierungsinstanz (HA) gemeldet werden.

22. Verfahren nach Anspruch 21, dadurch gekennzeichnet, dass die Statusinformationen (S-I) für Nutzungs- oder Lizenzverrechnungen verwendet werden.

23. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass jede neue Initialisierung eines Datenträgers (IM) für eine Nutzungs- oder Lizenzverrechnung über das Netzwerk (N) an die Autorisierungsinstanz (HA gemeldet wird.

24. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass jede Nutzung einer Applikation an einer Schreib- und Lesestation (WR) für eine Nutzungs- oder Lizenzverrechung über das Netzwerk (N) an die Autorisierungsinstanz (HA) gemeldet wird.

25. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass eine mehrstufige Initialisierung der Datenträger (IM) über Netzwerke (N) vorgesehen ist, welche im Rahmen des Autorisierungssystems (A) in hierarchisch abgestuften Schritten erfolgt.

26. Mobiler Datenträger (IMj) mit einer nach dem Verfahren von Anspruch 1 durch Autorisierung über ein Netzwerk (N) initialisierten Applikation (App).

27. Schreib- und Lesestation (WRk) mit einer nach dem Verfahren von Anspruch 1 durch Autorisierung über ein Netzwerk (N) initialisierten Applikation (k).

28. Anlage zur Initialisierung von mobilen Datenträgern (IM) mit zugeordneten dezentralen Schreib- und Lesestationen (WR) und/oder von dezentralen Schreib- und Lesestationen (WR) im Rahmen eines Autorisierungssystems (A), dadurch gekennzeichnet, dass

durch Autorisierungsmittel (AM) an einer Autorisierungsinstanz (HA) in einer gesicherten Umgebung (g) Initialisierungsdaten (DI, A-I, I-I) erzeugt und über ein Netzwerk (N) in einer gesicherten Kommunikation und mit dem Autorisierungssystem entsprechenden Sicherheitsregeln an eine dezentrale autorisierte Schreib- und Lesestation (A-WR) gesendet werden und dass die mobilen Datenträger (IM) an der Schreib- und Lesestation (A-WR) mit den Initialisierungsdaten (DI) entsprechend initialisiert werden (IMj)

und/oder dass die Initialisierungsdaten (DI) über das Netzwerk (N) an eine dezentrale Schreib- und Lesestation (WR) gesendet werden, womit die Schreib- und Lesestation (WR) initialisiert wird (WRk).

