(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2015-515217
(P2015-515217A)
(43)公表日　平成27年5月21日(2015.5.21)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
G06F 21/60	(2013.01)	G06F	21/60	320	

審査請求 有　予備審査請求 未請求　（全 18 頁）

(21)出願番号	特願2015-506144 (P2015-506144)
(86)(22)出願日	平成25年3月18日 (2013.3.18)
(85)翻訳文提出日	平成26年10月15日 (2014.10.15)
(86)国際出願番号	PCT/EP2013/055505
(87)国際公開番号	WO2013/156230
(87)国際公開日	平成25年10月24日 (2013.10.24)
(31)優先権主張番号	102012206202.5
(32)優先日	平成24年4月16日 (2012.4.16)
(33)優先権主張国	ドイツ(DE)

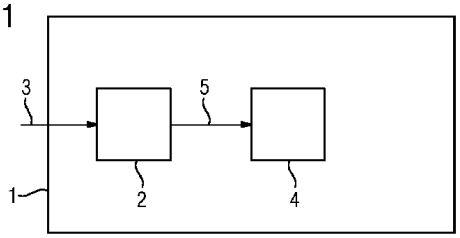
(71)出願人　390039413
シーメンス　アクチエンゲゼルシヤフト
Ｓｉｅｍｅｎｓ　Ａｋｔｉｅｎｇｅｓｅｌｌｓｃｈａｆｔ
ドイツ連邦共和国　Ｄ－８０３３３　ミュンヘン　ヴィッテルスバッハープラッツ　２
Ｗｉｔｔｅｌｓｂａｃｈｅｒｐｌａｔｚ　２，　Ｄ－８０３３３　Ｍｕｅｎｃｈｅｎ，　Ｇｅｒｍａｎｙ
(74)代理人　100114890
弁理士　アインゼル・フェリックス＝ラインハルト
(74)代理人　100099483
弁理士　久野　琢也

最終頁に続く

(54)【発明の名称】ドキュメントをディジタル化するための装置及び方法

(57)【要約】
本発明は、紙の形態で存在する少なくとも一つのドキュメントをディジタル化するように構成されているドキュメントスキャンユニットと、少なくとも一つのディジタル化されたドキュメントを、一度だけ有効な識別子、即ちワンタイムＩＤを基礎として、権限の無いアクセスから保護するように構成されているセキュリティユニットとを備えている、ドキュメントをディジタル化するための装置に関する。更に本発明は、対応する方法に関する。

FIG 1



【特許請求の範囲】
【請求項１】
ドキュメントをディジタル化するための装置（１）において、
紙の形態で存在する少なくとも一つのドキュメント（３）をディジタル化するように構成されているドキュメントスキャンユニット（２）と、
少なくとも一つのディジタル化ドキュメント（５）を、ワンタイムＩＤ（６）を基礎として、権限の無いアクセスから保護するように構成されているセキュリティユニット（４）と、
を備えていることを特徴とする、装置。
【請求項２】
前記セキュリティユニット（４）は鍵導出ユニット（７）を有しており、
前記鍵導出ユニット（７）は、前記少なくとも一つのディジタル化ドキュメント（５）を保護するための暗号的に安全な鍵を、前記ワンタイムＩＤ（６）から計算するように構成されている、請求項１に記載の装置。
【請求項３】
データメモリ（１０）が設けられており、
前記セキュリティユニット（４）は、前記少なくとも一つのディジタル化ドキュメント（５）を前記データメモリ（１０）に記憶し、該少なくとも一つのディジタル化ドキュメント（５）を、前記ワンタイムＩＤ（６）及び／又は前記計算された暗号的に安全な鍵を基礎とする、パスワードで保護された前記データメモリ（１０）へのアクセスによって保護するように構成されている、請求項２に記載の装置。
【請求項４】
前記セキュリティユニット（４）は、前記少なくとも一つのディジタル化ドキュメント（５）を、前記ワンタイムＩＤ（６）及び／又は前記計算された暗号的に安全な鍵を基礎として暗号化するように構成されている、請求項２又は３に記載の装置。
【請求項５】
前記セキュリティユニット（４）は乱数生成器（８）を有しており、該乱数生成器（８）は前記ワンタイムＩＤ（６）をランダムに決定するように構成されている、請求項１乃至４のいずれか一項に記載の装置。
【請求項６】
前記乱数生成器（８）は、前記少なくとも一つのディジタル化ドキュメント（５）に設定された秘密レベルに応じて前記ワンタイムＩＤ（６）をランダムに決定するように構成されている、請求項５に記載の装置。
【請求項７】
前記セキュリティユニット（４）は、前記ワンタイムＩＤ（６）をユーザに要求するように構成されている、請求項１乃至４のいずれか一項に記載の装置。
【請求項８】
ネットワークインタフェース（９）が設けられており、
制御ユニット（１１）が設けられており、
前記制御ユニット（１１）は、保護された前記少なくとも一つのディジタル化ドキュメント（５）を電子メッセージの添付として、前記ネットワークインタフェース（９）を介して、所定の受信器に送信するように構成されている、請求項１乃至７のいずれか一項に記載の装置。
【請求項９】
前記制御ユニット（１１）は、前記電子メッセージ及び該電子メッセージに含まれる添付を、送信の前に、対称暗号化方式及び／又は非対称暗号化方式によって暗号化するように構成されている、請求項８に記載の装置。
【請求項１０】
ドキュメントをディジタル化するための方法において、
紙の形態で存在する少なくとも一つのドキュメント（３）をディジタル化するステップ

