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

特許第4987939号
(P4987939)

(45)発行日　平成24年8月1日(2012.8.1)　(24)登録日　平成24年5月11日(2012.5.11)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	21/20	144D
G06K 17/00	(2006.01)	G06K	17/00	T
H04L 9/32	(2006.01)	G06K	17/00	F
		H04L	9/00	675A

請求項の数 8　(全 12 頁)

(21)出願番号	特願2009-234335 (P2009-234335)
(22)出願日	平成21年10月8日 (2009.10.8)
(65)公開番号	特開2010-134916 (P2010-134916A)
(43)公開日	平成22年6月17日 (2010.6.17)
審査請求日	平成21年10月8日 (2009.10.8)
(31)優先権主張番号	10-2008-0122747
(32)優先日	平成20年12月4日 (2008.12.4)
(33)優先権主張国	韓国 (KR)
(31)優先権主張番号	10-2009-0028572
(32)優先日	平成21年4月2日 (2009.4.2)
(33)優先権主張国	韓国 (KR)

(73)特許権者　596180076
韓國電子通信研究院
Electronics and Telecommunications Research Institute
大韓民国大田廣域市儒城區柯亭洞１６１
１６１ Kajong-dong, Yusong-gu, Taejon korea
(74)代理人　100075812
弁理士　吉武　賢次
(74)代理人　100088889
弁理士　橘谷　英俊
(74)代理人　100082991
弁理士　佐藤　泰和

最終頁に続く

(54)【発明の名称】保安モードに応じる手動型ＲＦＩＤ保安方法

(57)【特許請求の範囲】

【請求項１】

タグから第１ランダムナンバー、プロトコルコントロール情報、拡張プロトコルコントロール情報及び単一アイテム指示子情報を受信すると、前記第１ランダムナンバーを利用して第２ランダムナンバーを要請する段階；

前記タグから第２ランダムナンバーを受信すると、前記第２ランダムナンバーを含むメッセージを伝送しながら保安パラメターを要請する段階；

前記タグから暗号化されたデータを受信すると、認証サーバーに前記暗号化されたデータの認証結果を要請する段階；及び

前記認証サーバーから受信する前記暗号化されたデータの認証結果に応じて前記タグを認証する段階；

を含む保安方法。

【請求項２】

前記認証結果を要請する段階は、

前記保安パラメターを受信すると、前記タグに第２ランダムナンバーとリーダーが任意に生成されたランダムナンバーをパラメターとして前記暗号化されたデータを要請する段階；

前記タグから前記暗号化されたデータ及び前記暗号化されたデータを生成するために使用した暗号化ランダムナンバーを受信する段階；及び

前記認証サーバーに前記暗号化ランダムナンバー、前記リーダーが任意に生成されたラ

ンダムナンバー及び暗号化された認証データ、単一アイテム指示子情報及び第１ランダムナンバーを含んで前記暗号化された認証データの認証結果を要請する段階；
を含む、請求項１に記載の保安方法。
【請求項３】
前記認証サーバーが予め保存している前記単一アイテム指示子情報に対応する秘密キーを確認する段階；
前記第１ランダムナンバーと前記秘密キーを利用してセッションキーを生成する段階；
前記セッションキーを使用して前記暗号化ランダムナンバーを複号化しランダムナンバーを求める段階；
前記前記リーダーが任意に生成されたランダムナンバーと復号化された前記ランダムナンバーを利用して暗号化された認証データを求める段階；及び
前記求めた暗号化された認証データと前記受信した暗号化された認証データを比較して認証結果を生成して伝達する段階；
をさらに含むことを特徴とする、請求項２に記載の保安方法。
【請求項４】
前記拡張プロトコルコントロール情報には保安モード指示子が含まれている、請求項１に記載の保安方法。
【請求項５】
第１ランダムナンバーをパラメターとするメッセージをリーダーから受信すると、前記リーダーにプロトコル制御情報、拡張プロトコルコントロール情報及び単一アイテム指示子情報を伝送する段階；
前記第１ランダムナンバーをパラメターとするランダムナンバー要請メッセージを受信すると、第２ランダムナンバーを生成して前記リーダーに伝送する段階；及び
前記第２ランダムナンバーと前記リーダーが任意に生成したランダムナンバーをパラメターとする認証データ要請メッセージを受信すると、前記リーダーに暗号化された認証データと暗号化ランダムナンバーを伝達する段階；
と含む保安方法。
【請求項６】
前記暗号化ランダムナンバーを伝達する段階は、
前記リーダーが任意に生成したランダムナンバーをパラメターとする認証データ要請メッセージを受信する段階；
前記暗号化ランダムナンバーを生成する段階；
前記リーダーが任意に生成して伝送したランダムナンバーと前記ランダムナンバーを利用して認証データを作り、これを暗号化して暗号化された認証データを生成する段階；及び
前記リーダーに暗号化されたデータと暗号化ランダムナンバーを伝達する段階；
を含む、請求項５に記載の保安方法。
【請求項７】
前記拡張プロトコルコントロール情報には保安モード指示子が含まれている、請求項５に記載の保安方法。
【請求項８】
前記保安モード指示子は一般モード、認証モード、グループキー管理モード及び個別キー管理モードのうちのいずれかを示す、請求項７に記載の保安モードの保安方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は保安モードに応じる手動型ＲＦＩＤ保安方法に関するものである。
【背景技術】
【０００２】
半導体技術が発展することに伴って手動型ＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ

ＩＤｅｎｔｉｆｉｃａｔｉｏｎ、電波識別）タグでもＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）暗号アルゴリズムを駆動させる条件が作られている。これは保安技術適用の側面でデータを暗号化することができるということを意味する。つまり、自体の電源がなくてリーダーから電源の供給を受けなければならない手動型ＲＦＩＤタグでデータ暗号化を行なうようになると、これを利用して多様な保安プロトコルを実現することができる。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】ＵＳ２００７／１３３８０７Ａ１

【発明の概要】

【発明が解決しようとする課題】

【０００４】

この他に手動型ＲＦＩＤタグが保安強度または保安機能に応じて多様な保安モードに設定され得る。このような場合にはリーダーがタグの現在保安モードを確認し、それに適する保安機能を行なって当該ＲＦＩＤシステムが要求する保安強度を満足させなければならない。

【０００５】

つまり、従来は手動型ＲＦＩＤタグで暗号アルゴリズムの活用がなく、保安強度を示す保安モード活用がなくて柔軟な活用が難しいという問題があった。

【０００６】

したがって、本発明はＲＦＩＤリーダーがＲＦＩＤタグの保安モードを確認した後、保安モードに応じて認証プロトコルまたはデータ保護プロトコル動作を行うＲＦＩＤタグとリーダー間保安方法を提供する。

【課題を解決するための手段】

【０００７】

前記本発明の技術的課題を達成するための本発明の１つの特徴の保安方法は、

タグから第１ランダムナンバー、プロトコルコントロール情報、拡張プロトコルコントロール情報及び単一アイテム指示子情報を受信すると、前記第１ランダムナンバーを利用して第２ランダムナンバーを要請する段階；前記タグから第２ランダムナンバーを受信すると、前記第２ランダムナンバーを含むメッセージを伝送しながら保安パラメターを要請する段階；前記タグから暗号化されたデータを受信すると、認証サーバーに前記暗号化されたデータの認証結果を要請する段階；及び、前記認証サーバーから受信する前記暗号化されたデータの認証結果に応じて前記タグを認証する段階を含む。

【０００８】

前記本発明の技術的課題を達成するための本発明のまた他の特徴の保安方法は、第１ランダムナンバーをパラメターとするメッセージをリーダーから受信すると、前記リーダーにプロトコル制御情報、拡張プロトコルコントロール情報及び単一アイテム指示子情報を伝送する段階；前記第１ランダムナンバーをパラメターにするランダムナンバー要請メッセージを受信すると、第２ランダムナンバーを生成して前記リーダーに伝送する段階；及び、前記第２ランダムナンバーと前記リーダーが任意に生成したランダムナンバーをパラメターにする認証データ要請メッセージを受信すると、前記リーダーに暗号化された認証データと暗号化ランダムナンバーを伝達する段階を含む。

【発明の効果】

【０００９】

本発明によるとＲＦＩＤタグが自分の現在保安モードをリーダーに伝達するためにリーダーはＲＦＩＤタグの現在保安モードに応じて保安プロトコルを駆動させることができ、リーダーが保安モードを通じてタグの能力を知るために能力に適したプロトコルを動作させることができる。