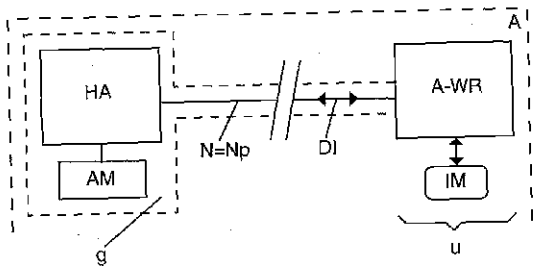


Fig. 1

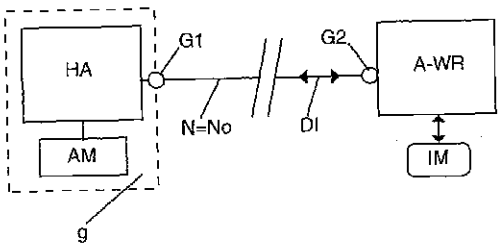


Fig. 2

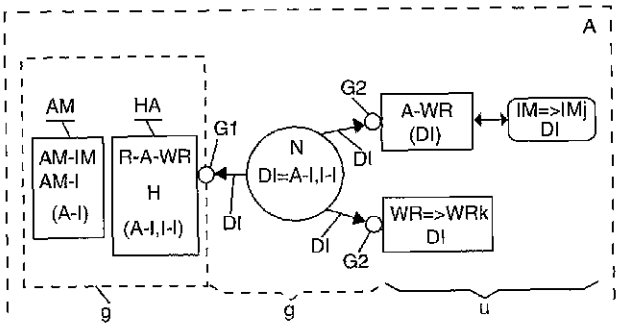

A
AM
HA
AM-IM
AM-I
(A-I)
R-A-WR
H
(A-I,I-I)
G1
N
DI=A-I,I-I
G2
A-WR
(DI)
IM=>IMj
DI
WR=>WRk
DI
g
g
u

Fig. 3

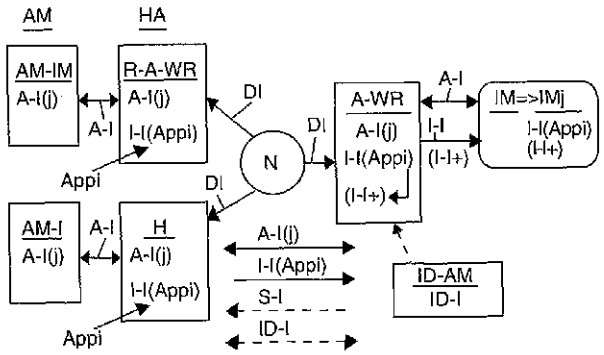

AM
HA
AM-IM
A-I(j)
R-A-WR
A-I(j)
I-I(Appi)
A-I
Appi
DI
N
A-WR
A-I(j)
I-I(Appi)
(I-I+)
A-I
I-I
IM=>IMj
I-I(Appi)
(I-I+)
AM-I
A-I(j)
H
A-I(j)
I-I(Appi)
A-I(j)
I-I(Appi)
S-I
ID-I
ID-AM
ID-I

Fig. 4

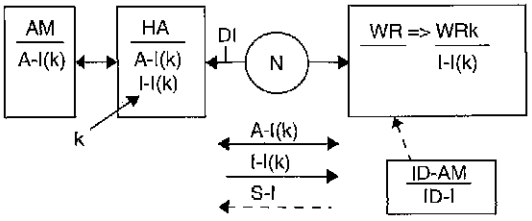

AM
A-I(k)
HA
A-I(k)
I-I(k)
DI
N
WR => WRk
I-I(k)
k
A-I(k)
I-I(k)
S-I
ID-AM
ID-I

Fig. 5

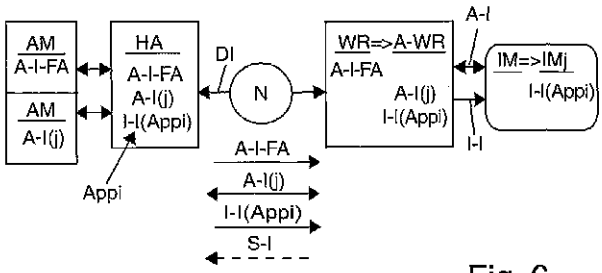

AM
A-I-FA
AM
A-I(j)
HA
A-I-FA
A-I(j)
I-I(Appi)
DI
N
WR=>A-WR
A-I-FA
A-I(j)
I-I(Appi)
A-I
IM=>IMj
I-I(Appi)
I-I
Appi
A-I-FA
A-I(j)
I-I(Appi)
S-I