（Ｓ１）と、
少なくとも一つのディジタル化ドキュメント（５）を、ワンタイムＩＤ（６）を基礎として、権限の無いアクセスから保護するステップ（Ｓ２）とを備えている、
ことを特徴とする、方法。
【請求項１１】
前記少なくとも一つのディジタル化ドキュメント（５）を保護するために、前記ワンタイムＩＤ（６）から暗号的に安全な鍵を計算するステップを更に備えている、請求項１０に記載の方法。
【請求項１２】
前記少なくとも一つのディジタル化ドキュメント（５）をデータメモリ（１０）に記憶するステップと、
前記少なくとも一つのディジタル化ドキュメント（５）を、前記ワンタイムＩＤ（６）及び／又は前記計算された暗号的に安全な鍵を基礎とする、パスワードで保護されたデータメモリ（１０）へのアクセスによって保護するステップとを更に備えている、請求項１１に記載の方法。
【請求項１３】
前記少なくとも一つのディジタル化ドキュメント（５）を、前記ワンタイムＩＤ（６）及び／又は前記計算された暗号的に安全な鍵を基礎として暗号化するステップを更に備えている、請求項１１又は１２に記載の方法。
【請求項１４】
前記ワンタイムＩＤ（６）を、特に前記少なくとも一つのディジタル化ドキュメント（５）に設定された秘密レベルに応じて、ランダムに決定するステップ、又は、
前記ワンタイムＩＤ（６）をユーザに要求するステップを更に備えている、請求項１０乃至１３のいずれか一項に記載の方法。
【請求項１５】
保護された前記少なくとも一つのディジタル化ドキュメント（５）を電子メッセージの添付として、特に対称暗号化方式及び／又は非対称暗号化方式によって暗号化された電子メッセージとして所定の受信器に送信するステップを更に備えている、請求項１０乃至１４のいずれか一項に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ドキュメントをディジタル化するための装置及び対応する方法に関する。
【背景技術】
【０００２】
以下では本発明を、特に複合プリンタに関連させて説明するが、本発明は複合プリンタに限定されるものではなく、本発明をあらゆる種類のディジタル化装置によって利用することができる。
【０００３】
今日のところ、特に産業界では、ドキュメントを郵便で遣り取りすること、又は郵便のみで遣り取りすることはもはや一般的ではない。むしろ、紙の形態で存在するドキュメントをディジタル化し、それらのドキュメントを電子的な形態で遣り取りするために電子的な手段が使用されている。
【０００４】
その種の機器として例えば単体のスキャナが挙げられる。それ以外にも、特に商業的な用途のための機器として、しかしながらまた個人的に使用するための機器として、いわゆる複合機（ＭＦＤ：Multi Functional Deviceとも称される）が公知である。それらのＭＦＤとして、例えば、プリンタとスキャナとＦＡＸが組み合わされたものが考えられる。
【０００５】
更に、その種の機器はネットワーク端子を一般的に有しており、そのネットワーク端子

