(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 253 559 A2

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
30.10.2002 Patentblatt 2002/44

(51) Int Cl.[7]: **G07C 9/00**

(21) Anmeldenummer: **02009033.8**

(22) Anmeldetag: **23.04.2002**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **23.04.2001 DE 10119832**

(71) Anmelder: **SimonsVoss Technologies AG**
85774 Unterföhring (DE)

(72) Erfinder: **Voss, Ludger**
80469 München (DE)

(74) Vertreter: **VOSSIUS & PARTNER**
Siebertstrasse 4
81675 München (DE)

(54) **Kartenhalter und Verfahren zur Vereinigung von Firmenausweis und Schlüsselfunktion**

(57) Die Erfindung betrifft einen Kartenhalter und ein Verfahren zur Vereinigung von Firmenausweis und Schlüsselfunktion. Der erfindungsgemäße Kartenhalter zur Vereinigung von Firmenausweis und Schlüsselfunktion weist eine Identkartenleseeinrichtung sowie eine Nahbereichsfunkschnittstelle und eine Steuereinrichtung auf, die eine Kommunikation mit einem Elektronikzylinder einer Schließanlage ermöglichen.

EP 1 253 559 A2

Beschreibung

[0001] Die Erfindung betrifft einen Kartenhalter und ein Verfahren zur Vereinigung von Firmenausweis und Schlüsselfunktion. Heutzutage gehen viele Großunternehmen dazu über, die visuelle Identifizierungsfunktion (mittels Foto auf Firmenausweis) sowie eine elektronische Identifizierungsfunktion auf ein and dasselbe Identmedium - beispielsweise eine SmartCard - zu bringen. Diese Vereinheitlichung von Firmenausweisverwaltung und Schlüsselverwaltung führt zu gewissen Einsparpotentialen.

[0002] SmartCards stoßen jedoch bei der Realisierung einer Schlüsselfunktion schnell an ihre Grenzen: möchte man z.B. eine komplette Schließanlage eines Unternehmens mit SmartCards betreiben - und dies ist Vorraussetzung für eine sinnvolle Vereinheitlichung von Firmenausweis und Schlüsselfunktion -, so wird neben jeder Tür ein SmartCard-Lesegerät benötigt. Die Installation derartiger Lesegeräte ist jedoch sehr aufwendig: Wände sind aufzustemmen, eine Verkabelung mit einer zentralen Auswerteeinheit ist durchzuführen, ferner ist der Türrahmen zu bearbeiten, um einen Elektroöffner anzubringen. Da Elektroöffner nur die "Fallen"-Funktion eines Türschlosses freigeben, nicht jedoch die Riegelfunktion, sind derartige Installationen obendrein noch versicherungstechnisch problematisch.

[0003] Um derartige Installationsprobleme zu umgehen, befinden sich seit einigen Jahren elektronische Schließzylinder auf dem Markt. Diese Elektronikzylinder realisieren in sich leistungsfähige flexible (d.h. jederzeit umprogrammierbare) Zutrittskontrollsysteme und sind in wenigen Minuten montierbar, da sie dieselbe mechanische Schnittstelle haben wie herkömmliche Mechanikzylinder und obendrein ohne jede Verkabelung auskommen (es ist einfach der Mechanikzylinder gegen den Elektronikzylinder auszutauschen). Die Schlüsselfunktion zu derartigen verkabelungsfreien Elektronikzylindern wird durch aktive bzw. passive Transponder über eine Nahbereichsfunkschnittestelle realisiert (siehe beispielsweise DE-A-196 14 215, insbesondere Spalte 2, Zeilen 25-45).

[0004] Die Integration einer Nahbereichsfunktionsschnittstelle, insbesondere die Integration der sehr leistungsfähigen aktiven Transpondertechnologie in SmartCards ist technisch äußerst problematisch bzw. schlicht bereits zu spät, wenn beispielsweise ein Unternehmen bereits 10 000e von SmartCards an Mitarbeiter ausgegeben hat und die Sicherheitsinfrastruktur an diese Karten angepaßt ist - eine Umrüstung wäre sehr kostenintensiv.