Fig. 6

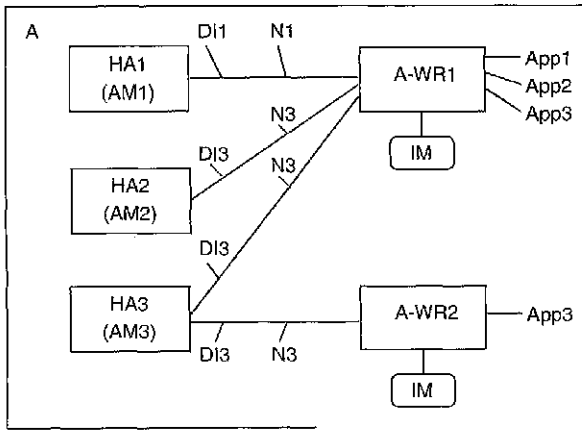

A
HA1
(AM1)
DI1
N1
A-WR1
App1
App2
App3
N3
IM
DI3
HA2
(AM2)
N3
DI3
HA3
(AM3)
A-WR2
App3
DI3
N3
IM

Fig. 7

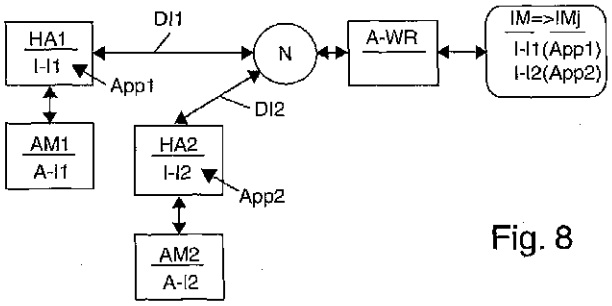

HA1
I-I1
DI1
N
A-WR
IM=>IMj
I-I1(App1)
I-I2(App2)
App1
DI2
AM1
A-I1
HA2
I-I2
App2
AM2
A-I2

Fig. 8

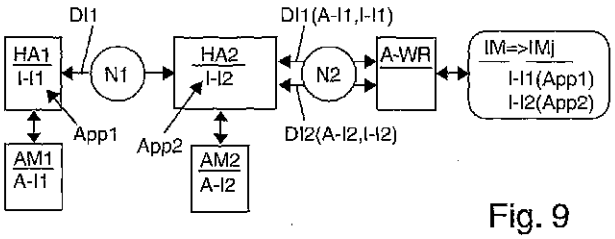

DI1
DI1(A-I1,I-I1)
HA1
I-I1
N1
HA2
I-I2
N2
A-WR
IM=>IMj
I-I1(App1)
I-I2(App2)
App1
App2
DI2(A-I2,I-I2)
AM1
A-I1
AM2
A-I2

Fig. 9

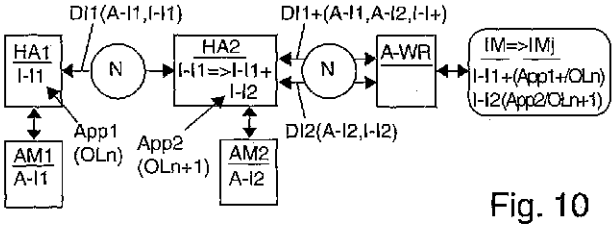

DI1(A-I1,I-I1)
DI1+(A-I1,A-I2,I-I+)
HA1
I-I1
N
HA2
I-I1=>I-I1+
I-I2
N
A-WR
IM=>IMj
I-I1+(App1+/OLn)
I-I2(App2/OLn+1)
App1
(OLn)
App2
(OLn+1)
DI2(A-I2,I-I2)
AM1
A-I1
AM2
A-I2

Fig. 10

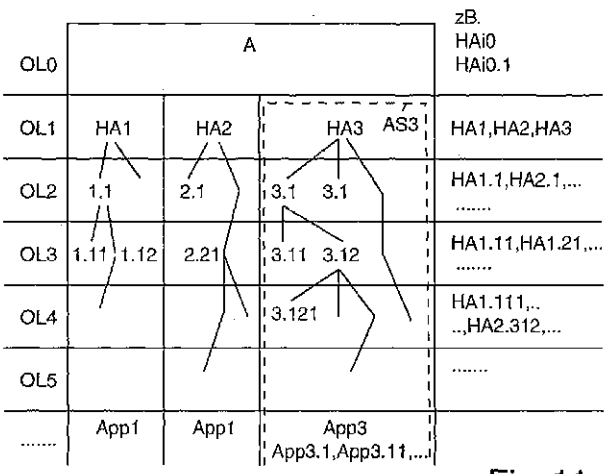

zB.
HAi0
HAi0.1
OL0
A
OL1
HA1
HA2
HA3
AS3
HA1,HA2,HA3
OL2
1.1
2.1
3.1
3.1
HA1.1,HA2.1,...
OL3
1.11
1.12
2.21
3.11
3.12
HA1.11,HA1.21,...
OL4
3.121
HA1.111,..
..,HA2.312,...
OL5
App1
App1
App3
App3.1,App3.11,...