を介して機器をデータネットワークに接続することができる。
【０００６】
ディジタル化ドキュメントを提供するために、ＭＦＤはウェブサーバを有することができ、このウェブサーバによって、ディジタル化ドキュメントをダウンロードすることができる。更に、それらのＭＦＤはＥメールサーバとのインタフェースも有することができ、このＥメールサーバによってディジタル化ドキュメントをＥメールでユーザに送信することができる。
【０００７】
ＭＦＤのウェブサーバに格納されているディジタル化ドキュメントへのアクセス並びにＥメールを用いたユーザへのディジタル化ドキュメントの送信は通常の場合、保護された形式では行われていない。
【発明の概要】
【発明が解決しようとする課題】
【０００８】
本発明の課題は、ディジタル化ドキュメントを保護するための実現手段を提供することがある。
【課題を解決するための手段】
【０００９】
この課題は、本発明によれば、独立請求項の特徴部分に記載されている構成を備えている装置及び方法によって解決される。
【００１０】
従って、本発明によれば、
－紙の形態で存在する少なくとも一つのドキュメントをディジタル化するように構成されているドキュメントスキャンユニットと、少なくとも一つのディジタル化ドキュメントを、一度だけ有効な識別子、即ちワンタイムＩＤを基礎として、権限の無いアクセスから保護するように構成されているセキュリティユニットとを備えている、ドキュメントをディジタル化するための装置と、
－紙の形態で存在する少なくとも一つのドキュメントをディジタル化するステップと、少なくとも一つのディジタル化ドキュメントを、ワンタイムＩＤを基礎として、権限の無いアクセスから保護するステップとを備えている、ドキュメントをディジタル化するための方法と、
が提供される。
【００１１】
本発明が基礎とする認識は、特に商業的な分野において、ドキュメントを機密に取り扱うことが実現できれば有利であろうということである。
【００１２】
本発明が基礎とする着想は、この認識に基づき、ワンタイムＩＤを基礎としてドキュメントを保護できるようにすることである。
【００１３】
本発明によれば、ドキュメントがドキュメントスキャンユニットによってディジタル化され、続いて、セキュリティユニットを用いて権限の無いアクセスから保護される。その際、ディジタル化プロセスの度に新たな識別子が利用される。
【００１４】
ワンタイムＩＤの使用によって、例えば大企業においてドキュメントが安全に編集されることを保証することができる。例えば、ある企業において標準的な識別子が使用されているケースを想定すると、その標準的な識別子が漏洩した場合には、潜在的な攻撃者がその企業の全てのドキュメントにアクセスすることが極めて簡単になる。
【００１５】
更には、本発明による装置のユーザが識別子を自由に選択できてしまう場合には、そのユーザが常に同じ識別子を選択するといった危険も生じてしまう。その結果、潜在的な攻

撃者が、そのユーザのドキュメントにアクセスすることは一層容易になる。つまり攻撃者は、そのユーザの全てのドキュメントにアクセスするためには、識別子を一つだけ入手しさえすればよい。

【００１６】

有利な実施の形態及び発展形態は、従属請求項並びに図面を参照する以下の説明より明らかになる。

【００１７】

一つの実施の形態においては、セキュリティユニットが鍵導出ユニットを有しており、この鍵導出ユニットは、少なくとも一つのディジタル化ドキュメントを保護するための暗号的に安全な鍵を、ワンタイムＩＤから計算するように構成されている。これによって、保護すべきディジタル化ドキュメントの安全性が向上し、またユーザが使用しやすいアプローチが実現される。つまり、鍵導出ユニットの使用によって、容易に記憶することができる識別子、例えば４桁の番号を、ユーザが容易に記憶することができる識別子として使用することができる。それにもかかわらず、ディジタル化ドキュメントを効果的に保護することができる。

【００１８】

それらの識別子が例えばディジタル化ドキュメントを保護するための鍵として直接的に使用されるのであれば、攻撃者によるそのドキュメントへのアクセスは簡単に達成されるであろう。

【００１９】

それに対し、暗号的に安全な鍵が識別子から導出される場合には、攻撃者がその保護されたディジタル化ドキュメントにアクセスすることは困難になるか、又は今日の一般的な計算能力では不可能である。

【００２０】

鍵導出ユニットは、暗号的に安全な鍵を、例えばＫＤＦ１，ＫＤＦ２，ＫＤＦ３，ＫＤＦ４，ＭＧＦ１，ＰＢＫＤＦ－Ｓｃｈｎｅｉｄｅｒ，ＰＢＫＤＦ１，ＰＢＫＤＦ２及び／又は暗号ベースのアルゴリズムを用いて導出することができる。

【００２１】

一つの実施の形態において、鍵導出ユニットは、ワンタイムＩＤを基礎として暗号的に安全な鍵を計算するために、いわゆる「ソルト（Salt）」を付加的に使用するように構成されている。暗号技術において、「ソルト」は、鍵を計算するために識別子が使用される場合には、その識別子を拡張するために用いられる、大抵の場合ランダムな文字列であると解される。

【００２２】

一つの実施の形態においては、データメモリが設けられている。更に、セキュリティユニットは、少なくとも一つのディジタル化ドキュメントをデータメモリに記憶し、その少なくとも一つのディジタル化ドキュメントを、ワンタイムＩＤ及び／又は計算された暗号的に安全な鍵を基礎とするパスワードで保護されたデータメモリへのアクセスによって保護するように構成されている。