[0005] Der Erfindung liegt die Aufgabe zu Grunde, einen Kartenhalter und ein Verfahren zur Vereinigung von Firmenausweis und Schlüsselfunktion bereitzustellen, die eine einfache Verbindung von Identkarte und Schlüsselfunktion ermöglichen. Diese Aufgabe wird mit den Merkmalen der Ansprüche gelöst.

[0006] Die Erfindung geht von folgendem Grundgedanken aus:

1. Die Nahbereichfunkschnittstelle wird in einen besonders angepaßten, vorzugsweise transparenten Kartenhalter integriert.

2. Dieser Kartenhalter weist die der Identkarte (z.B. SmartCard) fehlende Nahbereichsfunkschnittstelle, eine Identkarten-Leseeinheit, sowie eine geeignete Steuerungseinheit, die eine Kommunikation mit den Elektronikzylindern der Schließanlage ermöglicht, auf.

[0007] Grundidee des erfindungsgemäßen Verfahrens bzw. der erfindungsgemäßen Vorrichtung ist, daß der Kartenhalter ohne Karte völlig neutral und austauschbar ist. Eine Individualisierung dieser Kommunikationsschnittstelle mit den auf der Identkarte gespeicherten Identdaten des Kartenbesitzers erfolgt erst dann, wenn eine solche Identkarte in den erfindungsgemäßen Kartenhalter eingesteckt wird.

[0008] Der erfindungsgemäße Kartenhalter weist vorzugsweise eine mechanische Halteeinheit mit Identkartenleseeinrichtung, einen Taster, eine Stromversorgung (vorzugsweise Batterie), eine Sende-/Empfangseinrichtung für die drahtlose Kommunikation mit den elektronischen Schließvorrichtungen sowie einen Mikrocontroller auf. Der Mikrocontroller übernimmt die Ablaufsteuerung, die Ansteuerung der Funkschnittstelle und die Abarbeitung von Zutrittskontroll- bzw. Schlüsselinitialisierungstransaktionen über diese Schnittstelle sowie die Ansteuerung der Identkarten-Leseschnittstelle mit Datenver- und -entschlüsselung.

[0009] Auf der in den erfindungsgemäßen Kartenhalter einführbaren Identkarte befindet sich erfindungsgemäß ein geschützter Datenbereich, der genau die Informationen enthält, die ein elektronischer Schlüssel benötigt, um bestimmte Schließungen einer oder mehrerer verschiedener Schließanlagen öffnen zu können.

[0010] Diese Informationen werden durch einen oder mehrere Datensätze repräsentiert. Ein Datensatz besteht mindestens aus einer individuellen Schlüsselidentnummer, anhand derer eine Schließung ermitteln kann, ob dieser Schlüssel Zutritt hat oder nicht. Bei erhöhtem Sicherheitsbedarf enthält ein solcher Datensatz zusätzlich ein spezielles Paßwort, das Schließanlagenpaßwort, mit dessen Hilfe der Transponder z.B. via "Challenge-Response"-Verfahren der korrespondierenden Schließung beweisen kann, daß er von einer autorisierten Person initialisiert worden ist. Soll sich der Schlüssel in mehreren verschiedenen (n) Schließanlagen bewegen können, werden n Datensätze benötigt.

[0011] Auf diese Datensätze greift der erfindungsgemäße Kartenhalter schreibend (für Schlüsselinitialisierungsvorgänge) oder lesend (für die Abarbeitung von Zutrittskontrollaktionen mit einer elektronischen Schließung) zu. Die Daten werden verschlüsselt in der Identkarte abgelegt bzw. in verschlüsselter Form von dieser

zur Verfügung gestellt. Daher werden bei jedem Zugriff entsprechende Ver- bzw. Entschlüsselungsalgorithmen durch den Kartenhalter geführt.

[0012] Eine Zutrittskontrolltransaktion erfolgt wie im folgenden beschrieben. Bei Tastenbetätigung im Sendebereich eines elektronischen Schließzylinders werden zunächst die auf der Identkarte abgelegten Datensätze in den RAM-Bereich des Mikrocontrollers geladen und dort entschlüsselt. Anschließend führt der Kartenhalter mit der Schließung eine Zutrittskontrolltransaktion durch. Akzeptiert die Schließung Identnummer und Paßwort, so öffnet sie, anderenfalls eben nicht. Zuletzt löscht der Kartenhalter wieder die Datensätze in seinem Speicher, so daß er auf keinen Fall ohne Karte weiter benutzt werden kann.