Fig. 11

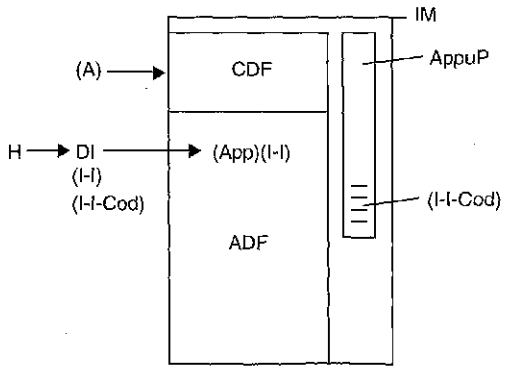

IM
(A)
CDF
AppuP
H
DI
(I-I)
(I-I-Cod)
(App)(I-I)
(I-I-Cod)
ADF

Fig. 12

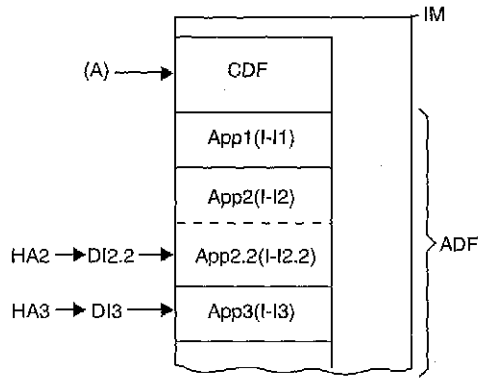

IM
(A)
CDF
App1(I-I1)
App2(I-I2)
HA2
DI2.2
App2.2(I-I2.2)
ADF
HA3
DI3
App3(I-I3)

Fig. 13

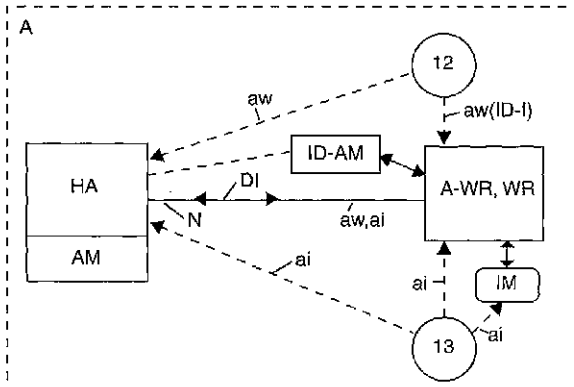

A
12
aw
aw(ID-I)
ID-AM
HA
DI
A-WR, WR
N
aw,ai
AM
ai
ai
IM
13
ai

Fig. 14

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 01/00433

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

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 G07F

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 197 20 431 A (BETA RESEARCH) 19 November 1998 (1998-11-19) cited in the application abstract; claims; figures	1-3,9, 14-19, 23,26-28
A	WO 98 52163 A (MONDEX INTERNATIONAL) 19 November 1998 (1998-11-19) abstract; claims; figures 1A,1B page 10, line 15 -page 13, line 14	1-3,9, 11,12, 14,16, 19,26-28

-/--

[X] Further documents are listed in the continuation of box C. [X] 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.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 November 2001	12/11/2001

Name and mailing address of the ISA	Authorized officer
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	David, J

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

	International Application No
	PCT/GB 01/00433

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 014 748 A (D.R. TUSHIE) 11 January 2000 (2000-01-11) abstract; claims; figures 1-13 column 2, line 38 -column 4, line 55 column 6, line 40 -column 8, line 10	1-3,8,9, 11,12, 14,16, 19,23, 26-28
A	WO 98 09257 A (GEMPLUS) 5 March 1998 (1998-03-05) abstract; claims; figures page 16, line 10 -page 20, line 19	1-3,5, 9-12,14, 16-19, 26-28
A	EP 0 949 595 A (CITICORP DEVELOPMENT CENTER) 13 October 1999 (1999-10-13) abstract; claims; figures column 15, line 6 -column 17, line 9	1-3, 9-12, 14-19, 25-28
A	US 5 534 857 A (S.G. LAING) 9 July 1996 (1996-07-09) abstract; claims; figures	1-3,9, 17-19
A	WO 98 52160 A (MONDEX INTERNATIONAL) 19 November 1998 (1998-11-19)	
A	WO 98 43212 A (VISA INTERNATIONAL SERVICE ASSOCIATION) 1 October 1998 (1998-10-01)	