【００１０】

また、複数のタグが存在する状況でもリーダーがタグとの通信を終了して継続してセッションを維持する必要がないためにリーダーと認証サーバー間の通信負担を減らすこともできる。

【図面の簡単な説明】

【００１１】

【図１】本発明の実施例にかかる保安モードを指示するデータフォーマットの例示図である。

【図２】本発明の実施例による応用サービス別保安ぜい弱性の例示図である。

【図３】本発明の実施例にかかるタグ認証モードの動作を示す流れ図である。

【発明を実施するための形態】

【００１２】

以下、添付した図面を参照して本発明の実施例について本発明が属する技術分野における通常の知識を有する者が容易に実施できるように詳しく説明する。しかし、本発明は多様で相異なる形態で実現することができ、ここで説明する実施例に限られない。また、図面で本発明を明確に説明するために説明上不要な部分は省略し、明細書全体にわたって類似の部分については類似の図面符号を付けた。

【００１３】

明細書全体である部分が何らかの構成要素を“含む”とする時、これは特に反対になる記載のない限り他の構成要素を除くことではなく他の構成要素をさらに含むことを意味する。

【００１４】

手動型ＲＦＩＤタグが付着される物品の高い保安強度を要求してＲＦＩＤタグ認証、ＲＦＩＤタグデータ気密性保護、ＲＦＩＤタグ無欠性保障などの保安機能が必要になると、このような保安機能を支援する演算能力を備え、それに適した保安モードを設定するＲＦＩＤタグを使用しなければならない。仮にＲＦＩＤタグデータ保護が必要なく単にＲＦＩＤタグ認証のみが必要な応用があるとすると、それに適する演算のみ処理して当該保安モードを設定すればよい。

【００１５】

つまり、本発明の実施例では応用が要求する保安強度を保安モードに設定し、ＲＦＩＤタグとリーダーが当該保安モードに応じて動作することによって応用が要求する保安サービスを提供し、最適化した演算を行なうことができる保安技術を提供する。本発明の実施例では手動型ＲＦＩＤタグの代表的な標準であるＩＳＯ/ＩＥＣ１８０００-６型Ｃ標準と互換性を有するように構成するか、必ずこれに限定されることではない。これについて以下で図面を参照して説明する。

【００１６】

図１は本発明の実施例にかかる保安モードを指示するデータフォーマットの例示図である。

【００１７】

図１に示されているように、１６ビットの拡張プロトコルコントロール（ＸＰＣ:Ｅｘｔｅｎｄｅｄ　Ｐｒｏｔｏｃｏｌ　Ｃｏｎｔｒｏｌ）データ構造が保安モード指示子を含むことができる。図１の保安モード指示子は２ビットで構成され、このビットが拡張プロトコルコントロールの余分のビットに含まれてもよい。

【００１８】

本発明の実施例では２ビットの保安モード指示子を利用するために全４個の保安モードを指示することができる。これに対して表１に保安モード別活用例及び保安モードフィールドを示した。表１について説明しながら本発明の実施例による応用サービス別代表的なサービスと、それについての保安考慮事項及びタグ認証モードの動作手続きについて図２及び図３を参照して説明する。

【表１】

［表１］

保安モード	特徴	効果	活用例	保安モードフィールド
モード１（非保安モード）	- UII露出 - 18000-6型C	-接近パスワード露出可能 -製品種類露出可能 -複製タグ登場可能 -タグ/リーダー通信データ盗聴可能	-単純物品認識	００
モード２（タグ認証モード）	- UII露出 -サーバーがタグ検証 -キーはタグとサーバーが共有 -認証プロトコル	-製品移動経路追跡可能 -タグ/リーダー通信データ 盗聴可能 -タグ珍品確認 -複製タグ防止(リーダーの悪意的な複製不可)	-農畜水産物珍品検証 -珍品の確認が必要な場合	０１
モード３（グループキー管理モード）	- UII保護 - タグ/リーダー通信データ保護 -フィーダーでグループキー管理 -データー保護プロトコル	-複製タグ防止(リーダーの悪意的なタグ複製可能) -製品移動経路追跡防止 -タグ/リーダー通信データ保護 -所有者プライバシー保護	-モバイルRFID -個人間所有権移転が必要な場合	１０
モード４（個別キー管理モード）	- UII保護 - タグ/リーダー通信データ保護 - UII別にキー管理	-複製タグ防止(リーダーの悪意的なタグ複製불가) -製品移動経路追跡防止 - タグ/リーダー通信データ保護 -所有者プライバシー保護	-農畜水産物珍品検証 -モバイルRFID -珍品確認/所有権移転が必要な場合	１１