【００２３】

ディジタル化ドキュメントが、パスワードで保護されたデータメモリへのアクセスによって保護される場合には、その保護されたディジタル化ドキュメントをユーザは種々の電子デバイスから非常に快適に検索することができる。

【００２４】

一つの実施の形態において、セキュリティユニットは、少なくとも一つのディジタル化ドキュメントを、ワンタイムＩＤ及び／又は計算された暗号的に安全な鍵を基礎として暗号化するように構成されている。

【００２５】

ディジタル化ドキュメントが暗号技術により暗号化される場合、対応するドキュメントをディジタル化したユーザがそのドキュメントを既に呼び出していれば、その後に攻撃者

がドキュメントを取得したとしても、攻撃者はそのドキュメントをもはや開くことはできない。このことは例えば、ユーザのコンピュータへの侵入によって行われる可能性がある。

【００２６】

一つの実施の形態においては、セキュリティユニットが乱数生成器を有しており、この乱数生成器はワンタイムＩＤをランダムに決定するように構成されている。これによって、攻撃者は先行の識別子から、又は装置の観察によって識別子を導出できないことを保証することができる。

【００２７】

一つの実施の形態においては、少なくとも一つのディジタル化ドキュメントに設定された秘密レベルに応じて、ワンタイムＩＤがランダムに決定されるように乱数生成器は構成されている。ディジタル化ドキュメントに対して種々の秘密レベルが設定され、且つ、識別子がその設定された秘密レベルに応じて決定される場合には、識別子、例えば識別子の複雑度を個々の秘密レベルに適合させることができる。

【００２８】

一つの実施の形態においては、ワンタイムＩＤをユーザに要求するようにセキュリティユニットが構成されている。これによって、ユーザ自身がワンタイムＩＤを決定することができる。

【００２９】

一つの実施の形態においては、乱数生成器によってワンタイムＩＤをランダムに決定し、ユーザに表示することができる。これによってユーザは、ユーザ自身が識別子を決定するのか、又は、ユーザはランダム生成された識別子をディジタル化ドキュメントの保護のために変更したくないのかを判断することができる。

【００３０】

一つの実施の形態においては、ネットワークインタフェースが設けられている。更に制御ユニットが設けられており、この制御ユニットは、保護された少なくとも一つのディジタル化ドキュメントを、電子メッセージの添付として、ネットワークインタフェースを介して所定の受信器に送信するように構成されている。

【００３１】

このことは、保護されたディジタル化ドキュメントのユーザへの自動的な送信を実現する。これによって、保護されたディジタル化ドキュメントを取得するために、ユーザが行わなければならない手間が低減される。ユーザは保護されたディジタル化ドキュメントの呼び出しを自身で行う必要がないので、それによって本発明による装置が更に広範に受け入れられるようになる。

【００３２】

一つの実施の形態において、制御ユニットは、電子メッセージ及びその電子メッセージに含まれる添付が、送信の前に、対称暗号化方式及び／又は非対称暗号化方式によって暗号化されるように構成されている。これによって、保護されたディジタル化ドキュメントの安全性を更に高めることができる。更にこれによって、ドキュメントが保護されるだけでなく、電子メッセージの内容がどのようなものであるかを第三者に対して完全に秘匿することができる。

【００３３】

更に、例えばディジタル化ドキュメントに設定された秘密レベルに基づき、対応するディジタル化ドキュメントがどの暗号化方式で保護されるかを判定することができる。

【００３４】

一つの実施の形態において、制御ユニットは、電子メッセージの受信器に鍵を要求するためにディレクトリサービスにアクセスするように構成されている。ディレクトリサービスは例えばＬＤＡＰディレクトリ又は任意の他のディレクトリで良く、それらのディレクトリは電子メッセージを受信することが可能な受信器に関する情報を有している。その種のディレクトリサービスを鍵サーバと称することもできる。これによって、電子メッセー

ジの送信者が個々の受信器の鍵を知らない場合であっても、暗号技術を用いて保護されているメッセージを複数のユーザに送信することができる。

【００３５】

一つの実施の形態においては、本発明による装置のユーザはワンタイムＩＤを本発明による装置の印刷ユニットにおいて印刷することができる。ユーザがワンタイムＩＤを印刷できる場合には、ユーザはそのワンタイムＩＤを記憶する必要はない。識別子は一度だけしか有効でないので、これはセキュリティ上の大きな危険にはならない。