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

rmation on patent family members

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
DE 19720431	A	19-11-1998	DE	19720431	A1	19-11-1998
			AU	8332998	A	08-12-1998
			WO	9852160	A1	19-11-1998
			EP	0981803	A1	01-03-2000
			ZA	9804060	A	25-11-1998
WO 9852163	A	19-11-1998	US	6230267	B1	08-05-2001
			AU	736325	B2	26-07-2001
			AU	6299698	A	09-09-1998
			AU	7776798	A	08-12-1998
			AU	7776898	A	08-12-1998
			AU	7776998	A	08-12-1998
			AU	7777098	A	08-12-1998
			AU	7777198	A	08-12-1998
			AU	7777298	A	08-12-1998
			AU	7777398	A	08-12-1998
			AU	7777498	A	08-12-1998
			EP	0963580	A1	15-12-1999
			EP	0981807	A2	01-03-2000
			EP	0985202	A1	15-03-2000
			EP	0985203	A1	15-03-2000
			EP	0976114	A2	02-02-2000
			EP	0985204	A1	15-03-2000
			EP	0981805	A1	01-03-2000
			WO	9837526	A1	27-08-1998
			WO	9852158	A2	19-11-1998
			WO	9852159	A2	19-11-1998
			WO	9852160	A2	19-11-1998
			WO	9852161	A2	19-11-1998
			WO	9852152	A2	19-11-1998
			WO	9852162	A2	19-11-1998
			WO	9852163	A2	19-11-1998
			WO	9852153	A2	19-11-1998
			JP	2001513231	T	28-08-2001
			US	6220510	B1	24-04-2001
			US	6164549	A	26-12-2000
US 6014748	A	11-01-2000	US	5889941	A	30-03-1999
			AU	717870	B2	06-04-2000
			AU	2729897	A	07-11-1997
			BR	9708673	A	04-01-2000
			CA	2251689	A1	23-10-1997
			EP	0894312	A1	03-02-1999
			JP	2000508794	T	11-07-2000
			NO	984821	A	15-12-1998
			WO	9739424	A1	23-10-1997
			US	6202155	B1	13-03-2001
WO 9809257	A	05-03-1998	US	5923884	A	13-07-1999
			AU	732887	B2	03-05-2001
			AU	4842897	A	19-03-1998
			CA	2233217	A1	05-03-1998
			EP	0858644	A1	19-08-1998
			WO	9809257	A1	05-03-1998
EP 0949595	A	13-10-1999	BR	9901213	A	11-01-2000
			EP	0949595	A2	13-10-1999
			JP	11345266	A	14-12-1999

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONAL SEARCH REPORT

ation on patent family members

1 application No
PCT/US 01/00433

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5534857	A	09-07-1996	AU	656245 B2	27-01-1995
			WO	9310509 A1	27-05-1993
			EP	0722596 A1	24-07-1996
			FI	942177 A	11-05-1994
			NO	941774 A	11-05-1994
WO 9852160	A	19-11-1998	AU	736325 B2	26-07-2001
			AU	6299698 A	09-09-1998
			AU	7776798 A	08-12-1998
			AU	7776898 A	08-12-1998
			AU	7776998 A	08-12-1998
			AU	7777098 A	08-12-1998
			AU	7777198 A	08-12-1998
			AU	7777298 A	08-12-1998
			AU	7777398 A	08-12-1998
			AU	7777498 A	08-12-1998
			EP	0963580 A1	15-12-1999
			EP	0981807 A2	01-03-2000
			EP	0985202 A1	15-03-2000
			EP	0985203 A1	15-03-2000
			EP	0976114 A2	02-02-2000
			EP	0985204 A1	15-03-2000
			EP	0981805 A1	01-03-2000
			WO	9837526 A1	27-08-1998
			WO	9852158 A2	19-11-1998
			WO	9852159 A2	19-11-1998
			WO	9852160 A2	19-11-1998
			WO	9852161 A2	19-11-1998
			WO	9852152 A2	19-11-1998
			WO	9852162 A2	19-11-1998
			WO	9852163 A2	19-11-1998
			WO	9852153 A2	19-11-1998
			JP	2001513231 T	28-08-2001
			US	6220510 B1	24-04-2001
			US	6230267 B1	08-05-2001
			US	6164549 A	26-12-2000
WO 9843212	A	01-10-1998	AU	6578698 A	20-10-1998
			EP	1004992 A2	31-05-2000
			EP	1021801 A1	26-07-2000
			US	6005942 A	21-12-1999
			US	6233683 B1	15-05-2001
			WO	9843212 A1	01-10-1998