【００１９】

まず、表１に示したように、保安モード値が００であるモード１は非保安モードとも言い、保安機能のない一般的なＩＳＯ/ＩＥＣ１８０００-６型Ｃ標準で動作するモードを意味する。この場合、ＲＦＩＤタグは単純にタグのＩＤ情報のみをリーダーに伝達し、リーダーは物品の情報をバックエンドネットワーク（Ｂａｃｋｅｎｄ Ｎｅｔｗｏｒｋ）を通じて別途のサーバーから収集する。

【００２０】

モード１の代表的なサービスとしては映画ポスターサービスがあり、これを含めて図２を参照して説明する。図２は本発明の実施例による応用サービス別代表的サービスとそれについての保安考慮事項の例示図である。

【００２１】

図２に示されているように、映画ポスターにＲＦＩＤタグが付着されていると、使用者はＲＦＩＤタグを読んでバックエンドサーバーから映画と関する情報を収集することができる。このようなサービスではＲＦＩＤタグのＩＤ情報が露出されても関係ないために認証及びデータ保護が要求されない。

【００２２】

次の表１の保安モード値が０１であるモード２はタグ認証モードとも言い、このモードの代表的なサービスは韓牛（韓国産牛）のような農畜水産物珍品検証サービスである。モード２の動作方法について説明すると、韓牛生産企業は韓牛にＲＦＩＤタグを付着して保安モード値を０１に設定した後、ＲＦＩＤタグに秘密キーを設定する。そして、韓牛生産企業は当該ＲＦＩＤタグの秘密キーを安全な認証サーバーに保存する。

【００２３】

韓牛販売店を訪問した消費者は陳列された韓牛に付着されたＲＦＩＤタグを通じて韓牛

の珍品可否を確認しようとする。この時、ＲＦＩＤタグを読んで珍品検証を行なうことができるリーダーは販売店のリーダーまたは消費者の携帯リーダーになり得る。このような場合、ＲＦＩＤタグの秘密キーが販売店のリーダーまたは消費者のリーダーに伝達されると悪意のある販売店または消費者によって複製されたＲＦＩＤタグが示される危険が存在する。

【００２４】

したがって、モード２ではリーダーは認証サーバーから認証結果のみの伝達を受けなければならない。本発明の実施例にかかるモード２はＩＳＯ/ＩＥＣ１８０００-６型Ｃ標準と互換性を有するように構成される。リーダーは認証サーバーと安全なチャンネルで通信すると仮定し、タグはＳｅｃＰａｒａｍ（Ｓｅｃｕｒｉｔｙ Ｐａｒａｍｅｔｅｒ、保安パラメター）を有していると仮定する。

【００２５】

保安パラメターは使用される暗号アルゴリズムと関する情報から構成された構造体であり、本発明の実施例では具体的な形態についての説明を省略する。本発明の実施例にかかるＲＦＩＤタグは内部に秘密キーが保存されていると仮定し、リーダーはタグの秘密キーを知らなく、単に認証サーバーのみがタグの秘密キー情報を有していると仮定する。モード２の動作手続きについて図３を参照して説明する。

【００２６】

図３は本発明の実施例にかかるタグ認証モードの動作を示す流れ図である。

【００２７】

図３に示されているように、リーダーはタグにクエリーメッセージを伝送する（Ｓ１００）。この時、クエリーメッセージに含まれて伝送されるパラメター（例えば、クエリー、Ｑｕｅｒｙ_Ａｄｊｕｓｔ、Ｑｕｅｒｙ_Ｒｅｐなど）は既に標準に定義されている命令語で、本発明の実施例では詳細な説明を省略する。クエリーメッセージを受けたタグはランダムナンバーを生成して（Ｓ１１０）第１ランダムナンバー（ＲＮ１６）に回答する（Ｓ１２０）。ここで、生成されたランダムナンバーは１６ビットであり、以下では説明の便宜上ＲＮ１６と言う。