【００３６】

上述の構成及び発展形態は、有効な範囲において相互に任意に組み合わせることができる。本発明の別の考えられる実施の形態、発展形態及び実現形態は、本発明の複数の実施例に関して上記において説明した、又は以下において説明する複数の特徴の明示的には示していない組み合わせも含む。特に当業者であれば、改善形態又は補完形態としての個々の態様を本発明の各基本形態に付加するであろう。

【００３７】

本明細書においてワンタイムＩＤという術語は、数字コード及び／又は英数字コードを表している。但し、これは暗号技術的な観点から見ると、それらのコードが暗号化のための鍵として直接的に利用される場合には、セキュリティが低いものである。

【００３８】

考えられる一つの実施の形態において、所定の期間に一度だけしか使用できない識別子がワンタイムＩＤであると解される。既に使用されてしまった識別子は必ずしも全て除外されるわけではない。例えば、４桁の数字から成る識別子の場合、例えば４桁の番号のセットから考えられる番号の組み合わせの内の８０％が既に使用されている場合には、既に使用された識別子を改めて使用することができる。別の桁数の識別子又は英数字識別子に対しても同様に所定の閾値又は期間を設定することができる。しかしながらこの期間を、数時間、数日、数週、数ヶ月及び／又は数年の単位で規定することもできる。

【００３９】

以下では、図面に概略的に図示されている複数の実施例に基づき本発明を詳細に説明する。

【図面の簡単な説明】

【００４０】

【図１】本発明による装置の実施例のブロック図を示す。

【図２】本発明による方法の実施例のフローチャートを示す。

【図３】本発明による装置の別の実施例のブロック図を示す。

【発明を実施するための形態】

【００４１】

全ての図面において、別個に記載がない限りは、同一の又は機能的に等しい構成要素及び装置乃至ユニットには同一の参照番号が付されている。

【００４２】

図１には、本発明による装置１の実施例がブロック図で示されている。図１に示した本発明による装置は、複合機（多機能機、ＭＦＤ：Multi Functional Device）として構成されている。別の実施の形態においては、装置１が例えば単体のスキャナ１として構成されていてもよい。

【００４３】

図１に示したＭＦＤは、紙の形態で存在するドキュメント３をディジタル化又はスキャンするように構成されているスキャナ２を有している。スキャナ２はセキュリティユニット４と接続されており、従って、スキャナ２からセキュリティユニット４にディジタル化ドキュメント５が伝送される。セキュリティユニット４は、一度だけ有効な識別子、即ちワンタイムＩＤ６を用いて、ディジタル化ドキュメント５を権限の無いアクセスから保護するように構成されている。

【００４４】

ワンタイムＩＤ６は、ＭＤＦ１のユーザが容易に記憶することができる、数字から成るＰＩＮ又は英数字から成るパスワードとして構成されている。例えば、ワンタイムＩＤ６は４桁又は６桁の番号で良い。

【００４５】

セキュリティユニット４は例えば、暗号計算に適したディジタル回路を有しているセキュリティモジュールで良い。例えば、この暗号計算に適したディジタル回路として「Trusted Platform Module（ＴＰＭ）」が挙げられる。しかしながらセキュリティユニット４を、ＭＦＤ１のプロセッサによって実行されるプログラムモジュールとして構成することもできる。

【００４６】

セキュリティユニット４は、ワンタイムＩＤ６を基礎として、種々の方式でディジタル化ドキュメント５を保護することができる。例えば、セキュリティユニット４は、ワンタイムＩＤ６を基礎として、ディジタル化ドキュメント５を暗号化することができる。その場合、セキュリティユニット４はディジタル化ドキュメント５を暗号化するための鍵として、ワンタイムＩＤ６を直接的に利用することができる。暗号的な見地からすると非常に短いワンタイムＩＤ６を基礎として計算を非常に簡単に実施することができることから、そのようなワンタイムＩＤ６の直接的な利用は、暗号化を非常に高速に実施できるという利点を有している。一つの別の実施の形態においては、セキュリティユニット４が、ディジタル化ドキュメント５を暗号化するための鍵として、ワンタイムＩＤ６を間接的に利用することができる。その種の実施の形態においては、セキュリティユニット４がワンタイムＩＤ６から、ディジタル化ドキュメント５を暗号化するための暗号的に安全な鍵を導出することができる。

【００４７】

一つの別の実施の形態においては、セキュリティユニット４が、ディジタル化ドキュメント５をパスワードで保護された記憶場所に格納することによって、ディジタル化ドキュメント５を権限の無いアクセスから保護することができる。その場合、記憶場所にアクセスするためのパスワードはワンタイムＩＤ６であるか、又はワンタイムＩＤ６から導出されたものである。