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

	Interes Aktenzeichen PCT/EP 01/00433

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07F7/10

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07F

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)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 197 20 431 A (BETA RESEARCH) 19. November 1998 (1998-11-19) in der Anmeldung erwähnt Zusammenfassung; Ansprüche; Abbildungen ---	1-3,9, 14-19, 23,26-28
A	WO 98 52163 A (MONDEX INTERNATIONAL) 19. November 1998 (1998-11-19) Zusammenfassung; Ansprüche; Abbildungen 1A,1B Seite 10, Zeile 15 -Seite 13, Zeile 14 --- -/--	1-3,9, 11,12, 14,16, 19,26-28

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° 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 zweifelhaft erscheinen 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 naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
2. November 2001	12/11/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

	Aktenzeichen
	01/00433

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 6 014 748 A (D.R. TUSHIE) 11. Januar 2000 (2000-01-11) Zusammenfassung; Ansprüche; Abbildungen 1-13 Spalte 2, Zeile 38 -Spalte 4, Zeile 55 Spalte 6, Zeile 40 -Spalte 8, Zeile 10	1-3,8,9, 11,12, 14,16, 19,23, 26-28
A	WO 98 09257 A (GEMPLUS) 5. März 1998 (1998-03-05) Zusammenfassung; Ansprüche; Abbildungen Seite 16, Zeile 10 -Seite 20, Zeile 19	1-3,5, 9-12,14, 16-19, 26-28
A	EP 0 949 595 A (CITICORP DEVELOPMENT CENTER) 13. Oktober 1999 (1999-10-13) Zusammenfassung; Ansprüche; Abbildungen Spalte 15, Zeile 6 -Spalte 17, Zeile 9	1-3, 9-12, 14-19, 25-28
A	US 5 534 857 A (S.G. LAING) 9. Juli 1996 (1996-07-09) Zusammenfassung; Ansprüche; Abbildungen	1-3,9, 17-19
A	WO 98 52160 A (MONDEX INTERNATIONAL) 19. November 1998 (1998-11-19)	
A	WO 98 43212 A (VISA INTERNATIONAL SERVICE ASSOCIATION) 1. Oktober 1998 (1998-10-01)	

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentl... in selben Patentfamilie gehören

os Aktenzeichen
PCT/CH 01/00433

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie			Datum der Veröffentlichung
DE 19720431	A	19-11-1998	DE	19720431	A1	19-11-1998
			AU	8332998	A	08-12-1998
			WO	9852150	A1	19-11-1998
			EP	0981803	A1	01-03-2000
			ZA	9804060	A	25-11-1998
WO 9852163	A	19-11-1998	US	6230267	B1	08-05-2001
			AU	736325	B2	26-07-2001
			AU	6299698	A	09-09-1998
			AU	7776798	A	08-12-1998
			AU	7776898	A	08-12-1998
			AU	7776998	A	08-12-1998
			AU	7777098	A	08-12-1998
			AU	7777198	A	08-12-1998
			AU	7777298	A	08-12-1998
			AU	7777398	A	08-12-1998
			AU	7777498	A	08-12-1998
			EP	0963580	A1	15-12-1999
			EP	0981807	A2	01-03-2000
			EP	0985202	A1	15-03-2000
			EP	0985203	A1	15-03-2000
			EP	0976114	A2	02-02-2000
			EP	0985204	A1	15-03-2000
			EP	0981805	A1	01-03-2000
			WO	9837526	A1	27-08-1998
			WO	9852158	A2	19-11-1998
			WO	9852159	A2	19-11-1998
			WO	9852160	A2	19-11-1998
			WO	9852161	A2	19-11-1998
			WO	9852152	A2	19-11-1998
			WO	9852162	A2	19-11-1998
			WO	9852163	A2	19-11-1998
			WO	9852153	A2	19-11-1998
			JP	2001513231	T	28-08-2001
			US	6220510	B1	24-04-2001
			US	6164549	A	26-12-2000
US 6014748	A	11-01-2000	US	5889941	A	30-03-1999
			AU	717870	B2	06-04-2000
			AU	2729897	A	07-11-1997
			BR	9708673	A	04-01-2000
			CA	2251689	A1	23-10-1997
			EP	0894312	A1	03-02-1999
			JP	2000508794	T	11-07-2000
			NO	984821	A	15-12-1998
			WO	9739424	A1	23-10-1997
			US	6202155	B1	13-03-2001
WO 9809257	A	05-03-1998	US	5923884	A	13-07-1999
			AU	732887	B2	03-05-2001
			AU	4842897	A	19-03-1998
			CA	2233217	A1	05-03-1998
			EP	0858644	A1	19-08-1998
			WO	9809257	A1	05-03-1998
EP 0949595	A	13-10-1999	BR	9901213	A	11-01-2000
			EP	0949595	A2	13-10-1999
			JP	11345266	A	14-12-1999