[0013] Die Schlüsselinitialisierung mit dem erfindungsgemäßen Kartenhalter läuft wie folgt ab. Bei Tastenbetätigung im Sendebereich eines speziellen Programmiergerätes mit Funkschnittstelle werden zunächst Datensatzdaten über die Funkschnittstelle empfangen, auf Konsistenz überprüft, dann verschlüsselt und schließlich im geschützten Datenbereich der Identkarte als Datensatz abgelegt, so daß sie anschließend für Zutrittskontrolltransaktionen zur Verfügung stehen.

[0014] Die Erfindung ist mit verschiedenen Vorteilen verbunden. Da die einfach zu installierenden, kostengünstigen modernen Elektronikzylinder ein Nachrüsten kompletter Schließanlagen ermöglichen und mit dem erfindungsgemäßen Kartenhalter/dem erfindungsgemäßen Verfahren eine leistungsfähige Schnittstelle zu SmartCards erhalten, können Firmenausweisverwaltung und Schlüsselverwaltung konsequent und kostengünstig vereinigt und vereinheitlicht werden. Ferner wird der Kartenbesitzer gezwungen, Schlüsselverluste (d.h. Identkartenverluste) sofort zu melden und die Ausweisverwaltung kann schnell und einfach auf Schlüsselverluste reagieren; es ist einfach der betroffene Schließzylinder umzuprogrammieren. Wird die SmartCard genutzt, um Rechnerarbeitsplätze zu sichern, so zwingt Integration der Schlüsselfunktion den Benutzer, seine SmartCard mitzunehmen, wenn er seinen Arbeitsplatz verläßt und ihn so abzusichern.

[0015] Der Kartenhalter weist vorzugsweise eine Ansteckvorrichtung und/oder eine Anhängeöse auf, die seinem Träger das offene Tragen seines Firmenausweises ermöglicht.

Patentansprüche

1. Identkartenhalter zur Vereinigung von Firmenausweis und Schlüsselfunktion, mit einer Identkarten-Leseeinrichtung, sowie einer Steuerungseinrichtung und einer Nahbereichsfunkschnittstelle, die eine Kommunikation mit einem Elektronikzylinder einer Schließanlage ermöglichen.

2. Identkartenhalter nach Anspruch 1, wobei die Steuereinrichtung einen Mikrocontroller zum Ansteuern der Nahbereichsfunkschnittstelle und zum Ansteuern der Identkarten-Leseeinrichtung aufweist.

3. Identkartenhalter nach Ansprich 2, wobei der Mikrocontroller Zutrittskontrollund Schlüsselinitialisierungsaktionen über die Nahbereichsfunkschnittstelle abarbeitet.

4. Identkartenhalter nach Anspruch 2 oder 3, wobei der Mikrocontroller eine Datenver- und -entschlüsselung über die Identkarten-Leseeinrichtung ausführt.

5. Identkartenhalter nach einem der Ansprüche 1 bis 4, der zum Aufnehmen und zeitweiligen Halten einer Identkarte geeignet ausgebildet ist.

6. Zutrittskontrollverfahren mit den Schritten:

   a) Auslesen von Datensätzen, die Schließinformationen enthalten, aus einer Identkarte in einen Speicherbereich eines Mikrocontrollers eines die Identkarte haltenden Kartenhalters;
   b) Entschlüsseln der Datensätze
   c) Durchführen einer Zutrittskontrollaktion durch den Mikrocontroller; und
   d) Löschen der Datensätze im Mikrocontroller.

7. Verfahren nach Anspruch 6, wobei die Datensätze je eine individuelle Schlüsselidentnummer aufweisen.

8. Verfahren zum Vereinigen von Firmenausweis und Schlüsselfunktion mit den Schritten:

   A) Speichern verschlüsselter Datensätze, die Schließinformationen enthalten, auf einer Identkarte;
   B) Einführen der Identkarte in einen Kartenhalter gemäß einer der Ansprüche 1 bis 5;
   C) Durchführen eines Zutrittskontrollverfahrens nach Anspruch 6 oder 7.