【００２８】

タグから第１ＲＮ１６を受けたリーダーはランダムナンバーを受けたことを知らせると同時にタグからプロトコルコントロール（ＰＣ:Ｐｒｏｔｏｃｏｌ Ｃｏｎｔｒｏｌ）、拡張プロトコルコントロール（ＸＰＣ:Ｅｘｔｅｎｄｅｄ Ｐｒｏｔｏｃｏｌ Ｃｏｎｔｒｏｌ）及び単一アイテム指示子（ＵＩＩ:Ｕｎｉｑｕｅ Ｉｔｅｍ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）情報を受けるためにＡＣＫ（Ａｃｋｎｏｗｌｅｄｇｅ）メッセージをタグに伝送する（Ｓ１３０）。その後、ＡＣＫメッセージを受信したタグは自分のプロトコルコントロール、拡張プロトコルコントロール及び単一アイテム指示子情報を含むメッセージをリーダーに伝送する（Ｓ１４０）。ここで、プロトコルコントロール、拡張プロトコルコントロール及び単一アイテム指示子は公知の事項であるので、本発明の実施例では詳細な説明を省略する。

【００２９】

プロトコルコントロール、拡張プロトコルコントロール及び単一アイテム指示子情報を受信したリーダーは新たなランダムナンバーを要請するランダムナンバー要請Ｒｅｑ_ＲＮ命令をタグに伝送するが（Ｓ１５０）が、Ｓ１１０段階で受信したランダムナンバーである第１ＲＮ１６をパラメターとして有している。ランダムナンバーをパラメターとして含む理由は一種のタグアドレスまたはセッションＩＤの概念で、複数のタグがランダムナンバー要請メッセージを受信するとしてもＳ１１０段階で第１ランダムナンバーＲＮ１６を伝送したタグのみ自分に伝送されたメッセージであることを把握できるようにするためである。

【００３０】

ランダムナンバー要請メッセージを受信したタグは新たに使用するランダムナンバーを生成してリーダーに回答する（Ｓ１６０、Ｓ１７０）。この時、新しく生成したランダム

ナンバーも１６ビットで行われ、第２ＲＮ１６またはハンドル（Ｈａｎｄｌｅ）と言う。

【００３１】

次に、Ｓ１４０段階でタグがリーダーに伝送する拡張プロトコルコントロールに現在支援する保安モードが指示されているために、リーダーはＳ１８０段階乃至Ｓ２５０段階を通じてタグ認証モードで動作を行う。つまり、図１で示したように全１６ビットの拡張プロトコルコントロールデータ構造の保安モードフィールドに２ビットで保安モードを示す二進数“０１”を指示すると、リーダーはＳ１８０段階乃至Ｓ２５０段階までのタグ認証モードで動作を行う。

【００３２】

まず、リーダーはタグに保安パラメターを要請する命令である保安パラメター要請メッセージ（Ｇｅｔ_ＳｅｃＰａｒａｍ）を伝送する（Ｓ１８０）。この時、保安パラメター要請メッセージを伝送する時、Ｓ１７０段階でタグから受信した第２ＲＮ１６のハンドルを含んで伝送する。リーダーはタグの秘密キーを知らないために常に平文でデータを伝送する。リーダーから保安パラメター要請メッセージを受信したタグは保安パラメターを回答する（Ｓ１９０）。

【００３３】

リーダーはタグが有しているデータを暗号化した暗号データＡｕｔｈ_ｄａｔａを得るためにタグに暗号データ要請Ｒｅｑ_Ａｕｔｈ命令を伝達するが（Ｓ２００）、この命令はチャレンジ（ｃｈａｌｌｅｎｇｅ）用としてリーダーが生成した１６ビットのランダムナンバーであるＣｈ１６とＳ１７０段階で受信した第２ＲＮ１６であるハンドルをパラメターとして有する。暗号データ要請命令を受信したタグは暗号データを作るために新たなランダムナンバーであるｎｅｗＲＮ１６を生成し、このｎｅｗＲＮ１６とリーダーから受信したＣｈ１６を組み合わせて（ＸＯＲ）認証データを作った後、ｎｅｗＲＮ１６と認証データを暗号化する（Ｓ２１０）。