Formblatt PCT/ISA/210 (Anhang Patentfamilie) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffer r selben Patentfamilie gehören

Ir tes Aktenzeichen
I ,/ 01/00433

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 5534857	A	09-07-1996	AU	656245 B2	27-01-1995
			WO	9310509 A1	27-05-1993
			EP	0722596 A1	24-07-1996
			FI	942177 A	11-05-1994
			NO	941774 A	11-05-1994
WO 9852160	A	19-11-1998	AU	736325 B2	26-07-2001
			AU	6299698 A	09-09-1998
			AU	7776798 A	08-12-1998
			AU	7776898 A	08-12-1998
			AU	7776998 A	08-12-1998
			AU	7777098 A	08-12-1998
			AU	7777198 A	08-12-1998
			AU	7777298 A	08-12-1998
			AU	7777398 A	08-12-1998
			AU	7777498 A	08-12-1998
			EP	0963580 A1	15-12-1999
			EP	0981807 A2	01-03-2000
			EP	0985202 A1	15-03-2000
			EP	0985203 A1	15-03-2000
			EP	0976114 A2	02-02-2000
			EP	0985204 A1	15-03-2000
			EP	0981805 A1	01-03-2000
			WO	9837526 A1	27-08-1998
			WO	9852158 A2	19-11-1998
			WO	9852159 A2	19-11-1998
			WO	9852160 A2	19-11-1998
			WO	9852161 A2	19-11-1998
			WO	9852152 A2	19-11-1998
			WO	9852162 A2	19-11-1998
			WO	9852163 A2	19-11-1998
			WO	9852153 A2	19-11-1998
			JP	2001513231 T	28-08-2001
			US	6220510 B1	24-04-2001
			US	6230267 B1	08-05-2001
			US	6164549 A	26-12-2000
WO 9843212	A	01-10-1998	AU	6578698 A	20-10-1998
			EP	1004992 A2	31-05-2000
			EP	1021801 A1	26-07-2000
			US	6005942 A	21-12-1999
			US	6233683 B1	15-05-2001
			WO	9843212 A1	01-10-1998

Formblatt PCT/ISA/210 (Anhang Patentfamilie)(Juli 1992)

フロントページの続き

(51)Int.Cl.[7]	ＦＩ	テーマコード（参考）
	Ｇ０６Ｋ 17/00 ＺＥＣＢ	

(74)代理人 100096792
弁理士 森下 八郎
(72)発明者 クロサ，クラウス・ウルリッヒ
スイス、ツェー・ハー－８６２７ グリュニンゲン、ドュルンターシュトラーセ、５０
(72)発明者 エッペンバーガー，ローマン
スイス、ツェー・ハー－８６３５ ドュルンテン、ヒンタードルフシュトラーセ、５

Ｆターム(参考) 5B017 AA03 BA05 CA14
5B058 CA25 KA04 KA33 YA20
5B085 AE02