【００４８】

図２には、本発明による方法の実施例のフローチャートが示されている。

【００４９】

ドキュメントをディジタル化するための本発明による方法は、紙の形態で存在する少なくとも一つのドキュメント３をディジタル化するステップＳ１でもって開始される。第２のステップＳ２においては、ワンタイムＩＤ６を基礎として、少なくとも一つのディジタル化ドキュメント５が権限の無いアクセスから保護される。

【００５０】

一つの実施の形態において、本方法は、少なくとも一つのディジタル化ドキュメント５を保護するために、ワンタイムＩＤ６から暗号的に安全な鍵を計算する更なるステップを備えている。このステップによって、簡単に記憶することができ、従って比較的短いワンタイムＩＤ６が使用される場合であっても、ドキュメントの信頼性の高い暗号化又は記憶場所のより堅固なパスワード保護が確保されていることを保証することができる。

【００５１】

暗号的に安全な鍵を計算するために、鍵導出関数を使用することができる。例えばそのような関数として、ＫＤＦ１、ＫＤＦ２、ＫＤＦ３、ＫＤＦ４、ＭＧＦ１、ＰＢＫＤＦ－Ｓｃｈｎｅｉｄｅｒ、ＰＢＫＤＦ１、ＰＢＫＤＦ２及び／又は暗号鍵導出関数（scrypt key derivation function）が挙げられる。一つの別の実施の形態においては、複数の鍵導出関数を組み合わせることができる。別の鍵導出関数が使用されてもよい。ここで鍵導出関数とは、ワンタイムＩＤ６から暗号的に安全な鍵を導出又は計算することができる、あらゆる関数であると解される。

【００５２】

一つの別の実施の形態においては、ディジタル化ドキュメント５がデータメモリ１０に記憶され、そのディジタル化ドキュメント５が、ワンタイムＩＤ６及び／又は計算された暗号的に安全な鍵を基礎とする、パスワードで保護されたデータメモリ１０へのアクセスによって保護される。

【００５３】

一つの別の実施の形態においては、ワンタイムＩＤ６及び／又は計算された暗号的に安全な鍵を基礎として、ディジタル化ドキュメント５が暗号化されることによって、ディジタル化ドキュメント５が権限の無いアクセスから保護される。その際に、種々の暗号化アルゴリズムを利用することができる。例えば、対称暗号化方式及び／又は非対称暗号化方式を用いて暗号化を実施することができる。以下に挙げるものは、使用できる暗号化方式の選択肢である：

・ＡＥＳ
・ＤＥＳ
・Ｔｒｉｐｌｅ－ＤＥＳ
・ＩＤＥＡ
・Ｂｌｏｗｆｉｓｈ
・Ｔｗｏｆｉｓｈ
・ＲＳＡ
・Ｍｅｒｋｌｅ－Ｈｅｌｌｍａｎ

別の方式も利用することができる。

【００５４】

一つの実施の形態においては、ワンタイムＩＤ６がランダムに決定される。一つの実施の形態においては、少なくとも一つのディジタル化ドキュメント５に設定された秘密レベルに応じてワンタイムＩＤ６を決定することができる。ディジタル化ドキュメント５に設定される秘密レベルを、例えば、「社外秘」、「機密」及び／又は「極秘」のような注意書きに基づいて決定することができる。しかしながら秘密レベルを例えば数字によって規定することもできる。

【００５５】

形成されるワンタイムＩＤ６が複雑になるほど、ディジタル化ドキュメント５の秘密レベルはより高く、ないしよりクリティカルになる。

【００５６】

一つの実施の形態においては、ワンタイムＩＤ６をユーザに要求することもできる。

【００５７】

最後に、一つの実施の形態においては、保護されたディジタル化ドキュメント５を、電子メッセージ、例えばＥメールの添付として所定の受信器に送信することができる。

【００５８】

電子メッセージを、例えば、対称暗号化方式及び／又は非対称暗号化方式によって暗号化された電子メッセージとして送信することができる。例えば、ＰＧＰと互換性のある暗号化を利用することができる。ディジタル化ドキュメント５自体を暗号化し、続いて暗号化された電子メッセージに添付させて伝送することができるか、又は、ディジタル化ドキュメント５を暗号化せずに電子メッセージに添付させて、その電子メッセージと一緒に暗号化することができる。ここでも上述の暗号化方式を使用することができる。別の暗号化方式も同様に使用することができる。