【００３４】

暗号化に使用されるセッションキーはタグが内蔵している秘密キーＫとＳ１１０段階で生成した第１ＲＮ１６から生成される。セッションキー生成方法については多様なアルゴリズムを利用することができ、本発明の実施例では具体的な方法を規定しない。その後、タグは暗号化されたｎｅｗＲＮ１６と認証データをパラメターとして含めてリーダーに回答する（Ｓ２２０）。この時、保安パラメター要請と認証データ要請に対する命令/応答メッセージフォーマットは表２乃至表５の通りである。

【表２】

［表２］

	命令(Command)	ランダムナンバー(RN)	CRC-16
サイズ(#of bits)	16	16	16
説明(description)	0xE101	ハンドル	

［表３］

	ヘッダ(Header)	保安パラメター(SecParam)	ランダムナンバー(RN)	CRC-16
サイズ(#of bits)	1	16	16	16
説明(description)	0 or 1	SecParam	ハンドル	

［表４］

	命令(Command)	チャレンジ	ランダムナンバー(RN)	CRC-16
サイズ(#of bits)	16	16	16	16
説明(description)	0xE104	Ch16	ハンドル	

［表５］

	命令(Command)	ランダムナンバー(RN)	認証データ(Auth_data)	ランダムナンバー(RN)	CRC-16
サイズ(#of bits)	16	16	16	16	16
説明(description)	0xE104	newRN16	Ch16⊕newRN16	ハンドル	

【００３５】

表２乃至表５の命令語コード（Ｃｏｍｍａｎｄ Ｃｏｄｅ）は例として挙げた値であるが、標準のＲｅｓｅｒｖｅｄ領域にある値のうちの１つであり、必ずこれに限定されることではない。

【００３６】

表２は保安パラメター要請メッセージでＳ１８０段階を通じてリーダーからタグに伝送されることであり、表３は保安パラメター要請メッセージに対する応答としてＳ１９０段階を通じてタグからリーダーに伝送されることである。表４は認証データ要請でＳ２００段階を通じてリーダーからタグに伝送されることであり、表５は認証データ要請に対する応答としてＳ２２０段階を通じてタグからリーダーに伝送されることである。この時、表５のランダムナンバーと認証データは暗号化された形態であり、残り値は平文で伝送され

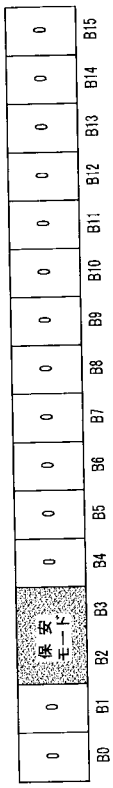
る。
【００３７】
図３を続けて説明すると、認証データまで受信したリーダーはタグとの通信を終了して認証サーバーとの通信を通じてタグが伝送してきた値を検証することによって珍品の可否を判断する。つまり、リーダーは認証サーバーにタグ認証要請（Ｒｅｑ_Ｖｅｒｉｆｙ）メッセージを伝送する（Ｓ２３０）。この時、メッセージに含まれるパラメターとしてはタグのＵＩＩ、第１ＲＮ１６、保安パラメター、Ｃｈ１６、Ｓ２２０段階で受けた暗号化された形態のｎｅｗＲＮ１６と認証データが含まれる。
【００３８】
認証サーバーはリーダーから受信したメッセージに基づいてタグに対する認証を行う（Ｓ２４０）。まず、認証サーバーはＵＩＩと関する秘密キーＫを検索し、第１ＲＮ１６とＫからセッションキーを生成する。セッションキー生成方法に対しては多様なアルゴリズムを使用することができるが、本発明の実施例ではタグとリーダーが同一なアルゴリズムを使用することを例に挙げて説明する。しかし、必ずこれに限定されることではない。認証サーバーがセッションキーを生成した後、セッションキーを利用して暗号化されたｎｅｗＲＮ１６を複号化しｎｅｗＲＮ１６を探索する。
【００３９】
Ｃｈ１６と探索したｎｅｗＲＮ１６を演算して（ＸＯＲ）認証データを求める。認証サーバーは自分が自体的に求めた認証データ値とリーダーから受信した認証データ値を比較する。比較を通じてもし２つの値が同一であれば認証に成功、同一でなければ認証に失敗したと判断する。また、これに対する結果をリーダーに回答する（Ｓ２５０）。このような手続きを通じてタグ認証モードの動作が行われる。
【００４０】
次の表１の保安モード値が１０であるモード３はグループキー管理モードとも言い、このモードの代表的なサービスはモバイルＲＦＩＤ技術を活用した個人所有物管理サービスである。ＲＦＩＤタグ付き製品を個人が購入して個人所有物になると、所有者がＲＦＩＤタグに直接秘密キーを入力しながら保安モード値を二進数“１０”に設定する。
【００４１】
このモードの主要特徴は個人所有化されたＲＦＩＤタグの単一アイテム指示子が暗号化されて伝送されるということである。また、キー管理が個人に任せられるためにグループキーとして管理される。ここで、グループキーとして管理されるということは、モード３の場合には秘密キーを知らなければ単一アイテム指示子を知るプロトコルを使用することができないために、所有者がＲＦＩＤタグ情報を活用するためには自分が所有した全てのタグの秘密キーを知らなければならない。しかし、単一アイテム指示子を知らない状況で所有者がすべてのタグの秘密キーを個別的に管理することはキー管理負担が大きいため、所有者は自分が所有した全てのタグに対して１つのグループとして認知して１つのグループキーとして管理する。
【００４２】
最後に表１の保安モード値が１１であるモード４は個別キー管理モードとも言い、モード２のタグ認証モードとモード３のキー管理モード特徴を同時に有する。モード４はＲＦＩＤタグ認証及びデータ保護が必要なすべてのサービスに活用することができる。
【００４３】
モード４でＲＦＩＤタグは自分の単一アイテム指示子を暗号化してリーダーに伝達するだけでなく、ＲＦＩＤタグに保存されたデータも暗号化されて伝送される。この時、暗号化に使用される秘密キーが個別ＲＦＩＤタグごとに異なって使用される。このような場合、リーダーがそれぞれのＲＦＩＤタグ秘密キーを使用するために保安性が強化される。本発明の実施例ではモード２に対する具体的なプロトコルは図３を通じて詳しく説明したが、モード３とモード４に対する具体的なプロトコルについては説明を省略する。
【００４４】
以上で説明した本発明の実施例は装置及び方法を通じてのみ実現されるわけではなく、

本発明の実施例の構成に対応する機能を実現するプログラムまたはそのプログラムが記録された記録媒体を通じて実現することもでき、このような実現は上述した実施例の記載から本発明が属する技術分野の専門家であれば容易に実現することができる。

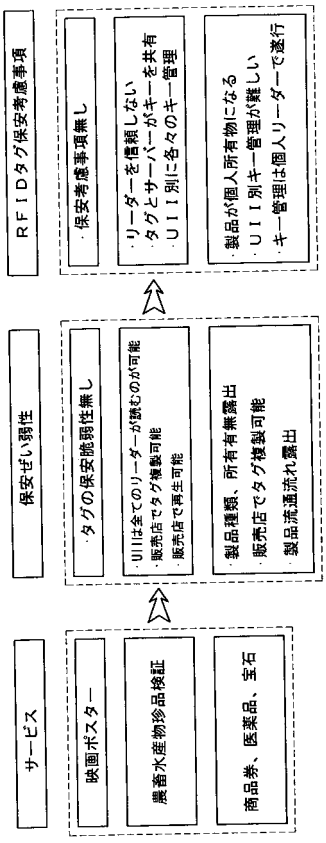
【００４５】

以上、本発明の実施例について詳細に説明したが、本発明の権利範囲はこれに限定されるわけではなく、請求範囲で定義している本発明の基本概念を利用した当業者の多様な変形及び改良形態もまた本発明の権利範囲に属する。