【００５９】

図３には、本発明による装置１の別の実施の形態のブロック図が示されている。

【００６０】

図３に示した装置１もやはりＭＦＤ１として構成されている。しかしながら別の実施の形態においては、装置１が単体のスキャナ１等として構成されていてもよい。

【００６１】

図３に示したＭＦＤ１と、図１に示したＭＦＤ１との相異点は、ドキュメントスキャン

ユニット２及びセキュリティユニット４の他に、別のコンポーネントが設けられていることである。

【００６２】

図３に示したセキュリティユニット４は鍵導出ユニット７を有しており、この鍵導出ユニット７は、ディジタル化ドキュメント５を保護するための暗号的に安全な鍵をワンタイムＩＤ６から計算することができる。更に乱数生成器８が設けられており、この乱数生成器８は鍵導出ユニット７にランダム生成されたワンタイムＩＤ６を供給する。更にユーザインタフェース１２が設けられており、このユーザインタフェース１２を介してユーザにワンタイムＩＤ６を要求し、そのワンタイムＩＤ６を鍵導出ユニット７に供給することができる。最後に、図３に示したセキュリティユニット４には計算ユニット１３が設けられており、この計算ユニット１３は、鍵導出ユニット７によって計算された暗号的に安全な鍵に基づきディジタル化ドキュメント５を保護する。

【００６３】

ＭＦＤ１には更にデータメモリ１０が設けられている。その種の実施の形態においては、ディジタル化ドキュメント５をデータメモリ１０に記憶し、そのデータメモリ１０に対するアクセスをパスワードで保護することによって、セキュリティユニット４はディジタル化ドキュメント５を保護することができる。

【００６４】

ＭＦＤ１は更にネットワークインタフェース９及び制御ユニット１１を有している。ネットワークインタフェース９及び制御ユニット１１を介して、例えばユーザはデータネットワークを経由してＭＦＤ１のデータメモリ１０にアクセスすることができる。

【００６５】

一つの実施の形態においては、保護されたディジタル化ドキュメント５を電子メッセージの添付として、ネットワークインタフェース９を介して、所定の受信器に送信するように制御ユニット１１が構成されている。電子メッセージ及びその電子メッセージに含まれる添付を、送信の前に、対称暗号化方式及び／又は非対称暗号化方式によって暗号化することができる。

【００６６】

上記においては、本発明を有利な実施例に基づき説明したが、本発明はそれらの実施例に限定されるものではなく、多種多様に修正することができる。特に、本発明の本質から逸脱することなく、本発明を種々に変更又は修正することができる。

【００６７】

一つの実施の形態においては、ドキュメントをディジタル化するための装置には、

－紙の形態で存在する少なくとも一つのドキュメント３をディジタル化するための手段Ｓ１と、

－少なくとも一つのディジタル化ドキュメント５を、ワンタイムＩＤ６を基礎として、権限の無いアクセスから保護するための手段Ｓ２と、

が設けられている。

【００６８】

一つの実施の形態においては、少なくとも一つのディジタル化ドキュメント５を保護するために、ワンタイムＩＤ６から暗号的に安全な鍵を計算するための手段が装置に設けられている。

【００６９】

一つの実施の形態においては、少なくとも一つのディジタル化ドキュメント５をデータメモリ１０に記憶するための手段と、少なくとも一つのディジタル化ドキュメント５を、ワンタイムＩＤ６及び／又は計算された暗号的に安全な鍵を基礎とするパスワードで保護されたデータメモリ１０へのアクセスによって保護するための手段とが装置に設けられている。

【００７０】

一つの実施の形態においては、少なくとも一つのディジタル化ドキュメント５を、ワン

タイムＩＤ６及び／又は計算された暗号的に安全な鍵を基礎として暗号化するための手段が装置に設けられている。

【００７１】

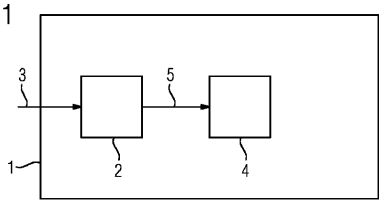
一つの実施の形態においては、特に少なくとも一つのディジタル化ドキュメント５に設定された秘密レベルに応じてワンタイムＩＤ６をランダムに決定するための手段、又はワンタイムＩＤ６をユーザに要求するための手段が装置に設けられている。

【００７２】

一つの実施の形態においては、少なくとも一つの保護されたディジタル化ドキュメント５を電子メッセージの添付として、特に対称暗号化方式及び／又は非対称暗号化方式によって暗号化された電子メッセージとして所定の受信器に送信するための手段が装置に設けられている。

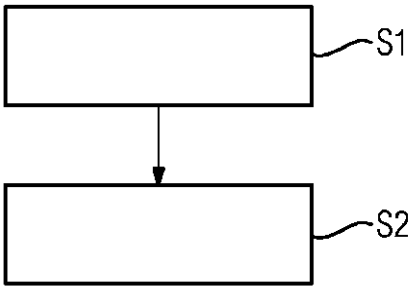
【図１】

FIG 1



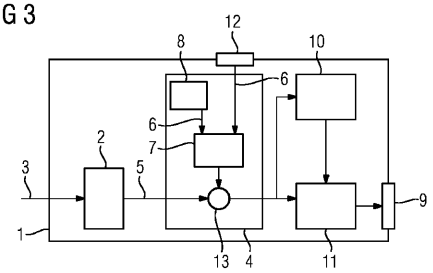
【図２】

FIG 2



【図３】

FIG 3



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/055505

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/60 G06F21/62
ADD.

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)
G06F

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 practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/271321 A1 (STAFFORD GRANT [AU]) 29 October 2009 (2009-10-29) paragraphs [0067] - [0070], [0093]; figures 2,3	1-15
Y	US 2005/210259 A1 (RICHARDSON TANNA M [US]) 22 September 2005 (2005-09-22) paragraphs [0022] - [0025]; figures 3,4,5	1-15
Y	US 7 395 436 B1 (NEMOVICHER KERRY [US]) 1 July 2008 (2008-07-01) column 6; figure 5b	1-15
X	US 2009/210695 A1 (SHAHINDOUST AMIR [US] ET AL) 20 August 2009 (2009-08-20) paragraphs [0023] - [0024]; figure 1	1-15
	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family 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 application or patent 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
28 June 2013	11/07/2013

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, Fax: (+31-70) 340-3016	Widera, Sabine

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/055505

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 692 048 A (GORMISH MICHAEL J [US] ET AL) 25 November 1997 (1997-11-25) claims 1-3; figure 8 -----	1-15

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/055505

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009271321 A1	29-10-2009	AU 2006202519 A1	27-07-2006
		AU 2007266259 A1	06-12-2007
		GB 2452879 A	18-03-2009
		US 2009271321 A1	29-10-2009
		WO 2007137368 A1	06-12-2007
US 2005210259 A1	22-09-2005	JP 2005295541 A	20-10-2005
		US 2005210259 A1	22-09-2005
US 7395436 B1	01-07-2008	NONE	
US 2009210695 A1	20-08-2009	NONE	
US 5692048 A	25-11-1997	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2013/055505

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/60 G06F21/62
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2009/271321 A1 (STAFFORD GRANT [AU]) 29. Oktober 2009 (2009-10-29) Absätze [0067] - [0070], [0093]; Abbildungen 2,3	1-15
Y	US 2005/210259 A1 (RICHARDSON TANNA M [US]) 22. September 2005 (2005-09-22) Absätze [0022] - [0025]; Abbildungen 3,4,5	1-15
Y	US 7 395 436 B1 (NEMOVICHER KERRY [US]) 1. Juli 2008 (2008-07-01) Spalte 6; Abbildung 5b	1-15
X	US 2009/210695 A1 (SHAHINDOUST AMIR [US] ET AL) 20. August 2009 (2009-08-20) Absätze [0023] - [0024]; Abbildung 1	1-15

-/--

[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" frühere Anmeldung oder Patent, die bzw. 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 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
28. Juni 2013	11/07/2013

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

1

Formblatt PCT/ISA/210 (Blatt 2) (April 2005)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2013/055505

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 692 048 A (GORMISH MICHAEL J [US] ET AL) 25. November 1997 (1997-11-25) Ansprüche 1-3; Abbildung 8 -----	1-15

1

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (April 2005)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2013/055505

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2009271321 A1	29-10-2009	AU 2006202519 A1	27-07-2006
		AU 2007266259 A1	06-12-2007
		GB 2452879 A	18-03-2009
		US 2009271321 A1	29-10-2009
		WO 2007137368 A1	06-12-2007
US 2005210259 A1	22-09-2005	JP 2005295541 A	20-10-2005
		US 2005210259 A1	22-09-2005
US 7395436 B1	01-07-2008	KEINE	
US 2009210695 A1	20-08-2009	KEINE	
US 5692048 A	25-11-1997	KEINE	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC

(72)発明者 フローリアン クライトマイアー
ドイツ連邦共和国 ホーエンブルン アンドレアスシュティフトシュトラーセ 1
(72)発明者 アンドレアス ケプフ
ドイツ連邦共和国 ミュンヘン マクシミリアン－コルベ－アレー １７

Ｆターム(参考) 5J104 AA16 AA32 AA41 EA03 EA04 EA08 EA18 EA19 JA03 JA21
NA02 NA05 NA27 NA36 NA37 PA14