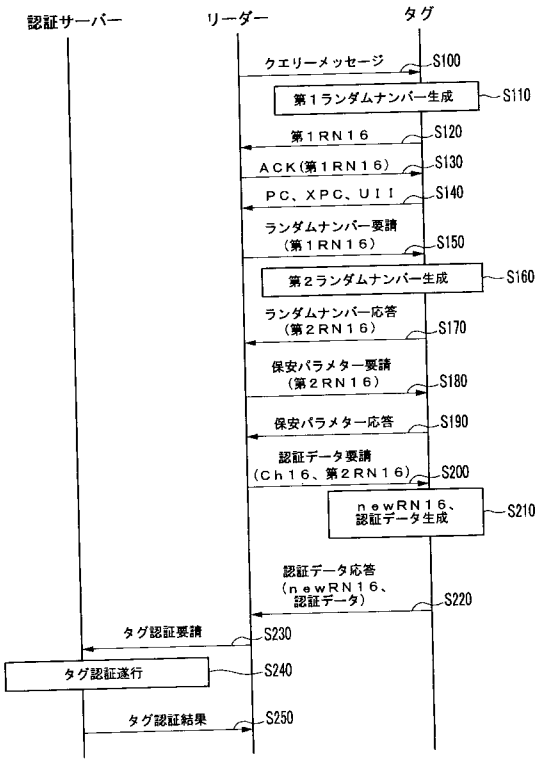
【図１】



【図２】



【図３】


認証サーバー
リーダー
タグ
クエリーメッセージ
S100
第１ランダムナンバー生成
S110
第１RN16
S120
ACK(第１RN16)
S130
PC、XPC、UII
S140
ランダムナンバー要請
(第１RN16)
S150
第２ランダムナンバー生成
S160
ランダムナンバー応答
(第２RN16)
S170
保安パラメター要請
(第２RN16)
S180
保安パラメター応答
S190
認証データ要請
(Ch16、第２RN16)
S200
newRN16、
認証データ生成
S210
認証データ応答
(newRN16、
認証データ)
S220
タグ認証要請
S230
タグ認証遂行
S240
タグ認証結果
S250

フロントページの続き

(74)代理人 100096921
弁理士 吉元 弘
(74)代理人 100103263
弁理士 川崎 康
(74)代理人 100118876
弁理士 鈴木 順生
(72)発明者 カン、ユー、スン
大韓民国テジョン、ユソン‐グ、シンソン‐ドン、テリム、デュレ、アパート、１０８－９０１
(72)発明者 チェ、ド、ホ
大韓民国チュンチョンナム‐ド、チョナン‐シ、チョンダン‐ドン、シンド、ブラニュー、アパート、１０１－５０１
(72)発明者 チェ、ヨン‐ジェ
大韓民国テジョン、ユソン‐グ、グワンピョン‐ドン、ハンワ、グメグリーン、アパート、１０４－２００２
(72)発明者 チュン、キョ、イル
大韓民国テジョン、ユソン‐グ、シンソン‐ドン、ハヌル、アパート、１０７－１１０２
(72)発明者 チョ、ヒュン、ソク
大韓民国テジョン、ユソン‐グ、グワンピョン‐ドン、テドク、テクノ、バリー、７‐ダンジ、クムソン、ベクジョ、アパート、７０１－５０１
(72)発明者 イ、ヒュン、スブ
大韓民国テジョン、ソ‐グ、マンニョン‐ドン、ガンビョン、アパート、１０７－９０４
(72)発明者 イ、サン、ヨウン
大韓民国テジョン、ソ‐グ、ドゥンサン‐ドン、センメオリ、アパート、２０１－１２０５
(72)発明者 イ、カン、ボク
大韓民国テジョン、ソ‐グ、ドゥンサン‐ドン、センメオリ、アパート、１０３－８０１
(72)発明者 シン、ドン‐ボム
大韓民国テジョン、ソ‐グ、ウォルピョン‐ドン、ベクハプ、アパート、１０１－９０５
(72)発明者 ジュン、ジェ‐ヤン
大韓民国テジョン、ユソン‐グ、ジジョク‐ドン、ヨルメ‐メウル、アパート、４０３－１４０５
(72)発明者 ピョ、チョル、シグ
大韓民国テジョン、ソ‐グ、マンニョン‐ドン、ガンビョン、アパート、１０９－７０１

審査官 平井 誠

(56)参考文献 特開２００７－２９３４８１（ＪＰ，Ａ）
特開２００８－０５９０１２（ＪＰ，Ａ）
特開２００８－２１７７６１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／
Ｇ０６Ｋ １７／００